ON THE COMPUTATION OF THE ZARISKI CLOSURE OF FINITELY GENERATED GROUPS OF MATRICES

KLARA NOSAN,[1] AMAURY POULY,[1,2] SYLVAIN SCHMITZ,[1,3] MAHSA SHIRMOHAMMADI,[1] AND JAMES WORRELL[2]

ABSTRACT. We investigate the complexity of computing the Zariski closure of a finitely generated group of matrices. The Zariski closure was previously shown to be computable by Derksen, Jeandel, and Koiran, but the termination argument for their algorithm appears not to yield any complexity bound. In this paper we follow a different approach and obtain a bound on the degree of the polynomials that define the closure. Our bound shows that the closure can be computed in elementary time. We also obtain upper bounds on the length of chains of linear algebraic groups, where all the groups are generated over a fixed number field.

1. INTRODUCTION

Finitely generated groups of matrices are fundamental mathematical objects that appear in a wide variety of areas in computer science, including algebraic complexity theory, quantum computation, dynamical systems, graph theory, control theory, and program verification. Unfortunately, matrix groups are challenging from the algorithmic point of view, with many natural problems being undecidable. For instance, already in the case of finitely generated subgroups of the group $SL_4(\mathbb{Z})$ of 4×4 integer matrices with determinant one, the membership problem and the conjugacy problem are undecidable [Mik66; Mil72].

In order to get a better handle on a finitely generated matrix group, it turns out to be worth over-approximating it by its Zariski closure. This closure is then a linear algebraic group and comes with a finite representation as an *algebraic variety*, i.e., as the locus of zeroes of a finite collection of polynomials. While this approximation is too coarse for solving the membership and conjugacy problems, it can nevertheless be extremely useful. Indeed, we gain access to a rich algorithmic toolbox, including Gröbner bases [BW93], Lie algebras [Gra17], and decision procedures for the first-order theories of algebraically closed fields and real closed fields [Ren92], that allows to manipulate the Zariski closure and solve other computational problems on this new representation.

A first case in point comes from the field of quantum computation. A "measure once" quantum finite automaton is essentially specified by a finite collection of unitary matrices of the same dimension, and a word is accepted if its value is strictly greater than a given threshold. As shown by Blondel, Jeandel, Koiran and Portier [BJKP05], the corresponding emptiness problem is decidable. This is somewhat miraculous considering that they also show that the non-strict version of the emptiness problem is undecidable, and considering that all versions of the language emptiness problem are undecidable for probabilistic automata, i.e., finite automata in which for each input letter the transition matrix is stochastic [Paz71; BC01]. The miracle is underpinned by two nontrivial facts. First, the Euclidean

closure of a group of unitary matrices is algebraic and therefore the Euclidean closure equals the Zariski closure. Second, there is an algorithm due to Derksen, Jeandel and Koiran [DJK05] to compute the Zariski closure of a finitely generated group of matrices. As noted in [BJKP05], quantum automata are not the sole application of the latter result: the question of whether a finite set of quantum gates is universal can be reduced to computing the Zariski closure of the associated group of unitary matrices. Decidability then follows by noting again that the (Euclidean) density of the group generated by those matrices can be tested on its Zariski closure using standard manipulations of algebraic varieties.

A second case in point comes from the field of program verification, where program invariants are a fundamental technique that allow one to compute an overapproximation of the set of reachable states (which is itself not-computable in general) and thereby verify whether a program meets a certain specification, such as loop termination. The crux of these techniques lies in being able to compute precise enough over-approximations [BM07]. A landmark 1976 result by Karr [Kar76] shows that the strongest affine invariant (or smallest linear variety, in the language of algebraic geometry) is computable in the case of so-called affine programs; those are programs having only non-deterministic (as opposed to conditional) branching and all of whose assignments are given by affine expressions. The problem of computing polynomial invariants rather than the coarser affine ones has been studied extensively and was finally answered positively in [HOPW18], wherein some of the authors extended the result of [DJK05] to compute the Zariski closure of finitely generated semigroups.

1.1. **Contributions.** The key result in the applications we mentioned above is the algorithm computing the Zariski closure of a finitely generated group of matrices due to Derksen, Jeandel and Koiran [DJK05]. Unfortunately, it is not clear how to analyse the complexity of this algorithm, or even whether it has an elementary complexity (see the discussion in Sec. 7.3 and App. C).

In this paper, we show that the Zariski closure of a finitely generated group of matrices is computable in elementary time. More precisely, we obtain a octuply exponential bound in the dimension and the number of the generators and the size of their entries (their height). We also obtain a quintuply exponential bound in the case where the group consists of orthogonal (or more generally unitary) transformations, as is always the case in quantum computing.

Degree Bound. Our main technical result is a quantitative structure lemma for algebraic groups, which may be of independent interest. It allows us to prove the following upper bound on the degree of the polynomials defining the Zariski closure of a finitely generated matrix group. Here, the *height* of a rational number $\frac{a}{b}$, with a, b coprime integers, is $\max(|a|, |b|)$, and its bitsize is the logarithm of its height. We denote by $\exp^k(x)$ iterated exponentiation in base 2, defined by $\exp^0(x) := x$ and $\exp^{k+1}(x) := 2^{\exp^k(x)}$.

Theorem 9 (Degree bound). *Let $n \in \mathbb{N}$ and let $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a finite set of matrices whose entries have height at most $h \in \mathbb{N}$. Then the Zariski closure of the group generated by S can be represented by finitely many polynomials of degree at most $(\log h)^{2^{|S|^{\exp^4(\mathrm{poly}(n))}}}$ with coefficients in $\mathbb{Q}$, forming a basis of the vanishing ideal of the group generated by S. Furthermore, if G contains only semisimple elements then the degree can be bounded by $(\log h)^{2^{|S|^{2^{\mathrm{poly}(n)}}}}$.*

Examples 13 and 14 in Sec. 7 show that the dependencies of the bound on the height h and the dimension n are unavoidable.

Our approach to proving Thm. 9 actually has more in common with an algorithm by Hrushovski for computing the Galois group of a linear differential equation [Hru02], than with the original algorithm from [DJK05]. Although Hrushovski's algorithm does not directly imply an algorithm to compute the Zariski closure of a finitely generated matrix group, our proof relies on a key insight about the structure of linear algebraic groups from [Hru02], namely the existence of a finite-index subgroup of computable degree that lies inside a given linear algebraic group; see Sec. 1.2 for an overview, and Secs. 2 to 5 for the main proof arguments.

Complexity of Computing the Zariski Closure. Now endowed with an *a priori* bound d on the degree of the polynomials that define a Zariski closure of a finitely generated matrix group, the closure itself can be computed using the following algorithm.

(1) There is a trivial reduction from computing the Zariski closure of a matrix group generated by a finite set S to computing the strongest polynomial invariant of an affine program [MS04]. Indeed, the group generated by S is the set of reachable configurations of an affine program with a single location and a single loop containing a nondeterministic choice between applying each generator in S; the strongest polynomial invariant of the program is then exactly the Zariski closure of the group generated by S.

(2) Müller-Olm and Seidl [MS04] show how to reduce the problem of computing the strongest polynomial invariant of degree at most d of an affine program with $m := n^2 + 1$ variables to that of computing the strongest affine invariant in higher dimension, and then apply a simplification of Karr's algorithm [Kar76], with an overall complexity of $O(|S| \cdot m^{3d})$ in the uniform cost model (i.e., every machine operation has constant cost).

The above algorithm together with the degree bound of Thm. 9 yields our main result.

Theorem 1 (Main result). *Let $n \in \mathbb{N}$ and let $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a finite set of matrices whose entries have height at most $h \in \mathbb{N}$. Then there is an algorithm that computes the Zariski closure of the group generated by S in time $2^{(\log h)^{2^{|S|^{\exp^4(\mathrm{poly}(n))}}}}$. The closure is represented by a finite basis of the vanishing ideal of the group generated by S.*

Chains of Linear Algebraic Groups. Finally, we also obtain an upper bound on the length of chains of linear algebraic groups generated over a fixed number field; see Sec. 6. This bound gives a quantitative version of the Noetherian property of subgroups of linear algebraic groups. In the case when all groups are generated by unitary matrices, the bound is singly exponential in the dimension of the matrices and degree of the number field over $\mathbb{Q}$.

1.2. **Overview.** Let us give a high-level account of the proof of the degree bound in Thm. 9. We also introduce some of the main definitions and notations along the way; we refer the reader to [Hum75] for more details. Throughout this section, we state the general definitions for a perfect field k with algebraic closure K, but our results will be framed in the case of $k = \mathbb{Q}$ the field of rational numbers and $K = \overline{\mathbb{Q}}$ the field of algebraic numbers.

1.2.1. *Algebraic Geometry.* Following a standard practice (see § 1.2.2), we are going to view our finitely generated matrix group as a subset $G \subseteq K^m$ of the affine space over K for some dimension m. Our overarching goal is to over-approximate G by

$$\mathbf{V}(I) := \{(a_1, \ldots, a_m) \in K^m : \forall f \in I, f(a_1, \ldots, a_m) = 0\} \tag{1}$$

the set of common zeroes of a set $I \subseteq K[x_1, \dots, x_m]$ of polynomials from the ring $K[x_1, \dots, x_m]$ of polynomials in variables $x_1, \dots, x_m$ and coefficients in K. Indeed, an (affine) *algebraic set* or *algebraic variety* $X \subseteq K^m$ is a set of the form $X = \mathbf{V}(I)$ for some $I \subseteq K[x_1, \dots, x_m]$; see [Hum75, Chap. 1]. In particular, X is

- *defined over k* if there exists a set $I \subseteq k[x_1, \dots, x_m]$ such that $X = \mathbf{V}(I)$,
- *d-bounded* if there exists a set $I \subseteq K[x_1, \dots, x_m]$ of polynomials all of degree at most $d \in \mathbb{N}$ such that $X = \mathbf{V}(I)$,
- *d-bounded over k* if there exists a set $I \subseteq k[x_1, \dots, x_m]$ of polynomials all of degree at most $d \in \mathbb{N}$ such that $X = \mathbf{V}(I)$.

Equation (1) provides a finitely represented approximation of G since, by Hilbert's Basis Theorem, there exists a finite subset $I' \subseteq I$ such that $\mathbf{V}(I) = \mathbf{V}(I')$. We want to compute the best possible such approximation, using the Zariski topology on K^m (that is, the topology whose closed sets are the algebraic sets): the *Zariski closure* $\overline{G}$ of a set $G \subseteq K^m$ is the smallest algebraic set that contains G.

1.2.2. *Linear Algebraic Groups.* A *linear group* over k is a subgroup of the *general linear group* $\mathrm{GL}_n(k)$ of all invertible $n \times n$ matrices with entries in k. We embed the latter as an algebraic set in K^m of dimension $m := n^2 + 1$ by writing

$$\mathrm{GL}_n(K) := \{(M, y) \in K^{n^2+1} : \det(M) \cdot y = 1\}. \tag{2}$$

A *linear algebraic group* is a Zariski-closed subgroup of $\mathrm{GL}_n(K)$ [Hum75, Chap. 7]. Given algebraic sets $X \subseteq K^m$ and $Y \subseteq K^p$, a *regular map* from X to Y is a function $\Phi \colon X \to Y$ defined by p polynomials $f_1, \dots, f_p \in K[x_1, \dots, x_m]$ by $\Phi(\boldsymbol{a}) := (f_1(\boldsymbol{a}), \dots, f_p(\boldsymbol{a}))$ for all $\boldsymbol{a} \in X$; regular maps are (Zariski) continuous [Hum75, Sec. 1.5]. Under the identification in (2), matrix multiplication is a regular map $\mathrm{GL}_n(K) \times \mathrm{GL}_n(K) \to \mathrm{GL}_n(K)$, and, by Cramer's rule, matrix inverse is also a regular map $\mathrm{GL}_n(K) \to \mathrm{GL}_n(K)$.

1.2.3. *Irreducible Sets and Connected Components.* An algebraic set $X \subseteq K^m$ is said to be *irreducible* if it is non-empty and cannot be written as the union $X = X_1 \cup X_2$ of two algebraic proper subsets X_1 and X_2. Because the Zariski topology is Noetherian, every algebraic set X can be written as the finite union of its *irreducible components*, i.e., of its maximal irreducible subsets. The closure $\overline{\Phi(X)}$ of the image of an irreducible set X under a regular map Φ is again irreducible [Hum75, Sec. 1.3].

As any linear algebraic group G is also an algebraic set, it is the finite union of its irreducible components, which turn out to be disjoint. We denote by G° the irreducible component of G containing the identity, called its *identity component*. Then G° is a normal subgroup of G and the irreducible components of G are the cosets of G° in G, called its *connected components* [Hum75, Sec. 7.3].

1.2.4. *Jordan-Chevalley Decomposition.* The starting point in the proof of Thm. 9 is the following decomposition of invertible matrices. Recall that a matrix $g \in \mathrm{GL}_n(k)$ is called *nilpotent* if there exists some positive integer p such that $g^p = 0$, it is *unipotent* if $g - \mathbb{1}$ is nilpotent (where $\mathbb{1}$ denotes the identity matrix), and *semisimple* if it is diagonalisable over K. The *Jordan-Chevalley decomposition* writes a matrix g as $g = g_s + g_n$, where g_s is semisimple, g_n is nilpotent, and g_s and g_n commute. It follows that $g = g_s g_u$, where $g_u := \mathbb{1} + g_s^{-1} g_n$ is unipotent, and g_s and g_u commute. This decomposition is unique. For a linear algebraic group G, we denote by $G_s := \{g_s : g \in G\}$ and $G_u := \{g_u : g \in G\}$ the semisimple and unipotent parts of G, respectively. It is a standard fact that both G_s and G_u are closed sets contained in G [Hum75, Sec. 15.3], but note that they might not be groups.

1.2.5. *Main Argument (Section 5).* Let $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a finite set of rational matrices and consider the closure $G = \overline{\langle S \rangle} \leq GL_n(\overline{\mathbb{Q}})$ of the group generated by S. Let $U := \overline{\langle G_u \rangle}$ be the closure of the group generated by G_u as per §1.2.4; note that U might contain non-unipotent elements. Our main technical result proven in Sec. 4 and summarised next in §1.2.6 identifies a subgroup H of G with good properties.

Lemma 7 (Quantitative Structure Lemma)**.** *Let* $n \in \mathbb{N}$, $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ *be a set of matrices, and* $G = \overline{\langle S \rangle}$. *Write* $U := \overline{\langle G_u \rangle}$ *for the closure of the subgroup generated by the unipotent elements of* G. *Then there exists a closed normal subgroup* H *of* G *such that* $U \trianglelefteq H \trianglelefteq G$ *and*

    (i) H/U *is commutative,*
    (ii) H *is a normal subgroup of* G *of index at most* $J'(n) := (2[(n^2 + D)^{4D^2} + 1]^2)!$, *where* $D := (n^3 + 1)^{2^{3n^2}}$.

We exploit these two properties in Sec. 5 to obtain a degree bound for G as follows.

    (1) We find a finite set of generators S' for $H = \overline{\langle S' \rangle}$ using the finite-index property. This relies on Schreier's Lemma; see Lem. 8 in Sec. 5.
    (2) We deduce a degree bound for H using the commutativity of H/U. Indeed, we have that
$$H = \overline{\left(\prod_{g \in S'} \overline{\langle g \rangle} \right) \cdot U}\ .$$

    In other words, we only need to compute the closure of individual elements $\overline{\langle g \rangle}$ for $g \in S'$. The latter can be done using Masser's bound on the group of multiplicative relations among the eigenvalues of a rational matrix; see Thm. 15 and Claim 9.3 in App. B.
    (3) Finally, by writing G as the union of $J'(n)$ cosets of H, we obtain a degree bound on G from the degree bound on H.

1.2.6. *Quantitative Structure Lemma (Sections 3 and 4).* Here we borrow several insights from Hrushovski's approach on proto-Galois groups [Hru02] and Feng's complexity analysis of the algorithm [Fen15]. First of all, and drawing from the works of Hrushovski and Feng, we show in Sec. 3 that $U = \overline{\langle G_u \rangle}$ is normal in G and that one can write polynomials for U whose degree depends only on the dimension n.

We use the fact that the quotient of the linear algebraic group G by its normal subgroup U is a linear algebraic group of higher dimension, which can be obtained through the *quotient map* $\phi_U \colon G \to \mathrm{GL}_p(\overline{\mathbb{Q}})$ [Hum75, Sec. 11.5]. This is a regular map that is also a group homomorphism (thus $G/\ker \phi_U \cong \phi_U(G)$ by the First Isomorphism Theorem) such that $U = \ker \phi_U$. Furthermore, since U contains G_u, we know that the quotient G/U consists solely of semisimple elements when viewed as a subgroup of $\mathrm{GL}_p(\overline{\mathbb{Q}})$. Then we can apply the following lemma, summarised next in §1.2.7, that yields another linear algebraic group P, called the *pistil* of G/U.

Lemma 4 (Pistil Lemma)**.** *Let* $n \in \mathbb{N}$, $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ *be a set of semisimple matrices, and* $G = \overline{\langle S \rangle}$. *Then there exists a closed group* $P \leqslant \mathrm{GL}_n(\overline{\mathbb{Q}})$ *such that*

    (i) P *is commutative,*
    (ii) $G \cap P$ *is a normal subgroup of* G *of index at most* $J(n) := (2(n^2 + 1)^2)!$.

The idea is then to "pull-back" the pistil P from G/U through the quotient map ϕ_U to the original group G. We use the following quantitative statement with a bound on the degree of the polynomials defining the quotient map and a bound on the dimension.

$$\mathrm{GL}_n(\overline{\mathbb{Q}}) \qquad\qquad \mathrm{GL}_p(\overline{\mathbb{Q}}) \qquad\qquad \mathrm{GL}_q(\overline{\mathbb{Q}})$$

$$\begin{array}{ccc}
 & \text{semisimple} & \text{finite} \\
G \xrightarrow{\ \ \phi_U\ \ } & G/U \xrightarrow{\ \ \phi_P\ \ } & \phi_P(G/U) \\
\text{Lem. 7} \Big\updownarrow & \Big\updownarrow \text{Lem. 4} & \\
H \xleftarrow{\ \ \phi_U^{-1}\ \ } & P \xleftarrow{\ \ \text{finite index property}} &
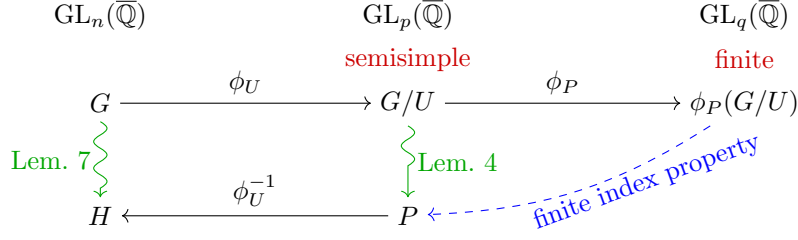\end{array}$$

FIGURE 1. Assembling the arguments of Lems. 4 and 7: we take two consecutive quotients to obtain a finite group. We then pull-back to obtain a group H with the desired properties. Note that the dimension increases after each quotient and the lemmata relate p and q to n.

Theorem 2 ([Fen15, Prop. B.6]). *Let $d, n \in \mathbb{N}$ and let $G \subseteq \mathrm{GL}_n(K)$ be a closed group. Let H be a normal subgroup of G that is d-bounded over k. Then there exists $p \leqslant (n^2 + d)^{2d^2}$ and a homomorphism $\phi_H \colon G \to \mathrm{GL}_p(K)$ defined by polynomials over k of degree bounded by $d(n^2 + d)^{2d^2+1}$ such that $H = \ker \phi_H$.*

Using Thm. 2 as described in Fig. 1, we define $H \leq \mathrm{GL}_n(\overline{\mathbb{Q}})$ to be the preimage of the pistil P under ϕ_U. Thanks to the properties of P and ϕ_U, H has the properties desired for the proof of Thm. 9, namely H is a normal subgroup of G of finite index depending only on n, and H/U is commutative.

1.2.7. *Pistil Lemma (Section 2).* Let $G = \overline{\langle S \rangle} \leqslant \mathrm{GL}_p(\overline{\mathbb{Q}})$ be the closure of a group generated by a set S of rational matrices. Assume that G consists exclusively of semisimple elements.

Since the identity component G° of G is connected and semisimple, it is a *torus* [Bor66, Thm 3.1]. As stated above in §1.2.3, G° is a normal subgroup of G and G/G° is finite. However we do not know how to directly bound the degree of G° nor the cardinality of G/G° in terms of the set S of generators and the dimension p. Instead, again following [Hru02], we identify another group $P \leqslant \mathrm{GL}_p(\overline{\mathbb{Q}})$, dubbed the *pistil* of G, and defined as the intersection of all the maximal tori that contain G°. This construction is explained in Sec. 2. Since maximal tori are 1-bounded, commutative, and closed, P is also 1-bounded, commutative, and closed. Observe that the quotient $G/(G \cap P)$ is finite because $G \cap P$ includes G°. We can bound the index $[G : G \cap P]$ of this quotient in terms of p, using the fact that the quotient map ϕ_P defined by Thm. 2 embeds into a *finite* subgroup of $\mathrm{GL}_q(\overline{\mathbb{Q}})$ for some q depending only on p; see Fig. 1.

1.2.8. *About Field Extensions.* The reader might have noticed that, in order to apply Thm. 2, we need to show that H is d-bounded *over* $\mathbb{Q}$. We resort routinely to the following folklore lemma, where L/k is any field extension and $\mathrm{Aut}(L/k)$ the group of automorphisms of L that fix k (see App. A for a proof).

Lemma 3. *Fix $m \in \mathbb{N}$, and let $X \subseteq L^m$ be a d-bounded algebraic set. Then X is d-bounded over k if any of the following holds:*

  (i) *X is stable under $\mathrm{Aut}(L/k)$ for some subfield k of L, or*
  (ii) *$X \cap k^m$ is dense in X.*

Lem. 4
$\mapsto P \leqslant \mathrm{GL}_n(\overline{\mathbb{Q}})$
$\mapsto G^\circ \lhd (G \cap P) \lhd G$
$\mapsto [G : G \cap P] \leqslant J(n)$
$\mapsto P$ is commutative
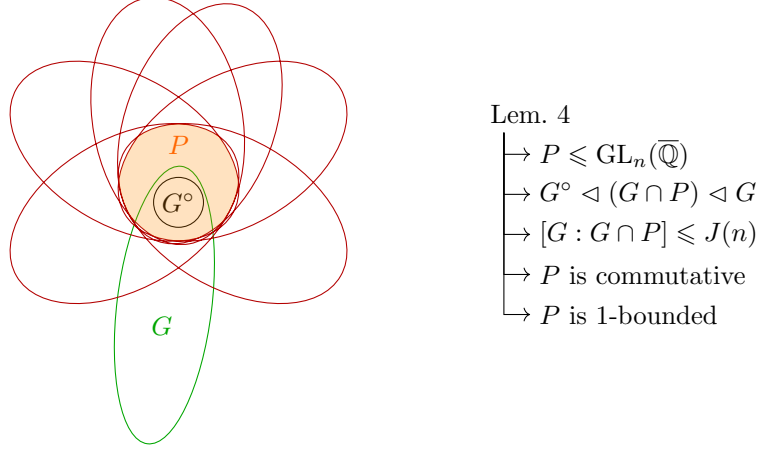$\mapsto P$ is 1-bounded

FIGURE 2. Graphical representation of Lem. 4: given a group $G = \overline{\langle S \rangle}$ for $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ a set of semisimple matrices, we define the pistil P as the intersection of the maximal tori containing G°; note that P is not necessarily a subgroup of G.

2. PISTIL LEMMA

Recall that a matrix $g \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ is *semisimple* if it is diagonalisable over $\overline{\mathbb{Q}}$. In this section, we study structural properties of algebraic groups $G = \overline{\langle S \rangle}$ defined as closures of groups of semisimple rational matrices. (We note in passing that such a group G need not be "semisimple as a subgroup" of $\mathrm{GL}_n(\overline{\mathbb{Q}})$, that is, conjugate to a group of diagonal matrices.) We show that such groups are virtually abelian: they contain an abelian subgroup of finite index. We define for this a group $P \leqslant \mathrm{GL}_n(\overline{\mathbb{Q}})$, which we call the *pistil* of G, and show that $P \cap G$ is a normal abelian subgroup of G with finite index.

Lemma 4 (Pistil Lemma). *Let $n \in \mathbb{N}$, $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a set of semisimple matrices, and $G = \overline{\langle S \rangle}$. Then there exists a closed group $P \leqslant \mathrm{GL}_n(\overline{\mathbb{Q}})$ such that*

(i) *P is commutative,*
(ii) *$G \cap P$ is a normal subgroup of G of index at most $J(n) := (2(n^2 + 1)^2)!$.*

Proof. The group P will be defined to encompass the identity component G° of G. By definition, G° is connected, and by assumption, G° is comprised exclusively of semisimple elements. Such groups are known as algebraic tori [Bor66, Thm 3.1]. Formally, an *algebraic torus* (henceforth simply a *torus*) is defined to be a connected group $T \leqslant \mathrm{GL}_n(\overline{\mathbb{Q}})$, consisting solely of semisimple elements. Equivalently, T is a torus if it is a connected diagonalisable subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}})$. Furthermore, it holds that the *maximal tori* in $\mathrm{GL}_n(\overline{\mathbb{Q}})$ are exactly those groups that are conjugate to the group of diagonal matrices in $\mathrm{GL}_n(\overline{\mathbb{Q}})$. Now G°, being a torus, is contained in some maximal torus in $\mathrm{GL}_n(\overline{\mathbb{Q}})$. We define the *pistil* of G to be the intersection of all maximal tori in $\mathrm{GL}_n(\overline{\mathbb{Q}})$ that contain G°; see Fig. 2, where the maximal tori containing G° are depicted as red ellipses. We now show that the pistil P has all the announced properties.

First note that, as an intersection of closed groups, P is closed.

Regarding (i), observe that the commutativity of P follows from the fact that it is obtained by intersecting commutative groups.

Regarding (ii), to prove that $G \cap P$ is a normal subgroup of G, it suffices to observe that the collection of all maximal tori containing G° is stable under conjugation by

all elements $g \in G$, and hence so is P. More precisely, fix $g \in G$ and observe that for every maximal torus T containing G°, gTg^{-1} is also a maximal torus, which moreover contains G° because $gG^\circ g^{-1} = G^\circ$ since G° is a normal subgroup of G. We thus see that conjugation by g induces a bijective self-map on the collection of maximal tori containing G°. It follows that $gPg^{-1} = P$ for all $g \in G$, i.e., G normalises P and hence $G \cap P$ is a normal subgroup of G.

The main difficulty of the proof lies in computing an upper bound on the index $[G : G \cap P]$. For this, we will argue that the quotient $G/(G \cap P)$ can be embedded as a finite subgroup of rational matrices in $\mathrm{GL}_p(\mathbb{Q})$ for some p. Recall from [KP02] that such a finite subgroup of rational matrices is conjugate to a finite subgroup of integer matrices, and furthermore that the order of any such finite subgroup of integer matrices divides $(2p)!$ [New72; GL06; BHKST20].[1]

Fact 4.1. For all $p \in \mathbb{N}$, every finite subgroup of $\mathrm{GL}_p(\mathbb{Q})$ has order at most $(2p)!$.

By Fact 4.1, the size of the quotient $G/(G \cap P) \in \mathrm{GL}_p(\mathbb{Q})$ depends on the dimension p, which in turn by Thm. 2 depends on n and the maximal degree of the defining polynomials of $G \cap P$. The latter is not directly accessible to us; however, we first show the following claim and will later bound p through the pistil and its normaliser.

Claim 4.1. P is 1-bounded over $\mathbb{Q}$.

Proof. Recall that all maximal tori of $\mathrm{GL}_n(\overline{\mathbb{Q}})$ are conjugate to the group of all diagonal matrices in $\mathrm{GL}_n(\overline{\mathbb{Q}})$ and hence 1-bounded. As P is defined to be the intersection of maximal tori, it follows that P is 1-bounded too. We further show that P is stable under $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$. Indeed, since G is defined over $\mathbb{Q}$, it is stable under the action $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathbb{Q}^{n^2+1}$. Now observe that all automorphisms $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ preserve connectedness, and thus permute the connected components of G. Note also that all automorphisms fix the identity matrix, and therefore must fix the connected component containing it, that is G°. Finally, the automorphisms in $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ also preserve maximality, and hence permute all maximal tori of $\overline{\mathbb{Q}}$. It follows that P, being the intersection of all maximal tori of $\mathrm{GL}_n(\mathbb{Q})$, is stable under $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$, and thus we can apply Lem. 3(i) to conclude the proof. $\triangleleft$

It remains to show that the index of the normal subgroup $G \cap P$ in G is bounded by $J(n)$. Let $N := \{g \in \mathrm{GL}_n(\overline{\mathbb{Q}}) : gP = Pg\}$ be the *normaliser* of P in $\mathrm{GL}_n(\overline{\mathbb{Q}})$, that is, the largest subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}})$ that normalises P. In particular, G is a subgroup of N.

Since P is defined over $\mathbb{Q}$, by quantifier elimination, N is also defined over $\mathbb{Q}$. Since P is both 1-bounded over $\mathbb{Q}$ (Claim 4.1) and a normal subgroup of N, by Thm. 2, there is a homomorphism $\phi_P \colon N \to \mathrm{GL}_p(\overline{\mathbb{Q}})$, for some $p \leq (n^2 + 1)^2$, such that ϕ_P has kernel P and is defined over $\mathbb{Q}$.

As $G \leqslant N$, we can look at the image of G under ϕ_P. Since G° has finite index in G and $G^\circ \subseteq P$, $G \cap P$ also has finite index in G, and therefore $\phi_P(G)$ is finite.

Furthermore, since $G = \overline{\langle S \rangle}$ for $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ and ϕ_P is defined over $\mathbb{Q}$, the rational points of $\phi_P(G)$ are dense in $\phi_P(G)$, that is, $\overline{\phi_P(G) \cap \mathbb{Q}^{p^2+1}} = \phi_P(G)$. Since $\phi_P(G)$ is finite, $\overline{\phi_P(G) \cap \mathbb{Q}^{p^2+1}} = \phi_P(G) \cap \mathbb{Q}^{p^2+1} = \phi_P(G)$ is a finite subgroup of $\mathrm{GL}_p(\mathbb{Q})$. The bound $J(n)$ on the index of $G \cap P$ now follows from Fact 4.1. $\square$

---

[1]Friedland [Fri97] showed that the better bound $2^n n!$ holds for all $n \geq 72$ but this relies on an incomplete manuscript by Weisfeiler [Wei85].

3. Unipotent-Generated Groups

Recall that a matrix $g \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ is unipotent if $(g - \mathbb{1})^n = 0$. In this section, we investigate for a given algebraic group G the closure U of the group generated by the unipotent elements of G. We remark that in general U need not consist exclusively of unipotent elements (that is, U differs in general from the so-called unipotent radical of G). We use instead the fact, noticed by Hrushovski [Hru02] and analysed more precisely by Feng [Fen15], that the closure of the group generated by the unipotent elements shares underlying similarities with the unipotent radical.

Before proceeding with the proof we recall the definition of matrix exponential and matrix logarithm [Hum75, Sec. 15.1]. Given a matrix $g \in \mathrm{GL}_n(\overline{\mathbb{Q}})$, its exponential is defined by $\exp(g) := \sum_{n=0}^{\infty} \frac{g^n}{n!}$.

A matrix g' is said to be a *matrix logarithm* of g if $\exp(g) = g'$. Since the exponential function is not one-to-one in $\overline{\mathbb{Q}}$, some matrices may have more than one logarithm. However, for a unipotent matrix g we can define the logarithm uniquely as $\log(g) := \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(g-\mathbb{1})^n}{n}$.

We also use the fact that, given a polynomial ideal, we have the following degree bound due to Dubé [Dub90] on the generators of the elimination ideal obtained by eliminating some of the variables.

Proposition 5 ([Dub90, Cor. 8.3]). *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal generated by polynomials with degree at most d. Then for all $i \in \{1, \ldots, n\}$ the elimination ideal $I \cap K[x_1, \ldots, x_i]$ is generated by polynomials with degree at most $(d+1)^{2^n}$.*

Lemma 6. *Let $n \in \mathbb{N}$ and $G \leqslant \mathrm{GL}_n(\overline{\mathbb{Q}})$ be defined over $\mathbb{Q}$. Let $U = \overline{\langle G_u \rangle}$ be the closure of the subgroup generated by the unipotent elements of G. Then U is a normal subgroup of G which is $(n^3 + 1)^{2^{3n^2}}$-bounded over $\mathbb{Q}$.*

Proof. Consider an arbitrary $g \in G$. Observe that the set G_u is closed under conjugation by g. Therefore $\langle G_u \rangle$ is also closed under conjugation by g. By Zariski continuity of conjugation, the closure $U = \overline{\langle G_u \rangle}$ of the group generated by the unipotent elements of G is also closed under conjugation by g, i.e., $gUg^{-1} = U$. Since $g \in G$ was arbitrary, U is a normal subgroup of G.

The degree bound in the following claim comes from [Fen15, Lemma B.8]; note that it only depends on the dimension.

Claim 6.1. U is irreducible and $(n^3 + 1)^{2^{3n^2}}$-bounded over $\mathbb{Q}$.

Proof. By [Gra17, Lem. 4.3.9], for any $h \in G_u$, there is a unique nilpotent matrix $\log(h)$ such that $h = \exp(\log(h))$. We furthermore have that $\overline{\langle h \rangle}$ is the closure of the image of the map $\Phi_h \colon \overline{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{Q}})$ given by $\Phi_h(z) := \exp(z \log(h))$. Indeed, Φ_h is a polynomial in z of degree at most n by the nilpotency of $\log(h)$, hence Zariski-continuous, hence $\overline{\langle h \rangle} = \overline{\Phi_h(\mathbb{Z})} = \overline{\Phi_h(\overline{\mathbb{Z}})} = \overline{\Phi_h(\overline{\mathbb{Q}})}$ is irreducible.

We recall a standard fact that given two irreducible varieties J and J', the cartesian product $J \times J'$ is again irreducible [see, e.g. Gra17, Thm. 1.1.9]. Since matrix multiplication is a regular map, $\overline{J \cdot J'}$ is then irreducible as well. As recalled later in Sec. 6.1, any strictly increasing chain of irreducible algebraic subsets of $\mathrm{GL}_n(\overline{\mathbb{Q}})$ has length at most $\dim(\mathrm{GL}_n(\overline{\mathbb{Q}})) = n^2$. Thus there exists $\ell \leq n^2$ and $h_1, \ldots, h_\ell \in G_u$ with

$$U = \overline{\overline{\langle h_1 \rangle} \cdots \overline{\langle h_\ell \rangle}} = \overline{\{\Phi_{h_1}(z_1) \cdots \Phi_{h_\ell}(z_\ell) : z_1, \ldots, z_\ell \in \overline{\mathbb{Q}}\}} .$$

In other words, U is the Zariski closure of the image of $\overline{\mathbb{Q}}^\ell$ under a polynomial map of degree at most n^3 with $n^2 + 1$ variables defining U and ℓ variables used in the polynomials $\Phi_{h_i}(z_i)$. Furthermore, by above it follows that U is irreducible.

We use Prop. 5 to eliminate all z_i. Therefore U is bounded by $(n^3 + 1)^{2^{(2n^2+1)}} \leq (n^3 + 1)^{2^{3n^2}}$. Furthermore, since both G and the collection of unipotent matrices in $\mathrm{GL}_n(\overline{\mathbb{Q}})$ are stable under $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$, U is also stable under $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Lem. 3(i), it follows that U is bounded by $(n^3 + 1)^{2^{3n^2}}$ over $\mathbb{Q}$. $\triangleleft$

This concludes the proof of Lem. 6. $\square$

4. Quantitative Structure Lemma

We now move to the general structural analysis described in §1.2.6, where we analyse an arbitrary algebraic group to identify a normal subgroup H with the following properties.

Lemma 7 (Quantitative Structure Lemma)**.** *Let $n \in \mathbb{N}$, $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a set of matrices, and $G = \overline{\langle S \rangle}$. Write $U := \overline{\langle G_u \rangle}$ for the closure of the subgroup generated by the unipotent elements of G. Then there exists a closed normal subgroup H of G such that $U \trianglelefteq H \trianglelefteq G$ and*

(i) *H/U is commutative,*
(ii) *H is a normal subgroup of G of index at most $J'(n) := (2[(n^2 + D)^{4D^2} + 1]^2)!$, where $D := (n^3 + 1)^{2^{3n^2}}$.*

Proof. Since G is an algebraic set, it is d-bounded for some $d \in \mathbb{N}$. We further have that the set of rational points of G is dense in G, hence by Lem. 3(ii), G is defined over $\mathbb{Q}$.

By Lem. 6, the closure U of the subgroup generated by the unipotent elements of G is a normal subgroup of G bounded by $D := (n^3 + 1)^{2^{3n^2}}$ over $\mathbb{Q}$. We can thus use Thm. 2 to obtain a homomorphism $\phi_U \colon G \to \mathrm{GL}_p(\overline{\mathbb{Q}})$ defined over $\mathbb{Q}$, with kernel U, where $p \leq (n^2 + D)^{2D^2}$. The image $\phi_U(G)$ of G under ϕ_U is isomorphic to G/U and will not have any (non-trivial) unipotent elements. Indeed, if $\phi_U(g)$ were unipotent, then g would also be, thus $g \in U$, hence $\phi_U(g) = \mathbb{1}$ would be the identity.

We apply Lem. 4 to $\phi_U(G)$ and examine the pistil P of $\phi_U(G)$. Recall that P is closed and commutative, and $\phi_U(G) \cap P$ is a normal subgroup of $\phi_U(G)$ of index at most $J(p)$. We define the group H as the preimage of the pistil P by ϕ_U. That is, we set $H := \phi_U^{-1}(P) \subseteq G$; see Fig. 3 for a depiction. Since P is closed, its pre-image H through the regular map ϕ_U is also closed. Since $U = \ker(\phi_U)$, we have $U \subseteq H$ and therefore U is a normal subgroup of H, ensuring that the quotient H/U is well-defined.

Regarding (i), we observe that ϕ_U induces an injective homomorphism between H and P, which is commutative, and therefore H/U is also commutative.

Regarding (ii), consider the homomorphism

$$\psi \colon G \to \phi_U(G)/(\phi_U(G) \cap P)$$

obtained by composing ϕ_U with the natural quotient map. Since

$$\phi_U^{-1}(\phi_U(G) \cap P) = \phi_U^{-1}(\phi_U(G)) \cap \phi_U^{-1}(P) = G \cap H = H,$$

the map ψ has kernel H, which implies by the First Isomorphism Theorem that H is a normal subgroup of G and

$$\begin{aligned}
[G : H] &= [G : \ker \psi] = |\psi(G)| = [\phi_U(G) : \phi_U(G) \cap P] \\
&\leq J(p) = (2[(n^2 + D)^{4D^2} + 1]^2)! \ .
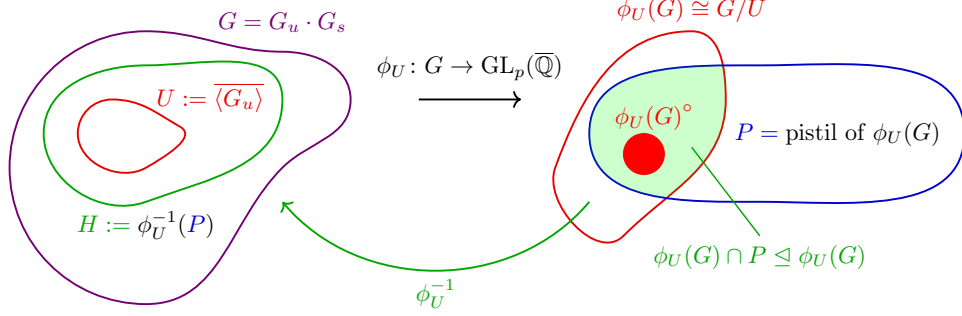\end{aligned}$$
$\square$

FIGURE 3.   Graphical representation of Lem. 7: given a group $G = \overline{\langle S \rangle}$ for $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ a set of rational matrices, we identify a normal subgroup H with the desired properties. We construct a homomorphism $\phi_U \colon G \to \mathrm{GL}_p(\overline{\mathbb{Q}})$ with kernel U, and define H to be the preimage of the pistil P of $\phi_U(G) \cong G/U$ under ϕ_U.

5. DEGREE BOUNDS

As sketched in § 1.2.5, we can now put everything together to obtain a degree bound on a linear algebraic group $G = \overline{\langle S \rangle}$ for $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ a finite set of rational matrices. We further obtain a bound for groups consisting exclusively of semisimple elements, which applies to groups generated by unitary transformations as appear, e.g., in quantum automata.

The obtained bound crucially depends on the height of the generators of the algebraic group that we are analysing. This dependency, in turn, comes from the analysis of the normal subgroup H of G, as defined in Lem. 7. In particular, we need the following lemma, which establishes that if a group is generated by a set S and H is a finite-index subgroup, then we can describe a set of generators of H from S and the index of the subgroup. Below, for $S \subseteq \mathrm{GL}_n(\mathbb{Q})$, we write $S^{\leq k}$ for the set of products of at most k elements from S.

Lemma 8. *Let $n \in \mathbb{N}$ and $G = \overline{\langle S \rangle}$ for some $S \subseteq \mathrm{GL}_n(\mathbb{Q})$. Let H be a closed normal subgroup of G with finite index d. Then $H = \overline{\langle S' \rangle}$ where $S' := H \cap (S \cup S^{-1})^{\leq 2d+1}$.*

Proof. Define $H' := \langle S \rangle \cap H$. We claim that $H' = \langle S' \rangle$. As H was assumed to be closed, it follows that

$$\overline{\langle S' \rangle} = \overline{H'} = \overline{\langle S \rangle \cap H} = \overline{\langle S \rangle} \cap H = H \,,$$

establishing the lemma.

It remains to establish the claim. To this end, observe that for $g, h \in \langle S \rangle$ we have $gh^{-1} \in H'$ if and only if $gh^{-1} \in H$, and hence

$$|\langle S \rangle / H'| \leq |G/H| = d \,.$$

Then, since H' is a subgroup of $\langle S \rangle$ of finite index at most d, we can apply Schreier's Lemma [Ser03, Lem. 4.2.1] to obtain that H' is generated by the set

$$H' \cap \{ t_1 \, s \, t_2^{-1} \mid s \in S' \text{ and } t_1, t_2 \in T \} \,,$$

for any set $T \subseteq \langle S \rangle$ that contains a representative of each right coset of H' in $\langle S \rangle$. But clearly we can take T to be $S^{\leq d}$. $\square$

We are now equipped to prove Thm. 9; see App. B for the detailed proofs of the claims.

Theorem 9 (Degree bound). *Let $n \in \mathbb{N}$ and let $S \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a finite set of matrices whose entries have height at most $h \in \mathbb{N}$. Then the Zariski closure of the group generated by S can be represented by finitely many polynomials of degree at most $(\log h)^{2^{|S|^{\exp^4(\mathrm{poly}(n))}}}$ with coefficients in $\mathbb{Q}$, forming a basis of the vanishing ideal of the group generated by S. Furthermore, if G contains only semisimple elements then the degree can be bounded by $(\log h)^{2^{|S|^{2^{\mathrm{poly}(n)}}}}$.*

Proof. Let $U := \overline{\langle G_u \rangle}$ be the closure of the group generated by the collection of unipotent elements in G. By Lem. 7, there exists a closed normal subgroup $H \trianglelefteq G$ defined over $\mathbb{Q}$, such that H/U is commutative, and the index of H in G is at most $J'(n)$, where J' is as in the statement of Lem. 7. We will now use the characteristic properties of U and H to obtain a bound on the degree of the polynomials defining G. We start by computing a bound on the degree of the polynomials defining H.

Since H is a closed normal subgroup of $G = \overline{\langle S \rangle}$ with index bounded by $J'(n)$, it follows from Lem. 8 that H is the closure of the group generated by $S' := H \cap (S \cup S^{-1})^{\leqslant 2J'(n)+1}$. Furthermore, since S' is constructed as a finite multiplication of elements of S, and their inverses, we can obtain the following bound.

Claim 9.1. The entries of the matrices in S' have height at most
$$h' := (h^{n^3+n^2} n! n)^{2J'(n)+1} .$$

Write $S' = \{g_1, \ldots, g_\ell\} \subseteq \mathrm{GL}_n(\mathbb{Q})$ where $\ell \leq (2|S|)^{2J'(n)+1}$. Recall from §1.2.3 that for $g \in \mathrm{GL}_n(\overline{\mathbb{Q}})$, we denote by g_s its semisimple part given by the unique decomposition $g = g_s g_u$. Then we have

$$
\begin{aligned}
H &= \overline{\langle S' \rangle \, U} && U \trianglelefteq H \text{ by Lem. 7} \\
&= \overline{\langle g_1 \rangle \cdots \langle g_\ell \rangle \, U} && H/U \text{ is commutative by Lem. 7(i)} \\
&= \overline{\langle (g_1)_s \rangle \cdots \langle (g_\ell)_s \rangle \, U} && gU = g_s U \text{ for all } g \in G \\
&= \overline{\overline{\langle (g_1)_s \rangle} \cdots \overline{\langle (g_\ell)_s \rangle} U} && (3)
\end{aligned}
$$

By the above, in order to compute a bound on the degree of the defining equations of H, it suffices to compute a bound on the degree of the equations that define U, as well as a bound on the degree of equations that define each of the $\overline{\langle (g_i)_s \rangle}$.

Given a matrix $g \in S'$, the eigenvalues $\lambda_1, \ldots, \lambda_n$ of g and g_s are the same. Masser's Theorem [Mas88; CLZ00], restated in Thm. 15 in App. B, provides a bound on the generators of the lattice of multiplicative relations of the form $\lambda_1^{k_1} \cdots \lambda_n^{k_n} = 1$ for integers $k_1, \ldots, k_n \in \mathbb{Z}$. By this bound and an argument similar to the one presented in [DJK05, Sec. 3.3], we obtain a degree bound for $\overline{\langle g_s \rangle}$. Define $f(n, h) := (cn^7 n! \log(h))^n$, where c is an absolute constant.

Claim 9.2. $\overline{\langle g_s \rangle}$ is bounded over $\mathbb{Q}$ by $n \cdot f(n, h')$ for $g \in S'$.

By Claim 6.1, U is bounded over $\mathbb{Q}$ by $(n^3+1)^{2^{3n^2}}$. Note that by Equ. (3) we have a system of equations with n^2+1 variables defining H, $\ell \cdot (n^2+1)$ variables defining the $\overline{\langle (g_i)_s \rangle}$ and n^2+1 variables defining U. We eliminate all variables from this system of equations except those defining H. In order to compute a bound on the degree increase that occurs in the elimination ideal of H, we use a result from Dubé [Dub90], stated earlier as Prop. 5. Setting $d := \max\left(n \cdot f(n, h'), (n^3+1)^{2^{3n^2}}\right)$, we obtain the following bound.

Claim 9.3. H is bounded over $\mathbb{Q}$ by $(d+1)^{2^{(\ell+2)(n^2+1)}}$.

To conclude, it suffices to look at G as the union of all the cosets of H in G. That is, G is the union of at most $J'(n)$ varieties, each of degree at most $(d+1)^{2^{(\ell+2)(n^2+1)}}$. Hence G is bounded over $\mathbb{Q}$ by $(d+1)^{2^{(\ell+2)(n^2+1)J'(n)}}$. The final bound for G as stated in the theorem is obtained from the bounds for d, ℓ, and J'. $\qquad\square$

6. Chains of Linear Algebraic Groups

In this section, we provide a quantitative version of the Noetherian property of subgroups of $\mathrm{GL}_n(\overline{\mathbb{Q}})$, i.e., a concrete bound on the length of chains of algebraic subgroups.

6.1. **Chains of Algebraic Sets.** Consider an algebraically closed field K. Because the Zariski topology is Noetherian, any strictly descending chain $X_0 \supsetneq X_1 \supsetneq \cdots$ of algebraic sets in K^m must be finite [Hum75, Chap. 1]. Ascending chains of algebraic sets can be infinite, but in the case of irreducible sets they are finite and we have a stronger statement. For irreducible algebraic sets J and J', if $J \subseteq J'$ then $\dim(J) \leq \dim(J')$ and if $\dim(J) = \dim(J')$ then $J = J'$, where $\dim(J)$ denotes the *dimension* of J [Hum75, Chap. 3]. Thus, for an irreducible algebraic set J, any chain $J_0 \subsetneq \cdots \subsetneq J_\ell$ of irreducible algebraic subsets of J has length $\ell \leq \dim(J)$. In particular, $\mathrm{GL}_n(K)$ has dimension $\dim(\mathrm{GL}_n(K)) = n^2$.

This translates in the context of polynomials in $K[x_1, \ldots, x_m]$ into, respectively, the ascending chain condition for ideals, and uniform bounds on the length of chains of prime ideals [BW93, Sec. 7.5]. Bounds on the length of ascending chains of polynomial ideals yield constructive versions of Hilbert's Basis Theorem, with applications for instance to the ideal membership problem, and have been investigated for a while [Sei72; MS92; GM94; NY99; Asc04]. Note that, in order to bound the length of ascending chains $I_0 \subsetneq I_1 \subsetneq \cdots$ of polynomial ideals, one must restrict the range of allowed polynomials, e.g., by requiring the degree of the polynomials in the basis for each I_i to be bounded by some function of the index i. The resulting upper bounds are ackermannian in the dimension [see, e.g., MS92; GM94], way beyond the elementary bounds of this paper.

6.2. **The Length of Chains of Linear Algebraic Groups.** We show that linear algebraic groups in dimension n over the rationals behave more like irreducible algebraic sets than general algebraic sets, in that there is a uniform bound on the length of their chains (regardless of whether the chain is ascending or descending) that depends only on n. We start with Lem. 10, which is restricted to the case in which each group in the chain exclusively consists of semisimple elements.

Lemma 10. *Let $n \in \mathbb{N}$ and $G_i = \overline{\langle S_i \rangle}$ for $S_i \subseteq \mathrm{GL}_n(\mathbb{Q})$, $1 \leq i \leq \ell$, be such that $G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_\ell$. If each S_i only consists of semisimple elements, then $\ell \leq n^2(2(n^2+1)^2)!$.*

Proof. For each linear algebraic group G_i, denote by P_i the pistil of G_i, that is, the intersection of all maximal tori that contain $(G_i)^\circ$. Since the sequence $(G_1)^\circ \subseteq (G_2)^\circ \subseteq \cdots \subseteq (G_\ell)^\circ$ is increasing, $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_\ell$ is also an increasing sequence.

By definition, each $(G_i)^\circ$ is irreducible, thus there are at most n^2 distinct possibilities for the $(G_i)^\circ$, and hence also for the P_i. Furthermore, as shown in Claim 4.1, each pistil P_i is bounded by 1. Since $G_i \cap P_i$ is a normal subgroup of G_i for all i by Lem. 4(ii), we can use Thm. 2 to show that each quotient $G_i/(G_i \cap P_i)$ is isomorphic to a finite linear group in dimension $m := (n^2+1)^2$. Furthermore, Lem. 4(ii) also shows that the order of each quotient $G_i/(G_i \cap P_i)$ will be at most $(2m)!$. Taking the product of the number of distinct P_i and the number of distinct finite

quotients $G_i/(G_i \cap P_i)$ we obtain the upper bound $n^2(2m)!$ for the length ℓ of the chain. $\qquad\square$

Note that Lem. 10 immediately applies to the case where the groups $G_1, \ldots, G_\ell$ are closures of groups generated by unitary matrices. For the general case, we provide the following bound.

Theorem 11. *Let $n \in \mathbb{N}$ and let $G_i = \overline{\langle S_i \rangle}$ for $S_i \subseteq \mathrm{GL}_n(\mathbb{Q})$, $1 \leq i \leq \ell$, be such that $G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_\ell$. Then we have $\ell \leq \exp^4(\mathrm{poly}(n))$.*

Proof. For each linear algebraic group G_i, let $U_i = \overline{\langle (G_i)_u \rangle}$ be the closure of the subgroup generated by the unipotent elements in G_i. By Claim 6.1, each U_i is d-bounded over $\mathbb{Q}$ for $d := (n^3 + 1)^{2^{3n^2}}$. Consequently, by Thm. 2 each quotient G_i/U_i is isomorphic to a linear algebraic group in dimension $p := (n^2 + d)^{2d^2}$, which moreover consists exclusively of semisimple elements.

Observe that the sequence $U_0 \subseteq U_1 \subseteq \cdots \subseteq U_\ell$ is increasing. Since by Claim 6.1 the U_i are irreducible, we can decompose this sequence into at most n^2 blocks where the dimension of the U_i is constant in each block but increases from one block to the next. Within each block, say from index k to r where $1 \leq k \leq r \leq \ell$, since the dimension is constant, $U := U_k = U_{k+1} = \cdots = U_r$. The sequence $(G_k/U) \subseteq \cdots \subseteq (G_r/U)$ is strictly increasing and hence by Lem. 10 has length at most $p^2(2(p^2 + 1)^2)!$. Taking the product of the number of blocks and the length of each block we obtain the upper bound $n^2p^2(2(p^2 + 1)^2)!$ for the length of the chain ℓ. $\qquad\square$

To conclude this section, recall that a number field k is a finite extension of the field of rational numbers $\mathbb{Q}$. As will be briefly discussed in Sec. 7.1, the order of a finite subgroup of $\mathrm{GL}_m(k)$ is at most $(2m[k : \mathbb{Q}])!$ where $[k : \mathbb{Q}]$ is the dimension of k as a vector space over $\mathbb{Q}$. This allows to extend Lem. 10 and Thm. 11 to a chain of linear algebraic groups generated over a number field, with the appropriate changes to the upper bound on the length ℓ of chain.

Corollary 12. *Let $n \in \mathbb{N}$, k be a number field, and $G_i = \overline{\langle S_i \rangle}$ for $S_i \subseteq \mathrm{GL}_n(k)$, $1 \leq i \leq \ell$, be such that $G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_\ell$. Then $\ell \leq \exp^1\big(\mathrm{poly}([k : \mathbb{Q}]) \exp^3(\mathrm{poly}(n))\big)$, and $\ell \leq 2^{\mathrm{poly}(n[k:\mathbb{Q}])}$ if each G_i consists of semisimple elements.*

7. Discussion

7.1. **Extension to Number Fields.** In this paper, we have focused on the case of rational matrices, but the results can be extended to matrices over a number field k at minimal additional expense. Upon inspection of our proofs, it turns out that the only place where working in this more general setting has an impact is on the order of finite subgroups of $\mathrm{GL}_p(\mathbb{Q})$ in Fact 4.1. Over a finite extension k of $\mathbb{Q}$, the bound needs to be updated to $(2p[k : \mathbb{Q}])!$ in order to take the dimension of k as a vector space over $\mathbb{Q}$ into account. The remainder of the bounds in the paper have to be adapted mutatis mutandis.

7.2. **Dependence on the Dimension and Height.** Our upper bound in Thm. 9 on the degree of the polynomials defining the Zariski closure of a finitely generated matrix group is a function of both the dimension of the generators and the height of the entries of the generators. The following examples illustrate that such a degree bound necessarily depends on both parameters.

Example 13 (Degree depends on the dimension). Recall that the special linear group $\mathrm{SL}_n(\mathbb{Z}) := \{M \in \mathrm{GL}_n(\mathbb{Z}) : \det(M) = 1\}$ is generated by three matrices with entries in $\{-1, 0, 1\}$ [Mac33, p. 35], i.e., with maximum height $h = 1$. The

Zariski closure of $\mathrm{SL}_n(\mathbb{Z})$ is $\mathrm{SL}_n(\overline{\mathbb{Q}})$.[2] We observe that *any* non-zero polynomial f that vanishes on $\mathrm{SL}_n(\overline{\mathbb{Q}})$ has (total) degree at least n. Indeed, evaluating f on the diagonal matrix $\mathrm{diag}(x, \ldots, x)$, for some variable x, yields a univariate polynomial g that vanishes on every n-th root of unity. It follows that $x^n - 1$ divides g and so g, and hence also f, has degree at least n.

Example 14 (Degree depends on the height). Consider the case of a single 2×2 matrix $g := \mathrm{diag}(2^p, 1/2)$ for some $p \in \mathbb{N}$, i.e., with height $h = 2^p$. By [DJK05, Lem. 6], the vanishing ideal of $\overline{\langle g \rangle}$ is generated by the multiplicative relations among the diagonal elements of g. These relations have one generator, namely $(2^p)^1 (1/2)^p = 1$. Any non-zero polynomial f that vanishes on $\overline{\langle g \rangle}$ must also vanish on $\{\mathrm{diag}(x, y) : xy^p = 1\}$, and thus be of degree at least $1 + p \geq \log h$.

7.3. **Related Work on the Algorithm of Derksen, Jeandel and Koiran.** Given a finite set of rational matrices, an algorithm computing the Zariski closure G of their generated group is presented in [DJK05]. In a nutshell, the algorithm computes better and better under-approximations H of the identity component G° until the quotient G/H is finite. The same principle is used in an algorithm described in [Gra17, Sec. 4.6], with part of the computation performed at the level of the Lie algebra of G. One obstacle to analysing the complexity of these algorithms is the following. In order to obtain a quantitative statement about H, it seems necessary to understand which elements will decrease the index of H in G if they are added to H. This, in turn, crucially relies not only on the degree (as analysed in Thm. 2), but also on the height of the coefficients of the quotient map ϕ_H [Nos20]. Bounding these coefficients requires a delicate analysis of the construction of ϕ_H. See App. C for more details.

7.4. **Related Work on Hrushovski's Algorithm.** Hrushovski's work has been subsequently pursued by Feng [Fen15] and Sun [Sun19], leading to a triple exponential algorithm for computing the Galois group of a linear differential equation. A different approach was recently pursued by Amzallag, Minchenko and Pogudin, who introduced the notion of toric envelope to obtain a single exponential bound for the first step in Feng's formulation of Hrushovski's algorithm, which is qualitatively optimal [AMP21; Amz18].

---

[2]This follows e.g. from the Borel Density Theorem [Mor01, Sec. 4.5 and Sec. 7.0], but can also be established directly by an elementary argument.

REFERENCES

[AMP21]   E. Amzallag, A. Minchenko and G. Pogudin. *Degree bound for toric envelope of a linear algebraic group*. 2021. arXiv: `1809.06489 [math.AG]`.

[Amz18]   E. Amzallag. "Galois groups of differential equations and representing algebraic sets". PhD thesis. CUNY Academic Works, 2018. URL: `https://academicworks.cuny.edu/gc_etds/2860`.

[Asc04]   M. Aschenbrenner. "Ideal membership in polynomial rings over the integers". In: *J. Amer. Math. Soc.* 17 (2004), pp. 407–441. DOI: `10.1090/S0894-0347-04-00451-5`.

[BC01]   V. Blondel and V. Canterini. "Undecidable problems for probabilistic automata of fixed dimension". In: *Theory Comput. Syst.* 36 (2001), pp. 231–245. DOI: `10.1007/s00224-003-1061-2`.

[BHKST20]   G. Bumpus, C. Haase, S. Kiefer, P.-I. Stoienescu and J. Tanner. "On the size of finite rational matrix semigroups". In: *Proc. ICALP 2020*. Vol. 168. LIPIcs. 2020, 115:1–115:13. DOI: `10.4230/LIPIcs.ICALP.2020.115`.

[BJKP05]   V. D. Blondel, E. Jeandel, P. Koiran and N. Portier. "Decidable and undecidable problems about quantum automata". In: *SIAM J. Comput.* 34(6) (2005), pp. 1464–1473. DOI: `10.1137/S0097539703425861`.

[BM07]   A. R. Bradley and Z. Manna. "Invariant generation". In: *The Calculus of Computation. Decision Procedures with Applications to Verification*. Springer, 2007. Chap. 12, pp. 311–346. DOI: `10.1007/978-3-540-74113-8_12`.

[Bor66]   A. Borel. "Linear algebraic groups". In: *Algebraic Groups and Discontinuous Subgroups*. Ed. by A. Borel and G. D. Mostow. Vol. 9. Proc. Symposia Pure Math. 1966, pp. 3–19. DOI: `10.1090/pspum/009`.

[BW93]   T. Becker and V. Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra*. Vol. 141. Graduate Texts in Mathematics. Springer, 1993. DOI: `10.1007/978-1-4612-0913-3`.

[CLZ00]   J. Cai, R. J. Lipton and Y. Zalcstein. "The complexity of the A B C problem". In: *SIAM J. Comput.* 29(6) (2000), pp. 1878–1888.

[DFO13]   A. S. Detinko, D. L. Flannery and E. A. O'Brien. "Recognizing finite matrix groups over infinite fields". In: *J. Symb. Comput.* 50 (2013), pp. 100–109. DOI: `10.1016/j.jsc.2012.04.002`.

[DJK05]   H. Derksen, E. Jeandel and P. Koiran. "Quantum automata and algebraic groups". In: *J. Symb. Comput.* 39(3–4) (2005), pp. 357–371. DOI: `10.1016/j.jsc.2004.11.008`.

[Dub90]   T. W. Dubé. "The Structure of polynomial ideals and Gröbner bases". In: *SIAM J. Comput.* 19(4) (1990), pp. 750–773. DOI: `10.1137/0219053`.

[Fen15]   R. Feng. "Hrushovski's Algorithm for computing the Galois group of a linear differential equation". In: *Adv. Appl. Math.* 65 (2015), pp. 1–37. DOI: `10.1016/j.aam.2015.01.001`.

[Fri97]   S. Friedland. "The maximal orders of finite subgroups in $GL_n(\mathbb{Q})$". In: *Proc. Am. Math. Soc.* 125(12) (1997), pp. 3519–3526. DOI: `10.1090/S0002-9939-97-04283-4`.

[Ge93]   G. Ge. "Algorithms Related to Multiplicative Representations of Algebraic Numbers". PhD thesis. U.C. Berkeley, 1993.

[GL06]   R. M. Guralnick and M. Lorenz. "Orders of finite groups of matrices". In: *Groups, Rings and Algebras*. Vol. 420. Contemp. Math. AMS, 2006, pp. 141–161. DOI: `10.1090/conm/420/07974`.

[GM94]   G. Gallo and B. Mishra. "A solution to Kronecker's Problem". In: *Appl. Algebra Eng. Commun.* 5 (1994), pp. 343–370. DOI: `10.1007/BF01188747`.

[Gra17]   W. A. de Graaf. *Computation with Linear Algebraic Groups*. Chapman & Hall/CRC Monographs. CRC Press, 2017.

[HOPW18]   E. Hrushovski, J. Ouaknine, A. Pouly and J. Worrell. "Polynomial invariants for affine programs". In: *Proc. LICS 2018*. ACM, 2018, pp. 530–539. DOI: `10.1145/3209108.3209142`.

[Hru02]   E. Hrushovski. "Computing the Galois group of a linear differential equation". In: *Banach Center Publications* 58(1) (2002), pp. 97–138. DOI: 10.4064/bc58-0-9.

[Hum75]   J. E. Humphreys. *Linear Algebraic Groups.* Vol. 21. Graduate Texts in Mathematics. Springer, 1975. DOI: 10.1007/978-1-4684-9443-3.

[Kar76]   M. Karr. "Affine relationships among variables of a program". In: *Acta Inf.* 6 (1976), pp. 133–151. DOI: 10.1007/BF00268497.

[KP02]   J. Kuzmanovich and A. Pavlichenkov. "Finite groups of matrices whose entries are integers". In: *Am. Math. Mon.* 109(2) (2002), pp. 173–186. DOI: 10.1080/00029890.2002.11919850.

[Mac33]   C. C. MacDuffee. *The Theory of Matrices.* Vol. 5. Ergebnisse der Mathematik und Ihrer Grenzgebiete. Springer, 1933. DOI: 10.1007/978-3-642-99234-6.

[Mas88]   D. W. Masser. "Linear relations on algebraic groups". In: *New Advances in Transcendence Theory.* Cambridge University Press, 1988, pp. 248–262. DOI: 10.1017/CBO9780511897184.016.

[Mik66]   K. A. Mikhailova. "The occurrence problem for direct products of groups". In: *Mat. Sb. (N.S.)* 70(112)(2) (1966), pp. 241–251. URL: http://mi.mathnet.ru/eng/msb4223.

[Mil72]   C. F. Miller. *On Group-Theoretic Decision Problems and Their Classification.* Vol. 68. Annals of Mathematics Studies. Princeton University Press, 1972. DOI: 10.1515/9781400881789.

[Min87]   H. Minkowski. "Zur Theorie der positiven quadratischen Formen". In: *J. Crelle* (101) (1887), pp. 196–202. DOI: 10.1515/crll.1887.101.196.

[Mor01]   D. W. Morris. *Introduction to Arithmetic Groups.* 2001. arXiv: math/0106063 [math.DG].

[MS04]   M. Müller-Olm and H. Seidl. "A note on Karr's Algorithm". In: *Proc. ICALP 2004.* Vol. 3142. Lect. Notes Comput. Sci. Springer, 2004, pp. 1016–1028. DOI: 10.1007/978-3-540-27836-8_85.

[MS92]   G. Moreno Socias. "Length of polynomial ascending chains and primitive recursiveness". In: *Math. Scand.* 71 (1992), pp. 181–205. DOI: 10.7146/math.scand.a-12421.

[New72]   M. Newman. *Integral Matrices.* Vol. 45. Pure and Applied Mathematics. Academic Press, 1972.

[Nos20]   K. Nosan. "On the complexity of computing the algebraic closure of a finitely generated matrix semigroup". Internship Report. École Polytechnique, 2020. URL: https://www.irif.fr/~nosan/Reports/M1report.pdf.

[NY99]   D. Novikov and S. Yakovenko. "Trajectories of polynomial vector fields and ascending chains of polynomial ideals". In: *Ann. Inst. Fourier* 49(2) (1999), pp. 563–609. DOI: 10.5802/aif.1683.

[Paz71]   A. Paz. *Introduction to Probabilistic Automata.* Computer Science and Applied Mathematics. Academic Press, Inc., 1971.

[Ren92]   J. Renegar. "On the computational complexity and geometry of the first-order theory of the reals. I, II, and III". In: *J. Symb. Comput.* 13(3) (1992), pp. 255–352. DOI: 10.1016/S0747-7171(10)80003-3.

[Sei72]   A. Seidenberg. "Constructive proof of Hilbert's Theorem on ascending chains". In: *Trans. Amer. Math. Soc.* 174 (1972), pp. 305–312. DOI: 10.1090/S0002-9947-1972-0314829-9.

[Ser03]   Á. Seress. *Permutation Group Algorithms.* Vol. 152. Cambridge Tracts in Mathematics. Cambridge University Press, 2003. DOI: 10.1017/CBO9780511546549.

[Sun19]   M. Sun. "A new bound on Hrushovski's Algorithm for computing the Galois group of a linear differential equation". In: *Commun. Algebra* 47(9) (2019), pp. 3553–3566. DOI: 10.1080/00927872.2019.1567750.

[Wei85]   B. Weisfeiler. "Post-classification version of Jordan's Theorem on finite linear groups". In: *Proc. Natl. Acad. Sci. U.S.A.* (81) (1985), pp. 5278–5279. DOI: 10.1073/pnas.81.16.5278.

Appendix A. Folklore Lemma

Lemma 3. *Fix $m \in \mathbb{N}$, and let $X \subseteq L^m$ be a d-bounded algebraic set. Then X is d-bounded over k if any of the following holds:*

  (i) X is stable under $\mathrm{Aut}(L/k)$ for some subfield k of L, or
  (ii) $X \cap k^m$ is dense in X.

Proof of (i). We may assume without loss of generality that X is the zero set of a *finite* collection of polynomials $I \subseteq L[\boldsymbol{x}]$ of degree at most d over a tuple $\boldsymbol{x}$ of variables. Let $F \subseteq L$ be the normal closure of the field extension of k generated by the coefficients of the polynomials in I. Then F is a finite Galois extension of k. Given a Galois extension F/k, we call the group of automorphims of F that fix k a *Galois group* and denote it by $\mathrm{Gal}(F/k)$.

Given $\alpha \in F$, write $\mathrm{Tr}(\alpha) := \sum_{\sigma \in \mathrm{Gal}(F/k)} \sigma(\alpha)$ for the trace of α relative to F/k. We extend Tr coefficient-wise to polynomials $p \in F[\boldsymbol{x}]$. Since F/k is a Galois extension of k, we have $\mathrm{Tr}(p) \in k[\boldsymbol{x}]$ for $p \in F[\boldsymbol{x}]$. Let $b_1, \ldots, b_n$ be a basis of F over k and consider the matrix $M = (\mathrm{Tr}(b_i b_j))_{ij}$ such that $\det(M)^2 \neq 0$ is the discriminant of the basis. Given $\alpha = \sum_{i=1}^n \alpha_i b_i \in F$, where $\alpha_1, \ldots, \alpha_n \in k$, for all $j \in \{1, \ldots, n\}$ we have $\mathrm{Tr}(\alpha b_j) = \sum_{i=1}^n \alpha_i \mathrm{Tr}(b_i b_j)$. Writing $M^{-1} = (c_{ij})$, it follows that for all $i \in \{1, \ldots, n\}$ we have $\alpha_i = \sum_j c_{ij} \mathrm{Tr}(ab_j)$. We conclude that $\alpha = \sum_{i,j=1}^n \mathrm{Tr}(\alpha b_j) c_{ij} b_i$. We then have that for any polynomial $p \in F[\boldsymbol{x}]$, $p = \sum_{i,j=1}^n \mathrm{Tr}(p b_j) c_{ij} b_i$, that is, p is a F-linear combination of the polynomials $\mathrm{Tr}(p b_1), \ldots, \mathrm{Tr}(p b_n)$ in $k[\boldsymbol{x}]$.

Suppose now that $p \in F[\boldsymbol{x}]$ is a polynomial that vanishes on X. Since each $\sigma \in \mathrm{Gal}(F/k)$ extends to a map in $\mathrm{Aut}(L/k)$, we have $\sigma(X) = X$ for all $\sigma \in \mathrm{Gal}(F/k)$. Thus each polynomial $\mathrm{Tr}(p b_i)$, for $i = 1, \ldots, n$, also vanishes on X. We conclude that X is also the zero set of the collection $I' := \{\mathrm{Tr}(b_i p) : i = 1, \ldots, n, p \in I\} \subseteq k[\boldsymbol{x}]$. But the polynomials in I' all have degree at most d. $\square$

Proof of (ii). We claim that X is stable under every automorphism $\sigma \in \mathrm{Aut}(L/k)$, which will prove that X is d-bounded over k by (i). To see this, let the polynomial $p \in L[\boldsymbol{x}]$ be a polynomial that vanishes on X and $\sigma \in \mathrm{Aut}(L/k)$. Then $p^\sigma \in L[\boldsymbol{x}]$, defined by applying σ point-wise to the coefficient of p, will vanish on $\sigma(X)$. But $\sigma(X)$ contains $\sigma(X \cap k^m) = X \cap k^m$, which is a dense subset of X. Hence p^σ vanishes on X, equivalently p vanishes on $\sigma^{-1}(X)$. We conclude that X is stable under σ^{-1}. Since σ was arbitrary, X is stable under $\mathrm{Aut}(L/k)$. $\square$

Appendix B. Computations of Degree Bounds

Claim 9.1. The entries of the matrices in S' have height at most

$$h' := (h^{n^3 + n^2} n! n)^{2J'(n)+1} .$$

Proof. To compute a height bound on the entries of S', it suffices to compute a height bound η on the entries of matrices in S and their inverses. Then by definition of S', the height of its elements will be bounded by the $(2J'(n) + 1)$-th power of $n\eta$.

Recall that the matrices in S have their entries bounded by h. Fix $g \in S$ and let $\ell \leq h^{n^2}$ be the least common multiple of the denominators of the entries of g. Recall that the e_k are the standard basis, where e_k denotes the vector with a 1 in the k-th coordinate and 0's elsewhere. The k-th column of g^{-1} can be computed by setting up $gX = e_k$. For simplicity of computation, we multiply both sides with the $n \times n$ diagonal matrix $\mathrm{diag}(\ell, \ldots, \ell)$. By Cramer's rule and an approximation on the magnitude of the determinant of g, we compute the bound $h^{n^3 + n^2} n!$ on the height of entries in g^{-1}. The claim immediately follows. $\square$

The following results are needed for the proof of Claim 9.2. Recall that a number is *algebraic* if it is the root of a non-zero polynomial in $\mathbb{Q}[x]$. For $\alpha \in \overline{\mathbb{Q}}$, the *defining polynomial* of α is the primitive polynomial in $\mathbb{Z}[x]$ of minimal degree having α as a root. The *height* of α is the maximum absolute value of the coefficients of its defining polynomial. Note that this yields the same notion of height as in the remainder of the paper: for a rational number $\frac{a}{b}$ with a, b coprime integers, the defining polynomial is $bx - a$ and the height is $\max(|a|, |b|)$.

We start by proving a bound on the generators of a lattice of multiplicative relations of the form $\lambda_1^{k_1} \cdots \lambda_n^{k_n} = 1$ for the algebraic numbers $\lambda_1, \ldots, \lambda_n$ and integers $k_1, \ldots, k_n \in \mathbb{Z}$. Such relations form an additive subgroup of $\mathbb{Z}^n$; see [Mas88; CLZ00].

Theorem 15 (Masser). *Fix any $n \geq 1$. Let $\lambda_1, \ldots, \lambda_n$ be non-zero algebraic numbers having height at most h over $\mathbb{Q}$ and let $D := [\mathbb{Q}(\lambda_1, \ldots, \lambda_n) : \mathbb{Q}]$. Then the group of multiplicative relations*

$$L := \{(k_1, \ldots, k_n) \in \mathbb{Z}^n : \lambda_1^{k_1} \cdots \lambda_n^{k_n} = 1\} \tag{4}$$

is generated (as a subgroup of $\mathbb{Z}^n$) by a collection of vectors all of whose entries have absolute value at most

$$(cn \log(h))^{n-1} D^{n-1} \frac{(\log(D+2))^{3n-3}}{(\log\log(D+2))^{3n-4}},$$

for some absolute constant c.

Corollary 16. *Let $g \in \mathrm{GL}_n(\mathbb{Q})$ have entries of height at most h. Writing $\lambda_1, \ldots, \lambda_n$ for the eigenvalues of g, the lattice L of multiplicative relations in (4) is generated by a collection of vectors, all of whose entries having absolute value at most $f(n, h) := (cn^7 n! \log(h))^n$ for some absolute constant c.*

Proof. Let $\ell \leq h^{n^2}$ be the least common multiple of the denominators of the entries of g. The eigenvalues of $g\ell$ are roots of the polynomial

$$P(x) := \det(x\mathbb{1} - g\ell) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} (x\mathbb{1} - g\ell)_{i,\sigma(i)}.$$

The coefficients of this polynomial are integers of absolute value at most $H := 2^n h^{n^3} n!$. Hence $\lambda_1, \ldots, \lambda_n$ have height at most H.

Applying Thm. 15, since the field $\mathbb{Q}(\lambda_1, \ldots, \lambda_n)$ has degree at most $D := n!$ over $\mathbb{Q}$, the lattice L of multiplicative relations in (4) is generated by vectors whose entries have absolute value at most $(cn^7 n! \log(h))^n$ for some absolute constant c. $\square$

The next proposition gives a degree bound for the Zariski-closure of the group generated by a single semisimple matrix.

Proposition 17. *Let $n \in \mathbb{N}$ and $g \in \mathrm{GL}_n(\mathbb{Q})$ have entries of height at most h. Then $\overline{\langle g_s \rangle}$ is bounded by $n \cdot f(n, h)$ over $\mathbb{Q}$, where $f(n, h) := (cn^7 n! \log(h))^n$ for some absolute constant c.*

Proof. Let g_s be written in the form $g_s = h^{-1} a h$, where $a = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ is diagonal. Write

$$L := \{(k_1, \ldots, k_n) \in \mathbb{Z}^n : \lambda_1^{k_1} \cdots \lambda_n^{k_n} = 1\}$$

for the group of multiplicative relations among $\lambda_1, \ldots, \lambda_n$. It is known (see, e.g., [DJK05]) that

$$\overline{\langle a \rangle} = \{\mathrm{diag}(x_1, \ldots, x_n) : x_1^{k_1} \cdots x_n^{k_n} = 1 \text{ for all } (k_1, \ldots, k_n) \in L\}.$$

But by Cor. 16, L is generated as an additive subgroup of $\mathbb{Z}^n$ by vectors $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ where the k_i have absolute value at most $f(n, h)$. It follows

that $\overline{\langle a \rangle}$ is bounded over $\mathbb{Q}$ by $nf(n,h)$. But then we have that $\overline{\langle g_s \rangle} = h^{-1}\overline{\langle a \rangle}h$ is also bounded by $nf(n,h)$ over $\mathbb{Q}$. $\qquad\square$

Claim 9.2. $\overline{\langle g_s \rangle}$ is bounded over $\mathbb{Q}$ by $n \cdot f(n,h')$ for $g \in S'$.

Proof. Recall that by Claim 9.1, all matrices $g \in S'$ have height bounded by h', where h' is as given in the statement of Claim 9.1. The proof of the claim then follows immediately from Prop. 17. $\qquad\square$

Claim 9.3. H is bounded over $\mathbb{Q}$ by $(d+1)^{2^{(\ell+2)(n^2+1)}}$.

Proof. By Lem. 6, U is bounded over $\mathbb{Q}$ by $(n^3+1)^{2^{3n^2}}$, and by Claim 9.2, each group $\overline{\langle (g_i)_s \rangle}$ is bounded over $\mathbb{Q}$ by $n \cdot f(n,h')$ where f is as in the statement of Cor. 16.

Let $d := \max\left(n \cdot f(n,h'), (n^3+1)^{2^{3n^2}}\right)$. By Prop. 5, H is bounded over $\mathbb{Q}$ by $(d+1)^{2^{(\ell+2)(n^2+1)}}$. $\qquad\square$

Appendix C. Analysis of the algorithm of Derksen, Jeandel, and Koiran

In this section, we give a quick overview of the algorithm of Derksen, Jeandel and Koiran [DJK05]. We then explain why analysing its complexity requires a delicate analysis that is unlikely to yield a good upper bound. We refer to [Nos20] for a more in-depth analysis.

C.1. **Overview.** In a nutshell, the algorithm builds the closure $G := \overline{\langle g_1, \ldots, g_N \rangle}$ of a finite set $\{g_1, \ldots, g_N\} \subseteq \mathrm{GL}_n(\mathbb{Q})$ by computing successive under-approximations $H \cdot S$ where H is an irreducible group and S a finite set, until $G = H \cdot S$. Initially, $H := \{\mathbb{1}\}$ and $S := \{\mathbb{1}, g_1, \ldots, g_N\}$. The algorithm performs a main loop and at each iteration, one of the following will happen:

(1) S increases in a way that makes $H \cdot S$ larger, or
(2) H increases, or
(3) the algorithm stops.

We do not repeat the details of the algorithm nor its proof of correctness. It suffices to know that H is an irreducible normal subgroup of G at the beginning of every iteration.[3] This implies that G/H is an algebraic group and, therefore, only two possibilities exist:

- If G/H is finite then H will not grow anymore and the algorithm essentially "fills up" the quotient G/H by adding elements to S, which takes finitely many steps.
- If G/H is infinite then the algorithm will eventually find an element h of infinite order in G/H and replace H by $\overline{H \cdot \overline{\langle h \rangle}}^{\circ}$ and then close H under various operations to ensure it is a still a normal subgroup of G.

By virtue of being an irreducible variety, H can only increase n^2 times, by the dimension argument recalled in Sec. 6.1. Hence, the delicate part of the analysis is to understand how long it takes for the algorithm to either discover an element of infinite order to make H grow, or to "fill up" G/H when it is finite.

---

[3]This is technically not true in the algorithm as written in [DJK05], but a minor modification ensures it without changing the complexity [Nos20].

C.2. **Case of a Finite Quotient.** Consider the latter situation: the quotient G/H is finite. In this case, the algorithm needs to discover all the elements of G/H by taking products of elements in S. Even if we disregard the fact that not all products will produce new elements, it might still take $|G/H|$ steps for the algorithm to finish. Hence, we need to obtain a bound on the size of G/H.

Now, G/H being an algebraic group, it can be embedded as a matrix group in some dimension d. It can be shown that, if the generators $g_1, \ldots, g_N$ have rational entries, then in fact G/H can be embedded in $\mathrm{GL}_d(\mathbb{Q})$ using the quotient map ϕ_H. It then follows by Fact 4.1 that the size of G/H is bounded by a function of d only $((2d)!$ is an upper bound). In other words, we need to obtain a bound on d. Such a bound is shown by Feng [Fen15] and recalled in Thm. 2, and depends on the degree of the polynomials that define H (and this bound cannot be improved in general).[4] In summary: we need to track the degree of (some) polynomial equations that define H.

C.3. **Case of an Infinite Quotient.** In order to track the degree of the equations defining H, we need to study the case where H grows. Recall that this happens when the algorithm finds an element h of infinite order in G/H, and then H becomes $\overline{H \cdot \overline{\langle h \rangle}^\circ}$. This, in turn, requires to bound the degree of equations defining $\overline{\langle h \rangle}^\circ$. It can be seen that $\overline{\langle h \rangle}^\circ$ essentially encodes the multiplicative relations between the eigenvalues of h. The only bound on the degree of those relations that we are aware of is given by Masser's Theorem [Mas88] (see Thm. 15).[5] The crucial issue, however, is that the *degree bound* given by Masser's Theorem depends on the *height of the coefficients*. In summary: we need to understand the height of elements h of infinite order in G/H.

The algorithm needs to find an element h of infinite order in G/H to make progress. The only approach that we are aware of to perform this task reduces the group G/H modulo some well-chosen prime p, and is used in the current state-of-the-art computational group theory algorithms [e.g., DFO13]. Indeed, a well-known lemma by Minkowski [Min87] shows that the kernel of the reduction map is torsion-free and therefore that it suffices to find two elements in G/H with the same reduction to obtain a matrix in the kernel that will then have infinite order. One can then use the fact that the image of the group through the reduction map has size at most p^{n^2} to argue that we only need to look at p^{n^2} products to find an element of infinite order. This means that, in order to bound the height of the element h of infinite order, we need a bound on p.

For this reduction to work, we need p not to divide any denominator of the coefficients of the generators of G/H. We are led, again, to the study of the quotient map in Thm. 2 since the generators of G/H are $\phi_H(g_1), \ldots, \phi_H(g_N)$. Unfortunately, the height of $\phi_H(g_i)$ depends on the height of the coefficients of ϕ_H, which is not analysed in Thm. 2. In fact, we are not aware of any result in the literature that provides a bound on this height. A good foundation to obtain such a bound is described in [Nos20] and could, in principle, be obtained by a combination of a careful analysis of the quotient, the use of quantifier elimination, and bounds on the degree of bases of polynomial ideals. Unfortunately, it is clear that it would in turn depend in a nontrivial way on the degree and height of the equations that define H. Furthermore, as conceived above, it would incur at least an exponential blow up.

---

[4]There is not necessarily a unique way of choosing polynomial equations for a given variety, but one could consider the smallest degree among all such equations.

[5]We note in passing that the complexity of finding those relations is a nontrivial topic in itself. The naive algorithm that enumerates all relations up to the bound and checks them one by one has a terrible complexity. A potentially more efficient algorithm is given by Ge [Ge93] but it does not improve the bound on the degree.

C.4. **Conclusion.** To summarise, a complete analysis of the algorithm of Derksen, Jeandel and Koiran [DJK05] seems to require to:

- analyse of the height of the quotient map in Thm. 2, and
- track the degree and height of the equations that define H.

Furthermore, we note again that both quantities (degree and height) potentially suffer from *at least* an exponential blow-up each time H increases. As H increases up to n^2 times, this means that the obtained bound would be at least a tower of n^2 exponentials, i.e., a non-elementary complexity bound. In conclusion, it is not clear what such a bound would be and the technical obstacles to obtain it are significant.