A new bound on Hrushovski's algorithm for computing the Galois group of a linear differential equation

Mengxiao Sun

Taylor & Francis
Taylor & Francis Group

Check for updates

A new bound on Hrushovski's algorithm for computing the Galois group of a linear differential equation

Mengxiao Sun

City University of New York Graduate School and University Center, New York, New York, USA

ABSTRACT

The complexity of computing the Galois group of a linear differential equation is of general interest. In a recent work, Feng gave the first degree bound on Hrushovski's algorithm for computing the Galois group of a linear differential equation. This bound is the degree bound of the polynomials used in the first step of the algorithm for finding a proto-Galois group (see Definition 2.7) and is sextuply exponential in the order of the differential equation. In this paper, we use Szántó's algorithm of triangular representation for algebraic sets to analyze the complexity of computing the Galois group of a linear differential equation and we give a new bound which is triple exponential in the order of the given differential equation.

1. Introduction

The differential Galois group (see Definition 2.5) is an analog for a linear differential equation of the classical Galois group for a polynomial equation. An important application of the differential Galois group is that a linear differential equation can be solved by integrals, exponentials and algebraic functions if and only if the connected component of its differential Galois group is solvable [8, 19]. For example [9, Appendix], the differential Galois group of Bessel's equation $t^2 y'' + ty' + (t^2 - \nu^2)y = 0$ over $\mathbb{C}(t)$ is isomorphic to $SL_2(\mathbb{C})$ (not solvable) when $\nu \notin \frac{1}{2} + \mathbb{Z}$. In other words, Bessel's equation cannot be solved by integrals, exponentials and algebraic functions unless $\nu \in \frac{1}{2} + \mathbb{Z}$. Computing the differential Galois groups would help us determine the existence of the solutions expressed in terms of elementary functions (integrals, exponentials and algebraic functions) and understand the algebraic relations among the solutions.

Hrushovski in [5] first proposed an algorithm for computing the differential Galois group of a general linear differential equation over $k(t)$ where k is a computable algebraically closed field of characteristic zero. Recently, Feng approached finding a complexity bound of the algorithm in [4], which is the degree bound of the polynomials used in the first step of the algorithm for finding a proto-Galois group (see Definition 2.7), but not for the whole algorithm. The bound given by Feng is sextuply exponential in the order n of the differential equation.

In this paper, we present a triple exponential degree bound using triangular sets instead of Gröbner bases for representing the algebraic sets. In general, the degrees of defining equations of a differential Galois group cannot be bounded by a function of n only. For example [13, Example

---

1.3.7, page 12], the differential Galois group of $y' = \frac{1}{mt}y$ over $\mathbb{C}(t)$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$ where m is a positive integer, which implies that the degree of the defining equation $x^m - 1$ is m.

A crucial point of Hrushovski's algorithm is that one can find a proto-Galois group which is an algebraic subgroup of $GL_n(k)$, provided that the degree bound of the defining equations of the proto-Galois group is computed. The differential Galois group can then be recovered from the proto-Galois group (more details in [4, 5]). Therefore, a bound for the proto-Galois group plays an important role in determining the complexity of Hrushovski's algorithm. Following Feng's approach, we prove that such a proto-Galois group exists by constructing a family $\mathcal{F}$ of algebraic subgroups such that the identity component of any algebraic subgroup $H' \subseteq GL_n(k)$ is contained in some H of $\mathcal{F}$ and $[H'H : H]$ is uniformly bounded. We also prove that the degrees of the defining equations of any element of $\mathcal{F}$ are bounded by $\bar{d}$ depending on the order n of the given differential equation. This is stated as Theorem 3.1. Then by collecting the algebraic subgroups $\bar{H}$ such that there is some H of $\mathcal{F}$ such that $[\bar{H} : H] \leq \bar{d}$, we obtain a family $\bar{\mathcal{F}}$ of algebraic subgroups in which one can always find a proto-Galois group for any linear differential equation. Moreover, we give a numerical degree bound of the defining equations of any algebraic subgroup of $\bar{\mathcal{F}}$. This is stated as Corollary 3.1.

Using degrees of defining equations of algebraic subgroups to bound $\bar{\mathcal{F}}$, one needs an upper degree bound of the defining equations of the algebraic subgroups of $\mathcal{F}$ and an upper bound of $[\bar{H} : H]$. Hence, a double-exponential degree bound for computing Gröbner bases would be involved if one chooses to represent an algebraic subgroup by the generating set of its defining ideal (generated by the defining equations). In order to give a better bound, we represent an algebraic subgroup by the triangular sets (see Definition 3.2) instead of the generating set in the process of constructing $\mathcal{F}$. In such a process, we need to take the differences between Gröbner bases and triangular sets into account. We apply Szántó's modified Wu-Ritt type decomposition algorithm [15, 16] which has been proved to be more efficient than computing a Gröbner basis and make use of the numerical bound for Szántó's algorithm [1] to adapt to the complexity analysis of Hrushovski's algorithm. In doing this, we are able to avoid working with Gröbner bases to get a better bound of the degrees of the defining equations of the algebraic subgroups of $\mathcal{F}$ which is triple exponential in the order n of the given differential equation. Additionally, we are able to not increase the degree bound of the defining equations of the algebraic subgroups of $\bar{\mathcal{F}}$. Each element $\bar{H}$ of $\bar{\mathcal{F}}$ is a union of at most $\bar{d}$ cosets of some element H of $\mathcal{F}$. The degree bound for the generating set of the ideal generated by the defining equations of $\bar{H}$ would be raised to an exponent at most $\bar{d}$, which results in a big increase on the degrees of the defining equations of the algebraic subgroups of $\bar{\mathcal{F}}$. However, this issue has been resolved when expressing the algebraic subgroups by triangular sets. More details can be found in Sections 2 and 3.

Besides Hrushovski's general algorithm, there are other algorithmic results in the Galois theory of linear differential equations. Kovacic in [10] presented an algorithm for computing the Galois group of a second-order linear differential equation. The Galois groups of second- and third-order linear differential equations were studied by Singer and Ulmer in [14]. Compoint and Singer in [2] proposed an algorithm for computing the Galois group if the differential equation is completely reducible. The numeric-symbolic computation of differential Galois groups was presented by van der Hoeven in [17]. For more details on the differential Galois theory from an algorithmic point of view, readers are referred to [18] and [13].

This paper is organized as follows. In Sections 2.1 and 2.2, we introduce the notations, definitions and facts from triangular sets and differential Galois groups. In Section 3.1, we state and prove the preparation lemmas which we use in analyzing the complexity of the algorithm. In Section 3.2, we present and prove the new complexity bound of Hrushovski's algorithm. In Section 4, we compare our bounds when $n = 2$ with the ones in [4, Proposition B.11, Proposition B.14].

2. Preliminaries

2.1. Triangular sets and Szántó's algorithm

Definition 2.1. Fix a monomial ordering with $x_1 < x_2 < ... < x_n$ in a polynomial ring $k[x_1, ..., x_n]$. Let $f \in k[x_1, ..., x_n]$. Then *class* (f) denotes the highest indeterminate in f.

Definition 2.2. Fix a monomial ordering with $x_1 < x_2 < ... < x_n$ in a polynomial ring $k[x_1, ..., x_n]$. A sequence of polynomials $\{g_1, ..., g_m\}$ is called a triangular set if *class* $(g_i) < $ *class* (g_j) for all $i < j$.

The pseudo division is a method of division for multivariate polynomials which is a generalization of the method of division for univariate polynomials.

Let $f \in k[x_1, ..., x_n]$ and $G = \{g_1, ..., g_m\}$ be a triangular set in $k[x_1, ..., x_n]$. We denote the leading coefficient of g_i by lc (g_i). There exist polynomials $q_1, ..., q_m$ and $\alpha_1, ..., \alpha_m \in \mathbf{N}$ such that lc $(g_1)^{\alpha_1}...$lc $(g_m)^{\alpha_m} f = \Sigma_{i=1}^m q_i g_i + f_0$ where $\deg_{x_{j_i}} (f_0) < \deg_{x_{j_i}} (g_i)$ if class $(g_i) = x_{j_i}$ for $1 \leq i \leq m$. We call f_0 the pseudo remainder of f by G, denoted by prem (f, G). If $f = $ prem (f, G), then we say that f is reduced modulo G.

Definition 2.3. A triangular set $G \subseteq k[x_1, ..., x_n]$ represents an ideal I if $I = \{f \in k[x_1, ..., x_n] : $ prem $(f, G) = 0\}$. We denote the ideal represented by G by *rep* (G).

In general, a triangular set is not a generating set of the ideal which it represents and has more zeros than the ideal. Consider a triangular set $G = \{xy\} \subseteq \mathbb{C}[x, y]$ with $x < y$. G has a zero $(0, -2)$ which is not in zero (rep (G)) because $y \in$ rep (G).

Note that rep (G) is not necessarily an ideal. Consider a triangular set $G = \{x, xy\} \subseteq \mathbb{C}[x, y]$ with $x < y$. y and $y + 1$ are in rep (G), but $y - (y + 1) = -1$ is not in rep (G).

Szántó in [15] and [16] presented a Wu-Ritt type decomposition algorithm expressing the radical of an ideal as an intersection of radical ideals represented by unmixed triangular sets. An unmixed triangular set is a triangular set with some certain conditions. For our purposes, we state the following theorem without emphasizing the" unmixed" property of triangular sets.

Theorem 2.1. [16, Theorem 4.1.7] *Let* $I \subseteq k[x_1, ..., x_n]$ *be an ideal. Then there is an algorithm which computes a triangular representation of I, that is computing a family of triangular sets* G_i *such that* $\sqrt{I} = \cap_{i=1}^m I_i$ *where* $I_i = $ rep (G_i) *for each* i.

Definition 2.4. An ideal $I \subseteq k[x_1, ..., x_n]$ is bounded by d if any polynomial p_j in the generating set $\{p_1, ..., p_m\}$ of I has degree not greater than d.

In order to get a numerical complexity bound for Hrushovski's algorithm, we need a numerical complexity bound for Szántó's algorithm, which is stated as the following theorem.

Theorem 2.2. [1, Theorem 3.5] *Suppose that* $n > 1$ *and* $I \subseteq k[x_1, ..., x_n]$ *is an ideal bounded by d. Then all the polynomials appearing during the computations and in the output of Szántó's algorithm have degrees not greater than* $nd^{5.5n^3}$.

2.2. Differential Galois groups and Hrushovski's algorithm

We consider a linear differential equation in the matrix form:

$$\delta(Y) = AY \qquad (1)$$

where Y is a vector containing n unknowns and A is an $n \times n$ matrix with entries in $k(t)$. Denote the Picard–Vessiot extension field of the differential field $k(t)$ by K with the derivation $\delta = \frac{d}{dt}$ and the solution space of (1) by V in K. Let $F \in GL_n(K)$ be a fundamental matrix of (1). Let $GL(V)$

be the group of automorphisms of the solution space V. Then there is a group isomorphism Φ_F: $GL(V) \rightarrow GL_n(k)$ sending $\sigma \in GL(V)$ to $M_\sigma \in GL_n(k)$ where $FM_\sigma = \sigma(F)$.

Definition 2.5. The Galois group $\mathcal{G}$ of (1) is the group of $k(t)$-automorphisms of K which commutes with the derivation and fixes $k(t)$ pointwise.

Definition 2.6. An algebraic subgroup H of $GL_n(k)$ is bounded by d if there exist finitely many polynomials $p_1, ..., p_m \in k[x_{i,j}]_{1<i,j<n}$ of degrees not greater than d such that $H = \text{zero } (p_1, ..., p_m) \cap GL_n(k)$.

Let $H \subseteq GL_n(k)$ be an algebraic subgroup. Let H^0 be the identity component of H and $\Phi_F(\mathcal{G})^0$ be identity component of $\Phi_F(\mathcal{G})$. Let $(H^0)^t$ be the intersection of kernels of all characters of H^0.

The definition of a proto-Galois group of (1) was introduced by Feng in [4], which is as follows:

Definition 2.7. ([4, Definition 1.1]). If there is an algebraic subgroup H of $GL_n(k)$ such that

$$(H^0)^t \trianglelefteq \Phi_F(\mathcal{G})^0 \subseteq \Phi_F(\mathcal{G}) \subseteq H,$$

then H is called a proto-Galois group of (1).

In Hrushovski's algorithm, one can compute an integer $\tilde{d}$ such that there is a proto-Galois group H of $GL_n(k)$ bounded by $\tilde{d}$. The bound $\tilde{d}$ is given by Feng in [4].

Example 2.1. Consider the first-order linear differential equation $y' = \frac{1}{3t}y$ over $\mathbb{C}(t)$. The differential Galois group is the subgroup $\{1, -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}-\frac{\sqrt{3}}{2}i\} \subseteq \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of complex numbers [13, Example 1.3.7, page 12]. The identity component of $\mathbb{C}^*$ is itself. The intersection of kernels of all characters of $\mathbb{C}^*$ is trivial because the identity map of $\mathbb{C}^*$ is a character. So in this case $\mathbb{C}^*$ is a proto-Galois group.

Example 2.2. Consider the Airy equation $y'' = ty$ over $\mathbb{C}(t)$. The differential Galois group is the subgroup $SL_2(\mathbb{C}) \subseteq GL_2(\mathbb{C})$ [19, Example 8.15, page 250]. The identity component of $SL_2(\mathbb{C})$ is itself because $SL_2(\mathbb{C})$ is connected. The identity component of $GL_2(\mathbb{C})$ is itself because $GL_2(\mathbb{C})$ is connected. A character ϕ of $GL_2(\mathbb{C})$ is of the form $\forall g \in GL_2(\mathbb{C})$ $\phi(g) = (\det(g))^n$ where det is the determinant map and $n \in \mathbb{N}$. So the intersection of kernels of all characters of $GL_2(\mathbb{C})$ is $SL_2(\mathbb{C})$. So $GL_2(\mathbb{C})$ is a proto-Galois group. From Definition 2.7, it is not hard to see the differential Galois group itself is a proto-Galois group.

Example 2.3. Consider the second-order linear differential equation $y'' + \frac{1}{t}y' = 0$ over $\mathbb{C}(t)$. The differential Galois group is

$$\left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbb{C} \right\}$$

[3, Example 4.1, page 90]. The same analysis in Example 2.2 shows that the intersection of kernels of all characters of $GL_2(\mathbb{C})$ is $SL_2(\mathbb{C})$. But $GL_2(\mathbb{C})$ is not contained in the identity component of the differential Galois group. So in this case $GL_2(\mathbb{C})$ cannot be a proto-Galois group. The intersection of kernels of all characters of $SL_2(\mathbb{C})$ is itself which is not contained in the identity component of the differential Galois group. So in this case $SL_2(\mathbb{C})$ cannot be a proto-Galois group.

Example 2.4. Consider the second-order linear differential equation $y''-2ty'-2y = 0$ over $\mathbb{C}(t)$. The differential Galois group is

$$\left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} : a, b, c \in \mathbb{C}, ab \neq 0 \right\}$$

[11, Example 6.10, pages 81,82,83]. The same analysis in Example 2.3 shows that in this case $GL_2(\mathbb{C})$ cannot be a proto-Galois group. The differential Galois group in this case is not even a subgroup of $SL_2(\mathbb{C})$, so $SL_2(\mathbb{C})$ cannot be a proto-Galois group.

Remark. The proto-Galois group of a linear differential equation is not unique. As shown in Examples 2.1 and 2.2, the proto-Galois group can be far from the differential Galois group. But a group being large does not make it a proto-Galois group as shown in Examples 2.3 and 2.4.

Hrushovski in [5, Corollary 3.7] proved that one can compute an integer d_3 such that there is a proto-Galois group H of $GL_n(k)$ bounded by d_3. Feng in [4, Proposition B.14] gave the first explicit bound for d_3 which is sextuply exponential in the order n of the given linear differential equation.

To understand the key role of the integer d_3 in analyzing the complexity of Hrushovski's algorithm, we separate the algorithm in three main steps following the way in which Feng in [4] described it.

Definition 2.8. Let $\tilde{V} = \{Fh : h \in GL_n(k)\}$. A subset V_0 of $\tilde{V}$ is defined by finitely many polynomials $p_1, ..., p_m$ if $V_0 = zero\ (p_1, ..., p_m) \cap \tilde{V}$ where $zero\ (p_1, ..., p_m)$ denotes the zero set of $\{p_1, ..., p_m\}$ in $k^{n \times n}$. If $p_1, ..., p_m$ have coefficients in k, we say that V_0 is k-definable subset of $\tilde{V}$.

- In the first step, we compute a proto-Galois group H of (1) bounded by d_3. The existence of H is guaranteed by [5, Corollary 3.7]. Let $N_{d_3}(\tilde{V})$ be the set of all subsets of $\tilde{V}$ defined by finitely many polynomials of degrees not greater than d_3. Then one can compute H by the intersection of the stabilizers of k-definable elements in $N_{d_3}(\tilde{V})$.
- In the second step, we compute the identity component $(\Phi_F(\mathcal{G}))^0$ of $\Phi_F(\mathcal{G})$. Let $\chi_1, \ldots, \chi_l$ be the generators of the character group of $(\Phi_F(\mathcal{G}))^0$. Let $\hat{k}$ be an algebraic extension of $k(t)$. Then $\chi(\Phi_F(\mathcal{G})^0)$ is the Galois group of some exponential extension $\hat{K}$ of $\hat{k}$ where $\chi = (\chi_1, \ldots, \chi_l)$. $\hat{K}$ can be obtained by computing hyperexponential solutions of some symmetric power system of (1). $(\Phi_F(\mathcal{G}))^0$ can be found by the pre-image of $\chi(\Phi_F(\mathcal{G})^0)$ in $(\Phi_F(\mathcal{H}))^0$.
- In the last step, we compute the differential Galois group $\mathcal{G}$ of (1). Let $\mathcal{G}^0$ be the pre-image of $(\Phi_F(\mathcal{G}))^0$. Find a Galois extension k_G of $k(t)$ and a k_G-definable subset V_{k_G} of $\tilde{V}$ such that $\mathcal{G}^0$ = stab (V_{k_G}) where stab (V_{k_G}) is the stabilizer of V_{k_G}. Then

$$\mathcal{G} = \bigcup_{i=0}^{m} \left\{ \sigma \in GL(V) | \sigma(V_{k_G}) = V_i \right\}$$

where V_i is the orbit of V_{k_G} under the action of Gal $(k_G/k(t))$.

From the first step of the algorithm, we can see that the integer d_3 determines the complexity of computing a proto-Galois group. The differential Galois group is obtained by recovering the proto-Galois group in the next two steps. Therefore d_3 plays an important role in determining the complexity of the whole algorithm.

3. Complexity bound on Hrushovski's algorithm

3.1. Preparation

Definition 3.1. We say that an ideal $I \subseteq k[x_1, ..., x_n]$ has a triangular representation if $\sqrt{I}$ is expressed by an intersection of radical ideals I_i such that for each i, $I_i =$ rep (G_i) where G_i is a triangular set in I_i. A triangular representation of I is bounded by d if every polynomial in G_i has degree not greater than d.

Definition 3.2. An algebraic subgroup $H \subseteq GL_n(k)$ is said to have a triangular representation if the ideal generated by the defining equations of H has a triangular representation. A triangular representation of H is bounded by d if every polynomial in the triangular representation has degree not greater than d.

Let $I \subseteq k[x_1, ..., x_n]$ be an ideal. In [4, Proposition B.2], Feng gave a degree bound for $I \cap k[x_1, ..., x_r]$ which is double-exponential in n using the computation of Gröbner bases. In the following lemma, we give a degree bound for the triangular representation of $I \cap k[x_1, ..., x_r]$ which is polynomial exponential in n.

Lemma 3.1. *Assume that $n > 1$. Let $I \subseteq k[x_1, ..., x_n]$ be an ideal bounded by d and $1 \leq r \leq n$. Then $I \cap k[x_1, ..., x_r]$ has a triangular representation bounded by $nd^{5.5n^3}$.*

Proof. Assume that $\sqrt{I} = \cap_i I_i$ is a triangular representation of I where $I_i = \text{rep } (G_i)$ and G_i is a triangular set of I_i. Since

$$\sqrt{I} \cap k[x_1, ..., x_r] = \sqrt{I \cap k[x_1, ..., x_r]},$$

it suffices to show that for each i

$$\text{rep } (G_i \cap k[x_1, ..., x_n]) \cap k[x_1, ..., x_r] = \text{rep } (G_i) \cap k[x_1, ..., x_r] \tag{2}$$

where $\text{rep } (G_i \cap k[x_1, ..., x_n])$ is an ideal in $k[x_1, ..., x_n]$. Let $g \in$ LHS of (2). Then

$$\text{prem } (g, G_i \cap k[x_1, ..., x_r]) = 0.$$

If $G_i \subseteq k[x_1, ..., x_r]$, then

$$\text{prem } (g, G_i) = \text{prem } (g, G_i \cap k[x_1, ..., x_r]).$$

So $\text{prem } (g, G_i) = 0$. If $G_i \nsubseteq k[x_1, ..., x_r]$, then G_i must have at least one polynomial containing terms larger than x_r. Let $G_i = \{g_{i,1}, ..., g_{i,s}\}$ and assume that $g_{i,j+1}, ..., g_{i,s}$ contain terms larger than x_r. Then

$$G_i \cap k[x_1, ..., x_r] = \{g_{i,1}, ..., g_{i,j}\}$$

with $j < s$. Since $g \in k[x_1, ..., x_r]$, g is reduced modulo $g_{i,j}, ..., g_{i,s}$. Then $\text{prem } (g, G_i) = 0$. So $g \in$ RHS of (2). Let $f \in$ RHS of (2). Then $f \in k[x_1, ..., x_r]$ and $\text{prem } (f, G_i) = 0$. Since $f \in k[x_1, ..., x_r]$, f is reduced modulo polynomials containing terms larger than x_r in G_i. So

$$\text{prem } (f, G_i \cap k[x_1, ..., x_r]) = 0.$$

So $f \in$ LHS of (2). Therefore, $I \cap k[x_1, ..., x_r]$ has a triangular representation which is

$$\sqrt{I \cap k[x_1, ..., x_r]} = \cap_i I_i'$$

where

$$I_i' = \text{rep } (G_i \cap k[x_1, ..., x_r])$$

where $\text{rep } (G_i \cap k[x_1, ..., x_r])$ is an ideal in $k[x_1, ..., x_r]$. By Theorem 2.1, the triangular representation of $I \cap k[x_1, ..., x_r]$ is bounded by $nd^{5.5n^3}$. □

Lemma 3.2. *Let $I, J \subseteq k[x_1, ..., x_n]$ be ideals. Assume that I and J have triangular representations bounded by d. Then IJ has a triangular representation bounded by d.*

Proof. Suppose that $\sqrt{I} = \cap_i I_i$ and $\sqrt{J} = \cap_j J_j$ are triangular representations of I and J. Then $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J} = (\cap_i I_i) \cap (\cap_j J_j)$. So if $I_i = \text{rep } (G^{I_i})$ and $J_j = \text{rep } (G^{J_j})$ for some triangular sets

G^{I_i} and G^{J_j}, then $\sqrt{IJ} = (\cap \mathrm{rep}(G^{I_i})) \cap (\cap \mathrm{rep}(G^{J_j}))$. Therefore, IJ has a triangular representation bounded by d. ☐

Definition 3.3. We say that a family $\mathcal{F}$ of algebraic subgroups in $GL_n(k)$ is represented by a family of triangular sets if any $H \in \mathcal{F}$ has a triangular representation, and $\mathcal{F}$ is bounded by d if the triangular representations of any $H \in \mathcal{F}$ are bounded by d.

Let $H \subseteq GL_n(k)$ be an algebraic subgroup. Let $\tau : H \to GL_l(k)$ be a homomorphism where l is a positive integer. Assume that $\tau = (\frac{P_{i,j}}{Q})$, where P and Q are polynomials with coefficients in k and $1 \le i, j \le l$. The homomorphism τ is said to be bounded by d if the polynomials $P_{i,j}$ and Q have degrees not greater than d.

In [4, Lemma B.5], Feng gave a degree bound for the generating set of the ideal generated by the defining equations of $\tau^{-1}(H' \cap \tau(H))$ where $H \subseteq GL_n(k)$ and $H' \subseteq GL_l(k)$. We use a similar argument to give in the following lemma a bound for the triangular representation of $\tau^{-1}(H' \cap \tau(H))$.

Lemma 3.3. *Assume that $n > 1$. Let $H \subseteq GL_n(k)$ be an algebraic subgroup whose triangular representation bounded by d and $H' \subseteq GL_l(k)$ be an algebraic subgroup whose triangular representation bounded by d'. Assume that the homomorphism $\tau : H \to GL_l(k)$ is bounded by m. Then $\tau^{-1}(H' \cap \tau(H))$ has a triangular representation bounded by $n(\max(d, md'))^{5.5n^3}$.*

Proof. Let $I(H)$ be the ideal generated by the defining equations of H and $I(H')$ be the ideal generated by the defining equations of H'. Let X be the set of indeterminates $x_{\alpha,\beta}, 1 \le \alpha, \beta \le n$ and Y be the set of indeterminates $y_{\zeta,\eta}, 1 \le \zeta, \eta \le l$. Assume that $\tau = (\frac{P_{i,j}}{Q})_{1 \le i,j \le l}$ where $P_{i,j}$ and Q are polynomials in $k[X]$. Assume that H has a triangular representation

$$\sqrt{I(H)} = \underset{r}{\cap} \mathrm{rep}(G_r)$$

and H' has a triangular representation

$$\sqrt{I(H')} = \underset{w}{\cap} \mathrm{rep}(F_w),$$

where G_r are triangular sets in $k[X]$ and F_w are triangular sets in $k[Y]$. $\{G_r\}$ and $\{F_w\}$ in the triangular representations of H and H' computed by Szántó's algorithm are unmixed triangular sets (see [15, Proposition 6]) which guarantee zero $(\cup_w F_w) = H'$ and zero $(\cup_r G_r) = H$. A subroutine called **unmixed** can transform a triangular set to an unmixed one (see [16, Section 4.2] for more details). Since zero $(\cup_w F_w) = H'$, composing every polynomial in each F_w with τ and clearing the denominators, we can get the sets E_w of polynomials in $k[X]$ such that zero $(\cup_w E_w) = \tau^{-1}(H')$. Since zero $(\cup_r G_r) = H$, zero $((\cup_r G_r) \cup (\cup_w E_w)) = \tau^{-1}(H' \cap \tau(H))$. Let J be the ideal generated by $((\cup_r G_r) \cup (\cup_w E_w))$. Thus, zero $(J) = \tau^{-1}(H' \cap \tau(H))$. Since the degrees of polynomials in G_r are not greater than d and the degrees of polynomials in E_w are not greater than md', by Theorem 2.2, J has a triangular representation bounded by $n(\max(d, md'))^{5.5n^3}$. That is, $\tau^{-1}(H' \cap \tau(H))$ has a triangular representation bounded by $n(\max(d, md'))^{5.5n^3}$. ☐

In [4, Proposition B.6], Feng uniformly bounded the homomorphisms defined in the following lemma by considering the bound for the generating set of the ideal generated by the defining equations of an algebraic subgroup. Instead, we present a bound for such homomorphisms by making use of the bound for the triangular representation of an algebraic subgroup. The proof is similar to the one in [4, Proposition B.6].

Lemma 3.4. *Assume that $n > 1$. Let H and H' be algebraic subgroups of $GL_n(k)$ such that $H \triangleleft EH'$. Assume that H has a triangular representation bounded by d. Then there exists a homomorphism*

$$\tau_{H',H} : H' \rightarrow GL_{d^*}(k)$$

bounded by n^* with $\ker(\tau_{H',H}) = H, d^* = \max_i \left\{ \left(\begin{pmatrix} n^2 + d \\ d \\ i \end{pmatrix} \right)^2 \right\}$ and $n^* = d^* d \begin{pmatrix} n^2 + d \\ d \end{pmatrix}$.

Proof. The existence of such a homomorphism is guaranteed by [6, Theorem, page 82]. Let $G(H)$ be the family of triangular sets in a triangular representation of H. Then $G(H)$ is a k-vector space with a finite dimension. Let $k[x_{i,j}]_{\leq d}$ be the set of polynomials of degrees not greater than d where $1 \leq i, j \leq n$. Let $I(H) = \{P(x_{i,j}) \in k[x_{i,j}]_{\leq d} | P(H) = 0\}$ and $l = \dim_k(I(H))$. Let

$$E = \bigwedge^l k[x_{i,j}]_{\leq d}, 1 \leq i, j \leq n$$

which is the lth exterior power of $k[x_{i,j}]_{\leq d}$. Since $k[x_{i,j}]_{\leq d}$ is a k-vector space with dimension $\begin{pmatrix} n^2 + d \\ d \end{pmatrix}$, $\dim_k(E) = \left(\begin{pmatrix} n^2 + d \\ d \\ l \end{pmatrix} \right)$ and $\bigwedge^l C(H) = kv$ for some $v \in E$ where $\bigwedge^l C(H)$ is the lth exterior power of $C(H)$. By a similar argument in the proof of [4, Lemma B.6], we can construct a desired homomorphism bounded by n^*. □

Let U be a subgroup generated by unipotent elements of $GL_n(k)$. In [4, Lemma B.8], Feng gave a degree bound for U which is double-exponential in n. In the following lemma, we bound the triangular representation of U. The bound we give is polynomial exponential in n.

Lemma 3.5. *Assume that $n > 1$. Let U be a subgroup generated by unipotent elements of $GL_n(k)$. Then U has a triangular representation bounded by*

$$3n^2 \left(2n^2(n-1) \right)^{148.5n^6}.$$

Proof. By [6, Lemma C, page 96], any one-dimensional subgroup H generated by unipotent elements of $GL_n(k)$ has the form

$$H = \left\{ I_n + Mx + \frac{M^2}{2!} x^2 + \dots + \frac{M^{n-1}}{(n-1)!} x^{n-1} : x \in \mathbb{C} \right\}$$

where $M \in \text{Mat}_n(k)$ with $M^n = 0$. By [6, Proposition, page 55], U is a product of at most $2\dim(U)$ one-dimensional subgroups generated by unipotent elements. Hence,

$$U = \prod_{i=1}^{2\dim(U)} H_i$$

where $H_i = \{ I_n + M_i x_i + \frac{M_i^2}{2!} x_i^2 + \dots + \frac{M_i^{n-1}}{(n-1)!} x_i^{n-1} : x_i \in \mathbb{C} \}$ is a one-dimensional subgroup generated by unipotent elements of $GL_n(k)$ and $M_i \in \text{Mat}_n(k)$ with $M_i^n = 0$. Since $\dim(U) \leq n^2$, the defining equations of U contain at most $3n^2$ variables and have degrees not greater than $2n^2(n-1)$. By Lemma 3.1, the ideal generated by the defining equations of U has a triangular representation bounded by

$$3n^2 \left(2n^2(n-1) \right)^{5.5(3n^2)^3} = 3n^2 \left(2n^2(n-1) \right)^{148.5n^6}.$$

□

Jordan in [7] proved that there exists a positive integer $J(n)$ depending on n such that every finite subgroup of $GL_n(k)$ contains a normal abelian subgroup of index at most $J(n)$. Schur in [12] provided an explicit bound which is

$$J(n) \leq \left(\sqrt{8n}+1\right)^{2n^2} - \left(\sqrt{8n}-1\right)^{2n^2}.$$

We use Schur's bound in our computations. Assume that $n > 1$. Let

$$D = 3n^2 \left(2n^2(n-1)\right)^{148.5n^6}, \tag{3}$$

$$d_1 = \max_i \left\{ \left(\binom{n^2+D}{D} \right)^2 \right\}, \tag{4}$$

$$d_2 = d_1 D \binom{n^2+D}{D}, \tag{5}$$

$$d_3 = n \left(d_2 \left(d_1^2+1\right) \max_i \left\{ \binom{d_1^2+1}{i}^2 \right\} \right)^{5.5n^3}, \tag{6}$$

and

$$\bar{d} = J \left(\max_i \left\{ \binom{d_1^2+1}{i}^2 \right\} \right). \tag{7}$$

Next we give numerical bounds for D, d_1, d_2, d_3 and $\bar{d}$ which will be used in the following theorems. Since

$$D = 3n^2 \left(2n^2(n-1)\right)^{148.5n^6} \leq 3n^2 \left(2n^3\right)^{148.5n^6}$$

and

$$\binom{n^2+D}{n^2} \leq \left(\frac{e(n^2+D)}{n^2} \right)^{n^2} \leq \left(e + 3e(2n^3)^{148.5n^6} \right)^{n^2} \leq 18^{n^2} (2n^3)^{148.5n^8},$$

$$d_1 \leq \left(2^{\binom{n^2+D}{D}} \right)^2 \leq \left(2^{18^{n^2}(2n^3)^{148.5n^8}} \right)^2 \leq \left(2^{(2n^3)^{149n^8}} \right)^2 \leq 4^{(2n^3)^{149n^8}},$$

$$d_2 \leq 4^{(2n^3)^{149n^8}} 3n^2 (2n^3)^{148.5n^6} 18^{n^2} (2n^3)^{148.5n^8} = 3n^2 18^{n^2} 4^{(2n^3)^{149n^8}} (2n^3)^{\left(148.5n^8+148.5n^6\right)},$$

$$
\begin{aligned}
d_3 &\leq n \left(3n^2 18^{n^2} (2n^3)^{148.5n^8+148.5n^6} 4^{(2n^3)^{149n^8}} \left(16^{(2n^3)^{149n^8}} + 1 \right) 4^{\left(16^{(2n^3)^{149n^8}}+1 \right)} \right)^{5.5n^3} \\
&\leq n \left((2n^3)^{149n^8+149n^6} 4^{(2n^3)^{149n^8}} \left(16^{(2n^3)^{149n^8}} + 1 \right) 4^{\left(16^{(2n^3)^{149n^8}}+1 \right)} \right)^{5.5n^3} \\
&\leq n \left(2(2n^3)^{149n^8+149n^6} 4^{(2n^3)^{149n^8}} 16^{(2n^3)^{149n^8}} 4^{\left(16^{(2n^3)^{149n^8}}+1 \right)} \right)^{5.5n^3} \\
&\leq n \left(8(2n^3)^{149n^8+149n^6} 4^{(2n^3)^{149n^8}} 16^{(2n^3)^{149n^8}} 4^{16^{(2n^3)^{149n^8}}} \right)^{5.5n^3} \\
&\leq n \left(8^{16^{(2n^3)^{149n^8}}} \right)^{5.5n^3} = n 8^{5.5n^3 16^{(2n^3)^{149n^8}}},
\end{aligned}
$$

and

$$\bar{d} \leq \left(\sqrt{8 \cdot 4^{d_1^2+1}} + 1\right)^{2n^2} - \left(\sqrt{8 \cdot 4^{d_1^2+1}} - 1\right)^{2n^2}$$

$$\leq \left(\sqrt{32} \cdot 2^{8^{(2n^3)^{149n^8}}} + 1\right)^{2n^2} - \left(\sqrt{32} \cdot 2^{8^{(2n^3)^{149n^8}}} - 1\right)^{2n^2}$$

$$\leq \left(2\sqrt{32} \cdot 2^{8^{(2n^3)^{149n^8}}}\right)^{2n^2} = 2^{10n^2} 4^{n^2 8^{(2n^3)^{149n^8}}}$$

where $n > 1$.

3.2. Complexity of Hrushovski's algorithm

In this section, when we say that a family $\mathcal{F}$ of algebraic subgroups of $GL_n(k)$ is bounded by an integer we mean that the triangular representations of all elements in $\mathcal{F}$ are bounded by that integer. We prove the following theorem and corollaries following the way in which Feng proved [4, Proposition B.11, Lemma B.12, Lemma B.13]. But in order to improve the bounds, we replace the use of Gröbner bases with the triangular representations. Our main result is stated as the following theorem.

Theorem 3.1. *Assume that $n > 1$. There is an integer*

$$\bar{d} \leq 2^{10n^2} 4^{n^2 8^{(2n^3)^{149n^8}}}$$

and a family $\mathcal{F}$ of algebraic subgroups of $GL_n(k)$ whose triangular representations are bounded by

$$d_3 \leq n 8^{5.5n^3 16^{(2n^3)^{149n^8}}}$$

with the following properties: for every algebraic subgroup $H' \subseteq GL_n(k)$, there exists an algebraic subgroup H of $\mathcal{F}$ such that

a. $(H')^\circ \subseteq H$
b. $H \trianglelefteq H'H \subseteq GL_n(k)$
c. $[H' : H \cap H'] = [H'H : H] \leq \bar{d}$
d. *Every unipotent element of H is in $(H')^\circ$*

where $(H')^\circ$ is the identity component of H'.

Proof. In the first case we assume that H' is a finite subgroup in $GL_n(k)$. Since every finite subgroup of $GL_n(k)$ contains a normal abelian subgroup of index at most $J(n)$, we choose such a normal abelian subgroup $\tilde{H}' \subseteq H'$. $\tilde{H}'$ is diagonalizable, so $\tilde{H}'$ is in some maximal torus of $GL_n(k)$. Let H be the intersection of maximal tori containing $\tilde{H}'$ in $GL_n(k)$. We prove that H satisfies $(a)-(d)$ for H'. (a) is true because of the construction of H. (b) is true because H normalizes H'. (c) is true because

$$[H'H : H] = [H' : H \cap H'] \leq [H' : \tilde{H}'] \leq J(n).$$

So we can choose $\bar{d} = J(n)$. (d) is true because there is only one unipotent element of H which is the identity. Let $\mathcal{F}$ be the family of all the intersections of maximal tori in $GL_n(k)$. Then $\mathcal{F}$ is the desired family of algebraic subgroups of $GL_n(k)$ with $d_3 = 1$.

In the second case we assume that H' is a subgroup whose identity component is a torus. Let T be the intersection of all maximal tori containing $(H')^\circ$ in $GL_n(k)$. Then T has a triangular representation bounded by 1. Let S be the normalizer of T in $GL_n(k)$. By Lemma 3.4, there is a homomorphism

$$\tau_{S,T} : S \to GL_{n'}(k)$$

bounded by

$$(n^2 + 1)\max_i\left\{\binom{n^2 + 1}{i}^2\right\}$$

such that $\ker(\tau_{S,T}) = T$ and $n' = \max_i\left\{\binom{n^2 + 1}{i}^2\right\}$. Since the identity component of H' is con-

tained in T, $\tau_{S,T}(H')$ is a finite subgroup of $GL_{n'}(k)$. Let $\mathcal{F}_1$ be the family of all the intersections of maximal tori of $GL_{n'}(k)$. By the first case, there exists $H_{\mathcal{F}_1} \in \mathcal{F}_1$ such that $(a)-(c)$ are true for $\tau_{S,T}(H')$ with $\bar{d} = J(n')$. Let

$$H = \tau_{S,T}^{-1}\big(\tau_{S,T}(S) \cap H_{\mathcal{F}_1}\big).$$

We prove that $(a)-(d)$ are true for H and H'. Since the identity component $(H')^\circ$ of H' is a torus and $T \subseteq H$, $(H')^\circ \subseteq H$. This proves (a). Let $h' \in H'$. Then

$$\tau_{S,T}\big(h'Hh'^{-1}\big) = \tau_{S,T}(h')\big(\tau_{S,T}(S) \cap H_{\mathcal{F}_1}\big)\tau_{S,T}(h'^{-1}).$$

Since $H_{\mathcal{F}_1} \trianglelefteq \tau_{S,T}(H')H_{\mathcal{F}_1}$,

$$\tau_{S,T}(h')\big(\tau_{S,T}(S) \cap H_{\mathcal{F}_1}\big)\tau_{S,T}(h'^{-1}) = \tau_{S,T}(S) \cap H_{\mathcal{F}_1} = \tau_{S,T}(H).$$

So $h'Hh'^{-1} \subseteq H$ and $H \trianglelefteq H'$. Hence, $H \trianglelefteq H'H \subseteq GL_n(k)$. This proves (b). Since $H' \subseteq S$ and $[\tau_{S,T}(H') : H_{\mathcal{F}_1} \cap \tau_{S,T}(H')] \leq J(n')$,

$$[H' : H \cap H'] = [H'H : H] = \big[\tau_{S,T}(H'H) : \tau_{S,T}(H)\big] = \big[\tau_{S,T}(H')\tau_{S,T}(H) : \tau_{S,T}(H)\big]$$

$$= \big[\tau_{S,T}(H') : \tau_{S,T}(H) \cap \tau_{S,T}(H')\big] = \big[\tau_{S,T}(H') : H_{\mathcal{F}_1} \cap \tau_{S,T}(H')\big] \leq J(n').$$

We can choose $\bar{d} = J(n') = J\left(\max_i\left\{\binom{n^2 + 1}{i}^2\right\}\right)$. This proves (c). Let $h \in H$ be a uni-

potent element. Then $\tau_{S,T}(h)$ is a unipotent element in $H_{\mathcal{F}_1}$. Since every element in $H_{\mathcal{F}_1}$ is semi-simple, $\tau_{S,T}(h) = 1$. So h must be in $\ker(\tau_{S,T}) = T$. By the definition of T, T is in some torus of $GL_n(k)$. So $h = 1$. Hence, every unipotent element of H is in $(H')^\circ$. This proves (d). By Lemma 3.3, H has a triangular representation bounded by

$$n(n^2 + 1)^{5.5n^3}\max_i\left\{\binom{n^2 + 1}{i}^{11n^3}\right\}.$$

Let $\mathcal{F}$ be the family of such subgroups H. Then $\mathcal{F}$ is the desired family with

$$d_3 \leq n(n^2 + 1)^{5.5n^3}\max_i\left\{\binom{n^2 + 1}{i}^{11n^3}\right\}.$$

The general case is proved as follows. Let H'_u be the intersection of kernels of all characters of $(H')^\circ$. $(H')^\circ$ is a connected subgroup of $GL_n(k)$, so H'_u is generated by all unipotent elements by [4, Lemma B.10]. By Lemma 3.5, H'_u has a triangular representation bounded by D. Let N be the normalizer of H'_u in $GL_n(k)$. By Lemma 3.4, there exists a homomorphism

$$\tau_{N,H'_u} : N \to GL_{d_1}(k)$$

bounded by

$$d_2 = d_1 D \binom{n^2 + D}{D}$$

such that $\ker(\tau_{N,H'_u}) = H'_u$ and

$$d_1 = \max_i \left\{ \left(\binom{n^2 + D}{D} \right)^2 \atop i \right\}.$$

The identity component of $\tau_{N,H'_u}(H')$ is a torus in $GL_{d_1}(k)$, by the second case, there exists $H'' \subseteq GL_{d_1}(k)$ whose triangular representation bounded by

$$(d_1^2 + 1) \max_i \left\{ \binom{d_1^2 + 1}{i}^2 \right\}$$

such that $(a)-(d)$ are true for $\tau_{N,H'_u}(H')$ with

$$\bar{d} = J\left(\max_i \left\{ \binom{d_1^2 + 1}{i}^2 \right\} \right) \leq 2^{10n^2} 4^{n^2 8^{(2n^3)^{149n^8}}}.$$

Let

$$H = \tau_{N,H'_u}^{-1}\left(H'' \cap \tau_{N,H'_u}(N) \right).$$

By Lemma 3.3, H has a triangular representation bounded by

$$d_3 = n\left(d_2(d_1^2 + 1) \max_i \left\{ \binom{d_1^2 + 1}{i}^2 \right\} \right)^{5.5n^3} \leq n8^{5.5n^3 16^{(2n^3)^{149n^8}}}.$$

By a similar argument in the proof of [4, Proposition B.11], $(a)-(d)$ are true for H and H'. Let $\mathcal{F}$ be the family of such algebraic subgroups H. Then $\mathcal{F}$ is the desired family with

$$d_3 \leq n8^{5.5n^3 16^{(2n^3)^{149n^8}}}.$$

$\square$

Corollary 3.1. Assume that $n > 1$. There exists a family $\bar{\mathcal{F}}$ of algebraic subgroups of $GL_n(k)$ whose triangular representations are bounded by

$$d_3 \leq n8^{5.5n^3 16^{(2n^3)^{149n^8}}}$$

such that for any algebraic subgroup $H' \subseteq GL_n(k)$ there exists $\bar{H}$ of $\bar{\mathcal{F}}$ such that $H' \subseteq \bar{H}$ and every unipotent element of $\bar{H}$ is in $(H')^\circ$.

Proof. Let $\bar{\mathcal{F}} = \{\bar{H} : there exists H \in \mathcal{F} such that H \trianglelefteq \bar{H} and [\bar{H} : H] \leq \bar{d}\}$. Let $H' \subseteq GL_n(k)$ be an algebraic subgroup. By Theorem 3.1, there is an $H \in \mathcal{F}$ such that $(a)-(d)$ are true for H and H'. Let $\bar{H} = H'H$. By (b) and (c) in Theorem 3.1, $\bar{H} \in \bar{\mathcal{F}}$. By (d) in Theorem 3.1, every unipotent element of H is in $(H')^\circ$. Since every unipotent element of $\bar{H}$ is in $\bar{H}^\circ \subseteq H^\circ$. Hence, every unipotent element of $\bar{H}$ is in $(H')^\circ$. Since $\bar{H}$ is the union of the cosets of some element in $\mathcal{F}$ and every element of $\mathcal{F}$ has a triangular representation bounded by d_3, by Lemma 3.2, we have that $\bar{H}$ has a triangular representation bounded by

$$d_3 \leq n8^{5.5n^3 16^{(2n^3)^{149n^8}}}.$$

Therefore, $\bar{\mathcal{F}}$ is bounded by $d_3 \leq n8^{5.5n^3 16^{(2n^3)^{149n^8}}}$.

$\square$

Corollary 3.2. *Let $\bar{\mathcal{F}}$ be the family in Corollary 3.1. Then for any algebraic subgroup $H' \subseteq GL_n(k)$, there exists $\bar{H}$ of $\bar{\mathcal{F}}$ such that*

$$\left(\bar{H}^\circ\right)^t \trianglelefteq (H')^\circ \subseteq H' \subseteq \bar{H}.$$

Proof. By Corollary 3.1, there exists $\bar{H}$ of $\bar{\mathcal{F}}$ such that $H' \subseteq \bar{H}$ and every unipotent element of $\bar{H}$ is in $(H')^\circ$. Since $\bar{H}^\circ$ is a connected subgroup of $GL_n(k)$, $\left(\bar{H}^\circ\right)^t$ is generated by all unipotent elements in $\bar{H}^\circ$ by [4, Lemma B.10]. Since $\left(\bar{H}^\circ\right)^t \trianglelefteq \bar{H}^\circ$ and every unipotent element in $\bar{H}^\circ$ is in $(H')^\circ$, $\left(\bar{H}^\circ\right)^t \trianglelefteq (H')^\circ$. Therefore, $\left(\bar{H}^\circ\right)^t \trianglelefteq (H')^\circ \subseteq H' \subseteq \bar{H}$. ☐

Remark. Since the differential Galois group of (1) is an algebraic subgroup in $GL_n(k)$, by Corollary 3.2, there exists an algebraic subgroup $\bar{H}$ bounded by d_3 such that $\left(\bar{H}^\circ\right)^t \trianglelefteq (H')^\circ \subseteq H' \subseteq \bar{H}$. By the definition of the proto-Galois group, this algebraic subgroup $\bar{H}$ is a proto-Galois group of (1).

4. Comparison

We compute $\bar{d}$ and d_3 explicitly for $n = 2$. We plug in $n = 2$ to the equations (3), (4), (5), (6), and (7) instead of the formulas in Theorem 3.1 and Corollary 3.1 to do calculations, which would give us more refined bounds. Feng in [4] roughly estimated that $\bar{d}$ is quintuply exponential in n and d_3 is sextuply exponential in n, but he did not give numerical bounds for them. In order to compare our bounds with the ones in [4], we also give numerical bounds in [4, Proposition 11, Proposition 14]. In [4, Proposition 11, Proposition 14], d_3 is denoted as $\tilde{d}$ and $\bar{d}$ is denoted as $I(n)$, respectively. The numerical bounds of $\tilde{d}$ and $I(n)$ are as follows:

$$\tilde{d} \leq 32^{2^{2^{2^{(2n)^2}(24n^2)}}} \quad, \quad I(n) \leq 4^{2^{2^{(2n)^2}(12n^2)}}.$$

When $n = 2$,

$$\bar{d} \leq 2^{2^{2^{2^{18}}}}, I(n) \leq 2^{2^{2^{2^{2^{96}}}}},$$

and

$$d_3 \leq 2^{2^{2^{2^{18}}}}, \tilde{d} \leq 2^{2^{2^{2^{2^{2^{194}}}}}}.$$

Acknowledgment

Funding

References

[1] Amzallag, E., Pogudin, G., Sun, M., Vo, N. T. (2018). Complexity of triangular representations of algebraic sets. *Preprint.* https://arxiv.org/abs/1609.09824.

[2] Compoint, E., Singer, M. F. (1999). Computing Galois groups of completely reducible differential equations. *J. Symb. Comput.* 28(4–5): 473–494. DOI: 10.1006/jsco.1999.0311.

[3] Crespo, T., Hajto, Z., Ruiz, J. J. M. (2007). *Introduction to Differential Galois Theory*. Cracow: Wydawnictwo PK.

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

[5] Hrushovski, E. (2002). Computing the Galois group of a linear differential equation. *Banach Cent. Publ.* 58(1):97–138. DOI: 10.4064/bc58-0-9.

[6] Humphreys, J. E. (1975). *Linear Algebraic Groups*. New York: Springer-Verlag. DOI: 10.1007/978-1-4684-9443-3.

[7] Jordan, C. (1877). Mémoire sur les équations différentielles linéaires à intégrale algèbriques. *J. Rein. Ang. Math.* 84:89–215. DOI: 10.1515/crll.1878.84.89.

[8] Kolchin, E. R. (1948). Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Ann. Math.* 49(1): 1–42. DOI: 10.2307/1969111.

[9] Kolchin, E. R. (1968). Algebraic groups and algebraic dependence. *Am. J. Math.* 90(4):1151–1164. DOI: 10.2307/2373294.

[10] Kovacic, J. J. (1986). An algorithm for solving second order linear homogeneous differential equations. *J. Sym. Comput.* 2(1):3–43. DOI: 10.1016/S0747-7171(86)80010-4.

[11] Magid, A. R. (1994). *Lectures on Differential Galois Theory*. American Mathematical Society. Providence, Rhode Island. https://doi.org/10.1090/ulect/007.

[12] Schur, I. (1911). Über gruppen periodischer substitutionen. *Sitzber. Preuss. Akad. Wiss.* 619–627.

[13] Singer, M. F. (2007). Introduction to the Galois theory of linear differential equations. *Preprint.* https://arxiv.org/abs/0712.4124.

[14] Singer, M. F., Ulmer, F. (1993). Galois groups of second and third order linear differential equations. *J. Symb. Comput.* 16(1): 9–36. DOI: 10.1006/jsco.1993.1032.

[15] Szántó, Á. (1997). Complexity of the Wu-Ritt decomposition. *Proceedings of the Second International Symposium on Parallel Symbolic Computation*, pp. 139–149. DOI: 10.1145/266670.266716.

[16] Szántó, Á. (1999). *Computation with polynomial systems*. PhD thesis, Cornell University.

[17] van der Hoeven, J. (2007). Around the numeric–symbolic computation of differential Galois groups. *J. Symb. Comput.* 42(1–2):236–264. DOI: 10.1016/j.jsc.2006.03.007.

[18] van der Put, M. (2005). Galois theory and algorithms for linear differential equations. *J. Symb. Comput.* 39(3-4):451–463. DOI: 10.1016/j.jsc.2004.11.013.

[19] van der Put, M., Singer, M. F. (2003). *Galois Theory of Linear Differential Equations*. Berlin: Springer-Verlag. DOI: 10.1007/978-3-642-55750-7.