Advances in Applied Mathematics 65 (2015) 1–37

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

Hrushovski's algorithm for computing the Galois group of a linear differential equation

Ruyong Feng [1]

KLMM, AMSS, Chinese Academy of Sciences, Beijing 100190, China

ARTICLE INFO

Article history:
Received 26 February 2014
Accepted 26 January 2015
Available online 6 February 2015

MSC:
34A30
12H05
68W30

Keywords:
Linear differential equation
Galois group
Algorithm

ABSTRACT

We present a detailed and modified version of Hrushovski's algorithm that determines the Galois group of a linear differential equation. Moreover, we give explicit degree bounds for the defining polynomials of various linear algebraic groups that appear in the algorithm. These explicit bounds will play an important role to understand the complexity of the algorithm.

1. Introduction

In [10], Hrushovski developed an algorithm to compute the Galois groups for general linear differential equations. To the best of my knowledge, this is the first algorithm that works for all linear differential equations with rational function coefficients. Before Hrushovski's results, the known algorithms were only valid for linear differential equations of special types, for instance, low order or completely reducible equations.

E-mail address: ryfeng@amss.ac.cn.

[1] This work is partially supported by a National Key Basic Research Project of China (2011CB302400) and by grants from NSFC (60821002, 10901156).

http://dx.doi.org/10.1016/j.aam.2015.01.001
0196-8858/

The algorithm due to Kovacic [13] deals with the second order equations. In [21], the authors determined the structural properties of the Galois groups of second and third order linear differential equations. In many cases these properties can be used to determine the Galois groups. In [2], the authors gave an algorithm to compute the Galois group of linear differential equations that are completely reducible. The reader is referred to [20,22] for the survey of algorithmic aspects of Galois groups and the references given there for more results. In particular, in [20], the author gave a clear explanation of the method based on the Tannakian philosophy and introduced the various techniques that were used in the known algorithms.

Throughout the paper, C denotes an algebraically closed field of characteristic zero and $k = C(t)$ is the differential field with the usual derivation $\delta = \frac{d}{dt}$. The algebraic closure of k is denoted by $\bar{k}$. Linear differential equations we consider here will be of the matrix form:

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

where Y is a vector with n unknowns and A is an $n \times n$ matrix with entries in k. Denote the Picard–Vessiot extension field of k for (1) by K and the solution space of (1) by V. Then the Galois group of (1) over k, denoted by $\mathrm{Gal}(K/k)$, is defined as the group of differential automorphisms of K that keep all elements of k fixed. For brevity, we usually use $\mathcal{G}$ to denote this group. One can readily see that $\mathcal{G}$ is a subgroup of $\mathrm{GL}(V)$, the group of automorphisms of V. A matrix in $\mathrm{GL}_n(K)$ whose columns form a basis of V is called a fundamental matrix of (1).

Elements of V^n are vectors with n^2 coordinates. For the sake of convenience, elements of V^n are also written in the matrix form. In such a case, $V^n = \{Fh \mid h \in \mathrm{Mat}_n(C)\}$, where F is a fundamental matrix of (1). Set

$$V^n_{inv} = \{Fh \mid h \in \mathrm{GL}_n(C)\}.$$

Then V^n_{inv} is an open subset of V^n. Note that if $F = I_n$, then $V^n_{inv} = \mathrm{GL}_n(C)$. In this paper, we will always use X to denote the $n \times n$ matrix whose entries are indeterminates $x_{i,j}$. Without any possible ambiguity, we will also use X to denote the set of indeterminates and use $k[X]$ (resp. $C[X]$, $K[X]$) to denote the ring of polynomials in X over the field k (resp. C, K). Let Z be a subset of V^n_{inv}. Z is said to be a Zariski closed subset of V^n_{inv} if there are polynomials $P_1(X), \cdots, P_m(X)$ such that $Z = \mathrm{Zero}(P_1(X), \cdots, P_m(X)) \cap V^n_{inv}$. In this case, we also say that Z is defined by $P_1(X), \cdots, P_m(X)$. We will use $N_d(V^n_{inv})$ to denote the set of all subsets of V^n_{inv}, which are defined by finitely many polynomials of degree not greater than d. Note that here we have no requirement for the coefficients of these polynomials. Suppose that $\tilde{k}$ is an extension field of k and $Z \subseteq V^n_{inv}$. If Z can be defined by polynomials with coefficients in $\tilde{k}$, then Z is said to be *$\tilde{k}$-definable*. Note that there is a naturel action of $\mathrm{GL}(V)$ on V^n_{inv}, which is defined as $\sigma \cdot u = \sigma(u)$ for all $\sigma \in \mathrm{GL}(V)$ and $u \in V^n_{inv}$. The *stabilizer* of Z, denoted by $\mathrm{stab}(Z)$, is defined as the

subgroup of $\mathrm{GL}(V)$ whose elements keep Z unchanged. Let $Z \in N_d(V_{inv}^n)$. In case that we emphasize the degree d of defining polynomials, we will also say "Z is bounded by d".

Let F be a fundamental matrix. For any $\sigma \in \mathrm{GL}(V)$, there exists $[\sigma] \in \mathrm{GL}_n(C)$ such that $\sigma(F) = F[\sigma]$. The map $\phi_F : \mathrm{GL}(V) \to \mathrm{GL}_n(C)$, given by $\phi_F(\sigma) = [\sigma]$, is a group isomorphism. Let $\mathcal{H}$ be a subgroup of $\mathrm{GL}_n(V)$. For ease of notations, we use $\mathcal{H}_F$ to denote $\phi_F(\mathcal{H})$. $\mathcal{H}$ is said to be an algebraic group if $\mathcal{H}_F$ is. It is known that $\mathcal{G}$ is an algebraic group. Assume that $\mathcal{H}$ is an algebraic group. Then $\mathcal{H}^\circ$, $\mathcal{H}^t$ are used to denote the pre-images of $\mathcal{H}_F^\circ$ and $\mathcal{H}_F^t$, where $\mathcal{H}_F^\circ$ denotes the identity component of $\mathcal{H}_F$ and $\mathcal{H}_F^t$ is the intersection of kernels of all characters of $\mathcal{H}_F$. $\mathcal{H}$ is said to be bounded by d if $\mathcal{H}_F$ is.

The key point of Hrushovski's algorithm is that one can compute an integer $\tilde{d}$ such that there is an algebraic subgroup $\mathcal{H}$ (or $\mathcal{H}_F$) of $\mathrm{GL}(V)$ bounded by $\tilde{d}$ satisfying

$$(*): \quad \left(\mathcal{H}^\circ\right)^t \trianglelefteq \mathcal{G}^\circ \leq \mathcal{G} \leq \mathcal{H}, \quad \text{or} \quad \left(\mathcal{H}_F^\circ\right)^t \trianglelefteq \mathcal{G}_F^\circ \leq \mathcal{G}_F \leq \mathcal{H}_F.$$

For simplicity of presentation, we introduce the following notion.

Definition 1.1. An algebraic group $\mathcal{H}$ (or $\mathcal{H}_F$) in $(*)$ is called a *proto-Galois group* of (1).

Roughly speaking, Hrushovski's approach includes the following steps.

($S1$) (Proto-Galois groups). One can compute an integer $\tilde{d}$ only depending on n such that there is a proto-Galois group of (1), which is bounded by $\tilde{d}$. In fact, if we let $\mathcal{H}$ be the intersection of the stabilizers of k-definable elements of $N_{\tilde{d}}(V_{inv}^n)$. Then $\mathcal{H}$ is a desired proto-Galois group of (1).

($S2$) (The toric part). Compute $\mathcal{H}_F^\circ$ and let $\chi_1, \cdots, \chi_l$ be generators of the character group of $\mathcal{H}_F^\circ$. Then the map $\varphi = (\chi_1, \cdots, \chi_l)$ is a morphism from $\mathcal{H}_F^\circ$ to $(C^*)^l$ and $\varphi(\mathcal{G}_F^\circ)$ is the Galois group of some exponential extension E of $\tilde{k}$ over $\tilde{k}$, where $\tilde{k}$ is an algebraic extension of k. One can find E by computing hyperexponential solutions of some symmetric power system of (1). Pulling $\varphi(\mathcal{G}_F^\circ)$ back to $\mathcal{H}_F^\circ$, one obtains $\mathcal{G}_F^\circ$.

($S3$) (The finite part). Find a finite Galois extension k_G of k and a k_G-definable subset Z of V_{inv}^n such that $\mathcal{G}^\circ = \mathrm{stab}(Z)$. Let $Z_1 = Z, Z_2, \cdots, Z_m$ be the orbit of Z under the action of $\mathrm{Gal}(k_G/k)$. Then $\mathcal{G} = \bigcup_{i=1}^m \{\sigma \in \mathrm{GL}(V) \mid \sigma(Z) = Z_i\}$.

We follow Hrushovski's approach, but take out the logical language and elaborate the details of the proofs that were only sketched in his paper. We hope this will be helpful for the reader to understand Hrushovski's approach. Meanwhile, we modify the step of his approach where a proto-Galois group is computed. To obtain a proto-Galois group, the step (b) of Algorithm B in [10] first computes the formulas for all k-definable elements of $N_d(V_{inv}^n)$ for some sufficiently large d, and then calculates the intersection of the stabilizers of these k-definable elements from their formulas. We shall show that the

intersection of those stabilizers is actually equal to the stabilizer of a certain k-definable element of $N_d(V_{inv}^n)$. In the sequel, one only needs to compute one k-definable element of $N_d(V_{inv}^n)$ to find a proto-Galois group. This improves the step (b) of Algorithm B in some sense (see Remark 2.5 for further discussions). Hrushovski showed in the part III of [10] how to compute the integer $\tilde{d}$ as claimed in (S1). As well as providing the detailed explanations of his proofs, we present an explicit estimate of the integer $\tilde{d}$, which is sextuply exponential in the order of matrices. The bound we estimated is much larger than the one guessed by Hrushovski in Remark 4.5 of [10]. To estimate $\tilde{d}$, we need Jordan bounds on finite groups and complexity bounds on Gröbner basis, which are exponential and doubly exponential respectively. The successive compositions of those bounds and central binomial coefficients result in a large bound for the integer $\tilde{d}$. The reader is referred to Remark B.3 for the details.

The paper is organized as follows. In Appendix A, we describe a method to find coefficient bounds for k-definable elements of $N_d(V_{inv}^n)$, that is, a method to bound the degrees of the coefficients of defining polynomials of such sets. In Appendix B, an explicit estimate of the integer $\tilde{d}$ that bounds the proto-Galois groups is presented. These bounds will guarantee the termination of the algorithm. In Sections 2 and 3, we show how to compute a proto-Galois group and then the Galois group. Some computation details are omitted in these sections and will be completed in Section 4.

2. Proto-Galois groups

This section will be devoted to finding a proto-Galois group of (1). Let $d \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ and $I \subseteq k[X]$. $I_{\leq d}$ denotes the set of polynomials in I with degree not greater than d. Set

$$I_{F,d} = \left\{P(X) \in k[X]_{\leq d} \;\middle|\; P(F) = 0\right\} \quad \text{and} \quad Z_{F,d} = \text{Zero}(I_{F,d}) \bigcap V_{inv}^n \tag{2}$$

When $d = \infty$, we use I_F and Z_F for short. I_F consists of algebraic relations among entries of the fundamental matrix F. The Galois group of (1) is considered as the subgroup of $\text{GL}(V)$ that preserves I_F. Precisely,

$$\mathcal{G} = \left\{\sigma \in \text{GL}(V) \;\middle|\; \sigma(Z_F) = Z_F\right\}.$$

Hence once I_F is computed, $\mathcal{G}$ will be determined. Of course, I_F has a basis that lies in some $F_{F,d}$ but we do not know how to directly calculate such a value of d. This is why we proceed as outlined in steps $(S1)$–$(S3)$. In this section, we shall show that if d is sufficiently large then $\text{stab}(Z_{F,d})$ is a proto-Galois group. Given an integer d, the results of Appendix A enable us to compute $I_{F,d}$ (see Section 4.1). Corollary B.15 in Appendix B gives us a bound on such a d. We also describe properties of a proto-Galois group that are needed to justify our algorithm. Let us start with three lemmas.

Lemma 2.1. *Assume that U is a C-definable Zariski closed subset of $\mathrm{GL}_n(C)$ such that $\mathcal{G} \subseteq \mathrm{stab}(FU)$. Then FU is a k-definable Zariski closed subset of V_{inv}^n. Moreover if U is bounded by d then so is FU.*

Proof. Assume that U is bounded by d. Let

$$J = \big\{P(X) \in C[X]_{\leq d} \;\big|\; \forall u \in U, P(u) = 0\big\}.$$

Since U is bounded by d, $U = \mathrm{Zero}(J) \cap \mathrm{GL}_n(C)$. Let $\tilde{I}$ be the ideal in $K[X]$ generated by $\{P(F^{-1}X) \mid P(X) \in J\}$. Set

$$\tilde{I}_{\leq d} = \tilde{I} \cap K[X]_{\leq d}.$$

Then $\{P(F^{-1}X) \mid P(X) \in J\} \subseteq \tilde{I}_{\leq d}$ and $FU = \mathrm{Zero}(\tilde{I}_{\leq d}) \cap V_{inv}^n$. Moreover, assume that $P(X)$ is a polynomial in $K[X]_{\leq d}$ satisfying that $P(Fu) = 0$ for any $u \in U$. Then one can easily see that $P(FX)$ is a K-linear combination of finitely many elements in J. Therefore $P(X) \in \tilde{I}_{\leq d}$. Now let

$$I_{\leq d} = \tilde{I}_{\leq d} \cap k[X].$$

We will show that $I_{\leq d}$ generates $\tilde{I}$. For this, it suffices to prove that $I_{\leq d}$ generates $\tilde{I}_{\leq d}$, since $\tilde{I}_{\leq d}$ generates $\tilde{I}$. We will use the an argument similar to the one given in (p. 23, [23]) to prove this. Let $\langle I_{\leq d}\rangle$ denote the ideal of $K[X]$ generated by $I_{\leq d}$. Assume that $\tilde{I}_{\leq d}$ is not a subset of $\langle I_{\leq d}\rangle$. Pick $Q(X) \in \tilde{I}_{\leq d} \setminus \langle I_{\leq d}\rangle$ such that $\mathrm{num}(Q(X))$, the number of the monomials of $Q(X)$, is minimal. If $\mathrm{num}(f) = 1$, it is clear that $Q(X) \in \langle I_{\leq d}\rangle$. Hence $\mathrm{num}(Q(X)) > 1$. Without loss of generality, we may assume that one of the coefficients of $Q(X)$ equals one and one of them, say c, is not in k. Let $\sigma \in \mathcal{G}$. We use $Q_\sigma(X)$ to denote the image of $Q(X)$ by applying σ to the coefficients of $Q(X)$. For every $u \in U$, since $Q(\sigma^{-1}(Fu)) = 0$,

$$\sigma\big(Q\big(\sigma^{-1}(Fu)\big)\big) = Q_\sigma\big(\sigma\big(\sigma^{-1}(Fu)\big)\big) = Q_\sigma(Fu) = 0.$$

This implies that $Q_\sigma(X) \in \tilde{I}_{\leq d}$ for all $\sigma \in \mathcal{G}$. Then the minimality of $\mathrm{num}(Q(X))$ implies that both $Q(X) - Q_\sigma(X)$ and $c^{-1}Q(X) - \sigma(c)^{-1}Q_\sigma(X)$ are in $\langle I_{\leq d}\rangle$. Therefore

$$\forall \sigma \in \mathcal{G}, \quad \big(\sigma(c)^{-1} - c^{-1}\big)Q(X) \in \langle I_{\leq d}\rangle.$$

Since $c \notin k$, there is $\sigma \in \mathcal{G}$ such that $\sigma(c) \neq c$. So $Q(X) \in \langle I_{\leq d}\rangle$, a contradiction. Hence $I_{\leq d}$ generates $\tilde{I}_{\leq d}$. □

The correctness of the statement below is almost obvious. However, since it will be used frequently, we state it as a lemma.

Lemma 2.2. *Let H be a subgroup of $\mathrm{GL}_n(C)$ and $\mathcal{N} = \mathrm{stab}(FH)$. Then $\mathcal{N}_F = H$.*

Proof. Recall that the action of $\mathrm{GL}(V)$ on V_{inv}^n is defined as $\sigma(Fu) = F[\sigma]u$ for each $u \in \mathrm{GL}_n(C)$, where $[\sigma] = F^{-1}\sigma(F)$. One can then see that $\mathcal{N}_F \subseteq H$. Assume that $h \in H$. Then there is an element σ_h in $\mathrm{GL}(V)$ satisfying that $\sigma_h(F) = Fh$. Now for any $h' \in H$,

$$\sigma_h\big(Fh'\big) = Fhh' \in FH \quad \text{and} \quad \sigma_h\big(Fh^{-1}h'\big) = Fh'.$$

These facts imply that $\sigma_h \in \mathcal{N}$ and then $h \in \mathcal{N}_F$. This concludes the lemma. □

From (2), one sees that $Z_{F,d}$ is minimal among those k-definable elements of $N_d(V_{inv}^n)$ which contain F. Furthermore, the following lemma implies that $\mathrm{stab}(Z_{F,d})$ is also minimal.

Lemma 2.3. *Let $\bar{Z}$ be a k-definable element of $N_d(V_{inv}^n)$. Then $\mathrm{stab}(Z_{F,d}) \subseteq \mathrm{stab}(\bar{Z})$.*

Proof. We may write $\bar{Z} = FU$ for some Zariski closed subset U of $\mathrm{GL}_n(C)$. We first claim that

$$\bar{Z} = \bigcup_{u \in U} Z_{F,d}u.$$

Obviously, $\bar{Z}$ is a subset of the right-hand side because $F \in Z_{F,d}$. Suppose that $\bar{Z}$ is defined by $\mathbb{S}$, a set of polynomials in $k[X]$ with degree $\leq d$. For any $u \in U$, one has that $P(Fu) = 0$ for all $P \in \mathbb{S}$. Due to the definition of $I_{F,d}$, $P(Xu) \in I_{F,d}$ for all $P \in \mathbb{S}$ and $u \in U$. Hence $P(zu) = 0$ for all $z \in Z_{F,d}$, $u \in U$ and $P \in \mathbb{S}$. So $Z_{F,d}u \subseteq \bar{Z}$ for all $u \in U$. This proves the claim. Now assume that $\sigma \in \mathrm{stab}(Z_{F,d})$. Then one has that

$$\sigma(\bar{Z}) = \bigcup_{u \in U} \sigma(Z_{F,d})u = \bigcup_{u \in U} Z_{F,d}u = \bar{Z}.$$

Therefore $\sigma \in \mathrm{stab}(\bar{Z})$. □

In Corollary B.15 of Appendix B, we produce an integer $\tilde{d}$ such that there is a family $\tilde{\mathcal{F}}$ of subgroups of $\mathrm{GL}_n(C)$ bounded by $\tilde{d}$ having the property that for any subgroup H of $\mathrm{GL}_n(C)$ there is an $\tilde{H} \in \tilde{\mathcal{F}}$ such that

$$\big(\tilde{H}^\circ\big)^t \trianglelefteq H^\circ \leq H \leq \tilde{H}.$$

Note that if we let $H = \mathcal{G}_F$, then $\tilde{H}$ is a proto-Galois group. In the following, $\tilde{d}$ always denotes the integer produced in Corollary B.15 of Appendix B.

Proposition 2.4. *Let $\mathcal{H} = \mathrm{stab}(Z_{F,\tilde{d}})$. Then $\mathcal{H}$ is a proto-Galois group of (1) and moreover, $Z_{F,\tilde{d}} = F\mathcal{H}_F$.*

Proof. We first show that $Z_{F,\tilde{d}} = F\mathcal{H}_F$. We may write $Z_{F,\tilde{d}} = FH$ for some set of matrices $H \subseteq \mathrm{GL}_n(C)$. If H is a group, then one has that $\mathcal{H}_F = H$ by Lemma 2.2. That is to say, $Z_{F,\tilde{d}} = FH = F\mathcal{H}_F$. Hence it suffices to show that H is a group. As $F \in Z_{F,\tilde{d}}$, we have that $I_n \in H$. Suppose that $h_1, h_2 \in H$. For any $P(X) \in I_{F,\tilde{d}}$, the equality $P(Fh_2) = 0$ implies that $P(Xh_2)$ is an element of $I_{F,\tilde{d}}$. Hence $P(Fh_1h_2) = 0$ and then $h_1h_2 \in H$. It remains to prove that for any $h \in H$, $h^{-1} \in H$. As H is closed under the multiplication, $Hh \subseteq H$. Multiplying both sides of $Hh \subseteq H$ by h repeatedly, we have that

$$\cdots \subseteq Hh^3 \subseteq Hh^2 \subseteq Hh \subseteq H.$$

It is easy to verify that H is a Zariski closed subset of $\mathrm{GL}_n(C)$ and so is Hh^i for all positive integer i. The stability of the above sequence indicates that $Hh^{i_0+1} = Hh^{i_0}$ for some $i_0 \geq 0$ and therefore $Hh = H$. So $h^{-1} \in H$.

Now we prove that $\mathcal{H}$ is a proto-Galois group of (1). First of all, as $Z_{F,\tilde{d}}$ is k-definable, $\mathcal{G} \subseteq \mathrm{stab}(Z_{F,\tilde{d}}) = \mathcal{H}$. By Corollary B.15, there is a proto-Galois group $\tilde{H}$ of (1) bounded by $\tilde{d}$. Since $\mathcal{G}_F \subseteq \tilde{H}$, $\mathcal{G} \subseteq \mathrm{stab}(F\tilde{H})$ and then by Lemma 2.1, $F\tilde{H}$ is a k-definable element of $N_{\tilde{d}}(V_{inv}^n)$. Lemmas 2.2 and 2.3 imply that $\mathcal{H}_F \subseteq \tilde{H}$. Note that $(\mathcal{H}_F^\circ)^t$ is generated by all unipotent elements of $\mathcal{H}_F^\circ$ and these elements must be in $\tilde{H}^\circ$. Hence

$$\left(\mathcal{H}_F^\circ\right)^t \subseteq \left(\tilde{H}^\circ\right)^t \subseteq \mathcal{G}_F^\circ \subseteq \mathcal{H}_F^\circ.$$

Then the conclusion follows from the fact that $(\mathcal{H}_F^\circ)^t$ is a normal subgroup of $\mathcal{H}_F^\circ$. □

Remark 2.5. Let $\bar{\mathcal{H}}$ be the intersection of the stabilizers of k-definable elements of $N_{\tilde{d}}(V_{inv}^n)$. The idea of Algorithm B of [10] to compute $\bar{\mathcal{H}}$ is as follows: find the formulas for k-definable elements of $N_d(V_{inv}^n)$ and then obtain the defining equations for $\bar{\mathcal{H}}$ from these formulas. More precisely, Corollary 1.4 of [10] states that k-definable elements of $N_d(V_{inv}^n)$ correspond to hyperexponential solutions (equivalently, one-dimensional k-definable subspaces of the solution space) of a linear differential equation, which is a symmetric and exterior power of (1). Due to Lemma 2.4 of [18] or Lemmas P1.1 and P1.2 of [10], one can effectively find all hyperexponential solutions of a given linear differential equation. By Proposition 1 of [10], one can obtain the formulas for k-definable elements of $N_d(V_{inv}^n)$ from the corresponding hyperexponential solutions. Note that Proposition 1 of [10] claims that one can effectively find the formulas for k-definable subspaces of V (and thus the formulas for k-definable elements of $N_d(V_{inv}^n)$), but its proof does not supply the details on how to deduce these formulas.

Due to Lemma 2.3, one has that

$$\mathrm{stab}(Z_{F,\tilde{d}}) \subseteq \bar{\mathcal{H}} \subseteq \mathrm{stab}(Z_{F,\tilde{d}}).$$

Hence $\mathrm{stab}(Z_{F,\tilde{d}}) = \bar{\mathcal{H}}$. In other words, it suffices to compute the k-definable element $Z_{F,\tilde{d}}$ to find $\bar{\mathcal{H}}$. In addition, Proposition 2.4 states that $\bar{\mathcal{H}}$ is a proto-Galois group. Our method

to compute the defining equations of $Z_{F,\tilde{d}}$ is described in Section 4.1. Our approach seems simpler than the one presented in the step (b) of Algorithm B in [10], since it reduces the number of k-definable elements which we need to compute. However, it is not clear whether the complexity of our method is better or not.

3. Recovering Galois groups

Throughout this section, $I_{F,\tilde{d}}$, $Z_{F,\tilde{d}}$ and $\mathcal{H}$ are as in Proposition 2.4. We will first compute a Zariski closed subset of $Z_{F,\tilde{d}}$ whose stabilizer is $\mathcal{G}^\circ$. Then using the Galois group of a finite Galois extension of k, we construct $I_{\tilde{F}}$ and then the Galois group $\mathcal{G}$, where $I_{\tilde{F}}$ is defined in (2) with some fundamental matrix $\tilde{F}$ and $d = \infty$. Note that $\mathcal{G}^\circ$ is defined as the pre-image of $\mathcal{G}_{\tilde{F}}^\circ$ under the map ϕ_F given in Section 1. It is well-known that $\mathcal{G}^\circ$ is equal to $\mathrm{Gal}(\bar{k}K/\bar{k})$ where $\bar{k}K$ is the Picard–Vessiot extension field of $\bar{k}$ for (1). In the coming sections, we will assume that the following problems can be solved algorithmically.

($P1$) Given an ideal in $k[X]$, compute a Gröbner basis of it with respect to some monomial ordering. The reader is referred to Chapter 2.7 of [4] for Buchberger's Algorithm.

($P2$) Given an unmixed ideal in $k[X]$, compute its primary decomposition and its associated primes. There are several methods for this problem, for instance the methods presented in [8], Section 4 of [6], parts 36 and 42 of [17].

($P3$) Given an irreducible polynomial $P \in k[z]$, compute the Galois group of P over k. A method to compute the Galois group of a polynomial over k was presented in [3]. Note that there are many algorithms to compute the Galois group of a polynomial over the field of rational numbers (see [11] for the survey) and most of them can be generalized to the field $\mathbb{Q}(t)$.

($P4$) Given an unmixed ideal $\mathbb{S}$ in $\bar{k}[X]$ with $\mathrm{Zero}(\mathbb{S}) \cap \mathrm{GL}_n(\bar{k}) \neq \emptyset$, compute a zero of $\mathbb{S}$ in $\mathrm{GL}_n(\bar{k})$. Let $\bar{\mathbb{S}} = \{\mathbb{S}, \det(X)z - 1\}$. By the algorithms developed in [7,14], one can find normal chains (or p-chains) $\mathcal{A}_i$ such that

$$\mathrm{Zero}(\bar{\mathbb{S}}) = \bigcup \mathrm{Zero}\big((\mathcal{A}_i) : I_{\mathcal{A}_i}^\infty\big)$$

where $I_{\mathcal{A}_i}$ is the product of initials of polynomials in $\mathcal{A}_i$. The polynomials in a normal chain $\mathcal{A}_i : P_1, \cdots, P_l$ are of the following form:

$$\begin{aligned} P_1(\mathbf{u}, y_1) &= I_1 y_1^{d_1} + \text{terms in which } y_1 \text{ has degree} < d_1, \\ P_2(\mathbf{u}, y_1, y_2) &= I_2 y_2^{d_2} + \text{terms in which } y_2 \text{ has degree} < d_2, \\ &\cdots \\ P_l(\mathbf{u}, y_1, \cdots, y_l) &= I_l y_l^{d_l} + \text{terms in which } y_l \text{ has degree} < d_l, \end{aligned}$$

where $\{\mathbf{u}\}$ is a set of parameters, $\{\mathbf{u}\} \cup \{y_1, \cdots, y_l\}$ is a permutation of $\{x_{1,1}, \cdots, x_{n,n}, z\}$ and $I_j \in k[\mathbf{u}]$. Fix a normal chain $\mathcal{A}_i$ and pick $\bar{\mathbf{u}} \in k^{n^2+1-l}$ such

that $I_{\mathcal{A}_i}(\bar{\mathbf{u}}) \neq 0$. Then one can compute a zero of $\bar{\mathbb{S}}$ by solving the system

$$\{P_1(\bar{\mathbf{u}}, y_1), P_2(\bar{\mathbf{u}}, y_1, y_2), \cdots, P_l(\bar{\mathbf{u}}, y_1, \cdots, y_l)\}.$$

3.1. Identity component $\mathcal{G}^\circ$

In Section 4.1, we will show how to compute $I_{F,\tilde{d}}$ and $\mathcal{H}_F$. For the moment, we assume that $\mathcal{H}_F$ has been computed. Using the algorithms for the problem $(P1)$, we obtain the identity component $\mathcal{H}_F^\circ$, which is given by the generators of its vanishing ideal. The defining equations of $\mathcal{H}_F^\circ$ will lead to a Zariski closed subset $Z_{\mathcal{H}^\circ}$ of $Z_{F,\tilde{d}}$ such that the stabilizer of $Z_{\mathcal{H}^\circ}$ is $\mathcal{H}^\circ$. Let $\chi_1, \cdots, \chi_l$ be generators of $X(\mathcal{H}_F^\circ)$, where $X(\mathcal{H}_F^\circ)$ is the group of characters of $\mathcal{H}_F^\circ$. We will show that each character corresponds to a hyperexponential element over $\bar{k}$. Assuming we can find $\chi_1, \cdots, \chi_l$ (and we will show how this can be done in Appendix B), the results in [2] allow us to find algebraic relations among hyperexponential elements associated with $\chi_1, \cdots, \chi_l$. These relations together with $Z_{\mathcal{H}^\circ}$ produce a Zariski closed subset Z of $Z_{\mathcal{H}^\circ}$ such that the identity component of $\mathrm{stab}(Z)$ is $\mathcal{G}^\circ$. Using an argument similar to the one used to construct $Z_{\mathcal{H}^\circ}$, we are able to find a Zariski closed subset whose stabilizer is $\mathcal{G}^\circ$.

Let $\bar{k}K$ be the Picard–Vessiot extension field of $\bar{k}$ for (1) and H a subgroup of $\mathrm{GL}_n(C)$. For brevity, we will use $H(\bar{k}K)$ to denote $\mathrm{Zero}(I(H)) \cap \mathrm{GL}_n(\bar{k}K)$ where $I(H)$ is the vanishing ideal of H in $C[X]$. Let $\mathcal{N}$ be an algebraic subgroup of $\mathrm{GL}_n(V)$ and γ an element of $\mathrm{GL}_n(\bar{k})$.

Proposition 3.1. *Suppose that $\gamma^{-1}F \in \mathcal{N}_F(\bar{k}K)$ and $\mathcal{N}_F^\circ$ is defined by $\mathbb{S}$, a set of polynomials in $C[X]$. Set*

$$Z_\gamma = \mathrm{Zero}\big(\{P(\gamma^{-1}X) \mid P(X) \in \mathbb{S}\}\big) \bigcap V_{inv}^n.$$

Then Z_γ is a nonempty subset of $F\mathcal{N}_F$ and $\mathrm{stab}(Z_\gamma) = \mathcal{N}^\circ$.

Proof. As $\mathcal{N}_F$ is an algebraic subgroup of $\mathrm{GL}_n(C)$, there is $g \in \mathcal{N}_F$ such that $\gamma^{-1}Fg \in \mathcal{N}_F^\circ(\bar{k}K)$. That is to say, $Fg \in Z_\gamma$. Hence Z_γ is nonempty. Now write $Z_\gamma = FH$ for some $H \subseteq \mathrm{GL}_n(C)$. For any $h \in \mathrm{GL}_n(C)$,

$$h \in H \quad \Leftrightarrow \quad \gamma^{-1}Fh \in \mathcal{N}_F^\circ(\bar{k}K) \quad \Leftrightarrow \quad \gamma^{-1}Fgg^{-1}h \in \mathcal{N}_F^\circ(\bar{k}K) \quad \Leftrightarrow \quad g^{-1}h \in \mathcal{N}_F^\circ.$$

This implies that $H = g\mathcal{N}_F^\circ$. One then has $Z_\gamma \subseteq F\mathcal{N}_F$ because $g \in \mathcal{N}_F$. This proves the first assertion. As $\mathcal{N}_F^\circ$ is normal in $\mathcal{N}_F$, one has that $H = \mathcal{N}_F^\circ g$. Let $\bar{\mathcal{N}} = \mathrm{stab}(Z_\gamma)$. We then have that

$$\bar{\mathcal{N}} = \mathrm{stab}\big(Z_\gamma g^{-1}\big) = \mathrm{stab}\big(F\mathcal{N}_F^\circ\big).$$

Lemma 2.2 implies that $\bar{\mathcal{N}}_F = \mathcal{N}_F^\circ$, i.e. $\bar{\mathcal{N}} = \mathcal{N}^\circ$. □

Lemma 3.2. *Let α be an element of $\mathrm{Zero}(I_{F,\tilde{d}}) \cap \mathrm{GL}_n(\bar{k})$. Then $\alpha^{-1}F \in \mathcal{H}_F(\bar{k}K)$.*

Proof. It suffices to show that $\alpha \in F\mathcal{H}_F(\bar{k}K)$. From the definition of $Z_{F,\tilde{d}}$, one can see that $Z_{F,\tilde{d}}$ is bounded by $\tilde{d}$ and so is $\mathcal{H}_F$. Assume that Q is a polynomial in $C[X]_{\leq \tilde{d}}$ such that $Q(h) = 0$ for all $h \in \mathcal{H}_F$. Then from the proof of Lemma 2.1, $Q(F^{-1}X)$ is a K-linear combination of elements of $I_{F,\tilde{d}}$. Hence $Q(F^{-1}\alpha) = 0$, which implies that $F^{-1}\alpha \in \mathcal{H}_F(\bar{k}K)$, i.e. $\alpha \in F\mathcal{H}_F(\bar{k}K)$. □

Let α be an element of $\mathrm{Zero}(I_{F,\tilde{d}}) \cap \mathrm{GL}_n(\bar{k})$ and $\mathbb{S}$ a set of polynomials in $C[X]$ which defines $\mathcal{H}_F^\circ$. Set

$$Z_{\mathcal{H}^\circ} = \mathrm{Zero}\big(\{P(\alpha^{-1}X) \mid P(X) \in \mathbb{S}\}\big) \bigcap V_{inv}^n.$$

Then Lemma 3.2 and Proposition 3.1 indicate that $Z_{\mathcal{H}^\circ}$ is a Zariski closed subset of $F\mathcal{H}_F$ and $\mathrm{stab}(Z_{\mathcal{H}^\circ}) = \mathcal{H}^\circ$. Let $\bar{F}$ be any element of $Z_{\mathcal{H}^\circ}$, i.e. $\alpha^{-1}\bar{F} \in \mathcal{H}_F^\circ(\bar{k}K)$. Then we have the following proposition.

Proposition 3.3. *Let $\chi : \mathcal{H}_F^\circ \to C^*$ be a character of $\mathcal{H}_F^\circ$, which is represented by a polynomial in $C[X, 1/\det(X)]$. Then $\chi(\alpha^{-1}\bar{F})$ is a hyperexponential element over $\bar{k}$. Moreover for any $h \in \mathcal{H}_F^\circ$,*

$$\chi\big(\alpha^{-1}\bar{F}h\big) = \chi\big(\alpha^{-1}\bar{F}\big)\chi(h).$$

Proof. Since χ is a character of $\mathcal{H}_F^\circ$, for any $h_1, h_2 \in \mathcal{H}_F^\circ(\bar{k}K)$, $\chi(h_1h_2) = \chi(h_1)\chi(h_2)$. Notice that $\alpha^{-1}\bar{F} \in \mathcal{H}_F^\circ(\bar{k}K)$. For any $h \in \mathcal{H}_F^\circ$,

$$\chi\big(\alpha^{-1}\bar{F}h\big) = \chi\big(\alpha^{-1}\bar{F}\big)\chi(h).$$

Suppose that $\sigma \in \mathcal{G}^\circ$. Then $\sigma(\alpha^{-1}\bar{F}) = \alpha^{-1}\bar{F}[\sigma]$ for some $[\sigma] \in \mathrm{GL}_n(C)$. As $\alpha^{-1}\bar{F}$ belongs to $\mathcal{H}_F^\circ(\bar{k}K)$ that is C-definable, we have that $\sigma(\alpha^{-1}\bar{F}) \in \mathcal{H}_F^\circ(\bar{k}K)$. It follows that $[\sigma] \in \mathcal{H}_F^\circ$. Hence for any $\sigma \in \mathcal{G}^\circ$,

$$\sigma\left(\frac{\chi(\alpha^{-1}\bar{F})'}{\chi(\alpha^{-1}\bar{F})}\right) = \frac{\chi(\alpha^{-1}\bar{F}[\sigma])'}{\chi(\alpha^{-1}\bar{F}[\sigma])} = \frac{\chi(\alpha^{-1}\bar{F})'\chi([\sigma])}{\chi(\alpha^{-1}\bar{F})\chi([\sigma])} = \frac{\chi(\alpha^{-1}\bar{F})'}{\chi(\alpha^{-1}\bar{F})}.$$

Thus $\frac{\chi(\alpha^{-1}\bar{F})'}{\chi(\alpha^{-1}\bar{F})} \in \bar{k}$. □

Suppose that $\chi_1, \cdots, \chi_l$ are the generators of $X(\mathcal{H}_F^\circ)$, all of which are nontrivial and represented by polynomials in $C[X]$. Then each character χ_i corresponds to a hyperexponential element $\chi_i(\alpha^{-1}\bar{F})$, denoted by h_i. Let $v_i = h_i'/h_i$ for all i with $1 \leq i \leq l$, and $E = \bar{k}(h_1, \cdots, h_l)$ that is the Picard–Vessiot extension of $\bar{k}$ for the equations

$$\delta(Y) = \mathrm{diag}(v_1, \cdots, v_l)Y.$$

Note that E is a subfield of $\bar{k}K$. Let $\mathbf{h} = \operatorname{diag}(h_1, \cdots, h_l)$. Then $\mathbf{h}$ is a fundamental matrix of the above equations and $\operatorname{Gal}(E/\bar{k})$ can naturally be embedded into $(C^*)^l$. Denote the image of $\operatorname{Gal}(E/\bar{k})$ by T under this embedding. That is to say,

$$T = \big\{(c_1, \cdots, c_l)^T \in \big(C^*\big)^l \mid \exists \sigma \in \operatorname{Gal}(E/\bar{k}) \text{ s.t. } \sigma(h_i) = c_i h_i,\ i = 1, \cdots, l\big\}.$$

In [2], the authors show that when C is an algebraically closed computable field, given $v_1, \cdots, v_l$, one can compute a set of elements $S = \{h_{\eta_1}, \cdots, h_{\eta_r}\} \subseteq \{h_1, \cdots, h_l\}$ such that

(*i*) $h_{\eta_1}, \cdots, h_{\eta_r}$ are algebraically independent over C;
(*ii*) for each $j \in \{1, \cdots, l\}$, there are an element $f_j \in \bar{k}$ and integers $m_j, m_{i,j}, m_j \neq 0$ satisfying

$$h_j^{m_j} = f_j \prod_{i=1}^{r} h_{\eta_i}^{m_{i,j}}$$

if S is nonempty, or $h_j^{m_j} = f_j$ if S is empty.

The equalities in (*ii*) generate almost all algebraic relations among $h_1, \cdots, h_l$. Due to the proof of Proposition 2.5 in [2], the set $\{y_j^{m_j} - \prod_{i=1}^{r} y_{\eta_i}^{m_{i,j}}, j = 1, 2, \cdots, l\}$ defines an algebraic subgroup of $(C^*)^l$, whose identity component is equal to T. As $\bar{F} \in F\mathcal{H}_F$, it follows from the normality of $\mathcal{H}_F^\circ$ in $\mathcal{H}_F$ that $\mathcal{H}_{\bar{F}}^\circ = \mathcal{H}_F^\circ$. Thus $\mathcal{G}_{\bar{F}}^\circ \subseteq \mathcal{H}_{\bar{F}}^\circ = \mathcal{H}_F^\circ$. Let $\varphi = (\chi_1, \cdots, \chi_l)$. Then we have

Lemma 3.4. $\varphi(\mathcal{G}_{\bar{F}}^\circ) = T$.

Proof. Note that $\mathcal{G}^\circ = \operatorname{Gal}(\bar{k}K/\bar{k})$ and $E \subseteq \bar{k}K$ is a Picard–Vessiot extension field. By the Galois theory, the map $\psi : \mathcal{G}^\circ \to \operatorname{Gal}(E/\bar{k})$ given by $\psi(\sigma) = \sigma|_E$ for any $\sigma \in \mathcal{G}^\circ$ is surjective. For any $[\sigma] \in \mathcal{G}_{\bar{F}}^\circ$, there is $\sigma \in \mathcal{G}^\circ$ such that $\sigma(\bar{F}) = \bar{F}[\sigma]$ and then

$$\begin{aligned}\psi(\sigma)(\mathbf{h}) = \sigma(\mathbf{h}) &= \big(\sigma(h_1), \cdots, \sigma(h_l)\big) = \big(\chi_1\big(\alpha^{-1}\bar{F}[\sigma]\big), \cdots, \chi_l\big(\alpha^{-1}\bar{F}[\sigma]\big)\big) \\ &= \big(\chi_1\big(\alpha^{-1}\bar{F}\big)\chi_1\big([\sigma]\big), \cdots, \chi_l\big(\alpha^{-1}\bar{F}\big)\chi_l\big([\sigma]\big)\big) = \big(\chi_1\big([\sigma]\big)h_1, \cdots, \chi_l\big([\sigma]\big)h_l\big).\end{aligned}$$

By the definition of T, we have that $\varphi([\sigma]) = (\chi_1([\sigma]), \cdots, \chi_l([\sigma])) \in T$. Now assume that $(c_1, \cdots, c_l)^T \in T$. Then there is $\sigma \in \operatorname{Gal}(E/\bar{k})$ such that $\sigma(h_j) = c_j h_j$ for all j with $1 \leq j \leq l$. Due to the surjectivity of ψ, there is $\hat{\sigma} \in \mathcal{G}^\circ$ such that $\psi(\hat{\sigma}) = \sigma$. Assume that $\hat{\sigma}(\bar{F}) = \bar{F}[\hat{\sigma}]$ for some $[\hat{\sigma}] \in \mathcal{G}_{\bar{F}}^\circ$. It follows that

$$c_j = \frac{\sigma(h_j)}{h_j} = \frac{\hat{\sigma}(h_j)}{h_j} = \frac{\chi_j(\alpha^{-1}\bar{F}[\hat{\sigma}])}{\chi_j(\alpha^{-1}\bar{F})} = \frac{\chi_j(\alpha^{-1}\bar{F})\chi_j([\hat{\sigma}])}{\chi_j(\alpha^{-1}\bar{F})} = \chi_j\big([\hat{\sigma}]\big), \quad j = 1, \cdots, l.$$

In other words, $(c_1, \cdots, c_l)^T$ is the image of $[\hat{\sigma}]$ under the morphism φ. So $\varphi(\mathcal{G}_{\bar{F}}^\circ) = T$. □

Set

$$J = \{P(\alpha^{-1}X) \mid P \in \mathbb{S}\} \bigcup \left\{ \chi_j(\alpha^{-1}X)^{m_j} - f_j \prod_{i=1}^{r} \chi_{\eta_i}(\alpha^{-1}X)^{m_{i,j}},\ j = 1, \cdots, l \right\},$$

where $\mathbb{S}$ is the set of generators of $I(\mathcal{H}^\circ_{\bar{F}})$. It is easy to see that $\bar{F}$ is a zero of J. Let $Z_J = \mathrm{Zero}(J) \cap V^n_{inv}$ and $\bar{\mathcal{H}} = \mathrm{stab}(Z_J)$.

Proposition 3.5.

(*a*) $\bar{\mathcal{H}}^\circ = \mathcal{G}^\circ$.
(*b*) *Suppose that* $\beta \in \mathrm{Zero}(J) \cap \mathrm{GL}_n(\bar{k})$. *Then* $\beta^{-1}\bar{F} \in \bar{\mathcal{H}}_{\bar{F}}(\bar{k}K)$.

Proof. Write $Z_J = \bar{F}\bar{H}$ for some $\bar{H} \subseteq \mathrm{GL}_n(C)$. We first claim that $\bar{H} = \bar{\mathcal{H}}_{\bar{F}}$. Recall that $\alpha^{-1}\bar{F} \in \mathcal{H}^\circ_{\bar{F}}(\bar{k}K)$. An easy calculation yields that

$$\bar{H} = \mathcal{H}^\circ_F \bigcap \mathrm{Zero}\left(\left\{ \chi_j^{m_j} - \prod_{i=1}^{r} \chi_{\eta_i}^{m_{i,j}},\ j = 1, 2, \cdots, l \right\} \right). \tag{3}$$

Therefore $\bar{H}$ is a group and then the claim follows from Lemma 2.2.

(*a*) To prove $\bar{\mathcal{H}}^\circ = \mathcal{G}^\circ$, it suffices to show that $\bar{\mathcal{H}}^\circ_{\bar{F}} = \mathcal{G}^\circ_{\bar{F}}$, i.e. $\bar{H}^\circ = \mathcal{G}^\circ_{\bar{F}}$. It is easy to see that

$$\varphi(\bar{H}) = \varphi(\mathcal{H}^\circ_F) \bigcap \mathrm{Zero}\left(\left\{ y_j^{m_j} - \prod_{i=1}^{r} y_{\eta_i}^{m_{i,j}},\ j = 1, 2, \cdots, l \right\} \right).$$

Lemma 3.4 and the discussion before it indicate that the identity component of $\varphi(\bar{H})$ is equal to T. Note that $\ker(\varphi) = (\mathcal{H}^\circ_F)^t = (\mathcal{H}^\circ_{\bar{F}})^t$. Then we have $\ker(\varphi) \subseteq \mathcal{G}^\circ_{\bar{F}}$, since $\mathcal{H}$ is a proto-Galois group. As Z_J is $\bar{k}$-definable, $\mathcal{G}^\circ \subseteq \bar{\mathcal{H}}$ and then $\mathcal{G}^\circ_{\bar{F}} \subseteq \bar{\mathcal{H}}_{\bar{F}} = \bar{H}$. Now we have

$$\left[\bar{H} : \mathcal{G}^\circ_{\bar{F}}\right] = \left[\bar{H}/\ker(\varphi) : \mathcal{G}^\circ_{\bar{F}}/\ker(\varphi)\right] = \left[\varphi(\bar{H}) : \varphi(\mathcal{G}^\circ_{\bar{F}})\right].$$

Owing to Lemma 3.4, $\varphi(\mathcal{G}^\circ_{\bar{F}})$ is equal to T that is the identity component of $\varphi(\bar{H})$. Hence $[\bar{H} : \mathcal{G}^\circ_{\bar{F}}]$ is finite. Thus $\bar{H}^\circ = \mathcal{G}^\circ_{\bar{F}}$, which proves (*b*).

(*b*) As both β and $\bar{F}$ are zeros of J, the construction of J implies that

$$\beta^{-1}\bar{F} \in \mathcal{H}^\circ_F(\bar{k}K) \quad \text{and} \quad \chi_j^{m_j}(\bar{F}^{-1}\beta) - \prod_{i=1}^{r} \chi_{\eta_i}^{m_{i,j}}(\bar{F}^{-1}\beta) = 0, \quad j = 1, \cdots, l.$$

Hence $\beta^{-1}\bar{F} \in \bar{H}(\bar{k}K)$. So $\beta^{-1}\bar{F} \in \bar{\mathcal{H}}_{\bar{F}}(\bar{k}K)$. □

Let β be a zero of J in $\mathrm{GL}_n(\bar{k})$. The above proposition implies that $\beta^{-1}\bar{F} \in \bar{\mathcal{H}}_{\bar{F}}(\bar{k}K)$. Assume that $\mathcal{G}^\circ_{\bar{F}}$ (and thus $\bar{\mathcal{H}}^\circ_{\bar{F}}$) is defined by $\bar{\mathbb{S}}$, a set of polynomials in $C[X]$. Set

$$Z_{\mathcal{G}^\circ} = \mathrm{Zero}\big(\{P(\beta^{-1}X) \mid P \in \bar{\mathbb{S}}\}\big) \cap V^n_{inv}.$$

Then Proposition 3.1 induces that $Z_{\mathcal{G}^\circ}$ is a Zariski closed subset of $\bar{F}\bar{\mathcal{H}}_{\bar{F}}$ and $\mathrm{stab}(Z_{\mathcal{G}^\circ}) = \mathcal{G}^\circ$.

3.2. Galois group $\mathcal{G}$

Let β and $Z_{\mathcal{G}^\circ}$ be as in the previous section and $\tilde{F}$ an element of $Z_{\mathcal{G}^\circ}$. Then $\beta^{-1}\tilde{F} \in \mathcal{G}^\circ_{\bar{F}}(\bar{k}K)$. Moreover, since $Z_{\mathcal{G}^\circ}$ is a subset of $\bar{F}\bar{\mathcal{H}}_{\bar{F}}$, one has that $\tilde{F} = \bar{F}h$ for some $h \in \bar{\mathcal{H}}_{\bar{F}}$. This implies that $\mathcal{G}^\circ_{\tilde{F}} = h^{-1}\mathcal{G}^\circ_{\bar{F}}h$. At the same time, by Proposition 3.5, $\mathcal{G}^\circ_{\bar{F}}$ is normal in $\bar{\mathcal{H}}_{\bar{F}}$. Therefore $h^{-1}\mathcal{G}^\circ_{\bar{F}}h = \mathcal{G}^\circ_{\bar{F}}$. In the sequel, $\mathcal{G}^\circ_{\tilde{F}} = \mathcal{G}^\circ_{\bar{F}}$.

Let k_G be the Galois closure of $k(\beta^{-1})$, where $k(\beta^{-1})$ denotes the extension field of k by joining the entries of β^{-1}. By the algorithms for $(P3)$, one can compute $\mathrm{Gal}(k_G/k)$. For any $\tau \in \mathrm{Gal}(k_G/k)$, set

$$J_{\tau(\beta)} = \big\langle \{P(\tau(\beta)^{-1}X) \mid P(X) \in I(\mathcal{G}^\circ_{\tilde{F}})\}\big\rangle$$

where $\langle * \rangle$ denotes the ideal in $k_G[X]$ generated by $*$.

Proposition 3.6. *Let $I_{\tilde{F}}$ be defined in (2) with $F = \tilde{F}$ and $d = \infty$. Then*

$$I_{\tilde{F}} = \Big(\bigcap_{\tau \in \mathrm{Gal}(k_G/k)} J_{\tau(\beta)}\Big) \bigcap k[X].$$

Proof. Denote the ideal in the right-hand side of the above equality by Φ. Suppose that $P(X) \in \Phi$. Then $P(X) \in J_\beta$. Note that $\mathrm{Zero}(J_\beta) \cap V^n_{inv} = Z_{\mathcal{G}^\circ}$. So $P(\tilde{F}) = 0$. That is to say, $P(X) \in I_{\tilde{F}}$. Thus $\Phi \subseteq I_{\tilde{F}}$. Conversely, suppose that $P(X) \in I_{\tilde{F}}$. Then $P(\tilde{F}) = 0$. Applying $\mathcal{G}^\circ$ to it, we obtain that $P(\tilde{F}g) = 0$ for every $g \in \mathcal{G}^\circ_{\tilde{F}}$ and thus $P(\tilde{F}g) = 0$ for all $g \in \mathcal{G}^\circ_{\tilde{F}}(\bar{k}K)$. Since $\beta^{-1}\tilde{F} \in \mathcal{G}^\circ_{\tilde{F}}(\bar{k}K)$, $\tilde{F}\mathcal{G}^\circ_{\tilde{F}}(\bar{k}K) = \beta\mathcal{G}^\circ_{\tilde{F}}(\bar{k}K)$. This implies that $P(\beta X)$ vanishes on $\mathcal{G}^\circ_{\tilde{F}}(\bar{k}K)$. Consequently, $P(\beta X)$ belongs to $\langle I(\mathcal{G}^\circ_{\tilde{F}})\rangle$ and so $P(X) \in J_\beta$. Because all coefficients of $P(X)$ are in k, $P(X) \in J_{\tau(\beta)}$ for all $\tau \in \mathrm{Gal}(k_G/k)$. Hence $P(X) \in \Phi$. □

If $I_{\tilde{F}}$ is computed, then it is easy to verify that

$$\mathcal{G}_{\tilde{F}} = \{g \in \mathrm{GL}_n(C) \mid \forall P(X) \in I_{\tilde{F}},\ P(Xg) \in I_{\tilde{F}}\}.$$

In the following, we present another method to compute $\mathcal{G}_{\tilde{F}}$ that avoids computing $I_{\tilde{F}}$. From Proposition 3.20 and Theorem 3.11 of [15], there is a Picard–Vessiot extension field, say $\tilde{K}$, of k that contains k_G and K as subfields. Then Galois theory implies that if

τ is an element of $\mathrm{Gal}(k_G/k)$ (or $\mathcal{G}$), then there is $\rho \in \mathrm{Gal}(\tilde{K}/k)$ such that the restriction of ρ on k_G (or K) is equal to τ. Let $\bar{\mathbb{S}}$ be a set of generators of $I(\mathcal{G}^\circ_{\tilde{F}})$. Set

$$\tilde{G} = \bigcup_{\tau \in \mathrm{Gal}(k_G/k)} \big\{ g \in \mathrm{GL}_n(C) \;\big|\; \forall Q \in \bar{\mathbb{S}},\ Q\big(\tau(\beta)^{-1}\tilde{F}g\big) = 0 \big\}.$$

Then we have

Proposition 3.7. $\mathcal{G}_{\tilde{F}} = \tilde{G}$.

Proof. We first prove that $\mathcal{G}_{\tilde{F}} \subseteq \tilde{G}$. Assume that $[\sigma] \in \mathcal{G}_{\tilde{F}}$. Then there is $\sigma \in \mathcal{G}$ such that $\sigma(\tilde{F}) = \tilde{F}[\sigma]$ and furthermore there is $\rho \in \mathrm{Gal}(\tilde{K}/k)$ such that $\rho|_K = \sigma$. Let $\tau = \rho|_{k_G}$. Note that $\tau \in \mathrm{Gal}(k_G/k)$. Then for all $Q \in \bar{\mathbb{S}}$,

$$\rho\big(Q\big(\beta^{-1}\tilde{F}\big)\big) = Q\big(\tau(\beta)^{-1}\sigma(\tilde{F})\big) = Q\big(\tau(\beta)^{-1}\tilde{F}[\sigma]\big) = 0.$$

This implies that $[\sigma] \in \tilde{G}$. Conversely, assume that $g \in \tilde{G}$. Then there is $\tau \in \mathrm{Gal}(k_G/k)$ such that $Q(\tau(\beta)^{-1}\tilde{F}g) = 0$ for all $Q \in \bar{\mathbb{S}}$. Meanwhile, there is $\rho \in \mathrm{Gal}(\tilde{K}/k)$ such that $\rho|_{k_G} = \tau^{-1}$. Since $\rho|_K \in \mathcal{G}$, there is $h \in \mathcal{G}_{\tilde{F}}$ such that $\rho|_K(\tilde{F}) = \tilde{F}h$. Now we have that

$$\forall Q \in \bar{\mathbb{S}}, \quad \rho\big(Q\big(\tau(\beta)^{-1}\tilde{F}g\big)\big) = Q\big(\beta^{-1}\tilde{F}hg\big) = 0.$$

Hence $\beta^{-1}\tilde{F}hg \in \mathcal{G}^\circ_{\tilde{F}}(\tilde{K})$, which implies that $hg \in \mathcal{G}^\circ_{\tilde{F}}$ and thus $g \in \mathcal{G}_{\tilde{F}}$. □

4. Modified Hrushovski's algorithm

Now we are ready to present the algorithm. Instead of $\mathcal{G}$, we shall compute $\mathcal{G}_{\tilde{F}}$ for some fundamental matrix $\tilde{F}$. Throughout this section, C will denote the algebraic closure of a computable field of characteristic zero.

Algorithm 4.1. Input: A linear differential equation (1) with coefficients in $C(t)$.
Output: the Galois group $\mathcal{G}_{\tilde{F}}$.

(*a*) By Corollary B.15, determine an integer $\tilde{d}$ such that there is a proto-Galois group of (1) bounded by $\tilde{d}$.
(*b*) Compute a fundamental matrix F (the first finitely many terms of its formal power series expansion at some point). Compute $I_{F,\tilde{d}}$ and then $\mathcal{H}_F$, where $I_{F,\tilde{d}}$ is defined in (2) and $\mathcal{H}$ is the stabilizer of $\mathrm{Zero}(I_{F,\tilde{d}}) \cap V^n_{inv}$. (See Section 4.1.)
(*c*) Compute $\mathcal{H}^\circ_F$ and find a zero α of $I_{F,\tilde{d}}$ in $\mathrm{GL}_n(\overline{C(t)})$ and an $\bar{F}$ in V^n_{inv} such that $\alpha^{-1}\bar{F}$ is an element of $\mathcal{H}^\circ_F(\bar{k}K)$. (See Section 4.2.)
(*d*) Compute generators of $X(\mathcal{H}^\circ_F)$, say $\chi_1, \cdots, \chi_l$, which are represented by polynomials in $C[X]$. Denote $\chi_i(\alpha^{-1}\bar{F})$ by h_i for $i = 1, 2, \cdots, l$. By Proposition 3.1, h_i is hyperexponential over $\overline{C(t)}$. Compute these h_i. (See Section 4.3.)

(e) Using the method developed in (Proposition 2.4, [2]), compute algebraic relations for $h_1, \cdots, h_l$, say

$$\left\{ h_j^{m_j} - f_j \prod_{i=1}^{r} h_{\eta_i}^{m_{i,j}},\ j = 1, 2, \cdots, l \right\}$$

where $f_j \in \overline{C(t)}$ and $h_{\eta_1}, \cdots, h_{\eta_r}$ are algebraically independent over $C(t)$.

(f) Denote a set of generators of $I(\mathcal{H}_F^\circ)$ by $\mathbb{S}$, a subset of $C[X]$ and set

$$J = \left\{ P\left(\alpha^{-1}X\right) \mid P \in \mathbb{S} \right\} \bigcup \left\{ \chi_j^{m_j}\left(\alpha^{-1}X\right) - f_j \prod_{i=1}^{r} \chi_{\eta_i}^{m_{i,j}}\left(\alpha^{-1}X\right),\ j = 1, \cdots, l \right\}.$$

Compute $\bar{\mathcal{H}} = \mathrm{stab}(\mathrm{Zero}(J) \cap V_{inv}^n)$ and then $\bar{\mathcal{H}}^\circ$ that is equal to $\mathcal{G}^\circ$.

(g) As in the step (c), compute $\mathcal{G}_{\bar{F}}^\circ$ and find β in $\mathrm{Zero}(J) \cap \mathrm{GL}_n(\overline{C(t)})$ and an $\tilde{F}$ in V_{inv}^n such that $\beta^{-1}\tilde{F} \in \mathcal{G}_{\bar{F}}^\circ(\bar{k}K)$. (See Section 4.2.)

(h) Denote a set of generators of $I(\mathcal{G}_{\bar{F}}^\circ)$ by $\bar{\mathbb{S}} \subseteq C[X]$. Let k_G be the Galois closure of $C(t)(\beta^{-1})$, where $C(t)(\beta^{-1})$ is the extension field of $C(t)$ by joining the entries of β^{-1}. Compute $\mathrm{Gal}(k_G/C(t))$ and

$$\mathcal{G}_{\tilde{F}} = \bigcup_{\tau \in \mathrm{Gal}(k_G/C(t))} \left\{ g \in \mathrm{GL}_n(C) \mid \forall Q \in \bar{\mathbb{S}},\ Q\left(\tau(\beta)^{-1}\tilde{F}g\right) = 0 \right\}.$$

(i) Return $\mathcal{G}_{\tilde{F}}$.

The correctness of the algorithm follows from the results in Sections 2 and 3. In the following, we will present several computation details omitted in the previous sections. Generally, it is difficult to find a fundamental matrix of (1). What we can compute is the first finitely many terms of formal power series solutions of (1) at some point of C. Let z be a generic point of C. Expanding A at $t = z$, we have

$$A = A_0 + A_1(t-z) + A_2(t-z)^2 + \cdots, \quad A_i \in \mathrm{Mat}_n\left(C\left[z, \frac{1}{q(z)}\right]\right) \tag{4}$$

where $q(z)$ is a polynomial in $C[z]$ such that $q(z)$ is the least common multiple of the denominators of the entries of A. Using the above expansion, we can compute a formal power series solutions of (1) that has the following form

$$\Gamma_z = I_n + D_1(t-z) + D_2(t-z)^2 + \cdots, \quad D_i \in \mathrm{Mat}_n\left(C\left[z, \frac{1}{q(z)}\right]\right).$$

Assume that a is an element of C such that $q(a) \neq 0$. Then Γ_z can be specialized to Γ_a that is a formal power series solution of (1) at $t = a$. The field k can be naturally embedded into $C((t-a))$, the field of Laurent series in $t-a$. Due to Proposition 1.22 of [23], $k(\Gamma_a)$

is a Picard–Vessiot field for (1) over k. Therefore K and $k(\Gamma_a)$ are k-isomorphic as differential fields. In other words, K can be embedded in to $C((t-a))$. Let $\phi_a : K \to C((t-a))$ be this embedding and $F_a = \phi_a^{-1}(\Gamma_a)$. Then F_a is a fundamental matrix of (1) with entries in K. Let γ be an element in $\bar{k}$. Assume further that a is a regular point of γ, i.e. γ has a formal power series expansion at $t = a$. Then the map ϕ_a can be extended into an embedding of $K(\gamma)$ into $C((t-a))$. Note that we do not know the element F_a since at this point we do not know K. So in the following sections, we shall only work with Γ_a during the process of computations.

4.1. Computing $I_{F_a,\tilde{d}}$ and $\mathcal{H}_{F_a}$

Since K and $k(\Gamma_a)$ are k-isomorphic, $I_{F_a,\tilde{d}} = I_{\Gamma_a,\tilde{d}}$. So to find $I_{F_a,\tilde{d}}$, it suffices to compute $I_{\Gamma_a,\tilde{d}}$. Corollary A.5 says that the coefficients of defining polynomials in $C(t)[X]_{\leq\tilde{d}}$ of $Z_{F,\tilde{d}}$ can be chosen to be rational functions bounded by an integer ℓ. Without loss of generality, we may assume that all these coefficients are polynomial in t which are bounded by 2ℓ. Let

$$P_{\mathbf{c}}(X) = \sum_{|\vec{m}|\leq\tilde{d}} \left(\sum_{0\leq i\leq 2\ell} c_{i,\vec{m}}(t-a)^i \right) X^{\vec{m}}, \quad \mathbf{c} = (\cdots, c_{i,\vec{m}}, \cdots),$$

where the $c_{i,\vec{m}}$ are indeterminates. A small modification of Theorem 1 in [1] yields the following theorem that bounds the order of $P_{\mathbf{c}}(\Gamma_a)$.

Theorem 4.2. *One can compute an integer N depending on A, n, ℓ such that*

$$P_{\mathbf{c}}(\Gamma_a) = 0 \quad \textit{or} \quad \operatorname{ord}_{t=a}\big(P_{\mathbf{c}}(\Gamma_a)\big) \leq N.$$

Proof. Note that Theorem 1 in [1] works for the case that $P_{\mathbf{c}}(X)$ is homogeneous in X. Consider Γ_a as a vector with n^2 entries. Then $(\Gamma_a, 1)$ is a solution of the system

$$\delta(Y) = \operatorname{diag}(\underbrace{A, A, \cdots, A}_{n}, 0)Y$$

and $P_{\mathbf{c}}(\Gamma_a)$ is homogeneous in the entries of $(\Gamma_a, 1)$. The theorem then follows from Theorem 1 in [1]. □

The above theorem can be generalized to the case that the coefficients of $P_{\mathbf{c}}(X)$ involve algebraic functions. More precisely, let γ be an algebraic function with minimal polynomial $Q(x)$ and let $l = \deg(Q(x))$. Assume that $\mathbf{w} = (1, \gamma, \gamma^2, \cdots, \gamma^{l-1})^T$. Then it is easy to see that $\mathbf{w}$ is a solution of linear differential equations $\delta(Y) = BY$ where $B \in \operatorname{Mat}_l(C(t))$ can be constructed from $Q(x)$. Let

$$\tilde{P}_{\mathbf{c}}(X) = \sum_{|\vec{m}|\le \tilde{d}} \left(\sum_{j=1}^{l} \Big(\sum_{0\le i\le 2\ell} c_{i,j,\vec{m}} (t-a)^i \Big) \gamma^j \right) X^{\vec{m}}, \quad \mathbf{c} = (\cdots, c_{i,j,\vec{m}}, \cdots).$$

Assume that $t = a$ is a regular point of γ. Then

Corollary 4.3. *There is an integer $\tilde{N}$ depending on A, $Q(x)$, n, ℓ such that*

$$\tilde{P}_{\mathbf{c}}(\Gamma_a) = 0 \quad or \quad \mathrm{ord}_{t=a} \tilde{P}_{\mathbf{c}}(\Gamma_a) \le \tilde{N}.$$

Proof. We only need to consider the system

$$\delta(Y) = \mathrm{diag}(\underbrace{A, \cdots, A}_{n}, B, 0)Y.$$

Then the corollary follows from the above theorem. □

Let $\mathcal{S}$ be the set of the coefficients of the first $N+2$ terms of $P_{\mathbf{c}}(\Gamma_a)$. Then $\mathcal{S}$ is a linear system in $\mathbf{c}$ and

$$P_{\bar{\mathbf{c}}}(\Gamma_a) = 0 \quad \Leftrightarrow \quad \bar{\mathbf{c}} \text{ is a solution of } \mathcal{S}.$$

So computing $I_{\Gamma_a,\tilde{d}}$ (and thus $I_{F_a,\tilde{d}}$) is reduced to solving the linear system $\mathcal{S}$.

Assume that $I_{F_a,\tilde{d}}$ is computed. Then we can compute $\mathcal{H}_{F_a}$ as follows. For any $h \in \mathcal{H}_{F_a}$, $F_a h \in Z_{F_a,\tilde{d}}$. It implies that for any $P(X) \in I_{F_a,\tilde{d}}$, $P(F_a h) = 0$ and so that $P(Xh) \in I_{F_a,\tilde{d}}$. This induces the defining equations for $\mathcal{H}_{F_a}$. More precisely, let $P_1(X), \cdots, P_\mu(X)$ be a $C(t)$-basis of $I_{F_a,\tilde{d}}$. Let $\mathbf{x} = (\cdots, X^{\vec{m}}, \cdots)$ be a vector consisting of all monomials in X with degree not greater than $\tilde{d}$, where $X^{\vec{m}} = x_{1,1}^{m_{1,1}} x_{1,2}^{m_{1,2}} \cdots x_{n,n}^{m_{n,n}}$. For any $h \in \mathrm{GL}_n(C)$, there is $[h] \in \mathrm{GL}_{\binom{n^2+\tilde{d}}{\tilde{d}}}(C)$ such that

$$h \cdot \mathbf{x} = \big(\cdots, (Xh)^{\vec{m}}, \cdots\big) = \mathbf{x}[h].$$

For any $i = 1, \cdots, \mu$, there is $\mathbf{p}_i \in C(t)^{\binom{n^2+\tilde{d}}{\tilde{d}}}$ such that $P_i(X) = \mathbf{x}\mathbf{p}_i$. Then we have

$$h \in \mathcal{H}_{F_a} \quad \Leftrightarrow \quad \forall i, P_i(Xh) = \mathbf{x}[h]\mathbf{p}_i \in I_{F_a,\tilde{d}} \quad \Leftrightarrow \quad \forall i, [h]\mathbf{p}_i \wedge \mathbf{p}_1 \wedge \mathbf{p}_2 \wedge \cdots \wedge \mathbf{p}_\mu = 0.$$

This induces the defining equations for $\mathcal{H}_{F_a}$.

Example 4.4. Consider the following equations

$$\delta \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \frac{t}{1-t^2} & -\frac{1}{1-t^2} \\ \frac{2}{1-t^2} & -\frac{2t}{1-t^2} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}. \tag{5}$$

We shall compute a proto-Galois group. Let us first compute $I_{\Gamma_0,1}$. We are not going to calculate the coefficient bound ℓ for $Z_{\Gamma_0,1}$. Instead, we compute $I_{\Gamma_0,1}$ as follows. Set

$$P(X) = \sum_{|\vec{m}|\leq 1} \left(\sum_{i=0}^{2} c_{i,\vec{m}} t^i \right) X^{\vec{m}}$$

where $c_{i,\vec{m}}$ is indeterminate. Then due to Theorems 1 and 1a of [1], we have that

$$\mathrm{ord}_{t=0}\big(P(\Gamma_0)\big) \leq sN + c_1 sh + c_2 s^2 = 30$$

where $N = 2$, $h = 1$, $s = 5$, $c_1 = -1$, $c_2 = 1$. Compute the first 31 terms of a formal power series solution Γ_0 of (5), say

$$\bar{\Gamma}_0 = I_2 + \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix} t + \begin{pmatrix} -\frac{1}{2} & 0 \\ 0 & -2 \end{pmatrix} t^2 + \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} t^3 + \cdots + \begin{pmatrix} -\frac{334305}{67108864} & 0 \\ 0 & 0 \end{pmatrix} t^{30}.$$

Denote the set of the coefficients of the first 31 terms of $P(\bar{\Gamma}_0)$ by $\mathcal{S}$. Then $\mathcal{S}$ is a linear system in $c_{i,\vec{m}}$ and each solution of $\mathcal{S}$ corresponds to an element of $I_{\Gamma_0,1}$. One then has that $I_{\Gamma_0,1}$ contains the following vector space

$$\mathcal{V} = \mathrm{span}_k\big\{x_{1,2} + t, x_{2,1} - 2tx_{1,1}, x_{2,2} + 2t^2 - 1\big\}.$$

One can verify that if $P \in k[X]_{\leq 1}$ and $P(\Gamma_0) = 0$, then $P \in \mathcal{V}$. Hence $\mathcal{V} = I_{\Gamma_0,1} = I_{F_0,1}$. Let $\mathcal{H} = \mathrm{stab}(Z_{F_0,1})$. Then

$$\mathcal{H}_{F_0} = \left\{ \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} \;\middle|\; c \in C \setminus \{0\} \right\}$$

Since elements of $\mathcal{H}_{F_0}$ are semi-simple, $\mathcal{H}_{F_0}$ is a proto-Galois group.

4.2. Computing α and $\bar{F}$

Assume that we have calculated $I_{F_a,\tilde{d}}$ and $\mathcal{H}_{F_a}$. The algorithms for the problem $(P1)$ enable us to obtain $\mathcal{H}^\circ_{F_a}$, which is given by a set of generators of $I(\mathcal{H}^\circ_{F_a})$. Compute a zero α of $I_{F_a,\tilde{d}}$ in $\mathrm{GL}_n(\overline{C(t)})$ by the method presented in $(P4)$. Assume that $b \in C$ is a regular point of α^{-1} and $q(b) \neq 0$, where $q(z)$ is as in (4). It is well-known that there is $g \in \mathrm{GL}_n(C)$ such that $\bar{F} = F_b g$. We are going to find such g. One has that $\alpha^{-1} F_b g \in \mathcal{H}^\circ_{F_a}(\bar{k}K)$ if and only if for any $P \in I(\mathcal{H}^\circ_{F_a})$, $P(\alpha^{-1} F_b g) = 0$. Assume that $P \in I(\mathcal{H}^\circ_{F_a})$. The application of ϕ_b to $P(\alpha^{-1} F_b g)$ yields that

$$P\big(\alpha^{-1} \Gamma_b g\big) = 0.$$

Using the bound given in Theorem 4.2, the above condition induces the defining equations for g. Compute such a g and let $\bar{F} = F_b g$.

Example 4.5. (Example 4.4 continued.) Let

$$\alpha = \begin{pmatrix} 1 & -t \\ 2t & 1-2t^2 \end{pmatrix}.$$

Then $\alpha \in \mathrm{Zero}(I_{F_0,1})$ and by Lemma 3.2, $\alpha^{-1}F_0 \in \mathcal{H}_{F_0}(\bar{k}K)$. Notice that $\mathcal{H}_{F_0} = \mathcal{H}^{\circ}_{F_0}$. We can take F_0 as $\bar{F}$.

4.3. Computing h_i

By Algorithm B.19 of Appendix B, we can find a set of generators of $X(\mathcal{H}^{\circ}_{F_a})$, say $\chi_1, \cdots, \chi_l$. Assume that $\chi_1, \cdots, \chi_l$ are represented by polynomials of degree not greater than an integer κ. Denote the monomials in the entries of $\alpha^{-1}\bar{F}$ with degree not greater than κ by $\mathbf{m}_1, \cdots, \mathbf{m}_m$. Then each $\mathbf{m}_i$ satisfies a linear differential operator L_i with coefficients in $C(t)(\alpha^{-1})$. Let L be the least common left multiple of $L_1, \cdots, L_m$. Then for each $i = 1, \cdots, l$, $h_i = \chi_i(\alpha^{-1}\bar{F})$ is a hyperexponential solution of L. To compute h_i, it means to calculate $v_i = h_i'/h_i$ where $i = 1, \cdots, l$. From [18], one can compute all hyperexponential solutions of L and then the bounds for minimal polynomials of $\bar{h}'/\bar{h}$ where $\bar{h}$ is any hyperexponential solution. Using these bounds and Hermite–Padé approximation, one can recover v_i from the series expansion of $\chi_i(\alpha^{-1}\bar{F})'/\chi_i(\alpha^{-1}\bar{F})$.

Example 4.6. (Example 4.5 continued.) One can readily see that $x_{1,1}$ represents a character of $\mathcal{H}^{\circ}_{F_0}$, say χ_1, and χ_1 generates $X(\mathcal{H}^{\circ}_{F_0})$. Meanwhile, $\alpha^{-1}\bar{F}$ is a fundamental matrix of

$$\delta \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \frac{t}{t^2-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

This implies that

$$\chi_1\big(\alpha^{-1}\bar{F}\big)' = \frac{t}{t^2-1}\chi_1\big(\alpha^{-1}\bar{F}\big), \quad \text{i.e. } v_1 = \frac{t}{t^2-1}.$$

In the following, we calculate the algebraic relations of $\chi_1(\alpha^{-1}\bar{F})$ and $\mathcal{G}^{\circ}_{\bar{F}}$. An easy calculation yields that $\chi_1(\alpha^{-1}\bar{F})^2 = c(t^2-1)$ for some $c \in C$. Note that $\bar{F} = F_0$. Applying ϕ_0 to $\chi_1(\alpha^{-1}\bar{F})^2 = c(t^2-1)$, one has that

$$\chi_1\big(\alpha^{-1}\Gamma_0\big)^2 = c\big(t^2-1\big).$$

Since $(\alpha^{-1}\Gamma_0)_{t=0} = I_2$, $\chi_1(\alpha^{-1}\Gamma_0)_{t=0} = 1$ and so $c = -1$. Let $\mathbb{S} = \{x_{1,2}, x_{2,1}, x_{2,2} - 1\}$. Then the ideal $I(\mathcal{H}^{\circ}_{F})$ is generated by $\mathbb{S}$. Set

$$J = \big\{P\big(\alpha^{-1}X\big) \mid P \in \mathbb{S}\big\} \bigcup \big\{\chi_1^2\big(\alpha^{-1}X\big) + \big(t^2-1\big)\big\}.$$

In other words,

$$J = \left\{ \begin{array}{ll} (1-2t^2)x_{1,2} + tx_{2,2}, & x_{2,1} - 2tx_{1,1}, \\ x_{2,2} - 2tx_{1,2} - 1, & ((1-2t^2)x_{1,1} + tx_{2,1})^2 + (t^2-1) \end{array} \right\}.$$

Let $\bar{\mathcal{H}} = \mathrm{stab}(Z_J)$. Then

$$\bar{\mathcal{H}}_{\bar{F}} = \left\{ \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, c^2 = 1 \right\}.$$

Hence $\mathcal{G}^{\circ}_{\bar{F}} = \bar{\mathcal{H}}_{\bar{F}} = I_2$.

4.4. Computing $\mathcal{G}_{\tilde{F}}$

The method described in Section 4.2 can be adapted to find β and $\tilde{F}$ in step (g). So far, in step (g), we obtain β and $\tilde{F}$ satisfying that $\beta^{-1}\tilde{F} \in \mathcal{G}^{\circ}_{\bar{F}}(\bar{k}K)$, and a set of generators of $I(\mathcal{G}^{\circ}_{\bar{F}})$, denoted by a subset $\bar{\mathbb{S}}$ of $C[X]$. Assume that $t = c$ is the point we pick to find β and $\tilde{F}$ in step (g). That is to say, $\phi_c(\tilde{F}) = \Gamma_c \tilde{g}$ for some $\tilde{g} \in \mathrm{GL}_n(C)$ and β^{-1} has a formal power series expansion at the point $t = c$. By Corollary 4.3, there is an integer $\tilde{N}$ such that for all $Q \in \bar{\mathbb{S}}$ and $\tau \in \mathrm{Gal}(k_G/C(t))$,

$$Q\big(\tau(\beta)^{-1}\Gamma_c \tilde{g}\mathbf{c}\big) = 0 \quad \text{or} \quad \mathrm{ord}_{t=c}\big(Q\big(\tau(\beta)^{-1}\Gamma_c \tilde{g}\mathbf{c}\big)\big) \leq \tilde{N}.$$

For each $\tau \in \mathrm{Gal}(k_G/C(t))$, let $\mathcal{S}_\tau$ be the set of coefficients of the first $\tilde{N}+2$ terms of all elements in $\{Q(\tau(\beta)^{-1}\Gamma_c \tilde{g}\mathbf{c}) \mid Q \in \bar{\mathbb{S}}\}$. Then for each $\tau \in \mathrm{Gal}(k_G/k)$, $\mathcal{S}_\tau$ is the set of polynomials in $\mathbf{c}$ and for any $g \in \mathrm{GL}_n(C)$, $Q(\tau(\beta)^{-1}\Gamma_c \tilde{g} g) = 0$ for all $Q \in \bar{\mathbb{S}}$ if and only if $g \in \mathrm{Zero}(\mathcal{S}_\tau)$. Let

$$\mathcal{G}_{\tilde{F}} = \Big(\bigcup_{\tau \in \mathrm{Gal}(k_G/k)} \mathrm{Zero}(\mathcal{S}_\tau) \Big) \bigcap \mathrm{GL}_n(C).$$

We then obtain the desired Galois group.

Example 4.7. (Example 4.6 continued.) Let

$$\beta = \begin{pmatrix} \sqrt{1-t^2} & -t \\ 2t\sqrt{1-t^2} & 1-2t^2 \end{pmatrix}.$$

Then $\beta \in \mathrm{Zero}(J) \cap \mathrm{GL}_2(\bar{k})$. One has that

$$\beta^{-1} = \begin{pmatrix} \frac{(1-2t^2)\sqrt{1-t^2}}{1-t^2} & \frac{t\sqrt{1-t^2}}{1-t^2} \\ -2t & 1 \end{pmatrix}.$$

We first find a $g \in \mathrm{GL}_2(C)$ such that $\beta^{-1}\bar{F}g \in \mathcal{G}^{\circ}_{\bar{F}}(\bar{k}K)$. Observe that 0 is a regular point of β^{-1}. The application of ϕ_0 to $\beta^{-1}\bar{F}g$ implies that

$$\beta^{-1}\Gamma_0 g \in \mathcal{G}^{\circ}_{\bar{F}}\big(C((t))\big).$$

Notice that $\mathcal{G}^{\circ}_{\bar{F}} = \{I_2\}$ and $(\beta^{-1}\Gamma_0)_{t=0} = I_2$. These imply that $g = I_2$. Thus $\beta^{-1}\bar{F} \in \mathcal{G}^{\circ}_{\bar{F}}(\bar{k}K)$, i.e. $\beta^{-1}\bar{F} = I_2$. The ideal $I(\mathcal{G}^{\circ}_{\bar{F}})$ is generated by $\{x_{1,1} - 1, x_{1,2}, x_{2,1}, x_{2,2} - 1\}$. One can readily see that $\mathrm{Gal}(k(\sqrt{1-t^2})/k) = \{1, \tau\}$, where $\tau(\sqrt{1-t^2}) = -\sqrt{1-t^2}$. Set

$$G_1 = \big\{g \in \mathrm{GL}_2(C) \;\big|\; Q\big(\beta^{-1}\bar{F}g\big) = 0, \forall Q \in I\big(\mathcal{G}^{\circ}_{\bar{F}}\big)\big\}$$

and

$$G_\tau = \big\{g \in \mathrm{GL}_2(C) \;\big|\; Q\big(\tau\big(\beta^{-1}\big)\bar{F}g\big) = 0, \forall Q \in I\big(\mathcal{G}^{\circ}_{\bar{F}}\big)\big\}.$$

Then $G_1 = \{I_2\}$ and $G_\tau = \{\mathrm{diag}(-1, 1)\}$. Hence $\mathcal{G}_{\bar{F}} = \{I_2, \mathrm{diag}(-1, 1)\}$.

Acknowledgments

Special thanks go to Michael F. Singer for his numerous significant suggestions that improve the paper a lot. In preparing the paper, the author was invited by Michael F. Singer to visit North Carolina State University for two weeks. The author thanks him for the invitation and financial support. Many thanks also go to Shaoshi Chen, Ziming Li and Daniel Rettstadt for their valuable discussions. The author also thanks the anonymous referee for his/her careful report, providing numerous valuable comments.

Appendix A. Coefficient bounds for k-definable elements of $N_d(V^n_{inv})$

In this appendix, the symbols in the previous sections are used. We will describe a method to find coefficient bounds for k-definable elements of $N_d(V^n_{inv})$, that is, a method to bound the degrees of the coefficients of defining polynomials of such sets. Let Z be a k-definable element of $N_d(V^n_{inv})$. In Section 3 of [24], the authors gave bounds for rational solutions of the symmetric power of (1), which allow us to calculate a subset of the defining polynomials of Z. The elements in this subset are of the form $Q(X) - c$ where $Q(X) \in C[X]$ and $c \in k$. However, we do not know if the polynomials of the above form define Z. In [9], the author presented coefficient bounds for k-definable subspaces of V (see Definition A.1). We shall generalize these coefficient bounds to k-definable elements of $N_d(V^n_{inv})$.

Let W be a C-vector subspace of V of dimension m and $\mathbf{w}_1, \cdots, \mathbf{w}_m$ be a basis of W.

Definition A.1. W is said to be k-definable if there exists $(n-m)\times n$ matrix M of the rank $n-m$ such that

$$M(\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_m) = 0. \tag{6}$$

M is said to be an annihilating matrix for W (see Lemma 1 of [9]).

Due to Lemma 1 of [9], W is k-definable if and only if W is a $\mathcal{G}$-submodule of V, where $\mathcal{G}$ is the Galois group of (1) over k.

Definition A.2. Let W be a k-definable subspace of V and l an integer. We call W bounded by l if there is M with $\deg(M) \leq l$ such that (6) holds, where $\deg(M)$ is defined as the maximum of the degrees of entries of M.

The theorem in [9] implies the following proposition.

Proposition A.3. *One can compute an integer ℓ such that all k-definable subspaces of V are bounded by ℓ.*

Since we restrict ourselves to Zariski closed subsets of V_{inv}^n, we need to consider the following two new systems. One is the n-direct sum of (1):

$$\delta(Y) = \operatorname{diag}(\underbrace{A, A, \cdots, A}_{n})Y = A^{\oplus n}Y. \tag{$A^{\oplus n}$}$$

Then V^n is the solution space of ($A^{\oplus n}$) and $\operatorname{diag}(\underbrace{F, F\cdots, F}_{n})$, denoted by $F^{\oplus n}$, is a fundamental matrix. The other is the symmetric power of ($A^{\oplus n}$). Define a map

$$\begin{aligned} S^{\leq d} : V^n &\longrightarrow K^{\binom{n^2+d}{d}} \\ \mathbf{v} = (v_{1,1}, v_{2,1}, \cdots, v_{n,n}) &\longrightarrow \big(\cdots, v_{1,1}^{\mu_{1,1}} v_{1,2}^{\mu_{1,2}} \cdots v_{n,n}^{\mu_{n,n}}, \cdots,\big), \qquad \sum_{1\leq i,j\leq n} \mu_{i,j} \leq d. \end{aligned}$$

Then $S^{\leq d}(\mathbf{v})$ is a solution of the symmetric power of ($A^{\oplus n}$), denoted by

$$\delta(Y) = \big(S^{\leq d}A^{\oplus n}\big)Y. \tag{$S^{\leq d}A^{\oplus n}$}$$

The matrix $S^{\leq d}A^{\oplus n}$ can be constructed from A and its entries are in k. More details about the symmetric power can be found in (p. 39, [23]) and [24]. Denote the solution space of ($S^{\leq d}A^{\oplus n}$) by $(V^n)^{\circledS \leq d}$.

Let Z be an element of $N_d(V_{inv}^n)$. Set

$$W_Z = \operatorname{span}_C\big\{S^{\leq d}(\mathbf{z}), \mathbf{z} \in Z\big\}.$$

Then W_Z is a subspace of $(V^n)^{\circledS \leq d}$.

Proposition A.4. *Assume that $Z \in N_d(V_{inv}^n)$. Then Z is k-definable if and only if W_Z is k-definable.*

Proof. Suppose that $S^{\leq d}(\mathbf{v}_1), \cdots, S^{\leq d}(\mathbf{v}_m)$ is a basis of W_Z. Denote $\mu = \binom{n^2+d}{d}$.

($\Rightarrow$) Assume that $\sigma \in \mathcal{G}$. Since Z is k-definable, $\sigma(\mathbf{v}) \in Z$ for all $\mathbf{v} \in Z$. This implies that for each $i = 1, \cdots, m$, $\sigma(S^{\leq d}(\mathbf{v}_i)) = S^{\leq d}(\sigma(\mathbf{v}_i)) \in W_Z$. Consequently, W_Z is a $\mathcal{G}$-module. By Lemma 1 in [9], W_Z is k-definable.

($\Leftarrow$) Assume that W_Z is k-definable. By Lemma 1 in [9], there exists $(\mu - m) \times \mu$ matrix M of the rank $\mu - m$ such that

$$M\big(S^{\leq d}(\mathbf{v}_1), \cdots, S^{\leq d}(\mathbf{v}_m)\big) = 0$$

Denote the ith-row of M by $\mathbf{m}_i$ for $i = 1, \cdots, \mu - m$. Let $\mathbf{x} = (\cdots, x_{1,1}^{\mu_{1,1}} \cdots x_{n,n}^{\mu_{n,n}}, \cdots)$ where $\mu_{1,1} + \mu_{1,2} + \cdots + \mu_{n,n} \leq d$. Then $P_i(X) = \mathbf{m}_i \cdot \mathbf{x}$ is a polynomial of degree at most d with the coefficients in k, where $i = 1, \cdots, \mu - m$. One can easily verify that

$$Z \subseteq \mathrm{Zero}\big(P_1(X), \cdots, P_{\mu-m}(X)\big) \bigcap V_{inv}^n.$$

Since Z is an element of $N_d(V_{inv}^n)$, there are $Q_1(X), \cdots, Q_l(X)$ in $K[X]$ with degree at most d, which define Z. By the dimension argument, for each $i = 1, \cdots, l$, $Q_i(X)$ is a K-linear combinations of $P_1(X), \cdots, P_{\mu-m}(X)$. Therefore the above inclusion relation is actually an equality. □

The above two propositions indicate the following corollary.

Corollary A.5. *One can compute an integer ℓ such that for every k-definable element Z of $N_d(V_{inv}^n)$, the coefficients of the defining equations of Z can be chosen to be rational functions with degrees not greater than ℓ.*

Proof. Let Z be a k-definable element of $N_d(V_{inv}^n)$. Then W_Z is a k-definable subspace of $(V^n)^{\mathbb{S}\leq d}$ by Proposition A.4. Moreover, from the proof of Proposition A.4, the coefficients of the defining equations of Z can be chosen to be the entries of the annihilating matrix of W_Z. Hence to prove the corollary, it suffices to show that one can compute an integer ℓ which bounds all k-definable subspaces of $(V^n)^{\mathbb{S}\leq d}$. This is done by applying Proposition A.3 to $(V^n)^{\mathbb{S}\leq d}$. □

Appendix B. Bounds for proto-Galois groups

In this appendix, we shall find an integer $\tilde{d}$ depending on n with the following property. For any algebraic subgroup G of $\mathrm{GL}_n(C)$, there is an algebraic subgroup H of $\mathrm{GL}_n(C)$, which is bounded by $\tilde{d}$, satisfying

$$(*): \quad \big(H^\circ\big)^t \trianglelefteq G^\circ \leq G \leq H.$$

Most of results in this section appeared in the part III of [10], where more families of algebraic subgroups of $\mathrm{GL}_n(C)$ that can be uniformly definable were given. Here we only present those we need. In addition, we will use the term "bounded by d" instead of "uniformly definable". As mentioned in Introduction, we elaborate the details of the proofs in [10] and present the explicit estimates of the bounds. Meanwhile, we will show how to compute a set of generators of the character group of a given connected algebraic subgroup. The following notation will be used frequently.

Notation B.1. Let H be an algebraic subgroup of $\mathrm{GL}_n(C)$ and S an arbitrary subset of H.

$\mathcal{F}$: a family of algebraic subgroups of $\mathrm{GL}_n(C)$;
$H_{\mathcal{F}}$: the intersection of all $H' \in \mathcal{F}$ with $H \subseteq H'$;
$N_H(H')$: the normalizer of H' in H where H' is an algebraic subgroup of H;
$\mathcal{F}_{mt}(H)$: the family of maximal tori of H;
$\mathcal{F}_{imt}(H)$: the family of intersections of maximal tori of H;
$\mathcal{F}_{up}$: the family of subgroups of $\mathrm{GL}_n(C)$ generated by unipotent elements;
$X(H)$: the group of characters of H;
H^t: the intersection of the kernels of all characters of H.

An algebraic subgroup H of $\mathrm{GL}_n(C)$ is said to be bounded by d if there are polynomials $Q_1(X), \cdots, Q_m(X)$ in $C[X]$ with degree not greater than d such that

$$H = \mathrm{Zero}\big(Q_1(X), \cdots, Q_m(X)\big) \bigcap \mathrm{GL}_n(C).$$

For a family of algebraic subgroups of $\mathrm{GL}_n(C)$, say $\mathcal{F}$, we say $\mathcal{F}$ is bounded by d, if every element of $\mathcal{F}$ is bounded by d. For an ideal I in $C[X]$, I is said to be bounded by d if there exist generators of I whose degrees are not greater than d. Throughout this appendix, unless otherwise specified, subgroups always mean algebraic subgroups.

B.1. Preparation lemmas

To achieve the integer $\tilde{d}$, we need the following degree bounds from computational algebraic geometry. For the moment, we assume that I is an ideal in $C[x_1, \cdots, x_n]$. Then we have

Proposition B.2. *Suppose that I is bounded by d. Then there is $\gamma(n,d)$ in $\mathbb{N}$ such that $I \cap C[x_1, \cdots, x_i]$ is bounded by $\gamma(n,d)$.*

Remark B.3. By Gröbner bases computation, $\gamma(n,d)$ can be chosen as $2(\frac{d^2}{2} + d)^{2^{n-1}}$, which is less than $(d+1)^{2^n}$. The reader is referred to (Corollary 8.3, [5]) for more details.

The following several lemmas play the key role in this appendix.

Lemma B.4. *Let H be a subgroup of $\mathrm{GL}_n(C)$ bounded by d. Then there exists a family $\mathcal{F}_{ad}(H)$ of subgroups of H bounded by $\max\{d, n\}$ such that for any connected subgroup H' of H, $N_H(H') \in \mathcal{F}_{ad}(H)$. Particularly, $\mathcal{F}_{ad}(\mathrm{GL}_n(C))$ is bounded by n.*

Proof. Let $\mathfrak{g}l(H)$ be the Lie algebra of H. Consider the adjoint action of H on $\mathfrak{g}l(H)$. Then $\mathfrak{g}l(H')$ is a subspace of $\mathfrak{g}l(H)$ and $N_H(H')$ is the stabilizer of $\mathfrak{g}l(H')$ under the adjoint action. Let $B_1, \cdots, B_l$ be a basis of $\mathfrak{g}l(H')$ and the $\mathbf{e}_{i,j}$ a basis of $\mathrm{Mat}_n(C)$. Then for any $h \in N_H(H')$, there is $g_h \in \mathrm{GL}_{n^2}(C)$ such that $h(\mathbf{e}_{1,1}, \cdots, \mathbf{e}_{n,n})h^{-1} = (\mathbf{e}_{1,1}, \cdots, \mathbf{e}_{n,n})g_h$. It is easy to see that the entries of g_h are of the form $P_{l,m}(h)/\det(h)$ where the $P_{l,m}(X)$ are polynomials with degree at most n. Assume that $B_s = (\mathbf{e}_{1,1}, \cdots, \mathbf{e}_{n,n})\mathbf{b}_s$ for $s = 1, \cdots, l$ where $\mathbf{b}_s = (b_{s,i,j}) \in C^{n^2}$. Then since $hB_sh^{-1} \in \mathfrak{g}l(H')$, there are $a_{s,1}, \cdots, a_{s,l} \in C$ such that $hB_sh^{-1} = \sum_\xi a_{s,\xi}B_\xi$. In other words,

$$hB_sh^{-1} = \sum_{i,j} b_{s,i,j}h\mathbf{e}_{i,j}h^{-1} = (\mathbf{e}_{1,1}, \cdots, \mathbf{e}_{n,n})g_h\mathbf{b}_s = (\mathbf{e}_{1,1}, \cdots, \mathbf{e}_{n,n})\sum_{\xi=1}^{l} a_{s,\xi}\mathbf{b}_\xi.$$

That is

$$g_h\mathbf{b}_s = \sum_{\xi=1}^{l} a_{s,\xi}\mathbf{b}_\xi.$$

The above nonhomogeneous linear equations have solutions if and only if

$$\mathrm{rank}(\mathbf{b}_1, \cdots, \mathbf{b}_l) = \mathrm{rank}(\mathbf{b}_1, \cdots, \mathbf{b}_l, g_h\mathbf{b}_s).$$

This leads to the equations that together with the defining equations of H define $N_H(H')$. Since the entries of g_h are of the form $P_{l,m}(h)/\det(h)$ where the $P_{l,m}(X)$ are polynomials with degree at most n, the defining ideal of $N_H(H')$ is generated by those of H and the polynomials with degree $\leq n$. Hence $\mathcal{F}_{ad}(H)$ is bounded by $\max\{d, n\}$. In particular, when $H = \mathrm{GL}_n(C)$, $\mathcal{F}_{ad}(\mathrm{GL}_n(C))$ is bounded by n. □

Let $\{\tau_{H,\lambda} : H \to \mathrm{GL}_\mu(C) \mid H \in \mathcal{F}, \lambda \in \Lambda\}$ be a family of homomorphisms from elements of $\mathcal{F}$ to $\mathrm{GL}_\mu(C)$ where μ is a positive integer and Λ is a set. Assume that

$$\tau_{H,\lambda} = \left(\frac{P_{i,j}^{H,\lambda}(X)}{Q^{H,\lambda}(X)}\right).$$

We will say that $\{\tau_{H,\lambda}\}$ is bounded by m if $\deg(P_{i,j}^{H,\lambda}(X)) \leq m$ and $\deg(Q^{H,\lambda}(X)) \leq m$.

Lemma B.5. *Let $\{\tau_{H,\lambda} \mid H \in \mathcal{F}, \lambda \in \Lambda\}$ be as above. Assume that $\mathcal{F}$ is bounded by d and $\{\tau_{H,\lambda} \mid H \in \mathcal{F}, \lambda \in \Lambda\}$ is bounded by m. Then*

(a) $\{\tau_{H,\lambda}(H)\}$ *is bounded by* $(\bar{d}+1)^{2^{\mu^2+n^2}}$ *where* $\bar{d}=\max\{m+1,d\}$.
(b) *If* $\mathcal{F}'$ *is a family of subgroups of* $\mathrm{GL}_\mu(C)$ *bounded by* d', *then*

$$\left\{\tau_{H,\lambda}^{-1}\left(H'\cap\tau_{H,\lambda}(H)\right)\;\middle|\; H'\in\mathcal{F}', H\in\mathcal{F},\lambda\in\Lambda\right\}$$

is bounded by $\max\{d,md'\}$.

Proof. Assume that H is defined by S_H, a set of polynomials in $C[X]$ with degree $\leq d$.

(a) $\tau_{H,\lambda}(H)$ is defined by

$$\left\langle Q^{H,\lambda}(X)y_{1,1}-P_{1,1}^{H,\lambda}(X),\cdots,Q^{H,\lambda}(X)y_{\mu,\mu}-P_{\mu,\mu}^{H,\lambda}(X),S_H\right\rangle\bigcap C[y_{1,1},y_{1,2},\cdots,y_{\mu,\mu}].$$

By Proposition B.2, $\tau_{H,\lambda}(H)$ is bounded by $(\bar{d}+1)^{2^{\mu^2+n^2}}$ where $\bar{d}=\max\{m+1,d\}$.

(b) Assume that H' is defined by $g_1(Y),\cdots,g_s(Y)$ where $\deg(g_i(Y))\leq d'$. Then one can see that $\tau_{H,\lambda}^{-1}(H'\cap\tau_{H,\lambda}(H))$ is defined by

$$S_H,\ g_1\left(\left(\frac{P_{i,j}^{H,\lambda}(X)}{Q^{H,\lambda}(X)}\right)\right),\cdots,g_s\left(\left(\frac{P_{i,j}^{H,\lambda}(X)}{Q^{H,\lambda}(X)}\right)\right).$$

Clearing the denominators, we obtain the defining polynomials of $\tau_{H,\lambda}^{-1}(H'\cap\tau_{H,\lambda}(H))$ in $C[X]$, whose degrees are not greater than $\max\{d,md'\}$. □

Given a non-negative integer d, set

$$d^*=\max_i\left\{\binom{\binom{n^2+d}{d}}{i}^2\right\},\qquad n^*=d^*d\binom{n^2+d}{d}.$$

A standard theorem in the theory of linear algebraic groups stats that if $H\trianglelefteq H'$ are linear algebraic groups, then there exists an integer N and a homomorphism $\tau:H'\to\mathrm{GL}_N(C)$ such that the kernel of τ is H (see Theorem 11.5, p. 82, [12]). The following shows that one can uniformly bound τ.

Proposition B.6. *Assume that* $\mathcal{F}$ *is bounded by* d *and let*

$$\mathcal{P}=\left\{\left(H',H\right)\;\middle|\; H'\in\mathrm{GL}_n(C),H\in\mathcal{F}\text{ with }H\trianglelefteq H'\right\}.$$

There is a family of homomorphisms $\{\tau_{H',H}\mid(H',H)\in\mathcal{P}\}$ *bounded by* n^* *such that* $\tau_{H',H}:H'\to\mathrm{GL}_{d^*}(C)$ *and* $\ker(\tau_{H',H})=H$. *Furthermore, if* H' *varies among a family of subgroups of* $\mathrm{GL}_n(C)$ *bounded by* d', *then* $\{\tau_{H',H}(H')\mid(H',H)\in\mathcal{P}\}$ *is bounded by*

$$(\bar{d}+1)^{2^{(d^*)^2+n^2}},\quad\text{where }\bar{d}=\max\left\{n^*+1,d'\right\}.$$

Proof. $C[X]_{\leq d}$ is a C-vector space with dimension $\binom{n^2+d}{d}$. The group $\mathrm{GL}_n(C)$ acts naturally on $C[X]_{\leq d}$, which is defined as follows

$$\forall g \in \mathrm{GL}_n(C), \quad P(x) \in C[X]_{\leq d}, \quad g \cdot P(X) = P(Xg).$$

Suppose that $H \in \mathcal{F}$. Let

$$I_{\leq d}(H) = \big\{P(X) \in C[X]_{\leq d} \;\big|\; P(H) = 0\big\}.$$

Then $I_{\leq d}(H)$ is also a C-vector space of finite dimension. Since $I_{\leq d}(H)$ defines H, one has $H = \mathrm{stab}(I_{\leq d}(H))$. Let $\nu = \dim_C(I_{\leq d}(H))$ and

$$E = \bigwedge^{\nu} C[X]_{\leq d}.$$

Then

$$\dim_C(E) = \binom{\binom{n^2+d}{d}}{\nu} \quad \text{and} \quad \bigwedge^{\nu} I_{\leq d}(H) = C\mathbf{v} \quad \text{for some } \mathbf{v} \in E.$$

The action of $\mathrm{GL}_n(C)$ on $C[X]_{\leq d}$ induces an action of $\mathrm{GL}_n(C)$ on E. We will still use $\cdot$ to denote this action. It is easy to see that $H = \mathrm{stab}(C\mathbf{v})$. Let $U = \bigoplus U_\chi$ where the χ are characters of H and

$$U_\chi = \big\{\mathbf{u} \in E \;\big|\; h \cdot \mathbf{u} = \chi(h)\mathbf{u}\big\}.$$

Note that the above direct sum runs over a finite set. Assume that $U = \bigoplus_{i=1}^{s} U_{\chi_i}$. It is clear that $\mathbf{v} \in U_{\chi_i}$ for some i. Let H' be a subgroup of $\mathrm{GL}_n(C)$ satisfying that $H \trianglelefteq H'$. Then U is invariant under the action of H'. Let $\mathcal{L}$ be the set of C-linear maps from U to U which leave each U_{χ_i} invariant. Then since $\dim_C(U) \leq \dim_C(E)$,

$$\dim_C(\mathcal{L}) \leq \big(\dim_C(U)\big)^2 \leq \big(\dim_C(E)\big)^2 = \binom{\binom{n^2+d}{d}}{\nu}^2.$$

Let $\mathbf{u}_1, \cdots, \mathbf{u}_l$ be a suitable basis of U such that under this basis, each element of $\mathcal{L}$ is represented as the matrix $\mathrm{diag}(M_1, \cdots, M_s)$ where $M_i \in \mathrm{Mat}_{\dim(U_{\chi_i})}(C)$. Furthermore every matrix of the form $\mathrm{diag}(M_1, \cdots, M_s)$ where $M_i \in \mathrm{Mat}_{\dim(U_{\chi_i})}(C)$ represents an element of $\mathcal{L}$. For any $h' \in H'$, there is $[h'] \in \mathrm{GL}_l(C)$ such that

$$\big(h' \cdot \mathbf{u}_1, \cdots, h' \cdot \mathbf{u}_l\big) = (\mathbf{u}_1, \cdots, \mathbf{u}_l)\big[h'\big].$$

An easy calculation yields the entries of $[h']$ are polynomials in those of h' with degree $\leq d\nu$. For any $L \in \mathcal{L}$, we will use $L^{\mathbf{u}}$ to denote the matrix in $\mathrm{GL}_l(C)$ satisfying

$$L((\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_l)) = (\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_l)L^{\mathbf{u}}.$$

The action of H' on U yields an adjoint action of H' on $\mathcal{L}$ as follows: for any $L \in \mathcal{L}$, $h' \in H'$,

$$\begin{aligned}\big(h' \cdot L\big)((\mathbf{u}_1, \cdots, \mathbf{u}_l)) &= h' \cdot L\big(h'^{-1} \cdot \mathbf{u}_1, \cdots, h'^{-1} \cdot \mathbf{u}_l\big) = h' \cdot L\big((\mathbf{u}_1, \cdots, \mathbf{u}_l)\big[h'\big]^{-1}\big) \\ &= h' \cdot \big((\mathbf{u}_1, \cdots, \mathbf{u}_l) L^{\mathbf{u}}\big[h'\big]^{-1}\big) = (\mathbf{u}_1, \cdots, \mathbf{u}_l)\big[h'\big] L^{\mathbf{u}}\big[h'\big]^{-1}.\end{aligned}$$

Fix a basis of $\mathcal{L}$, say $L_1, \cdots, L_m$, where $m \leq \binom{n^2+d}{\nu}^2$. Then the adjoint action induces a homomorphism from H' to $\mathrm{GL}_m(C)$

$$\tau_{H',H} : H' \longrightarrow \mathrm{GL}_m(C), \qquad \tau_{H',H}\big(h'\big) = \eta_{h'} \tag{7}$$

where $\eta_{h'} \in \mathrm{GL}_m(C)$ satisfies that

$$\big(\big[h'\big] L_1^{\mathbf{u}}\big[h'\big]^{-1}, \cdots, \big[h'\big] L_m^{\mathbf{u}}\big[h'\big]^{-1}\big) = \big(L_1^{\mathbf{u}}, \cdots, L_m^{\mathbf{u}}\big)\eta_{h'}.$$

We will show that $\ker(\tau_{H',H}) = H$. Suppose that $h' \in \ker(\tau_{H',H})$. Then $\eta_{h'} = I_m$. In other words, $[h']L^{\mathbf{u}} = L^{\mathbf{u}}[h']$ for all $L \in \mathcal{L}$. This implies that $[h']$ is of the following form:

$$\big[h'\big] = \mathrm{diag}(\underbrace{c_1, \cdots, c_1}_{\dim(V_{\chi_1})}, \cdots, \underbrace{c_s, \cdots, c_s}_{\dim(V_{\chi_s})}).$$

Particularly, $h' \cdot \mathbf{v} = c_i \mathbf{v}$ for some i. Hence $h' \in H = \mathrm{stab}(C\mathbf{v})$. One can easily see that $H \subseteq \ker(\tau_{H',H})$. Hence $H = \ker(\tau_{H',H})$. Since $m \leq d^*$, $\mathrm{GL}_m(C)$ can be naturally embedded into $\mathrm{GL}_{d^*}(C)$. Composing this embedding map with $\tau_{H',H}$ induces a homomorphism from H' to $\mathrm{GL}_{d^*}(C)$ with kernel H. We will still denote this homomorphism by $\tau_{H',H}$. An easy calculation implies that

$$\tau_{H',H}(X) = \left(\frac{P_{i,j}^{H',H}(X)}{Q^{H',H}(X)}\right)$$

where $P_{i,j}^{H',H}(X)$, $Q^{H',H}(X)$ are polynomials in $x_{i,j}$ and $Q^{H',H}(h') = \det([h'])$. Furthermore, the $P_{i,j}^{H',H}(h')$ are polynomials in the entries of $[h']$ with degree $\leq l$. Since the entries of $[h']$ are polynomials in those of h' with degree $\leq d\nu$, the $P_{i,j}^{H',H}(h')$ and $Q^{H',H}(h')$ are polynomials in the entries of h' with degree $\leq ld\nu$, which is not greater than n^*. This proves that $\{\tau_{H,\lambda} \mid H \in \mathcal{F}, \lambda \in \Lambda\}$ is bounded by n^*.

Finally, due to Lemma B.5, $\{\tau_{H',H}(H') \,|\, H' \in \mathcal{F}', H \in \mathcal{F} \text{ with } H \trianglelefteq H'\}$ is bounded by $(\bar{d}+1)^{2^{(d^*)^2+n^2}}$, where $\bar{d} = \max\{n^*+1, d'\}$. □

Remark B.7. As linear algebraic groups, $\tau_{H',H}(H')$ is isomorphic to H'/H. Therefore Proposition B.6 says that H'/H can be uniformly embedded into $\mathrm{GL}_{d^*}(C)$ and H'/H varies among a bounded family if H' does.

Lemma B.8. *$\mathcal{F}_{up}$ is bounded by $(2n)^{3\cdot 8^{n^2}}$.*

Proof. Assume that H is a subgroup generated by unipotent elements. Then by (p. 55, Proposition, [12]), it is the product of at most $2\dim(H)$ one-dimensional unipotent subgroups. From (p. 96, Lemma C, [12]), we know that any one-dimension unipotent subgroup is of the form:

$$I_n + \mathbf{m}x + \frac{\mathbf{m}^2}{2}x^2 + \cdots + \frac{\mathbf{m}^{n-1}}{(n-1)!}x^{n-1}, \quad \mathbf{m}^n = 0,\ x \in C,$$

where $\mathbf{m} \in \mathrm{Mat}_n(C)$ and $\mathbf{m}^n = 0$. Hence H has a polynomial parametrized representation

$$(Y) = \prod_{i=1}^{2\dim(H)} \left(I_n + \mathbf{m}_i x_i + \frac{\mathbf{m}_i^2}{2}x_i^2 + \cdots + \frac{\mathbf{m}_i^{n-1}}{(n-1)!}x_i^{n-1} \right).$$

Observe that $\dim(H) \leq n^2$. So the polynomials in the above representation contain at most $3n^2$ variables and are of degree not greater than $2n^2(n-1)$. Eliminating all x_i in the above representation, we will obtain the defining ideal of H. By Proposition B.2 and Remark B.3, $\mathcal{F}_{up}$ is bounded by

$$\left(2n^2(n-1)+1\right)^{2^{3n^2}} < (2n)^{3\cdot 8^{n^2}}. \qquad \square$$

Lemma B.9. *Both $\mathcal{F}_{mt}(\mathrm{GL}_n(C))$ and $\mathcal{F}_{imt}(\mathrm{GL}_n(C))$ are bounded by 1.*

Proof. Every maximal torus of $\mathrm{GL}_n(C)$ is conjugate to $(C^*)^n$. Hence it is equal to the intersection of $\mathrm{GL}_n(C)$ and a linear subspace of $\mathrm{Mat}_n(C)$. Consequently, $\mathcal{F}_{mt}(\mathrm{GL}_n(C))$ is bounded by 1. As the intersection of linear subspaces of $\mathrm{Mat}_n(C)$ is still linear, any element of $\mathcal{F}_{imt}(\mathrm{GL}_n(C))$ is the intersection of $\mathrm{GL}_n(C)$ and a linear subspace of $\mathrm{Mat}_n(C)$. So $\mathcal{F}_{imt}(\mathrm{GL}_n(C))$ is also bounded by 1. $\square$

Lemma B.10. *Assume that H is a connected subgroup of $\mathrm{GL}_n(C)$. Then H^t is generated by all unipotent elements of H.*

Proof. Since H/H^t is a torus, there are no nontrivial unipotent elements in H/H^t. Hence all unipotent elements of H are in H^t. From Lemma 2.1 in [19], H^t is generated by (P,P) and $R_u(H)$ where P is a Levi factor of H and $R_u(H)$ is the unipotent radical of H. Moreover (P,P) is semi-simple, so it is generated by unipotent elements. Therefore H^t is generated by all unipotent elements of H. $\square$

B.2. Main results

Let $J(n)$ be a Jordan bound, so that every finite subgroup of $\mathrm{GL}_n(C)$ contains a normal abelian subgroup of index at most $J(n)$. Various authors gave bounds for $J(n)$.

Below is a bound due to Schur [16]:

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

In the following, we will show the main results in this appendix. Denote

$$\kappa_1 = \max_i \left\{ \binom{\binom{n^2+(2n)^{3\cdot 8^{n^2}}}{n^2}}{i} \right\}^2 \quad \text{and} \quad \kappa_2 = \kappa_1 (2n)^{3\cdot 8^{n^2}} \binom{n^2+(2n)^{3\cdot 8^{n^2}}}{n^2}. \tag{8}$$

Proposition B.11. *There exists an integer $I(n)$ that is not greater than $J\big(\max_i\{\binom{\kappa_1^2+1}{i}\}\big)$ and a family $\mathcal{F}$ of subgroups of $\mathrm{GL}_n(C)$ bounded by*

$$\kappa_3 \triangleq \kappa_2(\kappa_1^2+1) \max_i \left\{ \binom{\kappa_1^2+1}{i} \right\} \tag{9}$$

with the following property. For every subgroup H of $\mathrm{GL}_n(C)$, there is $H' \in \mathcal{F}$ such that

(a) $H^\circ \leq H'$.
(b) H *normalizes* H'*; so* $H' \trianglelefteq HH' \leq \mathrm{GL}_n(C)$.
(c) $[H : H \cap H'] = [HH' : H'] \leq I(n)$.
(d) *Every unipotent element of* H' *lies in* H°.

We will show the proposition by separating three cases.

Lemma B.12. *Proposition B.11 is true for finite groups with $I(n) = J(n)$ and $\mathcal{F}$ is bounded by 1.*

Proof. Assume that $H \subset \mathrm{GL}_n(C)$ is a finite group. Let $\bar{H}$ be a normal abelian subgroup of H with $[H : \bar{H}] \leq J(n)$. As a finite abelian subgroup of $\mathrm{GL}_n(C)$ is diagonalizable, $\bar{H}$ is contained in some maximal tori of $\mathrm{GL}_n(C)$. Let H' be the intersection of maximal tori containing $\bar{H}$. Then $H' \in \mathcal{F}_{imt}(\mathrm{GL}_n(C))$. Clearly, H normalizes H'. Since $\bar{H} \subseteq H \cap H'$, $[H : H' \cap H] \leq [H : \bar{H}] \leq J(n)$. The only unipotent element of H' is the identity. So $(a)-(d)$ hold for H, H'. The lemma follows from the fact that $\mathcal{F}_{imt}(\mathrm{GL}_n(C))$ is bounded by 1. □

Lemma B.13. *Assume that H is a subgroup whose identity component is a torus. Then Proposition B.11 is true for H with $I(n) = J\big(\max_i\{\binom{n^2+1}{i}^2\}\big)$ and $\mathcal{F}$ is bounded by*

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

Proof. Let $M = (H^\circ)_{\mathcal{F}_{imt}(\mathrm{GL}_n(C))}$ and $N = N_{\mathrm{GL}_n(C)}(M)$. It is easy to verify that H normalizes M and thus $H \subseteq N$. Since M lies in the family $\mathcal{F}_{imt}(\mathrm{GL}_n(C))$ bounded

by 1, Lemma B.4 implies that N lies in the family $\mathcal{F}_{ad}(\mathrm{GL}_n(C))$ bounded by n. Let $\tilde{n} = \max_i\{\binom{n^2+1}{i}^2\}$. By Proposition B.6, there is a homomorphism

$$\tau_{N,M} : N \longrightarrow \mathrm{GL}_{\tilde{n}}(C)$$

satisfies that $\ker(\tau_{N,M}) = M$ and $\tau_{N,M}$ is bounded by $\tilde{n}(n^2+1)$. As $H^\circ \subseteq M$, $\tau_{N,M}(H)$ is a finite subgroup of $\mathrm{GL}_{\tilde{n}}(C)$. From Lemma B.12, there is $\tilde{M} \in \mathcal{F}_{imt}(\mathrm{GL}_{\tilde{n}}(C))$ such that (a)–(c) hold for $\tau_{N,M}(H)$, $\tilde{M}$ (with $I(\tilde{n}) = J(\tilde{n})$). Let $H' = \tau_{N,M}^{-1}(\tilde{M} \cap \tau_{N,M}(N))$. Note that $\mathcal{F}_{imt}(\mathrm{GL}_{\tilde{n}}(C))$ is bounded by 1. By Lemma B.5, H' is bounded by $\tilde{n}(n^2+1)$. We will show that the H' satisfy (a)–(d) with $I(n) = J(\tilde{n})$. It is clear that $H^\circ \leq H'$. For any $h \in H$, since $\tau_{M,N}(H)$ normalizes $\tilde{M}$ and $\tau_{N,M}(N)$,

$$\tau_{N,M}\big(hH'h^{-1}\big) = \tau_{N,M}(h)\big(\tilde{M} \cap \tau_{N,M}(N)\big)\tau_{N,M}(h)^{-1} = \tilde{M} \cap \tau_{N,M}(N) = \tau_{N,M}\big(H'\big).$$

Therefore $hH'h^{-1} \subseteq H'$. This indicate that $hH'h^{-1} = H'$ for any $h \in H$. In other words, H normalizes H'. This proves (b). Since both HH' and H' contain M,

$$\begin{aligned}\big[HH' : H'\big] &= \big[\tau_{N,M}\big(HH'\big) : \tau_{N,M}\big(H'\big)\big] = \big[\tau_{N,M}(H)\tau_{N,M}\big(H'\big) : \tau_{N,M}\big(H'\big)\big] \\ &= \big[\tau_{N,M}(H) : \tau_{N,M}(H) \cap \tau_{N,M}\big(H'\big)\big] = \big[\tau_{N,M}(H) : \tilde{M} \cap \tau_{N,M}(H)\big] \leq J(\tilde{n}).\end{aligned}$$

This proves (c). Suppose that h' is a unipotent element of H'. Then $\tau_{N,M}(h')$ is a unipotent element of $\tilde{M}$. However $\tilde{M}$ consists of semi-simple elements. Hence $\tau_{N,M}(h') = 1$. Then $h' \in M$. But M is contained in a torus, so $h' = 1$. This proves (d). □

Now we are ready to prove Proposition B.11 for the general case.

Proof. Let $U = (H^\circ)^t$. By Lemma B.10, U is generated by unipotent elements. Then it follows from Lemma B.8 that U is bounded by $(2n)^{3\cdot 8^{n^2}}$. Let $N = N_{\mathrm{GL}_n(C)}(U)$. Lemma B.4 indicates that N lies in $\mathcal{F}_{ad}(\mathrm{GL}_n(C))$ that is bounded by n. Let κ_1 and κ_2 be as in (8). Using Proposition B.6 again, there is a homomorphism

$$\phi_{N,U} : N \longrightarrow \mathrm{GL}_{\kappa_1}(C)$$

such that $\ker(\phi_{N,U}) = U$ and $\phi_{N,U}$ is bounded by κ_2. We first prove that $H \leq N$. For any $h \in H$ and any character χ of H°, $\chi(hXh^{-1})$ is a character of H°. Hence for any $u \in U$, $\chi(huh^{-1}) = 1$. So $huh^{-1} \in U$ for any $u \in U$. In other words, H normalizes U. So $H \leq N$. As H°/U is a torus, $\phi_{N,U}(H)^\circ$ is a torus in $\mathrm{GL}_{\kappa_1}(C)$. Lemma B.13 implies that there is $M' \leq \mathrm{GL}_{\kappa_1}(C)$ bounded by $(\kappa_1^2+1)\max_i\{\binom{\kappa_1^2+1}{i}^2\}$ such that (a)–(d) hold for $\phi_{N,U}(H)$, M' with $I(\kappa_1) = J\big(\max_i\{\binom{\kappa_1^2+1}{i}\}\big)$. Let $H' = \phi_U^{-1}(M' \cap \phi_{N,U}(N))$. Then by Lemma B.5, H' is bounded by κ_3, where κ_3 is defined in (9). An arguments similar to the once used in the proof of Lemma B.13 implies (a)–(c) hold for H, H' with $I(n) = J\big(\max_i\{\binom{\kappa_1^2+1}{i}\}\big)$. Now let us show that (d) holds. Assume that u is a unipotent

element of H'. Then $\phi_{N,U}(u)$ is a unipotent element of M'. Since M' and $\phi_{N,U}(H)^\circ$ satisfy (d), $\phi_{N,U}(u) \in \phi_{N,U}(H)^\circ$. Whereas $\phi_{N,U}(H)^\circ$ is a torus, $\phi_{N,U}(u) = 1$. Thus $u \in U \subseteq H^\circ$. □

Proposition B.14. *Let $I(n)$ and κ_3 be as in Proposition B.11. Then there exists a family $\tilde{\mathcal{F}}$ of subgroups of $\mathrm{GL}_n(C)$ bounded by*

$$\tilde{d} \triangleq (\kappa_3)^{I(n)-1}$$

with the following property. For any subgroup H of $\mathrm{GL}_n(C)$, there exists $\tilde{H} \in \tilde{\mathcal{F}}$ such that $H \leq \tilde{H}$, and every unipotent element of $\tilde{H}$ lies in H°.

Proof. Let $\mathcal{F}$ be as in Proposition B.11 and

$$\tilde{\mathcal{F}} = \{\bar{H} \mid \exists M \in \mathcal{F}, M \trianglelefteq \bar{H}, [\bar{H} : M] \leq I(n)\}.$$

Every element of $\tilde{\mathcal{F}}$ is the union of at most $I(n)$ cosets of some element in $\mathcal{F}$. It is well-known that the union of two varieties is defined by the product of their corresponding defining polynomials. Hence $\tilde{\mathcal{F}}$ is bounded by $\tilde{d}$. Assume that H is a subgroup of $\mathrm{GL}_n(C)$. Let H' be an element in $\mathcal{F}$ such that (a)–(d) in Proposition B.11 hold for H, H'. Let $\tilde{H} = HH'$. Then $\tilde{H} \in \tilde{\mathcal{F}}$ by Proposition B.11 (c). The unipotent elements of $\tilde{H}$ lie in $\tilde{H}^\circ$ and so lie in $(H')^\circ$. As the unipotent elements of H' lie in H°, so do the unipotent elements of $\tilde{H}$. □

Corollary B.15. *Let $\tilde{\mathcal{F}}$ be the family as in Proposition B.14. Then for any subgroup H of $\mathrm{GL}_n(k)$, there is $\tilde{H} \in \tilde{\mathcal{F}}$ such that*

$$\left(\tilde{H}^\circ\right)^t \trianglelefteq H^\circ \leq H \leq \tilde{H}.$$

Proof. By Proposition B.14, there is $\tilde{H} \in \tilde{\mathcal{F}}$ such that $H \leq \tilde{H}$ and the unipotent elements of $\tilde{H}$ lie in H°. Then the corollary follows from Lemma B.10 and the fact that $(\tilde{H}^\circ)^t$ is normal in $\tilde{H}^\circ$. □

Remark B.16. Assume that n is sufficiently large. Note that

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k \quad \text{and} \quad \max_i \left\{\binom{n}{i}\right\} = \binom{n}{\lfloor n/2 \rfloor}.$$

It is easy to verify that $(n^2 + (2n)^{3\cdot 8^{n^2}})/n^2 > (2n)^{2\cdot 8^{n^2}}$. This together with the above inequalities implies that

$$(2n)^{2n^2\cdot 8^{n^2}} < \binom{n^2 + (2n)^{3\cdot 8^{n^2}}}{n^2} < \left(n^2 + (2n)^{3\cdot 8^{n^2}}\right)^{n^2} < \left((2n)^{4\cdot 8^{n^2}}\right)^{n^2} = (2n)^{4n^2\cdot 8^{n^2}}.$$

Therefore one has the following bounds for κ_1:

$$2^{(2n)^{2n^2\cdot 8^{n^2}}} < \left(\sqrt{2}^{(2n)^{2n^2\cdot 8^{n^2}}}\right)^2 < \kappa_1 < \left(2^{(2n)^{4n^2\cdot 8^{n^2}}}\right)^2 = 4^{(2n)^{4n^2\cdot 8^{n^2}}}$$

Thus κ_1 is triply exponential in n and so is κ_2 by (8). An argument similar to the above one induces that $\max_i\left\{\binom{\kappa_1^2+1}{i}\right\}$ is quadruply exponential in n. Hence κ_3 is also quadruply exponential. Since $J(n)$ is exponential, $J\left(\max_i\left\{\binom{\kappa_1^2+1}{i}\right\}\right)$ is quintuply exponential in n. Let $I(n) = J\left(\max_i\left\{\binom{\kappa_1^2+1}{i}\right\}\right)$. Then $\tilde{d}(= \kappa_3^{I(n)-1})$ is sextuply exponential in n.

In the following, H is assumed to be connected. Proposition B.6 allows us to bound the degrees of generators of $X(H)$. As C is algebraically closed, $X(H)$ can be viewed as a subset of $C[H]$, the coordinate ring of H. The homomorphism $\varphi : H \to H'$ induces a homomorphism $\varphi^\circ : X(H') \to X(H)$.

Proposition B.17. *Let κ_2 be as in (8). Then there are generators of $X(H)$, which are represented by polynomials with degree $\leq \kappa_2$.*

Proof. From Lemmas B.10 and B.8, H^t is bounded by $(2n)^{3\cdot 8^{n^2}}$. By Proposition B.6, there is a homomorphism $\tau_{H,H^t} : H \to \mathrm{GL}_{\kappa_1}(C)$ satisfying $\ker(\tau_{H,H^t}) = H^t$ and τ_{H,H^t} is bounded by κ_2, where κ_1 is as in (8). The homomorphism τ_{H,H^t} is of the from

$$\left(\frac{P_{i,j}^{H,H^t}(X)}{Q^{H,H^t}(X)}\right) \quad \text{where } \deg\left(P_{i,j}^{H,H^t}(X)\right) \leq \kappa_2,\ \deg\left(Q^{H,H^t}(X)\right) \leq \kappa_2.$$

From the proof of Proposition B.6, $Q^{H,H^t}(I_n) = 1$ and for any $h, h' \in H$,

$$Q^{H,H^t}\left(hh'\right) = \det\left(\left[hh'\right]\right) = \det\left([h]\left[h'\right]\right) = \det\left([h]\right)\det\left(\left[h'\right]\right) = Q^{H,H^t}(h)Q^{H,H^t}\left(h'\right).$$

This implies that $Q^{H,H^t}(X) \in X(H)$. Notice that $X((C^*)^{\kappa_1})$ is generated by the characters $y_1, \cdots, y_{\kappa_1}$ that are the coordinate functions of $(C^*)^{\kappa_1}$, and so is the group of characters of any its subgroup. Since $\tau_{H,H^t}(H)$ is a torus in $\mathrm{GL}_{\kappa_1}(C)$, it is conjugate to a subgroup of $(C^*)^{\kappa_1}$. So $X(\tau_{H,H^t}(H))$ is generated by some linear polynomials. The homomorphism τ_{H,H^t} induces a group homomorphism:

$$\begin{aligned} \tau^\circ_{H,H^t} : X\left(\tau_{H,H^t}(H)\right) &\to X(H) \\ \chi' &\to \chi' \circ \tau_{H,H^t} \end{aligned}$$

For any $\chi \in X(H)$ and $h \in H$, since $\chi(hh') = \chi(h)$ for all $h' \in H^t$, there is $g \in C[\tau_{H,H^t}(H)]$ such that $g \circ \tau_{H,H^t} = \chi$ (see p. 84, Section 12.3, [12]). One can verify that g is actually a character of $\tau_{H,H^t}(H)$. Therefore τ°_{H,H^t} is surjective. Let $L_1, \cdots, L_s$

be linear polynomials, which generate $X(\tau_{H,H^t}(H))$. Then $L_1 \circ \tau_{H,H^t}, \cdots, L_s \circ \tau_{H,H^t}$ generate $X(H)$. Since $Q^{H,H^t}(X) \in X(H)$,

$$Q^{H,H^t}(X), (L_1 \circ \tau_{H,H^t})Q^{H,H^t}(X), \cdots, (L_s \circ \tau_{H,H^t})Q^{H,H^t}(X)$$

still generate $X(H)$ and are polynomials bounded by κ_2. □

Let $P_1(X), \cdots, P_l(X)$ be in $C[X]_{\leq \kappa_2}$ such that their images in $C[X]_{\leq \kappa_2}/(I(H))_{\leq \kappa_2}$ constitute a C-basis of $C[X]_{\leq \kappa_2}/(I(H))_{\leq \kappa_2}$, where $I(H)$ is the vanishing ideal of H in $C[X]$. Let $c_1, \cdots, c_l$ be indeterminates and $P_{\mathbf{c}}(X) = \sum_{i=1}^{l} c_i P_i(X)$, where $\mathbf{c} = (c_1, \cdots, c_l)$. Then the conditions

$$P_{\mathbf{c}}(I_n) = 1 \quad \text{and} \quad \forall h, h' \in H, \quad P_{\mathbf{c}}(h)P_{\mathbf{c}}\big(h'\big) - P_{\mathbf{c}}\big(hh'\big) = 0$$

induce a system of algebraic equations J for $\mathbf{c}$. Precisely, let I be the ideal in $C[X, Y]$ generated by $\{Q(X), Q(Y) \mid Q \in I(H)\}$ where Y denotes the set of indeterminates $y_{1,1}, y_{1,2}, \cdots, y_{n,n}$. Then I is the vanishing ideal of $H \times H$ in $C[X, Y]$. In the following, for ease of notation, Y also denotes the matrix $(y_{i,j})$. Assume that $\mathbb{G}$ is a Gröbner basis of I with respect to some monomial ordering. Denote by $\bar{P}_{i,j}$ the remainder of $P_i(X)P_j(Y)$ on division by $\mathbb{G}$ and $\tilde{P}_i$ the remainder of $P_i(XY)$ on the division by $\mathbb{G}$, i.e.

$$\bar{P}_{i,j} = \overline{P_i(X)P_j(Y)}^{\mathbb{G}}, \qquad \tilde{P}_i = \overline{P_i(XY)}^{\mathbb{G}}, \quad i, j = 1, \cdots, l.$$

Then J can be taken to be the union of $\{c_1P_1(I_n) + \cdots + c_lP_l(I_n) - 1\}$ and the set of coefficients of the polynomial

$$\sum_{1 \leq i,j \leq l} c_i c_j \bar{P}_{i,j} - \sum_{1 \leq i \leq l} c_i \tilde{P}_i.$$

Moreover, we have the following proposition.

Proposition B.18. $\dim(J) = 0$ *and for each* $\bar{\mathbf{c}} \in \mathrm{Zero}(J) \cap C^l$, $P_{\bar{\mathbf{c}}}(X)$ *is a character of* H.

Proof. Evidently, for each $\bar{\mathbf{c}} \in \mathrm{Zero}(J) \cap C^l$, $P_{\bar{\mathbf{c}}}(X)$ is a morphism from H to C^* and thus a character of H. Suppose that $\bar{\mathbf{c}}, \bar{\mathbf{c}}' \in \mathrm{Zero}(J) \cap C^l$ and $P_{\bar{\mathbf{c}}}(h) = P_{\bar{\mathbf{c}}'}(h)$ for all $h \in H$. Then this implies that $P_{\bar{\mathbf{c}}}(X) - P_{\bar{\mathbf{c}}'}(X) \in (I(H))_{\leq \kappa_2}$. Hence

$$\sum_{i=1}^{l} \big(\bar{c_i} - \bar{c_i}'\big) P_i(X) \equiv 0 \mod \big(I(H)\big)_{\leq \kappa_2}$$

where $\bar{\mathbf{c}} = (\bar{c_1}, \cdots, \bar{c_l})$ and $\bar{\mathbf{c}}' = (\bar{c_1}', \cdots, \bar{c_l}')$. Since $P_1(X), \cdots, P_l(X)$ modulo $(I(H))_{\leq \kappa_2}$ are linearly independent over C. So $\bar{\mathbf{c}} = \bar{\mathbf{c}}'$. That is to say, the map $\varphi : \mathrm{Zero}(J) \cap C^l \to X(H)$ defined by $\varphi(\bar{\mathbf{c}}) = P_{\bar{\mathbf{c}}}(X)$ is injective. Suppose that $\dim(J) > 0$. If C is

uncountable, then $\mathrm{Zero}(J) \cap C^l$ is uncountable and so is $X(H)$. However, it is known that $X(H)$ is a countable set, a contradiction. Hence in this case $\dim(J) = 0$. Now assume that C is countable. Then C can be embedded into $\mathbb{C}$, the field of complex numbers. One may check that if $\bar{\mathbf{c}} \in \mathrm{Zero}(J) \cap \mathbb{C}^l$, then $P_{\bar{\mathbf{c}}}(X)$ determines a character of $H(\mathbb{C})$ and the map $\bar{\varphi} : \mathrm{Zero}(J) \cap \mathbb{C}^l \to X(H(\mathbb{C}))$ is still injective. An argument similar to the one used previously implies that $\dim(J) = 0$. □

Given a connected subgroup H of $\mathrm{GL}_n(C)$, Propositions B.17 and B.18 allow us to compute a set of generators of $X(H)$ that are represented by polynomials in $C[X]$.

Algorithm B.19. Input: a set $\mathbb{S}$ of generators of $I(H)$, the vanishing ideal of a connected algebraic group H. Output: a set of generators of $X(H)$, the group of characters of H.

(*a*) Compute a Gröbner basis of $I(H)$ with respect to some monomial ordering, and find a C-basis of $C[X]_{\leq \kappa_2}/(I(H))_{\leq \kappa_2}$, say $P_1, \cdots, P_l$, where κ_2 is as in (8).

(*b*) Let $I = (\{Q(X), Q(Y) \mid Q \in \mathbb{S}\})$. Compute a Gröbner basis $\mathbb{G}$ of I and the following remainders on division by $\mathbb{G}$

$$\bar{P}_{i,j} = \overline{P_i(X)P_j(Y)}^{\mathbb{G}}, \qquad \tilde{P}_i = \overline{P_i(XY)}^{\mathbb{G}}, \quad i, j = 1, \cdots, l.$$

(*c*) Set

$$R = \sum_{1 \leq i,j \leq l} c_i c_j \bar{P}_{i,j} - \sum_{1 \leq i \leq l} c_i \tilde{P}_i,$$

where $c_1, \cdots, c_l$ are indeterminates. Let J be the union of $\{c_1 P_1(I_n) + \cdots + c_l P_l(I_n) - 1\}$ and the set of coefficients of R in X, Y. Solve J.

(*d*) Return $\{\bar{c}_1 P_1 + \cdots + \bar{c}_l P_l \mid (\bar{c}_1, \cdots, \bar{c}_l) \in \mathrm{Zero}(J) \cap C^l\}$.

The example below will demonstrate the above algorithm.

Example B.20. Consider

$$H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a^2 + b^2 \neq 0 \right\}.$$

Then H is an irreducible algebraic group and $I(H)$ is generated by $\{x_{1,1} - x_{2,2}, x_{1,2} + x_{2,1}\}$. We shall only compute the elements in $X(H)$, which can be represented by polynomials with degree not greater than one.

(*a*) One has that the images of $1, x_{2,1}, x_{2,2}$ are a C-basis of $C[x_{1,1}, \cdots, x_{2,2}]_{\leq 1}/(I(H))_{\leq 1}$. Let $P_1 = 1$, $P_2 = x_{2,1}$, $P_3 = x_{2,2}$.

(*b*) With respect to the monomial ordering $x_{1,1} > x_{1,2} > x_{2,1} > x_{2,2} > y_{1,1} > y_{1,2} > y_{2,1} > y_{2,2}$,

$$\{y_{1,2} + y_{2,1}, y_{1,1} - y_{2,2}, x_{1,2} + x_{2,1}, x_{1,1} - x_{2,2}\}$$

is a Gröbner basis of $I(H \times H)$. We can then compute

$$\bar{P}_{1,1} = 1, \quad \bar{P}_{1,2} = y_{2,1}, \quad \bar{P}_{1,3} = y_{2,2}, \quad \bar{P}_{2,1} = x_{2,1}, \quad \bar{P}_{2,2} = x_{2,1}y_{2,1},$$
$$\bar{P}_{2,3} = x_{2,1}y_{2,2}, \quad \bar{P}_{3,1} = x_{2,2}, \quad \bar{P}_{3,2} = x_{2,2}y_{2,1}, \quad \bar{P}_{3,3} = x_{2,2}y_{2,2},$$
$$\tilde{P}_1 = 1, \quad \tilde{P}_2 = x_{2,1}y_{2,2} + x_{2,2}y_{2,1}, \quad \tilde{P}_3 = x_{2,2}y_{2,2} - x_{2,1}y_{2,1}.$$

(*c*) Calculate the set J, which is defined in the step (c) of Algorithm B.19. Then one has

$$J = \{c_1 + c_3 - 1, c_1^2 - c_1, c_2^2 + c_3, c_2c_3 - c_2, c_3^2 - c_3, c_1c_2, c_1c_3\}.$$

Solving J, we obtain $\{c_1 = 1, c_2 = c_3 = 0\}$, $\{c_1 = 0, c_2 = \pm\sqrt{-1}, c_3 = 1\}$.

(*d*) Hence 1, $x_{2,2} \pm \sqrt{-1}x_{2,1}$ are all characters that can be represented by polynomials with degree not greater than one.

References

[1] D. Bertrand, F. Beukers, Équations différentielles linéaires et majorations de multiplicités, Ann. Sci. Éc. Norm. Supér. 4 (1985) 181–192.
[2] E. Compoint, M.F. Singer, Computing Galois groups of completely reducible differential equations, J. Symbolic Comput. 28 (1999) 473–494.
[3] O. Cormier, M.F. Singer, F. Ulmer, Computing the Galois group of a polynomial using linear differential equations, in: H. Barendegt, A.M. Cohen (Eds.), Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation, ACM Press, New York, 2000, pp. 78–85.
[4] D.A. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer-Verlag, New York, 1996.
[5] T.W. Dube, The Structure of polynomial ideals and Gröbner bases, SIAM J. Comput. 19 (1990) 750–773.
[6] D. Eisenbud, C. Huneke, W. Vasconcelos, Direct methods for primary decomposition, Invent. Math. 110 (1992) 207–235.
[7] X.S. Gao, S.C. Chou, Solving parametric algebraic systems, in: P.S. Wang (Ed.), Proceedings of the 1992 International Symposium on Symbolic and Algebraic Computation, ACM Press, New York, 1992, pp. 335–341.
[8] P. Gianni, B. Trager, G. Zacharias, Gröbner bases and primary decomposition of polynomials ideals, J. Symbolic Comput. 6 (1988) 149–167.
[9] D.Yu. Grigoriev, Complexity of irreducibility testing for a system of linear ordinary differential equations, in: S. Watanabe, M. Nagata (Eds.), Proceedings of the 1990 International Symposium on Symbolic and Algebraic Computation, ACM Press, New York, 1990, pp. 225–230.
[10] E. Hrushovski, Computing the Galois group of a linear differential equation, in: T. Crespo, Z. Hajto (Eds.), Differential Galois Theory, in: Banach Center Publ., vol. 58, Polish Acad. Sci., Warsaw, 2002, pp. 97–138.
[11] A. Hulpke, Techniques for the computation of Galois groups, in: B.H. Matzat, G.M. Greuel, G. Hiss (Eds.), Algorithmic Algebra and Number Theory, Springer-Verlag, Berlin, 1999, pp. 65–77.
[12] J.E. Humphreys, Linear Algebraic Groups, Springer-Verlag, New York, 1981.
[13] J.J. Kovacic, An algorithm for solving second order linear homogeneous differential equations, J. Symbolic Comput. 2 (1986) 3–43.

[14] B. Li, D. Wang, An algorithm for transforming regular chain into normal chain, in: D. Kapur (Ed.), Computer Mathematics, in: LNAI, vol. 5081, Springer-Verlag, Berlin, 2008, pp. 236–245.
[15] A.R. Magid, Lectures on Differential Galois Theory, Univ. Lecture Ser., vol. 7, American Mathematical Society, Providence, RI, 1994.
[16] I. Schur, Über gruppen periodischer substitutionen, Sitzber. Preuss. Akad. Wiss. (1911) 619–627.
[17] A. Seidenberg, Constructions in algebra, Trans. Amer. Math. Soc. 197 (1974) 273–313.
[18] M.F. Singer, Liouvillian solutions of linear differential equations with liouvillian coefficients, J. Symbolic Comput. 11 (1991) 251–274.
[19] M.F. Singer, Moduli of linear differential equations on the Riemann sphere with fixed Galois groups, Pacific J. Math. 160 (1993) 343–395.
[20] M.F. Singer, Introduction to the Galois theory of linear differential equations, in: M.A.H. MacCallum, A.V. Mikhalov (Eds.), Algebraic Theory of Differential Equations, in: London Math. Soc. Lecture Note Ser., vol. 357, Cambridge Univ. Press, Cambridge, 2009, pp. 1–82.
[21] M.F. Singer, F. Ulmer, Galois groups of second and third order linear differential equations, J. Symbolic Comput. 16 (1993) 9–36.
[22] M. van der Put, Galois theory and algorithms for linear differential equations, J. Symbolic Comput. 39 (2005) 451–463.
[23] M. van der Put, M.F. Singer, Galois Theory of Linear Differential Equations, Springer-Verlag, Berlin, 2003.
[24] M. van Hoeij, J.A. Weil, An algorithm for computing invariants of differential Galois groups, J. Pure Appl. Algebra 117/118 (1997) 353–379.