5-2019

On the Complexity of Computing Galois Groups of Differential Equations

Mengxiao Sun
The Graduate Center, City University of New York

On the Complexity of Computing Galois Groups of Differential Equations

by

Mengxiao Sun

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2019

The manuscript has been read and accepted for the
Graduate Faculty in Mathematics in satisfaction of the
Dissertation requirements for the degree of Doctor of Philosophy.

	Professor Alexey Ovchinnikov
Date	Chair of Examining Committee
	Professor Ara Basmajian
Date	Executive Officer

Professor Richard Churchill

Professor Alexey Ovchinnikov

Professor Vladimir Shpilrain

Supervisory Committee

The City University of New York

Abstract

On the Complexity of Computing Galois Groups of Differential Equations

by

Mengxiao Sun

Advisor: Professor Alexey Ovchinnikov

The differential Galois group is an analogue 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. 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 first proposed an algorithm for computing the differential Galois group of a general linear differential equation. Recently, Feng approached finding a complexity bound of the algorithm, which is the degree bound of the polynomials used in the first step of the algorithm for finding a proto-Galois group. The bound given by Feng is quintuply exponential in the order n of the differential equation. The complexity, in the worst case, of computing a Gröbner basis is doubly exponential in the number of variables. Feng chose to represent the radical of the ideal generated by the defining equations of a proto-Galois group by its Gröbner basis. Hence, a double-exponential degree bound for computing Gröbner bases was involved when Feng derived the complexity bound of computing a proto-Galois group.

Triangular decomposition provides an alternative method for representing the radical of an ideal. It represents the radical of an ideal by the triangular sets instead of its generators. The first step of Hrushovski's algorithm is to find a proto-Galois group which can be used

further to find the differential Galois group. So it is important to analyze the complexity for finding a proto-Galois group. We represent the radical of the ideal generated by the defining equations of a proto-Galois group using the triangular sets instead of the generating sets. We apply Szántó's modified Wu-Ritt type decomposition algorithm and make use of the numerical bound for Szántó's algorithm to adapt to the complexity analysis of Hrushovski's algorithm. We present a triple exponential degree upper bound for finding a proto-Galois group in the first step of Hrushovski's algorithm.

Acknowledgments

Firstly, I would like to extend my sincere thanks to my advisor Dr. Alexey Ovchinnikov for the continuous support of my Ph.D study and related research, for his patience, motivation, and immense knowledge.

I am indebted to my parents for providing me with continuous support and encouragement throughout my years of study. This accomplishment would not have been possible without them.

A special thanks to my sister, Mengyao, for supporting me spiritually throughout completing my degree and my life in general. Thank you for listening to my complaints and frustrations. I would like to express my deep gratitude for being the best friend always cheering me up.

Finally, but perhaps most importantly, I would like to thank my grandmother. I was truly sorry that I wasn't able to leave New York when I heard about her passing. I know she would be proud and I will forever be grateful for the knowledge and values she instilled in me.

The work in this thesis has been partially supported by NSF grants CCF-0952591, CCF-1563942, CCF-1708884, DMS-1606334, DMS-1760448, by the NSA grants #H98230-15-1-0245, #H98230-18-1-0016, by CUNY CIRG #2248, and by PSC-CUNY grants #69827-00 47 and #60098-00 48.

The material in Chapter 2 of this thesis is a collaborative work with Eli Amzallag, Gleb

Pogudin, and Thieu N. Vo which was presented in the following :

- E. Amzallag. Galois groups of differential equations and representing algebraic sets. Ph.D. thesis, The Graduate Center, City University of New York, 2018.
- E. Amzallag, M. Sun, G. Pogudin, and T. N. Vo. Complexity of triangular representations of algebraic sets. *Journal of Algebra*, 523 (2019): 342-364.

In memory of my grandmother, Bozhu Gao

Contents

Chapter 1

Introduction

The differential Galois group is an analogue 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 [19, 35]. For example [20, Appendix], the differential Galois group of Bessel's equation $t^2y'' + ty' + (t^2 - \nu^2)y = 0$ 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 [14] 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 [10], which is the degree bound of the polynomials used in the first step of the algorithm for finding a proto-Galois group, 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 [29, 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 [10, 14]). 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 4.4.1. 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 4.4.1.

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 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 [31, 33] which has been proved to be more efficient than computing a Gröbner basis and make use of the numerical bound for Szántó's algorithm [2] 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.

Besides Hrushovski's general algorithm, there are other algorithmic results in the Galois theory of linear differential equations. Kovacic in [21] 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 [30]. Compoint and Singer in [6] 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 [34].

This thesis is organized as follows. In chapter 2, we introduce the notations, definitions and facts from triangular representation. In chapter 3, we introduce the notations, definitions and facts from differential Galois group. In chapter 4, we state and prove the preparation lemmas which we use in analyzing the complexity of the algorithm, and present and prove

the new complexity bound of Hrushovskis algorithm. We also compare our bounds when $n = 2$ with the ones in [10, Proposition B.11, Proposition B.14].

The work in Chapter 2 is a collaborative work with Eli Amzallag, Gleb Pogudin and Thieu N. Vo. The material of this chapter appeared in the following:

- E. Amzallag. Galois groups of differential equations and representing algebraic sets. Ph.D. thesis, The Graduate Center, City University of New York, 2018.
- E. Amzallag, M. Sun, G. Pogudin, and T. N. Vo. Complexity of triangular representations of algebraic sets. *Journal of Algebra*, 523 (2019): 342-364.

This thesis is divided to two parts. The first part (Chapter 2) is on the triangular representations of algebraic sets and the second part (Chapters 3 and 4) is on the complexity of Hrushovski's algorithm for computing Galois groups of linear differential equations. We improve Feng's complexity bound of Hrushovski's algorithm using the numerical complexity bound of Szántó's algorithm for representing algebraic sets by triangular sets. The numerical complexity bound of Szántó's algorithm is the main result of the first part which is essential and helpful to present as a single chapter in this thesis.

Chapter 2

Triangular Representation

2.1 Introduction

Given polynomials $f_0, \ldots, f_r \in k[x_1, \ldots, x_n]$, where k is a computable subfield of $\mathbb{C}$, the set of all polynomials vanishing on the set of solutions of the system $f_0 = \ldots = f_r = 0$ is called *the radical* of the ideal generated by $f_0, \ldots, f_r$. Representing the radical of an ideal is important for computer algebra and symbolic computations, as well as for their applications (for example, [3, 26]).

Several techniques can be used to solve the problem: for example, Gröbner bases, geometric resolution, and triangular decomposition. Representing the radical of an ideal is an intermediate step in many other algorithms. Thus, it is crucial to understand the size of such a representation, as the size affects the complexity of the further steps. The size of the representation can be expressed in terms of a degree bound for the polynomials appearing in the representation and their number. In section 2.4, We present the first complete bound on the degrees (Theorem 2.4.2) and the number of components (Theorem 2.5.1) for the algorithm designed by A. Szántó in [33] for computing a triangular decomposition.

For Gröbner bases, a bound which is doubly-exponential in the number of variables is

given in [22]. Moreover, an example constructed in [4] shows that there are ideals such that every set of generators of the radical (even those sets that are not Gröbner bases) contains a polynomial of doubly-exponential degree. Geometric resolution and triangular decomposition do not represent the radical via its generators, so it was hoped that these representations might have better degree bounds. For geometric resolution, singly-exponential degree bounds were obtained in [12, 23, 24] (for prior results in this direction, see references in [24]).

Algorithms for triangular decomposition were an active area of research during the last two decades. Some results of this research were tight degree upper bounds for a triangular decomposition of an algebraic variety given that the decomposition is irredundant [9, 27], an efficient algorithm for zero-dimensional varieties [8], and implementations [1, 36].

However, to the best of our knowledge, there are only a few algorithms [11, 27, 33] for computing triangular decomposition with proven degree upper bounds for the output. The algorithms in [27] and [11] have restrictions on the input polynomial system. The algorithm in [27] requires the system to define an irreducible variety. The algorithm in [11, Theorem 4.14] produces a characteristic set of an ideal, which represents the radical of the ideal only if the ideal is characterizable [15, Definition 5.10] (for example, an ideal defined by x_1x_2 is not characterizable). Together with [15, Proposition 5.17] this means that the algorithm from [11] represents the radical of an ideal if the radical can be defined by a single regular chain.

The algorithm designed by [32, 33] does not have any restrictions on the input system. However, it turns out that the argument in [33] does not imply the degree bound $d^{O(m^2)}$ (m is the maximum codimension of the components of the ideal, d is a bound for degrees of the input polynomials) stated there. The reason is that the argument in [33] did not take into account possible redundancy of the output (see Remark 6). Moreover, in Example 2.3.1 we show that the sum of degrees of extra components produced by the algorithm can be significantly larger than the degree of the original variety.

We take these extra components into account and prove an explicit degree bound of the form $d^{\mathrm{O}(m^3)}$ for the algorithm. More precisely, we prove that:

Theorem 2.1.1. *Let $f_0, \ldots, f_r \in k[x_1, \ldots, x_n]$ be polynomials with $\deg f_i \leq d$ for all $0 \leq i \leq r$ ($d > 1$). Assume that the maximum codimension of prime components of the ideal $(f_0, \ldots, f_r)$ is $m \geq 2$, and $r \leq d^m$. Then the degree of any polynomial p appearing in the output of Szántó's algorithm or during the computation does not exceed*

$$\deg(p) \leq n d^{(\frac{1}{2}+\epsilon)m^3}$$

where ϵ is some decreasing function of m, d and ϵ is bounded by 5.

Theorem 2.1.2. *Let $F \subset k[x_1, \ldots, x_n]$ be a finite set of polynomials of degree at most d. Let m be the maximum of codimension of prime components of $\sqrt{(F)} \subseteq k[x_1, \ldots, x_n]$. Then the number of squarefree regular chains in the output of Szántó's algorithm applied to F is at most*

$$\binom{n}{m} \left((m+1)d^m + 1\right)^m.$$

2.2 Preliminaries

Throughout chapter 2, all fields are of characteristic zero and all logarithms are binary.

Throughout this section, let $R = k[x_1, x_2, \ldots, x_n]$, where k is a field. We fix an ordering on the variables $x_1 < x_2 < \cdots < x_n$. Consider a polynomial $p \in R$. We set $\mathrm{height}(p) := \max_i \deg_{x_i}(p)$. The highest indeterminate appearing in p is called its leader and will be defined by $\mathrm{lead}(p)$. By $\mathrm{lc}(p)$ we denote the leading coefficient of p when p is written as a univariate polynomial in $\mathrm{lead}(p)$.

Definition 2.2.1. *Given a sequence $\Delta = (g_1, g_2, \ldots, g_m)$ in R, we say that Δ is a* triangular set *if $\mathrm{lead}(g_i) < \mathrm{lead}(g_j)$ for all $i < j$.*

Remark 1. *Note that any subsequence of a triangular set is a triangular set. In what follows, the subsequences of* Δ *of particular interest are the ones of the form* $\Delta_j := (g_1, g_2, \ldots, g_j)$, $1 \leq j \leq m$ *and* $\Delta_0 := \varnothing$.

Triangular sets give rise to ideals via the following notion.

Definition 2.2.2. *Let* $f, g \in R$ *with* $\operatorname{lead}(g) = x_j$. *We consider* f *and* g *as univariate polynomials in* x_j *with the coefficients from the field* $k(x_1, x_2, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$ *and let* $f = \tilde{q}g + \tilde{r}$ *be the result of univariate polynomial division of* f *by* g *with coefficients in this field. Let* α *be the smallest nonnegative integer such that* $g := \operatorname{lc}(g)^\alpha \tilde{g}$ *and* $r := \operatorname{lc}(g)^\alpha \tilde{r}$ *are polynomials, so we obtain an equation*

$$\operatorname{lc}(g)^\alpha f = qg + r$$

with $q, r \in R, \deg_{x_j}(r) < \deg_{x_j}(g), \alpha \in \mathbb{N}$. *One can show that* $\alpha \leq \deg_{x_j}(f) - \deg_{x_j}(g) + 1$. *We say that* r *is* pseudoremainder of f by g *and denote it by* $\operatorname{prem}(f, g)$.

Definition 2.2.3. *Let* $\Delta = (g_1, g_2, \ldots, g_m)$ *be a triangular set and let* $f \in R$. *The* pseudoremainder of f with respect to Δ *is the polynomial* f_0 *in the sequence* $f_m = f, f_{s-1} = \operatorname{prem}(f_s, g_s), 1 \leq s \leq m$. *We denote* f_0 *by* $\operatorname{prem}(f, \Delta)$.

We say that f *is* reduced with respect to Δ *if* $f = \operatorname{prem}(f, \Delta)$.

Remark 2. *The computation of the pseudoremainder of* f *with respect to* Δ *gives rise to the equation*

$$\operatorname{lc}(g_m)^{\alpha_m} \ldots \operatorname{lc}(g_1)^{\alpha_1} f = \sum_{s=1}^{m} q_s g_s + f_0$$

where each $\alpha_s \leq \deg_{\operatorname{lead}(g_s)}(f_s) - \deg_{\operatorname{lead}(g_s)}(g_s) + 1$.

Definition 2.2.4. *Given a triangular set Δ in R, we define the ideal*

$$\mathrm{Rep}(\Delta) := \{p \in R \,|\, \exists N \,:\, H^N p \in \langle \Delta \rangle\}, \text{ where } H := \mathrm{lc}(g_1) \ldots \mathrm{lc}(g_m).$$

We say that a triangular set $\Delta \subset R$ represents *an ideal I if $I = \mathrm{Rep}(\Delta)$.*

Definition 2.2.5. *For an ideal $I \subset R$, we consider the irredundant prime decomposition $\sqrt{I} = I_1 \cap \ldots \cap I_r$ of its radical. We call the $I_1, \ldots, I_r$* the associated primes *of I and denote the set of associated primes of I by* $\mathrm{Ass}(I)$. *When $I = \mathrm{Rep}(\Delta)$, we will write* $\mathrm{Ass}(\Delta)$ *instead of* $\mathrm{Ass}(I)$.

We say that $\sqrt{I}$ and the corresponding variety $V(I)$ are unmixed *if all the associated prime ideals have the same dimension.*

Definition 2.2.6. *Let $\Delta = (g_1, g_2, \ldots, g_m)$ be a triangular set of R with $I = \mathrm{Rep}(\Delta)$ and, for each $1 \leq i \leq m-1$, let $\{P_{i,j}\}_{j=1}^{r_i}$ be the prime ideals in the irredundant prime decomposition of the radical of* $\mathrm{Rep}(\Delta_i)$.

(a) if $lc(g_{i+1}) \notin P_{i,j}$ for every for every $1 \leq i \leq m-1$ and $1 \leq j \leq r_i$, then Δ is called a regular chain, *see [15, Definition 5.7].*

(b) if g_{i+1} is square-free over $K(P_{i,j}) := Quot(R/P_{i,j})$ for every $1 \leq j \leq r_i$ and $1 \leq j \leq r_i$, then Δ is called a squarefree regular chain, *see [15, Definition 7.2]*
(Here, $Quot(R/P_{i,j})$ is the field of fractions of $R/P_{i,j}$.)

Theorem 2.2.1 (see [3, Proposition 2.7])**.** *If Δ is a regular chain, then* $\mathrm{Rep}(\Delta) = \{h \in R \,|\, \mathrm{prem}(h, \Delta) = 0\}$ *and all of the prime ideals in the irredundant prime decomposition of* $\mathrm{Rep}(\Delta)$ *have the same dimension.*

Theorem 2.2.2 (see [15, Corollary 7.3])**.** *If Δ is a squarefree regular chain, then* $\mathrm{Rep}(\Delta)$ *is a radical ideal.*

Remark 3. *We use terminology different from the one used in [33, Section 2.4.3]. The correspondence between these two terminologies is the following: a regular chain is called a weakly unmixed triangular set in [33] and a squarefree regular chain is called an unmixed triangular set in [33].*

Now we are ready to define the main object we will compute.

Definition 2.2.7. *The* triangular decomposition *of an ideal $I \subset R$ is a set $\{\Delta_1, \ldots, \Delta_s\}$ of squarefree regular chains such that*

$$\sqrt{I} = \bigcap_{i=1}^{s} \mathrm{Rep}(\Delta_i).$$

In the rest of the section, we introduce notions and recall results about computing modulo a triangular set.

Definition 2.2.8. *Let $\Delta = (g_1, \ldots, g_m)$ be a triangular set in R with $\mathrm{lead}\,(g_s) = x_{l+s}$ and $d_s := \deg_{x_{l+s}}(g_s)$ for every $1 \leq s \leq m$, where $l := n - m$. We define*

- *$A(\Delta) := k(x_1, x_2, \ldots, x_l)[x_{l+1}, \ldots, x_n]/(\Delta)_{k(x_1,x_2,\ldots,x_l)}$, where the subscript reminds us that we treat elements of the field $k(x_1, x_2, \ldots, x_l)$ as scalars and consider the quotient $A(\Delta)$ as an algebra over this field.*

- *The* standard basis *of $A(\Delta)$, which we will denote by $B(\Delta)$, is the set*

$$B(\Delta) := \{x_{l+1}^{\alpha_1} \ldots x_n^{\alpha_m} \mid 0 \leq \alpha_s < d_s, 1 \leq s \leq m\}.$$

- *The set of* structure constants *of $A(\Delta)$ is the collection of the coordinates of all products of pairs of elements of $B(\Delta)$ in the basis $B(\Delta)$. These structure constants may be organized into a table, which we will refer to as the* multiplication table *for $A(\Delta)$ and which we will denote by $M(\Delta)$.*

- *The* height of the structure constants of $A(\Delta)$ *is the maximum of the heights of the entries of* $M(\Delta)$. *We denote this quantity by* $\Gamma(\Delta)$ *or* Γ *when the triangular set under consideration is clear from context. We will also use the notation* Γ_j *for* $\Gamma(\Delta_j)$.

- *An element of* $A(\Delta)$ *is called* integral *if its coordinates in the standard basis* $B(\Delta)$ *belong to* $k[x_1, \ldots, x_l]$.

Propsition 2.2.1 (see [33, Prop. 3.3.1, p.76]). *Let* Δ *be a triangular set and let* $a_1, a_2, \ldots, a_k$ *be elements of* $A(\Delta)$ *with heights at most* d. *Moreover, assume that the denominators of the coordinates of* $a_1, a_2, \ldots, a_k$ *in the basis* $B(\Delta)$ *divide* $\prod_{s=1}^{m} \mathrm{lc}(g_s)^{\beta_s}$ *and also assume that* $\sum_{s=1}^{m} \beta_s \cdot \mathrm{height}(\mathrm{lc}(g_s)) \leq d'$. *Then*

- $\mathrm{height}(a_1 a_2) \leq \mathrm{height}(a_1) + \mathrm{height}(a_2) + 2(d' + \Gamma)$ *and*

- $\mathrm{height}(a_1 a_2 \ldots a_k) \leq kd + k \log k(d' + \Gamma)$.

In Proposition 2.2.1, if $a_1, \ldots, a_k$ are integral elements, then $\beta_1 = \ldots = \beta_s = 0$. In this case, one can choose $d' = 0$. We will also use denominator bounds in reducing an element modulo Δ.

Lemma 2.2.1. *Let* $\Delta := (g_1, \ldots, g_m) \subset k[x_1, \ldots, x_n]$ *be a squarefree regular chain such that* $\mathrm{height}(g_s) \leq d$ *for all* $s = 1, \ldots, m$. *Let* $f \in k[x_1, \ldots, x_n]$ *be a polynomial of height at most* t. *Then there exist* $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ *and* $q_1, \ldots, q_m, r \in k[x_1, \ldots, x_n]$ *such that:*

- $\mathrm{lc}(g_1)^{\alpha_1} \cdot \cdots \cdot \mathrm{lc}(g_m)^{\alpha_m} \cdot f = q_1 g_1 + \cdots + q_m g_m + f_0$,

- f_0 *is reduced modulo* Δ, *and*

- $\alpha_s \leq t(d+1)^{m-s},\ s = 1, 2, \ldots, m$.

Proof. Similar to [3, Lemma 3.7]. □

Remark 4. *Gallo and Mishra gave a bound in [11, Lemma 5.2] for the degree of the pseudoremainder f_0. We compare that bound with the corresponding bound on f_0 that can be derived from Lemma 2.2.1.*

In the table below, OB stands for "Our Bound" and GM stands for "Gallo-Mishra."

	$\text{height}(g_s) \leq d$ & $\text{height}(f) \leq t$	$\deg(g_s) \leq d$ & $\deg(f) \leq t$
$\deg(f_0)$	*OB:* $nt(d+1)^m$ *GM:* $(nt+1)(nd+1)^m$	*OB:* $nt(d+1)^m$ *GM:* $(t+1)(d+1)^m$
$\text{height}(f_0)$	*OB:* $t(d+1)^m$ *GM:* $(nt+1)(nd+1)^m$	*OB:* $t(d+1)^m$ *GM:* $(t+1)(d+1)^m$

We see that the only case in which the bound from [11, Lemma 5.2] is smaller than the corresponding one derived from Lemma 2.2.1 is represented by the upper-right cell, in which solely degrees are considered. In fact, [11] analyzes the complexity of the Ritt-Wu Characteristic Set Algorithm in terms of degrees. So our pseudoremainder bound cannot be used to improve their complexity analysis and vice versa, as can be seen by examining the lower-left cell in which heights are the focus.

2.3 Outline of Szántó's algorithm

In this section, we recall main steps of the algorithm in [33] for computing a triangular decomposition for a given algebraic set. The main algorithm is described in [33, Theorem 4.1.7, p. 118] and its proof.

Algorithm 1 Triangular decomposition algorithm

In A set of polynomials $F = \{f_0, f_1, \ldots, f_r\} \subset k[x_1, \ldots, x_n]$.

Out A set $\Theta(F)$ of squarefree regular chains such that

$$\sqrt{\langle F \rangle} = \bigcap_{\Delta \in \Theta} \mathrm{Rep}(\Delta).$$

(a) For every $\mathbf{i} \subsetneq \{1, \ldots, n\}$, compute a regular chain $\Delta_{\mathbf{i}}$ with leaders $\{x_j | j \notin \mathbf{i}\}$ such that for every prime component P of $\sqrt{(F)}$

$$\big(\dim(P) = |\mathbf{i}| \text{ and } P \cap k[x_i \mid i \in \mathbf{i}] = \{0\}\big) \Rightarrow \mathrm{Rep}(\Delta_{\mathbf{i}}) \subseteq P.$$

For details, see [33, Cor. 4.1.5, p. 115].

(b) For every $\mathbf{i} \subsetneq \{1, \ldots, n\}$, compute the multiplication table $M(\Delta_{\mathbf{i}})$ of the algebra $A(\Delta_{\mathbf{i}})$ (see Definition 2.2.8).

(c) For every $\mathbf{i} \subsetneq \{1, \ldots, n\}$, compute a set $\mathcal{U}(\Delta_{\mathbf{i}})$ of squarefree regular chains

$$\mathbf{unmixed}_{|\Delta_{\mathbf{i}}|}^{|\mathbf{i}|}(\Delta_{\mathbf{i}}, M(\Delta_{\mathbf{i}}), f, 1), \text{ where } f := \sum_{j=0}^{r} f_i x_{n+1}^j$$

using Algorithm 2 below.

(d) **Return** $\Theta(F) := \bigcup_{\mathbf{i} \subsetneq \{1,\ldots,n\}} \mathcal{U}(\Delta_{\mathbf{i}})$.

Step (c) of Algorithm 1 uses function **unmixed** with the following full specification. Parts concerning multiplication tables are technical and important only for efficiency.

Specification of unmixed$_m^l$.

In

1. Nonnegative integers m and l. We set $n := m + l$.
2. A regular chain $\Delta = \{g_1, \ldots, g_m\} \subset k[x_1, \ldots, x_n]$ such that for all $1 \leq s \leq m$
   - $\text{lead}(g_s) = x_{l+s}$;
   - $\text{lc}(g_s) \in k[x_1, \ldots, x_l]$;
   - g_s is reduced modulo $\{g_1, \ldots, g_{s-1}\}$.
3. The multiplication table $M(\Delta)$ of the algebra $A(\Delta)$, see Definition 2.2.8.
4. Polynomials f, h in $k[x_1, \ldots, x_{n+c}]$ for some $c > 0$ reduced with respect to Δ.

Out A set $\{(\Delta_1, M(\Delta_1)), \ldots, (\Delta_r, M(\Delta_r))\}$ such that

- Δ_i is a squarefree regular chain in $k[x_1, \ldots, x_n]$ for every $1 \leq i \leq r$;
- $M(\Delta_i)$ is the multiplication table of the algebra $A(\Delta_i)$ for every $1 \leq i \leq r$;
- $\bigcup_{i=1}^{r} \text{Ass}(\Delta_i) = \{P \in \text{Ass}(\Delta) \mid f \equiv 0,\ h \not\equiv 0 \mod P\}$ (see Definition 2.2.5);
- $\text{Ass}(\Delta_i) \cap \text{Ass}(\Delta_j) = \varnothing \ \forall\, i \neq j$.

Before describing the algorithm itself, we will give some intuition behind it.

Informally speaking, the main goal of **unmixed** is to transform a single regular chain Δ into a set of regular chains $\Delta_1, \ldots, \Delta_r$ such that

(a) $\Delta_1, \ldots, \Delta_r$ are squarefree regular chains;

(b) prime components of $\bigcap_{i=1}^{r} \text{Rep}(\Delta_i)$ are exactly the prime components of $\text{Rep}(\Delta)$, on which f vanishes and h does not vanish.

It is instructive first to understand how this transformation is performed in the univariate case, i.e. in the case when all regular chains consist of a single polynomial only. This case is also discussed in [33, p. 124-125]. Let Δ consist $g(x) \in k[x]$. A polynomial satisfying only

property ((b)) can be computed using gcd's as follows

$$\frac{\gcd_x(g, f)}{\gcd_x(g, f, h)}. \tag{2.1}$$

A set of polynomials satisfying only property ((a)) can be obtained by separating the roots of $g(x)$ according to their multiplicity again using gcd's

$$\frac{g \gcd_x(g, g', g'')}{\gcd_x^2(g, g')}, \frac{\gcd_x(g, g') \gcd_x(g, g', g'', g^{(3)})}{\gcd_x^2(g, g', g'')}, \ldots \tag{2.2}$$

Formulas (2.1) and (2.2) can be combined to yield to a set of polynomials satisfying both properties ((a)) and ((b)):

$$q_i := \frac{\gcd_x(g, \ldots, g^{(i-1)}, f) \gcd_x(g, \ldots, g^{(i+1)}, f) \gcd_x^2(g, \ldots, g^{(i)}, f, h)}{\gcd_x^2(g, \ldots, g^{(i)}, f) \gcd_x(g, \ldots, g^{(i-1)}, f, h) \gcd_x(g, \ldots, g^{(i+1)}, f, h)}, \quad i = 1, 2, \ldots, \deg g. \tag{2.3}$$

The generalization of this approach to the multivariate case is based on two ideas

(a) Perform the same manipulations with g_m considered as univariate polynomials in x_n.

(b) Replace the standard univariate gcd with the *generalized gcd* (denoted by ggcd), that is a gcd modulo a regular chain $\Lambda := \{g_1, \ldots, g_{m-1}\}$. Generalized gcds are described in [33, Lemma 3.1.3]. Formula (2.3) is replaced then by

$$q_i := \frac{\mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i-1)}, f) \mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i+1)}, f) \mathrm{ggcd}_{x_n}^2(\Lambda, g_m, \ldots, g_m^{(i)}, f, h)}{\mathrm{ggcd}_{x_n}^2(\Lambda, g_m, \ldots, g_m^{(i)}, f) \mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i-1)}, f, h) \mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i+1)}, f, h)} \tag{2.4}$$

for $i = 1, 2, \ldots, \deg_{x_n} g_m$.

Generalized gcd is always well-defined modulo a regular chain representing a prime ideal. If the ideal represented by the regular chain is not prime, then generalized gcds modulo

different prime components might have different degree, so it might be impossible to "glue" them together. In order to address this issue, the **unmixed** function splits $\mathrm{Rep}(\Lambda)$ into a union of varieties represented by regular chains, over which all the generalized gcds in (2.4) will be well defined. Interestingly, this can be done by calling **unmixed** recursively, because the fact that some generalized gcd is well-defined and has degree d can be expressed using equations and inequations. These equations and inequations can be further combined with f and h.

Algorithm 2 Function $\mathbf{unmixed}^l_m(\Delta, M(\Delta), f, h)$

Input and output are described in the specification above.

(a) If $m = 0$ (so $\Delta = \varnothing$), **return** $\varnothing$ if $f \neq 0$ or $h = 0$, and **return** $\{(\varnothing, \varnothing)\}$ otherwise

(b) Set $\Lambda := \Delta_{m-1} = \{g_1, \ldots, g_{m-1}\}$ and compute $M(\Lambda)$.

(c) For every $1 \leq i \leq \deg_{x_n} g_m$ and every tuple $\mathbf{v} \in \mathbb{Z}^6_{\geqslant 0}$ with entries not exceeding $\deg_{x_n} g_m$, compute a pair of polynomials $\phi_{i,\mathbf{v}}, \psi_{i,\mathbf{v}}$ as described in [33, p. 128] such that a system $\phi_{i,\mathbf{v}} = 0,\ \psi_{i,\mathbf{v}} \neq 0$ is equivalent to

- $f = 0$ and $h \neq 0$,
- all six generalized gcds in (2.4) are well-defined and their degrees are the entries of $\mathbf{v}$.

Formulas for $\phi_{i,\mathbf{v}}$ and $\psi_{i,\mathbf{v}}$ are given in the proof of Lemma 2.4.2 and in [33, p. 128].

(d) For every pair ($\phi_{i,\mathbf{v}}$, $\psi_{i,\mathbf{v}}$) computed in the previous step

(i) Compute

$$\mathcal{L}_{i,\mathbf{v}} := \mathbf{unmixed}^l_{m-1}(\Lambda, M(\Lambda), \phi_{i,\mathbf{v}}, \psi_{i,\mathbf{v}}).$$

(ii) For every $(\Lambda_{i,\mathbf{v}}, M(\Lambda_{i,\mathbf{v}})) \in \mathcal{L}_{i,\mathbf{v}}$ compute $q_{i,\mathbf{v}}$ using (2.4) (more details in the proof of Theorem 2.4.1 and in [33, p. 129-130])

(iii) For every $q_{i,\mathbf{v}}$ computed in the previous step, add $(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}, M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}))$ to the **output**

(e) **Return** the set of all pairs $(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}, M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}))$ computed in the previous step

Example 2.3.1. *In this example, we will show that the output of Algorithm 1 can be redun-*

dant confirming [3, Remark 2.9]. We fix a positive integer D and consider

$$F := \{(x_1 - 1)(x_1 - 2)\dots(x_1 - D)(x_2 - 1)(x_2 - 2)\dots(x_2 - D)\}. \tag{2.5}$$

Step (a) of Algorithm 1 will output the following regular chains (see [33, Corollary 4.1.5] for details)

$$\Delta_{\{1\}} = \Delta_{\{2\}} = \{(x_1 - 1)(x_1 - 2)\dots(x_1 - D)(x_2 - 1)(x_2 - 2)\dots(x_2 - D)\},$$
$$\Delta_{\varnothing} = \{(x_1 - 1)(x_1 - 2)\dots(x_1 - D)p_1(x_1), (x_2 - 1)(x_2 - 2)\dots(x_2 - D)p_2(x_2)\},$$

where $p_1(x_1)$ and $p_2(x_2)$ are additional factors, which can appear during the computation with Canny's generalized resultants (see [33, Proposition 4.1.2]).

*At Step (c) of Algorithm 1, $\textbf{\textit{unmixed}}_2^0(\Delta_{\varnothing}, M(\Delta_{\varnothing}), f, 1)$ will be computed. According to the specification of **unmixed**, the result of this computation will be a triangular decomposition of the set of common zeros of $\mathrm{Rep}(\Delta_{\varnothing})$ and F. Since the zero set of $\mathrm{Rep}(\Delta_{\varnothing})$ is finite, all these components are not components of the zero set of F. Points $\{(a_1, a_2) | a_1, a_2 \in \{1, 2, \dots, D\}\}$ are common zeros of $\mathrm{Rep}(\Delta_{\varnothing})$ and F, so the sum of the degrees of these extra components is at least D^2, and the degree of the zero set of F is just $2D$.*

Moreover, this example can be generalized to higher dimensions by replacing (2.5) by

$$F := \{(x_1 - 1)(x_1 - 2)\dots(x_1 - D)\dots(x_n - 1)(x_n - 2)\dots(x_n - D)\}.$$

The degree of the zero set of F is nD, but the sum of the degrees of extra components will be at least D^n.

2.4 Bounds for degrees

The following lemma is a refinement of [33, Proposition 3.3.4, p. 75].

Lemma 2.4.1. *Let* $\Delta = (g_1, \ldots, g_m)$ *be a squarefree regular chain such that* $\text{height}(g_s) \leq d$ *for all* s*. Suppose that for all* $1 \leq s \leq m$ *that*

1. $\text{lead}(g_s) = x_{l+s}$*;*
2. $lc(g_s) \in k[x_1, \ldots, x_l]$*;*
3. g_s *is reduced modulo* $\Delta_{s-1} = (g_1, \ldots, g_{s-1})$*, i.e.* $\forall t < s,\ \deg_{x_{l+t}}(g_s) < \deg_{x_{l+t}}(g_t)$.

Then the height $\Gamma(\Delta)$ *of the matrix* $M(\Delta)$ *of structure constants of* $A(\Delta)$ *(see Definition 2.2.8) does not exceed*

$$(d+2)^{m+1}(\log(d+2))^{m-1}.$$

Proof. We first apply the matrix description of the pseudoremainder (see Appendix) to products of the form $x_{l+1}^{e_1} x_{l+2}^{e_2} \ldots x_{l+m}^{e_m}$, where $e_s \leq 2d_s - 2$. Note that these products are the ones considered in computing the structure constants for $A(\Delta)$ and that such a product will play the role of what we call f in Appendix. Also, what we called g in the Appendix will be g_m in our application, as that is the first element we pseudo-divide by in reducing by Δ. We have two cases to consider: $e_m < d_m$ and $e_m \geq d_m$.

In the first case, the product of interest is already reduced modulo g_m and so can itself be selected as the pseudoremainder by g_m. So we can bound the height of its pseudoremainder by Δ by taking the maximum of $\Gamma_{m-1} := \Gamma(\Delta_{m-1})$ and d_m.

In the second case, what we denote by $\mathbf{f}^{\text{low}}$ in the Appendix is here a column vector with every entry 0 and what we denote by $\mathbf{f}^{\text{up}}$ has exactly one nonzero entry, namely $x_{l+1}^{e_1} x_{l+2}^{e_2} \ldots x_{l+m-1}^{e_{m-1}}$.

We first inspect the $G_0 \cdot \text{adj}(G_d)$ part of the pseudoremainder expression. In computing this product, one will obtain a $d_m \times d_m$ matrix and each of its entries will be sum of products

of at most $1 + (d_m - 1) = d_m$ reduced integral elements of $A(\Delta_{m-1})$. (Note that we have products of reduced integral elements of $A(\Delta_{m-1})$ because g_m is assumed to be reduced modulo Δ_{m-1}.)

Completing the analysis of the number of multiplications needed to compute the pseudoremainder by g_m, we note that the product $x_{l+1}^{e_1} x_{l+2}^{e_2} \dots x_{l+m-1}^{e_{m-1}}$ can be split into two factors where the exponent of each x_{l+s} is less than d_s (because $e_s \leq 2d_s - 2$). So multiplying $G_0 \cdot \mathrm{adj}(G_d)$ by the column vector $\mathbf{f}^{\mathrm{up}}$ results in sums of products of at most $d_m + 2$ reduced integral elements of $A(\Delta_{m-1})$.

So by Proposition 2.2.1 we have

$$\Gamma_m \leq (d_m + 2) \cdot d + (d_m + 2) \log(d_m + 2) \cdot \Gamma_{m-1}.$$

We first replace d_m by d and estimate the first term as $(d+2)^2$ to obtain

$$\Gamma_s < (d+2)^2 + (d+2) \log(d+2) \cdot \Gamma_{s-1}, \quad s = 2, \dots, m.$$

Combining these inequalities, we have

$$\Gamma_m \leq \left[(d+2)^2 \cdot \sum_{k=0}^{m-2} \left((d+2) \log(d+2) \right)^k \right] + \left((d+2) \log(d+2) \right)^{m-1} \Gamma_1.$$

Since the sum in brackets is a finite geometric series with $m-1$ terms and $\Gamma_1 \leq d^2$, we have

$$\Gamma_m \leq (d+2)^2 \left(\frac{\left((d+2) \log(d+2) \right)^{m-1} - 1}{(d+2) \log(d+2) - 1} \right) + \left((d+2) \log(d+2) \right)^{m-1} \cdot d^2.$$

So we obtain $\Gamma_m \leq (d+2)^{m+1} (\log(d+2))^{m-1}$. □

Theorem 2.4.1. *Let $\Delta = (g_1, \dots, g_m) \subset k[x_1, \dots, x_n]$ be a regular chain of height at most*

d ($d > 1$). Let $l := n - m$, and assume that the following conditions are satisfied for every $s = 1, \ldots, m$:

1. $\mathrm{lead}(g_s) = x_{l+s}$,
2. $lc(g_s) \in k[x_1, \ldots, x_l]$,
3. *g_s is reduced modulo $\Delta_{s-1} = (g_1, \ldots, g_{s-1})$.*

Let $M(\Delta)$ be the multiplication table for the algebra $A(\Delta)$. For $f, h \in A(\Delta)[x_{n+1}, \ldots, x_{n+c}]$, denote $d_f := \mathrm{height}(f)$ and $d_h := \mathrm{height}(h)$. Then for each polynomial p occurring in the computation of $\boldsymbol{unmixed}^l_m(\Delta, M(\Delta), f, h)$ (see Algorithm 2), we have:

$$\mathrm{height}(p) \leq 5.2 \cdot 242^m (d^2 + 2d)^m d^{\frac{1}{2}m(m+1)} \left(max\{d, d_f, d_h\} + 7(d+2)^m [\log(d+2)]^{m-1} \right) \log d.$$

Proof. Since for the case $m = 1$ unmixed representation can be obtained simply by taking square-free part of the corresponding polynomial (see [33, p. 124]), in what follows we assume that $m > 1$. Let

$$\{(\Delta_1, M(\Delta_1)), \ldots, (\Delta_r, M(\Delta_r))\} := \mathbf{unmixed}^l_m(\Delta, M(\Delta), f, h)$$

be the output of the algorithm $\mathbf{unmixed}^l_m$ applied to $(\Delta, M(\Delta), f, h)$. Assume that $\Delta_j = (g_{1,j}, \ldots, g_{m,j})$ for $j = 1, \ldots, r$. For each $s = 1, \ldots, m$, we denote

$$\tilde{d}_s := \max \left\{ \deg_{x_{l+s}} (g_{s,j}) \mid j = 1, \ldots, r \right\}. \tag{2.6}$$

The computation of $\mathbf{unmixed}^l_m$ has a tree structure. Consider a path of the computation tree with successive recursive calls:

$$\mathbf{unmixed}^l_m(\Delta_m, M(\Delta_m), f_m, h_m), \ldots, \mathbf{unmixed}^l_0(\Delta_0, M(\Delta_0), f_0, h_0)$$

where $f_m = f$, $h_m = h$ and f_s and h_s are computed from $(\Delta_{s+1}, M(\Delta_{s+1}), f_{s+1}, h_{s+1})$ for each $s = 0, \ldots, m-1$ as described in Step (c) of Algorithm 2 and [33, p. 128]. First we estimate the height of the input at each level.

Lemma 2.4.2. *Let* $\boldsymbol{Input}(s) := \max\{d, \text{height}(f_s), \text{height}(h_s)\}$ *for every* $s = 0, \ldots, m$. *Then*

$$\boldsymbol{Input}(s) \leq (6d)^{m-s} \left(\boldsymbol{Input}(m) + 7(d+2)^m (\log(d+2))^{m-1} \right).$$

Proof. We give an inductive analysis to obtain a bound on $\mathbf{Input}(s)$. For $s = m$, there is nothing to do. So we start with $s = m-1$ and consider the heights of f_{m-1}, h_{m-1}. Computation of these polynomials from the data of level m in Step (c) of Algorithm 2 can be summarized as follows (see also [33, p. 127-128]):

1. Compute the j-th sub-resultants

$$\varphi_k^{(j)}(y,z) := \text{Res}_{x_n}^{(j)} \left(g_m, f_m + \sum_{l=1}^{k} g_m^{(l)} y^{l-1} + z h_m \right),$$

   for $1 \leq k \leq d$ and $0 \leq j \leq d$. Here y, z are new variables (i.e. different from the ones which g_m, f_m, h_m are polynomials in).

2. For each $1 \leq i \leq d$ and $\mathbf{v} = (v_1, \ldots, v_6) \in \mathbb{Z}_{\geqslant 0}^6$, where $0 \leq v_t \leq d$ for $1 \leq t \leq 6$,

   (a) define the polynomial $\phi_{i,\mathbf{v}}(y,z,w)$ to be a linear combination of polynomials

$$\varphi_{i-1}^{(u_1)}(y,0), \;\; \varphi_i^{(u_2)}(y,0), \;\; \varphi_{i+1}^{(u_3)}(y,0), \;\; \varphi_{i-1}^{(u_4)}(y,z), \;\; \varphi_i^{(u_5)}(y,z), \;\; \varphi_{i+1}^{(u_6)}(y,z)$$

   for all $u_1, \ldots, u_6$ such that $u_i < v_i$ for $1 \leq i \leq 6$ by using the powers of a new variable w.

(b) define

$$\psi_{i,\mathbf{v}}(y,z) := \varphi_{i-1}^{(v_1)}(y,0) \cdot \varphi_i^{(v_2)}(y,0) \cdot \varphi_{i+1}^{(v_3)}(y,0) \cdot \varphi_{i-1}^{(v_4)}(y,z) \cdot \varphi_i^{(v_5)}(y,z) \cdot \varphi_{i+1}^{(v_6)}(y,z).$$

(c) reduce $\phi_{i,\mathbf{v}}$ and $\psi_{i,\mathbf{v}}$ with respect to Λ.

(d) Set $f_{m-1} := \phi_{i,\mathbf{v}}$ and $h_{m-1} := \psi_{i,\mathbf{v}}$ for this choice of $i, \mathbf{v}$.

Note that new variables y, z and w were introduced. In Algorithm 2, all new introduced variables are denoted by $x_{n+1}, \ldots, x_{n+c}$. Here we use names y, z, and w for notational simplicity.

In order to bound the heights of f_{m-1} and h_{m-1}, we bound the heights of the subresultants $\varphi_k^{(j)}(y,z)$. In the computation of a bound for the heights of the subresultants, the largest bound will be a bound for the 0-th subresultant, because higher ones are obtained by deleting rows and columns of the Sylvester matrix, whose determinant produces the 0-th subresultant.

Since we are taking subresultants with respect to x_n, all the entries of the Sylvester matrix are polynomials in $x_1, x_2, \ldots, x_{n-1}$. In particular, this means that their degrees in x_{l+i} are less than d_i for all $1 \leq i < m$. Size of this matrix is at most $d_m + d_m = 2d_m$. The first d_m is because $\deg_{x_n} g_m = d_m$. The second d_m is because f, h are reduced with respect to Δ.

Since f_{m-1}, h_{m-1} must be reduced modulo Δ_{m-1}, we will be carrying out all operations in $A(\Delta_{m-1})$. One can see that the bound for the height of h_{m-1} that we will obtain is larger than a similar computation would produce for f_{m-1}. So we focus on getting a bound for the height of h_{m-1}, thereby obtaining a bound for $\mathbf{Input}(m-1)$. In fact, our technique will give us a bound for $\mathbf{Input}(s)$ in terms of $\mathbf{Input}(s+1)$.

Since the computation of h_{m-1} involves a multiplication of six evaluated subresultants, we apply Proposition 2.2.1 to the sixth power of the 0th subresultant (as described above) in two stages:

1. For the first stage, note that each term of the sixth power of the 0-th subresultant is a product of $12d_m$ factors. We split these up into two groups: the $6d_m$ factors of any term coming from the coefficients of g_m (call the product of these C) and the rest from the coefficients of $f + \sum_{l=1}^{k} g_m^{(l)} y^{l-1} + zh$ (call the product of these D). In this first stage, we need not worry about denominator bounds because all of the factors of C and D are integral elements of $A(\Delta)$.
2. We then take these two groups of $6d_m$ factors, reduce them, and multiply them. In the reduction step, we obtain some denominators in general and so we will need to compute bounds on these.

Assume that the heights of denominators of C and D are bounded by d'. Our two-step analysis of the height of CD using Proposition 2.2.1 yields:

$$\begin{aligned}\text{height}(CD) &\leq \text{height}(C) + \text{height}(D) + 2\log(2) \cdot (\Gamma(\Delta_{m-1}) + d') \\ &\leq 6d_m \cdot d + 6d_m \cdot \mathbf{Input}(m) + 12d_m \log(6d_m) \cdot \Gamma(\Delta_{m-1}) + 2 \cdot (\Gamma(\Delta_{m-1}) + d') \\ &\leq 6d^2 + 6d \cdot \mathbf{Input}(m) + 12d \log(6d) \cdot \Gamma(\Delta_{m-1}) + 2 \cdot (\Gamma(\Delta_{m-1}) + d').\end{aligned}$$

We may bound d' by considering the sequence of exponents we obtain on $\text{lc}(g_i)$ when reducing C, D modulo Δ_{m-1}. Applying Lemma 2.2.1 with $\text{height}(C) \leq 6d^2 =: t$, we have

$$d' \leq \sum_{i=1}^{m-1} 6d^2(d+1)^{m-1-i} \cdot d = 6d^2(d+1)^{m-1} - 6d^2.$$

Therefore

$$\begin{aligned}\text{height}(h_{m-1}) \leq 6d^2 + 6d \cdot \mathbf{Input}(m) + 12d \log(6d) \cdot \Gamma(\Delta_{m-1}) + \\ + 2 \cdot \left(\Gamma(\Delta_{m-1}) + 6d^2(d+1)^{m-1} - 6d^2\right).\end{aligned}$$

As a result, we have

$$\mathbf{Input}(m-1) \leq \Gamma(\Delta_{m-1}) \cdot (12d\log(6d)+2) + 6d \cdot \mathbf{Input}(m) + 12d^2(d+1)^{m-1}.$$

Moreover, we can obtain a bound for $\mathbf{Input}(s)$ in term of $\mathbf{Input}(s+1)$ in a similar way. In particular, we have

$$\mathbf{Input}(s) \leq \Gamma(\Delta_s) \cdot (12d\log(6d)+2) + 6d \cdot \mathbf{Input}(s+1) + 12d^2(d+1)^s$$

for every $s = 0, \ldots, m-1$. Due to Lemma 2.4.1

$$\Gamma(\Delta_s) \leq (d+2)^{s+1}(\log(d+2))^{s-1}.$$

Using $d \geq 2$, it can be shown that

$$\frac{12d\log(6d)+2}{(d+2)\log(d+2)} \leq 17 \quad \text{and} \quad \frac{12d^2}{(d+1)^2} \leq 12.$$

We therefore modify our recursive bound and obtain

$$\mathbf{Input}(s) \leq 17 \cdot (d+2)^{s+2}(\log(d+2))^s + 6d \cdot \mathbf{Input}(s+1) + 12(d+1)^{s+2}$$

for $s = 0, 1, \ldots, m-1$. Thus, $\mathbf{Input}(s)$ does not exceed

$$(6d)^{m-s} \cdot \mathbf{Input}(m) + 17 \cdot \sum_{k=0}^{m-s-1} (6d)^k (d+2)^{s+k+2} (\log(d+2))^{s+k} + 12 \cdot \sum_{k=0}^{m-s-1} (6d)^k (d+1)^{s+k+2}.$$

Using the formula for geometric series and $d \geq 2$, we can deduce that

$$\mathbf{Input}(s) \leq (6d)^{m-s} \left(\mathbf{Input}(m) + 6(d+2)^m (\log(d+2))^{m-1} + 3.1(d+1)^m \right).$$

Using $d, m \geq 2$ we can further show that $3.1(d+1)^m \leq (d+2)^m(\log(d+2))^{m-1}$, so the above expression is bounded by

$$(6d)^{m-s}\left(\mathbf{Input}(m) + 7(d+2)^m(\log(d+2))^{m-1}\right). \qquad \square$$

We return to the proof of Theorem 2.4.1. Using the same notation as in [33, p. 141], we denote by $\mathbf{Output}(s)$ the maximum height of polynomials computed up to level s. For example, if $s = 0$, we have $\mathbf{Output}(0) = \mathbf{Input}(0)$.

We are going to derive an upper bound for $\mathbf{Output}(m)$ recursively. Assume that we have determined $\mathbf{Output}(m-1)$ which is an upper bound for all polynomials computed up to level $m-1$. Let $i \leq d$ and $\mathbf{v} \in \mathbb{Z}^6_{\geq 0}$ such that $0 \leq v_t \leq d$ for every $t = 1, 2, \ldots, 6$. Let $(\Lambda_{i,\mathbf{v}}, M(\Lambda_{i,\mathbf{v}}))$ be an arbitrary output after the recursive call at level $m-1$ for these i and $\mathbf{v}$ (see Steps (c) and (d) of Algorithm 2). The construction of the corresponding output $(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}, M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}))$ from Step (d) of Algorithm 2 (see also [33, p. 129]) is the following

1. Compute d_{t,i,v_t}, $1 \leq t \leq 6$, defined by (see [33, p. 127])

$$\begin{aligned}
d_{1,i,v_1} &:= \mathrm{ggcd}_{x_n}\left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i-1)}, f_m\right)\\
d_{2,i,v_2} &:= \mathrm{ggcd}_{x_n}\left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i)}, f_m\right)\\
d_{3,i,v_3} &:= \mathrm{ggcd}_{x_n}\left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i+1)}, f_m\right)\\
d_{4,i,v_4} &:= \mathrm{ggcd}_{x_n}\left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i-1)}, f_m, h_m\right)\\
d_{5,i,v_5} &:= \mathrm{ggcd}_{x_n}\left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i)}, f_m, h_m\right)\\
d_{6,i,v_6} &:= \mathrm{ggcd}_{x_n}\left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i+1)}, f_m, h_m\right)
\end{aligned}$$

Generalized gcd (ggcd) is described in [33, Lemma 3.1.3].

2. Compute

$$\overline{\mathrm{lc}(d_{t,i,v_t})} := \mathbf{pinvert}^l_{m-}\left(\Lambda_{i,\mathbf{v}}, M(\Lambda_{i,\mathbf{v}}), \mathrm{lc}(d_{t,i,v_t})\right) \text{ for } 1 \leq t \leq 6,$$

where the function $\mathbf{pinvert}^l_m(\Delta, M(\Delta), f)$ for computing the pseudo-inverse of f has the following specification (see also [33, Section 3.4])

In Δ: a squarefree regular chain in $k[x_1, \ldots, x_{l+m}]$, where $x_{l+1}, \ldots, x_{l+m}$ are the leaders of Δ;

$M(\Delta)$: the multiplication table of $A(\Delta)$ (see Definition 2.2.8);

f: a polynomial in $k[x_1, \ldots, x_{l+m}]$ such that $f \notin P$ for every $P \in \mathrm{Ass}(\Delta)$;

Out $\bar{f} \in k[x_1, \ldots, x_{m+l}]$ such that $\bar{f} \cdot \bar{f} \equiv r \pmod{\mathrm{Rep}(\Delta)}$, where $r \in k[x_1, \ldots, x_l] \setminus \{0\}$.

3. Compute $\overline{d}_{t,i,v_t} := \overline{\mathrm{lc}(d_{t,i,v_t})} \cdot d_{t,i,v_t}$ for $1 \leq t \leq 6$.

4. Compute

$$p^{(1)}_{i,\mathbf{v}} := \overline{d}_{1,i,v_1} \cdot \overline{d}_{3,i,v_3} \cdot \overline{d}^2_{5,i,v_5} \quad \text{and} \quad p^{(2)}_{i,\mathbf{v}} := \overline{d}^2_{2,i,v_2} \cdot \overline{d}_{4,i,v_4} \cdot \overline{d}_{6,i,v_6},$$

and then $q_{i,\mathbf{v}}$, the result of the pseudo-division $p^{(1)}_{i,\mathbf{v}}$ by $p^{(2)}_{i,\mathbf{v}}$.

5. Compute the multiplication table $M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\})$.

We are going to bound the heights of the polynomials appearing in each step.

Step 1. The construction of ggcd in [33, Lemma 3.1.3] implies that $\mathrm{height}(d_{t,i,v_t}) \leq \mathbf{Input}(m-1)$ for every $t = 1, \ldots, 6$.

Step 2. We denote by D_{m-1} the dimension of the algebra $A(\Delta)$ over k. Then $D_{m-1} = \prod_{i=1}^{m-1} \tilde{d}_i$ (see (2.6)). The coefficients of $\overline{\mathrm{lc}(d_{t,i,v_t})}$ are defined as the determinants of matrices of

size $D_{m-1} \times D_{m-1}$ (see [33, p. 84]). Every such matrix has a column of the form $[0, \ldots, 0, 1]^t$, and the entries of the matrix have the height at most

$$\text{height}(d_{t,i,v_t}) + \Gamma(\Lambda_{i,\mathbf{v}}) \leq \mathbf{Input}(m-1) + \mathbf{Output}(m-1).$$

Therefore

$$\text{height}(\overline{\text{lc}(d_{t,i,v_t})}) \leq (D_{m-1} - 1)(\mathbf{Input}(m-1) + \mathbf{Output}(m-1)).$$

Step 3. Now we compute $\overline{d}_{t,i,v_t} := \overline{\text{lc}(d_{t,i,v_t})} \cdot d_{t,i,v_t}$. Applying [33, Proposition 3.3.1, p. 66], we have

$$\begin{aligned}\text{height}(\overline{d}_{t,i,v_t}) &\leq \text{height}(\overline{\text{lc}(d_{t,i,v_t})}) + \text{height}(d_{t,i,v_t}) + 2\log 2 \cdot \Gamma(\Lambda_{i,\mathbf{v}}) \\ &= D_{m-1}\,\mathbf{Input}(m-1) + (D_{m-1}+1)\,\mathbf{Output}(m-1).\end{aligned}$$

Step 4. Note that, for each $t = 1, \ldots, 6$, we have $\deg_{x_n} \overline{d}_{t,i,v_t} = \deg_{x_n}(d_{t,i,v_t}) \leq d$. Therefore $p^{(1)}_{i,\mathbf{v}}$ and $p^{(2)}_{i,\mathbf{v}}$ are polynomials of degree at most $4d$ in x_n. By using the matrix representation for the quotient of the pseudo-division algorithm, the coefficients of $q_{i,v}$ are equal to a sum of products of at most $4d$ coefficients of $p^{(1)}_{i,\mathbf{v}}$ or $p^{(2)}_{i,\mathbf{v}}$. Each coefficient of $p^{(1)}_{i,\mathbf{v}}$ and $p^{(2)}_{i,\mathbf{v}}$ is a sum of products of 4 coefficients of $\overline{d}_{t,i,v_t}$, $t = 1, \ldots, 6$. Thus, coefficients of $q_{i,\mathbf{v}}$ are sums of products of at most $16d$ coefficients of $\overline{d}_{t,i,v_t}$, $t = 1, \ldots, 6$. Note that $\overline{d}_{t,i,v_t}$ are polynomials and are reduced by $\Lambda_{i,\mathbf{v}}$. Applying [33, Proposition 3.3.1, p. 66], we obtain

$$\begin{aligned}\text{height}(q_{i,\mathbf{v}}) &\leq 16d \cdot \max_{t=1,\ldots,6}\{\text{height}(\overline{d}_{t,i,v_t})\} + 16d\log(16d) \cdot \Gamma(\Lambda_{i,\mathbf{v}}) \\ &\leq (16dD_{m-1} + 16d + 16d\log(16d))\,\mathbf{Output}(m-1) + 16dD_{m-1}\,\mathbf{Input}(m-1).\end{aligned}$$

Step 5. As the last step of the computation at level m, we compute the multiplication

table $M(\Delta_{i,\mathbf{v}})$ for the algebra $A(\Delta_{i,\mathbf{v}})$, where $\Delta_{i,\mathbf{v}} := \Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}$. We already know that the height of any entry in the multiplication table $M(\Lambda_{i,\mathbf{v}})$ is at most $\mathbf{Output}(m-1)$. In order to obtain an upper bound for the heights of coefficients in $M(\Delta_{i,\mathbf{v}})$, we need to estimate the height of the remainder in the pseudo division of $x_{l+1}^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_m}$ by $q_{i,\mathbf{v}}$, where $0 \leq \alpha_s \leq 2\deg_{x_{l+s}}(g_s) - 2$, $1 \leq s \leq m$. Note that $q_{i,\mathbf{v}}$ is reduced modulo $\Lambda_{i,\mathbf{v}}$, and that $\deg_{x_n} q_{i,\mathbf{v}} \leq \tilde{d}_m$. By using the matrix representation of the remainder in the pseudo-division algorithm (see Appendix), the remainder obtained when we divide $x_{l+1}^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_m}$ by $q_{i,\mathbf{v}}$ is equal to a sum of products of at most $\tilde{d}_m + 2$ integral elements in $A(\Lambda_{i,\mathbf{v}})$. Therefore,

$$\Gamma(\Delta_{i,\mathbf{v}}) \leq (\tilde{d}_m + 2)\,\mathrm{height}(q_{i,\mathbf{v}}) + (\tilde{d}_m + 2)\log(\tilde{d}_m + 2)\Gamma(\Lambda_{i,\mathbf{v}}).$$

This is also an upper bound for all polynomials computed up to level m. In other words,

$$\mathbf{Output}(m) \leq (\tilde{d}_m + 2)\left(16dD_{m-1} + 16d + 16d\log(16d) + \log(\tilde{d}_m + 2)\right)\mathbf{Output}(m-1) + \\ + 16dD_{m-1}(\tilde{d}_m + 2)\,\mathbf{Input}(m-1).$$

We note that the computations are in the algebra $A(\Delta)$. Therefore we always have

$$\tilde{d}_i \leq d \text{ for every } i = 1, \ldots, m. \tag{2.7}$$

Thus $\mathbf{Output}(m)$ does not exceed

$$(d+2)(16d^m + 16d\log(32d) + \log(d+2))\,\mathbf{Output}(m-1) + \ + 16(d+2)d^m\,\mathbf{Input}(m-1).$$

A similar argument shows that $\mathbf{Output}(s)$ does not exceed

$$\mathbf{Output}(s) \leq (d+2)(16d^s+16d\log(32d)+\log(d+2))\,\mathbf{Output}(s-1)++16(d+2)d^s\,\mathbf{Input}(s-1) \tag{2.8}$$

for every $s = 1, \ldots, m$. Lemma 2.4.2 implies that

$$\mathbf{Input}(0) \leq I_0 := (6d)^m \left(\max\{d, d_f, d_h\} + 11(d+2)^m(\log(d+2))^{m-1}\right)$$

and

$$\mathbf{Input}(s-1) \leq (6d)^{-s+1} I_0.$$

Using this notation in (2.8), we see that

$$(6^s\,\mathbf{Output}(s)) \leq C(s)(6^{s-1}\,\mathbf{Output}(s-1)) + 96d(d+2)I_0 \tag{2.9}$$

where

$$C(s) := 6(d+2)(16d^s + 16d\log(32d) + \log(d+2)). \tag{2.10}$$

Now we unfold this recursion and rewrite $6^m\,\mathbf{Output}(m)$ using $6^{m-1}\,\mathbf{Output}(m-1)$ and so on, we see that

$$\begin{aligned} 6^m\,\mathbf{Output}(m) &\leq \left(\prod_{s=1}^{m} C(s)\right) \cdot \mathbf{Output}(0) + 96d(d+2)I_0 \sum_{s=2}^{m}\prod_{i=s}^{m} C(i) \\ &= \left(\prod_{s=1}^{m} C(s) + 96d(d+2)\sum_{s=2}^{m}\prod_{i=s}^{m} C(i)\right) \cdot I_0. \end{aligned} \tag{2.11}$$

We simplify (2.11) by applying Lemma 2.4.3. In particular, we have:

$$6^m\,\mathbf{Output}(m) < 5.2 \cdot (242(d+2))^m \cdot d^{\frac{1}{2}m(m+1)} \cdot \log d \cdot I_0.$$

The inequality obtained after canceling the factor 6^m from both sides is exactly the inequality we need to prove. □

Theorem 2.4.2. *Let $F := \{f_0, f_1, \ldots, f_r\} \subset k[x_1, \ldots, x_n]$ be a set of polynomials of degree at most d. Let m be the maximum codimension of prime components of $\sqrt{(F)}$. Then the degree of any polynomial p appearing in the output of Algorithm 1 applied to F or during the computation does not exceed*

$$B(m,d) := 5.2n \cdot 242^m (d^{2m}+2d^m)^m d^{\frac{1}{2}m^2(m+1)} \left(\max\{d^m, r\} + 7(d^m+2)^m (\log(d^m+2))^{m-1}\right) \log d^m. \tag{2.12}$$

In particular, in case r is not too large, for instance if $r \leq d^m$, we have

$$\deg p \leq n d^{(\frac{1}{2}+\epsilon)m^3}$$

where $\epsilon = \epsilon(m,d)$ is a decreasing function such that $\epsilon(m,d) < 5$ for every $d \geq 2$, $m \geq 2$, and $\lim_{m\to\infty} \epsilon(m,d) = 0$ for all d.

Remark 5. *[17, Lemma 3] implies that $f_0, \ldots, f_r$ can be replaced by their $n+1$ generic linear combinations, so one can achieve $r \leq n$.*

Proof. By [33, Corollary 4.1.5, p. 115], for every $\Delta \in \Sigma(F)$ computed in Step (a) of Algorithm 1, the height of polynomials in Δ is at most $d^{|\Delta|} \leq d^m$.

At Step (b) of Algorithm 1, for each $\Delta \in \Sigma(F)$, we compute the multiplication table $M(\Delta)$. Step (c) of Algorithm 1 is a computation of

$$\mathcal{U}(\Delta) := \mathbf{unmixed}_{|\Delta|}^{n-|\Delta|}(\Delta, M(\Delta), f, 1) \text{ for every } \Delta \in \Sigma(F)$$

where $f = f_0 + yf_1 + \ldots + y^r f_r \in k[x_1, \ldots, x_n, y]$. Note, that for each $\Delta \in \Sigma(F)$, we have $|\Delta| \leq m$.

By Theorem 2.4.1, for every polynomial p occurring in the computation of $\mathcal{U}(\Delta)$, we have

$$\text{height}(p) \leq \frac{1}{n} B(|\Delta|, d).$$

Since $B(m, d)$ is monotonic in m and $|\Delta| \leq m$, this implies (2.12).

In case $r \leq d^m$, we have $\max\{r, d^m\} = d^m$. Direct computation shows that the right hand side of (2.12) can be bounded by $\deg p \leq n d^{(\frac{1}{2}+\epsilon)m^3}$, where

$$\epsilon = \epsilon(m, d) := \frac{\log_d \left(\frac{1}{n} B(m, d)\right)}{m^3} - \frac{1}{2}$$

which is a decreasing function with $\epsilon(m, d) < 5$ for every $d \geq 2, m \geq 2$. Moreover, $\lim_{m \to \infty} \epsilon(m, d) = 0$ for all d. □

Remark 6. *Unlike [33, Theorem 4.1.7, p. 118], the height of polynomials occurring in the computations is bounded by $d^{O(m^3)}$. In general, Algorithm 1 might produce a redundant unmixed decomposition for a given algebraic set. Moreover, it can output varieties defined by regular chains whose irreducible components are not the irreducible components of the initial algebraic set (see Example 2.3.1). Therefore the inequality (4.13) in [33, p. 121] is not necessarily true in general. Instead of it we use* (2.7) *in order to bound $\tilde{d}_i$. The right-hand side of* (2.7) *is d^m in terms of the input data of Algorithm 1, and this makes our bound $d^{O(m^3)}$.*

Lemma 2.4.3. *Consider $C(s)$ defined as (see also* (2.10)*)*

$$C(s) := 6(d+2)(16d^s + 16d \log(32d) + \log(d+2)).$$

Then we have:

$$\prod_{s=1}^{m} C(s) \leq \frac{678 \cdot 387}{242^2} \cdot (242(d+2))^m \cdot d^{\frac{1}{2}m(m+1)} \log d, \quad \textit{and}$$

$$\sum_{s=2}^{m} \prod_{i=s}^{m} C(i) \leq \frac{387 \cdot 4}{967} \cdot (242(d+2))^{m-1} \cdot d^{\frac{1}{2}m(m+1)-1}.$$

Proof. Using $d \geq 2$, we can verify the following inequalities by direct computation

$$C(s) \leq \begin{cases} 242(d+2)d^s \text{ if } s > 2, \\ 387(d+2)d^s \text{ if } s = 2, \\ 678(d+2)d^s \log d \text{ if } s = 1. \end{cases}$$

This immediately implies the first inequality in the lemma. For the second one:

$$\begin{aligned} \sum_{s=2}^{m} \prod_{i=s}^{m} C(i) &\leq \frac{387}{242} \sum_{s=2}^{m} (242(d+2))^{m-s+1} \cdot d^{s+(s+1)+\ldots+m} \\ &\leq \frac{387}{242} d^{\frac{1}{2}m(m+1)-1} \sum_{s=1}^{m-1} (242(d+2))^s \\ &\leq \frac{387}{242} d^{\frac{1}{2}m(m+1)-1} \cdot (242(d+2)^{m-1} \cdot \frac{(242(d+2))}{(242(d+2))-1} \\ &\leq \frac{387 \cdot 4}{967} \cdot d^{\frac{1}{2}m(m+1)-1} \cdot (242(d+2))^{m-1}. \end{aligned}$$

□

2.5 Bound for the number of components

In this section, we study the number of components in the output of Szántó's algorithm.

Theorem 2.5.1. *Let $F \subset k[x_1, \ldots, x_n]$ be a finite set of polynomials of degree at most d. Let m be the maximum codimension of prime components of $\sqrt{(F)} \subseteq k[x_1, \ldots, x_n]$. Then*

the number of unmixed components in the output of Algorithm 1 applied to F is at most

$$\binom{n}{m}\left((m+1)d^m+1\right)^m.$$

Proof. Since the degree of the given polynomials is at most d, so is their height. Step (a) of Algorithm 1 produces a set $\Sigma(F) := \{\Delta_{\mathbf{i}} \mid \mathbf{i} \subsetneq [n]\}$ of regular chains such that for every prime component P of $\sqrt{(F)}$, we have

$$(\dim P = |\mathbf{i}| \text{ and } P \cap k[x_i \mid i \in \mathbf{i}] = 0) \Rightarrow \mathrm{Rep}(\Delta) \subseteq P.$$

Due to [15, Theorem 4.4], the number of elements in a regular chain Δ is equal to the codimension of the ideal $\mathrm{Rep}(\Delta)$. Therefore the number of regular chains in $\Sigma(F)$ is not larger than the number of proper subsets of $[n]$ which has cardinality at most m.

In Step (c), we use the function **unmixed** to transform each regular chain $\Delta \in \Sigma(F)$ to the set

$$\mathcal{U}(\Delta) := \mathbf{unmixed}_{|\Delta|}^{n-|\Delta|}(\Delta, M(\Delta), f, 1)$$

of squarefree regular chains (see Algorithm 2). Thus the number of squarefree regular chains in the output is

$$M(n,m,d) := \left|\bigcup_{\Delta\in\Sigma(F)} \mathcal{U}(\Delta)\right| \leq \sum_{\Delta\in\Sigma(F)} |\mathcal{U}(\Delta)|.$$

We fix a regular chain $\Delta = (g_1, \ldots, g_s)$ of codimension s. The collection of squarefree regular chains in the output of $\mathbf{unmixed}_{|\Delta|}^{s}$ is simple, meaning that any two distinct unmixed components have no common irreducible components (see [33, page 124]). Since all the components of $\mathrm{Rep}(\Delta)$ are of codimension s, $|\mathcal{U}(\Delta)|$ is bounded from above by the degree of $\mathrm{Rep}(\Delta)$. Due to the definition of $\mathrm{Rep}(\Delta)$, we have $\mathrm{Rep}(\Delta) \supset (\Delta)$. Moreover, since $V(\Delta)$ and

$V(\mathrm{Rep}(\Delta))$ coincide outside the zero set of the product of the initials of Δ, every irreducible component of $V(\mathrm{Rep}(\Delta))$ is an irreducible component of $V(\Delta)$. Hence, the degree of $\mathrm{Rep}(\Delta)$ does not exceed the sum of degrees of irreducible components of $V(\Delta)$. The latter can be bounded by $\deg g_1 \cdot \ldots \cdot \deg g_s$ due to [13, Theorem 1]. The proof of [33, Corollary 4.1.5] implies that every g_i depends on at most $s+1$ variables, so

$$\deg g_i \leq (s+1)\,\mathrm{height}\, g_i \leq (s+1)d^s.$$

Therefore

$$|\mathcal{U}(\Delta)| \leq (s+1)^s d^{s^2} \leq \left((m+1)d^m\right)^s.$$

Since for each $s = 1, \ldots, m$, there are $\binom{n}{s}$ squarefree regular chains in $\Sigma(F)$ of cardinality s,

$$M(n,m,d) \leq \sum_{s=1}^{m} \binom{n}{s} \left((m+1)d^m\right)^s.$$

Since $\binom{n}{s} \leq \binom{n}{m} \cdot \binom{m}{s}$, we have that $M(n,m,d) \leq \binom{n}{m}\left((m+1)d^m+1\right)^m$. □

Chapter 3

Differential Galois Groups

3.1 Differential rings

Definition 3.1.1. *A derivation of a ring R is a map $d : R \to R$ such that $\forall a, b \in R, d(a+b) = d(a) + d(b)$ and $d(ab) = d(a)b + ad(b)$.*

Definition 3.1.2. *A differential ring (R, d) is a commutative ring R with identity endowed with a derivation d.*

Definition 3.1.3. *$(R_1, d_1) \subset (R_2, d_2)$ is a differential ring extension if $R_1 \subset R_2$ and $d_2|_{R_1} = d_1$.*

Definition 3.1.4. *If (R_1, d_1) and (R_2, d_2) are differential rings, a map $f : R_1 \to R_2$ is a differential morphism if it satisfies:*

- $f(a + b) = f(a) + f(b), f(ab) = f(a)f(b), \forall a, b \in R_1, f(1) = 1.$
- $d_2(f(a)) = f(d_1(a)), \forall a \in R_1.$

A differential morphism from a differential ring R to itself is called a differential endomorphism.

Definition 3.1.5. *(K, d) is called a differential field if K is a field and (K, d) is a differential ring.*

Definition 3.1.6. *Let (R, d) is a differential ring. If $a \in R$ and $d(a) = 0$, then a is called a constant in this differential ring.*

Definition 3.1.7. *If (K, d) is a differential field, then the field of constants of K is the subfield $\{c \mid d(c) = 0\}$.*

3.2 Picard-Vessiot extensions

In the following sections of this chapter, K is a differential field of characteristic zero.

Consider a linear differential equation over K, with field of constants C:

$$\mathcal{L} := Y^n + a_{n-1}Y^{n-1} + \cdots + a_1Y' + a_0Y = 0, a_i \in K.$$

Definition 3.2.1. *Given a linear differential equation $\mathcal{L}(Y) = 0$ of order n over K, a differential extension $K \subset L$ is a Picard-Vessiot extension for $\mathcal{L}$ if*

- *$L = K\langle y_1, \ldots, y_n\rangle$, where $y_1, \ldots, y_n$ is a fundamental set of solutions of $\mathcal{L}(Y) = 0$ in L.*
- *Every constant of L lies in K.*

Example 3.2.1. *Consider $\mathcal{L}(Y) = Y'' + Y = 0$ over $\mathbb{C}(t)$. $\sin t$ and $\cos t$ are two linearly independent solutions over $\mathbb{C}$, so $\{\sin t, \cos t\}$ is a set of fundamental solutions. $\cos t = \frac{e^{it}+e^{-it}}{2}$ and $\sin t = \frac{-ie^{it}+ie^{-it}}{2}$ where e^{it} and e^{-it} are exponentials of integrals of $i, -i \in \mathbb{C}(t)$ respectively. $(\sin t)' = \cos t$ and $(\cos t)' = -\sin t$. Assume that the polynomial $\sum_{j=0}^{n} a_j(e^{it})^j$, where $a_j \in \mathbb{C}(t)$, is a constant in $K\langle \sin t, \cos t\rangle$. So $0 = \sum_{j=0}^{n}(a_j' + a_j ij)e^{ijt}$. Assume that e^{it} is algebraic over K. Let $p(x) = x^m + \sum_{k=0}^{m-1} b_k x^k$ be its minimal irreducible polynomial*

over K. Then $(e^{it})^m + b_{m-1}(e^{it})^{m-1} + \cdots + b_1 e^{it} + b_0 = 0$. Differentiating it, we have $mi(e^{it})^m + b_{m-1}(e^{it})^{m-1} + b_{m-1}(m-1)i(e^{it})^{m-1} + \cdots + b_1' e^{it} + b_1 i e^{it} + b_0' = 0$. Subtracting this equation from mi times the first equation, we have $(ib_{m-1} - b_{m-1}')(e^{it})^{m-1} + (2ib_{m-2} - b_{m-2}')(e^{it})^{m-2} + \cdots + ((m-1)ib_1 - b_1')e^{it} + mib_0 - b_0' = 0$. Since $y' = kiy$, where $1 \leq k \leq m$, has no nonzero solutions in $\mathbb{C}(t)$, $kib_{m-k} - b_{m-k}' \neq 0$ for $1 \leq k \leq m$. So there is a polynomial of degree less than m where e^{it} vanishes. This is a contradiction. So e^{it} is transcendental over K. This implies that $a_j' + a_j ij = 0$ and $a_j' = -jia_j$. Since $((e^{it})^{-j})' = -ji(e^{it})^{-j}$, $(e^{it})^{-j} = ca_j$ where $c \in \mathbb{C}$. This is a contradiction that e^{it} is transcendental over $\mathbb{C}(t)$. Assume that the rational function $\frac{g(e^{it})}{h(e^{it})}$, where $h(e^{it})$ is monic of the minimum degree ≥ 1, is a constant in $K\langle \sin t, \cos t\rangle$. So $0 = \frac{ie^{it}g'(e^{it})h(e^{it}) - ie^{it}g(e^{it})h'(e^{it})}{h^2(e^{it})}$. This implies that $\frac{g(e^{it})}{h(e^{it})} = \frac{g'(e^{it})}{h'(e^{it})}$. Since the polynomial h is not a constant in $K\langle \sin t, \cos t\rangle$, h' has lower degree than h which is a contradiction. So adding $\sin t$ and $\cos t$ to $\mathbb{C}(t)$ does not create new constants. The Picard-Vessiot extension of $\mathcal{L}(Y) = Y'' + Y = 0$ is $L = K\langle \sin t, \cos t\rangle$.

Example 3.2.2. *Consider $\mathcal{L}(Y) = Y'' + \frac{1}{t}Y = 0$ over $\mathbb{C}(t)$. 1 and $\ln t$ are two linearly independent solutions over $\mathbb{C}$, so $\{1, \ln t\}$ is a set of fundamental solutions. $\ln t$ is an integral of $\frac{1}{t} \in \mathbb{C}(t)$. Assume that the polynomial $\sum_{i=0}^{n} a_i(\ln t)^i$, where $a_i \in \mathbb{C}(t)$, is a constant in $K\langle \ln t\rangle$. So $0 = a_n'(\ln t)^n + (\frac{na_n}{t} + a_{n-1}')(\ln t)^{n-1} +$ terms of degree $\leq n-2$. Assume that $\ln t$ is algebraic over K. Let $p(x) = x^m + \sum_{j=1}^{m-1} b_j x^j$ is a minimal irreducible polynomial of $\ln t$ over K. Then $0 = (\ln t)^m + \sum_{j=1}^{m-1} b_j(\ln t)^j$. Differentiating it, we have $0 = (\frac{m}{t} + b_{m-1}')(\ln t)^{m-1} +$ terms of degree $\leq m-2$. So $\frac{m}{t} + b_{m-1}' = 0$ and $\frac{1}{t} = \frac{-b_{m-1}'}{m} = (\frac{-b_{m-1}}{m})'$. This is a contradiction that $\frac{1}{t}$ is not a derivative in $\mathbb{C}(t)$. Hence, $\ln t$ is transcendental in K. This implies that $a_n' = 0$ and $\frac{na_n}{t} + a_{n-1}' = 0$. So $\frac{1}{t} = \frac{-a_{n-1}'}{na_n} = (\frac{-a_{n-1}}{na_n})'$. This is a contradiction that $\frac{1}{t}$ is not a derivative in $\mathbb{C}(t)$. Assume that the rational function $\frac{g(\ln t)}{h(\ln t)}$, where $h(\ln t)$ is monic of the minimum degree ≥ 1, is a constant in $K\langle \ln t\rangle$. So $0 = \frac{\frac{1}{t}g'(\ln t)h(\ln t) - \frac{1}{t}g(\ln t)h'(\ln t)}{h^2(\ln t)}$. This implies that $\frac{g(\ln t)}{h(\ln t)} = \frac{g'(\ln t)}{h'(\ln t)}$. Since the polynomial h is not a constant in $K\langle \ln t\rangle$, h' has lower degree than h which is a contradiction. So adding $\ln t$ to $\mathbb{C}(t)$ does not create new constants. The*

Picard-Vessiot extension of $\mathcal{L}(Y) = Y'' + \frac{1}{t}Y = 0$ *is* $L = K\langle \ln t \rangle$.

Theorem 3.2.1 (see [19])**.** *Let* K *be a differential field with algebraically closed field of constants* C*, let* $\mathcal{L}(Y) = Y^n + a_{n-1}Y^{n-1} + \cdots + a_1Y' + a_0Y = 0$ *be defined over* K*. Then there exists a Picard-Vessiot extension* L *of* K *for* L *and it is unique up to differential* K*-isomorphism.*

3.3 Algebraic groups

Let C be an algebraically closed field of characteristic zero.

Definition 3.3.1. *An algebraic group over* C *is an algebraic variety* G *defined over* C *such that* $f : G \times G \to G$*,* $f(x, y) = xy$ *and* $g : G \to G$*,* $g(x) = x^{-1}$ *are morphisms of varieties.*

For example, the group $GL_n(C)$ of all invertible n by n matrices with entries in C and the group $SL_n(C)$ of all n by n matrices with entries in C and determinant being 1 are algebraic groups.

Propsition 3.3.1. *Let* $G_1, \ldots, G_m$ *be the distinct irreducible components of* G*. Then there is a unique irreducible component containing the identity of* G*. This irreducible component containing the identity is called the identity component of* G*, denoted by* G^0*.*

Definition 3.3.2. *If* $G = G^0$*, then* G *is said to be connected.*

For example, the algebraic group $SL_n(C)$ is connected.

3.4 Differential Galois groups

Definition 3.4.1. *Let* $K \subset L$ *be a field extension. Let*

$$\mathrm{Gal}(L|K) := \{\phi \in \mathrm{Aut}(L) |\ \phi|_K (K) = K\}$$

where $\mathrm{Aut}(L)$ *is the group of automorphisms of* L *over* K*. Then* $\mathrm{Gal}(L|K)$ *is called the Galois group of the extension* $K \subset L$*.*

The definition of the differential Galois group is an analogue of the classical Galois group, which is stated as follows.

Definition 3.4.2. *If* $K \subset L$ *is a differential field extension, the group* $G(L|K)$ *of differential* K*-automorphisms fixing* K *is called the differential Galois group of the extension* $K \subset L$*.*

Definition 3.4.3. *If* $K \subset L$ *is a Picard-Vessiot extension for* $\mathcal{L}(Y) = 0$*, the group* $G(L|K)$ *of differential* K*-automorphisms of* L *is the differential Galois group of* $\mathcal{L}(Y) = 0$*.*

In this thesis, we consider a linear differential equation in the matrix form:

$$\delta(Y) = AY$$

where Y is a vector containing n unknowns and A is an n by n matrix with entries in $K = k(t)$ where k is a computable algebraically closed field of characteristic zero.

Any n-th order linear differential equation $\mathcal{L}(y) = a_n y^n + a_{n-1} y^{n-1} + \cdots + a_1 y' + a_0 y = 0$ can be written in the matrix form $\delta(Y) = AY$ where

$$Y = \begin{pmatrix} y \\ y' \\ \vdots \\ y^{n-1} \end{pmatrix}, A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -\frac{a_0}{a_n} & -\frac{a_1}{a_n} & -\frac{a_2}{a_n} & \dots & -\frac{a_{n-1}}{a_n} \end{pmatrix}$$

.

Definition 3.4.4. *Let* K *be a field of characteristic zero and* $\delta(Y) = AY$ *be an* n*-th order*

linear differential equation with coefficients in K written in the matrix form, then

$$F = \begin{pmatrix} y_1 & y_2 & \dots & y_n \\ y_1' & y_2' & \dots & y_n' \\ \vdots & \vdots & \dots & \vdots \\ y_1^{n-1} & y_2^{n-1} & \dots & y_n^{n-1} \end{pmatrix}$$

is said to be a fundamental matrix of $Y' = AY$ if $\{y_1, y_2, \dots, y_n\}$ is a fundamental set of solutions of this n-th order linear differential equation.

Remark 7. *A fundamental set of solutions of an n-th order linear differential equation $\delta(Y) = AY$ with coefficients in K is a basis for an n-dimensional vector space over C where C is the field of constants of K. This n-dimensional vector space over C is called the solution space of $\delta(Y) = AY$.*

Example 3.4.1. *Consider the differential equation $\mathcal{L}(y) = y'' + \frac{1}{t}y' = 0$. It can be written in the matrix form*

$$\delta \begin{pmatrix} y \\ y' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & \frac{1}{t} \end{pmatrix} \begin{pmatrix} y \\ y' \end{pmatrix}.$$

$\{1, \ln t\}$ is a fundamental set of solutions and

$$F = \begin{pmatrix} 1 & \ln t \\ 0 & \frac{1}{t} \end{pmatrix}$$

is a fundamental matrix of this differential equation.

Example 3.4.2. *Consider the differential equation $\mathcal{L}(y) = y'' + y = 0$. It can be written in the matrix form*

$$\delta \begin{pmatrix} y \\ y' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y \\ y' \end{pmatrix}.$$

$\{\cos t, \sin t\}$ *is a fundamental set of solutions and*

$$F = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$$

is a fundamental matrix of this differential equation.

Let L be the Picard-Vessiot extention of the differential field K with the derivation $\delta = \frac{d}{dt}$ and V be the solution space of (1) in L. Let $F \in GL_n(L)$ 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: $GL(V) \to GL_n(k)$ sending $\sigma \in GL(V)$ to $M_\sigma \in GL_n(k)$ where $FM_\sigma = \sigma(F)$.

The differential Galois group of a linear differential equation of order n defined over the differential field K is isomorphic to a subgroup of the general linear group $GL_n(C)$ where C is the constant field K. Differential Galois groups can be viewed as linear algebraic groups [7, Proposition 4.1, page 23].

Example 3.4.3. *Let $K = \mathbb{C}(t)$ and $L = K\langle \ln t \rangle$ be the Picard-Vessiot extension of $\mathcal{L}(Y) = Y'' + \frac{1}{t}Y' = 0$. Let σ be a K-automorphism in the differential Galois group $\mathrm{Gal}\,(L|K)$ of $\mathcal{L}(Y) = 0$. Then σ must fix $Y = 1 \in \mathbb{C}$ and send $\ln t$ to $c_1 + c_2 \ln t$ for some c_1 and c_2 in $\mathbb{C}$. Since σ must commute with the derivation $d = \frac{d}{dt}$, in other words, $\sigma(d(\ln t)) = d(\sigma(\ln t))$, this implies that $\frac{1}{t} = \frac{c_2}{t}$. So $c_2 = 1$ and σ sends $\ln t$ to $c + \ln t$. Let $f : \mathrm{Gal}\,(L|K) \to \mathbb{C}$ be a map sending σ to c where $\sigma \in \mathrm{Gal}\,(L|K)$ such that $\sigma(\ln t) = c + \ln t$. Let $\sigma_1, \sigma_2 \in \mathrm{Gal}\,(L|K)$ such that $\sigma_1(\ln t) = c_1 + \ln t$ and $\sigma_2(\ln t) = c_2 + \ln t$. Then $\sigma_1\sigma_2(\ln t) = \sigma_1(c_2 + \ln t) = c_1 + c_2 + \ln t$. So $f(\sigma_1\sigma_2) = c_1 + c_2$. Since $f(\sigma_1) + f(\sigma_2) = c_1 + c_2$, $f(\sigma_1\sigma_2) = f(\sigma_1) + f(\sigma_2)$. So f is a group homomorphism. Let $\Phi : \mathbb{C}(t)[x_{11}, x_{12}, x_{21}, x_{22}] \to \mathbb{C}(t)[1, \ln t, 0, \frac{1}{t}]$ be substitution homomorphism , where $\{x_{11}, x_{12}, x_{21}, x_{22}\}$ is a set of indeterminates and $\{1, \ln t\}$ is a set of fundamental solutions of $\mathcal{L}(Y) = 0$. Let $S = \ker \Phi$. So $S = \{Q \in \mathbb{C}(t)[x_{11}, x_{12}, x_{21}, x_{22}] :$*

$Q(1, \ln t, 0, \frac{1}{t}) = 0\}$. *Assume that the coefficients of monomials containing* x_{12} *in* Q *are nonzero. Since* $Q(1, \ln t, 0, \frac{1}{t}) = 0$, *this implies that* $\ln t$ *is algebraic over* $\mathbb{C}(t)$ *which is a contradiction with the fact that* $\ln t$ *is transcendental over* $\mathbb{C}(t)$ *(see Example 3.2.2). So the coefficients of monomials containing* x_{12} *in* Q *are zero. By [5, Theorem 6.3.1, page 120],* $\mathrm{Gal}\,(L|K)$ *is isomorphic to* $G = \{g \in GL_2(\mathbb{C}) : Q(g(1, \ln t), g(1, \ln t)') = 0 \ \forall Q \in S\}$. *Any* $h = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{C})$ *sends* $(1, \ln t)$ *to* $(1, \ln t + c)$ *and* $h(1, \ln t)'$ *to* $(0, \frac{1}{t})$. *Then* $Q\big(h(1, \ln t), h(1, \ln t)'\big) = Q(1, \ln t + c, 0, \frac{1}{t})$. *Since the coefficients of monomials containing* x_{12} *in* Q *are zero,* $Q\big(h(1, \ln t), h(1, \ln t)'\big) = Q(1, \ln t + c, 0, \frac{1}{t}) = Q(1, \ln t, 0, \frac{1}{t}) = 0$. *So* $h \in G$. *Since any* $\sigma \in \mathrm{Gal}\,(L|K)$ *must send* 1 *to* 1 *and* $\ln t$ *to* $\ln t + c$, $\mathrm{Gal}\,(L|K)$ *is isomorphic to*

$$\left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbb{C} \right\} \subset GL_2(\mathbb{C}).$$

Since $\mathbb{C}$ *is isomorphic to*

$$\left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbb{C} \right\} \subset GL_2(\mathbb{C}),$$

the differential Galois group $\mathrm{Gal}\,(L|K)$ *of* $\mathcal{L}(Y) = 0$ *is isomorphic to the linear algebraic group* $\mathbb{C}$.

Example 3.4.4. *Let* $K = \mathbb{C}(t)$ *and* $L = K\langle \sin t, \cos t \rangle$ *be the Picard-Vessiot extension of* $\mathcal{L}(Y) = Y'' + Y = 0$. *Let* σ *be a* K*-automorphism in the differential Galois group* $\mathrm{Gal}\,(L|K)$ *of* $\mathcal{L}(Y) = 0$. *Then* σ *must send* $\sin t$ *to* $c_1 \sin t + c_2 \cos t$ *and* $\cos t$ *to* $c_3 \sin t + c_4 \cos t$ *for some* c_1, c_2, c_3, c_4 *in* $\mathbb{C}$. *Since* σ *must commute with the derivation* $d = \frac{d}{dt}$, *in other words,* $\sigma\big(d(\sin t)\big) = d\big(\sigma(\sin t)\big)$ *and* $\sigma\big(d(\cos t)\big) = d\big(\sigma(\cos t)\big)$, *this implies that* $c_3 \sin t + c_4 \cos t = c_1 \cos t - c_2 \sin t$ *and* $-c_1 \sin t - c_2 \cos t = c_3 \cos t - c_4 \sin t$. *So* $c_1 = c_4$ *and* $c_2 = -c_3$. *Since*

$\sin^2 t + \cos^2 t = 1$, *applying* σ, *we have* $c_1^2 + c_2^2 = 1$. *Let*

$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2 = 1 \right\} \subset GL_2(\mathbb{C})$$

Let $f : \mathrm{Gal}\,(L|K) \to G$ *be a map sending* σ *to* $g = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$ *where* $\sigma \in \mathrm{Gal}\,(L|K)$ *such that* $\sigma(\sin t, \cos t) = (\sin t, \cos t) \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. *Let* $\sigma_1, \sigma_2 \in \mathrm{Gal}\,(L|K)$ *such that* $\sigma_1(\sin t, \cos t) = (\sin t, \cos t) \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}$ *and* $\sigma_2(\sin t, \cos t) = (\sin t, \cos t) \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$. *Then*

$$\sigma_1\sigma_2(\sin t, \cos t) = (\sin t, \cos t) \begin{pmatrix} a_1a_2 - b_1b_2 & a_2b_1 + a_1b_2 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_2b_2 \end{pmatrix}$$

and

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_2b_1 + a_1b_2 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_2b_2 \end{pmatrix}.$$

So f *is a group homomorphism. Let* $\Phi : \mathbb{C}(t)[x_{11}, x_{12}, x_{21}, x_{22}] \to \mathbb{C}(t)[\sin t, \cos t, \sin t', \cos t']$ *be substitution homomorphism , where* $\{x_{11}, x_{12}, x_{21}, x_{22}\}$ *is a set of indeterminates and* $\{\sin t, \cos t\}$ *is a set of fundamental solutions of* $\mathcal{L}(Y) = 0$. *Let* $S = \ker \Phi$. *So* $S = \{Q \in \mathbb{C}(t)[x_{11}, x_{12}, x_{21}, x_{22}] : Q(\sin t, \cos t, \sin t', \cos t') = 0\}$. *Since* $\sin^2 t + \cos^2 t = 1$, *if* Q *has a factor* $x_{11}^2 + x_{12}^2 - 1$ *or* $x_{21}^2 + x_{22}^2 - 1$ *or* $x_{11}^2 + x_{21}^2 - 1$ *or* $x_{12}^2 + x_{22}^2 - 1$, *then for any* $h = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in GL_2(\mathbb{C})$ *with* $a^2 + b^2 = 1$ *sends* $(\sin t, \cos t)$ *to* $(a \sin t + b \cos t, -b \sin t + a \cos t)$, $Q\big(h(\sin t, \cos t), h(\sin t, \cos t)'\big) = Q(a \sin t + b \cos t, -b \sin t + a \cos t, a \cos t - b \sin t, -b \cos t - a \sin t) = 0$. *If* Q *has no such factors, because* $Q(\sin t, \cos t, \cos t, -\sin t) = 0$, *we have*

$Q(x_{11}, x_{12}, x_{12}, -x_{11}) = 0$. *Otherwise,* $\sin t, \cos t$ *would be algebraic over* $\mathbb{C}(t)$ *which is a contradiction with the fact that* $\sin t, \cos t$ *are transcendental over* $\mathbb{C}(t)$. $\sin t, \cos t$ *are transcendental over* $\mathbb{C}(t)$ *because* e^{it} *is transcendental over* $\mathbb{C}(t)$ *(see Example 3.2.1) and* $\sin t = \frac{-ie^{it}+ie^{-it}}{2}, \cos t = \frac{e^{it}+e^{-it}}{2}$. *So for any* $h = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in GL_2(\mathbb{C})$ *with* $a^2 + b^2 = 1$,

$$Q(h(\sin t, \cos t), h(\sin t, \cos t)') = Q(a\sin t + b\cos t, -b\sin t + a\cos t, a\cos t - b\sin t, -b\cos t - a\sin t) = 0$$

because $a\sin t + b\cos t = -(-b\cos t - a\sin t)$ *and* $-b\sin t + a\cos t = a\cos t - b\sin t$. *By [5, Theorem 6.3.1, page 120],* $\mathrm{Gal}\,(L|K)$ *is isomorphic to*

$$G = \{g \in GL_2(\mathbb{C}) : Q(g(\sin t, \cos t), g(\sin t, \cos t)') = 0 \forall Q \in S\}$$

. *So* $h \in G$. *Since any* $\sigma \in \mathrm{Gal}\,(L|K)$ *must send* $\sin t$ *to* $a\sin t + b\cos t$ *and* $\cos t$ *to* $-b\sin t + a\cos t$ *with* $a^2 + b^2 = 1$, $\mathrm{Gal}\,(L|K)$ *is isomorphic to*

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2 = 1 \right\} \subset GL_2(\mathbb{C}).$$

3.5 Liouville extensions

Definition 3.5.1. *A differential field extension* $K \subset L$ *is called a Liouville extension if there exists a chain of intermediate differential fields* $K = K_1 \subset K_2 \subset \cdots \subset K_n = L$ *such that* $K_{i+1} = K_i\langle\alpha_i\rangle$, *where*

- α_i *is algebraic over* K_i
- $\alpha_i' \in K_i$ *(*α_i *is called a primitive element over* K_i*)*

- *or* $\alpha_i'/\alpha_i \in K_i$ *(*α_i *is called an exponential element over* K_i*).*

Definition 3.5.2. *An algebraic group* G *is solvable if there is a chain of closed subgroups* $1 = G_0 \subset G_1 \subset \cdots \subset G_n = G$ *such that* G_i *is normal in* G_{i+1} *and* G_{i+1}/G_i *is abelian* $\forall$ $0 \leq i \leq n-1$.

Propsition 3.5.1. *Let* $K \subset L$ *be a Liouville extension of the differential field* K*. Suppose that the field of constants of* L *is the same as that of* K*. Then the differential Galois group* $\mathrm{Gal}\,(L|K)$ *is solvable.*

Definition 3.5.3. *Consider a linear differential equation* $\mathcal{L}(Y) = 0$ *over* K*. A solution* $y \in K$ *is called Liouvillian if*

- y *is algebraic over* K
- y *is the integral of an element in* K
- y *is the exponential of an element in* K

Theorem 3.5.1. *Consider a linear differential equation* $\mathcal{L}(Y) = 0$ *over* K*. Let* L *be the Picard-Vessiot field for* $\mathcal{L}(Y) = 0$ *over* K*.* $\mathcal{L}(Y) = 0$ *is solvable by Liouvillian functions if and only if the identity component of* $\mathrm{Gal}\,(L|K)$ *is solvable.*

Chapter 4

Complexity of Hrushovski's Algorithm

4.1 Introduction

The complexity of computing the Galois group of a linear differential equation is of general interest. 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. 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.

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 and is quintuply exponential in the order of the differential equation. 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.

4.2 Preliminaries

We consider a linear differential equation in the matrix form:

$$\delta(Y) = AY \tag{1}$$

where Y is a vector containing n unknowns and A is an nn matrix with entries in $k(t)$. Denote the Picard-Vessiot extention 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: $GL(V) \to GL_n(k)$ sending $\sigma \in GL(V)$ to $M_\sigma \in GL_n(k)$ where $FM_\sigma = \sigma(F)$.

Definition 4.2.1. *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 4.2.2. *An algebraic subgroup H of $GL_n(k)$ is bounded by d if there exist finitely many polynomials $p_1, \ldots, p_m \in k[x_{i,j}]_{1<i,j<n}$ of degrees not greater than d such that $H =$ zero $(p_1, \ldots, p_m) \cap GL_n(k)$.*

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 [10], which is as follows:

Definition 4.2.3 ([10, 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 [10].

Example 4.2.1. *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 [29, 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 4.2.2. *Consider the Airy equation $y'' = ty$ over $\mathbb{C}(t)$. The differential Galois group is the subgroup $SL_2(\mathbb{C}) \subseteq GL_2(\mathbb{C})$ [35, 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 4.2.3, it is not hard to see the differential Galois group itself is a proto-Galois group.*

Example 4.2.3. *Consider the second order linear differential equation $y'' + \frac{1}{t}y' = 0$ over $\mathbb{C}(t)$. The differential Galois group is*

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

[7, Example 4.1, page 90]. The same analysis in Example 4.2.2 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 4.2.4. *Consider the second order linear differential equation $y'' - 2ty' - 2y = 0$ over $\mathbb{C}(t)$. The differential Galois group is*

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

[25, Example 6.10, pages 81,82,83]. The same analysis in Example 4.2.3 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 8. *The proto-Galois group of a linear differential equation is not unique. As shown in Examples 4.2.1 and 4.2.2, 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 4.2.3 and 4.2.4.*

Hrushovski in [14, 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 [10, Propostion 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 [10] described it.

Definition 4.2.4. *Let $\tilde{V} = \{Fh : h \in GL_n(k)\}$. A subset V_0 of $\tilde{V}$ is defined by finitely many polynomials $p_1, \ldots, p_m$ if $V_0 = \text{zero}\,(p_1, \ldots, p_m) \cap \tilde{V}$ where $\text{zero}\,(p_1, \ldots, p_m)$ denotes the zero set of $\{p_1, \ldots, p_m\}$ in k^{nn}. If $p_1, \ldots, p_m$ 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 [14, 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 $\big(\Phi_F(\mathcal{G})\big)^0$. Let $\hat{k}$ be an algebraic extension of $k(t)$. Then $\chi\big(\Phi_F(\mathcal{G})^0\big)$ 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). $\big(\Phi_F(\mathcal{G})\big)^0$ can be found by the pre-image of $\chi\big(\Phi_F(\mathcal{G})^0\big)$ in $\big(\Phi_F(\mathcal{H})\big)^0$.

- In the last step, we compute the differential Galois group $\mathcal{G}$ of (1). Let $\mathcal{G}^0$ be the pre-image of $\big(\Phi_F(\mathcal{G})\big)^0$. Find a Galois extension k_G of $k(t)$ and a k_G-definable subset V_{k_G} of $\tilde{V}$ such that $\mathcal{G}^0 = \text{stab}\,(V_{k_G})$ where $\text{stab}\,(V_{k_G})$ is the stabilizer of V_{k_G}. Then

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

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

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.

4.3 Preparation lemmas

Definition 4.3.1. *We say that an ideal $I \subseteq k[x_1, \ldots, x_n]$ has a triangular representation if $\sqrt{I}$ is expressed by an intersection of radical ideals I_i such that for each i, $I_i = \mathrm{rep}\,(G_i)$ 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 4.3.2. *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 $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. In [10, Proposition B.2], Feng gave a degree bound for $I \cap k[x_1, \ldots, x_r]$ 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 $I \cap k[x_1, \ldots, x_r]$ which is polynomial exponential in n.

Lemma 4.3.1. *Assume that $n > 1$. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal bounded by d and $1 \leq r \leq n$. Then $I \cap k[x_1, \ldots, x_r]$ has a triangular representation bounded by $nd^{5.5n^3}$.*

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

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

it suffices to show that for each i

$$\mathrm{rep}\left(G_i \cap k[x_1, \ldots, x_n]\right) \cap k[x_1, \ldots, x_r] = \mathrm{rep}\,(G_i) \cap k[x_1, \ldots, x_r] \tag{2}$$

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

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

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

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

So $\text{prem}\,(g, G_i) = 0$. If $G_i \not\subseteq k[x_1, \ldots, x_r]$, then G_i must have at least one polynomial containing terms larger than x_r. Let $G_i = \{g_{i,1}, \ldots, g_{i,s}\}$ and assume that $g_{i,j+1}, \ldots, g_{i,s}$ contain terms larger than x_r. Then

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

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

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

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

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

where

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

where rep $\big(G_i \cap k[x_1, \ldots, x_r]\big)$ is an ideal in $k[x_1, \ldots, x_r]$. By [33, Theorem 4.1.7], the trian-

gular representation of $I \cap k[x_1, \ldots, x_r]$ is bounded by $nd^{5.5n^3}$. □

Lemma 4.3.2. *Let $I, J \subseteq k[x_1, \ldots, x_n]$ 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 $\sqrt{I} = \bigcap_i I_i$ and $\sqrt{J} = \bigcap_j J_j$ are triangular representations of I and J. Then $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J} = \big(\bigcap I_i\big) \cap \big(\bigcap J_j\big)$. So if $I_i = \mathrm{rep}\,(G^{I_i})$ and $J_j = \mathrm{rep}\,(G^{J_j})$ for some triangular sets G^{I_i} and G^{J_j}, then $\sqrt{IJ} = \big(\bigcap \mathrm{rep}\,\big(G^{I_i}\big)\big) \cap \big(\bigcap \mathrm{rep}\,(G^{J_j})\big)$. Therefore, IJ has a triangular representation bounded by d. □

Definition 4.3.3. *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 $\tau : H \longrightarrow GL_l(k)$ 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 $1 \leq i, j \leq l$. 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 [10, Lemma B.5], Feng gave a degree bound for the generating set of the ideal generated by the defining equations of $\tau^{-1}\big(H' \cap \tau(H)\big)$ 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 $\tau^{-1}\big(H' \cap \tau(H)\big)$.

Lemma 4.3.3. *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 $\tau : H \longrightarrow GL_l(k)$ is bounded by m. Then $\tau^{-1}\big(H' \cap \tau(H)\big)$ has a triangular representation bounded by $n\big(\max(d, md')\big)^{5.5n^3}$.*

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 $x_{\alpha,\beta}$, $1 \leq$

$\alpha, \beta \leq n$ and Y be the set of indeterminates $y_{\zeta,\eta}$, $1 \leq \zeta, \eta \leq l$. Assume that $\tau = (\frac{P_{i,j}}{Q})_{1\leq i,j\leq l}$ where $P_{i,j}$ and Q are polynomials in $k[X]$. Assume that H has a triangular representation

$$\sqrt{I(H)} = \bigcap_r \mathrm{rep}\,(G_r)$$

and H' has a triangular representation

$$\sqrt{I(H')} = \bigcap_w \mathrm{rep}\,(F_w),$$

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 [31, Proposition 6]) which guarantee $\mathrm{zero}\,(\bigcup_w F_w) = H'$ and $\mathrm{zero}\,(\bigcup_r G_r) = H$. A subroutine called **unmixed** can transform a triangular set to an unmixed one (see [33, Section 4.2] for more details). Since $\mathrm{zero}\,(\bigcup_w F_w) = H'$, 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 $\mathrm{zero}\,(\bigcup_w E_w) = \tau^{-1}(H')$. Since $\mathrm{zero}\,(\bigcup_r G_r) = H$, $\mathrm{zero}\,\big((\bigcup_r G_r) \cup (\bigcup_w E_w)\big) = \tau^{-1}\big(H' \cap \tau(H)\big)$. Let J be the ideal generated by $\big((\bigcup_r G_r) \cup (\bigcup_w E_w)\big)$. Thus, $\mathrm{zero}\,(J) = \tau^{-1}\big(H' \cap \tau(H)\big)$. 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 [33, Theorem 4.1.7], J has a triangular representation bounded by $n\big(\max(d, md')\big)^{5.5n^3}$. That is, $\tau^{-1}\big(H' \cap \tau(H)\big)$ has a triangular representation bounded by $n\big(\max(d, md')\big)^{5.5n^3}$. □

In [10, 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 [10, Proposition B.6].

Lemma 4.3.4. *Assume that $n > 1$. Let H and H' be algebraic subgroups of $GL_n(k)$ such that $H \trianglelefteq H'$. Assume that H has a triangular representation bounded by d. Then there exists a homomorphism*

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

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

Proof. The existence of such a homomorphism is guaranteed by [16, 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 $\binom{n^2+d}{d}$, $\dim_k(E) = \binom{\binom{n^2+d}{d}}{l}$ 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 [10, 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 [10, 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 4.3.5. *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 [16, Lemma C, page 96], any one-dimensional subgroup H generated by unipotent

elements of $GL_n(k)$ has the form

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

where $M \in \mathrm{Mat}_n(k)$ with $M^n = 0$. By [16, 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 $H_i = \{I_n + M_i x_i + \frac{M_i^2}{2!}x_i^2 + \cdots + \frac{M_i^{n-1}}{(n-1)!}x_i^{n-1} : x_i \in \mathbb{C}\}$ is a one-dimensional subgroup generated by unipotent elements of $GL_n(k)$ and $M_i \in \mathrm{Mat}_n(k)$ 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 4.3.1, the ideal generated by the defining equations of U has a triangular representation bounded by

$$3n^2\big(2n^2(n-1)\big)^{5.5(3n^2)^3} = 3n^2\big(2n^2(n-1)\big)^{148.5n^6}. \qquad \square$$

Jordan in [18] 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 [28] provided an explicit bound which is

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

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

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

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

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

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

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

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

and

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

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

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

$$
\begin{aligned}
d_3 \leq & n\Big(3n^2 18^{n^2}(2n^3)^{148.5n^8+148.5n^6}4^{(2n^3)^{149n^8}}\big(16^{(2n^3)^{149n^8}}+1\big)4^{\left(16^{(2n^3)^{149n^8}}+1\right)}\Big)^{5.5n^3}\\
\leq & n\Big((2n^3)^{149n^8+149n^6}4^{(2n^3)^{149n^8}}\big(16^{(2n^3)^{149n^8}}+1\big)4^{\left(16^{(2n^3)^{149n^8}}+1\right)}\Big)^{5.5n^3}\\
\leq & n\Big(2(2n^3)^{149n^8+149n^6}4^{(2n^3)^{149n^8}}16^{(2n^3)^{149n^8}}4^{\left(16^{(2n^3)^{149n^8}}+1\right)}\Big)^{5.5n^3}\\
\leq & n\Big(8(2n^3)^{149n^8+149n^6}4^{(2n^3)^{149n^8}}16^{(2n^3)^{149n^8}}4^{16^{(2n^3)^{149n^8}}}\Big)^{5.5n^3}\\
\leq & n\big(8^{16^{(2n^3)^{149n^8}}}\big)^{5.5n^3} = n8^{5.5n^3 16^{(2n^3)^{149n^8}}},
\end{aligned}
$$

and

$$
\begin{aligned}
\bar{d} \leq & \big(\sqrt{8\cdot 4^{d_1^2+1}}+1\big)^{2n^2}-\big(\sqrt{8\cdot 4^{d_1^2+1}}-1\big)^{2n^2}\\
\leq & \big(\sqrt{32}\cdot 2^{8^{(2n^3)^{149n^8}}}+1\big)^{2n^2}-\big(\sqrt{32}\cdot 2^{8^{(2n^3)^{149n^8}}}-1\big)^{2n^2}\\
\leq & \big(2\sqrt{32}\cdot 2^{8^{(2n^3)^{149n^8}}}\big)^{2n^2} = 2^{10n^2}4^{n^2}8^{(2n^3)^{149n^8}}
\end{aligned}
$$

where $n > 1$.

4.4 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 [10, 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 4.4.1. *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 4.3.4, there is a homomorphism

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

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 contained 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

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

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

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

We can choose $\bar{d} = J(n') = J\big(\max_i \big\{ \binom{n^2+1}{i}^2 \big\}\big)$. This proves (c). Let $h \in H$ be a unipotent 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 4.3.3, 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 [10, Lemma B.10]. By Lemma 4.3.5, H'_u has a triangular representation bounded by D. Let N be the normalizer of H'_u in $GL_n(k)$. By Lemma 4.3.4, there exists a homomorphism

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

bounded by

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

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

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

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

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

By Lemma 4.3.3, H has a triangular representation bounded by

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

By a similar argument in the proof of [10, 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

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

Corollary 4.4.1. *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 $\bar{\mathcal{F}} = \{\bar{H} : \text{ there exists } H \in \mathcal{F} \text{ such that } H \trianglelefteq \bar{H} \text{ and } [\bar{H} : H] \leq \bar{d}\}$. Let $H' \subseteq GL_n(k)$ be an algebraic subgroup. By Theorem 4.4.1, 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 4.4.1, $\bar{H} \in \bar{\mathcal{F}}$. By (d) in Theorem 4.4.1, 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 4.3.2, 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 $d_3 \leq n8^{5.5n^3 16^{(2n^3)149n^8}}$. □

Corollary 4.4.2. *Let $\bar{\mathcal{F}}$ be the family in Corollary 4.4.1. Then for any algebraic subgroup $H' \subseteq GL_n(k)$, there exists $\bar{H}$ of $\bar{\mathcal{F}}$ such that*

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

Proof. By Corollary 4.4.1, 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 $GL_n(k)$, $(\bar{H}^\circ)^t$ is generated by all unipotent elements in $\bar{H}^\circ$ by [10, Lemma B.10]. Since $(\bar{H}^\circ)^t \trianglelefteq \bar{H}^\circ$ and every unipotent element in $\bar{H}^\circ$ is in $(H')^\circ$, $(H^\circ)^t \trianglelefteq (H')^\circ$. Therefore, $(\bar{H}^\circ)^t \trianglelefteq (H')^\circ \subseteq H' \subseteq \bar{H}$. □

Remark 9. *Since the differential Galois group of* (1) *is an algebraic subgroup in $GL_n(k)$,*

by Corollary 4.4.2, there exists an algebraic subgroup $\bar{H}$ bounded by d_3 such that $(\bar{H}^\circ)^t \trianglelefteq (H')^\circ \subseteq H' \subseteq \bar{H}$. By the definition of the proto-Galois group, this algebraic subgroup $\bar{H}$ is a proto-Galois group of (1).

4.5 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 4.4.1 and Corollary 4.4.1 to do calculations, which would give us more refined bounds. Feng in [10] 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 [10], we also give numerical bounds in [10, Proposition 11, Proposition 14]. In [10, 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:

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

When $n = 2$,

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

and

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

Appendix

Appendix

The following results on matrix representations of pseudoremainders are used in Section 2.4. They are mentioned and used in [33, Section 3.3]. We include here a shortened and refined version of them.

Let $f \in k[x_1, x_2, \ldots, x_l], g \in k[x_1, x_2, \ldots, x_n]$ with k a field and $l \geq n$. We wish to describe the pseudoremainder of f by g with respect to x_n in matrix form. More specifically, we wish to describe this pseudoremainder when $\deg_{x_n}(g) = d$ and $\deg_{x_n}(f) \leq 2d-2$, (the application in mind being computing the structure constants for $A(\Delta)$, see Definition 2.2.8). We will allow the degree of f to go up to $2d-1$ in fact. We first write f and g as univariate polynomials in x_n with coefficients $k[x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_l]$:

$$f = f_0 + f_1 x_n + \cdots + f_{2d-1} x_n^{2d-1}, \quad g = g_0 + g_1 x_n + \cdots + g_d x_n^d.$$

Note that the difference between the degrees in x_n of f and g is $d-1$. Thus, the pseudoremainder equation we consider (in scalar form) is $g_d^d f = gq + r$ where the degrees in x_n of r, q are less than d. Writing q and r as we wrote f, g above and substituting these expressions

into the pseudoremainder equation, we obtain:

$$g_d^d(f_0 + \ldots + f_{2d-1}x_n^{2d-1}) = (g_0 + \ldots + g_d x_n^d)(q_0 + \ldots + q_{d-1}x_n^{d-1}) + r_0 + \ldots + r_{d-1}x_n^{d-1}.$$

Comparing coefficients of the powers of x_n from d to $2d-1$, we obtain the following linear system

$$\begin{pmatrix} g_d & 0 & 0 & \ldots & 0 \\ g_{d-1} & g_d & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ g_1 & g_2 & \ldots & \ldots & g_d \end{pmatrix} \begin{pmatrix} q_{d-1} \\ q_{d-2} \\ \ldots \\ q_0 \end{pmatrix} = \begin{pmatrix} f_{2d-1} \\ f_{2d-2} \\ \ldots \\ f_d \end{pmatrix} g_d^d.$$

We write the system above as $G_d\mathbf{q} = \mathbf{f}^{\text{up}}g_d^d$. Since $g_d \neq 0$ (as g is assumed to have degree d in x_n), we can find the coefficients of the desired quotient by inverting G_d.

Since $r = g_d^d f - qg$, after substituting we obtain one more linear system

$$\begin{pmatrix} r_{d-1} \\ r_{d-2} \\ \ldots \\ r_0 \end{pmatrix} = g_d^d \begin{pmatrix} f_{d-1} \\ f_{d-2} \\ \ldots \\ f_0 \end{pmatrix} - \begin{pmatrix} g_0 & g_1 & \ldots & \ldots & g_{d-1} \\ 0 & g_0 & g_1 & \ldots & g_{d-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & g_0 \end{pmatrix} \begin{pmatrix} q_{d-1} \\ q_{d-2} \\ \ldots \\ q_0 \end{pmatrix}.$$

We write this system as $\mathbf{r} = g_d^d\mathbf{f}^{\text{low}} - G_0\mathbf{q}$. Combining with the equation for $\mathbf{q}$, we obtain

$$\mathbf{r} = g_d^d\mathbf{f}^{\text{low}} - g_d^d G_0 G_d^{-1}\mathbf{f}^{\text{up}}.$$

To count multiplications in the formula for the pseudoremainder, we re-express G_d^{-1} using Cramer's Rule: $G_d^{-1} = g_d^{-d} \cdot \text{adj}(G_d)$ where $\text{adj}(G_d)$ denotes the adjugate of G_d, (i.e. its matrix of cofactors transposed). So we have $\mathbf{r} = g_d^d\mathbf{f}^{\text{low}} - G_0 \cdot \text{adj}(G_d)\mathbf{f}^{\text{up}}$.

Observe that the entries of $\text{adj}(G_d)$ are sums of products of $d-1$ entries of G_d.

Bibliography

[1] P. Alvandi, C. Chen, S. Marcus, M. M. Maza, É. Schost, and P. Vrbik. Doing algebraic geometry with the RegularChains library. In H. Hong and C. Yap, editors, *Mathematical Software – ICMS 2014*, pages 472–479. Springer Berlin Heidelberg, 2014.

[2] E. Amzallag, G. Pogudin, M. Sun, and N. T. Vo. Complexity of triangular representations of algebraic sets. *Preprint*, 2016. URL `https://arxiv.org/abs/1609.09824`.

[3] P. Bürgisser and P. Scheiblechner. On the complexity of counting components of algebraic varieties. *Journal of Symbolic Computation*, 44(9):1114 – 1136, 2009.

[4] A. Chistov. Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal. *St. Petersbg. Math. J.*, 20(6):983–1001, 2009.

[5] R. C. Churchill and J. J. Kovacic. Introduction to differential Galois theory. In *Kolchin Seminar in Differential Algebra, Posted Papers*. Citeseer, 2006.

[6] E. Compoint and M. F. Singer. Computing Galois groups of completely reducible differential equations. *Journal of Symbolic Computation*, 28(4-5):473–494, 1999. URL `https://dx.doi.org/10.1006/jsco.1999.0311`.

[7] T. Crespo, Z. Hajto, and J. J. M. Ruiz. *Introduction to differential Galois theory*. Wydawnictwo PK, Cracow, Poland, 2007.

[8] X. Dahan, M. Moreno Maza, E. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM, New York, 2005.

[9] X. Dahan and E. Schost. Sharp estimates for triangular sets. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, pages 103–110, New York, NY, USA, 2004. ACM.

[10] R. Feng. Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Advances in Applied Mathematics*, 65:1–37, 2015. URL `http://dx.doi.org/10.1016/j.aam.2015.01.001`.

[11] G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Effective methods in algebraic geometry*, pages 119–142. Springer, 1991.

[12] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[13] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239 – 277, 1983.

[14] E. Hrushovski. Computing the Galois group of a linear differential equation. *Banach Center Publications*, 58(1):97–138, 2002. URL `https://dx.doi.org/10.4064/bc58-0-9`.

[15] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems. In *Proceedings of the 2nd International Conference on Symbolic and Numerical Scientific Computation*, SNSC'01, pages 1–39, Berlin, Heidelberg, 2003. Springer-Verlag.

[16] J. E. Humphreys. *Linear Algebraic Groups*. Springer-Verlag, New York, 1975. URL `http://dx.doi.org/10.1007/978-1-4684-9443-3`.

[17] G. Jeronimo and J. Sabia. Effective equidimensional decomposition of affine varieties. *Journal of Pure and Applied Algebra*, 169(2):229 – 248, 2002.

[18] C. Jordan. Mmoire sur les quations diffrentielles linaires intgrale algbriques. *Journal fr die reine und angewandte Mathematik*, 84:89–215, 1877. URL `http://eudml.org/doc/148348`.

[19] E. R. Kolchin. Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Annals of Mathematics*, 49(1):1–42, 1948. URL `https://dx.doi.org/10.2307/1969111`.

[20] E. R. Kolchin. Algebraic groups and algebraic dependence. *American Journal of Mathematics*, 90(4):1151–1164, 1968. URL `https://dx.doi.org/10.2307/2373294`.

[21] J. J. Kovacic. An algorithm for solving second order linear homogeneous differential equations. *Journal of Symbolic Computation*, 2(1):3–43, 1986. URL `https://dx.doi.org/10.1016/s0747-7171(86)80010-4`.

[22] S. Laplagne. An algorithm for the computation of the radical of an ideal. In *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, ISSAC '06, pages 191–195, New York, NY, USA, 2006. ACM.

[23] G. Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, pages 209–216, 2000.

[24] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4):564 – 596, 2003.

[25] A. R. Magid. *Lectures on Differential Galois Theory*. American Mathematical Society, 1994. URL `https://doi.org/10.1090/ulect/007`.

[26] A. Ovchinnikov, G. Pogudin, and N. T. Vo. Effective differential elimination. Submitted., 2016.

[27] E. Schost. Complexity results for triangular sets. *Journal of Symbolic Computation*, 36(34):555 – 594, 2003. ISSAC 2002.

[28] I. Schur. Über gruppen periodischer substitutionen. *Sitzber. Preuss. Akad. Wiss*, pages 619–627, 1911.

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

[30] M. F. Singer and F. Ulmer. Galois groups of second and third order linear differential equations. *Journal of Symbolic Computation*, 16(1):9–36, 1993. URL `https://dx.doi.org/10.1006/jsco.1993.1032`.

[31] Á. Szántó. Complexity of the Wu-Ritt decomposition. *Proceedings of the Second International Symposium on Parallel Symbolic Computation*, pages 139–149, 1997. URL `https://dx.doi.org/10.1145/266670.266716`.

[32] A. Szántó. Complexity of the Wu-Ritt decomposition. In *Second international symposium on parallel symbolic computation, PASCO '97, Maui, HI, USA, July 20–22*, pages 139–149. New York, NY: ACM Press, 1997.

[33] A. Szántó. *Computation with polynomial systems*. PhD thesis, Cornell University, 1999.

[34] J. van der Hoeven. Around the numeric–symbolic computation of differential Galois groups. *Journal of Symbolic Computation*, 42(1-2):236–264, 2007. URL `https://dx.doi.org/10.1016/j.jsc.2006.03.007`.

[35] M. van der Put and M. F. Singer. *Galois theory of linear differential equations*. Springer-Verlag, Berlin, 2003. URL `https://dx.doi.org/10.1007/978-3-642-55750-7`.

[36] D. Wang. Epsilon: A library of software tools for polynomial elimination. In *Mathematical Software*, pages 379–389. World Scientific, 2002.