MATHEMATICS OF COMPUTATION
Volume 87, Number 310, March 2018, Pages 941–965
http://dx.doi.org/10.1090/mcom/3232
Article electronically published on June 27, 2017

ON THE COMPUTATION OF THE GALOIS GROUP OF LINEAR DIFFERENCE EQUATIONS

RUYONG FENG

Abstract. We present an algorithm that determines the Galois group of linear difference equations with rational function coefficients.

1. Introduction

The current algorithms for computing the Galois groups of linear difference equations were only valid for equations of special types, such as second order equations, equations of diagonal form or with constant coefficients and so on. In [11, 12], a (q-)difference analogue of Kovacic's algorithm was developed for linear (q-)difference equations of order two. For the basic hypergeometric equations and Mahler equations of order two, algorithms were given in [23, 24]. In [31], algorithms for linear difference equations of diagonal form were developed. For linear difference equations with constant coefficients, an algorithm can be found in [29], where the author further showed that there is a recursive procedure that derives the Galois group from the ideal of algebraic relations among solutions, and vice versa. In [7], some general properties of Galois groups were established for linear difference equations of order two on elliptic curves and were applied to the calculation of some Galois groups. In [19], upper and lower bounds were given for the Galois groups of Frobenius difference equations over $(\mathbb{F}_q(s,t),\phi_q)$, where $\phi_q(s)=s^q$ and $\phi_q(a)=a$ for all $a\in\mathbb{F}_q(t)$. In contrast, algorithms for computing the Galois groups of linear differential equations have been well-developed (see [2, 3, 14, 17, 27]). Particularly, in [14], Hrushovski developed an algorithm that calculates the Galois group of all linear differential equations with rational function coefficients. His algorithm involved many arguments from logical language and has recently been reworked by Rettstadt in [22] and by the author in [9]. In this paper, we develop an algorithm for computing the Galois group of linear difference equations with rational function coefficients of arbitrary order. Our algorithm can be considered as a difference analogue of Hrushovski's algorithm.

The philosophy of computing the Galois groups of linear difference equations is quite similar to that of linear differential equations. Galois groups of these two kinds of equations are linear algebraic groups over the field of constants. Hence bounds for the defining equations of linear algebraic groups developed for the differential case can be applied to the difference case without any modification. However, there exist some results in differential algebra whose difference analogues are no longer

Received by the editor June 2, 2015 and, in revised form, September 2, 2016 and September 20, 2016.

2010 *Mathematics Subject Classification.* Primary 39A06, 12H10, 68W30.

This work was partially supported by a National Key Basic Research Project of China (2011CB302400) and by a grant from NSFC (11371143).

correct, and vice versa. For example, associated primes of a radical differential ideal are still differential ideals, while those of a radical σ-ideal need not be σ-ideals but σ^δ-ideals for some integer δ. This forces us to consider σ^δ-ideals. Another example is that the Picard-Vessiot extension ring for a linear differential equation is not necessarily the coordinate ring of a trivial torsor for the Galois group, while that for a linear difference equation is the coordinate ring of a trivial torsor. This implies that one only needs to consider objects such as hypergeometric elements that are defined over the base field.

Throughout this paper, C stands for the algebraic closure of a field that is finitely generated over the rational numbers. k stands for the field of rational functions in x with coefficients in C and $\bar{k}$ denotes the algebraic closure of k. The difference field which we are interested in is the field k with an automorphism σ given by $\sigma(x) = x + 1$ and $\sigma(c) = c$ for $c \in C$. Consider the linear difference equation

$$\sigma(Y) = AY, \tag{1.1}$$

where Y is an $n \times 1$ vector with indeterminate entries and $A \in \mathrm{GL}_n(k)$. Let R be the Picard-Vessiot extension ring of k for (1.1). The Galois group of (1.1) over k, denoted by $\mathrm{Gal}(R/k)$, is defined to be the set of σ-k-automorphisms of R, i.e., k-automorphisms of R that commute with σ. Let F be a fundamental matrix of (1.1) with entries in R, i.e., $F \in \mathrm{GL}_n(R)$ satisfying $\sigma(F) = AF$. Then for any $\phi \in \mathrm{Gal}(R/k)$, $\phi(F)$ is another fundamental matrix of (1.1). Thus there exists $[\phi] \in \mathrm{GL}_n(C)$ such that $\phi(F) = F[\phi]$. The map given by $\phi \to [\phi]$ is a group homomorphism of $\mathrm{Gal}(R/k)$ into $\mathrm{GL}_n(C)$. Denote by G the set $\{[\phi] \mid \phi \in \mathrm{Gal}(R/k)\}$. It was proved in (Theorem 1.13, page 11 of [31]) that G is a linear algebraic group defined over C. The reader is referred to Chapter 1 of [31] for more information about the Galois theory of linear difference equations.

The group G can be reformulated as the stabilizer of some ideal in a σ-ring, which we describe below. Let Y denote an $n \times n$ matrix $(y_{i,j})$, where the $y_{i,j}$ are indeterminates. Sometimes, in brief, we also consider Y as a set of indeterminates. By setting $\sigma(Y) = AY$, one can extend σ from k to $k[Y, 1/\det(Y)]$ so that it becomes a difference extension ring of k. An ideal $I \subseteq k[Y, 1/\det(Y)]$ is called a σ-ideal if $\sigma(I) \subseteq I$. The results in section 1.1 of [31] imply that R is isomorphic to $k[Y, 1/\det(Y)]/I$ for some maximal σ-ideal I. Define an action of $\mathrm{GL}_n(C)$ on $k[Y, 1/\det(Y)]$ given by $g \cdot Y = Yg$ for all $g \in \mathrm{GL}_n(C)$. Suppose that J is an ideal of $k[Y, 1/\det(Y)]$. The *stabilizer* of J, denoted by $\mathrm{stab}(J)$, is defined as

$$\mathrm{stab}(J) = \{g \in \mathrm{GL}_n(C) \mid P(Yg) \in J,\ \forall\ P \in J\},$$

which is an algebraic subgroup of $\mathrm{GL}_n(C)$. Set

$$I_F = \{P \in k[Y, 1/\det(Y)] \mid P(F) = 0\}.$$

Then I_F is a maximal σ-ideal and $G = \mathrm{stab}(I_F)$. By the uniqueness of the Picard-Vessiot extension ring of k for (1.1), one sees that for any maximal σ-ideal I of $k[Y, 1/\det(Y)]$, there is $g \in \mathrm{GL}_n(C)$ such that $g \cdot I = I_F$. From this, one can readily verify that the stabilizers of maximal σ-ideals in $k[Y, 1/\det(Y)]$ are conjugate. In other words, as linear algebraic groups, these stabilizers are isomorphic. Therefore we shall also call the stabilizer of a maximal σ-ideal of $k[Y, 1/\det(Y)]$ the Galois group of (1.1) over k. Using the Gröbner basis method, one can easily obtain the defining equations of $\mathrm{stab}(I)$ once a Gröbner basis of I is known. Thus, the above definition indicates that finding a maximal σ-ideal of $k[Y, 1/\det(Y)]$ will suffice to

determine the Galois group. We shall give in this paper an algorithm that computes a maximal σ-ideal of $k[Y, 1/\det(Y)]$.

The rest of the paper is organized as follows. In section 2, we introduce some basic results that provide the theoretical background of our algorithm. Meanwhile, we introduce some basic definitions such as proto-groups, proto-maximal σ-ideals and so on. In section 3, we show how to compute a proto-maximal σ-ideal. In section 4, we describe a method to extend a proto-maximal σ-ideal to a maximal σ^δ-ideal so that one can easily obtain a maximal σ-ideal by taking the intersection of ideals. In section 5, the methods developed in the previous sections are summarized as an algorithm, and an example is presented to illustrate the algorithm. In Appendix A, we describe a method to find coefficient bounds for generators of a proto-maximal σ-ideal. In Appendix B, an algorithm for computing σ^δ-hypergeometric elements in $k[Y, 1/\det(Y)]/I_{\text{irr}}$ is developed, where I_{irr} is a prime σ^δ-ideal.

2. Some basic results

In this section, we shall introduce some basic results about proto-groups, k-torsors and several related problems whose algorithmic solutions will be needed in our algorithm.

Let H be an algebraic subgroup of $\mathrm{GL}_n(C)$. For ease of notation, we shall use $H(k)$ (resp. $H(\bar{k})$) to denote k-points (resp. $\bar{k}$-points) of H. H_u stands for the algebraic subgroup of H generated by unipotent elements and H° denotes the identity component of H.

2.1. **Proto-groups.** As in the differential case, degree bounds on proto-groups play a central role in the main algorithm presented in this paper. In this subsection, we will first introduce the notion of proto-groups and then present a degree bound on them as well as a property of them.

Definition 2.1. Let H be an algebraic subgroup of $\mathrm{GL}_n(C)$. H is said to be bounded by a positive integer d if there is a set $\mathbb{S} \subseteq C[Y]$ such that H is the set of zeroes of $\mathbb{S}$ in $\mathrm{GL}_n(C)$ and elements of $\mathbb{S}$ are of degree not greater than d.

Definition 2.2. Let G, H be two algebraic subgroups of $\mathrm{GL}_n(C)$. H is said to be a proto-group of G if they satisfy the following condition:

$$H_u \leq G^\circ \leq G \leq H.$$

In the case that G is the Galois group of (1.1) over k, H is called a proto-Galois group of (1.1) over k.

Remark 2.3. Let G, H be two algebraic subgroups of $\mathrm{GL}_n(C)$ and $G \leq H$.

(a) Suppose that H is a proto-group of G and $\bar{H}$ is an algebraic group satisfying $G \leq \bar{H} \leq H$. Then $\bar{H}$ is also a proto-group of G, since $\bar{H}_u \leq H_u$.
(b) If $H_u = 1$, then H is reductive. However, in general, the converse is not true. For instance, let $H = \mathrm{GL}_n(C)$. Then H is reductive but $H_u = \mathrm{SL}_n(C)$.
(c) Due to the Theorem on page 99 of [13], $H_u = 1$ if and only if H consists of semisimple elements. This implies that $H_u = 1$ if and only if H° is a torus. Therefore, if H° is a torus, then H is a proto-group of G. Conversely, if H is a proto-group of G and G° is a torus, then H° is a torus too.
(d) If H is a proto-Galois group of (1.1) over k and I is a maximal σ-ideal of $k[Y, 1/\det(Y)]$, then H is a proto-group of some algebraic group conjugate to $\mathrm{stab}(I)$.

Below are some examples of algebraic groups and their proto-groups.

Example 2.4.

(1) Let H be an algebraic group satisfying $\mathrm{SL}_n(C) \leq H \leq \mathrm{GL}_n(C)$. Then H is a proto-group of $\mathrm{SL}_n(C)$, since $H_u = \mathrm{SL}_n(C)$.

(2) Let $G^{\mu,\nu} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \begin{array}{c} a, c \in C^\times, b \in C \\ a^\mu c^\nu = 1 \end{array} \right\}$ where $\mu, \nu \in \mathbb{Z}$ and $C^\times$ is the multiplicative group of C. Then $G^{0,0}$ is a maximal proto-group of $G^{\mu,\nu}$ for all $\mu, \nu \in \mathbb{Z}$, since

$$G_u^{\mu,\nu} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in C \right\}$$

and if $g \in \mathrm{GL}_2(C) \setminus G^{0,0}$, then the algebraic subgroup of $\mathrm{GL}_2(C)$ generated by g and $G^{0,0}$ contains a unipotent element not in $G_u^{\mu,\nu}$.

(3) Let

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in C^\times \right\} \cup \left\{ \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \middle| a, b \in C^\times \right\}.$$

Then H is a proto-group of any of its algebraic subgroups, since $H_u = 1$.

(4) Let G be an element in $\left\{ A_4^{\mathrm{SL}_2}, S_4^{\mathrm{SL}_2}, A_5^{\mathrm{SL}_2} \right\}$ where $*^{\mathrm{SL}_2}$ stands for the preimage of $*$ under the canonical projection from $\mathrm{SL}_2(C)$ to $\mathrm{PSL}_2(C)$. Then $C^\times \cdot G$ is a proto-group of G.

The key point of Hrushovski's algorithm is the following proposition, which provides a degree bound on proto-groups.

Proposition 2.5 (Corollary 3.7 of [14], Corollary B.15 of [9])**.** *One can find an integer $\tilde{d}$ only depending on n such that for any algebraic subgroup G of $\mathrm{GL}_n(C)$, there is a proto-group of G bounded by $\tilde{d}$.*

The above proposition implies that given any linear difference equation of order n, there exists a proto-Galois group of it bounded by the integer $\tilde{d}$. The integer $\tilde{d}$ can be explicitly given as follows (see Corollary B.15 of [9] for details). Set

$$\kappa_1 = \max_i \left\{ \binom{\binom{n^2+(2n)^{3\cdot 8^{n^2}}}{n^2}}{i}^2 \right\}, \qquad \kappa_2 = \kappa_1 (2n)^{3\cdot 8^{n^2}} \binom{n^2 + (2n)^{3\cdot 8^{n^2}}}{n^2} \tag{2.1}$$

and

$$\kappa_3 = \kappa_2(\kappa_1^2+1) \max_i \left\{ \binom{\kappa_1^2+1}{i} \right\}, \quad I(n) = J\left(\max_i \left\{ \binom{n^2+1}{i}^2 \right\} \right),$$

where $J(m)$ is an integer value function called Jordan bound and it is not greater than $\left(\sqrt{8m}+1\right)^{2m^2} - \left(\sqrt{8m}-1\right)^{2m^2}$. Then

$$\tilde{d} = (\kappa_3)^{I(n)-1}. \tag{2.2}$$

It is well-known in the theory of linear algebraic groups that any algebraic subgroup of a diagonalizable group D is the intersection of the kernels of some characters of D (see the Proposition on page 103 of [13]). Given a connected algebraic group H, the following proposition describes algebraic subgroups of H, which are characterized by characters of H.

Proposition 2.6. *Suppose that H is a connected algebraic subgroup of $\mathrm{GL}_n(C)$. Then G is the intersection of the kernels of some characters of H if and only if H is a proto-group of G.*

Proof. Assume that H is a proto-group of G. Let $\chi_1, \cdots, \chi_\ell$ be generators of $X(H)$, the group of characters of H. Define a map $\psi : H \to (C^\times)^\ell$ given by $\psi(h) = (\chi_1(h), \cdots, \chi_\ell(h))$. Then $\psi(H)$ is a diagonalizable group and $\psi(G)$ is one of its algebraic subgroups. Due to the Proposition on page 103 of [13], $\psi(G)$ is the intersection of the kernels of some characters of $\psi(H)$. Denote these characters by $\bar{\chi}_1, \cdots, \bar{\chi}_l$. Notice that ψ induces a group homomorphism

$$\psi^* : X\left((C^\times)^\ell\right) \to X(H),$$
$$\chi \to \chi \circ \psi.$$

We claim that $G = \bigcap_{i=1}^{l} \ker\left(\psi^*(\bar{\chi}_i)\right)$. Obviously, $G \subseteq \cap_{i=1}^{l} \ker\left(\psi^*(\bar{\chi}_i)\right)$. Suppose that $h \in \cap_{i=1}^{l} \ker\left(\psi^*(\bar{\chi}_i)\right)$. Then $\bar{\chi}_i(\psi(h)) = 1$ for all $1 \le i \le l$. This implies that $\psi(h) \in \psi(G)$. Lemma B.10 of [9] states that $H_u = \ker(\psi)$. Hence $\ker(\psi) \subseteq G$ and then $h \in G$. In what follows, $\bigcap_{i=1}^{l} \ker\left(\psi^*(\bar{\chi}_i)\right) \subseteq G$. This proves the claim.

Conversely, assume that G is the intersection of the kernels of some characters of H. Then $H_u = \ker(\psi) \subseteq G$. Since H_u is connected, $H_u \subseteq G^\circ$. Thus H is a proto-group of G. □

The connection between proto-groups and σ-ideals in $k[Y, 1/\det(Y)]$ is provided by geometric objects called k-torsors, which are introduced in the next section.

2.2. **k-Torsors.** Throughout the paper, we shall use $\mathrm{Zero}(J)$ to denote the set of zeroes of J in $\mathrm{GL}_n(\bar{k})$, where J is a subset of $k[Y, 1/\det(Y)]$. Suppose that $Z \subseteq \mathrm{GL}_n(\bar{k})$ is a variety defined over k. We shall use $\mathbf{I}_k(Z)$ to denote the set of all polynomials in $k[Y, 1/\det(Y)]$ that vanish on Z.

Definition 2.7. (see Definition 3.13 of [29]) Let $Z \subseteq \mathrm{GL}_n(\bar{k})$ be a variety defined over k and H an algebraic subgroup of $\mathrm{GL}_n(\bar{k})$ defined over k. Z is said to be a k-torsor for H if for any $z_1, z_2 \in Z$, there is a unique $h \in H$ such that $z_1 = z_2 h$. A k-torsor Z for H is said to be trivial if $Z \cap \mathrm{GL}_n(k) \neq \emptyset$, i.e., $Z = BH$ for some $B \in \mathrm{GL}_n(k)$.

Remark 2.8. Note that if Z is a trivial k-torsor for H, then $Z = BH$ for any $B \in Z \cap \mathrm{GL}_n(k)$.

Let I be a maximal σ-ideal of $k[Y, 1/\det(Y)]$. Then one has that

Proposition 2.9 (Proposition 1.20, p. 15 of [31])**.** $\mathrm{Zero}(I)$ *is a trivial k-torsor for $G(\bar{k})$, where $G = \mathrm{stab}(I)$.*

For convenience, we introduce proto-maximal σ-ideals, which are defined to be the ideals of trivial k-torsors for proto-Galois groups.

Definition 2.10. Let I be a σ-ideal in $k[Y, 1/\det(Y)]$ and $G = \mathrm{stab}(I)$. Then I is said to be *proto-maximal* if G is a proto-Galois group of (1.1) over k and $\mathrm{Zero}(I)$ is a trivial k-torsor for $G(\bar{k})$.

Remark 2.11.

(a) Proposition 2.9 implies that maximal σ-ideals are proto-maximal.

(b) Suppose that I is a proto-maximal σ-ideal and $\tilde{I}$ is a maximal σ-ideal containing I. Let $H = \mathrm{stab}(I)$ and $G = \mathrm{stab}(\tilde{I})$. We claim that H is a proto-group of G. In fact, let B be an element in $\mathrm{Zero}(\tilde{I}) \cap \mathrm{GL}_n(k)$. As $\mathrm{Zero}(I)$ and $\mathrm{Zero}(\tilde{I})$ are trivial k-torsors,

$$\mathrm{Zero}(\tilde{I}) = BG(\bar{k}) \subseteq \mathrm{Zero}(I) = BH(\bar{k}).$$

Hence $G \leq H$. By Remark 2.3, since H is a proto-Galois group, there is $g \in \mathrm{GL}_n(C)$ such that H is a proto-group of gGg^{-1}, i.e., $H_u \leq gGg^{-1} \leq H$. Note that $g^{-1}H_u g \leq H_u$ because $g^{-1}H_u g$ is generated by unipotent elements and $g^{-1}H_u g \leq G \leq H$. As H_u is connected and both $g^{-1}H_u g$ and H_u are of the same dimension, $g^{-1}H_u g = H_u$. Therefore $H_u \leq G$, which implies that H is a proto-group of G.

Suppose that H is a connected algebraic subgroup of $\mathrm{GL}_n(C)$ and Z is a trivial k-torsor for $H(\bar{k})$. Then for any $B \in Z \cap \mathrm{GL}_n(k)$, the map given by

$$k[Y, 1/\det(Y)]/\mathbf{I}_k(H) \to k[Y, 1/\det(Y)]/\mathbf{I}_k(Z) \tag{2.3}$$
$$P(Y) \to P(B^{-1}Y)$$

is an isomorphism of k-algebras. A theorem of Rosenlicht ([18, 25, 28]) implies that invertible regular functions on Z are closely related to characters of H. This theorem states: let G be a connected linear algebraic group defined over an algebraically closed field $\bar{k}$ and let y be a regular function on G with $1/y$ also a regular function, then y is a $\bar{k}$ multiple of a character. Notice that characters of H can be viewed as elements in $C[Y, 1/\det(Y)]/\mathbf{I}_C(H)$.

Lemma 2.12. *Suppose that J is a prime σ^δ-ideal of $k[Y, 1/\det(Y)]$ where $\delta \geq 1$, and $\mathrm{Zero}(J)$ is a trivial k-torsor for $H(\bar{k})$ where H is a connected algebraic subgroup of $\mathrm{GL}_n(C)$. Let $B \in \mathrm{Zero}(J) \cap \mathrm{GL}_n(k)$. If χ is a character of H, then $\chi(B^{-1}Y)$ is invertible in $k[Y, 1/\det(Y)]/J$. Conversely, if P is an invertible element in $k[Y, 1/\det(Y)]/J$, then $P = r\chi(B^{-1}Y)$ for some $r \in k$ and some character χ of H.*

Proof. We only need to prove the second assertion. Since C is algebraically closed, $H(\bar{k})$ viewed as a linear algebraic group defined over $\bar{k}$ is still connected. The map (2.3) implies that $P(BY)$ is invertible in $k[Y, 1/\det(Y)]/\mathbf{I}_k(H)$. Applying the above theorem of Rosenlicht to $P(BY)$, one has that $P(BY) = r\chi$ for some $r \in \bar{k}$ and some character χ. Observe that $k[Y, 1/\det(Y)]/J$ is a σ^δ-extension domain of k. Due to Lemma 1.19 on page 15 of [31], $(k[Y, 1/\det(Y)]/J) \cap \bar{k} = k$. Hence $(k[Y, 1/\det(Y)]/\mathbf{I}_k(H)) \cap \bar{k} = k$. We then conclude that $r \in k$ and $P = r\chi(B^{-1}Y)$. □

In section 4, one will see that invertible elements of $k[Y, 1/\det(Y)]/J$ are actually σ^δ-hypergeometric over k. In the case where $\delta = 1$ and J is a proto-maximal σ-ideal, algebraic relations among these σ-hypergeometric elements will reveal the characters of $\mathrm{stab}(J)$ that determine the Galois group G.

2.3. **Some related problems.** In this paper, we shall need algorithmic solutions of the following problems.

(P1) Given an ideal in $k[Y]$, compute a Gröbner basis of it with respect to some monomial ordering. The reader is referred to section 2.7 of [5] and section 5.5 of [1] for the algorithms.

(P2) Given an ideal in $k[Y]$, compute its radical and its associated primes. There are several methods for this problem, for instance the methods presented in [10], sections 2 and 4 of [8], section 8.7 of [1], parts 36 and 42 of [26].

(P3) Compute the Galois group of linear difference equations of diagonal form. Equivalently, given $b_1, \cdots, b_\ell \in k$, compute a set of generators of the following $\mathbb{Z}$-module:

$$\left\{ (z_1, \cdots, z_\ell) \in \mathbb{Z}^\ell \;\middle|\; \exists\, f \in k^\times \text{ s.t. } \prod_{i=1}^{\ell} b_i^{z_i} = \frac{\sigma^\delta(f)}{f} \right\}, \text{ where } \delta \geq 1.$$

When $k = \mathbb{Q}(x)$, a method was described in section 2.2 of [31]. Using the results in section 3.2 of [6], one can adapt the method in [31] to solve the problem with $k = C(x)$. This problem is the bottleneck in extending our algorithm to equations over a larger base field.

(P4) Given linear difference equations with coefficients in k, compute all hypergeometric solutions. The reader is referred to ([4, 20]) for algorithms.

3. The computation of proto-maximal σ-ideals

Let F be a fundamental matrix of (1.1) and let d be a positive integer or ∞. Denote

$$I_{F,d} = \langle \{P(Y) \in k[Y]_{\leq d} \mid P(F) = 0\} \rangle, \tag{3.1}$$

where $k[Y]_{\leq d}$ denotes the set of polynomials in $k[Y]$ with degrees not greater than d, and $\langle * \rangle$ denotes the ideal in $k[Y, 1/\det(Y)]$ generated by $*$. When $d = \infty$, $I_{F,d}$ is equal to I_F defined in the Introduction. One can readily verify that $I_{F,d}$ is a σ-ideal and furthermore I_F is a maximal σ-ideal. The fact that $k[Y, 1/\det(Y)]$ is a Noetherian ring implies that for sufficiently large d, $I_{F,d}$ is a proto-maximal σ-ideal. Therefore to achieve a proto-maximal σ-ideal, one only needs to solve the following two problems: (a) Given an integer d, how does one compute $I_{F,d}$? (b) When is the integer d large enough such that $I_{F,d}$ is proto-maximal?

3.1. **The computation of $I_{F,d}$.** In [16], Kauers and Zimmerman presented an algorithm for computing generators for the ideal of algebraic relations among solutions of linear difference equations with constant coefficients. Their algorithm relies on the fact that one can explicitly write down solutions of the equations of such type. Here, our task is different. We only compute the ideal generated by algebraic relations with bounded degree, while we are interested in linear difference equations with coefficients in k.

We first show which fundamental matrix F we take in this section. Let $\mathcal{S}_C$ be the difference ring of germs at infinity of C (see Example 1.3 on page 4 of [31] for the definition). Let ρ be a nonnegative integer such that i is not a pole of entries of A and $\det(A(i)) \neq 0$ if $i \geq \rho$. Define an element $\mathbf{Z} = (Z_0, Z_1, \cdots)$ of $\mathrm{GL}_n(\mathcal{S}_C)$ as follows: $Z_i = 0$ for $0 \leq i < \rho$, $Z_\rho \in \mathrm{GL}_n(C)$ (arbitrary) and $Z_{i+1} = A(i)Z_i$ for $i \geq \rho$. Define a map

$$\psi : k[Y, 1/\det(Y)] \to \mathcal{S}_C$$

as follows:

$$\text{for } f \in k, \psi(f) = (0, \cdots, 0, f(i), f(i+1), \cdots,) \text{ and } \psi(Y) = \mathbf{Z},$$

where i is a nonnegative integer such that j is not a pole of f if $j \geq i$. Proposition 4.1 on page 45 of [31] states that ψ induces an embedding of $k[Y, 1/\det(Y)]/I$ into

$\mathcal{S}_C$, where $I = \ker(\psi)$ that is a maximal σ-ideal. Let F be the image of Y in $k[Y, 1/\det(Y)]/I$. From this construction, we have that $I_{F,d} = I_{\mathbf{Z},d}$.

The results in Appendix A imply that one can compute an integer ℓ such that $I_{F,d}$ has a set of generators consisting of polynomials in $C[x][Y]$ whose degrees in x are not greater than ℓ. Let $N = \binom{d+n^2}{d} - 1$ and $\mathbf{m}_0, \cdots, \mathbf{m}_N$ be all elements in $\mathbb{Z}_{\geq 0}^{n^2}$ with $|\mathbf{m}_i| \leq d$. Write $P = \sum_{i=0}^{\ell} \sum_{j=0}^{N} c_{j(\ell+1)+i} x^i Y^{\mathbf{m}_j}$ for generators P, where $Y^{\mathbf{m}_i} = \prod y_{j,l}^{m_{i,j,l}}$ with $\mathbf{m}_i = (m_{i,j,l})$. We can then reduce the original problem to the following one: find a basis of the vector space

$$U = \left\{ (c_0, c_1, \cdots, c_{(N+1)(\ell+1)-1}) \in C^{(N+1)(\ell+1)} \;\middle|\; \sum_{i=0}^{\ell} \sum_{j=0}^{N} c_{j(\ell+1)+i} x^i F^{\mathbf{m}_j} = 0 \right\}.$$

We are going to solve the latter problem. Observe that $\sigma(x^i F^{\mathbf{m}_j})$ is a k-linear combination of the monomials $F^{\mathbf{m}_0}, \cdots, x^i F^{\mathbf{m}_j}, \cdots, x^\ell F^{\mathbf{m}_N}$. Hence there is a nonzero linear difference operator L in $C[x][\sigma]$ such that $L(x^i F^{\mathbf{m}_j}) = 0$ for all $0 \leq i \leq \ell$ and $0 \leq j \leq N$. This operator L can be computed using equation (1.1). Notice that at present, we do not know the ideal I and thus do not know F. Fortunately, one can easily compute the first many terms of the sequence solution $\mathbf{Z}$ that can be considered as a difference analogue of formal power series solutions of linear differential equations.

For convenience, write (1.1) and L in the form of linear recurrence equations

$$Y_{m+1} = A(m) Y_m, m \geq \rho \tag{3.2}$$

and

$$L = a_l(m) y_{m+l} + a_{l-1}(m) y_{m+l-1} + \cdots + a_0(m) y_m, \; m \geq \nu, \tag{3.3}$$

where ρ is a positive integer such that i is not a pole of entries of $A(x)$ and $\det(A(i)) \neq 0$ for all $i \geq \rho$, and ν is an integer greater than the integer roots of $a_l(x) a_0(x) = 0$. One easily sees that

Lemma 3.1. *Assume that $\{s_\nu, s_{\nu+1}, \cdots, \}$ is a solution of (3.3). If there is a nonnegative integer j such that $s_{\nu+j} = \cdots = s_{\nu+l-1+j} = 0$, then $s_i = 0$ for all $i \geq \nu$.*

Let κ be an integer greater than ρ and ν. Notice that the sequence $\{Z_\rho, Z_{\rho+1}, \cdots\}$ is a solution of (3.2) and for all $0 \leq i \leq \ell$ and $0 \leq j \leq N$, the sequence $\{\kappa^i Z_\kappa^{\mathbf{m}_j}, (\kappa+1)^i Z_{\kappa+1}^{\mathbf{m}_j}, \cdots, \}$ is a solution of (3.3). Set

$$P_{\mathbf{c}}(x, Y) = \sum_{i=0}^{\ell} \sum_{j=0}^{N} c_{j(\ell+1)+i} x^i Y^{\mathbf{m}_j}, \text{where } \mathbf{c} = (c_0, \cdots, c_{N\ell+N+\ell}) \in C^{(N+1)(\ell+1)}.$$

Then the sequence $\{P_{\mathbf{c}}(\kappa, Z_\kappa), P_{\mathbf{c}}(\kappa+1, Z_{\kappa+1}), \cdots, \}$ is also a solution of (3.3).

Proposition 3.2. *$\mathbf{c} \in U$ if and only if $P_{\mathbf{c}}(i, Z_i) = 0$ for all $\kappa \leq i \leq \kappa + l - 1$.*

Proof. Assume that $\mathbf{c} \in U$. Then $P_{\mathbf{c}}(x, F) = 0$ and thus $\psi(P_{\mathbf{c}}(x, F)) = 0$. In other words, there is a positive integer j such that $P_{\mathbf{c}}(i, Z_i) = 0$ for all $i \geq j$. Lemma 3.1 implies that $P_{\mathbf{c}}(i, Z_i) = 0$ for all $\kappa \leq i \leq \kappa + l - 1$. Conversely, suppose that $P_{\mathbf{c}}(i, Z_i) = 0$ for all $\kappa \leq i \leq \kappa + l - 1$. By Lemma 3.1 again, $P_{\mathbf{c}}(i, Z_i) = 0$ for all $i \geq \kappa$. This implies that $\psi(P_{\mathbf{c}}(x, F)) = 0$. Equivalently, $P_{\mathbf{c}}(x, F) = 0$. Hence $\mathbf{c} \in U$. □

The conditions $P_{\mathbf{c}}(i, Z_i) = 0$ for all $\kappa \le i \le \kappa + l - 1$ induce a linear system for $\mathbf{c}$. Solving this system, we obtain a basis of U.

Algorithm 3.3. *Compute a basis of $I_{F,d}$.*

(i) *Using the results in Appendix A, compute an integer ℓ such that $I_{F,d}$ has generators consisting of polynomials in $C[x][Y]$ whose degrees in x are not greater than ℓ.*

(ii) *Construct a nonzero operator L in $C[x][\sigma]$ that annihilates $x^i F^{\mathbf{m}_j}$ for all $0 \le i \le \ell$ and $0 \le j \le N$, where $\mathbf{m}_0, \cdots, \mathbf{m}_N$ are all elements in $\mathbb{Z}_{\ge 0}^{n^2}$ satisfying $|\mathbf{m}_i| \le d$*

(iii) *Let κ be an integer that is greater than both ρ and all integer roots of the leading and trailing coefficients of L.*

(iv) *Compute $Z_\kappa, Z_{\kappa+1}, \cdots, Z_{\kappa+l-1}$, where $l = \operatorname{ord}(L)$. Set*

$$P_{\mathbf{c}}(x, Y) = \sum_{i=0}^{\ell} \sum_{j=0}^{N} c_{j(\ell+1)+i} x^i Y^{\mathbf{m}_j}, \mathbf{c} = (c_0, \cdots, c_{(N+1)(\ell+1)-1}).$$

Putting

$$P_{\mathbf{c}}(\kappa, Z_\kappa) = \cdots = P_{\mathbf{c}}(\kappa + l - 1, Z_{\kappa+l-1}) = 0,$$

we obtain a linear system $\mathcal{L}$ in $c_0, c_1, \cdots, c_{(N+1)(\ell+1)-1}$.

(v) *Solve $\mathcal{L}$ and return $\left\{ P_{\bar{\mathbf{c}}}(x, Y) \;\middle|\; \bar{\mathbf{c}} \text{ is a zero of } \mathcal{L} \text{ in } C^{(N+1)(\ell+1)} \right\}$.*

Example 3.4. Consider the Fibonacci numbers $F(n)$. It satisfies that

$$\begin{pmatrix} F(n+1) \\ F(n+2) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} F(n) \\ F(n+1) \end{pmatrix}.$$

Let

$$\mathbf{Z} = \left(I_2, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2, \cdots \right).$$

We are going to calculate $I_{\mathbf{Z},2}$. Using the results in Appendix A, one sees that there are generators of $I_{\mathbf{Z},2}$ whose degrees in x are zero. Let $\mathbf{m}_0, \cdots, \mathbf{m}_{14}$ be all vectors in $\mathbb{Z}_{\ge 0}^4$ satisfying $|\mathbf{m}_i| \le 2$. Let

$$L = \sigma^6 - 4\sigma^5 + 2\sigma^4 + 6\sigma^3 - 4\sigma^2 - 2\sigma + 1.$$

Then L annihilates $\mathbf{Z}^{\mathbf{m}_i}$ for all $0 \le i \le 14$. Set $\kappa = 0$. Computing the first 6 terms of $\mathbf{Z}$, denoted by Z_i for $i = 0, \cdots, 5$. Set $\mathbf{c} = (c_0, c_1, \cdots, c_{14})$ and let $P_{\mathbf{c}}(x, Y)$ be defined as in step (iv). Then

$$\begin{aligned}
P_{\mathbf{c}}(0, Z_0) &= c_0 + c_1 + c_4 + c_5 + c_8 + c_{14}, \\
P_{\mathbf{c}}(1, Z_1) &= c_0 + c_2 + c_3 + c_4 + c_9 + c_{10} + c_{11} + c_{12} + c_{13} + c_{14}, \\
P_{\mathbf{c}}(2, Z_2) &= c_0 + c_1 + c_2 + c_3 + 2c_4 + c_5 + c_6 + c_7 + 2c_8 + c_9 + c_{10} \\
&\quad + 2c_{11} + c_{12} + 2c_{13} + 4c_{14}, \\
P_{\mathbf{c}}(3, Z_3) &= c_0 + c_1 + 2c_2 + 2c_3 + 3c_4 + \cdots + 4c_{12} + 6c_{13} + 9c_{14}, \\
P_{\mathbf{c}}(4, Z_4) &= c_0 + 2c_1 + 3c_2 + 3c_3 + 5c_4 + \cdots + 9c_{12} + 15c_{13} + 25c_{14}, \\
P_{\mathbf{c}}(5, Z_5) &= c_0 + 3c_1 + 5c_2 + 5c_3 + 8c_4 + \cdots + 25c_{12} + 40c_{13} + 64c_{14}.
\end{aligned}$$

Solving the linear system $\{P_{\mathbf{c}}(i, Z_i)|i = 0, \cdots, 5\}$, one has that

$$c_0 = 0, c_1 = -c_4, c_2 = -c_4 - c_3, c_5 = -c_8 - c_{14},$$
$$c_6 = -c_8 - 2c_{14} - c_7 - c_{11} - c_{13}, c_9 = -c_{14} - c_{10} - c_{11} - c_{12} - c_{13}.$$

From this, one sees that $I_{\mathbf{Z},2}$ is generated by $y_{2,1} - y_{1,2},\ y_{2,2} - y_{1,2} - y_{1,1}$.

3.2. **When is $I_{F,d}$ proto-maximal?** Let $\tilde{d}$ be a bound on the degree of a proto-group as given in (2.2). In this section, we shall show that $I_{F,\tilde{d}}$ is proto-maximal. Before proving this, we first present two properties of $I_{F,d}$. The first one is that $I_{F,d}$ is locally maximal, i.e., it is maximal among proper σ-ideals in $k[Y, 1/\det(Y)]$ which are generated by polynomials in $k[Y]_{\leq d}$. The second one is that $\mathrm{Zero}(I_{F,d})$ is a trivial k-torsor for $H_{F,d}(\bar{k})$ where $H_{F,d} = \mathrm{stab}(I_{F,d})$.

Proposition 3.5. *Suppose that J is a proper σ-ideal in $k[Y, 1/\det(Y)]$ generated by polynomials in $k[Y]_{\leq d}$. If $I_{F,d} \subseteq J$, then $I_{F,d} = J$.*

Proof. Since J is a σ-ideal, it is contained in some maximal proper σ-ideal. Hence there is a fundamental matrix $\bar{F}$ of (1.1) such that $\bar{F}$ is a zero of J. Suppose that $\bar{F} = Fg$ for some $g \in \mathrm{GL}_n(C)$. Define an automorphism ϕ_g of $k[Y, 1/\det(Y)]$ as follows: $\phi_g(f(Y)) = f(Yg)$ for all $f \in k[Y, 1/\det(Y)]$. Let $\bar{J} = \phi_g(J)$. One easily sees that $\bar{J}$ is still a σ-ideal in $k[Y, 1/\det(Y)]$ generated by polynomials in $k[Y]_{\leq d}$. Furthermore, F is a zero of $\bar{J}$. Hence by the definition of $I_{F,d}$, one has

$$\phi_g(J) = \bar{J} \subseteq I_{F,d} \subseteq J.$$

Successive application of ϕ_g^{-1} to J yields the following sequence:

$$J \subseteq \phi_g^{-1}(J) \subseteq \phi_g^{-2}(J) \subseteq \cdots.$$

The Noetherian property of $k[Y, 1/\det(Y)]$ implies that there is some integer l such that $\phi_g^{-l}(J) = \phi_g^{-l+1}(J)$. As ϕ_g^{-1} is an automorphism, $J = \phi_g(J)$. So $J = I_{F,d}$. □

Corollary 3.6. *Suppose that $\bar{F}$ is a fundamental matrix of (1.1). If $\bar{F}$ is a zero of $I_{F,d}$, then $I_{F,d} = I_{\bar{F},d}$.*

Proof. From the assumption, one has that $I_{F,d} \subseteq I_{\bar{F},d}$. Then the corollary follows from Proposition 3.5, because $I_{\bar{F},d}$ is a proper σ-ideal generated by polynomials in $k[Y]_{\leq d}$. □

Note that $I_{F,d}$ is contained in the maximal σ-ideal I_F. Proposition 2.9 states that $\mathrm{Zero}(I_F)$ is a trivial k-torsor, i.e., $\mathrm{Zero}(I_F) \cap \mathrm{GL}_n(k) \neq \emptyset$. We shall show that the same property holds for $I_{F,d}$. For short, we denote by $H_{F,d}$ the stabilizer of $I_{F,d}$. The ideal $I_{F,d}$ is generated by polynomials in $k[Y]_{\leq d}$. Using linear algebra, one has that $H_{F,d}$ is bounded by d, i.e., there is a set $\mathbb{S}$ of polynomials in $C[Y]_{\leq d}$ such that $H_{F,d} = \mathrm{Zero}(\mathbb{S}) \cap \mathrm{GL}_n(C)$. Precisely, let $\bar{I} = I_{F,d} \cap k[Y]_{\leq d}$. Then $\bar{I}$ is a k-vector space of finite dimension and $I_{F,d}$ is generated by $\bar{I}$. Let $P_1, \cdots, P_m$ be a basis of $\bar{I}$ and $u_1, u_2, \cdots, u_l$ be monomials in Y such that $\{P_1, \cdots, P_m, u_1, \cdots, u_l\}$ is a basis of $k[Y]_{\leq d}$. Then for $g \in \mathrm{GL}_n(C)$, $g \in H_{F,d}$ if and only if the coefficient of u_j in $P_i(Yg)$ is zero for all $1 \leq i \leq m, 1 \leq j \leq l$. Now suppose that g is an $n \times n$ matrix with indeterminate entries. Let $c_{i,j}$ be the coefficient of u_j in $P_i(Yg)$ where $i = 1, \cdots, m, j = 1, \cdots, l$. For all i, j, write $c_{i,j} = \frac{1}{a_{i,j}} \sum_{s=0}^{e_{i,j}} c_{i,j,s} x^s$, where $a_{i,j} \in C[x]$ and $c_{i,j,s} \in C[g]$. One easily sees that $c_{i,j,s}$ is of degree not greater than d and the set $\{c_{i,j,s}|i = 1, \cdots, m, j = 1, \cdots, l, s = 0, \cdots, e_{i,j}\}$ defines $H_{F,d}$.

Proposition 3.7. $\mathrm{Zero}(I_{F,d})$ *is a trivial* k*-torsor for* $H_{F,d}(\bar{k})$*, i.e.,* $\mathrm{Zero}(I_{F,d}) = BH_{F,d}(\bar{k})$ *for any* $B \in \mathrm{Zero}(I_{F,d}) \cap \mathrm{GL}_n(k)$.

Proof. Let B be an element of $\mathrm{Zero}(I_F) \cap \mathrm{GL}_n(k)$. Since $I_{F,d} \subseteq I_F$, $B \in \mathrm{Zero}(I_{F,d})$. It suffices to show that $\mathrm{Zero}(I_{F,d}) = BH_{F,d}(\bar{k})$. Let J be the ideal in $k[Y, 1/\det(Y)]$ generated by

$$\left\{Q(B^{-1}Y) \mid Q \in \mathbf{I}_C(H_{F,d}) \cap C[Y]_{\leq d}\right\}.$$

Because $H_{F,d}$ is bounded by d, one has that $\mathrm{Zero}(J) = BH_{F,d}(\bar{k})$. We shall show that $J = I_{F,d}$. Let $G = \mathrm{stab}(I_F)$. For any $g \in G$ and $P \in I_{F,d} \cap k[Y]_{\leq d}$, $P(Yg) \in k[Y]_{\leq d}$ and then it belongs to $k[Y]_{\leq d} \cap I_F$ which is a subset of $I_{F,d}$. Hence $g \in H_{F,d}$. Consequently, $G \subseteq H_{F,d}$. Due to Proposition 2.9, $\mathrm{Zero}(I_F) = BG(\bar{k})$. Therefore $\mathrm{Zero}(I_F) \subseteq \mathrm{Zero}(J)$. As I_F is radial, $J \subseteq I_F$. This implies that F is a zero of J. By the definition of $I_{F,d}$, $J \subseteq I_{F,d}$. It remains to show that $I_{F,d} \subseteq J$. Suppose that P is an element of $k[Y]_{\leq d} \cap I_{F,d}$. Then for each $h \in H_{F,d}$, $P(Yh) \in I_{F,d}$ and therefore $P(Bh) = 0$. Write

$$P(BY) = \sum_{i=1}^{l} c_i P_i(Y),$$

where $P_i(Y) \in C[Y]$ and $c_1, \cdots, c_l$ are linearly independent over C. Obviously, for all i with $1 \leq i \leq l$, the degree of $P_i(Y)$ is not greater than d and $P_i(h) = 0$ for all $h \in H_{F,d}$. In other words, $P_i(Y) \in \mathbf{I}_C(H_{F,d}) \cap C[Y]_{\leq d}$ for all $i = 1, \cdots, l$. Hence $P \in J$ and then $I_{F,d} \subseteq J$. □

Remark 3.8. As an algebraic subgroup of $\mathrm{GL}_n(\bar{k})$, the irreducible components of $H_{F,d}(\bar{k})$ are equidimensional. Hence $\sqrt{I_{F,d}}$ is an unmixed ideal.

Corollary 3.9. *Let* I_{irr} *be an associated prime of* $\sqrt{I_{F,d}}$*. Then* $\mathrm{stab}(I_{\mathrm{irr}}) = H^{\circ}_{F,d}$*. Moreover* $\mathrm{Zero}(I_{\mathrm{irr}})$ *is a trivial* k*-torsor for* $H^{\circ}_{F,d}(\bar{k})$.

Proof. Let B be an element of $\mathrm{Zero}(I_{\mathrm{irr}}) \cap \mathrm{GL}_n(k)$. By Proposition 3.7,

$$\mathrm{Zero}(I_{\mathrm{irr}}) = BH_i(\bar{k}),$$

where H_i is an irreducible component of $H_{F,d}$. Since $B \in \mathrm{Zero}(I_{\mathrm{irr}})$, $H_i = H^{\circ}_{F,d}$. Thus $\mathrm{Zero}(I_{\mathrm{irr}})$ is a trivial k-torsor for $H^{\circ}_{F,d}(\bar{k})$. It remains to show that $\mathrm{stab}(I_{\mathrm{irr}}) = H^{\circ}_{F,d}$. Suppose that $h \in \mathrm{stab}(I_{\mathrm{irr}})$. Then $P(Yh) \in I_{\mathrm{irr}}$ for any $P(Y) \in I_{\mathrm{irr}}$. Hence $P(Bh) = 0$ for any $P(Y) \in I_{\mathrm{irr}}$, i.e., $Bh \in \mathrm{Zero}(I_{\mathrm{irr}})$. Therefore $h \in H^{\circ}_{F,d}$. Conversely, suppose that $h \in H^{\circ}_{F,d}$. Then $BH^{\circ}_{F,d}(\bar{k})h = BH^{\circ}_{F,d}(\bar{k})$. This implies that for any $P(Y) \in I_{\mathrm{irr}}$ and $Z \in \mathrm{Zero}(I_{\mathrm{irr}})$, $P(Zh) = 0$. As I_{irr} is prime, $P(Yh) \in I_{\mathrm{irr}}$ for any $P(Y) \in I_{\mathrm{irr}}$. Hence $h \in \mathrm{stab}(I_{\mathrm{irr}})$. □

Proposition 3.10. $H_{F,\tilde{d}}$ *is a proto-group of* $\mathrm{stab}(I)$*, where* I *is any maximal* σ*-ideal containing* $I_{F,\tilde{d}}$*. Furthermore,* $I_{F,\tilde{d}}$ *is proto-maximal.*

Proof. Let $G = \mathrm{stab}(I)$ and H be an algebraic subgroup of $\mathrm{GL}_n(C)$ that is bounded by $\tilde{d}$ and is a proto-group of G. Such H exists by Proposition 2.5. Observe that there is a fundamental matrix $\bar{F}$ such that $I = I_{\bar{F}}$. Since $\bar{F}$ is a zero of I and thus a zero of $I_{F,\tilde{d}}$ too, we have that $I_{\bar{F},\tilde{d}} = I_{F,\tilde{d}}$ due to Corollary 3.6. Let B be an element of $\mathrm{Zero}(I) \cap \mathrm{GL}_n(k)$ and set

$$J = \left\{Q(B^{-1}Y) \mid Q \in \mathbf{I}_C(H) \cap C[Y]_{\leq \tilde{d}}\right\}.$$

Since H is bounded by $\tilde{d}$, i.e., there is a set $\mathbb{S}$ of polynomials in $\mathbf{I}_C(H) \cap C[Y]_{\leq \tilde{d}}$ such that $\mathrm{Zero}(\mathbb{S}) = H(\bar{k})$, $\mathrm{Zero}(J) = BH(\bar{k})$. By Proposition 2.9, $\mathrm{Zero}(I) = BG(\bar{k})$. Therefore $J \subseteq I$, because I is radical and H is a proto-group of G. One then has that $\bar{F}$ is a zero of J. This implies that

$$J \subseteq I_{\bar{F},\tilde{d}} = I_{F,\tilde{d}} \subseteq I.$$

The first inclusion holds because J is generated by a set of polynomials in $k[Y]_{\leq \tilde{d}}$. Proposition 3.7 implies that

$$G \leq H_{F,\tilde{d}} \leq H.$$

Then the first assertion of the proposition follows from Remark 2.3, and the second assertion follows from Proposition 3.7 and the first assertion. □

Example 3.11. Consider

$$\sigma \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ x & 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}. \tag{3.4}$$

Using the method developed in section 3.1, we can compute a σ-ideal

$$\begin{aligned} I_{\mathbf{Z},2} = \langle & y_{1,1}y_{1,2}, y_{1,1}y_{1,3}, y_{1,1}y_{2,1}, y_{1,1}y_{2,3}, y_{1,1}y_{3,1}, y_{1,1}y_{3,2}, y_{1,2}y_{1,3}, y_{1,2}y_{2,1}, y_{1,2}y_{2,2}, \\ & y_{1,2}y_{3,2}, y_{1,2}y_{3,3}, y_{1,3}y_{2,2}, y_{1,3}y_{2,3}, y_{1,3}y_{3,1}, y_{1,3}y_{3,3}, y_{2,1}y_{2,2}, y_{2,1}y_{2,3}, y_{2,1}y_{3,1}, \\ & y_{2,1}y_{3,3}, y_{2,2}y_{2,3}, y_{2,2}y_{3,1}, y_{2,2}y_{3,2}, y_{2,3}y_{3,2}, y_{2,3}y_{3,3}, y_{3,1}y_{3,2}, y_{3,1}y_{3,3}, y_{3,2}y_{3,3} \rangle. \end{aligned}$$

Furthermore, one has that

$$\begin{aligned} \mathrm{stab}(I_{\mathbf{Z},2}) = & \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \, \alpha\beta\gamma \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & \alpha & 0 \\ 0 & 0 & \beta \\ \gamma & 0 & 0 \end{pmatrix} \middle| \, \alpha\beta\gamma \neq 0 \right\} \\ & \cup \left\{ \begin{pmatrix} 0 & 0 & \alpha \\ \beta & 0 & 0 \\ 0 & \gamma & 0 \end{pmatrix} \middle| \, \alpha\beta\gamma \neq 0 \right\}. \end{aligned}$$

Since $\mathrm{stab}(I_{\mathbf{Z},2})^\circ$ is a torus, $\mathrm{stab}(I_{\mathbf{Z},2})$ is a proto-Galois group of (1.1) over k. Moreover, $\mathrm{Zero}(I_{\mathbf{Z},2}) = \mathrm{stab}(I_{\mathbf{Z},2})(\bar{k})$, i.e., $I_{\mathbf{Z},2}$ is a trivial k-torsor. So $I_{\mathbf{Z},2}$ is a proto-maximal σ-ideal. This example will be continued in Example 4.7.

4. The computation of maximal σ^δ-ideals

The results in the previous section enable us to calculate a proto-maximal σ-ideal. Suppose that we have obtained a proto-maximal σ-ideal, say $I_{F,\tilde{d}}$. Let I_{irr} be an associated prime of $\sqrt{I_{F,\tilde{d}}}$. It can be obtained with an algorithmic solution of problem (P2). Since $I_{F,\tilde{d}}$ is a σ-ideal and so is its radical, I_{irr} is a σ^δ-ideal for some positive integer δ. In the following, we will enlarge I_{irr} to obtain a maximal σ^δ-ideal. By Corollary 3.9, one sees that for any $B \in \mathrm{Zero}(I_{\mathrm{irr}}) \cap \mathrm{GL}_n(k)$,

$$\mathrm{Zero}(I_{\mathrm{irr}}) = BH^\circ_{F,\tilde{d}}(\bar{k}) \text{ and } \mathrm{stab}(I_{\mathrm{irr}}) = H^\circ_{F,\tilde{d}}. \tag{4.1}$$

Let I_δ be a maximal σ^δ-ideal that contains I_{irr} and $G_\delta = \mathrm{stab}(I_\delta)$. Obverse that Proposition 2.9 still holds for maximal σ^δ-ideals. This implies that $\mathrm{Zero}(I_\delta) = BG_\delta(\bar{k})$ for any $B \in \mathrm{Zero}(I_\delta) \cap \mathrm{GL}_n(k)$. Then equation (4.1) implies that $G_\delta \subseteq H^\circ_{F,\tilde{d}}$. We shall show that $H^\circ_{F,\tilde{d}}$ is a proto-group of G_δ.

Lemma 4.1. *Let $\tilde{I}$ be a maximal σ^δ-ideal and $I = \tilde{I} \cap \sigma(\tilde{I}) \cap \cdots \cap \sigma^{\delta-1}(\tilde{I})$. Then*

(a) *I is a maximal σ-ideal, and*

(b) $[\mathrm{stab}(I) : \mathrm{stab}(\tilde{I})] \leq \delta$.

Proof. (a) Suppose that $\bar{I}$ is a maximal σ-ideal containing I. We claim that $\bar{I} \subseteq \tilde{I}$. Suppose on the contrary that $\bar{I} \setminus \tilde{I} \neq \emptyset$. Then $\bar{I} \setminus \sigma^i(\tilde{I}) \neq \emptyset$ for all $1 \leq i \leq \delta - 1$, since σ is an isomorphism and $\bar{I}$ is a σ-ideal. Observe that $\sigma^i(\tilde{I})$ is σ^δ-maximal for all $0 \leq i \leq \delta - 1$. Therefore $\bar{I} + \sigma^i(\tilde{I}) = k[Y, 1/\det(Y)]$ for all $0 \leq i \leq \delta - 1$. In other words, there are $a_i \in \bar{I}, b_i \in \sigma^i(\tilde{I})$ such that $a_i + b_i = 1$ for all $0 \leq i \leq \delta - 1$. One then has that

$$1 = \prod_{i=0}^{\delta-1}(a_i + b_i) = \prod_{i=0}^{\delta-1} b_i + \bar{a}$$

where $\bar{a} \in \bar{I}$. From the assumption, $\prod_{i=0}^{\delta-1} b_i \in I$ which is a subset of $\bar{I}$. Hence $1 \in \bar{I}$, a contradiction. This proves the claim. The claim implies that $\bar{I} \subseteq \sigma^i(\tilde{I})$ for all $0 \leq i \leq \delta - 1$. Consequently, $\bar{I} \subseteq I$. Therefore $I = \bar{I}$, which is a maximal σ-ideal.

(b) Let $G = \mathrm{stab}(I)$ and $\tilde{G} = \mathrm{stab}(\tilde{I})$. Let B be an element of $\mathrm{Zero}(\tilde{I}) \cap \mathrm{GL}_n(k)$. Due to Proposition 2.9, one has that

$$\mathrm{Zero}(I) = BG(\bar{k}) \text{ and } \mathrm{Zero}(\tilde{I}) = B\tilde{G}(\bar{k}). \tag{4.2}$$

It is easy to see that $\sigma^i(\tilde{I})$ is a maximal σ^δ-ideal for all $0 \leq i \leq \delta - 1$. Hence there are $g_1, \cdots, g_{\delta-1} \in \mathrm{GL}_n(C)$ such that $\phi_{g_i}(\sigma^i(\tilde{I})) = \tilde{I}$, where ϕ_{g_i} is an isomorphism of $k[Y, 1/\det(Y)]$ given by $\phi_{g_i}(Y) = Yg_i$. This implies that

$$\mathrm{Zero}(\sigma^i(\tilde{I})) = B\tilde{G}(\bar{k})g_i, \ i = 0, 1, \cdots, \delta - 1. \tag{4.3}$$

Equations (4.2) and (4.3) imply that $G = \bigcup_{i=0}^{\delta-1} \tilde{G}g_i$. In what follows, $[G : \tilde{G}] \leq \delta$. □

Let $I = I_\delta \cap \sigma(I_\delta) \cap \cdots \cap \sigma^{\delta-1}(I_\delta)$. Then $I_{F,\tilde{d}} \subseteq I$. The above lemma together with Proposition 3.10 implies that $H_{F,\tilde{d}}$ is a proto-group of $\mathrm{stab}(I)$, i.e.,

$$\left(H_{F,\tilde{d}}\right)_u \leq (\mathrm{stab}(I))^\circ \leq \mathrm{stab}(I) \leq H_{F,\tilde{d}}.$$

Observe that $\left(H_{F,\tilde{d}}\right)_u = \left(H^\circ_{F,\tilde{d}}\right)_u$. Due to the above lemma again, $(\mathrm{stab}(I))^\circ = G^\circ_\delta$. Thus

$$\left(H^\circ_{F,\tilde{d}}\right)_u \leq G^\circ_\delta \leq G_\delta \leq H^\circ_{F,\tilde{d}},$$

i.e., $H^\circ_{F,\tilde{d}}$ is a proto-group of G_δ. Proposition 2.6 then implies that G_δ is the intersection of the kernels of some characters of $H^\circ_{F,\tilde{d}}$. Suppose that $\bar{\chi}_1, \cdots, \bar{\chi}_l$ are characters of $H^\circ_{F,\tilde{d}}$ such that

$$\ker(\bar{\chi}_1) \cap \cdots \cap \ker(\bar{\chi}_l) = G_\delta.$$

Then we have the following lemma.

Lemma 4.2. *Let B be an element of $\mathrm{Zero}(I_\delta) \cap \mathrm{GL}_n(k)$ and set*

$$\mathbb{S} = I_{\mathrm{irr}} \cup \{\bar{\chi}_i(B^{-1}Y) - 1 \mid i = 1, \cdots, l\}.$$

Then $\mathrm{Zero}(I_\delta) = \mathrm{Zero}(\mathbb{S})$.

Proof. It suffices to show that $\mathrm{Zero}(\mathbb{S}) = BG_\delta(\bar{k})$. From (4.1), one has that $\mathrm{Zero}(I_{\mathrm{irr}}) = BH^\circ_{F,\tilde{d}}(\bar{k})$ because $B \in \mathrm{Zero}(I_{\mathrm{irr}}) \cap \mathrm{GL}_n(k)$. Suppose that $Z \in BG_\delta(\bar{k})$. As G_δ is the intersection of the kernels of the characters $\bar{\chi}_1, \cdots, \bar{\chi}_l$, one sees that $Z \in \mathrm{Zero}(\mathbb{S})$. Conversely, assume that $Z \in \mathrm{Zero}(\mathbb{S})$. Then $Z \in \mathrm{Zero}(I_{\mathrm{irr}})$ and thus $Z = Bh$ for some $h \in H^\circ_{F,\tilde{d}}(\bar{k})$. Meanwhile for each $i = 1, \cdots, l$,

$$\bar{\chi}_i(B^{-1}Z) = \bar{\chi}_i(h) = 1.$$

This implies that $h \in G_\delta(\bar{k})$. Therefore $\mathrm{Zero}(\mathbb{S}) = BG_\delta(\bar{k})$. □

Lemma 2.12 states that $\bar{\chi}_i(B^{-1}Y)$ is invertible in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$. This together with the above lemma implies that for computing I_δ, it suffices to find suitable invertible elements of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$. In the following, we first prove that invertible elements of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ are actually σ^δ-hypergeometric over k and then show that algebraic relations among σ^δ-hypergeometric elements enable us to find I_δ. We start with a definition.

Definition 4.3. A nonzero element P of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ is said to be σ^δ-hypergeometric over k if P is invertible in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ and $\sigma^\delta(P) = rP$ for some $r \in k$. Suppose that P_1, P_2 are two σ^δ-hypergeometric elements over k of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$. We say P_1 and P_2 are *similar* if there is $r \in k$ such that $P_1 = rP_2$.

Elements of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ are represented by elements of $k[Y, 1/\det(Y)]$. Let P be an element of $k[Y, 1/\det(Y)]$. The image of P in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ is σ^δ-hypergeometric over k if and only if

$$\mathrm{Zero}(P) \cap \mathrm{Zero}(I_{\mathrm{irr}}) = \emptyset \text{ and } \sigma^\delta(P) - rP \in I_{\mathrm{irr}}$$

for some $r \in k$.

Proposition 4.4. *Let B be an element of $\mathrm{Zero}(I_{\mathrm{irr}}) \cap \mathrm{GL}_n(k)$ and χ a character of $H^\circ_{F,d}$ that is represented by an element of $C[Y, 1/\det(Y)]$. Then $\chi(B^{-1}Y)$ is a σ^δ-hypergeometric element over k of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$. Furthermore, if χ_1 and χ_2 are two distinct characters, then $\chi_1(B^{-1}Y)$ and $\chi_2(B^{-1}Y)$ are not similar.*

Proof. Obviously, $\chi(B^{-1}Y)$ is invertible in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$. It remains to show that $\sigma^\delta(\chi(B^{-1}Y)) - r\chi(B^{-1}Y) \in I_{\mathrm{irr}}$ for some $r \in k$. We first claim that

$$\sigma^\delta(B^{-1})A_\delta B \in H^\circ_{F,\tilde{d}}(k),$$

where $A_\delta = \sigma^{\delta-1}(A)\sigma^{\delta-2}(A)\cdots\sigma(A)A$. For any $Q \in \mathbf{I}_C(H^\circ_{F,\tilde{d}})$, it follows from (4.1) that $Q(B^{-1}Y) \in I_{\mathrm{irr}}$. As I_{irr} is a σ^δ-ideal, one has $Q(\sigma^\delta(B^{-1})A_\delta Y) \in I_{\mathrm{irr}}$. Since $B \in \mathrm{Zero}(I_{\mathrm{irr}})$, $Q(\sigma^\delta(B^{-1})A_\delta B) = 0$. This proves the claim. Now for any $h \in H^\circ_{F,\tilde{d}}(\bar{k})$,

$$\chi(\sigma^\delta(B^{-1})A_\delta Bh) - \chi(\sigma^\delta(B^{-1})A_\delta B)\chi(B^{-1}Bh) = 0.$$

This implies that

$$\chi(\sigma^\delta(B^{-1})A_\delta Y) - \chi(\sigma^\delta(B^{-1})A_\delta B)\chi(B^{-1}Y) \in I_{\mathrm{irr}}.$$

In other words,

$$\sigma^\delta(\chi(B^{-1}Y)) - \chi(\sigma^\delta(B^{-1})A_\delta B)\chi(B^{-1}Y) \in I_{\mathrm{irr}},$$

i.e., $\chi(B^{-1}Y)$ is a σ^δ-hypergeometric element over k of $k[Y, 1/\det(Y)]/I_{\text{irr}}$. This proves the first assertion.

Now assume that $\chi_1(B^{-1}Y) - r\chi_2(B^{-1}Y) \in I_{\text{irr}}$ for some $r \in k$. Then for any $h \in H^\circ_{F,\tilde{d}}$,

$$\chi_1(h) = \chi_1(B^{-1}Bh) = r\chi_2(B^{-1}Bh) = r\chi_2(h).$$

Particularly, putting $h = I_n$, one then has that $r = 1$. Thus $\chi_1 = \chi_2$, a contradiction. □

Let κ_2 be a bound as given in (2.1). Proposition B.17 of [9] states that $X(H^\circ_{F,\tilde{d}})$ has generators that are represented by polynomials in $C[Y]_{\le\kappa_2}$. In the following, we show how to obtain such generators from a set of σ^δ-hypergeometric elements over k in $k[Y, 1/\det(Y)]/I_{\text{irr}}$. Denote

$$\mathcal{H} = \left\{ P \in k[Y]_{\le\kappa_2} \;\middle|\; \begin{array}{c} P \text{ is } \sigma^\delta\text{-hypergeometric over } k \text{ in } k[Y, 1/\det(Y)]/I_{\text{irr}}, \\ P - rQ \notin I_{\text{irr}}, \forall\, r \in k,\ \forall\, Q \in \mathcal{H} \setminus \{P\} \end{array} \right\}.$$

Note that $\mathcal{H}$ contains all σ^δ-hypergeometric elements over k in $k[Y, 1/\det(Y)]/I_{\text{irr}}$ that are not pairwise similar and are presented by polynomials in $k[Y]$ with degree not greater than κ_2. It follows from Lemma 2.12 that one can construct characters of $H^\circ_{F,\tilde{d}}$ from elements of $\mathcal{H}$. Precisely, let $B \in \text{Zero}(I_{\text{irr}}) \cap \text{GL}_n(k)$ and define a map τ_B from $\mathcal{H}$ to $X(H^\circ_{F,\tilde{d}})$ as follows:

$$\begin{aligned} \tau_B : \mathcal{H} &\longrightarrow X(H^\circ_{F,\tilde{d}}) \\ P &\longrightarrow \chi, \end{aligned} \tag{4.4}$$

where χ satisfies that $P - r\chi(B^{-1}Y) \in I_{\text{irr}}$. By Lemma 2.12, for each $P \in \mathcal{H}$, there is a character χ such that $\tau_B(P) = \chi$, and such a character is unique by Proposition 4.4. Therefore τ_B is well-defined. Now suppose that χ is an element of $X(H^\circ_{F,\tilde{d}})$ that is presented by a polynomial in $C[Y]_{\le\kappa_2}$. Due to Proposition 4.4 again, $\chi(B^{-1}Y)$ is a σ^δ-hypergeometric element over k in $k[Y, 1/\det(Y)]/I_{\text{irr}}$. Note that $\chi(B^{-1}Y) \in k[Y]_{\le\kappa_2}$. So there is some P in $\mathcal{H}$ which is similar to $\chi(B^{-1}Y)$. One sees easily that $\tau_B(P) = \chi$. In the sequel, $\tau_B(\mathcal{H})$ contains all elements of $X(H^\circ_{F,\tilde{d}})$ that are represented by polynomials in $C[Y]_{\le\kappa_2}$. Therefore $\tau_B(\mathcal{H})$ is the desired set of generators of $X(H^\circ_{F,\tilde{d}})$.

We can compute $\mathcal{H}$ by Algorithm B.1 in Appendix B. Suppose that we have obtained such $\mathcal{H}$ and assume that $\mathcal{H} = \{P_1, \cdots, P_\nu\}$. Let b_j be the certificate of P_j, i.e., $\sigma^\delta(P_j) - b_j P_j \in I_{\text{irr}}$ for all $1 \le j \le \nu$. Set

$$\mathcal{Z} = \left\{ (m_1, \cdots, m_\nu) \in \mathbb{Z}^\nu \;\middle|\; \exists\, f \in k^\times,\ \text{s.t. } \prod_{j=1}^{\nu} b_j^{m_j} = \frac{\sigma^\delta(f)}{f} \right\}.$$

Then $\mathcal{Z}$ is a finitely generated $\mathbb{Z}$-module. The solution of problem (P3) allows us to compute a set of generators of $\mathcal{Z}$. Assume that $\mathbf{m}_1, \cdots, \mathbf{m}_\mu$ are generators of $\mathcal{Z}$ and further suppose that

$$\prod_{j=1}^{\nu} b_j^{m_{i,j}} = \frac{\sigma^\delta(f_i)}{f_i},$$

where $f_i \in k^\times$ and $\mathbf{m}_i = (m_{i,1}, \cdots, m_{i,\mu})$. For each $i = 1, \cdots, \mu$, write $\mathbf{m}_i = \mathbf{m}_i^+ - \mathbf{m}_i^-$, where $\mathbf{m}_i^+, \mathbf{m}_i^-$ are in $\mathbb{Z}^\nu_{\ge 0}$ and $\mathbf{m}_i^+ \left(\mathbf{m}_i^-\right)^T = 0$. Denote by $\mathbf{P}$ the vector

$(P_1, \cdots, P_\mu)$ and $\mathbf{P}^{\mathbf{m}} = \prod_{j=1}^{\nu} P_j^{m_j}$, where $\mathbf{m} = (m_1, \cdots, m_\nu)$. Set

$$\mathcal{P}_{\mathbf{c}} = \left\langle I_{\mathrm{irr}} \cup \left\{ \mathbf{P}^{\mathbf{m}_i^+} - c_i f_i \mathbf{P}^{\mathbf{m}_i^-} \;\middle|\; i = 1, \cdots, \mu \right\} \right\rangle, \tag{4.5}$$

where $\mathbf{c} = (c_1, \cdots, c_\mu) \in (C^\times)^\mu$. It is easy to verify that $\mathcal{P}_{\mathbf{c}}$ is a σ^δ-ideal.

Lemma 4.5. *There exists a $\mathbf{c} = (c_1, \cdots, c_\mu) \in (C^\times)^\mu$ such that $\mathcal{P}_{\mathbf{c}}$ is a proper σ^δ-ideal of $k[Y, 1/\det(Y)]$.*

Proof. Let I_δ be a maximal σ^δ-ideal containing I_{irr} and F_δ a fundamental matrix of $\sigma^\delta(Y) = A_\delta Y$ such that F_δ is a zero of I_δ, where $A_\delta = \sigma^{\delta-1}(A)\sigma^{\delta-2}(A)\cdots A$. Then F_δ is also a zero of I_{irr}. So for all j with $1 \leq j \leq \nu$,

$$\sigma^\delta(P_j)(F_\delta) - b_j P_j(F_\delta) = \sigma^\delta(P_j(F_\delta)) - b_j P_j(F_\delta) = 0.$$

This implies that for all i with $1 \leq i \leq \mu$,

$$\sigma^\delta(\mathbf{P}^{\mathbf{m}_i}(F_\delta)) - \prod_{j=1}^{\nu} b_j^{m_{i,j}} \mathbf{P}^{\mathbf{m}_i}(F_\delta) = \sigma^\delta(\mathbf{P}^{\mathbf{m}_i}(F_\delta)) - \frac{\sigma^\delta(f_i)}{f_i} \mathbf{P}^{\mathbf{m}_i}(F_\delta) = 0.$$

Hence for each $i = 1, \cdots, \mu$, $\mathbf{P}^{\mathbf{m}_i}(F_\delta) = c_i f_i$ for some $c_i \in C^\times$. Set $\mathbf{c} = (c_1, \cdots, c_\mu)$. Then one sees that F_δ is a zero of $\mathcal{P}_{\mathbf{c}}$. Consequently, $\mathcal{P}_{\mathbf{c}}$ is proper. □

We can calculate a $\mathbf{c}$ such that $\mathcal{P}_{\mathbf{c}}$ is proper as follows: let $Q_1, \cdots, Q_l \in k[Y]$ generate the ideal I_{irr} and z a new indeterminate. Consider $c_1, \cdots, c_\mu$ as parameters and denote by $J_{\mathbf{c}}$ the ideal in $k[Y, z, c_1, \cdots, c_\mu]$ generated by

$$Q_1, \cdots, Q_l, \det(Y)z - 1, \mathbf{P}^{\mathbf{m}_1^+} - c_1 f_1 \mathbf{P}^{\mathbf{m}_1^-}, \cdots, \mathbf{P}^{\mathbf{m}_\mu^+} - c_\mu f_\mu \mathbf{P}^{\mathbf{m}_\mu^-}.$$

Then algorithms for comprehensive Gröbner systems allow us to find a suitable $\mathbf{c} \in (C^\times)^\mu$ such that $J_{\mathbf{c}}$ is a proper ideal. The reader is referred to [15, 21, 30, 32] and the references cited therein for the algorithms.

Proposition 4.6. *Assume that $\mathcal{P}_{\mathbf{c}}$ is proper and I_δ is a maximal σ^δ-ideal containing $\mathcal{P}_{\mathbf{c}}$. Then*

$$\mathrm{Zero}(\mathcal{P}_{\mathbf{c}}) = \mathrm{Zero}(I_\delta), \quad \textit{i.e.}, \; I_\delta = \sqrt{\mathcal{P}_{\mathbf{c}}}.$$

Proof. Let B be an element of $\mathrm{Zero}(I_\delta) \cap \mathrm{GL}_n(k)$ and $G_\delta = \mathrm{stab}(I_\delta)$. Due to Proposition 2.9,

$$\mathrm{Zero}(I_\delta) = BG_\delta(\bar{k}).$$

Obviously, I_δ is a maximal σ^δ-ideal containing I_{irr}. The discussion after Lemma 4.1 states that $H^\circ_{F,\tilde{d}}$ is a proto-group of G_δ. By Proposition 2.6, G_δ is the intersection of the kernels of some characters of $H^\circ_{F,\tilde{d}}$. Let Λ be the set of these characters. Note that $\tau_B(\mathcal{H})$ is a set of generators of $X(H^\circ_{F,\tilde{d}})$ where τ_B is defined as in (4.4). Suppose that $\bar{\chi} \in \Lambda$. Then

$$\bar{\chi} = \prod_{i=1}^{\nu} \tau_B(P_i)^{\alpha_i}, \tag{4.6}$$

where $\alpha_i \in \mathbb{Z}$. From the definition of the map τ_B, for each $i = 1, \cdots, \nu$, there is $r_i \in k^\times$ such that

$$P_i(Y) - r_i \tau_B(P_i)(B^{-1}Y) \in I_{\mathrm{irr}}. \tag{4.7}$$

Lemma 4.2 implies that $\bar{\chi}(B^{-1}Y) - 1 \in I_\delta$. Denote by $\bar{Y}$ the image of Y in $k[Y, 1/\det(Y)]/I_\delta$. Then $\bar{\chi}(B^{-1}\bar{Y}) - 1 = 0$. This together with (4.6) and (4.7) implies that

$$\prod_{i=1}^{\nu} \tau_B(P_i)^{\alpha_i}(B^{-1}\bar{Y}) - 1 = \prod_{i=1}^{\nu} r_i^{-\alpha_i} P_i^{\alpha_i}(\bar{Y}) - 1 = 0. \tag{4.8}$$

Applying σ^δ to (4.8), one has that

$$\prod_{i=1}^{\nu} \sigma^\delta\left(r_i^{-\alpha_i}\right) b_i^{\alpha_i} P_i^{\alpha_i}(\bar{Y}) - 1 = 0. \tag{4.9}$$

Combining (4.8) and (4.9), one has that

$$\prod_{i=1}^{\nu} b_i^{\alpha_i} = \prod_{i=1}^{\nu} \frac{\sigma^\delta\left(r_i^{\alpha_i}\right)}{r_i^{\alpha_i}}.$$

Set $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_\nu) \in \mathbb{Z}^\nu$. Then $\boldsymbol{\alpha} \in \mathcal{Z}$. So there are integers $z_1, \cdots, z_\mu$ such that $\boldsymbol{\alpha} = z_1\mathbf{m}_1 + \cdots + z_\mu\mathbf{m}_\mu$.

Let Z be an element of $\mathrm{Zero}(\mathcal{P}_\mathbf{c})$. Then one has that $\mathbf{P}^{\mathbf{m}_j}(Z) = c_j f_j$ for all $1 \le j \le \mu$, because $\mathbf{P}^{\mathbf{m}_j}(Z) \neq 0$. By (4.6) and (4.7) again,

$$\begin{aligned}\bar{\chi}(B^{-1}Z) - 1 &= \prod_{i=1}^{\nu} \tau_B(P_i)^{\alpha_i}(B^{-1}Z) - 1 = \mathbf{P}^{\boldsymbol{\alpha}}(Z) \prod_{i=1}^{\nu} r_i^{-\alpha_i} - 1 \\ &= \prod_{j=1}^{\mu} \mathbf{P}^{z_j\mathbf{m}_j}(Z) \prod_{i=1}^{\nu} r_i^{-\alpha_i} - 1 = \prod_{j=1}^{\mu} (c_j f_j)^{z_j} \prod_{i=1}^{\nu} r_i^{-\alpha_i} - 1.\end{aligned}$$

This implies that the polynomial $\bar{\chi}(B^{-1}Y) - 1$ takes a constant value on $\mathrm{Zero}(\mathcal{P}_\mathbf{c})$. Particularly, putting $Z = B$, one has that $\bar{\chi}(B^{-1}B) - 1 = \prod_{j=1}^{\mu}(c_j f_j)^{z_j} \prod_{i=1}^{\nu} r_i^{-\alpha_i} - 1 = 0$. In the sequel, $\bar{\chi}(B^{-1}Z) - 1 = 0$ for all $Z \in \mathrm{Zero}(\mathcal{P}_\mathbf{c})$. Therefore

$$\mathrm{Zero}(\mathcal{P}_\mathbf{c}) \subseteq \mathrm{Zero}(I_{\mathrm{irr}} \cup \{\bar{\chi}(B^{-1}Y) - 1 \mid \bar{\chi} \in \Lambda\}).$$

The former set contains $\mathrm{Zero}(I_\delta)$ and the latter one is equal to $\mathrm{Zero}(I_\delta)$ by Lemma 4.2. Consequently, $\mathrm{Zero}(\mathcal{P}_\mathbf{c}) = \mathrm{Zero}(I_\delta)$. □

Suppose that a proper $\mathcal{P}_\mathbf{c}$ has been calculated. One can then compute $\sqrt{\mathcal{P}_\mathbf{c}}$ with an algorithmic solution of problem (P2) and $I = \sqrt{\mathcal{P}_\mathbf{c}} \cap \sigma(\sqrt{\mathcal{P}_\mathbf{c}}) \cap \cdots \cap \sigma^{\delta-1}(\sqrt{\mathcal{P}_\mathbf{c}})$ with the algorithm presented in (section 6.3, page 260 of [1]). Then the ideal I is a maximal σ-ideal by Lemma 4.1.

Example 4.7. (Example 3.11 continued) $I_{\mathbf{Z},2}$ is radical and we have the following irreducible decomposition:

$$\begin{aligned}I_{\mathbf{Z},2} =& \langle y_{1,1}, y_{1,2}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,3}\rangle \cap \langle y_{1,1}, y_{1,3}, y_{2,1}, y_{2,2}, y_{3,2}, y_{3,3}\rangle \\ & \cap \langle y_{1,2}, y_{1,3}, y_{2,1}, y_{2,3}, y_{3,1}, y_{3,2}\rangle.\end{aligned}$$

Set $I_{\mathrm{irr}} = \langle y_{1,1}, y_{1,2}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,3}\rangle$. Then one can easily verify that I_{irr} is a σ^3-ideal and

$$\mathrm{stab}(I_{\mathrm{irr}}) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \, \alpha\beta\gamma \neq 0 \right\}.$$

$X(\mathrm{stab}(I_{\mathrm{irr}}))$ is generated by $y_{1,1}, y_{2,2}, y_{3,3}$. Thus we only need to compute σ^3-hypergeometric elements in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ which are represented by linear

polynomials in $k[Y]$. By Algorithm B.1, we can see that $y_{1,3}, y_{2,1}, y_{3,2}$ are σ^3-hypergeometric elements of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ and further they are not pairwise similar. More precisely,

$$\sigma^3(y_{1,3}) = (x+2)y_{1,3},\ \sigma^3(y_{2,1}) = xy_{2,1}\ \sigma^3(y_{3,2}) = (x+1)y_{3,2}.$$

An easy calculation yields that $(0,0,0)$ is the only element (m_1, m_2, m_3) in $\mathbb{Z}^3$ such that

$$x^{m_1}(x+1)^{m_2}(x+2)^{m_3} = \sigma^3(f)/f$$

for some $f \in k$. When $m_1 = m_2 = m_3 = 0$, we can take $f = 1$ and then Proposition 4.6 implies that I_{irr} is a maximal σ^3-ideal. Let

$$I = I_{\mathrm{irr}} \cap \sigma(I_{\mathrm{irr}}) \cap \sigma^2(I_{\mathrm{irr}}) = I_{\mathbf{Z},2}.$$

Lemma 4.1 implies that $I_{\mathbf{Z},2}$ is a maximal σ-ideal. Thus the Galois group is $\mathrm{stab}(I_{\mathbf{Z},2})$, which has already been explicitly given in Example 3.11.

5. The algorithm and an example

We are now ready to present the algorithm for computing the Galois group $\mathrm{stab}(I)$, where I is a maximal σ-ideal of $k[Y, 1/\det(Y)]$.

Algorithm 5.1. *Input: a linear difference equation of the form* (1.1).
Output: the Galois group of (1.1) *over* k.

(i) *Compute a proto-maximal* σ*-ideal* $I_{F,\tilde{d}}$ *by Algorithm* 3.3.

(ii) *Using the algorithms for problem* (P2)*, compute an associated prime of* $\sqrt{I_{F,\tilde{d}}}$*, denoted by* I_{irr}*. Compute a positive integer* δ *such that* I_{irr} *is a* σ^δ*-ideal.*

(iii) *By Algorithm* B.1*, compute a set of* σ^δ*-hypergeometric elements over* k *in* $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$*, whose elements are represented by polynomials in* $k[Y]_{\leq \kappa_2}$*, and are not pairwise similar. Denote them by* $P_1, \cdots, P_\nu$.

(iv) *Let* b_i *be the certificates of* P_i*, i.e.,* $\sigma^\delta(P_i) - b_i P_i \in I_{\mathrm{irr}}$ *where* $b_i \in k^\times$ *and* $i = 1, \cdots, \nu$*. Using the method for problem* (P3)*, compute a set of generators of the following* $\mathbb{Z}$*-module:*

$$\mathcal{Z} = \left\{ (m_1, \cdots, m_\nu) \in \mathbb{Z}^\nu \;\middle|\; \exists\ f \in k^\times, s.t.\ \prod_{i=1}^{\nu} b_i^{m_i} = \frac{\sigma^\delta(f)}{f} \right\}.$$

Denote those generators by $\mathbf{m}_1, \cdots, \mathbf{m}_\mu$.

(v) *Set* $\mathbf{P} = (P_1, \cdots, P_\nu)$ *and find* f_i*, the element in* $k^\times$ *such that* $\mathbf{P}^{\mathbf{m}_i} = \sigma^\delta(f_i)/f_i$*, where* $i = 1, \cdots, \nu$*. Set*

$$\mathcal{P}_{\mathbf{c}} = I_{\mathrm{irr}} \cup \left\{ \mathbf{P}^{\mathbf{m}_i^+} - c_i f_i \mathbf{P}^{\mathbf{m}_i^-} \;\middle|\; i = 1, \cdots, \mu \right\},$$

where $\mathbf{c} = (c_1, \cdots, c_\mu) \in (C^\times)^\mu$*, and* $\mathbf{m}_i^+, \mathbf{m}_i^-$ *are elements in* $\mathbb{Z}_{\geq 0}^\nu$ *satisfying* $\mathbf{m}_i^+ - \mathbf{m}_i^- = \mathbf{m}_i$ *and* $\mathbf{m}_i^+ \left(\mathbf{m}_i^-\right)^T = 0$*. By the algorithms developed in* [15, 21, 30, 32]*, compute a* $\mathbf{c} \in (C^\times)^\mu$ *such that* $\mathcal{P}_{\mathbf{c}}$ *is proper.*

(vi) *With the algorithms for problem* (P2) *and the algorithm presented in (section 6.3, page 260 of* [1]*), compute* $\sqrt{\mathcal{P}_{\mathbf{c}}}$ *and*

$$I = \sqrt{\mathcal{P}_{\mathbf{c}}} \cap \sigma\left(\sqrt{\mathcal{P}_{\mathbf{c}}}\right) \cap \cdots \cap \sigma^{\delta-1}\left(\sqrt{\mathcal{P}_{\mathbf{c}}}\right).$$

Due to Proposition 4.6, $\sqrt{\mathcal{P}_{\mathbf{c}}}$ *is a maximal* σ^{δ}*-ideal and then* I *is a maximal* σ*-ideal by Lemma* 4.1.

(vii) *Using Gröbner basis computation, compute* $\mathrm{stab}(I)$ *and then return* $\mathrm{stab}(I)$.

Correctness of the algorithm comes from the results presented in the previous sections.

Remark 5.2.

(a) One may suspect that the complexity of the algorithm would be very high, since the degree bounds $\tilde{d}$ and κ_2 given in (2.1) and (2.2) are quite large. These degree bounds guarantee the termination of the algorithm. Additionally, one needs to find a coefficient bound for generators of $I_{F,\tilde{d}}$ (see Appendix A). It seems that there does not exist a universal coefficient bound, i.e., a coefficient bound only depending on $\tilde{d}$, the order n, and the degrees of the coefficients of equations.

(b) Except for one particular case where the Galois group has a torus as its identity component, we are not able to decide whether $I_{F,d}$ is proto-maximal or not when $d < \tilde{d}$. This is why our algorithm does not begin by computing $I_{F,d}$ with $d = 1, 2, \cdots$. On the other hand, assume that the Galois group has a torus as its identity component. Then the first step of the algorithm can be improved as follows. For $d \geq 0$ and $e \geq 0$, denote by $I_{F,d,e}$ the σ-ideal generated by polynomials in

$$\{P \in C[x][Y] \,|\, P(F) = 0, \deg_x(P) \leq e, \deg_Y(P) \leq d\},$$

where $\deg_Y(P)$ stands for the total degree of P in $y_{1,1}, \cdots, y_{n,n}$. We first set $d = 1$ and $e = 0$ and compute $I_{F,d,e}$ by the method developed in section 3.1. Then decide if $I_{F,1,0}$ is proto-maximal. If $I_{F,1,0}$ is proto-maximal, then we are done. Otherwise, increase d or e and repeat the process. Note that by Remark 2.3 $\mathrm{stab}(I_{F,d,e})$ is a proto-Galois group if and only if $\mathrm{stab}(I_{F,d,e})^{\circ}$ is a torus. Using the Gröbner basis method, one can verify whether $\mathrm{stab}(I_{F,d,e})^{\circ}$ is a torus and whether $\mathrm{Zero}(I_{F,d,e})$ is a k-torsor for $\mathrm{stab}(I_{F,d,e})(\bar{k})$ once a zero of $I_{F,d,e}$ in $\mathrm{GL}_n(\bar{k})$ is computed. As $\mathrm{Zero}(I_{F,d}) \subseteq \mathrm{Zero}(I_{F,d,e})$, if $\mathrm{Zero}(I_{F,d,e})$ is a k-torsor, then it must be a trivial k-torsor. In the sequel, one can verify whether $I_{F,d,e}$ is proto-maximal.

(c) In Examples 3.11 and 5.3, since the coefficient matrices are monomial (see page 57 of [13] for the definition), the Galois groups are algebraic subgroups of the group of monomial matrices and thus their identity components are tori. Therefore, in these two examples, a small d such as 2 is large enough to obtain proto-maximal σ-ideals.

In the following, we give an example to illustrate the algorithm.

Example 5.3. Consider the following linear difference equation:

$$\sigma \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ x & 0 & 0 \\ 0 & 0 & \frac{1}{x} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}. \tag{5.1}$$

(i) Using the method developed in section 3.1, we compute an ideal $\tilde{I}$ generated by polynomials in $I_{F,2} \cap C[Y]$:

$$\tilde{I} = \langle y_{3,2}, y_{3,1}, y_{2,3}, y_{2,1}y_{2,2}, y_{1,3}, y_{1,2}y_{2,2}, y_{1,1}y_{2,1}, y_{1,1}y_{1,2} \rangle.$$

$\tilde{I}$ is a σ-ideal and

$$\mathrm{stab}(\tilde{I}) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \, \alpha\beta\gamma \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & \alpha & 0 \\ \beta & 0 & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \, \alpha\beta\gamma \neq 0 \right\}.$$

As $\mathrm{stab}(\tilde{I})^\circ$ is a torus, $\mathrm{stab}(\tilde{I})$ is a proto-Galois group of (5.1) over k. Furthermore, it is easy to verify that $\mathrm{Zero}(\tilde{I})$ is a trivial k-torsor. Thus $\tilde{I}$ is a proto-maximal σ-ideal.

(ii) $\tilde{I}$ is radical and one can compute its irreducible decomposition as follows:

$$\tilde{I} = \langle y_{1,1}, y_{1,3}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,2} \rangle \cap \langle y_{1,2}, y_{1,3}, y_{2,1}, y_{2,3}, y_{3,1}, y_{3,2} \rangle.$$

Set $I_{\mathrm{irr}} = \langle y_{1,1}, y_{1,3}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,2} \rangle$. Then I_{irr} is a σ^2-ideal and

$$\mathrm{stab}(I_{\mathrm{irr}}) = \{\mathrm{diag}(\alpha, \beta, \gamma) | \alpha\beta\gamma \neq 0\}.$$

(iii) Observe that the group of characters of $\mathrm{stab}(I_{\mathrm{irr}})$ is generated by linear polynomials. Using Algorithm B.1, we can find that σ^2-hypergeometric elements of $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ that are represented by linear polynomials in $k[Y]$ are $y_{1,2}, y_{2,1}, y_{3,3}$. Precisely,

$$\sigma^2(y_{1,2}) = x y_{1,2},\ \sigma^2(y_{2,1}) = (x+1) y_{2,1},\ \sigma^2(y_{3,3}) = \frac{1}{x(x+1)} y_{3,3}.$$

(iv) Set

$$\mathcal{Z} = \left\{ (m_1, m_2, m_3) \in \mathbb{Z}^3 \ \middle| \ \exists\, f \in k^\times, \text{s.t. } x^{m_1}(x+1)^{m_2} \left(\frac{1}{x(x+1)} \right)^{m_3} = \frac{\sigma^2(f)}{f} \right\}.$$

One sees that $\mathcal{Z}$ is generated by $(1,1,1)$ and when $m_1 = m_2 = m_3 = 1$, one can take $f = 1$.

(v) Let $\mathcal{P}_c = \langle I_{\mathrm{irr}} \cup \{y_{1,2} y_{2,1} y_{3,3} - c\} \rangle$ where $c \in C^\times$. One sees that for any $c \in C^\times$, $\mathcal{P}_c$ is proper. Take $c = 1$. Then one can verify that $\mathcal{P}_1$ is a radical ideal and thus it is a maximal σ^2-ideal.

(vi) Compute $I = \mathcal{P}_1 \cap \sigma(\mathcal{P}_1)$. One has that

$$I = \langle y_{3,2}, y_{3,1}, y_{2,3}, y_{2,2} y_{2,1}, y_{1,3}, y_{2,2} y_{1,2}, y_{1,2} y_{2,1}^2 y_{3,3} - y_{2,1}, y_{1,2}^2 y_{2,1} y_{3,3} - y_{1,2},$$
$$y_{1,2} y_{2,1} y_{3,3} + y_{1,1} y_{2,2} y_{3,3} - 1, y_{1,1} y_{2,1}, y_{1,1} y_{1,2} \rangle.$$

(vii) Using Gröbner basis computation, we have that

$$\mathrm{stab}(I) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \, \alpha\beta\gamma = 1 \right\} \cup \left\{ \begin{pmatrix} 0 & \alpha & 0 \\ \beta & 0 & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \, \alpha\beta\gamma = 1 \right\}.$$

Appendix A. Coefficient bounds for generators of $I_{F,d}$

Note that $I_{F,d}$ is generated by

$$\mathbb{S} = \{P(Y) \in k[Y]_{\leq d} \mid P(F) = 0\},$$

which is a k-vector space of finite dimension. We are going to find coefficient bounds for $\mathbb{S}$. Precisely, we shall find an integer ℓ such that there is a basis of $\mathbb{S}$ satisfying that the coefficients of elements in this basis are of degree $\leq \ell$. Let $N = \binom{d+n^2}{d}$

and $M_1, \cdots, M_N$ be the monomials in entries of F with degrees not greater than d. Observe that for a basis of $\mathbb{S}$, it suffices to find a basis of the following vector space

$$\left\{ (a_1, \cdots, a_N) \in k^N \;\middle|\; \sum_{i=1}^{N} a_i M_i = 0 \right\}.$$

Furthermore, one sees that $(M_1, \cdots, M_N)^T$ is a solution of a linear difference equation, which can be constructed from (1.1). Hence our original problem can be reduced to the following one.

Problem A.1. Assume that $\mathbf{v} = (v_1, \cdots, v_n)^T$ is a nonzero solution of (1.1), where the v_i are in some Picard-Vessiot extension ring of k. Set

$$W = \{(a_1, a_2, \cdots, a_n) \in k^n \mid a_1 v_1 + \cdots + a_n v_n = 0\}.$$

Find an integer ℓ depending on n and A, such that W has a basis consisting of vectors whose entries are of degree not greater than ℓ.

Without loss of generality, we may assume that $v_1, \cdots, v_r$ are linearly independent over k and

$$v_{r+i} = c_{i,1} v_1 + \cdots + c_{i,r} v_r, \ i = 1, \cdots, n-r.$$

For all i with $1 \leq i \leq n-r$, denote $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \cdots, c_{i,n})$, where $c_{i,r+i} = -1$ and $c_{i,r+j} = 0$ for all $1 \leq j \leq n-r$ with $j \neq i$. Then $\{\mathbf{c}_1, \cdots, \mathbf{c}_{n-r}\}$ is a basis of W. Actually, for any $\mathbf{a} = (a_1, \cdots, a_n) \in W$, we have that $\mathbf{a} = -(a_{r+1}\mathbf{c}_1 + \cdots + a_n \mathbf{c}_{n-r})$. In the following, we are going to find a bound for $\deg(c_{i,j})$, where $i = 1, \cdots, n-r, j = 1, \cdots, r$. Let V be the solution space of (1.1) and set

$$\tilde{V} = \{\mathbf{w} \in V \mid \mathbf{c}_i \mathbf{w}^T = 0, \ \forall \ i = 1, \cdots, n-r\}.$$

Then $\tilde{V}$ is a C-vector space of finite dimension. Moreover, we have

Lemma A.2. $\dim(\tilde{V}) = r$.

Proof. Clearly, $\mathbf{v} \in \tilde{V}$. Suppose that $\{\mathbf{v}_1, \cdots, \mathbf{v}_\mu\}$ is a basis of the vector space over C spanned by the orbit of $\mathbf{v}$ under the action of $\mathrm{Gal}(K/k)$, the Galois group of (1.1), where K is the ring of fractions of the Picard Vessiot extension of k for (1.1). Then $\mathbf{v}_i \in \tilde{V}$ for all i with $1 \leq i \leq \mu$. Hence $\dim(\tilde{V}) \geq \mu$. In the following, we shall prove that $\mu \geq r$. Denote the matrix consisting of the first μ rows of $(\mathbf{v}_1, \cdots, \mathbf{v}_\mu)$ by D and the remaining ones by U. For any $\phi \in \mathrm{Gal}(K/k)$, there is $[\phi] \in \mathrm{GL}_\mu(C)$ such that $\phi(D) = D[\phi]$ and $\phi(U) = U[\phi]$. Without loss of generality, we may assume that $\det(D) \neq 0$. As for any $\phi \in \mathrm{Gal}(K/k)$, $\phi(\det(D)) = \det(D)\det([\phi])$. One sees from Corollary 1.15 of [29] that $\det(D)$ is invertible in K and therefore D is invertible. Now for any $\phi \in \mathrm{Gal}(K/k)$,

$$\phi(UD^{-1}) = U[\phi][\phi]^{-1} D^{-1} = UD^{-1}.$$

The Galois theory implies that $C = UD^{-1} \in k^{(n-\mu)\times\mu}$. Set $\tilde{C} = (-C, I_{n-\mu})$. Then

$$\tilde{C} \begin{pmatrix} D \\ U \end{pmatrix} = 0.$$

Particularly, $\tilde{C}\mathbf{v} = 0$. This implies that $\dim(W) = n - r \geq n - \mu$ and then $\mu \geq r$. So $\dim(\tilde{V}) \geq r$. On the other hand, one has that $\dim(\tilde{V}) + n - r \leq n$ and then $\dim(\tilde{V}) \leq r$. Hence $\dim(\tilde{V}) = r$. □

Assume that $\{\mathbf{v}_1 = \mathbf{v}, \mathbf{v}_2, \cdots, \mathbf{v}_r\}$ is a basis of $\tilde{V}$ and M is the $n \times r$ matrix consisting of the vectors $\mathbf{v}_1, \cdots, \mathbf{v}_r$. For $1 \leq i_1 < \cdots < i_r \leq n$, denote the determinant of the sub-matrix consisting of the i_1-th,i_2-th, $\cdots$, i_r-th rows of M by $d_{i_1,i_2,\cdots,i_r}$. Then an easy calculation implies that

$$d_{i_1,i_2,\cdots,i_r} = b_{i_1,i_2,\cdots,i_r} d_{1,2,\cdots,r}, \text{where } b_{i_1,i_2,\cdots,i_r} \in k.$$

Particularly,

$$b_{1,2,\cdots,j-1,j+1,\cdots,r,r+i} = (-1)^{r-j} c_{i,j}, \text{for all } 1 \leq i \leq n-r \text{ and all } 1 \leq j \leq r.$$

Let $\mathbf{b} = (b_{1,2,\cdots,r}, \cdots, b_{n-r+1,n-r+2,\cdots,n})^T$. On the other hand, one can construct from A an invertible matrix $\tilde{A}_r$ with entries in k such that $\mathbf{b}d_{1,2,\cdots,r}$ is a solution of $\sigma(Y) = \tilde{A}_r Y$. Notice that the matrix $\tilde{A}_r$ only depends on A and r. Moreover, one can easily verify that $d_{1,2,\cdots,r}$ is σ-hypergeometric over k. This implies that $\mathbf{b}d_{1,2,\cdots,r}$ is a σ-hypergeometric solution. By means of cyclic vector, the system of the form (1.1) can be reduced into a scalar linear difference equation. Then the algorithms for problem (P4) allow us to find all σ-hypergeometric solutions of (1.1). Therefore one can find an integer $\ell/2$ such that σ-hypergeometric solutions of $\sigma(Y) = \tilde{A}_r Y$ are of the form $\mathbf{w}h$ where h is σ-hypergeometric over k and $\mathbf{w}$ is a vector whose entries are elements in k with degree not greater than $\ell/2$. Particularly, $\mathbf{b}d_{1,2,\cdots,r} = \bar{\mathbf{w}}\bar{h}$ where $\bar{\mathbf{w}} = (\bar{w}_1, \cdots, \bar{w}_n) \in k^n$ satisfying $\deg(\bar{w}_i) \leq \ell/2$ and $\bar{h}$ is hypergeometric over k. Observe that $b_{1,2,\cdots,r} = 1$. Then one has that $\mathbf{b} = \bar{\mathbf{w}}/\bar{w}_1$. Hence entries of $\mathbf{b}$ are of degree $\leq \ell$. Specially, $\deg(c_{i,j}) \leq \ell$.

In the case that we do not know the dimension of $\tilde{V}$, we can take $r = 1, 2, \cdots, n-1$ and construct the corresponding systems $\sigma(Y) = \tilde{A}_1 Y, \cdots, \sigma(Y) = \tilde{A}_{n-1} Y$, respectively. Compute all σ-hypergeometric solutions of these systems and let $\ell/2$ be an integer such that these σ-hypergeometric solutions are of the form $\mathbf{w}h$ where h is σ-hypergeometric over k and $\mathbf{w}$ is a vector whose entries are rational functions in x with degrees not greater than $\ell/2$. Then we have that $\deg(c_{i,j}) \leq \ell$. This solves Problem A.1.

Appendix B. σ^δ-Hypergeometric elements

In this appendix, we shall describe a method to compute σ^δ-hypergeometric elements in $k[Y, 1/\det(Y)]/I_{\text{irr}}$. In fact, instead of all σ^δ-hypergeometric elements in $k[Y, 1/\det(Y)]/I_{\text{irr}}$, we only find those σ^δ-hypergeometric elements that are not pairwise similar and are represented by polynomials in $k[Y]_{\leq d}$, the set of polynomials in $k[Y]$ with degrees not greater than d. Assume that $\mathbf{m}_1, \cdots, \mathbf{m}_\ell$ are polynomials in $k[Y]_{\leq d}$ satisfying that $\{\bar{\mathbf{m}}_1, \cdots, \bar{\mathbf{m}}_\ell\}$ is a k-basis of $k[Y]_{\leq d}/(I_{\text{irr}} \cap k[Y]_{\leq d})$, where $\bar{\mathbf{m}}_i$ is the image of $\mathbf{m}_i$. With Gröbner basis computation, one can find these $\mathbf{m}_i$. As σ^δ preserves the degrees of elements of $k[Y]$, there is $\tilde{A} \in \mathrm{GL}_\ell(k)$ such that

$$\sigma^\delta((\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \cdots, \bar{\mathbf{m}}_\ell)) = (\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \cdots, \bar{\mathbf{m}}_\ell)\tilde{A}.$$

The invertible matrix $\tilde{A}$ can be constructed from A. Now suppose that $P = \sum c_i \mathbf{m}_i$ is a σ^δ-hypergeometric element, where $c_i \in k$, i.e., $\sigma^\delta(P) - rP \in I_{\text{irr}}$ for some $r \in k$ and P is invertible in $k[Y, 1/\det(Y)]/I_{\text{irr}}$. Then one can verify that $c_1, \cdots, c_\ell$ and r satisfying

$$\tilde{A}\sigma^\delta \begin{pmatrix} c_1 \\ \vdots \\ c_\ell \end{pmatrix} = r \begin{pmatrix} c_1 \\ \vdots \\ c_\ell \end{pmatrix}.$$

Let h be a σ^δ-hypergeometric element satisfying $\sigma^\delta(h) = r^{-1}h$. Then $(c_1, \cdots, c_\ell)^T h$ is a σ^δ-hypergeometric solution of the following linear difference equation

$$\sigma^\delta(Y) = \tilde{A}^{-1}Y. \tag{B.1}$$

Consequently, for those $c_1, \cdots, c_\ell$ and r, it suffices to find all σ^δ-hypergeometric solutions of the above linear difference equation. Using the algorithms for problem (P4), one can find all σ^δ-hypergeometric solutions of (B.1). In particular, one can find σ^δ-hypergeometric solutions $\mathbf{c}_1 h_1, \cdots, \mathbf{c}_l h_l$ that are not pairwise similar where $h_1, \cdots, h_l$ are σ^δ-hypergeometric and $\mathbf{c}_1, \cdots, \mathbf{c}_l$ are vectors with entries in k. Here two vectors $\mathbf{h}_1, \mathbf{h}_2$ are said to be similar if $\mathbf{h}_1 = r\mathbf{h}_2$ for some $r \in k^\times$. Furthermore, if $\mathbf{h}$ is a σ^δ-hypergeometric solution of (B.1), then there is a unique j with $1 \le j \le l$ such that $\mathbf{h} = b\mathbf{c}_j h_j$ for some $b \in k$. Write $\mathbf{c}_i = (c_{i,1}, \cdots, c_{i,\ell})$ and set $P_i = \sum_{j=1}^{\ell} c_{i,j}\mathbf{m}_j$, where $i = 1, 2, \cdots, l$. Then $\sigma^\delta(P_i) - r_i P_i \in I_{\mathrm{irr}}$ for some $r_i \in k$. It remains to select those P_i that are invertible in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$. Note that P_i is invertible in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ if and only if $\mathrm{Zero}(P_i) \cap \mathrm{Zero}(I_{\mathrm{irr}}) = \emptyset$. The latter condition can be detected by Gröbner basis computation. Precisely, it suffices to decide if 1 is in the ideal $\langle I_{\mathrm{irr}}, P_i\rangle$. The previous results are summarized in the following algorithm.

Algorithm B.1. *Compute all σ^δ-hypergeometric elements in $k[Y, 1/\det(Y)]/I_{\mathrm{irr}}$ that are represented by polynomials in $k[Y]_{\le d}$ and are not pairwise similar.*

(a) *Compute a Gröbner basis for $I_{\mathrm{irr}} \cap k[Y]$ and then find the monomials $\mathbf{m}_1, \cdots, \mathbf{m}_\ell$ in $k[Y]_{\le d}$ such that $\{\bar{\mathbf{m}}_1, \cdots, \bar{\mathbf{m}}_\ell\}$ is a k-basis of $k[Y]_{\le d}/(I_{\mathrm{irr}} \cap k[Y])_{\le d}$, where $\bar{\mathbf{m}}_i$ denotes the image of $\mathbf{m}_i$ in $k[Y]_{\le d}/(I_{\mathrm{irr}} \cap k[Y])_{\le d}$.*

(b) *Construct an invertible matrix $\tilde{A} \in \mathrm{GL}_\ell(k)$ such that*

$$\sigma^\delta((\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \cdots, \bar{\mathbf{m}}_\ell)) = (\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \cdots, \bar{\mathbf{m}}_\ell)\tilde{A}.$$

(c) *Compute σ^δ-hypergeometric elements of $\sigma^\delta(Y) = \tilde{A}^{-1}Y$, which are not pairwise similar. Denote them by $\mathbf{c}_1 h_1, \cdots, \mathbf{c}_l h_l$, where $h_1, \cdots, h_l$ are σ^δ-hypergeometric and $\mathbf{c}_1, \cdots, \mathbf{c}_l$ are vectors with entries in k.*

(d) *Write $\mathbf{c}_i = (c_{i,1}, \cdots, c_{i,\ell})$ and set $P_i = \sum_{j=1}^{\ell} c_{i,j}\mathbf{m}_j$, where $i = 1, 2, \cdots, l$.*

(e) *Decide whether 1 is in $\langle I_{\mathrm{irr}} \cap k[Y], P_i, \det(Y)z - 1\rangle$ with Gröbner basis computation. Return those P_i satisfying $1 \in \langle I_{\mathrm{irr}} \cap k[Y], P_i, \det(Y)z - 1\rangle$.*

Acknowledgements

The author thanks Michael F. Singer for his numerous significant suggestions. Particularly, he suggested that the author consider σ^δ-ideals. These suggestions influenced the course of this research and led to a number of improvements. The author also thanks the anonymous referees for useful comments.

References

[1] T. Becker and V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993. MR1213453

[2] M. A. Barkatou, T. Cluzeau, L. Di Vizio and J. A. Weil, *Computing the Lie algebra of the differential Galois group of a linear differential system*, ISSAC'16 (2016), 63-70.

[3] E. Compoint and M. F. Singer, *Computing Galois groups of completely reducible differential equations*, J. Symbolic Comput. **28** (1999), no. 4-5, 473–494, DOI 10.1006/jsco.1999.0311. MR1731934

[4] T. Cluzeau and M. van Hoeij, *Computing hypergeometric solutions of linear recurrence equations*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 2, 83–115, DOI 10.1007/s00200-005-0192-x. MR2233774

[5] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*: *An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997. MR1417938

[6] H. Derksen, E. Jeandel, and P. Koiran, *Quantum automata and algebraic groups*, J. Symbolic Comput. **39** (2005), no. 3-4, 357–371, DOI 10.1016/j.jsc.2004.11.008. MR2168287

[7] T. Dreyfus and J. Roques, *Galois groups of difference equations of order two on elliptic curves*, SIGMA Symmetry Integrability Geom. Methods Appl. **11** (2015), Paper 003, 23, DOI 10.3842/SIGMA.2015.003. MR3313679

[8] D. Eisenbud, C. Huneke, and W. Vasconcelos, *Direct methods for primary decomposition*, Invent. Math. **110** (1992), no. 2, 207–235, DOI 10.1007/BF01231331. MR1185582

[9] R. Feng, *Hrushovski's algorithm for computing the Galois group of a linear differential equation*, Adv. in Appl. Math. **65** (2015), 1–37, DOI 10.1016/j.aam.2015.01.001. MR3320755

[10] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. **6** (1988), no. 2-3, 149–167, DOI 10.1016/S0747-7171(88)80040-3. MR988410

[11] P. A. Hendriks, *An algorithm for computing a standard form for second-order linear q-difference equations*, J. Pure Appl. Algebra **117/118** (1997), 331–352, DOI 10.1016/S0022-4049(97)00017-0. MR1457845

[12] P. A. Hendriks, *An algorithm determining the difference Galois group of second order linear difference equations*, J. Symbolic Comput. **26** (1998), no. 4, 445–461, DOI 10.1006/jsco.1998.0223. MR1646675

[13] J. E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, New York-Heidelberg, 1975. Graduate Texts in Mathematics, No. 21. MR0396773

[14] E. Hrushovski, *Computing the Galois group of a linear differential equation*, Differential Galois theory (Będlewo, 2001), Banach Center Publ., vol. 58, Polish Acad. Sci., Warsaw, 2002, pp. 97–138, DOI 10.4064/bc58-0-9. MR1972449

[15] D. Kapur, Y. Sun, and D. Wang, *An efficient method for computing comprehensive Gröbner bases*, J. Symbolic Comput. **52** (2013), 124–142, DOI 10.1016/j.jsc.2012.05.015. MR3018131

[16] M. Kauers and B. Zimmermann, *Computing the algebraic relations of C-finite sequences and multisequences*, J. Symbolic Comput. **43** (2008), no. 11, 787–803, DOI 10.1016/j.jsc.2008.03.002. MR2432957

[17] J. J. Kovacic, *An algorithm for solving second order linear homogeneous differential equations*, J. Symbolic Comput. **2** (1986), no. 1, 3–43, DOI 10.1016/S0747-7171(86)80010-4. MR839134

[18] A. R. Magid, *Finite generation of class groups of rings of invariants*, Proc. Amer. Math. Soc. **60** (1976), 45–48 (1977). MR0427306

[19] A. Maier, *A difference version of Nori's theorem*, Math. Ann. **359** (2014), no. 3-4, 759–784, DOI 10.1007/s00208-014-1012-z. MR3231015

[20] M. Petkovšek, *Hypergeometric solutions of linear recurrences with polynomial coefficients*, J. Symbolic Comput. **14** (1992), no. 2-3, 243–264, DOI 10.1016/0747-7171(92)90038-6. MR1187234

[21] A. Montes and M. Wibmer, *Gröbner bases for polynomial systems with parameters*, J. Symbolic Comput. **45** (2010), no. 12, 1391–1425, DOI 10.1016/j.jsc.2010.06.017. MR2733386

[22] Rettstadt, D. *On the computation of the differential Galois group*, Ph.D. thesis, RWTH Aachen University, 2014.

[23] J. Roques, *On the algebraic relations between Mahler functions*, 2015, https://www-fourier.ujf-grenoble.fr/~jroques/mahler.pdf.

[24] J. Roques, *Galois groups of the basic hypergeometric equations*, Pacific J. Math. **235** (2008), no. 2, 303–322, DOI 10.2140/pjm.2008.235.303. MR2386226

[25] M. Rosenlicht, *Toroidal algebraic groups*, Proc. Amer. Math. Soc. **12** (1961), 984–988. MR0133328

[26] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313. MR0349648

[27] M. F. Singer and F. Ulmer, *Galois groups of second and third order linear differential equations*, J. Symbolic Comput. **16** (1993), no. 1, 9–36, DOI 10.1006/jsco.1993.1032. MR1237348

[28] M. F. Singer, *Algebraic relations among solutions of linear differential equations*, Trans. Amer. Math. Soc. **295** (1986), no. 2, 753–763, DOI 10.2307/2000062. MR833707
[29] M. F. Singer *Algebraic and Algorithmic Aspects of Difference Equations*, Lecture notes at CIMPA conference in Santa Marta Columbia, 2012.
[30] A. Suzuki and Y. Sato, *A simple algorithm to compute comprehensive Gröbner bases*, ISSAC 2006 (2006), 326-331.
[31] M. van der Put and M. F. Singer, *Galois Theory of Difference Equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997. MR1480919
[32] V. Weispfenning, *Comprehensive Gröbner bases*, J. Symbolic Comput. **14** (1992), no. 1, 1–29, DOI 10.1016/0747-7171(92)90023-W. MR1177987

KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences and UCAS, Chinese Academy of Sciences, Beijing 100190, People's Republic of China
E-mail address: ryfeng@amss.ac.cn