9-2018

Galois Groups of Differential Equations and Representing Algebraic Sets

Eli Amzallag

The Graduate Center, City University of New York

How does access to this work benefit you? Let us know!

Follow this and additional works at: https://academicworks.cuny.edu(gc_etds

Part of the Algebra Commons, Algebraic Geometry Commons, and the Ordinary Differential Equations and Applied Dynamics Commons

Recommended Citation

https://academicworks.cuny.edu/gc_etds/2860

This Dissertation is brought to you by CUNY Academic Works. It has been accepted for inclusion in All Dissertations, Theses, and Capstone Projects by an authorized administrator of CUNY Academic Works. For more information, please contact deposit@gc.cuny.edu.
Galois Groups of Differential Equations
and Representing Algebraic Sets

by

Eli Amzallag

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.

2018
This 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.

(required signature)

Date Alexey Ovchinnikov
Chair of Examining Committee

(required signature)

Date Ara Basmajian
Executive Officer

Alexey Ovchinnikov

Vladimír Shpilrain

Benjamin Steinberg

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK
Abstract

Galois Groups of Differential Equations and Representing Algebraic Sets

by

Eli Amzallag

Advisor: Alexey Ovchinnikov

The algebraic framework for capturing properties of solution sets of differential equations was formally introduced by Ritt and Kolchin. As a parallel to the classical Galois groups of polynomial equations, they devised the notion of a differential Galois group for a linear differential equation. Just as solvability of a polynomial equation by radicals is linked to the equation’s Galois group, so too is the ability to express the solution to a linear differential equation in “closed form” linked to the equation’s differential Galois group. It is thus useful even outside of mathematics to be able to compute and represent these differential Galois groups, which can be realized as linear algebraic groups; indeed, many algorithms have been written for this purpose. The most general of these is Hrushovski’s algorithm and so its complexity is of great interest. A key step of the algorithm is the computation of a group called a proto-Galois group, which contains the differential Galois group. As a proto-Galois group
is an algebraic set and there are various ways to represent an algebraic set, a natural matter to investigate in this regard is which representation(s) are expected to be the “smallest.”

Some typical representations of algebraic sets are equations (that have the given algebraic set as their common solutions) and, for the corresponding radical ideal, Groebner bases or triangular sets. In computing any of these representations, it can be helpful to have a degree bound on the polynomials they will feature based on the given differential equation. Feng gave such a bound for a Groebner basis for a proto-Galois group’s radical ideal in terms of the size of the coefficient matrix. We first discuss an improvement of this bound achieved by focusing on equations that define such a group instead of its corresponding ideal. This bound also produces a smaller degree bound for Groebner bases than the one Feng obtained. Recent work by M. Sun shows that Feng’s bound can also be improved by replacing Feng’s uses of Groebner bases by triangular sets. Sun’s bound relies on results on the complexity of triangular representations of algebraic sets, results that we shall present and that more generally suggest using triangular sets in place of Groebner bases to potentially reduce complexity.
Acknowledgements

I thank my advisor Alexey Ovchinnikov for introducing me to the field of differential algebra, supervising my oral exam and dissertation, and providing me with constructive and useful career advice, including career workshops and recommendations on which conferences to attend and present at. I thank my research collaborators Richard Gustavson, Andrei Minchenko, Gleb Pogudin, Mengxiao Sun, and Ngoc Thieu Vo. Gleb, Thieu, and Richard have especially provided me with much of their time to discuss research and I owe a great deal of my understanding of how research mathematicians think to them.

I also thank the following people, who all helped me develop my mathematical skills in one fashion or another:

- Graduate Center Faculty and Staff: M. Bendersky, A. Champanerkar, J. Dodziuk, Z. Huang, D. Kebabiae, R. Kossak, R. Landsman, R. Miller, M. Nathanson, V. Pan, R. Parikh, M.H. Reis, M. Sabitova, D. Saric, H. Schoutens, D. Silverman, S. Zakeri

• Kolchin Seminar: P. Cassidy, R. Churchill, A. Medvedev, R. Nagloo, W. Sit


• City College (CCNY): E. Akin, A. Amarasingham, M. Auth, J. Bak, G. Chinta, S. Cleary, B. Feigon, P. Hooper, J. Jorgenson, H. Jue, R. Kopperman, S. Merenkov, S. Ocken, C.S. Park, T. Pignataro, L. Rawlings, J. Redman, R. Ring, B. Santoro, V. Shpilrain, M. Shub, B. Steinberg, C. Wolf

• Family: Danny, Margie, Kathy, Diane, Allen, Abe, Rachel B., Rachel G., Ilya, David, Danielle, Andy, Bella, Becky, Jenny, Vicky, Robert

• Also: R. Basak, S. Brodetskiy, L. Espina
Contents

Introduction 1

1 Differential Galois Groups 3
   1.1 Differential Rings and Fields 3
   1.2 Matrix Differential Equations 4
   1.3 Differential Automorphisms 5
   1.4 Liouville Extensions 8

2 Computing Differential Galois Groups 10
   2.1 Known Algorithms 10
   2.2 Proto-Galois Groups 12
   2.3 Hrushovski’s Algorithm 13

3 Proto-Galois Groups for $n = 2$ 15

4 General Bounds for
   Proto-Galois Groups 22
   4.1 Preliminaries 22
4.2 Main results .................................................. 24
4.3 Application to Hrushovski’s algorithm .................. 25
4.4 Proof ingredients ............................................. 26
  4.4.1 Auxiliary lemmas ........................................ 27
  4.4.2 Degree bound for unipotent groups .................. 30
  4.4.3 Degree bound for reductive groups .................. 31
  4.4.4 Degree bound for product ............................ 37
4.5 Proof of Theorem 12 ....................................... 38

5 Complexity of Triangular Set Representation ............ 40
  5.1 Introduction ............................................... 41
  5.2 Preliminaries ............................................. 44
  5.3 Outline of Szanto’s algorithm .......................... 49
  5.4 Bounds for degrees ...................................... 55
  5.5 Bound for the number of components .................. 71

Appendix A: Matrix Representation of Pseudoremainder 74

Appendix B: Maple Code for $n = 2$ .......................... 76
Introduction

Differential equations arise in many fields. Although numerical methods exist to solve them to a sufficient degree of accuracy in practice, finding exact solutions and understanding their properties can help reduce error produced by approximate solutions. An algebraic framework was developed by Ritt and Kolchin to address the latter task. Perhaps the most powerful tool they constructed for this purpose, at least in the case of linear differential equations, was the differential Galois group. The desire to compute this group for given differential equations has led to the development of various algorithms.

As Hrushovski’s algorithm is the most general algorithm known for computing a differential Galois group, its complexity is of great interest. A key step of the algorithm involves the computation of proto-Galois group, a group that satisfies some special containments with respect to the Galois group. Although addressing the complexity of this one step alone does not address the complexity of the entire algorithm, it is a crucial step in that direction.

Feng gave a degree bound for proto-Galois groups in [9]. His bound is for the polynomials in a Groebner basis for the radical ideal corresponding to the group and
is quintuply exponential in the order of the given differential equation, (or size of the coefficient matrix in case one writes a scalar differential equation as a matrix equation). Using an alternative approach in seeking a bound, (specifically seeking equations that define a proto-Galois group instead of its corresponding radical ideal), turns out to produce equations of significantly lower degree. Yet another approach to obtain equations of lower degree is to use triangular sets in place of Groebner bases in Feng’s analysis, as demonstrated in [31].

We explore these matters in the text that follows. We first give a description of the differential Galois group in Chapter 1, writing all of our differential equations as matrix equations with coefficient matrix having size $n \times n$. Then we provide some background on algorithms to compute differential Galois groups and an outline of Hrushovski’s algorithm in Chapter 2, where we include a discussion of what a proto-Galois group is and Feng’s bound. In Chapter 3, we explain how we obtained a smaller bound for the case $n = 2$. In Chapter 4, we give the development of our smaller bound for general $n$. Finally, in Chapter 5 we provide a complexity analysis of Szanto’s algorithm to represent ideals by triangular sets, an analysis that was recently used by Sun to also obtain a bound lower than Feng’s original bound.
Chapter 1

Differential Galois Groups

In this chapter, we discuss some Differential Galois Theory to understand the object we are interested in computing. Note that all rings considered have characteristic zero and are unital.

1.1 Differential Rings and Fields

Definition 1. A derivation $\delta$ of a ring $R$ is a function $\delta : R \to R$ such that

- $\delta(r + s) = \delta(r) + \delta(s)$ for all $r, s \in R$
- $\delta(rs) = \delta(r)s + r\delta(s)$ for all $r, s \in R$

Remark. When $\delta$ is clear from context, we typically write $a'$ in place of $\delta(a)$

Lemma 1 (Power Rule). Suppose $\delta$ is a derivation on a ring $R$. Then $\delta(1) = 0$ and, for all $a \in R, n \in \mathbb{Z}$ we have $(a^n)' = na^{n-1}a'$.

Definition 2. We say that $(R, \delta)$ is a differential ring if $\delta$ is a derivation on $R$. If $\delta$ is understood from context, we typically just write $R$ in place of $(R, \delta)$. If $R$ is a field, we call it a differential field.
**Definition 3.** Let $k$ be a differential field. The field of constants or constant field of $k$ is the subfield $\{a \in k \mid a' = 0\}$ and often denoted by $C$.

**Lemma 2.** Let $k$ be a differential field. Then $C$, the field of constants of $k$, is a field.

### 1.2 Matrix Differential Equations

We now restrict our attention to an important base differential field.

**Definition 4.** Let $k = C(t)$, with $C$ algebraically closed. Take the derivation $\delta$ on $k$ to be the usual derivative operator $\frac{d}{dt}$. A matrix linear differential equation over $k$ is an equation of the form

$$Y' = AY$$

where $A \in \text{Mat}_n(k)$ and $Y = (y_1 \ y_2 \ \ldots \ y_n)^T$.

**Remark.** Any scalar linear differential equation of order $n$

$$y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1y' + a_0y = 0, a_i \in k$$

can be transformed into a matrix differential equation by letting $y_1 = y, y_2 = y', \ldots, y_n = y^{(n-1)}$. Then the given differential equation can be used to express the highest derivative $y^{(n)}$ in terms of the indeterminates $y_i$. Nonhomogeneous differential equations can also be transformed into such equations.

**Definition 5.** Suppose $Y' = AY$ has $n$ linearly independent (over $C$) solutions in some differential extension $L$ of $k$. We call these solutions a fundamental set of solutions. If we organize these solutions into an $n \times n$ matrix $F$ by making each
solution a column, the resulting matrix satisfies $F' = AF$ (where differentiation of a matrix is done entry-wise), is in $GL_n(L)$, and is referred to as a fundamental solution matrix. For technical reasons that will not be addressed here, we also stipulate that $C_L = C$.

Fix a fundamental set of solutions $Y_1, Y_2, \ldots, Y_n$. Consider the differential field generated over $k$ by the entries of these column vectors, denoted $K := k\langle Y_1, \ldots, Y_n \rangle$. For a given fundamental solution matrix $F \in GL_n(K)$, there may be another fundamental solution matrix $\bar{F} \in GL_n(K)$. (For instance, we might order the solutions differently in placing them in columns.) Since the columns of these two matrices are linearly independent, however, they must be related by a change of basis matrix. That is, we must have $\bar{F} = FM$ for some $M \in GL_n(K)$. We can actually say more about the entries of this change of basis matrix.

**Lemma 3.** Any change-of-basis matrix that relates one fundamental solution matrix to another has constant entries.

### 1.3 Differential Automorphisms

**Definition 6.** Let $k$ be a differential field. An automorphism $\sigma : k \to k$ is said to be a differential automorphism if $\sigma(a') = \sigma(a)'$ for all $a \in k$.

So a differential automorphism is one that commutes with the derivation. Consider a differential automorphism $\sigma$ of $K$, where $K$ is a differential extension of $k = C(t)$ generated by a fundamental set of solutions to a differential equation $Y'' = AY$ and
adding no new constants. If there is such a $\sigma$ that fixes $C(t)$ pointwise, we have the following for a fundamental solution matrix

$$\sigma(F)' = \sigma(F') = \sigma(AF) = \sigma(A)\sigma(F) = A\sigma(F)$$

That is, such a $\sigma$ produces new fundamental solution matrix out of the chosen one. (It is still an invertible matrix because $\sigma(\det(F)) = \det(\sigma(F))$ and $\det(F) \neq 0$.)

**Definition 7.** The collection of all differential automorphisms of $K$ that fix $k$ pointwise is called the *differential Galois group* for $Y' = AY$. It may be henceforth denoted by $Gal(K/C(t))$ or simply $G$ when there is no ambiguity.

We can represent such automorphisms by matrices, starting with a fixed fundamental solution matrix $F$. These automorphisms produce further fundamental solution matrices out of the fixed one. By our discussion in the previous section, fundamental solution matrices are related by a change-of-basis matrix. So $\sigma$ can be represented by the change-of-basis matrix that relates $F$ to the new fundamental solution matrix $\sigma$ gives rise to.

Now suppose $\sigma$ is represented by $M_1$ and $\tau$ is represented by $M_2$. What can be said about a representation of $\sigma \tau$? Recalling that such representations must have constant entries from the previous section, we have

$$\sigma(\tau(F)) = \sigma(FM_2) = \sigma(F)\sigma(M_2) = \sigma(F)M_2 = (FM_1)M_2 = F(M_1M_2)$$

So we see that composition of differential automorphisms translates to matrix multiplication in the corresponding order using matrix representations. All of this
suggests that the differential Galois group can be represented as a linear algebraic group over $\mathbb{C}$. In fact, we can say more.

**Theorem 4.** The differential Galois group for $Y' = AY$ can be realized as a closed linear algebraic subgroup of $GL_n(\mathbb{C})$.

We illustrate how this result can be used to determine the Galois group of a given differential equation.

**Example 1.** Consider the differential equation

$$y' = y$$

with coefficients in $C(t)$. (Here, $n = 1$.) There is no solution to this differential equation in $C(t)$, as the quotient rule applied to a rational function shows that the degree of the numerator minus the degree of the denominator is reduced by 1 upon differentiation. So we look for a solution in a differential closure of $C(t)$ and we denote this solution by $e^t$. As before, the “solution field” $K$ can be written as $C(t)\langle e^t \rangle = C(t)\langle e^t, (e^t)', (e^t)'' , \ldots \rangle = C(t)(e^t) = C(t, e^t)$. Suppose we now wish to compute the differential Galois group of $K$ over $k$. We know this will be a subgroup of $GL_1(\mathbb{C}) \cong \mathbb{C}^*$. The closed subgroups of $\mathbb{C}^*$ are the following:

- $\{ \zeta \mid \zeta^n = 1 \}$ for $n \in \mathbb{N}_{>0}$
- $\mathbb{C}^*$ itself

If the differential Galois group was the former, then we would have that $(e^t)^n \in C(t)$ for some $n \in \mathbb{N}_{>0}$. But $[(e^t)^n]' = n[e^t]^{n-1} \cdot (e^t)' = n[e^t]^n$. This implies that we have a
nonzero solution in $C(t)$ to the equation

$$\frac{dz}{dt} = nz$$

But again, by comparison of degrees, this cannot be the case. Say this solution is expressible as $\frac{f}{g}$, with $\deg(f) = m$ and $\deg(g) = n$. Then the degree of this rational function is $m - n$. But the degree of the derivative $(m + n - 1) - 2n = m - n - 1$. So a rational function cannot be a multiple of its own derivative unless it is constant. But if $\frac{f}{g}$ is constant, $n$ would have to be zero, another impossibility since $n$ is positive. So we conclude that the differential Galois group cannot be the group of $n$th roots of unity for some $n$. Thus, we see that the differential Galois group must be $C^*$.  

### 1.4 Liouville Extensions

In this section, we connect the notion of “solvability by quadratures” to differential extensions. To do this, we introduce the following notion.

**Definition 8.** A differential field extension $L \subset M$ is said to be a *Liouville extension* of $L$ if there exist intermediate differential fields $L = F_1 \subset F_2 \subset \cdots \subset F_n = M$ such that $F_{i+1}$ is obtained from $F_i$ by:

* adjunction of an integral,

* adjunction of the exponential of an integral,

* or the adjunction of an element algebraic over $F_i$.  

Informally speaking, the elements of $M$ can be written with elements from $L$ using only a few basic operations. In fact, the differential Galois group (endowed with the Zariski topology) allows us to detect if this is the case. (Recall that the identity component of a topological group $G$ is the maximal connected subset of the group containing the identity element and is typically denoted by $G^0$. Given a topological group $G$, $G^0$ is a (normal) subgroup.)

**Theorem 5.** Suppose $M$ is a differential extension of $L$ for a matrix equation $Y' = AY$ defined over $L$. Then $M$ is a Liouville extension of $L$ if and only if the identity component of $\text{Gal}(M/L)$ is solvable.
Chapter 2

Computing Differential Galois Groups

2.1 Known Algorithms

F. Ulmer and J.-A. Weil stated that algorithms for finding rational solutions date back as far as Liouville (1833). So algorithms to compute differential Galois groups have beginnings dating back to the early 19th century, even though the algebraic framework was not yet in place by then to formally make this application. (In addition, the notion of algorithm was only formalized shortly before Ritt and Kolchin founded the field of differential algebra. So there may have been a notion of “algorithm” previously adopted in the literature that does not coincide with the notion of an algorithm today.) F. Ulmer and J.-A. Weil also suggest that algorithms for finding algebraic solutions were proposed by Pepin (1878) and Fuchs (1881), although a complete decision procedure for the procedures they described does not seem to have been provided until later. Baldassari and Dwork fixed this aspect of those procedures.

Picard-Vessiot theory offers a rigorous way of saying what it means for a solution to
be expressible in “closed form,” a property referred to as Liouvillian in the literature. As this theory was developed further by Kolchin, algorithms to compute Liouvilian solutions were proposed (or recognized as such, if they had previously existed). The original one has implementation obstacles. But work by Abramov, Bronstein, Singer, Ulmer, and Weil addressed a number of these obstacles.

Algorithms to address various special cases also emerged in the meantime. Kovacic invented one for second-order equations, one which he describes as a “brute-force” algorithm that relies on previous classifications of subgroups of the special linear group. As his work demonstrated that understanding the shape of candidates for the differential Galois group could assist in determining which one is the group for a given equation, Singer and Ulmer investigated groups that can arise for second and third order differential equations. Later, Singer and Compoint gave an algorithm in [5] to compute the differential Galois group if it is known in advance that the group is reductive. There has also been work done on the numeric-symbolic computation of differential Galois groups, notably by van der Hoeven in [35].

Hrushovski’s algorithm does not have any of the limitations of the above algorithms. It can be used to compute the differential Galois group of a given equation, regardless of order or anticipated properties of the group. However, the algorithms listed above may be more efficient for the special cases in which they are appropriate.
2.2 Proto-Galois Groups

As Feng describes Hrushovski’s algorithm in [9], an important ingredient is the computation of a group containing the differential Galois group. Such a group is found by computing the first finitely many terms of a fundamental solution matrix expressed as a power series in $t$. (The required number of terms can be determined by results of Bertrand and Beukers). Then one computes the polynomials in $n^2$ indeterminates that vanish on the (truncated) fundamental solution matrix. To determine these polynomials, it is sufficient to bound their degrees by some integer $\tilde{d}$. Substitution of the (truncated) fundamental matrix into the polynomials of this maximal degree $\tilde{d}$ produces a linear system for their coefficients, from which the polynomials can be determined using linear algebra techniques.

**Definition 9.** Let $G$ be an algebraic group, (for example the differential Galois group for an equation $Y' = AY$). We say that $H$ is a proto-Galois group for $G$ (or $Y' = AY$ when $G$ is the corresponding differential Galois group) if $H$ satisfies the chain of containments

$$(H^o)^t \leq G^o \leq G \leq H,$$

where $H^o$ is the identity component of $H$ and the leftmost item is the subgroup of $H^o$ generated by its unipotent elements.

Informally speaking, such an $H$ captures the unipotent and semisimple parts of $G$ and reduces the problem to the case of a composition of hyperexponential and
algebraic extensions. Put another way, such an $H$ captures the noncommutative part of the identity component.

Equations that define such a group as a variety are found by solving an appropriate system of equations. In setting up this system of equations, it is sufficient to have a degree bound on defining equations for such a group. To formally discuss the bounds we seek, we introduce a definition.

**Definition 10.** A algebraic subvariety $X \subset GL_n(C)$ is said to be *bounded by* $d$, where $d$ is a positive integer, if there exist polynomials $f_1, \ldots, f_M \in C[x_{11}, x_{12}, \ldots, x_{nn}]$ of degree at most $d$ such that

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

Note that algebraic groups are instances of algebraic subvarieties. So it makes sense to apply this definition to algebraic groups.

Given $Y' = AY$ with $A$ in $M_n(C(t))$, there exists a bound $\tilde{d}$ for a proto-Galois group for this equation solely depending on $n$.

**Theorem 6** (Feng, 2013).  

$$\tilde{d} = O\left(n^{n^nn^{O(1)}}\right)$$

### 2.3 Hrushovski’s Algorithm

Here we describe Hrushovski’s algorithm with a level of detail sufficient for our purposes, providing a simplified overview. For a more complete description of the al-
algorithm, the reader is referred to [9]. Hrushovski’s algorithm for computing the differential Galois group [16] of a linear differential equation of order \( n \) consists of the following three steps as outlined in [9, Section 1] :

1. Compute a proto-Galois group of the differential Galois group of the equation using an a priori upper bound \( \tilde{d} \) for the degrees of the defining equations.

2. Determine the identity component of the Galois group by computing the pullback of a torus to the proto-Galois group, using the algorithm by Compoint and Singer [5].

3. Recover the Galois group from its identity component and a finite Galois group, one which somehow captures the various translates of the identity component within the Galois group.
Chapter 3

Proto-Galois Groups for $n = 2$

We consider bounds for proto-Galois groups in the case $n = 2$. So we note that a proto-Galois group must contain the connected component of the identity of $G$. This allows a first step in reducing the problem by suggesting that we start by looking at connected subgroups of $GL_n(C)$. We will reduce this problem, however, to subgroups of $SL_2(C)$ and prove the following theorem, the main theorem of this section.

**Theorem 7.** Suppose $G$ is an algebraic subgroup of $GL_2(C)$. Then there exists a proto-Galois group of $G$ bounded by 6.

**Proof.** We begin with two reductions. In the following, let $Z_n := Z(GL_n(C)) \cong C^* \cdot I_n$, where $I_n$ is the $n \times n$ identity matrix.

**Lemma 8.** Suppose $G$ is an algebraic subgroup of $GL_n(C)$. Then a proto-Galois group for $G_Z := G \cdot Z_n$ (where the dot signifies usual multiplication of matrices) is also a proto Galois group for $G$.

**Proof.** We are given a proto-Galois group $H$ for $G_Z$. So we have $(H^\circ)^t \unlhd (G_Z)^\circ \unlhd G_Z \unlhd H$. We wish to show that $(H^\circ)^t \unlhd G^\circ \unlhd G \unlhd H$. We establish this by handling
the individual containments from right to left. The rightmost containment is satisfied because \( G_Z \supset G \). The next containment is also satisfied by definition of \( G^0 \). (In other
cwords, this containment actually has nothing to do with \( H \)). It remains to show that
\( G^0 \supseteq (H^0)' \). We address this by establishing two claims.

**Claim 1:** \((G_Z)^0 = G^0 \cdot Z_n\).

First, \( G^0 \cdot Z_n \supseteq (G_Z)^0 \) because the product of the connected groups on the left-
hand side is connected. (This can be seen by taking the map \( m : G^0 \times Z_n \to GL_n(C) \)
defined by usual multiplication of matrices. The domain is irreducible because each
component is irreducible and the product variety formed from two irreducible varieties
is irreducible by [13, Problem 3.15]. As every irreducible space is connected, the
domain is connected. Also, the map \( m \) is continuous. The continuous image of a
connected space is connected and the image of \( m \) is exactly \( G^0 \cdot Z_n \).)

We next show the reverse containment. Write \( G \) as the disjoint union \( g_1 G^0 \sqcup \cdots \sqcup g_m G^0 \) and, without loss of generality, assume \( g_1 = e \). Then \( G_Z = Z_n \cdot G = g_1 G^0 \cdot Z_n \cup \cdots \cup g_m G^0 \cdot Z_n \). Note that after multiplication by \( Z_n \), the union is no
longer necessarily disjoint.

But we now claim that if \( g_i G^0 \cdot Z_n \cap g_j G^0 \cdot Z_n \neq \emptyset \), then \( g_i G^0 \cdot Z_n = g_j G^0 \cdot Z_n \). For this intersection is nonempty there exist \( g, g' \in G^0 \) and \( c, c' \in C \) such that
\( g_i g c = g_j g' c' \). But then \( g_i g c G^0 \cdot Z_n = g_j g' c' G^0 \cdot Z_n \). Since \( g G^0 = g' G^0 = G^0 \), we have
\( g_i G^0 \cdot Z_n = g_j G^0 \cdot Z_n \).

Therefore we can write \( G_Z \) as a disjoint union using certain representatives that
CHAPTER 3. PROTO-GALOI GROUS FOR $N = 2$

appear in the disjoint union for $G$. That is, we can write $G_Z$ as $G^0 \cdot Z_n \sqcup g_i G^0 \cdot Z_n \cdot \cdots \sqcup g_i G^0 \cdot Z_n$. The first piece of the union is still $G^0 \cdot Z_n$. This is connected. It is normal in $G_Z$ because $G^0$ is normal in $G$ and $Z_n$ commutes with everything. Finally, it is of finite index because we see that $G_Z$ has only finitely many cosets of $G^0 \cdot Z_n$.

This shows that $G^0 \cdot Z_n \subseteq (G_Z)^0$ and gives us the desired equality, establishing the claim.

Claim 2: $(H^0)^t$, which is contained in $(G_Z)^0$ by assumption, is contained in $G^0$.

We establish the claim above by showing that if $A \in G^0 \cdot Z_n (= (G_Z)^0$ by Claim 1) and $A$ is unipotent, then $A \in G^0$. Because $A$ is unipotent, there exists a basis in which it is upper-triangular. In this basis, write $A = cg, c \in C^*, g \in G^0$. Note that $g = c^{-1}A$ is then also upper-triangular (in the chosen basis). Since $G^0$ is an algebraic group, there exists a unique decomposition of $g$ into semisimple and unipotent elements of $G^0$ by [18, Section 15.3, p. 99]. But $c^{-1}A = (c^{-1}I_n)A$ is such a decomposition of $g$.

That is, we have $c^{-1}I_n$ is the semisimple part of $g$ and $A$ is the unipotent part of $g$. In particular, $A \in G^0$.

We make a further reduction of this case as follows.

Lemma 9. Suppose $G = G_Z$. Then $G$ can be represented as $Z_n \cdot G_{SL}$, where $G_{SL}$ is an algebraic subgroup of $SL_n(C)$. (In particular, when $G$ is finite $G_{SL}$ will be.)

Proof. If $g \in G$, observe that we can write $g$ as $g = \sqrt{\det(g)}I_n \cdot \frac{1}{\sqrt{\det(g)}}g$. The second matrix in this product is in $SL_n(C) \cap G$ (because $G$ contains scalar matrices).
(This uses the fact that $C$ is algebraically closed.) So a candidate for $G_{SL}$ is this intersection. Since the intersection of algebraic subgroups is algebraic, we have the result.

According to Kovacic in [21, p. 5], there are now 4 cases to consider. This is because the algebraic subgroups of $SL_2(C)$ can be classified as follows:

1) $G_{SL}$ is triangularizable.

2) $G_{SL}$ is conjugate to a subgroup of

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

3) $G_{SL}$ is finite and neither of the previous two cases hold.

4) $G_{SL} = SL_2$

We examine each of these cases individually below.

1. $G_{SL}$ is triangularizable. (So there exists a basis in which $G_{SL}$ can be represented by upper-triangular matrices.)

**Lemma 10.** Assume that, after selection of an appropriate basis, $G_{SL}$ is a subset of $B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in C, ac \neq 0 \right\}$ with at least one non-diagonal matrix. Then $B$ can be taken as a proto-Galois group for $G_{SL}$.

**Proof.** For any element in $G_{SL}$, there exists a decomposition into semisimple and unipotent parts, with each factor being again in $G_{SL}$. Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ be an
element in $G_{SL}$ with $b \neq 0$, (which exists since the group is assumed to have at least one nondiagonal matrix). Then $A$ can be written as $\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix}$ in the chosen basis. This is a decomposition of $A$ into its unipotent and semisimple parts. So both of the factors that appear in this decomposition are also in $G_{SL}$ ([18, Section 15.3]). Because the second factor is a nonidentity matrix ($b \neq 0$), its powers generate a (non-algebraic) subgroup of $G$ isomorphic to $\mathbb{Z}$. The Zariski closure of this subgroup is

$$\left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbb{C} \right\} = \langle B^0 \rangle$$

This is therefore a subgroup of $G_{SL}$. It is also connected and contains the identity matrix. So in fact $\langle B^0 \rangle \leq G_{SL}^0$. □

**Remark.** (a) Note that $B$ is bounded by 1, as it can be described in $GL_n(\mathbb{C})$ as the subset $B = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, d \in \mathbb{C}, c = 0 \}$. (So we see that $B$ can be defined by an equation of degree 1.)

(b) All conjugates of $B$ are also bounded by 1, so the bound remains valid with different choices of basis.

(c) Case 2 below addresses the situation in which $G_{SL}$ does not contain a nondiagonal matrix.

2. $G$ is conjugate to a subgroup of

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{C}, ad \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : b, c \in \mathbb{C}, bc \neq 0 \right\}$$
In this case, we claim that $D$ (or an appropriate conjugate $D'$) can be taken as a proto-Galois group. Such groups are bounded by 2. The reason $D$ (or some $D'$) can be taken as a proto-Galois groups is that the connected component is the collection of diagonal matrices, so that the intersection of the kernels of all characters of the identity component is $\{E\}$. (To see this, note that projections of the diagonal constitute character maps. So the only matrix that is in the kernel of the two possible projections is the identity matrix.)

3. $G_{SL}$ is finite and neither of the previous two cases hold.

Classifications of finite subgroups of $SL_2$ have been written about in [21] and [29]. We use presentations of these groups that they have provided and Maple code to bound a proto-Galois group in each case. The five cases that it suffices to consider are as follows:

(a) Cyclic Groups. Cyclic groups are diagonalizable by [11, p. 2]. So this group is contained in $D$ and addressed above.

(b) Binary Dihedral Group

(c) Binary Octahedral Group

(d) Binary Tetrahedral Group

(e) Binary Icosahedral Group

In cases 2-5, we carry out the following algorithm

(a) Input presentation of group.
(b) Generate group.

(c) Compute a Groebner basis for the group multiplied by scalar matrices, using grlex ordering.

(d) Identify element of Groebner basis of maximal degree.

This algorithm is described in more detail in the Appendix, where Maple code used for the algorithm is provided. When all of these cases are run through the algorithm, it is evident that all of the subcases here are bounded by 6.


In this case, $GL_2$ can be taken as a proto-Galois group for $G_{SL}$. Note that $GL_2$ is bounded by 0.
Chapter 4

General Bounds for Proto-Galois Groups

In this chapter, we develop a bound for proto-Galois groups for linear differential equations of order $n$. To do this, we first consider toric envelopes. Such objects have a convenient algebraic description in terms of products, with factors that we bound individually. Moreover, such groups turn out to be proto-Galois groups.

4.1 Preliminaries

Throughout this chapter, $C$ denotes an algebraically closed field of characteristic zero.

**Definition 11.** A *torus* is a commutative connected algebraic subgroup $T \subset GL_n(C)$ such that every element of $T$ is diagonalizable.

**Definition 12.** Consider a linear algebraic group $G \subset GL_n(C)$. We say that an algebraic group $H \subset GL_n(C)$ is a *toric envelope* of $G$ if there exists a torus $T \subset GL_n(C)$ such that $H = T \cdot G$ (product as abstract groups).

**Remark.** Although every toric envelope is a product of the form $T \cdot G$, the structure
of this product might be complicated. For example, $T$ does not necessarily normalize $G$ (Example 5) and $G$ does not necessarily normalize $T$ (Example 4). However, one can show that $T$ normalizes $G^o$ and $G$ normalizes $T \cdot G^o$.

Example 2. Every linear algebraic group $G \subset GL_n(C)$ is a toric envelope of itself (with $T = \{e\}$).

The following notion of the degree of a variety (we specialize it to subvarieties of $GL_n(C)$, for more general treatment we refer to [14, Section 2]) is a generalization of the notion of the degree of a polynomial.

Definition 13. Let $X \subset GL_n(C)$ be a subvariety such that all irreducible components of $X$ are of the same dimension $m$ (for example, this is the case if $X$ is a linear algebraic group). Then

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

For example, the degree of a hypersurface is equal to the degree of its defining polynomial [14, Remark 2].

Proposition 11 (follows from [14, Proposition 3]). Let $X \subset GL_n(C)$ be a subvariety of degree $D$. Then $X$ can be defined by equations of degree at most $D$.

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

Example 3. Let $N$ be a positive integer and $G \subset GL_1(C)$ be the group of all $N$-th roots of unity. It is defined by inside $GL_n(C)$ by a single equation $x^N - 1 = 0$ of degree
N, so it has degree N. The whole \( GL_1(C) \) is a toric envelope of \( G \) with \( T = GL_1(C) \) and is of degree 1.

**Example 4.** Consider

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

\( G \) is the intersection of \( GL_2(C) \) and a hypersurface in the space of all triangular matrices of degree 2018, so \( \deg G = 2018 \). Let \( T \) be the group of all diagonal matrices. Then the group of all triangular matrices in \( GL_2(C) \) is a toric envelope of \( G \) because it is equal to \( T \cdot G \). This group is defined by a single linear equation, so it has degree 1.

**Example 5.** Consider a dihedral group

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

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

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

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

### 4.2 Main results

**Theorem 12.** Let \( G \subset GL_n(C) \) be a linear algebraic group. Then there exists a toric envelope \( H \) of \( G \) of degree at most \((4n)^{3n^2}\). In particular, \( H \) is bounded by this
Remark. A sharper bound for Theorem 12 is given by (4.5.1).

Remark. Let us show that the bound in Theorem 12 is qualitatively optimal by presenting a single-exponential lower bound. Fix a positive integer $n$ and fix a basis in $C^n$. Let $D$ and $P$ be the group of all diagonal matrices and the group of all permutation matrices in this basis, respectively. Since $P$ normalizes $D$, $G = PD \subset GL_n(C)$ is an algebraic group. One can show that since $G^\circ$ is a maximal torus in $GL_n(C)$, the only possible toric envelope of $G$ is $G$ itself. Since $P \cap D = \{e\}$, the number of connected components of $G$ is equal to $|P| = n!$. Since $G^\circ = D$, every component has the degree $\text{deg } D = 1$. Thus, we obtain a single-exponential lower bound

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

The same example gives a single-exponential lower degree bound for a proto-Galois group (see Section 4.3) as well.

### 4.3 Application to Hrushovski’s algorithm

Recall Definition 9 of a proto-Galois group. In this section, we show (Lemma 13) that every toric envelope of an algebraic group $G \subset GL_n(C)$ is a proto-Galois group of $G$. It follows that the bounds from Theorem 12 can be used in the first step of Hrushovski’s algorithm instead of the bound given in [9, Proposition B.11].
**Lemma 13.** If $H \subset GL_n(C)$ is a toric envelope of $G \subset GL_n(C)$, then $H$ is a proto-Galois group of $G$.

**Proof.** Since $H$ is a toric envelope of $G$, $G \subset H$, so inclusions $G^o \subset G \subset H$ from Definition 9 hold. [30, Lemma 2.1] implies that $(H^o)^t$ is exactly the subgroup of $H$ generated by all unipotent elements of $H^o$. Due to Lemma 15, it coincides with the subgroup of $G^o$ generated by all unipotents in $G^o$, and such a subgroup is normal in $G^o$.

**Corollary 14.** For every linear algebraic group $G \subset GL_n(C)$, there exists a proto-Galois group $H$ bounded by $(4n)^{3n^2}$.

### 4.4 Proof ingredients

**Notation 1.** In what follows we will use the following notation.

- We denote the set of all $n \times n$ (resp., $n \times m$) matrices over $C$ by $\text{Mat}_n(C)$ (resp., $\text{Mat}_{n,m}(C)$).
- As in Chapter 3, denote the subgroup of all scalar matrices in $GL_n(C)$ by $Z_n \subset GL_n(C)$.
- For a subset $X \subset \text{Mat}_n(C)$, we denote the normalizer and centralizer subgroups of $X$ by $N(X)$ and $Z(X)$, respectively.
- For a subgroup $G \subset GL_n(C)$, we denote the center by $C(G)$.
- For a Lie subalgebra $u \subset \mathfrak{gl}_n(C)$, we denote the normalizer and centralizer subalgebras by $\mathfrak{n}(u)$ and $\mathfrak{z}(u)$, respectively.
• For a positive integer $n$, $J(n)$ is the minimal number such that every finite subgroup of $GL_n(C)$ contains a normal abelian subgroup of index at most $J(n)$. We will use the Schur’s bound [6, Theorem 36.14]

\[ J(n) \leq (\sqrt{8n} + 1)^{2n^2} - (\sqrt{8n} - 1)^{2n^2} \] (4.4.1)

• For a positive integer $n$, $A(n)$ is the maximal size of a finite abelian subgroup of $GL_n(Z)$. Some known values are $A(1) = 2$, $A(2) = 6$ (see [25, p. 180]), and $A(3) = 12$ (see [34, p. 170]).

4.4.1 Auxiliary lemmas

**Lemma 15.** An algebraic group $H \subset GL_n(C)$ is a toric envelope of an algebraic group $G \subset GL_n(C)$ if and only if

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

**Proof.** Let $H$ be a toric envelope of $G$. Then there exists torus $T \subset GL_n(C)$ such that $H = T \cdot G$. Since $T$ is connected, $T \subset H^\circ$, so $H \supset G \cdot H^\circ \supset G \cdot T = H$, so (2) holds. Consider any unipotent element $A \in H^\circ$. Since $H^\circ = T \cdot G^\circ$, then there are $B \in T$ and $C \in G^\circ$ such that $A = BC$. Since $T$ is a torus, $B$ is a semisimple element. Then $C = B^{-1}A$ is a Jordan decomposition of $C$. Due to [26, Theorem 6, p. 115], $A, B \in G^\circ$. Thus, every unipotent element of $H^\circ$ belongs to $G^\circ$. Since also $G \subset H$, (1) holds.
Assume that properties (1) and (2) hold for $G$ and $H$. Let $H = H_0 \rtimes U$ be a Levi decomposition of $H$ (see [26, Theorem 4, p. 286]). Due to [38, Lemma 10.10], $H_0$ can be written as a product $\Gamma H_0^\circ$ for some finite group $\Gamma \subset GL_n(C)$. [2, Proposition, p. 181] implies that $H_0^\circ$ can be written as $ST$, where $T := C(H_0^\circ)^\circ$ is a torus and $S := [H_0^\circ, H_0^\circ]$ is semisimple. Since $\Gamma$ normalizes $H_0$ and the center is a characteristic subgroup, $\Gamma$ normalizes $T$. Since $U$ and $S$ are generated by unipotents, $U, S \subset G^\circ$. Then

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

so $H = T \cdot G$ and $H$ is a toric envelope of $G$. \hfill \Box

**Corollary 16.** If $H_2 \subset GL_n(C)$ is a toric envelope of $H_1 \subset GL_n(C)$ and $H_1$ is a toric envelope of $H_0 \subset GL_n(C)$, then $H_2$ is a toric envelope of $H_0$.

**Proof.** Lemma 15 implies that $H_0^\circ, H_1^\circ,$ and $H_2^\circ$ have the same set of unipotents. Since $H_1 \subset H_2$, we have $H_1^\circ \subset H_2^\circ$. Together with Lemma 15 this implies that $H_2 = H_2^\circ \cdot H_1 = H_2^\circ \cdot H_1^\circ \cdot H_0 = H_2^\circ \cdot H_0$. Lemma 15 implies that $H_2$ is a toric envelope of $H_0$. \hfill \Box

**Corollary 17.** Any toric envelope of a reductive group is again a reductive group.

**Proof.** Let $G$ be a reductive group and $H$ be its toric envelope. Assume that $H$ is not reductive. Then it contains a nontrivial connected normal unipotent subgroup $U$. Since $G^\circ$ and $H^\circ$ have the same unipotents, $U \subset G^\circ$. This contradicts the reductivity of $G$. \hfill \Box
Corollary 18. Let $G$ be an algebraic subgroup of $GL_n(C)$. Then every toric envelope of $G Z_n$ is a toric envelope of $G$.

The following geometric lemma is a modification of [20, Lemma 3].

Lemma 19. Let $X \subset \mathbb{A}^N$ be an algebraic variety of dimension $\leq d$ and degree $D$. Consider polynomials $f_1, \ldots, f_M \in C[\mathbb{A}^N]$ such that $\deg f_i \leq D_1$ for every $1 \leq i \leq M$. Then the sum of the degrees of the components of $Y := X \cap \{f_1 = \ldots = f_M = 0\}$ of dimension $\geq d'$ does not exceed $D \cdot D_1^{d - d'}$.

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

Let $d > d'$. Considering every component of $X$ separately, we may reduce to the case that $X$ is irreducible. If every $f_i$ vanishes on $X$, then $X = Y$ and the only component of $Y$ of dimension $\geq d'$ has degree $D$. Otherwise, assume that $f_1$ does not vanish everywhere on $X$. Then $\dim X \cap V(f_1) \leq d - 1$ and $\deg(X \cap V(f_1)) \leq DD_1$ due to [13, Theorem 7.7, Chapter 1]. Applying the induction hypothesis to $X \cap V(f_1)$ and the same $d'$, we show that the sum of the degrees of the components of $Y$ of dimension at least $d'$ is at most

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

$\square$

Corollary 20. For every collection of algebraic subgroups $G_0, G_1, \ldots, G_k \subset GL_n(C)$

$$\deg G \leq n^{\dim G_0 - \dim G} \deg G_0,$$

where $G := G_0 \cap N(G_1) \cap \ldots \cap N(G_k)$. 
CHAPTER 4. GENERAL BOUNDS FOR PROTO-GALOIS GROUPS

30

Proof. [9, Lemma B.4] implies that $N(G_1) \cap \ldots \cap N(G_k)$ is defined by polynomials of degree at most $n$. Then the statement of the corollary follows from Lemma 19 with $D_1 = n$. □

Lemma 21. $A(n) \leq 2 \cdot 3^{[n^2/4]}$, where $[x]$ means the integer part of $x$.

Proof. Consider a finite abelian subgroup $A \subset GL_n(\mathbb{Z})$. Let $A_0 := A \cap SL_n(\mathbb{Z})$, then $|A| \leq 2|A_0|$. Consider the homomorphism $\varphi: SL_n(\mathbb{Z}) \to SL_n(\mathbb{F}_3)$ defined by reducing modulo 3. [25, Theorem IX.8] implies that $|A_0| = |\varphi(A_0)|$. According to [36, Table 2], the size of an abelian subgroup of $SL_n(\mathbb{F}_3)$ does not exceed $3^{[n^2/4]}$. □

4.4.2 Degree bound for unipotent groups

Lemma 22. Let $U \subset GL_n(C)$ be a connected unipotent group. Then, $\deg U \leq \prod_{k=1}^{n-1} k!$.

Proof. Due to Engel’s theorem [26, Corollary 1, p. 125], there exists a basis such that $\text{Lie}U$ is contained in a subspace $\mathcal{T} \subset \text{Mat}_n(C)$ of strictly upper triangular matrices. From now on, we fix such a basis. Due to [26, Theorem 7, p. 126], $U$ is equal to $\varphi(\text{Lie}U)$, where $\varphi$ is the exponential map. Since every matrix in $\mathcal{T}$ is nilpotent of index at most $n - 1$, $\varphi$ is defined everywhere on $\mathcal{T}$ by the following formula

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

Consider an algebraic variety

$$W := \{(X,Y) \in \mathcal{T} \times GL_n(C) \mid Y = \varphi(X) \& X \in \text{Lie}(U)\}.$$
Since the projection of $W$ onto $GL_n(C)$ is equal to $\varphi(\text{Lie}U) = U$, $\deg U \leq \deg W$.

The condition $X \in \text{Lie}(U)$ is defined by linear equations. Direct computation shows that

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

where by $(\varphi(X))_{i,j}$ we denote the $(i,j)$-th entry of the matrix $\varphi(X)$ whose entries are polynomials in the entries of $X$. The condition $Y = \varphi(X)$ is defined by $\frac{n(n+1)}{2}$ linear equations, $n - 2$ quadratic equations, $n - 3$ equations of degree 3, $\ldots$, one equation of degree $n - 1$. Thus, Bezout’s theorem [13, Theorem 7.7, Chapter 1] implies that

$$\deg W \leq 2^{n-2}3^{n-3}\ldots(n-2)^2(n-1) = \prod_{k=1}^{n-1} k!.$$

**4.4.3 Degree bound for reductive groups**

All statements in this section will be about a reductive group $G \subset GL_n(C)$ such that $G \subset N(F)$, where $F \subset GL_n(C)$ is some connected group. In our proofs, $G$ and $F$ will be the reductive and unipotent parts of a Levi decomposition of an arbitrary algebraic group, respectively.

**Lemma 23.** Let $G \subset GL_n(C)$ be a reductive algebraic group such that $G \subset N(F)$ for some connected algebraic group $F \subset GL_n(C)$. Then there is a toric envelope $H \subset N(F)$ of $G$ such that

$$[H : H^0] \leq J(n)A(n-1)n^{n-1}.$$  

*Proof.* Using Corollary 18 we replace $G$ with $GZ_n$, so in what follows we assume that $Z_n \subset G$. 
Due to [38, Lemma 10.10], $G$ can be written as a product $\Gamma G^\circ$ for some finite group $\Gamma \subset GL_n(C)$. [2, Proposition, p. 181] implies that $G^\circ$ can be written as $ST$, where $T := C(G^\circ)^\circ$ is a torus and $S := [G^\circ, G^\circ]$ is semisimple. Since centers and connected components of the identity are characteristic subgroups, $\Gamma$ normalizes $T$.

By the definition of $J(n)$ (see Notation 1), there exists a normal abelian subgroup $\Gamma_{ab} \subset \Gamma$ of index at most $J(n)$. Since $Z_n \subset G$, $T$ contains $Z_n$. Then Lemma 9 implies that $T = Z_n \cdot (T \cap SL_n(C))$. The action of $\Gamma_{ab}$ on $T$ by conjugation defines a group homomorphism $\varphi: \Gamma_{ab} \to \text{Aut}(T \cap SL_n(C))$. Since $T \cap SL_n(C) \cong (C^*)^d$ for some $d \leq n - 1$ (see [26, Problem 10, p. 114]), $\text{Aut}(T \cap SL_n(C)) \cong GL_d(Z)$. Let $\Gamma_0 := \text{Ker}\varphi$. Since $\Gamma_0 = \Gamma_{ab} \cap Z(T)$ and both $\Gamma_{ab}$ and $T$ are normalized by $\Gamma$, $\Gamma_0$ is a normal subgroup in $\Gamma$.

We set $H_0$ to be the intersection of all the maximal tori in $GL_n(C)$ containing $\Gamma_0 \cdot T$. Since $\Gamma_0 \cdot T$ is a quasitorus, it is diagonalizable (see [26, Theorem 3, p. 113]), so there is at least one maximal torus containing $\Gamma_0 \cdot T$. Thus, $H_0$ is a torus. Since $\Gamma_0 \cdot T$ is normalized by $\Gamma$, $H_0$ is also normalized by $\Gamma$. We set $H_1 = H_0 \cap N(S) \cap N(F)$ and

$$H := T_0 \cdot G, \text{ where } T_0 := H_1^\circ. \quad (4.4.2)$$

The lemma follows from the following two claims.

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

$$H = T_0 \cdot G = T_0 \cdot \Gamma \cdot T \cdot S = \Gamma \cdot (T_0 \cdot S). \quad (4.4.3)$$
The latter is a group, because \( T_0 \) normalizes \( S \) and \( \Gamma \) normalizes \( T_0 \) and \( S \).

**Claim 2:** \([H : H^0] \leq J(n)A(n-1)n^{n-1}\). From (4.4.3) we have \( H = (\Gamma \cdot T_0) \cdot (T_0 \cdot S) \).

Since \( T_0 \cdot S \) is connected, \( H \) has at most as many connected components as \( \Gamma \cdot T_0 \).

Since \( T_0 = H_1^0 \), the latter is bounded by the number of connected components of \( \Gamma \cdot H_1 \). We have

\[
\deg(\Gamma \cdot H_1) \leq [\Gamma : \Gamma_0] \cdot \deg H_1 = [\Gamma : \Gamma_{ab}] \cdot [\Gamma_{ab} : \Gamma_0] \cdot \deg H_1. \tag{4.4.4}
\]

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

Since \( H_0 \) is defined by linear polynomials, \( \deg H_0 = 1 \). Since \( H_0 \) is a torus, \( \dim H_0 \leq n \). Since \( \dim (H_0 \cap N(S) \cap N(F)) \geq \dim Z_n = 1 \), Corollary 20 implies that

\[
\deg H_1 = \deg (H_0 \cap N(S) \cap N(F)) \leq n^{n-1}. \tag{4.4.5}
\]

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

**Corollary 24.** In the notation of Lemma 23, if \( G^0 \) is a torus, then \( \deg H \leq J(n)A(n-1)n^{n-1} \).

**Proof.** In this case, \( S \) from the proof of Lemma 23 is trivial. Since \( T \subset T_0 \), \( H = \Gamma \cdot T_0 \).

Then \( \deg H \leq (\deg \Gamma \cdot H_1) \). The latter is bounded by \( J(n)A(n-1)n^{n-1} \) due to (4.4.4) and (4.4.5). \( \square \)
Lemma 25. Let $G \subset GL_n(C)$ be a connected reductive group such that $G \subset N(F)$ for some connected group $F \subset GL_n(C)$. Then there exists a toric envelope $H \subset N(F)$ of $G$ such that

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

Proof. Using Corollary 18 we may replace $G$ with $GZ_n$, so we will assume that $Z_n \subset G$. We set

$$H := (Z(G) \cap Z(Z(G)) \cap N(F))^0 \cdot G.$$

The lemma follows from the following three claims

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

Since $G$ is reductive, its representation in $C^n$ is completely reducible (see [15, Theorem 4.3, p. 117]). Let $C^n = V_1 \oplus V_2 \oplus \ldots \oplus V_\ell$ be a decomposition of $C^n$ into isotypic components. Each $V_i$ can be written as $W_i \otimes C^{m_i}$, where $W_i$ is the corresponding irreducible representation of $G$ and $C^{m_i}$ is a trivial representation. Let $d_i := \dim W_i$ for $1 \leq i \leq \ell$. Then Schur’s lemma implies that

$$Z(G) = \bigoplus_{i=1}^\ell (C^* I_{d_i} \otimes GL_{m_i}(C)),$$

where $I_{d_i}$ is a $d_i \times d_i$ identity matrix.

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

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

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

Let \( g := \text{Lie}(G) \) and \( s := \text{Lie}(S) \). Consider an element \( a \in n(s) \). The map \( s \rightarrow s \) defined by \( g \mapsto [a, g] \) satisfies the requirements of Whitehead’s lemma [19, Lemma 3, p. 77].

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

\[ n(s) = s \oplus \mathfrak{z}(s). \]  

(4.4.6)

Decomposition (4.4.6) implies that

\[ N(S)^\circ = S \cdot Z(S)^\circ. \]  

(4.4.7)

We can write \( \hat{H}^{\circ} \) as follows

\[ \hat{H}^{\circ} = (N(S) \cap Z(Z(G)) \cap N(F))^{\circ} = (N(S) \cap Z(Z(G)) \cap N(F))^{\circ} = (\text{using (4.4.7)}) = \]

\[ = ((S \cdot Z(S)^\circ) \cap Z(Z(G)) \cap N(F))^{\circ} = (\text{using } S \subset Z(Z(G)) \cap N(F)) = \]

\[ = (Z(S)^\circ \cap Z(Z(G)) \cap N(F))^{\circ} \cdot S = (\text{using } Z(Z(G)) \subset Z(T)) = \]

\[ = ((Z(S) \cap Z(T)) \cap Z(Z(G)) \cap N(F))^{\circ} \cdot S = (Z(G) \cap Z(Z(G)) \cap N(F))^{\circ} \cdot S = \]

\[ = (\text{using } T \subset Z(G) \cap Z(Z(G)) \cap N(F)) = (Z(G) \cap Z(Z(G)) \cap N(F))^{\circ} \cdot G = H \]

Thus, \( \deg H \leq \deg \hat{H} \). Since any centralizer is defined by linear equations, \( \deg Z(Z(G)) = 1 \).

Due to Corollary 20
\[ \deg \hat{H} \leq n^{\dim Z(G)} \cdot \deg \hat{H} \deg Z(G) \leq n^{n^2 - \dim G}. \]

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

**Lemma 26.** Let \(G \subset GL_n(C)\) be a reductive subgroup such that \(G \subset N(F)\) for some connected group \(F \subset GL_n(C)\). Then there exists a toric envelope \(H \subset N(F)\) of \(G\) such that
\[ \deg H \leq J(n)A(n-1)n^{n^2+n-5}. \]

**Proof.** Using Corollary 18, we may replace \(G\) with \(GZ_n\), so we will assume that \(Z_n \subset G\). In the case that \(G^{\circ}\) is a torus, the lemma follows from Corollary 24. Otherwise, \(\dim G \geq \dim Z_n + \dim SL_2(C) = 4\).

Since being a toric envelope is a transitive relation (see Corollary 16), applying Lemma 23, we will further assume that \([G : G^{\circ}] \leq J(n)A(n-1)n^{n-1}\). [38, Lemma 10.10] implies that \(G = \Gamma G^{\circ}\) for some finite group \(\Gamma\). Lemma 25 implies that there exists a toric envelope \(H_0 \subset N(F)\) of \(G^{\circ}\) such that \(N(G^{\circ}) \cap N(F) \subset N(H_0)\) and \(\deg H_0 \leq n^{n^2-4}\). Let \(H := \Gamma H_0\). Since \(\Gamma \subset N(G^{\circ}) \cap N(F) \subset N(H_0)\), \(H\) is an algebraic group. Since \(G^{\circ} \subset H_0\), \(G \subset H\). Since \(H^{\circ} = H_0\), all unipotent elements of \(H^{\circ}\) belong to \(G^{\circ}\). Since also \(H^{\circ}G \supset H^{\circ}\Gamma = H\), Lemma 15 implies that \(H\) is a toric envelope of \(G\).
Since $H = H_0G$ where $H_0 = H^\circ$, $[H : H^\circ] \leq [G : G^\circ]$. Then

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

\[\square\]

### 4.4.4 Degree bound for product

**Lemma 27.** Let $G = G_0 \cdot U \subset GL_n(C)$, where $U$ is a connected unipotent group, $G_0$ is a reductive group, and $G \subset N(U)$. Let $\deg G_0 = D_1$, $\deg U = D_2$. Then $\deg G \leq D_1D_22^{n(n-1)/2}$.

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

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

There exists $s < n$ such that $V_1 \not\subset V_2 \not\subset \ldots \not\subset V_s = C^n$. Since $G_0$ normalizes $U$, $V_i$ is invariant with respect to $G_0$ for every $i \geq 0$. Since $G_0$ is reductive, there exists a decomposition $V_i = V_{i-1} \oplus W_i$ into a direct sum of $G_0$-representations for every $1 \leq i \leq s$. Thus, there is a decomposition $C^n = W_1 \oplus \ldots \oplus W_s$ into a direct sum of $G_0$-invariant subspaces. Let $n_i := \dim W_i$ for $1 \leq i \leq s$. We fix a basis of $C^n$ that is a union of bases of $W_1, \ldots, W_s$. In this basis, every element of $G_0$ is of the form

$$\begin{pmatrix}
X_1 & 0 & \ldots & 0 \\
0 & X_2 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & X_s
\end{pmatrix}, \text{ where } X_i \in Mat_{n_i}(C) \text{ for every } 1 \leq i \leq s. \quad (4.4.8)$$

And every element of $U$ is of the form

$$\begin{pmatrix}
I_{n_1} & Y_{12} & \ldots & Y_{1n} \\
0 & I_{n_2} & \ldots & Y_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & I_{n_s}
\end{pmatrix}, \text{ where } Y_{ij} \in Mat_{n_i,n_j}(C) \text{ for every } 1 \leq i < j \leq s. \quad (4.4.9)$$
CHAPTER 4. GENERAL BOUNDS FOR PROTO-GALOIS GROUPS

We denote the spaces of all the invertible matrices of the form (4.4.8) and (4.4.9) by $\mathcal{D}$ and $\mathcal{T}$, respectively. Consider the following variety

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

Let $\pi: \mathcal{D} \times \mathcal{T} \times GL_n(C) \rightarrow GL_n(C)$ be the projection onto the last coordinate. Then $G = \pi(P)$, so $\deg G \leq \deg P$. Consider $P$ as an intersection of the variety $G_0 \times U \times GL_n(C)$ of degree $D_1D_2$ with the variety defined by the $n^2$ equations $XY = Z$. Since the product $XY$ is of the form

$$(X_1 \begin{bmatrix} X_{11} & X_{12} & \ldots \end{bmatrix} \begin{bmatrix} Y_1 \ldots Y_n \end{bmatrix} \begin{bmatrix} X_2 \ldots X_n \end{bmatrix} \begin{bmatrix} \ldots \ldots \end{bmatrix} \begin{bmatrix} 0 \ldots X_n \end{bmatrix})
$$

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

$$\frac{n(n-1)}{2} - \frac{n_1(n_1-1)}{2} - \ldots - \frac{n_s(n_s-1)}{2} \leq \frac{n(n-1)}{2}$$

quadratic polynomials and the rest are linear. Thus, $\deg G \leq \deg P \leq D_1D_22^{n(n-1)/2}$.

4.5 Proof of Theorem 12

Proof of Theorem 12. Due to [26, Theorem 4, p. 286], $G$ can be written as a semidirect product $G_0 \rtimes U$, where $U$ is the unipotent radical of $G$ and $G_0$ is a reductive subgroup of $G$.

We apply Lemma 26 with $G = G_0$ and $F = U$ and obtain a toric envelope $H_s \subset N(U)$ of $G_0$. Let $H_s = T \cdot G_0$, where $T$ is a torus. We set $H := H_s \cdot U$. Since
$H_s \subset N(U)$, $H$ is an algebraic group. Since $H = T \cdot G_0 \cdot U = T \cdot G$, $H$ is a toric envelope of $G$. Corollary 17 implies that $H_s$ is reductive. Then Lemma 27 implies that

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

Using bounds for $H_s$ and $U$ from Lemmas 26 and 22, respectively, we obtain

$$\deg H \leq J(n) A(n - 1) n^{n^2 + n - 5/2} \prod_{k=1}^{n-1} k!.$$  \hspace{1cm} (4.5.1)$$

Using $\sqrt{8n} + 1 < \sqrt{16n}$ and (4.4.1), we derive $J(n) \leq 4^{2n^2} n^{n^2}$. Using Lemma 21 and $2 \cdot 3^{(n-1)^2/4} \leq 4^{n^2}$, we derive $A(n - 1) \leq 4^{n^2}$. Using $n! \leq (n/2)^n$, we derive

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

Substituting all these bounds to (4.5.1), we obtain $\deg H \leq (4n)^{3n^2}$. \hfill \Box
Chapter 5

Complexity of Triangular Set Representation

Sun showed in [31] that yet another way to obtain an improved bound for proto-Galois groups, (as opposed to seeking defining equations for the group instead of the corresponding radical ideal), is to use triangular sets in place of Gröbner bases in Feng’s analysis. Care has to be taken there, as triangular sets do not function exactly like Gröbner bases. But Sun was able to show that these replacements do not impede the algorithm and that they achieve a smaller upper bound for the degree of a representation of a proto-Galois group. Moreover, if one uses the triangular representation from Szanto’s algorithm to then compute a Gröbner basis for the corresponding ideal, Sun’s work also demonstrates that one can expect significantly lower degrees than those suggested by Feng’s bound.

The complexity analysis presented in the current chapter contributed to obtaining a better bound for the complexity analysis of the first step of Hrushovski’s algorithm. This work is also of interest in the complexity analysis of other algorithms from
computational algebra, as it addresses the general consideration of degree bounds for representing an algebraic set by a collection of triangular sets and is not specific to proto-Galois groups.

5.1 Introduction

The general problem considered here is: given polynomials $f_0, \ldots, f_r \in k[x_1, \ldots, x_n]$, where $k$ is a computable subfield of $\mathbb{C}$, represent the set of all polynomials vanishing on the set of solutions of the system $f_0 = \ldots = f_r = 0$. This set of polynomials is called the radical of the ideal generated by $f_0, \ldots, f_r$. The problem is important for computer algebra and symbolic computations, as well as for their applications (for example, [27, 3]). 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. The main result of this section is the first complete bound on the degrees (Theorem 35) and the number of components (Theorem 37) for the algorithm designed by Szanto in [33] for computing a triangular decomposition.

An upper bound on the degrees of elements of a Gröbner basis for the radical of a given ideal, one that is doubly-exponential in the number of variables, was given by Laplagne in [22]. Moreover, an example constructed in [4] by Chistov 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 \cite{12, 23, 24} (for prior results in this direction, see references in \cite{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 (\cite{28, 8}), an efficient algorithm for zero-dimensional varieties (\cite{7}), and implementations (\cite{37, 1}). However, to the best of our knowledge, there are only a few algorithms, (specifically those in\cite{10, 33, 28}), for computing triangular decomposition with proven degree upper bounds for the output. The algorithms in \cite{28} and \cite{10} have restrictions on the input polynomial system. The algorithm in \cite{28} requires the system to define an irreducible variety. The algorithm in \cite[Theorem 4.14]{10} produces a characteristic set of an ideal, which represents the radical of the ideal only if the ideal is characterizable, (in the sense of \cite[Definition 5.10]{17}; for example, an ideal defined by $x_1x_2$ is not characterizable). Together with \cite[Proposition 5.17]{17}, this means that the algorithm from \cite{10} represents the radical of an ideal if the radical can be defined by a single regular chain.

The algorithm designed by Szanto in \cite{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 5.4). Moreover, in Example 6 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. In this section, we take these extra components into account and
prove an explicit degree bound of the form $d^{O(m^3)}$ for the algorithm. More precisely,
we prove that:

**Theorem.** [Theorem 35] 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 Szanto’s algorithm or during the computation
does not exceed

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

where $\epsilon$ is some decreasing function of $m, d$ and $\epsilon$ is bounded by 5 (for a more general
statement, we refer to Section 5.4).

**Theorem.** [Theorem 37] 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 the codimensions of prime components of
$\sqrt{(F)} \subseteq k[x_1, \ldots, x_n]$. Then the number of squarefree regular chains in the output of
Szanto’s algorithm applied to $F$ is at most

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

### 5.2 Preliminaries

Throughout this section, 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 $\text{height}(p) := \max_i \deg_{x_i}(p)$. The highest indeterminate appearing in $p$ is called its leader and will be defined by $\text{lead}(p)$. By $\text{lc}(p)$ we denote the leading coefficient of $p$ when $p$ is written as a univariate polynomial in $\text{lead}(p)$.

**Definition 14.** Given a sequence $\Delta = (g_1, g_2, \ldots, g_m)$ in $R$, we say that $\Delta$ is a **triangular set** if $\text{lead}(g_i) < \text{lead}(g_j)$ for all $i < j$.

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

Triangular sets give rise to ideals via the following notion.

**Definition 15.** Let $f, g \in R$ with $\text{lead}(g) = x_j$. 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 $\alpha$ be the smallest nonnegative integer such that $g := \text{lcf}(g)^\alpha \tilde{g}$ and $r := \text{lcf}(g)^\alpha \tilde{r}$ are polynomials, so that we obtain an equation of the form

$$\text{lcf}(g)^\alpha f = qg + r$$

with $q, r \in R, \text{deg}_x(r) < \text{deg}_x(g), \alpha \in \mathbb{N}$. One can show that $\alpha \leq \text{deg}_x(f) - \text{deg}_x(g) + 1$. For uniqueness of $q, r$, we require $\alpha$ to be minimal. We say that $r$ is pseudoremainder of $f$ by $g$ and denote it by $\text{sprem}(f, g)$.

**Definition 16.** 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 $\Delta$ is the polynomial $f_0$ in the sequence $f_m = f, f_{s-1} = \text{sprem}(f_s, g_s), 1 \leq s \leq m$. We denote $f_0$ by $\text{sprem}(f, \Delta)$.

We say that $f$ is reduced with respect to $\Delta$ if $f = \text{sprem}(f, \Delta)$.

**Remark.** The computation of the pseudoremainder of $f$ with respect to $\Delta$ gives rise to the equation

$$\text{lcm}(g_m)^{\alpha_m} \cdots \text{lcm}(g_1)^{\alpha_1} f = \sum_{s=1}^{m} q_s g_s + f_0$$

where each $\alpha_s \leq \text{deg}_{\text{lead}(g_s)}(f_s) - \text{deg}_{\text{lead}(g_s)}(g_s) + 1$.

**Definition 17.** Given a triangular set $\Delta$ in $R$, we define the ideal

$$\text{Rep}(\Delta) := \{ p \in R \mid \exists N : H^N p \in \langle \Delta \rangle \}, \text{ where } H := \text{lcf}(g_1) \cdots \text{lcf}(g_m)$$

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

**Definition 18.** 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 $\text{Ass}(I)$. When $I = \text{Rep}(\Delta)$, we will write $\text{Ass}(\Delta)$ instead of $\text{Ass}(I)$.

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

**Definition 19.** Let $\Delta = (g_1, g_2, \ldots, g_m)$ be a triangular set of $R$ with $I = \text{Rep}(\Delta)$ 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 $\text{Rep}(\Delta_i)$.

(a) if $\text{lcm}(g_{i+1}) \notin P_{i,j}$ for every $1 \leq i \leq m - 1$ and $1 \leq j \leq r_i$, then $\Delta$ is called a \textit{regular chain}, see [17, Definition 5.7].

(b) if $g_{i+1}$ is square-free over $K(P_{i,j}) := \text{Quot}(R/P_{i,j})$ for every $1 \leq j \leq r_i$ and $1 \leq j \leq r_i$, then $\Delta$ is called a \textit{squarefree regular chain}, see [17, Definition 7.2] (Here, Quot($R/P_{i,j}$) is the field of fractions of $R/P_{i,j}$.)

**Theorem 28** (see [3, Proposition 2.7]). If $\Delta$ is a regular chain, then $\text{Rep}(\Delta) = \{h \in R | \text{sprem}(h, \Delta) = 0\}$ and all of the prime ideals in the irredundant prime decomposition of $\text{Rep}(\Delta)$ have the same dimension.

**Theorem 29** (see [17, Corollary 7.3]). If $\Delta$ is a squarefree regular chain, then $\text{Rep}(\Delta)$ is a radical ideal.

**Remark.** 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].
CHAPTER 5. COMPLEXITY OF TRIANGULAR SET REPRESENTATION

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

**Definition 20.** The triangular decomposition of an ideal $I \subset R$ is a set $\{\Delta_1, \ldots, \Delta_s\}$ of squarefree regular chains such that

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

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

**Definition 21.** Let $\Delta = (g_1, \ldots, g_m)$ be a triangular set in $R$ with $\text{lead}(g_s) = x_{l+s}$ 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 $M(\Delta)$ (when considered as polynomials in the variables $x_{l+1}, \ldots, x_n$).
CHAPTER 5. COMPLEXITY OF TRIANGULAR SET REPRESENTATION 48

We denote this quantity by $\Gamma(\Delta)$ or $\Gamma$ when the triangular set under consideration is clear from context. We will also use the notation $\Gamma_j$ for $\Gamma(\Delta_j)$.

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

**Proposition 30** (see [33, Prop. 3.3.1, p.76]). Let $\Delta$ 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 $\prod_{s=1}^m \text{lc}(g_s)^{\beta_s}$ and also assume that $\sum_{s=1}^m \beta_s \cdot \text{height}(\text{lc}(g_s)) \leq d'$. Then

- $\text{height}(a_1a_2) \leq \text{height}(a_1) + \text{height}(a_2) + 2(d' + \Gamma)$ and
- $\text{height}(a_1a_2 \ldots a_k) \leq kd + k \log k (d' + \Gamma)$.

In Proposition 30, 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 $\Delta$.

**Lemma 31.** Let $\Delta := (g_1, \ldots, g_m) \subset k[x_1, \ldots, x_n]$ be a squarefree regular chain such that $\text{height}(g_s) \leq d$ 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:

- $\text{lc}(g_1)^{\alpha_1} \ldots \text{lc}(g_m)^{\alpha_m} \cdot f = q_1g_1 + \cdots + q_mg_m + f_0$. 

CHAPTER 5. COMPLEXITY OF TRIANGULAR SET REPRESENTATION

• \( f_0 \) is reduced modulo \( \Delta \), and

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

**Proof.** Similar to [3, Lemma 3.7].

**Remark.** Gallo and Mishra gave a bound in [10, 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 31. In the table below, OB stands for “Our Bound” and GM stands for “Gallo-Mishra.”

<table>
<thead>
<tr>
<th>( \text{deg}(f_0) )</th>
<th>( \text{height}(g_s) \leq d ) &amp; ( \text{height}(f) \leq t )</th>
<th>( \text{deg}(g_s) \leq d ) &amp; ( \text{deg}(f) \leq t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>OB: ( nt(d + 1)^m )</td>
<td>GM: ( (nt + 1)(nd + 1)^m )</td>
<td>OB: ( nt(d + 1)^m )</td>
</tr>
<tr>
<td>GM: ( (nt + 1)(nd + 1)^m )</td>
<td>GM: ( (t + 1)(d + 1)^m )</td>
<td></td>
</tr>
</tbody>
</table>

We see that the only case in which the bound from [10, Lemma 5.2] is smaller than the corresponding one derived from Lemma 31 is represented by the upper-right cell, in which solely degrees are considered. In fact, [10] 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.

### 5.3 Outline of Szanto’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 in 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

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

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

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

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

(b) For every $i \subsetneq \{1, \ldots, n\}$, compute the multiplication table $M(\Delta_i)$ of the algebra $A(\Delta_i)$ (see Definition 21).

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

$$\text{unmixed}^{[i]}_{\Delta_i}(\Delta_i, M(\Delta_i), f, 1),$$

using Algorithm 2 below.

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

---

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**.

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 $1 \leq s \leq m$
lead\(g_s) = x_{l+s};
\lc(g_s) \in k[x_1, \ldots, x_l];
\quad g_s is reduced modulo \{g_1, \ldots, g_{s-1}\}.

3. The multiplication table \(M(\Delta)\) of the algebra \(A(\Delta)\), see Definition 21.

4. Polynomials \(f, h\) in \(k[x_1, \ldots, x_{n+c}]\) for some \(c > 0\) reduced with respect to \(\Delta\).

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

- \(\Delta_i\) 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 \(1 \leq i \leq r\);
- \(\bigcup_{i=1}^{r} \Ass(\Delta_i) = \{P \in \Ass(\Delta) \mid f \equiv 0, h \neq 0 \mod P\}\) (see Definition 18);
- \(\Ass(\Delta_i) \cap \Ass(\Delta_j) = \emptyset \forall i \neq j\).

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

Informally speaking, the main goal of \textbf{unmixed} is to transform a single regular chain \(\Delta\) 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 \(\bigcap_{i=1}^{r} \Rep(\Delta_i)\) are exactly the prime components of \(\Rep(\Delta)\),

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 in which all regular chains consist of a single polynomial.
only. This case is also discussed in [33, p. 124-125]. Let \( \Delta \) consist \( g(x) \in k[x] \). A polynomial satisfying only property (b) can be computed using gcd’s as follows

\[
g(x, f) = \frac{\gcd_x(g, f)}{\gcd_x(g, f, h)}.
\] (5.3.1)

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

\[
g(x, f) = \frac{\gcd_x(g, g', g'')}{\gcd_x^2(g, g')}, \frac{\gcd_x(g, g')}{\gcd_x^2(g, g')}, \ldots
\] (5.3.2)

Formulas (5.3.1) and (5.3.2) can be combined to yield to a set of polynomials satisfying both properties (a) and (b):

\[
q_i := \frac{\gcd_x(g, \ldots, g^{(i-1)}, f) \gcd_x(g, \ldots, g^{(i+1)}, f) \gcd_x^2(g, \ldots, g^{(i)}, f, h)}{\gcd_x^2(g, \ldots, g^{(i)}, f) \gcd_x(g, \ldots, g^{(i+1)}, f, h)}, \quad i = 1, \ldots, \deg g.
\] (5.3.3)

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 (5.3.3) is replaced then by

\[
q_i := \frac{\ggcd_{x_n}(\Lambda, g_m, \ldots, g^{(i-1)}, f) \ggcd_{x_n}(\Lambda, g_m, \ldots, g^{(i+1)}, f) \ggcd_{x_n}^2(\Lambda, g_m, \ldots, g^{(i)}, f, h)}{\ggcd_{x_n}^2(\Lambda, g_m, \ldots, g^{(i)}, f) \ggcd_{x_n}(\Lambda, g_m, \ldots, g^{(i-1)}, f, h) \ggcd_{x_n}(\Lambda, g_m, \ldots, g^{(i+1)}, f, h)}
\] (5.3.4)

for \( i = 1, 2, \ldots, \deg_{x_n} g_m \).
CHAPTER 5. COMPLEXITY OF TRIANGULAR SET REPRESENTATION  53

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 \texttt{unmixed} function splits $\text{Rep}(\Lambda)$ into a union of varieties represented by regular chains, over which all the generalized gcds in (5.3.4) will be well defined. Interestingly, this can be done by calling \texttt{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 unmixed\(_m^l(\Delta, M(\Delta), f, h)\)

Input and output are described in the specification above.

(a) If \(m = 0\) (so \(\Delta = \emptyset\)), return \(\emptyset\) if \(f \neq 0\) or \(h = 0\), and return \(\{(\emptyset, \emptyset)\}\) 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 \(v \in \mathbb{Z}_{\geq 0}^6\) with entries not exceeding \(\deg_{x_n} g_m\), define a pair of polynomials \(\phi_{i,v}, \psi_{i,v}\) such that a system \(\phi_{i,v} = 0, \psi_{i,v} \neq 0\) is equivalent to
   - \(f = 0\) and \(h \neq 0\),
   - all six generalized gcds in (5.3.4) are well-defined and their degrees are the entries of \(v\).

Formulas for \(\phi_{i,v}\) and \(\psi_{i,v}\) are given in the proof of Lemma 34 and in [33, p. 128].

(d) For every pair \((\phi_{i,v}, \psi_{i,v})\) computed in the previous step
   (i) Compute \(L_{i,v} := \text{unmixed}_{m-1}^l(\Lambda, M(\Lambda), \phi_{i,v}, \psi_{i,v})\).
   (ii) For every \((\Lambda_{i,v}, M(\Lambda_{i,v})) \in L_{i,v}\) compute \(q_{i,v}\) using (5.3.4) (more details in the proof of Theorem 33 and in [33, p. 129-130])
   (iii) For every \(q_{i,v}\) computed in the previous step, add \((\Lambda_{i,v} \cup \{q_{i,v}\}, M(\Lambda_{i,v} \cup \{q_{i,v}\}))\) to the output

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

Example 6. In this example, we will show that the output of Algorithm 1 can be redundant confirming [3, Remark 2.9]. We fix a positive integer \(D\) and consider

\[
F := \{(x_1 - 1)(x_1 - 2) \ldots (x_1 - D)(x_2 - 1)(x_2 - 2) \ldots (x_2 - D)\}. \tag{5.3.5}
\]

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

\[ \Delta_1 = \Delta_2 = \{(x_1 - 1)(x_1 - 2)\ldots(x_1 - D)(x_2 - 1)(x_2 - 2)\ldots(x_2 - D)\}, \]

\[ \Delta_0 = \{(x_1 - 1)(x_1 - 2)\ldots(x_1 - D)p_1(x_1), (x_2 - 1)(x_2 - 2)\ldots(x_2 - D)p_2(x_2)\}, \]

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, \( \text{unmixed}^0_2(\Delta_0, M(\Delta_0), f, 1) \) will be computed. According to the specification of \( \text{unmixed} \), the result of this computation will be a triangular decomposition of the set of common zeros of \( \text{Rep}(\Delta_0) \) and \( F \). Since the zero set of \( \text{Rep}(\Delta_0) \) is finite, all these components are not components of the zero set of \( F \). Points \( \{(a_1, a_2)|a_1, a_2 \in \{1, 2, \ldots, D\}\} \) are common zeros of \( \text{Rep}(\Delta_0) \) 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 (5.3.5) by

\[ F := \{(x_1 - 1)(x_1 - 2)\ldots(x_1 - D)\ldots(x_n - 1)(x_n - 2)\ldots(x_n - D)\}. \]

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

## 5.4 Bounds for degrees

The following lemma is a refinement of [33, Proposition 3.3.4, p. 75].
Lemma 32. 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. $\text{lc}(g_s) \in k[x_1, \ldots, x_l];$
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 21) does not exceed

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

Proof. We first apply the matrix description of the pseudoremainder (see Appendix A: Matrix Representation of Pseudoremainder) to products of the form $x_1^{e_1} x_2^{e_2} \cdots x_l^{e_l}$, 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 A: Matrix Representation of Pseudoremainder. Also, what we called $g$ in the Appendix A: Matrix Representation of Pseudoremainder will be $g_m$ in our application, as that is the first element we pseudo-divide by in reducing by $\Delta$.

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 $\Delta$ by taking the maximum of $\Gamma_{m-1} := \Gamma(\Delta_{m-1})$ and $d_m$. 
In the second case, what we denote by \( f_{\text{low}} \) in the Appendix A: Matrix Representation of Pseudoremainder is here a column vector with every entry 0 and what we denote by \( f_{\text{up}} \) has exactly one nonzero entry, namely \( x_{e_1}^{e_1} x_{e_2}^{e_2} \ldots x_{e_{m-1}}^{e_{m-1}}. \)

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 \( \Delta_{m-1} \).)

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

So by Proposition 30 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

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

Combining these inequalities, we have

\[
\Gamma_m \leq \left[ (d + 2)^2 \cdot \sum_{k=0}^{m-2} ((d + 2) \log(d + 2))^k \right] + ((d + 2) \log(d + 2))^{m-1} \Gamma_1.
\]
Since the sum in brackets is a finite geometric series with \( m - 1 \) terms and \( \Gamma_1 \leq d^2 \), we have

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

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

**Theorem 33.** Let \( \Delta = (g_1, \ldots, g_m) \subset k[x_1, \ldots, x_n] \) 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. 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 \( A(\Delta) \). For \( f, h \in A(\Delta)[x_{n+1}, \ldots, x_{n+c}] \), denote \( d_f := \text{height}(f) \) and \( d_h := \text{height}(h) \). Then for each polynomial \( p \) occurring in the computation of \( \text{unmixed}_m(\Delta, M(\Delta), f, h) \) (see Algorithm 2), we have:

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

**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

\[
\{(\Delta_1, M(\Delta_1)), \ldots, (\Delta_r, M(\Delta_r))\} := \text{unmixed}_m(\Delta, M(\Delta), f, h)
\]
be the output of the algorithm $\text{unmixed}_m$ 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
\[
\tilde{d}_s := \max \left\{ \deg_{x_{s+j}} (g_{s,j}) \mid j = 1, \ldots, r \right\} \tag{5.4.1}
\]

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

\[
\text{unmixed}_m(\Delta_m, M(\Delta_m), f_m, h_m), \ldots, \text{unmixed}_0(\Delta_0, M(\Delta_0), f_0, h_0)
\]

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

Then
\[
\text{Input}(s) \leq (6d)^{m-s} \left( \text{Input}(m) + 7(d + 2)^m (\log(d + 2))^{m-1} \right).
\]

**Proof.** We give an inductive analysis to obtain a bound on $\text{Input}(s)$. 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
\[
\varphi_k^{(j)}(y, z) := \text{Res}_{x_n}^{(j)} \left( g_m, f_m + \sum_{l=1}^{k} g_m^{(l)} y^{l-1} + zh_m \right),
\]
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 $\mathbf{v} = (v_1, \ldots, v_6) \in \mathbb{Z}_{\geq 0}^6$, 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 $\Lambda$.

(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 $x_{i+1}$ 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 $\Delta$.

Since $f_{m-1}, h_{m-1}$ must be reduced modulo $\Delta_{m-1}$, we will carrying out all opera-
tions 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 $\text{Input}(m - 1)$.
In fact, our technique will give us a bound for $\text{Input}(s)$ in terms of $\text{Input}(s + 1)$.

Since the computation of $h_{m-1}$ involves a multiplication of six evaluated subresul-
tants, we apply Proposition 30 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 30 yields:

\[
\text{height}(CD) \leq \text{height}(C) + \text{height}(D) + 2\log(2) \cdot (\Gamma(\Delta_{m-1}) + d')
\]

\[
\leq 6d_m \cdot d + 6d_m \cdot \text{Input}(m) + 12d_m \log(6d_m) \cdot \Gamma(\Delta_{m-1}) + 2 \cdot (\Gamma(\Delta_{m-1}) + d')
\]

\[
\leq 6d^2 + 6d \cdot \text{Input}(m) + 12d \log(6d) \cdot \Gamma(\Delta_{m-1}) + 2 \cdot (\Gamma(\Delta_{m-1}) + d')
\]

We need to bound \(d'\) by considering the sequence of exponents we obtain on \(\text{lc}(g_i)\) when reducing \(C, D\) modulo \(\Delta_{m-1}\). Applying Lemma 31 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

\[
\text{height}(h_{m-1}) \leq 6d^2 + 6d \cdot \text{Input}(m) + 12d \log(6d) \cdot \Gamma(\Delta_{m-1}) + 2 \cdot (\Gamma(\Delta_{m-1}) + 6d^2(d + 1)^{m-1} - 6d^2).
\]

As a result, we have

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

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

\[
\text{Input}(s) \leq \Gamma(\Delta_s) \cdot (12d \log(6d) + 2) + 6d \cdot \text{Input}(s + 1) + 12d^2(d + 1)^s
\]

for every \(s = 0, \ldots, m - 1\). Due to Lemma 32

\[
\Gamma(\Delta_s) \leq (d + 2)^{s+1}(\log(d + 2))^{s-1}.
\]
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
\[
\text{Input}(s) \leq 17 \cdot (d + 2)^{s+2}(\log(d + 2))^s + 6d \cdot \text{Input}(s + 1) + 12(d + 1)^{s+2}
\]
for \( s = 0, 1, \ldots, m - 1 \). Thus, \( \text{Input}(s) \) does not exceed
\[
(6d)^{m-s} \cdot \text{Input}(m) + 6 \cdot (d^2 + 2m)(\log(d + 2))^{m-1} + 12(6d)^{m+2}.
\]
Using the formula for geometric series and \( d \geq 2 \), we can deduce that
\[
\text{Input}(s) \leq (6d)^{m-s} \left( \text{Input}(m) + 6(d + 2)^m(\log(d + 2))^{m-1} + 3.1(d + 1)^m \right).
\]
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
\[
(6d)^{m-s} \left( \text{Input}(m) + 7(d + 2)^m(\log(d + 2))^{m-1} \right).
\]

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

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

1. Compute $d_{t,i,v_1}$, $1 \leq t \leq 6$, defined by (see [33, p. 127])

$$d_{1,i,v_1} := \gcd_{x_n} (\Lambda_{i,v} \cup \{g_m\}, g_m', \ldots, g_m^{(i-1)}, f_m)$$

$$d_{2,i,v_2} := \gcd_{x_n} (\Lambda_{i,v} \cup \{g_m\}, g_m', \ldots, g_m^{(i)}, f_m)$$

$$d_{3,i,v_3} := \gcd_{x_n} (\Lambda_{i,v} \cup \{g_m\}, g_m', \ldots, g_m^{(i+1)}, f_m)$$

$$d_{4,i,v_4} := \gcd_{x_n} (\Lambda_{i,v} \cup \{g_m\}, g_m', \ldots, g_m^{(i-1)}, f_m, h_m)$$

$$d_{5,i,v_5} := \gcd_{x_n} (\Lambda_{i,v} \cup \{g_m\}, g_m', \ldots, g_m^{(i)}, f_m, h_m)$$

$$d_{6,i,v_6} := \gcd_{x_n} (\Lambda_{i,v} \cup \{g_m\}, g_m', \ldots, g_m^{(i+1)}, f_m, h_m)$$

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

2. Compute

$$\mathbf{lc}(d_{t,i,v_1}) := \text{pinvert}_{m-}^l (\Lambda_{i,v}, M(\Lambda_{i,v}), \mathbf{lc}(d_{t,i,v_1}))$$

for $1 \leq t \leq 6$, where the function $\text{pinvert}_{m}^l (\Delta, M(\Delta), f)$ for computing the pseudo-inverse of $f$ has the following specification (see also [33, Section 3.4])

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

$M(\Delta)$: the multiplication table of $A(\Delta)$ (see Definition 21);

$f$: a polynomial in $k[x_1, \ldots, x_{l+m}]$ such that $f \not\in P$ for every $P \in \text{Ass}(\Delta)$;

Generalized gcd ($\gcd$) is described in [33, Lemma 3.1.3].
\textbf{Out} \ \bar{f} \in k[x_1, \ldots, x_{m+l}] \text{ such that } \bar{f} \cdot \bar{f} \equiv r \pmod{\text{Rep}(\Delta)}, \\text{where } r \in k[x_1, \ldots, x_l] \setminus \{0\}.

3. Compute \(d_{t,i,v} := \text{lc}(d_{t,i,v}) \cdot d_{t,i,v} \) for \(1 \leq t \leq 6\).

4. Compute

\[
p_{i,v}^{(1)} := \bar{d}_{1,i,v_1} \cdot \bar{d}_{3,i,v_3} \cdot \bar{d}_{5,i,v_5} \quad \text{and} \quad p_{i,v}^{(2)} := \bar{d}_{2,i,v_2} \cdot \bar{d}_{4,i,v_4} \cdot \bar{d}_{6,i,v_6},
\]

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

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

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

\textbf{Step 1.} The construction of \text{gcd} in [33, Lemma 3.1.3] implies that \(\text{height}(d_{t,i,v}) \leq \text{Input}(m-1)\) for every \(t = 1, \ldots, 6\).

\textbf{Step 2.} We denote by \(D_{m-1}\) the dimension of the algebra \(A(\Delta)\) over \(k\). Then \(D_{m-1} = \prod_{i=1}^{m-1} \bar{d}_i\) (see (5.4.1)). The coefficients of \(\text{lc}(d_{t,i,v})\) 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

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

Therefore

\[
\text{height}(\text{lc}(d_{t,i,v})) \leq (D_{m-1} - 1)(\text{Input}(m-1) + \text{Output}(m-1)).
\]
CHAPTER 5. COMPLEXITY OF TRIANGULAR SET REPRESENTATION  66

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

\[
\text{height}(\overline{d}_{t,i,v_t}) \leq \text{height}(\overline{lc}(d_{t,i,v_t})) + \text{height}(d_{t,i,v_t}) + 2 \log 2 \cdot \Gamma(\Lambda_{i,v})
\]

\[
= D_{m-1} \text{Input}(m - 1) + (D_{m-1} + 1) \text{Output}(m - 1).
\]

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

\[
\text{height}(q_{i,v}) \leq 16d \cdot \max_{t=1,\ldots,6} \{\text{height}(\overline{d}_{t,i,v_t})\} + 16d \log(16d) \cdot \Gamma(\Lambda_{i,v})
\]

\[
\leq (16dD_{m-1} + 16d + 16d \log(16d)) \text{Output}(m - 1) + 16dD_{m-1} \text{Input}(m - 1).
\]

Step 5. As the last step of the computation at level $m$, we compute the multiplication table $M(\Delta_{i,v})$ for the algebra $A(\Delta_{i,v})$, where $\Delta_{i,v} := \Lambda_{i,v} \cup \{q_{i,v}\}$. We already know that the height of any entry in the multiplication table $M(\Lambda_{i,v})$ is at most $\text{Output}(m - 1)$. In order to obtain an upper bound for the heights of coefficients in $M(\Delta_{i,v})$, we need to estimate the height of the remainder in the pseudo division of $x_{i+1}^{\alpha_1} \cdots x_n^{\alpha_m}$ by $q_{i,v}$, where $0 \leq \alpha_s \leq 2 \deg_{x_{i+s}}(g_s) - 2$, $1 \leq s \leq m$. Note that $q_{i,v}$ is
CHAPTER 5. COMPLEXITY OF TRIANGULAR SET REPRESENTATION

reduced modulo $\Lambda_{i,v}$, and that $\deg_{x_n} q_{i,v} \leq \tilde{d}_m$. By using the matrix representation of the remainder in the pseudo-division algorithm (see Appendix A: Matrix Representation of Pseudoremainder), the remainder obtained when we divide $x_{i+1}^{a_{i+1}} \cdots x_n^{a_m}$ by $q_{i,v}$ is equal to a sum of products of at most $\tilde{d}_m + 2$ integral elements in $A(\Lambda_{i,v})$. Therefore,

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

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

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

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

$$\tilde{d}_i \leq d \text{ for every } i = 1, \ldots, m. \quad (5.4.2)$$

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

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

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

$$\text{Output}(s) \leq (d+2)(16d^s + 16d \log(32d) + \log(d+2)) \text{Output}(s-1) + +16(d+2)d^s \text{Input}(s-1) \quad (5.4.3)$$
for every \( s = 1, \ldots, m \). Lemma 34 implies that
\[
\text{Input}(0) \leq I_0 := (6d)^m \left( \max\{d, d_f, d_h\} + 11(d + 2)^m \left( \log(d + 2) \right)^{m-1} \right)
\]
and
\[
\text{Input}(s - 1) \leq (6d)^{-s+1} I_0.
\]

Using this notation in (5.4.3), we see that
\[
(6^s \text{Output}(s)) \leq C(s)(6^{s-1} \text{Output}(s - 1)) + 96d(d + 2)I_0 \tag{5.4.4}
\]
where
\[
C(s) := 6(d + 2)(16d^s + 16d \log(32d) + \log(d + 2)). \tag{5.4.5}
\]

Now we unfold this recursion and rewrite \( 6^m \text{Output}(m) \) using \( 6^{m-1} \text{Output}(m - 1) \) and so on, we see that
\[
6^m \text{Output}(m) \leq \left( \prod_{s=1}^{m} C(s) \right) \cdot \text{Output}(0) + 96d(d + 2)I_0 \sum_{s=2}^{m} \prod_{i=s}^{m} C(i) \\
= \left( \prod_{s=1}^{m} C(s) + 96d(d + 2) \sum_{s=2}^{m} \prod_{i=s}^{m} C(i) \right) \cdot I_0. \tag{5.4.6}
\]

We simplify (5.4.6) by applying Lemma 36. In particular, we have:
\[
6^m \text{Output}(m) < 5.2 \cdot (242(d + 2))^m \cdot d^{4^m(m+1)} \cdot \log d \cdot I_0.
\]

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

\[ \square \]

**Theorem 35.** 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 of the codimensions 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

\[
B(m, d) := 5.2n \cdot 242^m (d^{2m} + 2d^m)^m d^{\frac{3}{2}(m+1)} \left( \max \{d^m, r\} + 7(d^m + 2)^m (\log(d^m + 2))^{m-1} \right) \log d^m. \tag{5.4.7}
\]

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

\[
\deg p \leq nd^{\left(\frac{1}{2} + \epsilon\right)m^3}
\]

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.** [20, 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 \(\Delta\) 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

\[
\mathcal{U}(\Delta) := \text{unmixed}_{|\Delta|}(\Delta, M(\Delta), f, 1) \text{ for every } \Delta \in \Sigma(F)
\]

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 33, for every polynomial \(p\) occurring in the computation of \(\mathcal{U}(\Delta)\), we have
height\( (p) \leq \frac{1}{n} B(|\Delta|, d). \)

Since \( B(m, d) \) is monotonic in \( m \) and \( |\Delta| \leq m \), this implies (5.4.7).

In case \( r \leq d^m \), we have \( \max\{r, d^m\} = d^m \). Direct computation shows that the right hand side of (5.4.7) can be bounded by \( \deg p \leq nd^{\left(\frac{1}{2} + \epsilon \right)m^3} \), 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,

\[
\lim_{m \to \infty} \epsilon(m, d) = 0 \quad \text{for all } d.
\]

Remark. 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 6). Therefore the inequality (4.13) in [33, p. 121] is not necessarily true in general. Instead of it we use (5.4.2) in order to bound \( \tilde{d}_i \). The right-hand side of (5.4.2) is \( d^m \) in terms of the input data of Algorithm 1, and this makes our bound \( d^{O(m^3)} \).

Lemma 36. Consider \( C(s) \) defined as (see also (5.4.5))

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

Then we have:

\[
\prod_{s=1}^{m} C(s) \leq \frac{678 \cdot 387}{242^2} \cdot (242(d + 2))^m \cdot d^{\frac{3m(m + 1)}{2}} \log d, \quad \text{and}
\]
\[
\sum_{s=2}^{m} \prod_{i=s}^{m} C(i) \leq \frac{387 \cdot 4}{967} \cdot (242(d+2))^{m-1} \cdot d_{\frac{1}{2}(m+1)-1}.
\]

**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:

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

\[
\leq \frac{387}{242} d_{\frac{1}{2}(m+1)-1} \sum_{s=1}^{m-1} (242(d+2))^s
\]

\[
\leq \frac{387}{242} d_{\frac{1}{2}(m+1)-1} \cdot (242(d+2))^{m-1} \cdot \frac{(242(d+2))}{(242(d+2))} - 1
\]

\[
\leq \frac{387 \cdot 4}{967} \cdot d_{\frac{1}{2}(m+1)-1} \cdot (242(d+2))^{m-1}.
\]

### 5.5 Bound for the number of components

We now study the number of components in the output of Szanto’s algorithm.

**Theorem 37.** 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 the codimensions 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

\[
\binom{n}{m} ((m+1)d^m + 1)^m.
\]

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

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

Due to [17, Theorem 4.4], the number of elements in a regular chain $\Delta$ is equal to the codimension of the ideal 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 $\text{unmixed}$ to transform each regular chain $\Delta \in \Sigma(F)$ to the set

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

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 $\text{unmixed}^{|\Delta|}_{1}$ is simple, meaning that any two distinct unmixed components have no common irreducible components (see [33, page 124]). Since all the components of Rep($\Delta$) are of codimension $s$, $|\mathcal{U}(\Delta)|$ is bounded from above by the degree of Rep($\Delta$). Due to the definition of Rep($\Delta$), we have $\text{Rep}(\Delta) \supsetneq (\Delta)$. Moreover, since $V(\Delta)$ and $V(\text{Rep}(\Delta))$ coincide outside the zero set of the product of the initials of $\Delta$, every irreducible component of $V(\text{Rep}(\Delta))$ is an irreducible component of $V(\Delta)$. Hence, the degree of 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 \text{ due to } [14, \text{Theorem 1}]. \text{ The proof of } [33, \text{Corollary 4.1.5}] \text{ implies that every } g_i \text{ depends on at most } s + 1 \text{ variables, so }

\deg g_i \leq (s + 1) \text{height} g_i \leq (s + 1)d^s.

Therefore

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

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

\[ M(n, m, d) \leq \sum_{s=1}^{m} \binom{n}{s} ((m + 1)d^m)^s. \]

Since \( \binom{n}{s} \leq \binom{n}{m} \cdot \binom{m}{s} \), we have that \( M(n, m, d) \leq \binom{n}{m} ((m + 1)d^m + 1)^m \). \qed
Appendix A: Matrix Representation of Pseudoremainder

The following results on matrix representations of pseudoremainders are used in Section 5.4. 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 21). 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 \( k[x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_l] \):

\[
\begin{align*}
f &= f_0 + f_1 x_n + \cdots + f_{2d-1} x_n^{2d-1}, \\
g &= g_0 + g_1 x_n + \cdots + g_d x_n^d.
\end{align*}
\]

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 \( g_d f = gq + r \) 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:

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

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

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

We write the system above as \( G_dq = f_{\text{up}}^d g_d^d \). 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

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

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

\[ r = g_d^d f_{\text{low}} - g_d^d G_0 G_d^{-1} f_{\text{up}}. \]

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 \( r = g_d^d f_{\text{low}} - G_0 \cdot \text{adj}(G_d) f_{\text{up}} \).

Observe that the entries of \( \text{adj}(G_d) \) are sums of products of \( d - 1 \) entries of \( G_d \).
Appendix B: Maple Code for $n = 2$

In the pages that follow, we include the Maple code that was used to obtain degree bounds for the finite subgroups of $SL_2(C)$.
> with(combinat):
> with(LinearAlgebra):
> with(Algebraic);
> a := RootOf(x^4 + x^3 + x^2 + x + 1, x, index = 1);
> b := RootOf(x^2 - 5, x);
> alpha := RootOf(x^4 - 2 * x^2 + 9, x, index = 1);
> imag := RootOf(x^2 + 1, x, index = 1);
> c := RootOf(x^2 - 2, x, index = 1);
> groups := table(
>   binary_tetrahedron = table(
>     gens = [
>       Matrix(2, 2, [[imag, 0], [0, -imag]]),
>       Matrix(2, 2, [[0, 1], [-1, 0]]),
>       1/2 * Matrix(2, 2, [[1 + imag, -1 + imag], [1 + imag, 1 - imag]])
>     ],
>     # 9 is a square root of -1 mod 41
>     gens_char = [
>       Matrix(2, 2, [[9, 0], [0, -9]]),
>       Matrix(2, 2, [[0, 1], [-1, 0]]),
>       1/2 * Matrix(2, 2, [[1 + 9, -1 + 9], [1 + 9, 1 - 9]])
>     ],
>     size = 24,
>     modulus = 41
>   ),
>   binary_icosahedron = table(
>     gens = [
>       Matrix(2, 2, [[a^3, 0], [0, a^2]]),
>       Matrix(2, 2, [[0, 1], [-1, 0]]),
>       1/b * Matrix(2, 2, [[a^4 - a, -a^3 + a^2], [-a^3 + a^2, -a^4 + a]])
>     ],
>     # 83816 is a 5th primitive root of unity mod 102001
>     # 24747 is a square root of 5 mod 102001
>     gens_char = [
>       Matrix(2, 2, [[83816^3, 0], [0, 83816^2]]),
>       Matrix(2, 2, [[0, 1], [-1, 0]]),
>       1/24747 * Matrix(2, 2, [[83816^4 - 83816, -83816^3 + 83816^2], [-83816^3 + 83816^2, -83816^4 + 83816]])
>     ],
>     size = 120,
>     modulus = 102001
>   ),
>   binary_octahedron = table(
>     gens = [
>       1 / c * Matrix(2, 2, [[1 + imag, 0], [0, 1 - imag]]),
>       Matrix(2, 2, [[0, 1], [-1, 0]]),
>       1/2 * Matrix(2, 2, [[1 + imag, -1 + imag], [1 + imag, 1 - imag]])
>     ],
>     # 67719 is a square root of 2 mod 102001
>     # 24989 is a square root of -1 mod 102001
>     gens_char = [
>       1/7 * 67719 * Matrix(2, 2, [[1 + 24989, 0], [0, 1 - 24989]]),
> Matrix(2, 2, [[0, 1], [-1, 0]]),
> 1 / 2 * Matrix(2, 2, [[1 + 24989, -1 + 24989], [1 + 24989, 1 - 24989]])
> ],
> size = 48,
> modulus = 102001
> ])
> ]);

> GenerateGroup := proc (gens, size, char := 0)
> local to_add, G, g, h, T, t, gens_count, n;
> description "generate group G of given size from set of generators";
> n := LinearAlgebra[RowDimension](gens[1]);
> G := [LinearAlgebra[IdentityMatrix](n, n)];
> gens_count := 1;
> while nops(G) < size do
> T := cartprod([G, gens]);
> while not T[finished] do
> t := T[nextvalue]();
> g := evala(t[1].t[2]);
> to_add := true;
> for h in G do
> if
> (char = 0 and LinearAlgebra[Equal](evala(g - h), Matrix(n)))
> or
> (char > 0 and LinearAlgebra[Equal](g - h mod char, Matrix(n)))
> then
> to_add := false;
> end if;
> end do;
> if to_add then
> G := [op(G), g]
> end if;
> end do;
> print(nops(G));
> gens_count := gens_count + 1;
> end do;
> G;
> end proc;

> DegreeBoundChar := proc(group_data)
> local G, G_vectors, J, n, i, j, G_mod, G_vectors_mod, J_mod,
> J_elim_mod, vanishing_ideal_mod, char,
> vars, v_sub, max_deg, result, d;
> n := LinearAlgebra[RowDimension](group_data[gens][1]);
> vars := [];
> for i from 1 to n do
> for j from 1 to n do
> vars := [op(vars), cat(x, i, j)];
> end do;
> end do:
# Generating group and finding vanishin ideal modulo suitable prime number

char := group_data[modulus];
G_mod := GenerateGroup(group_data[gens_char], group_data[size], char);
G_vectors_mod := map(m -> convert(m, list), G_mod);
vanishing_ideal_mod := PolynomialIdeals[VanishingIdeal](G_vectors_mod, vars, char):
print("Vanishing ideal modulo prime ", vanishing_ideal_mod);
J_mod := Groebner[Homogenize]( vanishing_ideal_mod, h );
J_elim_mod := PolynomialIdeals[EliminationIdeal](J_mod, {op (vars)});
print("J_elim_mod", J_elim_mod);

# Rational reconstruction + checking the result
J_elim := PolynomialIdeals[PolynomialIdeal](
  map(p -> iratrecon(p, char),
  PolynomialIdeals[Generators](J_elim_mod))
);
G := GenerateGroup(group_data[gens], group_data[size]);
G_vectors := map(m -> convert(m, list), G);
for v in G_vectors do
  v_sub := zip((x, val) -> x = val, vars, v);
  for p in PolynomialIdeals[Generators](J_elim) do
    if evala(subs(v_sub, p)) <> 0 then
      print("PANIK: polynomial ", p, "is not zero at ", v);
    end if;
  end do;
end do;
if Groebner[HilbertPolynomial](J_elim) <> group_data[size] / n then
  print("PANIK: Hilbert polynomial is ", Groebner[HilbertPolynomial](J_elim));
end if;
print("The result of the reconstruction has been checked");
print("J_elim reconstructed ", J_elim);

# Finding the minimum degree
max_deg := max( map( p -> degree(p, vars), PolynomialIdeals[Generators](J_elim) ) );
print("max deg is ", max_deg);
result := max_deg;
for d from 0 to max_deg do
  polys := select( p -> evalb(degree(p, vars) < max_deg - d),
  PolynomialIdeals[Generators](J_elim) )
  print(max_deg - d - 1, polys);
  if PolynomialIdeals[IdealContainment](
    J_elim,
    PolynomialIdeals[Radical](PolynomialIdeals[PolynomialIdeal](polys))
  ) then
    result := max_deg - d - 1;
  end if;
end do;
result;
end proc;
\[
\begin{align*}
l &:= \text{DegreeBoundChar}(\text{groups}[\text{binary_octahedron}]) ; \\
a &:= \text{RootOf}(\\n\quad _Z^4 + _Z^3 + _Z^2 + _Z + 1, \text{index} = 1) \\
b &:= \text{RootOf}(\\n\quad _Z^2 - 5) \\
\alpha &:= \text{RootOf}(\\n\quad _Z^4 - 2 _Z^2 + 9, \text{index} = 1) \\
\text{imag} &:= \text{RootOf}(\\n\quad _Z^2 + 1, \text{index} = 1) \\
c &:= \text{RootOf}(\\n\quad _Z^2 - 2, \text{index} = 1)
\end{align*}
\]

\[
groups := \text{table} \begin{cases} \\
\text{binary_octahedron} = \text{table} \begin{cases} \\
gens_char = \begin{bmatrix} \frac{8330}{22573} & 0 \\
0 & \frac{-24988}{67719} \end{bmatrix} , \\
0 & 1 \\
-1 & 0 \\
12495 & 12494 \\
-12495 & -12494 \end{bmatrix} , \text{modulus} = 102001 , \text{size} = 48 , \text{gens} \\
0 & 1 \\
-1 & 0 \\
\end{cases}
\end{cases}
\]

\[
\begin{align*}
\begin{bmatrix} \\
1 + \text{RootOf}(\\n\quad _Z^2 + 1, \text{index} = 1) \\
\text{RootOf}(\\n\quad _Z^2 - 2, \text{index} = 1) \\
0 \\
0 \\
\end{bmatrix} \begin{bmatrix} \\
0 \\
\frac{1 - \text{RootOf}(\\n\quad _Z^2 + 1, \text{index} = 1)}{\text{RootOf}(\\n\quad _Z^2 - 2, \text{index} = 1)} \\
-1 & 0 \\
\end{bmatrix} , \\
\begin{bmatrix} \\
\frac{1}{2} + \text{RootOf}(\\n\quad _Z^2 + 1, \text{index} = 1) \frac{1}{2} \\
\frac{1}{2} + \text{RootOf}(\\n\quad _Z^2 + 1, \text{index} = 1) \frac{1}{2} \\
\frac{1}{2} - \text{RootOf}(\\n\quad _Z^2 + 1, \text{index} = 1) \frac{1}{2} \\
\frac{1}{2} - \text{RootOf}(\\n\quad _Z^2 + 1, \text{index} = 1) \frac{1}{2} \\
\end{bmatrix}
\end{align*}
\]

\[
\text{binary_tetrahedron} = \text{table} \begin{cases} \\
gens_char = \begin{bmatrix} 9 & 0 \\
0 & -9 \\
0 & 1 \\
-1 & 0 \\
5 & 4 \\
5 & -4 \end{bmatrix} , \text{modulus}
\end{cases}
\]
\[
= 41, \text{ size } = 24, \text{ gens } = \begin{bmatrix}
\text{RootOf}(\sqrt{2} + 1, \text{ index } = 1) & 0 \\
0 & -\text{RootOf}(\sqrt{2} + 1, \text{ index } = 1)
\end{bmatrix},
\]

\[
\begin{bmatrix}
0 & 1 \\
-1 & 0
\end{bmatrix}
= \begin{bmatrix}
\frac{1}{2} + \text{RootOf}(\sqrt{2} + 1, \text{ index } = 1) \\
\frac{1}{2} + \text{RootOf}(\sqrt{2} + 1, \text{ index } = 1)
\end{bmatrix}
- \begin{bmatrix}
\frac{1}{2} + \text{RootOf}(\sqrt{2} + 1, \text{ index } = 1) \\
\frac{1}{2} - \text{RootOf}(\sqrt{2} + 1, \text{ index } = 1)
\end{bmatrix},\]

\[
\text{binary_icosahedron} = \text{table}
\begin{bmatrix}
\text{gens_char} = \begin{bmatrix}
588817613482496 & 0 \\
0 & 7025121856
\end{bmatrix},

\begin{bmatrix}
\frac{49352337091648800920}{24747} & -\frac{588810588360640}{24747} \\
-\frac{588810588360640}{24747} & -\frac{49352337091648800920}{24747}
\end{bmatrix}, \text{modulus}
\end{bmatrix}
= 102001, \text{ size } = 120, \text{ gens } = \left[\left[ \begin{bmatrix}
\text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1}, \text{ index } = 1)^3, 0 \\
0, \text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1}, \text{ index } = 1)^2)
\end{bmatrix}, \begin{bmatrix}
0 & 1 \\
-1 & 0
\end{bmatrix}\right] \left[
\begin{bmatrix}
\frac{1}{\text{RootOf}(\sqrt{2} - 5)} (\text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1}, \text{ index } = 1)^4 - \text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1} + 1, \text{ index } = 1)), \frac{1}{\text{RootOf}(\sqrt{2} - 5)} (-\text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1} + 1, \text{ index } = 1)^3 + \text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1} + 1, \text{ index } = 1)^2)\right]
\left[\frac{1}{\text{RootOf}(\sqrt{2} - 5)} (-\text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1} + 1, \text{ index } = 1)^3 + \text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1} + 1, \text{ index } = 1)^2), \frac{1}{\text{RootOf}(\sqrt{2} - 5)} (-\text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1} + 1, \text{ index } = 1)^4 + \text{RootOf}(\sqrt{4} + \sqrt{3} + \sqrt{2} + \sqrt{1} + 1, \text{ index } = 1)^3))\right]\right]\right].
GenerateGroup := proc(gens, size, char := 0)
    local to_add, G, g, h, T, t, gens_count, n;
    description "generate group G of given size from set of generators";
    n := LinearAlgebra[LinearAlgebra:-RowDimension](gens[1]);
    G := [LinearAlgebra[LinearAlgebra:-IdentityMatrix](n, n)];
    gens_count := 1;
    while nops(G) < size do
        T := combinat-cartprod([G, gens]);
        while not T[finished] do
            t := T[nextvalue]();
            g := evala(`\`(t[1], t[2]));
            to_add := true;
            for h in G do
                if char = 0 and LinearAlgebra[LinearAlgebra:-Equal](evala(g - h), Matrix(n)) or 0 < char and LinearAlgebra[LinearAlgebra:-Equal](g - h mod char, Matrix(n)) then
                    to_add := false
                end if;
                end do;
            end if;
        end do;
        if to_add then G := [op(G), g] end if
    end do;
    print(nops(G));
    gens_count := gens_count + 1
end do;
G
end proc

DegreeBoundChar := proc(group_data)
    local G, G_vectors, J, i, j, G_mod, G_vectors_mod, J_mod, J_elim_mod,
    vanishing_ideal_mod, char, vars, v_sub, max_deg, result, d, J_elim, v, p, polys;
    n := LinearAlgebra[LinearAlgebra:-RowDimension](group_data[gens][1]);
    vars := [ ];
    for i to n do for j to n do vars := [op(vars), cat(x, i, j)] end do end do;
    char := group_data[modulus];
    G_mod := GenerateGroup(group_data[gens_char], group_data[size], char);
    G_vectors_mod := map(m->convert(m, list), G_mod);
    vanishing_ideal_mod := PolynomialIdeals[VanishingIdeal](G_vectors_mod, vars, char);
    print("Vanishing ideal modulo prime ", vanishing_ideal_mod);
    J_mod := Groebner[Homogenize](vanishing_ideal_mod, h);
    J_elim_mod := PolynomialIdeals[EliminationIdeal](J_mod, {op(vars)});
    print("J_elim_mod", J_elim_mod);
    J_elim := PolynomialIdeals[PolynomialIdeal](map(p->iratrecon(p, char), PolynomialIdeals[Generators](J_elim_mod)));
end proc
\begin{verbatim}
G := GenerateGroup(group_data[gens], group_data[size]);
G_vectors := map(m->convert(m, list), G);
for v in G_vectors do
    v_sub := zip((x, val) -> x = val, vars, v);
    for p in PolynomialIdeals[Generators](J_elim) do
        if evalat(subs(v_sub, p)) <> 0 then
            print("PANIK: polynomial ", p, " is not zero at ", v)
        end if
    end do
end do;
if Groebner[HilbertPolynomial](J_elim) <> group_data[size]/n then
    print("PANIK: Hilbert polynomial is ", Groebner[HilbertPolynomial](J_elim))
end if;
print("The result of the reconstruction has been checked");
print("J_elim reconstructed ", J_elim);
max_deg := max(map(p->degree(p, vars), PolynomialIdeals[Generators](J_elim)));
poly := max_deg
result := max_deg;
for d from 0 to max_deg do
    polys := select(p->evalb(degree(p, vars) < max_deg - d), PolynomialIdeals[Generators](J_elim));
    print(max_deg - d - 1, polys);
    if PolynomialIdeals[IdealContainment](J_elim, PolynomialIdeals[Radical](PolynomialIdeals[PolynomialIdeal](polys))) then
        result := max_deg - d - 1
    end if
end do;
result
end proc
\end{verbatim}

"Vanishing ideal modulo prime ", \{x21 x22^9 + 6375 x21 x22, x22^17 + 6374 x22^9 + 95626 x22,
54408 x22^15 + 47592 x22^7 + x11, 95202 x22^13 + x22 x21^4 + 6799 x22^5, x21^7 + 7 x21^3 x22^4
+ x12, 95186 x22^16 + x21^8 + 6816 x22^8 + 102000\}

"J_elim_mod", \{x11^4 + 102000 x22^4, x12^4 + 102000 x21^4, x21^5 x22 + 102000 x21 x22^5,
x11 x21 x22^2 + x12 x21^2 x22, x11 x21^3 + x12 x22^3, x11 x12 x22^2 + x12^2 x21 x22, x11 x12^3
+ x21 x22^3, x11^2 x21 x22 + x11 x12 x21^2, x11^2 x21^2 + 102000 x12^2 x22^2, x11^2 x12
+ x11 x12^2 x21, x11^2 x21^2 + 102000 x21^2 x22^2, x11^3 x21 + x12^3 x22, x11^3 x12 + x21^3 x22\}
"The result of the reconstruction has been checked"

\[ J_{\text{elim reconstructed}}, \{x11^4 - x22^4, x12^4 - x21^4, x21^5 x22 - x21 x22^5, x11 x21 x22^2 \\
+ x12 x21^2 x22, x11 x21^3 + x12 x22^3, x11 x12 x22^2 + x12^2 x21 x22, x11 x12^3 + x21 x22^3, \\
x11^2 x21 x22 + x11 x12 x21^2, x11^2 x21^2 - x12^2 x22^2, x11^2 x12 x22 + x11 x12^2 x21, x11^2 x12^2 \\
- x21^2 x22^2, x11^3 x21 + x12^3 x22, x11^3 x12 + x21^3 x22\} \]

"max deg is ", 6

5, \{x11^4 - x22^4, x12^4 - x21^4, x11 x21 x22^2 + x12 x21^2 x22, x11 x21^3 + x12 x22^3, x11 x12 x22^2 \\
+ x12^2 x21 x22, x11 x12^3 + x21 x22^2, x11^2 x21 x22 + x11 x12 x21^2, x11^2 x21^2 - x12^2 x22^2, \\
x11^2 x12 x22 + x11 x12^2 x21, x11^2 x12^2 - x21^2 x22^2, x11^3 x21 + x12^3 x22, x11^3 x12 \\
+ x21^3 x22\} \]

4, \{x11^4 - x22^4, x12^4 - x21^4, x11 x21 x22^2 + x12 x21^2 x22, x11 x21^3 + x12 x22^3, x11 x12 x22^2 \\
+ x12^2 x21 x22, x11 x12^3 + x21 x22^2, x11^2 x21 x22 + x11 x12 x21^2, x11^2 x21^2 - x12^2 x22^2, \\
x11^2 x12 x22 + x11 x12^2 x21, x11^2 x12^2 - x21^2 x22^2, x11^3 x21 + x12^3 x22, x11^3 x12 \\
+ x21^3 x22\} \]

3, $\emptyset$
2, $\emptyset$
1, $\emptyset$
0, $\emptyset$
-1, $\emptyset$
l := 4
Bibliography


