DEGREE BOUND FOR TORIC ENVELOPE OF A LINEAR ALGEBRAIC GROUP

ELI AMZALLAG, ANDREI MINCHENKO, AND GLEB POGUDIN

ABSTRACT. Algorithms working with linear algebraic groups often represent them via defining polynomial equations. One can always choose defining equations for an algebraic group to be of degree at most the degree of the group as an algebraic variety. However, the degree of a linear algebraic group $G \subset \mathrm{GL}_n(C)$ can be arbitrarily large even for $n = 1$. One of the key ingredients of Hrushovski's algorithm for computing the Galois group of a linear differential equation was an idea to "approximate" every algebraic subgroup of $\mathrm{GL}_n(C)$ by a "similar" group so that the degree of the latter is bounded uniformly in n. Making this uniform bound computationally feasible is crucial for making the algorithm practical.

In this paper, we derive a single-exponential degree bound for such an approximation (we call it a *toric envelope*), which is qualitatively optimal. As an application, we improve the quintuply exponential bound due to Feng for the first step of Hrushovski's algorithm to a single-exponential bound. For the cases $n = 2, 3$ often arising in practice, we further refine our general bound.

1. INTRODUCTION

1.1. Representing linear algebraic groups in algorithms.

A linear algebraic group is a subgroup of the group $\mathrm{GL}_n(C)$ of invertible $n \times n$ matrices over a field C that is defined by a system of polynomial equations in matrix entries. Such groups arise naturally in different areas of mathematics.

For algorithms dealing with arbitrary linear algebraic groups, there are two standard ways of representing such a group [7, Section 3.13]

(R1) by a system of defining polynomial equations
(R2) by a set of generators of a dense subgroup.

The approach **(R1)** is convenient, for example, for membership testing and for computing the dimension and the Lie algebra. **(R2)** is useful for computing normalizers and centralizers. Other ways of representing are available if some additional information (e.g., being connected or reductive) is known about the group. We refer to [7, Section 3.13] for a discussion.

In this paper, we will focus on **(R1)**, the representation of linear algebraic groups by a system of defining equations. It is known [13, Proposition 3] that an affine variety can be defined by a system of polynomial equations of degree at most the

degree of the variety. Thus, the degree of an algebraic group as an algebraic variety becomes a natural measure of complexity if **(R1)** is chosen. In addition to that, the degrees of an algebraic group and its orbits play an important role in constructive invariant theory [8, 9] (see also [19, 4] for bounds in the case of a reductive group). The degree of a linear algebraic group can be arbitrarily large even in the case of $n = 1$ (see Example 2.8). However, as we show in this paper, every linear algebraic group can be "approximated" by a group of degree at most $(4n)^{3n^2}$ (see Section 1.3).

1.2. **Hrushovski's algorithm.** Our main motivation comes from Hrushovski's algorithm for computing the Galois group of a linear differential equation [15]. A Galois group is associated to every linear differential equation and captures such properties of the solutions of the equation as solvability by quadratures and algebraicity of relations among solutions (for details, see [36]). Galois theory of differential equations has applications in integrable systems [25] and number theory [2], among other areas.

In contrast with the Galois theory of polynomial equations, in which Galois groups are finite, the Galois group of a linear differential equation is a linear algebraic group and so it is usually infinite. Moreover, it is known [34, 24, 11] that every linear algebraic group over an algebraically closed field C of characteristic zero can appear as the Galois group of a linear differential equation over $C(t)$. Several algorithms were designed for computing the differential Galois group in special cases [20, 5, 31], computing invariants [37] and the Lie algebra [1] of the differential Galois group, and computing the differential Galois group approximately [35].

Let C be an algebraically closed field of characteristic zero. The first general algorithm for computing the Galois group of a linear differential equation over $C(t)$ due to Hrushovski [15] appeared in 2002. The algorithm was used, for example, to design algorithms for computing the Galois group of a linear differential equation with parameters in several cases [22, 23]. For the last decade, it has been a challenge to understand the complexity of Hrushovski's algorithm and make it practical, see [10, 32, 28] for recent progress in this direction. One of the key ingredients of the algorithm is the following fact, which is of independent interest to the effective and computational theory of algebraic groups. There exists a function $\boldsymbol{d}(n)$ such that for every algebraic group $G \subset \mathrm{GL}_n(C)$ there exists an algebraic group $H \subset \mathrm{GL}_n(C)$ containing G such that

(H1) H *approximates* G in the following sense: there is a set of characters of H° such that G° is equal to the intersection of their kernels (X° denotes the connected component of identity in X).

(H2) H can be defined by equations of degree *at most* $\boldsymbol{d}(n)$.

Constructing such an approximation H of the differential Galois group G is the first step of Hrushovski's algorithm. The bound on the degrees of defining equations allows one to search for defining equations of H using undetermined coefficients. With such an approximation H at hand, the algorithm then proceeds to compute G by using the algorithm by Compoint and Singer [5].

Hrushovski himself did not provide an explicit expression for $\boldsymbol{d}(n)$ but showed its existence [15, Corollary 3.7]. He also conjectured that the overall complexity of the algorithm is at most double-exponential [15, Remark 4.4]. Feng [10, Proposition B.14] found the first explicit formula for such a $\boldsymbol{d}(n)$ by presenting a function of

quintuply exponential growth in n that could be used as $\boldsymbol{d}(n)$ in **(H2)** (see also [32] for a related bound for H).

1.3. **Summary of the main results.** In this paper, we show that every linear algebraic group $G \subset \mathrm{GL}_n(C)$ can be approximated in the sense of **(H1)** by a group of degree at most

$$(1.1) \qquad \begin{cases} 1 & \text{for } n = 1, \\ 6 & \text{for } n = 2, \\ 360 & \text{for } n = 3, \\ (4n)^{3n^2} & \text{for } n > 3. \end{cases}$$

More precisely, we formalize **(H1)** by the notion of a *toric envelope*. We say that $H \subset \mathrm{GL}_n(C)$ is a *toric envelope* of an algebraic group $G \subset \mathrm{GL}_n(C)$ if there exists a torus $T \subset \mathrm{GL}_n(C)$ such that H can be written as a product $T \cdot G$ (as a product of abstract groups). Theorems 3.1, 3.2, and 3.3 state that every algebraic subgroup of $\mathrm{GL}_n(C)$ has a toric envelope of degree at most (1.1).

In particular, we show that one can take $\boldsymbol{d}(n) = (4n)^{3n^2}$ (see Section 4). This improves Feng's result dramatically. Our bound is qualitatively optimal (see Remark 3.5) in the sense that any such bound is at least single-exponential.

1.4. **Outline of the approach.** We derive a general bound in Theorem 3.1 for a group $G \subset \mathrm{GL}_n(C)$ in the following steps.

Divide. By the Levi decomposition, G is a product of a reductive group and the unipotent radical.

Conquer (reductive). We find a toric envelope of bounded degree for the reductive group (Section 5.3). We reduce the problem to the case of a connected reductive group by deriving a bound (Lemma 5.11) analogous to the Jordan bound for finite subgroups of $\mathrm{GL}_n(C)$ [18]. We construct a toric envelope in the case of a connected group using the Lie correspondence and theory of reductive Lie algebras (Lemma 5.13). We put everything together in Lemma 5.14.

Conquer (unipotent). We derive a degree bound for any unipotent subgroup of $\mathrm{GL}_n(C)$ via representing it as the image of the exponential map (Section 5.2).

Combine. We combine the obtained bounds to produce a toric envelope of G (Section 5.4).
The proof of Theorem 3.2 takes a different approach based on a classification of subgroups of $\mathrm{SL}_2(C)$ and computer-assisted computation of the degree bound for the hardest special cases (Section 7). The proof of Theorem 3.3 refines the ideas from the proof of Theorem 3.1 in the case $n = 3$ (Section 8).

1.5. **Structure of the paper.** The rest of the paper is organized as follows. Section 2 contains the notions used to state the main results and illustrates them by examples. Section 3 contains the main results of the paper. Section 4 describes the application of the main results to Hrushovski's algorithm for computing the differential Galois group of a linear differential equation. Sections 5, 6, 7, and 8 contain proofs of the main results.

2. Preliminaries

Throughout the paper, C denotes an algebraically closed field of characteristic zero.

Definition 2.1. A *torus* is a commutative connected algebraic subgroup $T \subset \mathrm{GL}_n(C)$ such that every element of T is diagonalizable.

Definition 2.2. Consider a linear algebraic group $G \subset \mathrm{GL}_n(C)$. We say that an algebraic group $H \subset \mathrm{GL}_n(C)$ is *a toric envelope* of G if there exists a torus $T \subset \mathrm{GL}_n(C)$ such that $H = T \cdot G$ (product as abstract groups).

Remark 2.3. The product $T \cdot G$ is not necessarily semidirect. More precisely, T does not necessarily normalize G (Example 2.10) and G does not necessarily normalize T (Example 2.9).

Example 2.4. Every linear algebraic group $G \subset \mathrm{GL}_n(C)$ is a toric envelope of itself (with $T = \{e\}$).

Definition 2.5. A algebraic subvariety $X \subset \mathrm{GL}_n(C)$ is said to be *bounded by d*, where d is a positive integer, if there exist polynomials $f_1, \ldots, f_M \in C[x_{11}, x_{12}, \ldots, x_{nn}]$ of degree at most d such that

$$X = \mathrm{GL}_n(C) \cap \{f_1 = f_2 = \ldots = f_M = 0\}.$$

The following notion of the degree of a variety (we specialize it to subvarieties of $\mathrm{GL}_n(C)$, see [13, Section 2] for a general treatment) is a generalization of the notion of degree of a polynomial.

Definition 2.6. Let $X \subset \mathrm{GL}_n(C)$ be a subvariety such that all irreducible components of X are of the same dimension m (for example, this is the case if X is a linear algebraic group). Then

$$\deg X := \max\left\{|X \cap H| : H \text{ is a hyperplane of codimension } m \text{ such that } |X \cap H| \text{ is finite}\right\}.$$

By [13, Remark 2], the degree of a hypersurface is equal to the degree of its defining polynomial.

Proposition 2.7 (follows from [13, Proposition 3])**.** *Let $X \subset \mathrm{GL}_n(C)$ be a subvariety of degree D. Then X can be defined by equations of degree at most D.*

The following examples show that the degree of a toric envelope of a group can be much smaller that the degree of the group itself.

Example 2.8. Let N be a positive integer and $G \subset \mathrm{GL}_1(C)$ be the group of all N-th roots of unity. It is defined inside $\mathrm{GL}_1(C)$ by a single equation $x^N - 1 = 0$ of degree N, so it has degree N. The whole $\mathrm{GL}_1(C)$ is a toric envelope of G with $T = \mathrm{GL}_1(C)$ and is of degree 1.

Example 2.9. Consider

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{2018} \end{pmatrix} \mid a \in C^*,\ b \in C \right\}.$$

One can show that the degree of G is 2018. Let T be the group of all diagonal matrices. Then the group of all triangular matrices in $\mathrm{GL}_2(C)$ is a toric envelope of G because it is equal to $T \cdot G$. This group is defined by a single linear equation, so it has degree 1.

Example 2.10. Consider a dihedral group

$$G = \left\{ \begin{pmatrix} \varepsilon^m & 0 \\ 0 & \varepsilon^{-m} \end{pmatrix} \mid m \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} 0 & \varepsilon^m \\ \varepsilon^{-m} & 0 \end{pmatrix} \mid m \in \mathbb{Z} \right\},$$

where ε is a primitive 2018-th root of unity. Since G is a zero-dimensional variety consisting of 4036 points, $\deg G = 4036$. Let T be the group of all diagonal matrices. Then

$$T \cdot G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in C^* \right\} \cup \left\{ \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \mid a, b \in C^* \right\}$$

is a toric envelope of G. Since $T \cdot G$ is a union of two two-dimensional spaces, $\deg(T \cdot G) = 2$.

3. Main results

Theorem 3.1. *Let C be an algebraically closed field of characteristic zero. Let $G \subset \mathrm{GL}_n(C)$ be a linear algebraic group. Then there exists a* toric envelope *H of G of degree at most $(4n)^{3n^2}$. In particular, H is bounded by this number.*

Theorem 3.2. *Let C be an algebraically closed field of characteristic zero. Let $G \subset \mathrm{GL}_2(C)$ be a linear algebraic group. Then there exists a* toric envelope *H of G such that H is bounded by 6.*

Theorem 3.3. *Let C be an algebraically closed field of characteristic zero. Let $G \subset \mathrm{GL}_3(C)$ be a linear algebraic group. Then there exists a* toric envelope *H of G of degree at most 360. In particular, H is bounded by 360.*

Remark 3.4. A sharper bound for Theorem 3.1 is given by (6.1) in Section 6.

Remark 3.5. Let us show that the bound in Theorem 3.1 is qualitatively optimal by presenting a single-exponential lower bound. Fix a positive integer n. Let D and P be the group of all diagonal matrices and the group of all permutation matrices in this basis, respectively. Since P normalizes D, their product $G := P \cdot D \subset \mathrm{GL}_n(C)$ is an algebraic group [27, §3 and Theorem 3 on p. 102]. One can show that, since G° is a maximal torus in $\mathrm{GL}_n(C)$, the only possible toric envelope of G is G itself. Since $P \cap D = \{e\}$, the number of connected components of G is equal to $|P| = n!$. Since $G^\circ = D$, every component has degree $\deg D = 1$. Thus, we obtain a single-exponential lower bound

$$\deg G = n! = n^{\mathrm{O}(n)}.$$

The same example gives a single-exponential lower degree bound for a proto-Galois group (see Section 4) as well.

4. Application to Hrushovski's algorithm

Hrushovski's algorithm for computing the differential Galois group [15] of a linear differential equation of order n consists of the following three steps as outlined in [10, Section 1]

(1) Computing a proto-Galois group of the differential Galois group of the equation using an a priori upper bound for the degrees of the defining equations.
(2) Compute the toric part using the algorithm by Compoint and Singer [5].
(3) Compute the finite part.

In this section, we show (Lemma 4.2) that every toric envelope of an algebraic group $G \subset \mathrm{GL}_n(C)$ is a proto-Galois group of G. It follows that the bounds from Theorems 3.1, 3.2, and 3.3 can be used in the first step of Hrushovski's algorithm instead of the bound given in [10, Proposition B.11].

Feng [10, Definition 1.1] defined a proto-Galois group as follows.

Definition 4.1 (proto-Galois group)**.** Let $G \subset \mathrm{GL}_n(C)$ be an algebraic group. An algebraic group $H \subset \mathrm{GL}_n(C)$ is called a *proto-Galois group* of G if

$$(H^\circ)^t \trianglelefteq G^\circ \subset G \subset H,$$

where $(H^\circ)^t$ denotes the intersection of the kernels of all characters of H°.

Lemma 4.2. *If $H \subset \mathrm{GL}_n(C)$ is a toric envelope of $G \subset \mathrm{GL}_n(C)$, then H is a proto-Galois group of G.*

Proof. Since H is a toric envelope of G, $G \subset H$, so inclusions $G^\circ \subset G \subset H$ from Definition 4.1 hold. [30, Lemma 2.1] implies that $(H^\circ)^t$ is exactly the subgroup of H generated by all unipotent elements of H°. By Lemma 5.2, it coincides with the subgroup of G° generated by all unipotents in G°, and such a subgroup is normal in G°. □

Corollary 4.3. *Let C be an algebraically closed field of characteristic zero. For every linear algebraic group $G \subset \mathrm{GL}_n(C)$*

- *there exists a proto-Galois group H bounded by $(4n)^{3n^2}$;*
- *if $n = 2$, there exists a proto-Galois group H bounded by 6;*
- *if $n = 3$, there exists a proto-Galois group H bounded by 360.*

5. Proof ingredients

Notation 5.1. In what follows we will use the following notation.
- By C we denote an algebraically closed field of characteristic zero.
- We denote the set of all $n \times n$ (resp., $n \times m$) matrices over C by $\mathrm{Mat}_n(C)$ (resp., $\mathrm{Mat}_{n,m}(C)$).
- We denote the subgroup of all scalar matrices in $\mathrm{GL}_n(C)$ by $Z_n \subset \mathrm{GL}_n(C)$.
- For a subset $X \subset \mathrm{Mat}_n(C)$, we denote the normalizer and centralizer subgroups of X by $N(X)$ and $Z(X)$, respectively.
- For a subgroup $G \subset \mathrm{GL}_n(C)$, we denote the center by $C(G)$ and the connected component of the identity by G°.
- For a Lie subalgebra $\mathfrak{u} \subset \mathfrak{gl}_n(C)$, we denote the normalizer and centralizer subalgebras by $\mathfrak{n}(\mathfrak{u})$ and $\mathfrak{z}(\mathfrak{u})$, respectively.
- For a positive integer n, $J(n)$ is the minimal number such that every finite subgroup of $\mathrm{GL}_n(C)$ contains a normal abelian subgroup of index at most $J(n)$. We will use Schur's bound [6, Theorem 36.14]

$$(5.1) \qquad\qquad J(n) \leqslant \left(\sqrt{8n}+1\right)^{2n^2} - \left(\sqrt{8n}-1\right)^{2n^2}$$

- For a positive integer n, $A(n)$ is the maximal size of a finite abelian subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Some known values are $A(1) = 2$, $A(2) = 6$ (see [26, p. 180]), and $A(3) = 12$ (see [33, p. 170]), a general upper bound is given by Lemma 5.9.

5.1. Auxiliary lemmas.

Lemma 5.2. *An algebraic group $H \subset \mathrm{GL}_n(C)$ is a* toric envelope *of an algebraic group $G \subset \mathrm{GL}_n(C)$ if and only if*

    (1) H° and G° have the same set of unipotents;
    (2) $H = G \cdot H^\circ$.

Proof. Let H be a toric envelope of G. Then there exists torus $T \subset \mathrm{GL}_n(C)$ such that $H = T \cdot G$. Since T is connected, $T \subset H^\circ$, so $H \supset G \cdot H^\circ \supset G \cdot T = H$, so (2) holds. Consider any unipotent element $A \in H^\circ$. Since $H^\circ = T \cdot G^\circ$, then there are $B \in T$ and $C \in G^\circ$ such that $A = BC$. Since T is a torus, B is a semisimple element. Then $C = B^{-1}A$ is a Jordan-Chevalley decomposition of C. By [27, Theorem 6, p. 115], $A, B \in G^\circ$. Thus, every unipotent element of H° belongs to G°. Since also $G \subset H$, (1) holds.

Assume that properties (1) and (2) hold for G and H. Let $H = H_0 \ltimes U$ be a Levi decomposition of H (see [27, Theorem 4, p. 286]). By [39, Lemma 10.10], H_0 can be written as a product ΓH_0° for some finite group $\Gamma \subset \mathrm{GL}_n(C)$. [3, Proposition, p. 181] implies that H_0° can be written as ST, where $T := C(H_0^\circ)^\circ$ is a torus and $S := [H_0^\circ, H_0^\circ]$ is semisimple. Since Γ normalizes H_0 and the center is a characteristic subgroup, Γ normalizes T. Since U and S are generated by unipotents, $U, S \subset G^\circ$. Then

$$H \supset T \cdot G = T \cdot G^\circ \cdot G \supset T \cdot S \cdot U \cdot G = H^\circ \cdot G = H,$$

so $H = T \cdot G$ and H is a toric envelope of G. $\qquad\square$

Corollary 5.3. *If $H_2 \subset \mathrm{GL}_n(C)$ is a* toric envelope *of $H_1 \subset \mathrm{GL}_n(C)$ and H_1 is a toric envelope of $H_0 \subset \mathrm{GL}_n(C)$, then H_2 is a toric envelope of H_0.*

Proof. Lemma 5.2 implies that H_0°, H_1°, and H_2° have the same set of unipotents. Since $H_1 \subset H_2$, we have $H_1^\circ \subset H_2^\circ$. Together with Lemma 5.2 this implies that $H_2 = H_2^\circ \cdot H_1 = H_2^\circ \cdot H_1^\circ \cdot H_0 = H_2^\circ \cdot H_0$. Lemma 5.2 implies that H_2 is a toric envelope of H_0. $\qquad\square$

Corollary 5.4. *Any* toric envelope *of a reductive group is again a reductive group.*

Proof. Let G be a reductive group and H be a toric envelope of G. Assume that H is not reductive. Then it contains a nontrivial connected normal unipotent subgroup U. Since G° and H° have the same unipotents, $U \subset G^\circ$. This contradicts the reductivity of G. $\qquad\square$

Corollary 5.5. *Let G be an algebraic subgroup of $\mathrm{GL}_n(C)$. Then every* toric envelope *of GZ_n is a toric envelope of G.*

Lemma 5.6. *Let $G \subset \mathrm{GL}_n(C)$ be an algebraic group such that $Z_n \subset G$. Then $G = Z_n \cdot (G \cap \mathrm{SL}_n(C))$.*

Proof. Let $A \in G$. Since $Z_n \subset G$, $\frac{1}{\sqrt[n]{\det A}}A \in G \cap \mathrm{SL}_n(C)$. Thus, $A \in Z_n \cdot (G \cap \mathrm{SL}_n(C))$. $\qquad\square$

The following geometric lemma is a modification of [17, Lemma 3].

Lemma 5.7. *Let $X \subset \mathbb{A}^N$ be an algebraic variety of dimension $\leqslant d$ and degree D. Consider polynomials $f_1, \ldots, f_M \in C[\mathbb{A}^N]$ such that $\deg f_i \leqslant D_1$ for every $1 \leqslant i \leqslant M$. Then the sum of the degrees of the components of $Y := X \cap \{f_1 = \ldots = f_M = 0\}$ of dimension $\geqslant d'$ does not exceed $D \cdot D_1^{d-d'}$.*

Proof. We will prove the lemma by induction on $d - d'$. The base case is $d = d'$. In this case, the set of components of Y of dimension at least d' is a subset of the set of components of X of dimension d, and the sum of their degrees is at most $\deg X = D$.

Let $d > d'$. Considering every component of X separately, we may reduce to the case that X is irreducible. If every f_i vanishes on X, then $X = Y$ and the only component of Y of dimension $\geqslant d'$ has degree D. Otherwise, assume that f_1 does not vanish everywhere on X. Then $\dim X \cap V(f_1) \leqslant d - 1$ and $\deg(X \cap V(f_1)) \leqslant DD_1$ by [12, Theorem 7.7, Chapter 1]. Applying the induction hypothesis to $X \cap V(f_1)$ and the same d', we show that the sum of the degrees of the components of Y of dimension at least d' is at most

$$\deg(X \cap V(f_1))D_1^{d-1-d'} \leqslant DD_1^{d-d'}. \qquad \square$$

Corollary 5.8. *For every collection of algebraic subgroups $G_0, G_1, \ldots, G_k \subset \mathrm{GL}_n(C)$*

$$\deg G \leqslant n^{\dim G_0 - \dim G} \deg G_0, \ \textit{where} \ G := G_0 \cap N(G_1) \cap \ldots \cap N(G_k).$$

Proof. [10, Lemma B.4] implies that $N(G_1) \cap \ldots \cap N(G_k)$ is defined by polynomials of degree at most n. Then the statement of the corollary follows from Lemma 5.7 with $D_1 = n$. $\qquad \square$

Lemma 5.9. $A(n) \leqslant 2 \cdot 3^{[n^2/4]}$, *where $[x]$ means the integer part of x.*

Proof. Consider a finite abelian subgroup $A \subset \mathrm{GL}_n(\mathbb{Z})$. Let $A_0 := A \cap \mathrm{SL}_n(\mathbb{Z})$, then $|A| \leqslant 2|A_0|$. Consider the homomorphism $\varphi \colon \mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{F}_3)$ defined by reducing modulo 3. [26, Theorem IX.8] implies that $|A_0| = |\varphi(A_0)|$. According to [38, Table 2], the size of an abelian subgroup of $\mathrm{SL}_n(\mathbb{F}_3)$ does not exceed $3^{[n^2/4]}$. $\qquad \square$

5.2. Degree bound for unipotent groups.

Lemma 5.10. *Let $U \subset \mathrm{GL}_n(C)$ be a connected unipotent group. Then*

$$\deg U \leqslant \prod_{k=1}^{n-1} k!.$$

Proof. By Engel's theorem [27, Corollary 1, p. 125], there exists a basis such that $\mathrm{Lie}\, U$ is contained in a subspace $\mathcal{T} \subset \mathrm{Mat}_n(C)$ of strictly upper triangular matrices. From now on, we fix such a basis. By [27, Theorem 7, p. 126], $U = \varphi(\mathrm{Lie}\, U)$, where φ is the exponential map. Since every matrix in $\mathcal{T}$ is nilpotent of index at most n, φ is defined everywhere on $\mathcal{T}$ by the following formula

$$\varphi(X) = I_n + X + \frac{X^2}{2!} + \ldots + \frac{X^{n-1}}{(n-1)!} \ \text{for } X \in \mathcal{T}.$$

Consider the affine variety

$$W := \{(X, Y) \in \mathcal{T} \times \mathrm{GL}_n(C) \mid Y = \varphi(X) \ \& \ X \in \mathrm{Lie}\, U\}.$$

Since the projection of W to $\mathrm{GL}_n(C)$ is equal to $\varphi(\mathrm{Lie}\, U) = U$, $\deg U \leqslant \deg W$ by [13, Lemma 2]. The condition $X \in \mathrm{Lie}\, U$ is defined by linear equations. A direct computation shows that

$$\deg(\varphi(X))_{i,j} \leqslant \begin{cases} -\infty, & \text{if } i > j, \\ j - i, & \text{otherwise,} \end{cases}$$

where $(\varphi(X))_{i,j}$ denotes the (i,j)-th entry of the matrix $\varphi(X)$ whose entries are polynomials in the entries of X. The condition $Y = \varphi(X)$ is defined by $\frac{n(n+1)}{2}$ linear equations, $n-2$ quadratic equations, $n-3$ equations of degree 3, ..., one equation of degree $n-1$. Thus, Bezout's theorem [12, Theorem 7.7, Chapter 1] implies that $\deg W \leqslant 2^{n-2}3^{n-3}\ldots(n-2)^2(n-1) = \prod\limits_{k=1}^{n-1} k!$. $\square$

5.3. **Degree bound for reductive groups.** All statements in this section will be about a reductive group $G \subset \mathrm{GL}_n(C)$ such that $G \subset N(F)$, where $F \subset \mathrm{GL}_n(C)$ is some connected group. In our proofs, G and F will be the reductive and unipotent parts of a Levi decomposition of an arbitrary linear algebraic group, respectively.

Lemma 5.11. *Let $G \subset \mathrm{GL}_n(C)$ be a reductive algebraic group such that $G \subset N(F)$ for some connected algebraic group $F \subset \mathrm{GL}_n(C)$. Then there is a* toric envelope *$H \subset N(F)$ of G such that*

$$[H : H^\circ] \leqslant J(n)A(n-1)n^{n-1}.$$

Proof. Using Corollary 5.5, we replace G with GZ_n, so in what follows, we assume that $Z_n \subset G$.

By [39, Lemma 10.10], G can be written as a product ΓG° for some finite group $\Gamma \subset \mathrm{GL}_n(C)$. [3, Proposition, p. 181] implies that G° can be written as ST, where $T := C(G^\circ)^\circ$ is a torus and $S := [G^\circ, G^\circ]$ is semisimple. Since centers and connected components of the identity are preserved by any automorphism of a group, and conjugation by an element of Γ induces an automorphism of G°, Γ normalizes T.

By the definition of $J(n)$ (see Notation 5.1), there exists a normal abelian subgroup $\Gamma_{\mathrm{ab}} \subset \Gamma$ of index at most $J(n)$. Since $Z_n \subset G$, T contains Z_n. Then Lemma 5.6 implies that

$$T = Z_n \cdot (T \cap \mathrm{SL}_n(C)).$$

For every algebraic group F, by $\mathrm{AlgAut}(F)$ we will denote the group of algebraic automorphisms of F. The action of Γ_{ab} on T by conjugation defines a group homomorphism $\varphi \colon \Gamma_{ab} \to \mathrm{AlgAut}(T \cap \mathrm{SL}_n(C))$. Since $T \cap \mathrm{SL}_n(C) \cong (C^*)^d$ for some $d \leqslant n-1$ (see [27, Problem 10, p. 114]),

$$\mathrm{AlgAut}(T \cap \mathrm{SL}_n(C)) \cong \mathrm{GL}_d(\mathbb{Z}).$$

Let $\Gamma_0 := \mathrm{Ker}\,\varphi$. Since $\Gamma_0 = \Gamma_{\mathrm{ab}} \cap Z(T)$ and both Γ_{ab} and T are normalized by Γ, Γ_0 is a normal subgroup in Γ.

We set H_0 to be the intersection of all the maximal tori in $\mathrm{GL}_n(C)$ containing $\Gamma_0 \cdot T$. Since $\Gamma_0 \cdot T$ is a quasitorus, it is diagonalizable (see [27, Theorem 3, p. 113]), so there is at least one maximal torus containing $\Gamma_0 \cdot T$. Thus, H_0 is a torus. Since $\Gamma_0 \cdot T$ is normalized by Γ, H_0 is also normalized by Γ. We set $H_1 = H_0 \cap N(S) \cap N(F)$ and

$$(5.2) \qquad\qquad H := T_0 \cdot G, \text{ where } T_0 := H_1^\circ.$$

The lemma follows from the following two claims.

Claim 1: H is a group.   Since $T \subset T_0$ and Γ normalizes T_0, we have

$$(5.3) \qquad\qquad H = T_0 \cdot G = T_0 \cdot \Gamma \cdot T \cdot S = \Gamma \cdot (T_0 \cdot S).$$

The latter is a group, because T_0 normalizes S and Γ normalizes T_0 and S.

Claim 2: $[H : H^\circ] \leqslant J(n)A(n-1)n^{n-1}$**.**   From (5.3) we have $H = (\Gamma \cdot T_0) \cdot (T_0 \cdot S)$. Since $T_0 \cdot S$ is connected, H has at most as many connected components as $\Gamma \cdot T_0$. Since $T_0 = H_1^\circ$, the latter is bounded by the number of connected components of $\Gamma \cdot H_1$. We have

$$(5.4) \qquad \deg(\Gamma \cdot H_1) \leqslant [\Gamma : \Gamma_0] \cdot \deg H_1 = [\Gamma : \Gamma_{\mathrm{ab}}] \cdot [\Gamma_{\mathrm{ab}} : \Gamma_0] \cdot \deg H_1.$$

We have already shown that $[\Gamma : \Gamma_{\mathrm{ab}}] \leqslant J(n)$. The index $[\Gamma_{\mathrm{ab}} : \Gamma_0] = |\varphi(\Gamma_{\mathrm{ab}})|$ does not exceed the maximal size of a finite abelian subgroup of $\mathrm{GL}_d(\mathbb{Z})$. Since $d \leqslant n-1$, this number is at most $A(n-1)$.

Since H_0 is defined by linear polynomials, $\deg H_0 = 1$. Since H_0 is a torus, $\dim H_0 \leqslant n$. Since $\dim (H_0 \cap N(S) \cap N(F)) \geqslant \dim Z_n = 1$, Corollary 5.8 implies that

$$(5.5) \qquad\qquad \deg H_1 = \deg (H_0 \cap N(S) \cap N(F)) \leqslant n^{n-1}.$$

Thus, H has at most $[\Gamma : \Gamma_0] \cdot \deg H_1 \leqslant J(n)A(n-1)n^{n-1}$ connected components.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

Corollary 5.12. *In the notation of Lemma 5.11, if G° is a torus, then*

$$\deg H \leqslant J(n)A(n-1)n^{n-1}.$$

Proof. In this case, S from the proof of Lemma 5.11 is trivial. Since $T \subset T_0$, $H = \Gamma \cdot T_0$. Then $\deg H \leqslant (\deg \Gamma \cdot H_1)$. The latter is bounded by $J(n)A(n-1)n^{n-1}$ due to (5.4) and (5.5). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

Lemma 5.13. *Let $G \subset \mathrm{GL}_n(C)$ be a connected reductive group such that $G \subset N(F)$ for some connected group $F \subset \mathrm{GL}_n(C)$. Then there exists a toric envelope $H \subset N(F)$ of G such that*

$$\deg H \leqslant n^{n^2 - \dim G} \quad\text{and}\quad N(G) \cap N(F) \subset N(H).$$

Proof. Using Corollary 5.5 we may replace G with GZ_n, so we will assume that $Z_n \subset G$. We set

$$H := (Z(G) \cap Z(Z(G)) \cap N(F))^\circ \cdot G.$$

The lemma follows from the following three claims

Claim 1: H **is a toric envelope of** G**.**   Since $Z(G)$ normalizes G, H is a group. We will show that the connected component of identity of $Z(G) \cap Z(Z(G))$ is a torus. Then the connected component of the identity of $Z(G) \cap Z(Z(G)) \cap N(F)$ will also be a torus.

Since G is reductive, its representation in C^n is completely reducible (see [14, Theorem 4.3, p. 117]). Let $C^n = V_1 \oplus V_2 \oplus \ldots \oplus V_\ell$ be a decomposition of C^n into isotypic components. Each V_i can be written as $W_i \otimes C^{n_i}$, where W_i is the corresponding irreducible representation of G and C^{n_i} is a trivial representation. Let $d_i := \dim W_i$ for $1 \leqslant i \leqslant \ell$. Then Schur's lemma implies that

$$Z(G) = \bigoplus_{i=1}^{\ell} (C^* I_{d_i} \otimes \mathrm{GL}_{n_i}(C)), \text{ where } I_{d_i} \text{ is a } d_i \times d_i \text{ identity matrix.}$$

Since $Z(G) \cap Z(Z(G))$ is the center of $Z(G)$, we have

$$Z(G) \cap Z(Z(G)) = \bigoplus_{i=1}^{\ell} (C^* I_{d_i} \otimes C^* I_{n_i}) = \bigoplus_{i=1}^{\ell} C^* I_{n_i d_i}.$$

Thus, $Z(G) \cap Z(Z(G))$ is a torus. So the claim is proved.

Claim 2: $\deg H \leqslant n^{n^2 - \dim G}$. [3, Proposition, p. 181] implies that G can be written as ST, where $T := C(G)^\circ$ is a torus and $S := [G, G]$ is semisimple. Consider $\widehat{H} := N(S) \cap Z(Z(G)) \cap N(F)$. Then $H \subset \widehat{H}$. We will show that $H = \widehat{H}^\circ$.

Let $\mathfrak{g} := \operatorname{Lie} G$ and $\mathfrak{s} := \operatorname{Lie} S$. Consider an element $a \in \mathfrak{n}(\mathfrak{s})$. The map $\mathfrak{s} \to \mathfrak{s}$ defined by $g \mapsto [a, g]$ satisfies the requirements of Whitehead's lemma [16, Lemma 3, p. 77].

Hence there exists $h \in \mathfrak{s}$ such that $[h, g] = [a, g]$ for every $g \in \mathfrak{s}$, so a can be written as $a = h + (a - h)$, where $a - h \in \mathfrak{z}(\mathfrak{s})$. Since $\mathfrak{s}$ is semisimple, $\mathfrak{s} \cap \mathfrak{z}(\mathfrak{g}) = 0$, so

$$\mathfrak{n}(\mathfrak{s}) = \mathfrak{s} \oplus \mathfrak{z}(\mathfrak{s}). \tag{5.6}$$

Decomposition (5.6) implies that

$$N(S)^\circ = S \cdot Z(S)^\circ. \tag{5.7}$$

We can write $\widehat{H}^\circ$ as

$$\widehat{H}^\circ = \left(N(S) \cap Z(Z(G)) \cap N(F) \right)^\circ.$$

Using (5.7), we obtain

$$\widehat{H}^\circ = \left((S \cdot Z(S)^\circ) \cap Z(Z(G)) \cap N(F) \right)^\circ.$$

Using consequently the inclusions $S \subset Z(Z(G)) \cap N(F)$ and $Z(Z(G)) \subset Z(T)$, we can further write

$$\widehat{H}^\circ = (Z(S)^\circ \cap Z(Z(G)) \cap N(F))^\circ \cdot S = ((Z(S) \cap Z(T)) \cap Z(Z(G)) \cap N(F))^\circ \cdot S$$

Since $Z(G) = Z(S) \cap Z(T)$, the latter is equal to $(Z(G) \cap Z(Z(G)) \cap N(F))^\circ \cdot S$. Using $T \subset Z(G) \cap Z(Z(G)) \cap N(F)$, we conclude that

$$\widehat{H}^\circ = (Z(G) \cap Z(Z(G)) \cap N(F))^\circ \cdot S = (Z(G) \cap Z(Z(G)) \cap N(F))^\circ \cdot G = H.$$

Thus, $\deg H \leqslant \deg \widehat{H}$. Since any centralizer is defined by linear equations, $\deg Z(Z(G)) = 1$. By Corollary 5.8

$$\deg \widehat{H} \leqslant n^{\dim Z(Z(G)) - \dim \widehat{H}} \deg Z(Z(G)) \leqslant n^{n^2 - \dim G}.$$

Claim 3. $N(G) \cap N(F) \subset N(H)$. Consider $A \in N(G) \cap N(F)$. Since A normalizes G, it normalizes $Z(G)$. Likewise, A normalizes $Z(Z(G))$. Since A also normalizes $N(F)$, we have $A \in N(H)$. $\square$

Lemma 5.14. *Let $G \subset \operatorname{GL}_n(C)$ be a reductive subgroup such that $G \subset N(F)$ for some connected group $F \subset \operatorname{GL}_n(C)$. Then there exists a toric envelope $H \subset N(F)$ of G such that*

$$\deg H \leqslant J(n) A(n-1) n^{n^2 + n - 5}.$$

Proof. Using Corollary 5.5, we may replace G with GZ_n, so we will assume that $Z_n \subset G$. In the case that G° is a torus, the lemma follows from Corollary 5.12. Otherwise, $\dim G \geqslant \dim Z_n + \dim \operatorname{SL}_2(C) = 4$.

Since being a toric envelope is a transitive relation (see Corollary 5.3), applying Lemma 5.11, we will further assume that $[G : G^\circ] \leqslant J(n) A(n-1) n^{n-1}$. [39, Lemma 10.10] implies that $G = \Gamma G^\circ$ for some finite group Γ. Lemma 5.13 implies that there exists a toric envelope $H_0 \subset N(F)$ of G° such that $N(G^\circ) \cap N(F) \subset N(H_0)$ and $\deg H_0 \leqslant n^{n^2 - 4}$. Let $H := \Gamma H_0$. Since $\Gamma \subset N(G^\circ) \cap N(F) \subset N(H_0)$,

H is an algebraic group. Since $G^\circ \subset H_0$, $G \subset H$. Since $H^\circ = H_0$, all unipotent elements of H° belong to G°. Since also $H^\circ G \supset H^\circ \Gamma = H$, Lemma 5.2 implies that H is a toric envelope of G.

Since $H = H_0 G$ where $H_0 = H^\circ$, $[H : H^\circ] \leqslant [G : G^\circ]$. Then

$$\deg H = [H : H^\circ] \cdot \deg H^\circ \leqslant J(n) A(n-1) n^{n-1} \cdot n^{n^2-4} = J(n) A(n-1) n^{n^2+n-5}. \quad \square$$

5.4. Degree bound for product.

Lemma 5.15. *Let $G = G_0 \cdot U \subset \mathrm{GL}_n(C)$, where U is a connected unipotent group, G_0 is a reductive group, and $G \subset N(U)$. Let $\deg G_0 = D_1$, $\deg U = D_2$. Then $\deg G \leqslant D_1 D_2 2^{n(n-1)/2}$.*

Proof. The ambient space C^n carries a filtration by subspaces

$$V_i := \{ v \in C^n \mid \forall A \in U \ (A - I_n)^i v = 0 \}.$$

There exists $s < n$ such that $V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_s = C^n$. Since G_0 normalizes U, V_i is invariant with respect to G_0 for every $i \geqslant 0$. Since G_0 is reductive, there exists a decomposition $V_i = V_{i-1} \oplus W_i$ into a direct sum of G_0-representations for every $1 \leqslant i \leqslant s$. Thus, there is a decomposition $C^n = W_1 \oplus \ldots \oplus W_s$ into a direct sum of G_0-invariant subspaces. Let $n_i := \dim W_i$ for $1 \leqslant i \leqslant s$. We fix a basis of C^n that is a union of bases of $W_1, \ldots, W_s$. In this basis, every element of G_0 is of the form

$$(5.8) \qquad \begin{pmatrix} X_1 & 0 & \ldots & 0 \\ 0 & X_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & X_s \end{pmatrix}, \text{ where } X_i \in \mathrm{Mat}_{n_i}(C) \text{ for every } 1 \leqslant i \leqslant s.$$

And every element of U is of the form

$$(5.9) \qquad \begin{pmatrix} I_{n_1} & Y_{12} & \ldots & Y_{1n} \\ 0 & I_{n_2} & \ldots & Y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & I_{n_s} \end{pmatrix}, \text{ where } Y_{ij} \in \mathrm{Mat}_{n_i,n_j}(C) \text{ for every } 1 \leqslant i < j \leqslant s.$$

We denote the spaces of all the invertible matrices of the form (5.8) and (5.9) by $\mathcal{D}$ and $\mathcal{T}$, respectively. Consider the following variety

$$P := \{ (X, Y, Z) \in \mathcal{D} \times \mathcal{T} \times \mathrm{GL}_n(C) \mid X \in G_0, \ Y \in U, \ XY = Z \} \subset \mathcal{D} \times \mathcal{T} \times \mathrm{GL}_n(C).$$

Let $\pi \colon \mathcal{D} \times \mathcal{T} \times \mathrm{GL}_n(C) \to \mathrm{GL}_n(C)$ be the projection onto the last coordinate. Then $G = \pi(P)$, so $\deg G \leqslant \deg P$. Consider P as an intersection of the variety $G_0 \times U \times \mathrm{GL}_n(C)$ of degree $D_1 D_2$ with the variety defined by the n^2 equations $XY = Z$. Since the product XY is of the form

$$\begin{pmatrix} X_1 & X_1 Y_{12} & \ldots & X_1 Y_{1n} \\ 0 & X_2 & \ldots & X_2 Y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & X_n \end{pmatrix},$$

out of n^2 entries of $XY - Z$ there are

$$(5.10) \qquad \frac{n(n-1)}{2} - \frac{n_1(n_1-1)}{2} - \ldots - \frac{n_s(n_s-1)}{2} \leqslant \frac{n(n-1)}{2}$$

quadratic polynomials and the rest are linear. Thus, $\deg G \leqslant \deg P \leqslant D_1 D_2 2^{n(n-1)/2}$.

$\square$

6. Proof of Theorem 3.1

Proof of Theorem 3.1. By [27, Theorem 4, p. 286], G can be written as a semidirect product $G_0 \ltimes U$, where U is the unipotent radical of G and G_0 is a reductive subgroup of G.

We apply Lemma 5.14 with $G = G_0$ and $F = U$ and obtain a toric envelope $H_s \subset N(U)$ of G_0. Let $H_s = T \cdot G_0$, where T is a torus. We set $H := H_s \cdot U$. Since $H_s \subset N(U)$, H is an algebraic group. Since $H = T \cdot G_0 \cdot U = T \cdot G$, H is a toric envelope of G. Corollary 5.4 implies that H_s is reductive. Then Lemma 5.15 implies that

$$\deg H \leqslant 2^{n(n-1)/2} \deg H_s \deg U.$$

Using bounds for H_s and U from Lemmas 5.14 and 5.10, respectively, we obtain

$$(6.1) \qquad \deg H \leqslant J(n)A(n-1)n^{n^2+n-5}2^{(n-1)n/2}\prod_{k=1}^{n-1} k!.$$

Using $\sqrt{8n} + 1 < \sqrt{16n}$ and (5.1), we derive $J(n) \leqslant 4^{2n^2}n^{n^2}$. Using Lemma 5.9 and $2 \cdot 3^{(n-1)^2/4} \leqslant 4^{n^2}$, we derive $A(n-1) \leqslant 4^{n^2}$. Using $n! \leqslant (\frac{n+1}{2})^n$, we derive

$$\prod_{k=1}^{n-1} k! \leqslant \left(\frac{n}{2}\right)^{n(n-1)/2}.$$

Substituting all these bounds to (6.1), we obtain $\deg H \leqslant (4n)^{3n^2}$. $\square$

7. Proof of Theorem 3.2

Proof. Using Corollary 5.5, from now on we assume that G contains Z_2, the group of all scalar matrices in $\mathrm{GL}_2(C)$. Lemma 5.6 implies that $G = Z_2 G_{\mathrm{SL}}$, where $G_{\mathrm{SL}} := G \cap \mathrm{SL}_2(C)$. According to [20, p.7], there are only four options for G_{SL}.

    (a) G_{SL} is triangularizable but not diagonalizable.
    (b) G_{SL} is conjugate to a subgroup of

$$D = \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in C, ad \neq 0\right\} \cup \left\{\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \mid b, c \in C, bc \neq 0\right\}$$

    (c) G_{SL} is finite and neither of the previous two cases hold.
    (d) $G_{SL} = SL_2$

We examine each of these cases individually below.

Case (a): G_{SL} is triangularizable but not diagonalizable. We fix a basis in which G_{SL} can be represented by upper-triangular matrices. In this basis, G is also represented by upper-triangular matrices. Consider any non diagonalizable matrix in G

$$(7.1) \qquad A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix}.$$

The last expression in (7.1) is the Jordan decomposition of A. By [27, Theorem 6, p. 115], $\begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix}$ belongs to G. Since $a^{-1}b \neq 0$, the powers of this matrix generate a Zariski dense subgroup in the group U of unipotent upper-triangular matrices.

Thus, $U \subset G$. Consider the group B of all invertible upper-triangular matrices. Since B is connected and the set of unipotent elements of B is U, Lemma 5.2 implies that B is a toric envelope of G. B is defined by linear equations, so it is bounded by 1. Moreover, B is a variety of dimension 3 and degree 1.

Case (b): G_{SL} **is a subgroup of** D**.** Then G is also contained in D. Since D° is the group of diagonal matrices, the only unipotent element in D° is the identity matrix. Since D has two connected components, Lemma 5.2 implies that either D is a toric envelope of G or, if G is diagonalizable, D° is a toric envelope of G. Since D is defined inside $\mathrm{GL}_2(C)$ by quadratic equations $x_{11}x_{12} = x_{21}x_{22} = 0$, it is bounded by 2. D° is defined by linear equations and bounded by 1. Moreover, D is a variety of degree 2 and dimension 2 and D° is of degree 1 and dimension 2.

Case (c): G_{SL} **is finite and neither of the two previous cases hold.** We will use a classification of finite subgroups of $\mathrm{SL}_2(\mathbb{C})$ given in [21, §§101-103] (for a more modern treatment, see [29, Chapter 2]). Based on this classification, G_{SL} must be one of the following five types:

  (1) Cyclic Groups [21, §101, case A]
  (2) Binary Dihedral Group [21, §101, case B]
  (3) Binary Tetrahedral Group [21, §102, case C]
  (4) Binary Octahedral Group [21, §102, case D]
  (5) Binary Icosahedral Group [21, §103, case E]

In cases (1) and (2), G_{SL} is conjugate to a subgroup of D (see [21, §101, case A and B]), so these cases are already considered in Case (b). For cases (3)-(5), we take $G = Z_2 G_{\mathrm{SL}}$ to be a toric envelope of itself. Then we find a d such that G is bounded by d using Algorithm 1 (for a MAPLE code, see https://github.com/pogudingleb/ToricEnvelopes.git).

Algorithm 1 Finding a degree bound for a toric envelope of a finite subgroup of $\mathrm{SL}_2(C)$

Input: Generators of a finite subgroup $G_{\mathrm{SL}} \subset \mathrm{SL}_2(C)$
Output: Positive integer d such that $G := Z_2 G_{\mathrm{SL}}$ is bounded by d

  (1) Compute the list of all elements in G_{SL}
  (2) Compute generators of the vanishing ideal I of $G := Z_2 G_{\mathrm{SL}}$
  (3) Compute the reduced Gröbner basis B of I with respect to graded lexicographic ordering
  (4) Check all d from 1 to $\max_{p \in B} \deg p$ and find the minimum d such that

$$\sqrt{(p \in B \mid \deg p \leqslant d)} = I$$

  (5) Return d found in the previous step

Algorithm 1 outputs bounds 3, 4, and 6 for cases (3), (4), and (5), respectively. The dimension of G is one. Since each of the groups (3) (4), and (5) contains $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, the degree of G is at most half of the maximum of the cardinalities of these groups. Thus, $\deg G \leqslant 60$.

Case (d): $G_{\mathrm{SL}} = \mathrm{SL}_2(C)$**.** Then $G = Z_2 \, \mathrm{SL}_2(C) = \mathrm{GL}_2(C)$ is bounded by 0. In this case, G is a variety of dimension 4 and degree 1.

Collecting together the results for cases (a)-(d), we conclude that every algebraic subgroups $G \subset \mathrm{SL}_2(C)$ has a toric envelope bounded by six. □

From the proof of Theorem 3.2, we can extract additional information about possible toric envelopes.

Corollary 7.1. *Let $G \subset \mathrm{GL}_2(C)$ is an algebraic group. Then there exists a toric envelope H for G containing Z_2 and satisfying one of the following*

- *$\dim H = 4$ and $\deg H = 1$;*
- *$\dim H = 3$ and $\deg H = 1$;*
- *$\dim H = 2$ and $\deg H = 2$;*
- *$\dim H = 2$ and $\deg H = 1$;*
- *$\dim H = 1$ and $\deg H \leqslant 60$.*

8. Proof of Theorem 3.3

Proof. By [27, Theorem 4, p. 286], G can be written as a semidirect product $G_0 \ltimes U$, where U is the unipotent radical of G and G_0 is a reductive subgroup of G. Since G_0 is reductive, its representation in C^3 is completely reducible (see [14, Theorem 4.3, p. 117]). There are three cases for the dimensions of G_0-irreducible components of C^3.

(a) $C^3 = W_1 \oplus W_2 \oplus W_3$, where $\dim W_1 = \dim W_2 = \dim W_3 = 1$ and W_1, W_2, and W_3 are irreducible G_0-representations;

(b) $C^3 = V_1 \oplus V_2$, where $\dim V_1 = 1$, $\dim V_2 = 2$, and V_1 and V_2 are irreducible G_0-representations;

(c) C^3 is G_0-irreducible.

Case (a): $C^3 = W_1 \oplus W_2 \oplus W_3$, where $\dim W_1 = \dim W_2 = \dim W_3 = 1$ and W_1, W_2, and W_3 are irreducible representations of G_0. Then G_0 is diagonalizable in some basis, we fix such a basis. Let D be the group of all diagonal matrices in the basis. We consider $H := (D \cap N(U))^\circ \cdot G$. Since $D \cap N(U)$ commutes with G_0 and normalizes U, it normalizes G. So H is an algebraic group. Hence, H is a toric envelope of G.

Since $\deg D = 1$ and $3 \geqslant \dim(D \cap N(U)) \geqslant \dim Z_3 = 1$, Corollary 5.8 implies that $\deg(D \cap N(U)) \leqslant 9$. Lemma 5.10 implies that $\deg U \leqslant 2$. Since $D \cap N(U)$ is reductive, Lemma 5.15 implies that

$$\deg(D \cap N(U)) \cdot U \leqslant 9 \cdot 2 \cdot 8 = 144.$$

Then $\deg H \leqslant \deg(D \cap N(U))G = \deg(D \cap N(U))U \leqslant 144$.

Case (b): $C^3 = V_1 \oplus V_2$. , where $\dim V_1 = 1$, $\dim V_2 = 2$, and V_1 and V_2 are irreducible representations of G_0. According to the presentations (5.8) and (5.9) for G_0 and U constructed in the proof of Lemma 5.15, one of the following two cases holds:

either $G_0 \subset \left\{ \begin{pmatrix} A & 0 \\ 0 & b \end{pmatrix} \mid A \in \mathrm{GL}_2(C), b \in C^* \right\}$ and $U \subset \left\{ \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix} \mid u, v \in C \right\}$,

or $G_0 \subset \left\{ \begin{pmatrix} b & 0 \\ 0 & A \end{pmatrix} \mid A \in \mathrm{GL}_2(C), b \in C^* \right\}$ and $U \subset \left\{ \begin{pmatrix} 1 & u & v \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid u, v \in C \right\}$

We will consider the former. The latter is completely analogous.

Let T_1 be the group of the matrices of the form $\mathrm{diag}(1, 1, a)$, where $a \in C^*$. Since $T_1 \subset Z(G_0)$, $T_1 G_0$ is an algebraic group. Moreover, there is a decomposition $G_0 = T_1 G_1$, where G_1 acts trivially on V_1. Then G_1 can be considered as a subgroup of $\mathrm{GL}(V_2) \cong \mathrm{GL}_2(C)$. Let H_1 be a toric envelope for G_1 given by Corollary 7.1. Then there exists a torus $T_2 \subset \mathrm{GL}(V_2)$ such that $H_1 = T_2 G_1$. Then T_2 and T_1 commute, so $T := T_1 T_2$ is a torus. Thus, $H_0 := TG_0$ is a toric envelope for G_0.

We set $H := (H_0 \cap N(U)) \cdot U$. Since $G_0 \subset N(U)$, $H = (T \cap N(U))G_0 U$, so H is a toric envelope of $G = G_0 U$. Using Lemma 5.15 with more precise bound given by (5.10), we obtain

$$(8.1) \qquad\qquad \deg H \leqslant 4 \deg(H_0 \cap N(U)) \deg U.$$

Direct computation shows that any subgroup of

$$\left\{ \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; u, v \in C \right\}$$

is an affine subspace of $\mathrm{Mat}_3(C)$, so $\deg U = 1$. Both T_1 and $Z_2 \subset H_1$ normalize U, so $\dim(H_0 \cap U) \geqslant 2$. Using Corollary 5.8 and classification from Corollary 7.1, we obtain

$$\deg(H_0 \cap N(U)) \leqslant 3^{\dim H_1 - 1} \deg H_1 \leqslant \max(27 \cdot 1, 9 \cdot 1, 3 \cdot 2, 1 \cdot 60) = 60.$$

Plugging all the bounds into (8.1), we obtain $\underline{\deg H \leqslant 240}$.

Case (c): C^3 **is G_0-irreducible.** Since the space of fixed vectors of U is G_0-invariant, it coincides with C^3, so $U = \{e\}$. [3, Proposition, p. 181] implies that G_0° can be written as ST, where $T := C(G_0^\circ)^\circ$ is torus and $S := [G_0^\circ, G_0^\circ]$ is semisimple.

If C^3 is an irreducible S-representation, let $H := Z_3 \cdot G$. As in the proof of Lemma 5.13 (see (5.7)), one can show that $N(S)^\circ = SZ(S)^\circ$. Schur's lemma implies that $Z(S) = Z_3$. Since $H \subset N(S)$ and $H^\circ \supset S \cdot Z(S)$, we obtain that $H^\circ = N(S)^\circ$, so $\deg H \leqslant \deg N(S)$. Since $\dim N(S) \geqslant \dim Z_3 + \dim S \geqslant 4$, Corollary 5.8 applied with $G_0 = \mathrm{GL}_3(C)$ and $G_1 = S$ implies that $\underline{\deg H \leqslant 3^5 = 243}$.

If C^3 is not an irreducible representation of S, then there exists an S-invariant one-dimensional subspace spanned by a vector v. Since $[S, S] = S$, $gv = v$ for every $g \in S$. Consider a subspace $I = \{u \in C^3 \mid \forall g \in S \ gu = u\}$. Since $v \in I$, $\dim I > 0$. Since S is normal in G_0, I is G_0-invariant. Since C^3 is G_0-irreducible, $I = C^3$, so $S = \{e\}$. Since $U = S = \{e\}$, [39, Lemma 10.10] implies that $G = G_0 = \Gamma T$ for some finite Γ.

Let T_0 be any maximal element of the set of all the tori containing T and normalized by Γ. We set $H := T_0 \cdot G$, then H is a toric envelope of G. Since T_0 is a torus, all its irreducible representations are one-dimensional and are described by characters of T_0. We denote distinct characters of T_0 by $\chi_1, \ldots, \chi_s$. Then we write

$$C^3 = \bigoplus_{i=1}^{s} V_{\chi_i}, \text{ where } V_{\chi_i} := \{v \mid \forall g \in T_0 \ gv = \chi_i(g)v\} \neq \{0\} \text{ for } i = 1, \ldots, s.$$

Since Γ normalizes T_0, for every $1 \leqslant i \leqslant s$, there exists $1 \leqslant j \leqslant s$ such that $\Gamma(V_{\chi_i}) \subset V_{\chi_j}$. Consider possible values of s

s = 1. Then $T \subset Z_3$, so $T_0 = Z_3$. By Lemma 5.6, we can further assume that $\Gamma \subset \mathrm{SL}_3(C)$. We will use the classification of finite subgroups of $\mathrm{SL}_3(C)$ from [40, p. 2-3] (see also [29, §3]).

Since there is no torus strictly containing Z_3 that is normalized by Γ, Γ is an imprimitive subgroup of $\mathrm{SL}_3(C)$ (see [40, p. 10]). Thus, only cases (E)-(K) from [40, p. 2-3] are possible. One can see that every group Γ of types (E)-(K) satisfies one of the following

- $|\Gamma| \leqslant 360$ (cases (E), (F), (H), (I), and (J));
- $|\Gamma| \leqslant 1080$ and Γ contains a matrix ωI_3, where ω is a primitive cubic root of unity and I_3 is the identity matrix (cases (J), (L), and (K)).

In both cases we have $\deg H \leqslant |\Gamma|/|\Gamma \cap Z_3| \leqslant 360$.

s = 2. Without loss of generality we can assume that $\dim V_{\chi_1} = 2$ and $\dim V_{\chi_2} = 1$. Then V_{χ_1} is an invariant subspace for both Γ and T_0. This contradicts the assumption that C^3 is an irreducible G_0-representation.

s = 3. If we choose a basis e_1, e_2, e_3 such that $e_i \in V_{\chi_i}$ for $1 \leqslant i \leqslant s$, every element of G can be written in this basis as a product of a diagonal matrix and a permutation matrix. Let D be a group of all diagonal matrices in this basis. Then Γ normalizes D and $T_0 \subset D$, so $T_0 = D$. Thus, $H := \Gamma D$. Since the number of connected component of H does not exceed the number of permutation matrices and $\deg D = 1$, we have $\deg H \leqslant 3! = 6$.

In all the cases above, we constructed a toric envelope H of G such that $\deg H \leqslant 360$. $\square$

References

1. Moulay Barkatou, Thomas Cluzeau, Jacques-Arthur Weil, and Lucia Di Vizio, *Computing the Lie algebra of the differential Galois group of a linear differential system*, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, 2016, pp. 63–70.
2. Frits Beukers, *Differential galois theory*, From Number Theory to Physics (Michel Waldschmidt, Pierre Moussa, Jean-Marc Luck, and Claude Itzykson, eds.), Springer Berlin Heidelberg, 1992, pp. 413–439.
3. Armand Borel, *Linear algebraic groups*, 2nd ed., Springer-Verlag New York, 1991.
4. Michel Brion, *Groupe de Picard et nombres caractéristiques des variétés sphériques*, Duke Mathematical Journal **58** (1989), no. 2, 397–424.
5. Elie Compoint and Michael F. Singer, *Computing Galois groups of completely reducible differential equations*, Journal of Symbolic Computation **28** (1999), no. 4, 473–494.
6. Chales W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, John Wiley & Sons, 1962.
7. Willem Adriaan de Graff, *Computation with linear algebraic groups*, CRC Press, 2017.
8. Harm Derksen, *Computation of invariants for reductive groups*, Advances in Mathematics **141** (1999), no. 2, 366 – 384.
9. _____, *Polynomial bounds for rings of invariants*, Proceedings of American Mathematical Society **129** (2001), 955–963.
10. Ruyong Feng, *Hrushovski's algorithm for computing the Galois group of a linear differential equation*, Advances in Applied Mathematics **65** (2015), 1–37.
11. Julia Hartmann, *On the inverse problem in differential Galois theory*, Journal für die reine und angewandte Mathematik **2005**, no. 586, 21–44.

12. Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, no. 52, Springer, 1977.

13. Joos Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoretical Computer Science **24** (1983), no. 3, 239–277.

14. Gerhard P. Hochschild, *Basic theory of algebraic groups and Lie algebras*, Springer-Verlag New York, 1981.

15. Ehud Hrushovski, *Computing the Galois group of a linear differential equation*, Banach Center Publications **58** (2002), no. 1, 97–138.

16. N. Jacobson, *Lie algebras*, Dover books on advanced mathematics, Dover, 1979.

17. Gabriela Jeronimo and Juan Sabia, *Effective equidimensional decomposition of affine varieties*, Journal of Pure and Applied Algebra **169** (2002), no. 2, 229–248.

18. C. Jordan, *Mémoire sur les équations différentielles linéaires à intégrale algébrique*, Journal für die reine und angewandte Mathematik **84** (1878), 89–215.

19. Boris Ya. Kazarnovskii, *Newton polyhedra and Bezout's formula for matrix functions of finite-dimensional representations*, Functional Analysis Applications **21** (1987), no. 4, 319–321.

20. Jerald J. Kovacic, *An algorithm for solving second order linear homogeneous differential equations*, Journal of Symbolic Computation **2** (1986), no. 1, 3–43.

21. G.A. Miller, H.F. Blichfeldt, and L.E. Dickson, *Theory and applications of finite groups*, John Wiley & Sons, 1916.

22. Andrei Minchenko, Alexey Ovchinnikov, and Michael F. Singer, *Unipotent differential algebraic groups as parameterized differential Galois groups*, Journal of the Institute of Mathematics of Jussieu **13** (2014), no. 4, 671–700.

23. ———, *Reductive linear differential algebraic groups and the Galois groups of parameterized linear differential equations*, International Mathematics Research Notices **2017** (2015), no. 7, 1733–1793.

24. Claude Mitschi and Michael F. Singer, *Connected linear groups as differential Galois groups*, Journal of Algebra **184** (1996), no. 1, 333–361.

25. Juan J. Morales-Ruiz, *Integrable systems and difierential galois theory*, pp. 1–33, Springer International Publishing, 2016.

26. Morris Newman, *Integral matrices*, Academic Press, 1972.

27. A.L. Onishchik and E.B. Vinberg, *Lie groups and algebraic groups*, Springer-Verlag, 1990.

28. Daniel Rettstadt, *On the computation of the differential Galois group*, Ph.D. thesis, 2014.

29. Javier Carrasco Serrano, *Finite subgroups of $(2, \mathbb{C})$ and $(3, \mathbb{C})$*, Ph.D. thesis, University of Warwick, 2014.

30. Michael F. Singer, *Moduli of linear differential equations on the Riemann sphere with fixed Galois groups.*, Pacific Journal of Mathematics **160** (1993), no. 2, 343–395.

31. Michael F. Singer and Felix Ulmer, *Galois groups of second and third order linear differential equations*, Journal of Symbolic Computation **16** (1993), no. 1, 9–36.

32. Mengxiao Sun, *A new bound on Hrushovski's algorithm for computing the Galois group of a linear differential equation*, 2018, preprint.

33. Ken-Ichi Tahara, *On the finite subgroups of $\mathrm{GL}(3, \mathbb{Z})$*, Nagoya Math. J. **41** (1971), 169–209.

34. Carol Tretkoff and Marvin Tretkoff, *Solution of the inverse problem of differential Galois theory in the classical case*, American Journal of Mathematics **101** (1979), no. 6, 1327–1332.

35. Joris van der Hoeven, *Around the numeric-symbolic computation of differential Galois groups*, Journal of Symbolic Computation **42** (2007), no. 1, 236–264.

36. Marius van der Put and Michael F. Singer, *Galois theory of linear differential equations*, Springer-Verlag Berlin Heidelberg, 2003.

37. Mark van Hoeij and Jacques-Arthur Weil, *An algorithm for computing invariants of differential Galois groups*, Journal of Pure and Applied Algebra **117–118** (1997), 353–379.

38. E. P. Vdovin, *Maximal orders of abelian subgroups in finite Chevalley groups*, Mathematical Notes **69** (2001), no. 3, 475–498.

39. Bertram A. F. Wehrfritz, *Infinite linear groups*, Springer, Berlin, Heidelberg, 1973.

40. Stephen S.-T. Yau and Yung Yu, *Gorenstein quotient singularities in dimension three*, Memoirs of the AMS, no. 505, American Mathematical Society, 1993.

DEPARTMENT OF MATHEMATICS, CUNY GRADUATE CENTER, 365 FIFTH AVENUE, NEW YORK, USA

Current address: Department of Mathematics, The City College of New York, New York, USA

Email address: `eamzallag@gradcenter.cuny.edu`

FACULTY OF MATHEMATICS, UNIVERSITY OF VIENNA, OSKAR-MORGENSTERN-PLATZ 1, VIENNA, AUSTRIA

Email address: `an.minchenko@gmail.com`

COURANT INSTITUTE OF MATHEMATICAL SCIENCES, NEW YORK UNIVERSITY, 251 MERCER ST., NEW YORK, USA

Current address: LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, Palaiseau, France

Email address: `gleb.pogudin@polytechnique.edu`