Note on the construction of Picard-Vessiot rings for linear differential equations

Ruyong Feng

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

Abstract
In this note, we describe a method to construct the Picard-Vessiot ring of a given linear differential equation.

1 Introduction
Throughout this note, \( C \) stands for an algebraically closed field of characteristic zero and \( k = C(t) \) denotes the ring of rational functions in \( t \). We use \( \delta \) to denote the usual derivation with respect to \( t \). Then \( k \) is a differential ring with derivation \( \delta \). \( X \) denotes \( n \times n \) matrix \((X_{i,j})\) with indeterminate entries \( X_{i,j} \). Consider linear differential equation

\[
\delta(Y) = AY
\]

where \( A \in \text{Mat}_n(k) \). Denote the ring over \( k \) generated by the entries of \( X \) and \( 1/\det(X) \) by \( k[X, 1/\det(X)] \). By setting \( \delta(X) = AX \), we may endow \( k[X, 1/\det(X)] \) with a structure of differential ring that extends the differential ring \( k \). An ideal \( I \) of \( k[X, 1/\det(X)] \) is called a differential ideal (or \( \delta \)-ideal for short) if \( \delta(I) \subset I \). Let \( m \) be a maximal \( \delta \)-ideal. Then the quotient ring

\[
R = k[t][X, 1/\det(X)]/m
\]

is the Picard-Vessiot ring of (1) over \( k \). Recently, the construction of Picard-Vessiot rings receives many attentions. In this note, we shall describe a method to construct this ring, i.e. a method to compute a maximal \( \delta \)-ideal \( m \). Denote by \( \text{Gal}(R/k) \) the Galois group of (1) over \( k \) that is defined to be the set of \( k \)-automorphisms of \( R \) which commute with \( \delta \). Let \( F \) be a fundamental matrix of (1) with entries in \( R \). Then \( F \) induces an injective group homomorphism from \( \text{Gal}(R/k) \) to \( \text{GL}_n(C) \). The image of this homomorphism can be described via the stabilizer of the maximal \( \delta \)-ideal with \( F \) as a zero.

Definition 1.1 For an ideal \( I \) in \( k[X, 1/\det(X)] \), the stabilizer of \( I \), denoted by \( \text{stab}(I) \), is defined to be

\[
\{ g \in \text{GL}_n(C) | \forall P \in I, P(Xg) \in I \}.
\]

This research was supported by NSFC under Grants No.11771433 and No.11688101, and Beijing Natural Science Foundation (Z190004).
Let $\text{stab}(I)$ be a maximal $\delta$-ideal and $\bar{G}$ be a maximal $\delta$-torsor over $k$. Therefore $\text{stab}(\mathcal{I}(F, \nu)) = \{g \in \text{GL}_n(C) | \forall P \in \mathcal{I}(F, \nu), P(Fg) = 0\}$. Therefore $F \text{stab}(\mathcal{I}(F, \nu)) = \text{Zero}(\mathcal{I}(F, \nu))$.

2. For an ideal $I$ in $k[X, 1/\det(X)]$, one can verify that $\text{stab}(I) \subset \text{stab}(\sqrt{I})$. Generally, the stabilizers of $I$ and $\sqrt{I}$ are not equal. For instance, set $n = 2$ and

$$I = \langle x_{11}^2, x_{22}^2, x_{12}^3, x_{21}^3 \rangle.$$ 

Then $\sqrt{I} = \langle x_{ij} : i, j = 1, 2 \rangle$. One has that $\text{stab}(\sqrt{I}) = \text{GL}_2(C)$ but $\text{stab}(I) = \{\text{diag}(c_1, c_2) | c_1c_2 \neq 0\}$. While for $I = \mathcal{I}(F, \nu)$, an easy calculation yields that $\text{stab}(I) = \text{stab}(\sqrt{I})$.

3. Let $\mu$ be an integer greater than $\nu$. Then $\mathcal{I}(F, \nu) \subset \mathcal{I}(F, \mu)$ and from 1, one sees that $\text{stab}(\mathcal{I}(F, \mu)) \subset \text{stab}(\mathcal{I}(F, \nu))$.

Let $m$ be a maximal $\delta$-ideal and $G = \text{stab}(m)$. Theorem 1.28 on page 22 of [10] states that $\mathcal{V}_{\bar{k}}(m)$ is a $G$-torsor over $k$. The following proposition implies that the similar property holds for $\mathcal{V}_{\bar{k}}(\mathcal{I}(F, \nu))$. 

2 Toric maximal $\delta$-ideals
Proposition 2.3 \( \forall_k(\mathcal{I}(F, \nu)) \) is an \( H \)-torsor over \( k \), where \( H = \text{stab}(\mathcal{I}(F, \nu)) \).

Proof. Let \( K = \overline{k}(F) \). We first show that \( FH(K) = \forall_k(\mathcal{I}(F, \nu)) \). Let \( S \subset C[X, 1/\det(X)] \) be a finite set of polynomials defining \( H \). Since \( \mathcal{I}(F, \nu) \) is generated by some polynomials with degree not greater than \( \nu \), we may assume that elements of \( S \) are of degree not greater than \( \nu \). Then \( \{P(\mathcal{F}^{-1}X)|P \in S\} \) defines \( FH(K) \) and it consists of polynomials with degree not greater than \( \nu \). Let \( J \) be the ideal in \( k(F)[X, 1/\det(X)] \) generated by \( S \). As \( H \) contains the Galois group of \( (1) \) over \( k \), one sees that \( J \) is \( \text{Gal}(k(F)/k) \)-invariant. The proof of Lemma 1.29 on page 23 of [10] implies that \( J \) is generated by \( J \cap k[X, 1/\det(X)] \) and furthermore \( J \cap k[X, 1/\det(X)] \) is generated by some polynomials with degree not greater than \( \nu \). Hence \( J \cap k[X, 1/\det(X)] \subset \mathcal{I}(F, \nu) \). This implies that \( \forall_k(\mathcal{I}(F, \nu)) \subset FH(K) \). By Remark 2.2, \( FH(K) \subset \forall_k(\mathcal{I}(F, \nu)) \). Therefore \( FH(K) = \forall_k(\mathcal{I}(F, \nu)) \). Suppose that \( \alpha \in \forall_k(\mathcal{I}(F, \nu)) \). Then \( \alpha = FH \) for some \( h \in H(K) \) and one has that
\[
\alpha H(K) = FH(K) = \forall_k(\mathcal{I}(F, \nu)).
\]
From this, one sees easily that \( \alpha H(\overline{k}) = \forall_k(\mathcal{I}(F, \nu)) \). \( \square \)

Definition 2.4 An algebraic subvariety \( X \) of \( GL_n(C) \) is said to be bounded by \( d \), where \( d \) is a positive integer, if there are polynomials \( f_1, \ldots, f_s \subset C[X] \) of degree at most \( d \) such that
\[
X = GL_n(C) \cap \forall_C(f_1, \ldots, f_s).
\]

Set
\[
d(n) = \begin{cases} 
6, & n = 2 \\
360, & n = 3 \\
(4n)^{3n^2}, & n \geq 4
\end{cases}
\]

Theorem 2.5 (Theorems 3.1, 3.2 and 3.3 of [1]) Let \( G \subset GL_n(C) \) be a linear algebraic group. Then there exists a toric envelope of \( G \) bounded by \( d(n) \).

Proposition 2.6 The radical of \( \mathcal{I}(F, d(n)) \) is a toric maximal \( \delta \)-ideal.

Proof. Set \( J = \sqrt{\mathcal{I}(F, d(n))} \) and \( m = \mathcal{I}(F, \infty) \). Then \( J \) is a radical \( \delta \)-ideal and \( \text{stab}(m) \subset \text{stab}(\mathcal{I}(F, d(n))) = \text{stab}(J) \). Let \( H \) be a toric envelope of \( \text{stab}(m) \) bounded by \( d(n) \), and denote
\[
\tilde{J} = \{P \in k[X, 1/\det(X)]|\forall h \in H, P(Fh) = 0\}.
\]
Then \( F \tilde{J} = \text{Zero}(\tilde{J}) \) and moreover Lemma 2.1 of [3] implies that \( \tilde{J} \) is generated by some polynomials in \( k[X] \) of degree not greater than \( d(n) \). In other words, \( \tilde{J} \subset \mathcal{I}(F, d(n)) \). One sees that
\[
\text{Zero}(m) \subset \text{Zero}(\mathcal{I}(F, d(n))) \subset \text{Zero}(\tilde{J}).
\]
By Remark 2.2, we have that
\[
F\text{stab}(m) \subset F\text{stab}(\mathcal{I}(F, d(n))) \subset FH
\]
which implies that \( \text{stab}(m) \subset \text{stab}(J) \subset H \). By Lemma 5.1 of [1], \( \text{stab}(J) \) is also a toric envelope of \( \text{stab}(m) \). So \( J \) is a toric maximal \( \delta \)-ideal. \( \square \)

The method described in Section 4.1 of [3] allows one to compute a \( k \)-basis of (2) i.e. a set of generators of \( \mathcal{I}(F, \nu) \). By Gröbner bases computation one can compute the toric maximal \( \delta \)-ideal \( \sqrt{\mathcal{I}(F, d(n))} \).
3 Maximal $\delta$-ideals in $\overline{k}[X, 1/\det(X)]$

From now on, assume that we have already computed a set of generators of $\mathcal{I}(\mathcal{F}, d(n))$. Let $H = \text{stab}(\mathcal{I}(\mathcal{F}, d(n)))$ and let $\alpha \in \mathcal{V}(\mathcal{I}(\mathcal{F}, d(n)))$. Then $\mathcal{V}_{\overline{k}}(\mathcal{I}(\mathcal{F}, d(n))) = \alpha H(\overline{k})$. Denote by $\sqrt{\mathcal{I}(\mathcal{F}, d(n))}_{\overline{k}}$ the ideal in $\overline{k}[X, 1/\det(X)]$ generated by $\mathcal{I}(\mathcal{F}, d(n))$ and decompose $\sqrt{\mathcal{I}(\mathcal{F}, d(n))}_{\overline{k}}$ into prime ideals:

$$\sqrt{\mathcal{I}(\mathcal{F}, d(n))}_{\overline{k}} = \mathcal{Q}_1 \cap \cdots \cap \mathcal{Q}_s.$$

Remark that the above decomposition can be done over the field $k(\alpha)$. Precisely, decompose $\sqrt{\mathcal{I}(\mathcal{F}, d(n))}_{k(\alpha)}$ into prime ideals in $k(\alpha)[X, 1/\det(X)]$, say $\mathcal{Q}_1, \ldots, \mathcal{Q}_s$. Then each $\mathcal{V}(\mathcal{Q}_i)$ is an $H^\circ$-torsor over $k(\alpha)$. Hence $\mathcal{Q}_i$ generates a prime ideal in $\overline{k}[X, 1/\det(X)]$ and then from these $\mathcal{Q}_i$ we obtain $\mathcal{Q}_i$. Without loss of generality, we assume that $\alpha \in \mathcal{V}(\mathcal{Q}_1)$. Denote $\mathcal{R} = \mathcal{Q}_1/\det(X)]/\mathcal{Q}_1$. Remark that $\mathcal{R}$ is a $\delta$-ring and all $\mathcal{Q}_i$ are $\delta$-ideals. Let $\mathcal{I}_{\mathcal{R}}(H^\circ)$ be the vanishing ideal of $H^\circ$ in $\overline{k}[X, 1/\det(X)]$. Consider the map

$$\phi : \overline{k}[X, 1/\det(X)]/\mathcal{I}_{\mathcal{R}}(H^\circ) \rightarrow \mathcal{R}$$

$$P(X) \rightarrow P(\alpha^{-1}X).$$

One sees that $\phi$ is an isomorphism of $\overline{k}$-algebras.

**Definition 3.1** An element $h \in R$ is said to be hyperexponential over $k$ if $h$ is invertible in $R$ and $\delta(h) = \lambda h$ for some $\lambda \in \overline{k}$. Suppose that $h_1$ and $h_2$ are hyperexponential over $\overline{k}$. We say $h_1$ and $h_2$ are similar if $h_1 = rh_2$ for some $r \in \overline{k}$.

The following proposition reveals the relation between hyperexponential elements of $R$ and characters of $H^\circ$.

**Proposition 3.2** If $\chi$ is a character of $H^\circ$, then $\chi(\alpha^{-1}X)$ is hyperexponential over $k$ where $X$ denotes the image of $X$ in $R$ under the natural homomorphism. Conversely, if $h \in R$ is hyperexponential over $k$ then $h = r\chi(\alpha^{-1}X)$ for some character $\chi$ and some $r \in k$.

**Proof**. Obviously, $\chi(\alpha^{-1}X)$ is invertible. We shall prove that $\chi(\alpha^{-1}X)$ is hyperexponential over $k$. Set $r = \delta(\chi(\alpha^{-1}X))|_{X = \alpha}$. We claim that

$$\delta(\chi(\alpha^{-1}X)) = r\chi(\alpha^{-1}X).$$

Denote

$$P(X) = \chi(X^{-1}\alpha)\delta(\chi(X^{-1})) = \chi(X^{-1}\alpha)\sum_{i,j} \frac{\partial \chi}{\partial X_{i,j}}(\alpha^{-1}X)(\delta(\alpha^{-1})X + \alpha^{-1}AX)_{i,j}$$

where for a matrix $M$, $M_{i,j}$ denotes its $(i,j)$-entry. Since $F$ is a zero of $\sqrt{\mathcal{I}(\mathcal{F}, d(n))}_{\overline{k}}$, there is $h \in H$ such that $Fh \in \mathcal{V}_{\overline{k}(\mathcal{F})}(Q_1) = \alpha H^\circ(\overline{k}(\mathcal{F})).$ Set $F = h$. Then $\mathcal{V}_{\overline{k}(\mathcal{F})}(Q_1) = \mathcal{F}H^\circ(\overline{k}(\mathcal{F})).$ We can view $P(X)$ as a regular function on $\mathcal{V}_{\overline{k}(\mathcal{F})}(Q_1)$, and then view $P(\overline{F}X)$ as a regular function on...
Proposition 3.3 $J$ is a maximal $\delta$-ideal in $\bar{k}[X, 1/\det(X)]$. 

Thus, for any $g \in H^\circ$, $$
\delta(\chi(\alpha^{-1}X))|_{X=fg} = \delta(\chi(\alpha^{-1}\mathcal{F}g)) = \delta(\chi(\alpha^{-1}\mathcal{F})\chi(g)) = \delta(\chi(\alpha^{-1}\mathcal{F}))\chi(g),
$$
which implies that for any $g \in H^\circ$, one has that

$$
P(\mathcal{F}g) - P(\mathcal{F}) = \chi(\bar{X}^{-1}\alpha)\delta(\chi(\alpha^{-1}\bar{X}))|_{X=fg} - P(\mathcal{F}) = \chi(g^{-1}\mathcal{F}^{-1}\alpha)\delta(\chi(\alpha^{-1}\mathcal{F}))\chi(g) - P(\mathcal{F}) = P(\mathcal{F}) - P(\mathcal{F}) = 0.
$$

Hence the subvariety of $H^\circ(\bar{k}(\mathcal{F}))$ defined by $P(\mathcal{F}X) - P(\mathcal{F})$ contains $H^\circ$. One can verify that the subvariety of $H^\circ(\bar{k}(\mathcal{F}))$ containing $H^\circ$ must be $H^\circ(\bar{k}(\mathcal{F}))$ itself. Thus $P(\mathcal{F}X)$ is equal to $P(\mathcal{F})$ and so is $P(X)$. Now assigning $X = \alpha$ in $P(X)$ yields that

$$
P(\mathcal{F}) = P(\alpha) = \delta(\chi(\alpha^{-1}\bar{X}))|_{X=\alpha} = r.
$$

This proves our claim.

Conversely, assume that $h \in R$ is hyperexponential over $\bar{k}$. Then $h$ is invertible in $R$, i.e., $h(\alpha X)$ is invertible in $k[X, 1/\det(X)]/\mathbb{Z}_k(H^\circ)$. Equivalently, both $h(\alpha X)$ and $1/h(\alpha X)$ are regular functions on $H^\circ(\bar{k})$. Since $H^\circ(\bar{k})$ is a connected algebraic subgroup of $GL_n(\bar{k})$. Rosenlicht’s Theorem (see [6, 8] for instance) implies that $h(\alpha X) = r\chi(X)$ for some $r \in \bar{k}$ and some character $\chi$ of $H^\circ$. That is to say, $h(\bar{X}) = r\chi(\alpha^{-1}\bar{X})$. □

Denote by $\chi(H^\circ)$ the group of characters of $H^\circ$ and assume that $\{\chi_1, \ldots, \chi_l\}$ is a set of generators of $\chi(H^\circ)$. By Proposition 2.3, $\chi_i(\alpha^{-1}X)$ is hyperexponential over $\bar{k}$. Let $r_i$ be the certificate of $\chi_i(\alpha^{-1}X)$ for all $i = 1, \ldots, l$. Set

$$
Z = \left\{(m_1, \ldots, m_l) \in \mathbb{Z}^l \mid \exists f \in \bar{k} \setminus \{0\} \text{ s.t. } \sum_{i=1}^l m_ir_i = \frac{\delta(f)}{f} \right\}.
$$

Then $Z$ is a finitely generated $\mathbb{Z}$-module. Let $\{m_1, \ldots, m_l\}$ be a set of generator of $Z$ and $f_i \in \bar{k} \setminus \{0\}$ satisfy that $\sum_{j=1}^l m_{ij}r_j = \delta(f_i)/f_i$, where $m_i = (m_{i1}, \ldots, m_{il})$. Let $\mathcal{F}$ be as in the proof of Proposition 2.3. Then $\mathcal{F}$ is a fundamental matrix of (1) and for all $i = 1, \ldots, l$,

$$
\delta \left( \prod_{j=1}^l \chi_j(\alpha^{-1}\mathcal{F})^{m_{ij}} \right) = \frac{\delta(f_i)}{f_i}.
$$

Thus $\prod_{j=1}^l \chi_j(\alpha^{-1}\mathcal{F})^{m_{ij}} = c_if_i$ for some constant $c_i$ in $\bar{k}(\mathcal{F})$ that is $C$. Now let $J$ be the radical ideal in $\bar{k}[X, 1/\det(X)]$ generated by

$$
Q_1 \cup \left\{ \prod_{j=1}^l \chi_j(\alpha^{-1}X)^{m_{ij}} - c_if_i \mid i = 1, \ldots, l \right\}.
$$

Proposition 3.3 $J$ is a maximal $\delta$-ideal in $\bar{k}[X, 1/\det(X)]$. 

5
**Proof.** Denote \( \tilde{J} = \{ P \in \tilde{k}[X, 1/\det(X)] | |P(F)| = 0 \} \) and \( \tilde{G} = \text{stab}(\tilde{J}) \). Then \( \tilde{J} \) is a maximal \( \delta \)-ideal containing \( J \) and \( \tilde{G} \) is the identity component of the Galois group \( G \) of (1) over \( k \). We shall prove that \( J = \tilde{J} \). Let \( \tilde{a} \in \mathbb{V}_k(\tilde{J}) \). Then by Proposition 2.3, \( \mathbb{V}_k(\tilde{J}) = \tilde{a}\tilde{G}(\tilde{k}) \) and \( \mathbb{V}_k(Q_1) = \tilde{a}H^0(\tilde{k}) \). So \( \tilde{G} \subset H^0 \). Because \( H \) is a toric envelope of \( G \), one sees that \( H^0 \) is a toric envelope of \( \tilde{G} \). By Lemma 4.1 of [1] and Proposition 2.6 of [4], \( \tilde{G} \) is defined by some characters of \( H^0 \), i.e. \( \tilde{G} = \cap_{\chi \in S \ker(\chi)} \) where \( S \) is a finite subset of \( \chi(H^0) \). Suppose that \( \chi \in S \). Since \( \tilde{a}^{-1}F \in \tilde{G}(\tilde{k}(F)) \), \( \chi(\tilde{a}^{-1}F) = 1 \). So \( \chi(\alpha^{-1}F) = \chi(\alpha^{-1}\tilde{a}) \). Write \( \chi = \prod_{i=1}^{l} \chi_i^{d_i} \) with \( d_i \in \mathbb{Z} \). One then has that

\[
\delta \left( \prod_{i=1}^{l} \chi_i(\alpha^{-1}F)^{d_i} \right) = \sum_{i=1}^{l} d_i \delta(\chi_i(\alpha^{-1}F)) = \sum_{i=1}^{l} d_i r_i = \frac{\delta(\chi(\alpha^{-1}\tilde{a}))}{\chi(\alpha^{-1}\tilde{a})}.
\]

This implies that \( (d_1, \ldots, d_l) \in \mathbb{Z} \). Write \( (d_1, \ldots, d_l) = \sum_{j=1}^{\ell} s_j m_{j i} \), where \( s_j \in \mathbb{Z} \). Now for any \( g \in \mathbb{V}_k(J) \), one has that \( \prod_{j=1}^{l} \chi_j(\alpha^{-1}g)^{m_{j i}} = c_if_i \) for all \( i = 1, \ldots, \ell \) and then

\[
\chi(\alpha^{-1}g) = \prod_{j=1}^{l} \chi_j(\alpha^{-1}g)^{d_i} = \prod_{j=1}^{l} \chi_j(\alpha^{-1}g)^{\sum_{j=1}^{l} s_j m_{j i}} = \prod_{i=1}^{\ell} \left( \prod_{j=1}^{l} \chi_j(\alpha^{-1}g)^{m_{j i}} \right)^{s_i} = \prod_{i=1}^{\ell} (c_if_i)^{s_i}.
\]

In particular, one has that \( \chi(\alpha^{-1}\tilde{a}) = \prod_{i=1}^{l} (c_if_i)^{s_i} \). On the other hand, for any \( g \in \mathbb{V}_k(J) \), one has that \( g = \tilde{a}g \) for some \( \tilde{g} \in H^0(\tilde{k}) \) and then

\[
\chi(\alpha^{-1}\tilde{a}) = \prod_{i=1}^{\ell} (c_if_i)^{s_i} = \chi(\alpha^{-1}g) = \chi(\alpha^{-1}\tilde{a}g) = \chi(\alpha^{-1}\tilde{a})\chi(\tilde{g}).
\]

This implies that \( \chi(\tilde{g}) = 1 \). By the choice of \( \chi \), one sees that \( \tilde{g} \in \tilde{G}(\tilde{k}) \). Consequently, \( \mathbb{V}_k(J) \subset \tilde{a}\tilde{G}(\tilde{k}) = \mathbb{V}_k(\tilde{J}) \). Since \( J \) is radical, \( \tilde{J} \subset J \). Thus \( \tilde{J} = J \).

\[\square\]

Given \( \mathcal{H} = \{ \chi_1(\alpha^{-1}X), \ldots, \chi_l(\alpha^{-1}X) \} \), a method described in [2] allows one to compute a set of generators of \( \mathbb{Z} \), say \( \{ m_1, \ldots, m_\ell \} \) and the corresponding \( f_1, \ldots, f_\ell \). Thus in order to compute the maximal \( \delta \)-ideal \( J \), it suffices to compute \( \mathcal{H} \). Proposition 3.2 indicates that \( \mathcal{H} \) can be obtained via computing suitable hyperexponential elements in \( R \). Remark that for any two \( \chi_1, \chi_2 \in \chi(H^0) \), \( \chi_1(\alpha^{-1}X) \) and \( \chi_2(\alpha^{-1}X) \) are similar if and only if \( \chi_1 = \chi_2 \). To see this, assume that \( \chi_1(\alpha^{-1}X) = r\chi_2(\alpha^{-1}X) \) for some \( r \in \tilde{k} \). Then taking \( \tilde{X} = \alpha \), one sees that \( r = 1 \) and thus \( \chi_1 = \chi_2 \). Hence elements in \( \mathcal{H} \) are not similar to each other and take value 1 at \( \tilde{X} = \alpha \). Furthermore, by Proposition B.17 of [3], there are generators of \( \chi(H^0) \) that can be represented by polynomials in \( \mathcal{C}[\tilde{X}] \) with degree not greater than

\[
\kappa = (2n)^{3s^2} \left( \frac{n^2 + (2n)^3 s^2}{n^2} \right)^{\max_i \left\{ \left( \frac{n^2 + (2n)^3 s^2}{n^2} \right)^i \right\}}.
\]
A small modification of the method developed in [4] enables us to compute \( \mathcal{H} \).

Denote \( \bar{R}_{\leq k} = k[X]_{\leq k}/(Q_1 \cap \bar{k}[X])_{\leq k} \). Then \( R_{\leq k} \) is a \( \bar{k} \)-vector space of finite dimension. Moreover \( R_{\leq k} \) is a \( \delta \)-vector space, i.e. \( \delta(R_{\leq k}) \subset R_{\leq k} \). Assume that \( \{P_1, \ldots, P_s\} \) is a basis of \( R_{\leq k} \) where \( s = \dim(R_{\leq k}) \). Then there is a \( s \times s \) matrix \( B \) with entries in \( \bar{k} \) such that

\[
\delta \begin{pmatrix} P_1 \\ \vdots \\ P_s \end{pmatrix} = B \begin{pmatrix} P_1 \\ \vdots \\ P_s \end{pmatrix}.
\]

Suppose that \( h = \sum_{i=1}^s c_i P_i \) with \( c_i \in \bar{k} \) is hyperexponential over \( \bar{k} \), i.e. \( \delta(h) = rh \) for some \( r \in k \). An easy calculation yields that

\[
\delta \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} - r \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} = -B^t \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix}
\]

where \( B^t \) denotes the transpose of \( B \). Let \( \bar{h} \) be a hyperexponential element over \( k \) satisfying that \( \delta(\bar{h}) = -rh \) and \( c = (c_1, \ldots, c_s)^t \). Then \( \bar{c} h \) is a hyperexponential solution of \( \delta(Y) = -B^t Y \). The algorithm developed in [9] allows us to compute a \( C \)-basis of the solution space of \( \delta(Y) = -B^t Y \) that consists of hyperexponential solutions, say \( c_1 h_1, \ldots, c_d h_d \). Write \( c_i = (c_{i,1}, \ldots, c_{i,s}) \).

Then \( \sum_{j=1}^s c_{i,j} P_j \) is a hyperexponential element in \( R \) and one easily sees that \( \sum_{j=1}^s c_{i,j} P_j \) and \( \sum_{j=1}^s c'_{i,j} P_j \) are similar if and only if \( c_i = r c_i' \) for some nonzero \( r \in k \). Without loss of generality, we may assume that \( \{c_1, \ldots, c_d\} \) is a \( \bar{k} \)-basis of the vector space over \( \bar{k} \) spanned by \( c_1, \ldots, c_d \). Set \( h_i = \sum_{j=1}^s c_{i,j} P_j \) for all \( i = 1, \ldots, d' \). Multiplying a suitable element in \( k \), we may assume that \( h_i \) takes value 1 at \( \bar{X} = \alpha \). Then \( \{h_1, \ldots, h_d\} \) is the required set.

**Remark 3.4** One has that for a character \( \chi \) of \( H^\circ \), \( \chi(\alpha^{-1} \bar{X}) \) is actually a hyperexponential element over \( k(\alpha) \) in \( k(\alpha)[X, 1/\det(X)]/Q_1 \). So in practice computation, one only need to compute solutions that are hyperexponential over \( k(\alpha) \).

### 4 Maximal \( \delta \)-ideals in \( k[X, 1/\det(X)] \)

The previous section enables us to compute a maximal \( \delta \)-ideal in \( k[X, 1/\det(X)] \).

Now assume that we have such a maximal \( \delta \)-ideal \( \mathfrak{I} \) in hand. Suppose that \( \mathfrak{I} \) is generated by a finite set \( S \subset k[X, 1/\det(X)] \). Let \( \bar{k} \) be a finite Galois extension of \( k \) such that \( S \subset \bar{k}[X, 1/\det(X)] \). We define the action of \( \text{Gal}(\bar{k}/k) \) on an element \( f \in S \) to be the action of \( \text{Gal}(\bar{k}/k) \) to the coefficients of \( f \). Assume that \( \{\rho_1(S), \ldots, \rho_d(S)\} \) is the orbit of \( S \) under the action of \( \text{Gal}(\bar{k}/k) \). Denote

\[
\mathfrak{m} = k[X, 1/\det(X)] \cap_{i=1}^d \langle \rho_i(S) \rangle_{\bar{k}}
\]

where \( \langle \rho_i(S) \rangle_{\bar{k}} \) denotes the ideal in \( \bar{k}[X, 1/\det(X)] \) generated by \( \rho_i(S) \). We claim that \( \mathfrak{m} \) is a maximal \( \delta \)-ideal in \( k[X, 1/\det(X)] \). Since \( \cap_{i=1}^d \langle \rho_i(S) \rangle_{\bar{k}} \) is invariant under the action of \( \text{Gal}(\bar{k}/k) \), one has that

\[
\langle \mathfrak{m} \rangle_{\bar{k}} = \cap_{i=1}^d \langle \rho_i(S) \rangle_{\bar{k}}.
\]
Let $I$ be a maximal $\delta$-ideal in $k[X, 1/det(X)]$ containing $m$. Decompose $\langle I \rangle_{\bar{k}}$ into prime ideals in $\bar{k}[X, 1/det(X)]$:

$$\langle I \rangle_{\bar{k}} = Q_1 \cap \cdots \cap Q_s.$$ 

Since $\langle I \rangle_{\bar{k}}$ is a $\delta$-ideal, all $Q_i$ are $\delta$-ideals. Furthermore, one can verify that $\{Q_1, \ldots, Q_s\}$ is the orbit of $Q_1$ under the action of $\text{Gal}(\bar{k}/k)$. Because $\langle m \rangle_{\bar{k}} \subset \langle I \rangle_{\bar{k}}$, there exists $\rho \in \text{Gal}(\bar{k}/k)$ such that $\langle \rho(S) \rangle_{\bar{k}} \subset Q_1$. Remark that $\langle \rho(S) \rangle_{\bar{k}}$ is a maximal $\delta$-ideal as so is $\langle S \rangle_{\bar{k}}$. Thus $\langle \rho(S) \rangle_{\bar{k}} = Q_1$. Therefore

$$\langle m \rangle_{\bar{k}} = \cap_{i=1}^d \langle \rho_i(S) \rangle_{\bar{k}} = Q_1 \cap \cdots \cap Q_s = \langle I \rangle_{\bar{k}}$$

which implies that $m = I$, because $m = \langle m \rangle_{\bar{k}} \cap k[X, 1/det(X)]$ and $I = \langle I \rangle_{\bar{k}} \cap k[X, 1/det(X)]$. This proves our claim.

References

[1] Amzallag, E., Minchenko A. and Pogudin G., Degree bound for toric envelope of a linear algebraic group, arxiv.org/abs/1809.06489v3, 2018.

[2] Compoint, E. and Singer, F., Computing Galois groups of completely reducible differential equations, J. Symbolic Comput., 11, 1-22, 1998.

[3] Feng, R., Hrushovski’s algorithm for computing the Galois group of a linear differential equation, Adv. in App. Math., 65, 1-37, 2015.

[4] Feng, R. On the computation of the Galois groups of linear difference equations, Math. Comp., 87, 941-965, (2018). DOI:10.1090/mcom/3232.

[5] Fried, D.M. and Jarden, M., Field arithmetic, Springer-Verlag, Berlin, 1986.

[6] Magid, A.R., Finite generation of class groups of rings of invariants, Proc. Amer. Math. Soc., 60 (1976), 45C48 (1977). MR0427306.

[7] Hrushovski, E. Computing the Galois group of a linear differential equation. Banach Center Publ. 58, 97-138, 2002.

[8] Singer, M.F., Algebraic relations among solutions of linear differential equations, Trans. Amer. Math. Soc., 295 (1986), no. 2, 753C763, DOI 10.2307/2000662. MR833707.

[9] Singer, M.F.M., Liouvillian solutions of linear differential equations with liouvillian coefficients, J. Symbolic Comput., 11,251C274, 1991.

[10] Van der Put M. and Singer, M., Galois Theory of Linear Differential Equations, Springer-Verlag, Berlin Heidelberg, 2003.