Liouvillian Solutions of Ordinary Linear Difference Equations

Raphaël Bomboy

INRIA Sophia Antipolis
2004, route des Lucioles, B.P. 93
06 902 SOPHIA ANTIPOLIS, FRANCE
Raphael.Bomboy@sophia.inria.fr

Abstract. We give an algorithm for computing liouvillian solutions of an ordinary linear difference equation which involves only computations of rational solutions of auxiliary systems of equations and computations of hypergeometric solutions of such systems which do not involve extension of the coefficient field.

1 Introduction

Peter Anne Hendriks and Michael F. Singer give in [5] a definition of *liouvillian* solutions of ordinary linear difference equations. They also give an algorithm for computing a basis of the space of liouvillian solutions of such an equation. However, that algorithm is based on the computation of the *hypergeometric* solutions of a family of associated operators. Algorithms for computing such solutions have been given in [8] (See also [12]), but they can imply numerous computations in some extensions of the coefficient field of the operator, which can be very costly.

We adapt here the ideas given for differential equations by Michael F. Singer in [10] to give an algorithm for computing liouvillian solutions of ordinary linear difference equations which uses as far as possible computations of rational (i.e. *in the coefficient field*) solutions of associated systems.

In some cases, it may happen that our algorithm needs to compute hypergeometric solutions of associated systems. However, in that case, we show that we just need to compute such solutions *without extending the coefficient field*.

A partial version of this algorithm for order two equations has been implemented in the Maple package LREfactor[1]. Note that LREfactor call the Aldor library $\sum^{it}$ by using SHASTA[2]. As far as we know, this is the first attempt to implement an algorithm for computing liouvillian solutions of linear ordinary difference equation.

The rest of the article is organized as follow. Section 2 and 3 contain general results on Galois theory and reducibility of linear difference equations and systems.

In section 4, we define the Eigenring of a equation or system and show how computing successive Eigenrings give us a first decomposition algorithm (subsection 4.2).

Since these sections are essentially expository, we did not include proofs. One can find a full description of the Galois theory in [11] (see also [3]) and a full study of reducibility properties of an operator or system in [3].

In section 5, we define *liouvillian* sequences. The most important result of that section is corollary 1, which shows that an irreducible equation admiting a liouvillian solution has such a solution of particular form.

Section 6 is devoted to our algorithm. We first show in subsection 6.1 and 6.2 how to obtain a basis of the space of liouvillian solutions of an operator from the basis of liouvillian solutions of its factors. We can then give a full algorithm for computation of the liouvillian solutions of an equation in subsection 6.3.

We conclude by some examples.

2 Galois Theory

A *difference ring* (respectively *difference field*) (R, σ) is a ring (respectively field) R together with an injective endomorphism $\sigma : R \to R$. We say that a ring (R_1, σ_1) can be embedded in (R_2, σ_2) if and only

[1] www.inria.fr/cafe/Raphael.Bomboy/en-index.html
[2] www.inria.fr/cafe/Manuel.Bronstein/sumit

if R_1 can be embedded in R_2 and the restriction of σ_2 to R_1 coincide to σ_1. In that case, we will often use the same notation for σ_1 and σ_2.

Let $k = C(z)$ be the field of rational fractions in one indeterminate z with coefficients in a field C of characteristic 0, and σ the morphism letting C invariant and sending z to $z + m$, where m is a positive integer. In this paper, we consider *ordinary difference equations*, i.e. equations of the form

$$\sigma^n(x) + a_{n-1}\sigma^{n-1}(x) + \ldots + a_0 x = 0 \tag{1}$$

where $a_0, \ldots, a_{n-1} \in k$ and $a_0 \neq 0$.

We will also need ordinary linear difference *systems* of order n, i.e. systems of the form

$$\sigma(X) = AX \tag{2}$$

where $A \in Gl_n(k)$ and X is a vector of n indeterminates.

Note that we can associate to the linear equation (1) the system $\sigma(X) = A_L X$, where

$$A_L = \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ -a_{n-1} & \ldots & \ldots & -a_0 \end{pmatrix}$$

is the companion matrix of the equation. It will allow us to restrict ourself to linear difference system for the further definitions.

Let C be a field of characteristic 0. Consider the ring of sequences with coefficients in C. One can define an equivalence relation on this ring by identifying two sequences which are equal except for a finite number of terms. We denote by $\mathcal{S}$ the quotient of the ring of sequences by this relation. One can define on $\mathcal{S}$ the shift morphism σ sending the sequence $(a_0, \ldots, a_n, \ldots)$ to $(a_1, \ldots, a_{n+1}, \ldots)$.

The difference ring $(C(z), \sigma)$ can be embedded in $(\mathcal{S}, \sigma)$ by sending a rational function to the sequence $(F(0),\ldots,F(\frac{n}{m}),\ldots)$ and completing the sequence arbitrary at the points where F is not defined if necessary.

We call a sequence $a \in \mathcal{S}$ *rational* if and only if $a \in C(z)$. We call it hypergeometric if and only if there is a rational sequence b such that $\sigma(a) = ba$ (note that rational sequences are hypergeometric).

Assume that C is algebraically closed. We define the *Picard-Vessiot extension* of (2) as the subring of $\mathcal{S}$ generated by the solutions of the system.

The set V of solutions of (2) in $\mathcal{S}$ is called the *solution space* of the system. It is a C-vector space of dimension n. A *fundamental system of solutions* of (2) is a invertible matrix $X \in Gl_n(R)$ such that $\sigma(X) = AX$.

Note that in the case where C is not algebraically closed, we can alway consider (2) as a system with coefficients in the extended field $\overline{C}(z)$. In that case, the Picard-Vessiot extension and solution space of the system are defined as the Picard-Vessiot extension and solution space of the system *seen as a system with coefficients in* $\overline{C}(z)$.

Let R be the Picard-Vessiot extension of (2). The *Galois group* G of the system is the set of isomorphisms of R commuting with σ and fixing k pointwise. It is a linear algebraic subgroup of $Gl_n(C)$.

3 Reducibility

Define now the notion of reducibility of a linear difference equation.

The ring $k[E;\sigma]$ of the *skew polynomials* with coefficients in k is the ring of polynomials in one variable E together with the product defined by $E * a = \sigma(a)E$ for all $a \in k$. The product of two skew polynomials $L_1 * L_2$ will often be noted $L_1 L_2$.

The ring $k[E;\sigma]$ is a non-commutative ring, both left and right Euclidean. We call its elements *operators*.

We can associate to any linear difference equations of the form (1) the operator $L = E^n + a_{n-1}E^{n-1} + \ldots + a_0$.

An operator L of order n is *reducible* if and only if there are nontrivial L_1 and L_2 in $k[E;\sigma]$ such that $L = L_1L_2$. It is *decomposable* if and only if there are operators L_1, L_2 or respective orders n_1, n_2 such that $L = llcm(L_1, L_2)$ and $n = n_1 + n_2$.

We state now the link between the divisibility properties of an operator and the structure of its solution space (for a deeper study, see [3]).

Proposition 1. *1. P is a right factor of L if and only if the solution space of P is included in the solution space of L. Moreover, in that case, the Galois group of P is a quotient group of the Galois group of L.*

2. L is reducible if and only if its solution space V has a proper G-invariant subspace.

3. L is decomposable if and only if its solution space V has two proper G-invariant subspace V_1 and V_2 such that $V = V_1 \oplus V_2$.

The decomposition of an operator into irreducible operators is not necessarily unique. However, we have a partial result.

Two operators L and P are said to be *equivalent* if and only if there exists $L_1 \in k[E;\sigma]$, such that L_1 and P have no nontrivial common right factor and LL_1 is divisible by P on the right. This is equivalent to saying that they have G-isomorphic solution spaces.

Theorem 1. *[7, Theorem 1]*
Let $L = P_1 \dots P_k$ and $L = Q_1 \dots Q_l$ two factorization of L into irreducible linear difference operators. Then $k = l$ and the factors are equivalent in pair.

We can extend our definitions of reducibility and decomposability to linear difference systems. We say that two linear systems $\sigma(X) = AX$ and $\sigma(X) = BX$ are *equivalent* if and only if there is $P \in Gl_n(k)$ such that $\sigma(P)AP^{-1} = B$. A linear system $\sigma(X) = AX$ is *reducible* if and only if it is equivalent to a system of the form

$$\sigma(X) = \begin{pmatrix} A_1 & A_2 \\ & A_3 \end{pmatrix} X \tag{3}$$

It is *decomposable* if and only if it is equivalent to a matrix of the form

$$\sigma(X) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_p \end{pmatrix} X \tag{4}$$

The results of 1 remains true for linear difference system. Moreover, a linear difference equation is reducible (respectively decomposable) if and only if the associated system is reducible (respectively decomposable).

4 Eigenring and Decomposition

4.1 The Eigenring

We can now define the notion of Eigenring of a operator.

Definition 1. *The Eigenring $\mathcal{E}(L)$ of L is the set of equivalence classes $\overline{P} \in k[E;\sigma]/k[E;\sigma]L$ such that LP is divisible by L on the right.*

Note that $\mathcal{E}(A)$ is a C-vector space.

Each element of $\mathcal{E}(L)$ induces a G-endomorphism of the solution space V of L. Furthermore, one can show that every element of $End_G(V)$ is of this type (see [3, Prop. 41]).

Let us extend now our definition of Eigenring to linear difference system.

Definition 2. *The Eigenring $\mathcal{E}(A)$ of (2) is the set of $B \in Gl_n(k)$ such that $\sigma(B)A = AB$.*

Once again, one can show that $\mathcal{E}(A)$ is in bijection with $End_G(V)$ (see [3, Prop. 44]). As awaited, the Eigenring of an equation is in bijection with the Eigenring of the associated system.

By definition, computing the Eigenring of an order n linear difference operator or system means to compute the rational solutions of a linear difference system of order n^2. An algorithm for solving this type of system is given was [2]. However, our package LREfactor compute Eigenring by calling the $\sum^{it}$ library, which uses a new algorithm for computing rational solutions that is described in [1].

Note that in the case where C is not algebraically closed, we defined the Picard-Vessiot extension of L as being the Picard-Vessiot extension of L seen as an operator with coefficients in $\overline{C}(z)$. Hence the Eigenring of this system is *a priori* a vector space of matrix with coefficients in $\overline{C}(z)$. However, the next result ensure us that we can compute the Eigenring by restricting ourself to compute rational solutions *in* $C(z)$ of the associated system.

Proposition 2. *[3, Lemme 18] $\mathcal{E}(A)$ has a basis consisting of matrices with coefficients in $C(z)$.*

4.2 The Decomposition Algorithm

We can now show how the computation of the Eigenring can help us to factorize a linear difference system.

Let $\sigma(X) = AX$ be a linear difference system with coefficients in $C(z)$, where C is a non necessary algebraically closed field of characteristic 0.

Schur's lemma ensure us if $\sigma(X) = AX$ is irreducible, it has a trivial Eigenring (for Schur's lemma, see for example [6, ch. XVII]). Furthermore, in [2], the author how to explicitely construct a right factor of the system from a nontrivial element of the Eigenring.

When the system is not only reducible, but decomposable, we can say more.

The next lemma has been suggested to me by Michael F. Singer in [9].

Lemma 1. *The system $\sigma(X) = AX$ is indecomposable if and only if any element of $\mathcal{E}(A)$ has an unique eigenvalues.*

Once again, we can give a constructive version of the above lemma.

Lemma 2. *[3, lemme 19] Let $B \in \mathcal{E}(A)$, $\lambda_1, \dots, \lambda_p$ the Eigenvalues of B and $n_1, \dots, n_p$ their respective orders. Then one can construct a system equivalent to A of the form*

$$\sigma(X) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_p \end{pmatrix} X \tag{5}$$

where $\sigma(X) = A_i X$ is a system of order n_i with coefficients in $C(\lambda_1, \dots, \lambda_i)(z)$ for all $i \in \{1, \dots, p\}$.

Iterated applications of lemma 2 give us an algorithm of decomposition of a system in indecomposable factors.

Theorem 2. *[3, Prop. 46]*
By recursive computation of Eigenring, one can construct a linear difference system equivalent to $\sigma(X) = AX$ of the form

$$\sigma(X) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_p \end{pmatrix} X \tag{6}$$

where each of the system $\sigma(X) = A_i X$ is indecomposable.
Moreover, if $A = A_L$ is the companion system of a linear difference operator L, each of the block $\sigma(X) = A_i X$ is the companion system of an operator L_i of order n_i, and $L = llcm(L_1, \sigma^{-n_1}(L_2), \dots, \sigma^{-(n_1+\dots+n_{p-1})}(L_p))$.

For an example of application of theorem 2, see section 6.4 below.

5 Liouvillian Sequences

5.1 Sections, Spreads, Interlacings

Before being able to define liouvillian solutions of linear difference equations, we need to study sections and spreads of sequences.

Definition 3. *Let* $a = (a(n))_{n\in\mathbb{N}} \in \mathcal{L}$.

The i^{th} *m-spread of a is the sequence* $a^{\overrightarrow{m}+i}$ *defined by*

$$a^{\overrightarrow{m}+i}(kn+i) = a(k)$$

for all $k \in \mathbb{N}$ *and* $a^{\overrightarrow{m}+i}(n) = 0$ *for all* $n \in \mathbb{N}$ *such that* $n \neq i \bmod m$.

The i^{th} *m-section of a is the sequence defined by* $a^{\overleftarrow{m}-i}(n) = a(mn+i)$.

Note that for all $a \in \mathcal{S}$, $(a^{\overrightarrow{m}+i})^{\overleftarrow{m}-i} = a$. Furthermore, we have $\sigma(a^{\overrightarrow{m}+i}) = a^{\overrightarrow{m}+i-1}$ and $\sigma(a^{\overleftarrow{m}-i}) = a^{\overleftarrow{m}-m+i}$.

For all matrices X with coefficients in $\mathcal{S}$, we note $X^{\overrightarrow{m}+i}$ (respectively $X^{\overleftarrow{m}-i}$) the matrix whose coefficients are the i^{th} m-spread (respectively the i^{th} m-section) of the coefficients of X.

Definition 4. *Let* $a_1, \ldots, a_m \in \mathcal{S}$. *The interlacing of* $a_1, \ldots, a_m$ *is the sequence*

$$\biguplus_{1\leq i\leq m} a_i = \sum_{1\leq i\leq m} a^{\overrightarrow{m}+i-1} = (a_1(0), \ldots, a_m(0), a_1(1), \ldots)$$

We define now the notion of iterated system of a linear difference system. These systems are closely related to the section of the solutions of the initial system.

Definition 5. *Let m be a positive integer. The* m^{th} *iterated system associated to* $\sigma(X) = AX$ *is the system*

$$\sigma^m(X) = \sigma^{m-1}(A)\ldots AX \tag{7}$$

seen as a system with coefficients in (k, σ^m).

We note $\prod_m^\sigma A$ the matrix $\sigma^{m-1}(A)\ldots A$.

Note that by induction, each fundamental system of solutions of $\sigma(X) = AX$ is a fundamental system of solutions of $\sigma^m(X) = (\prod_m^\sigma A)X$.

5.2 Liouvillian Sequences

We can now define the notion of *liouvillian* sequence.

Definition 6. *The ring* $\mathcal{L}$ *of liouvillian sequences is the smallest subring of* $\mathcal{S}$ *such that*

1. $C(z) \subset \mathcal{L}$
2. *if* $a \in C(z)$ *and b is a solution of* $\sigma(x) = ax$, $b \in \mathcal{L}$
3. *if* $a \in \mathcal{L}$ *and b is a solution of* $\sigma(x) = a + x$, $b \in \mathcal{L}$
4. *if* $a_1, \ldots, a_m \in \mathcal{L}$, $\biguplus_{1\leq i\leq m} a_i \in \mathcal{L}$

As in classical and differential Galois theories, there is a connection between integrability in finite terms and equations with solvable Galois groups.

Theorem 3. *[5, Theorem 3.4] A sequence a is liouvillian if and only if there exists an operator L such that a is a solution of L and L has a solvable Galois groups.*

We let the reader refer to the above article for a proof.

The aim of the rest of this section is to show that if an operator has a liouvillian solution, it has such a solution of particular form.

The following result could have been seen has as a consequence of proposition 4. However, we thought it was more natural to prove it directly.

Proposition 3. *An irreducible ordinary linear difference operator L has a liouvillian solution if and only if all its solutions are liouvillian.*

Proof. Let a be such a solution. By theorem 3, there is a linear difference operator P such that $P(a) =$ and P has a solvable Galois group. Let $Q = grcd(L, P)$. Since P and L have a common solution, Q is nontrivial by proposition 1 and since L is irreducible, $Q = L$ and L is a right factor of P. By proposition 1, the Galois group of L is a quotient group of the Galois group of P, so its solvable. By theorem 3, it follows that every solutions of L are liouvillian.

The next proposition shows that if an irreducible operator has a liouvillian solution, it has a solution of particular form.

Proposition 4. *([5, 4.1 to 5.1] ; [3, Prop. 55]) Let L be an irreducible linear difference operator of order n. The following are equivalent.*

1. *L has a liouvillian solution.*
2. *there exists $a \in k$ such that L is equivalent to the system*

$$A_L = \begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ a & 0 & \dots & 0 \end{pmatrix}$$

3. *L has a solution which is the interlacing of n hypergeometric sequences.*

We let the reader see the above references for a proof.

The following corollary will be used in our algorithm for computing liouvillian solutions of an operator.

Corollary 1. *Let L be an irreducible linear difference operator of order n. The following are equivalent.*

1. *L has a liouvillian solution.*
2. *All solutions of L are liouvillian.*
3. *The iterated operator $\sigma^n(X) = (\prod_n^\sigma A_L)X$ is diagonalizable.*

Moreover, given a diagonalization of the iterated system, one can compute an explicit basis of solutions of L.

Proof. The equivalence between (1) and (2) was already proved in proposition 3.

(1) ⇒ (3) Assume that L has a liouvillian solutions. By proposition 4, $\sigma(X) = A_L X$ is equivalent to a system of the form

$$\begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ a & 0 & \dots & 0 \end{pmatrix}$$

hence $\sigma^n(X) = (\prod_n^\sigma A_L)X$ is diagonal.

(3) ⇒ (2) Assume now that there exists $P \in Gl_n(k)$ such that the matrix $\sigma^m(P)(\prod_m^\sigma A_L)P^{-1}$ is of the form

$$\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

Let $B = \sigma(P)A_L P^{-1}$. Note that

$$\begin{aligned} \textstyle\prod_m^\sigma B &= \sigma^m(B)\sigma^{m-1}(A)\sigma^{m-1}(B^{-1})\sigma^{m-1}(B)\dots AB \\ &= \sigma^m(P)(\textstyle\prod_m^\sigma A_L)P^{-1} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \end{aligned}$$

Let $N \in \mathbb{N}$ such that for all $k \geq N$, $d_1(k) \dots d_n(k) \neq 0$. We define a fundamental system of solutions of $\sigma(X) = BX$ by $X(N) = Id$ and $X(k+1) = BX(k)$ for all $k \geq N$.

Let (x_{ij}) be the coefficients of X. One can verify that for all (i,j) and for all $l \in \{0,\dots,n-1\}$ the l^{th} n-section of x_{ij} is a hypergeometric sequence. Finally, $Y = PX$ is a fundamental system of solutions of $\sigma(X) = AX$, whose coefficients are linear combinations with coefficients in $C(z)$ of coefficients of X, hence are liouvillian.

Note that proposition 4 admits a generalization to non necessarily irreducible operators (see [5, Theorem 5.1]). However, we do not need it for our algorithm.

6 The Algorithm

6.1 Reconstruction of the Liouvillian Solutions

Before describing our algorithm, we need to show how to reconstruct the liouvillian solutions of a operator from the liouvillian solutions of its right factors.

Consider first the case where L is the least left common multiple of a finite set of operators.

Let L be an linear operator of order n and $L_1,\dots,L_p$ be operators of respective orders $n_1,\dots,n_p$ such that L is the left least common multiple of $L_1,\dots,L_p$ and $n = n_1 + \dots + n_p$.

Let V be the solution space of L and V_i be the solution space of L_i for all $i \in \{1,\dots,p\}$. By proposition 1, $V_1 + \dots + V_p = V$, and, since $n = n_1 + \dots + n_p$, $V = V_1 \oplus \dots \oplus V_p$.

Let $i \in \{1,\dots,p\}$ and $\widetilde{L_i} = llcm_{j\neq i}(L_i)$. By proposition 1, the solution space of $\widetilde{L_i}$ is $\oplus_{j\neq i} V_j$. Moreover, since $\oplus_{j\neq i} V_j$ and V_i are in direct sum, $\widetilde{L_i}$ and L_i have no common right factor. Hence, by Bezout's theorem, there exists $P, \widetilde{P} \in k[E;\sigma]$ such that

$$PL_i + \widetilde{P}\widetilde{L_i} = 1$$

Lemma 3. *Let Π_i be the natural projection of V onto V_i for all $i \in \{1,\dots,p\}$. For all $x \in \mathcal{S}$, $\Pi_i(x) = \widetilde{P}\widetilde{L_i}(x)$, where $\widetilde{P}$ is defined as above.*

Proof. Since $PL_i + \widetilde{P}\widetilde{L_i} = 1$, $PL_i(x) + \widetilde{P}\widetilde{L_i}(x) = x$. Let us show that $P_iL_i(x) \in V_i$ and $\widetilde{P}\widetilde{L_i}(x) \in \oplus_{j\neq i} V_j$.

Let $Q = L_i\widetilde{P}\widetilde{L_i}$; Q is a left multiple of $\widetilde{L_i}$, and, since $Q = L_i(1 - P_iL_i) = (1 - L_iP)L_i$, Q is a left multiple of L_i. Hence L is a right factor of Q and, since x is a solution of L, $L_i(\widetilde{P}\widetilde{L_i}(x)) = Q(x) = 0$. Similarly, $\widetilde{L_i}(P_iL_i(x)) = 0$ and $x \in \oplus_{j\neq i} V_j$, that concludes.

Proposition 5. *Let L be a ordinary linear operator of order n and $L_1,\dots,L_p$ be a finite number of operators of respective orders $n_1,\dots,n_p$ such that $L = llcm(L_1,\dots,L_p)$ and $N = n_1 + \dots + n_p$. Let $\widetilde{V}$ be the space of liouvillian solutions of L and $\widetilde{V_i}$ be the space of liouvillian solutions of L_i for all $i \in \{1,\dots,p\}$. Then*

$$\widetilde{V} = \widetilde{V_1} \oplus \dots \oplus \widetilde{V_p}$$

Proof. For all $i \in \{1,\dots,p\}$, $\widetilde{V_i} \subset V_i$, hence the space $\widetilde{V_i}$ are in direct sum. Since a sum of liouvillian sequences is liouvillian, $\widetilde{V_i} \oplus \dots \oplus \widetilde{V_i} \subset \widetilde{V}$. Consider now x a liouvillian solutions of L ; $x = x_1 + \dots + x_p$, where $x_i \in V_i$ for all i. Furthermore, since $x_i = \widetilde{P_i}\widetilde{L_i}(x)$ by lemma 3, $x_i \in \widetilde{V_i}$.

We turn now to the case where L is a reducible indecomposable operator. Although these results were prooved in [5], we choose to include full proofs to make the presentation complete.

Proposition 6. *[5, lemma 5.4] Let L be an ordinary linear difference operator of order n and $L = L_1L_2$ a factorisation of L in two nontrivial operators of order p and q. Then*

1. if $\{u_1,\dots,u_n\}$ is a basis of the solution space of L, one can compute a set of vectors $\{(c_{i1},\dots,c_{in})\}_{1\leq i\leq q}$ with coefficients in k such that

$$w_1 = \sum_{1\leq j\leq n} c_{1j}u_j, \dots, w_q = \sum_{1\leq j\leq n} c_{qj}u_j$$

is a basis of solutions of L_2

2. if $w_1, \ldots w_q$ is a basis of L_2 and v a solution of L_1, one can compute a set of sequences $c_1, \ldots, c_q \in \mathcal{S}$ such that $\sum_{1 \le i \le q} c_i w_i = v$.

Moreover, the sequences c_i can be obtained from v and the w_i by using σ, field operations and finite summations.

Proof. 1. Let $x_1, \ldots, x_n$ be constant indeterminates. We want to determine conditions on the x_i such that $u = x_1 u_1 + \ldots + x_n u_n$ is a solution of L_2.

Let $v = L_2(u)$ and, for all $i \in \{1, \ldots, p\}$, $v_i = L_2(u_i)$. Let N be an integer greater than all the poles and zeroes of the coefficients of L, L_1 and L_2.

Assume that $L_2(u) = \sum_{1 \le i \le n} x_i v_i = 0$. For all $k \in \{0, \ldots, p-1\}$, we have

$$v(k) = \sum_{1 \le i \le n} x_i v_i(N + k) = 0 \tag{8}$$

Assume now that $x_1, \ldots, x_n$ satisfy (8) for all $k \in \{0, \ldots, p-1\}$. Since v is a solution of L_1 and L_1 is of order p, $v(k) = 0$ for all $k \in \mathbb{N}$, i.e. $v = L_2(u) = 0$. Hence the space of solutions of (8) is of dimension q and a basis of solutions $\{(c_{i1}, \ldots, c_{in})\}_{1 \le i \le q}$ of this equation gives a basis of solutions of L_2.

2. This part of the result is proved by using a difference version of the variation of the parameters. Let M be the $p \times p$ matrix of coefficients $(\sigma^{j-1}(w_i))_{1 \le i,j \le p}$ and B be the column vector whose $p-1$ first rows are equal to zero and last row is equal to v. For all $w \in \mathcal{S}$, $L_2(w) = 0$ if and only if the vector $(w, \ldots, \sigma^{p-1}(w))^t$ is a solution of $\sigma(X) = A_{L_2} X + B$.

Let C be a vector of p indeterminates. A short computation shows that MC is a solution of $\sigma(X) = A_{L_2} X + B$ if and only if and only if C is a solution of $\sigma(C) - C = (A_{L_2} M)^{-1} B$. This last equation has a solution of the desired form, that concludes.

Those results allow one to construct a basis of solution of L from basis of solutions L_1 and L_2.

Corollary 2. *Let $v_1, \ldots v_p$ be a basis of solutions of L_1, $w_1, \ldots, w_q$ be a basis of solutions of L_2. Then one can compute from the v_i and w_i a basis of solutions $u_1, \ldots, u_n$ of L such that*

1. $\forall i \in \{1, \ldots, q\}$, $u_i = w_i$
2. $\forall i \in \{1, \ldots, p\}$, $L_2(u_{q+i}) = v_i$

Moreover, if all solutions of L_2 are liouvillian and there exists $r \le p$ such that $v_1, \ldots, v_r$ is a basis of the space of liouvillian solutions of L_1, $\{u_1, \ldots, u_{q+r}\}$ is a basis of the space of liouvillian solutions of L.

Proof. By proposition 6, one can construct a family $u_1, \ldots, u_n$ such that $u_i = w_i$ for all $i \in \{1, \ldots, q\}$ and $L_2(u_{q+i}) = v_i$ for all $i \in \{1, \ldots, p\}$. One can check that $\{u_1, \ldots, u_n\}$ is free, hence is a basis of solutions of L.

Moreover, if $w_1, \ldots, w_q$ and $v_1, \ldots v_r$ satisfy the conditions of the second part of the proposition, $u_1, \ldots, u_{p+r}$ are liouvillian by the second part of proposition 6. We need to show that these sequences generate the full space of solutions of L. Let u be a liouvillian solution of L ; $L_2(u)$ is liouvillian, and is a solution of L_1. It follows that the dimension of the space of liouvillian solution of L is smaller than $q + r$, that concludes.

6.2 Indecomposable Operators

The proposition 7 is a keystone of our algorithm. It shows that if L is an indecomposable operator with coefficients in $C(z)$, where C is non necessary algebraically closed, we need to search only right factor of L *in that field*, without extending our coefficients field to $\overline{C}(z)$.

Proposition 7. *Let L be a indecomposable linear difference operator with coefficients in $C(z)$, where C is a non necessary algebraically closed field of characteristic 0. If L has a liouvillian solution, it admits a nontrivial right factor P with coefficients in $C(z)$ such that all solutions of P are liouvillian.*

Proof. Let a be a liouvillian solution of L. By theorem 3, a is solution of an operator Q such that Q has a solvable Galois group. Let $R = grcd(L, Q)$ and S be an irreducible right factor of R. The operator S is a right factor of L. Moreover, since S is a right factor of Q, its Galois group is the quotient of the Galois group of G, hence is solvable, and all its solutions are liouvillian.

Let now l be the extension of C generated by the coefficients of S, and G be the (classical) Galois group of l over C. The group G is finite; let $\{g_0, \dots, g_{k-1}\}$ be its elements and $P = llcm(g_0(S), \dots, g_{k-1}(S))$. The operator P is a right factor of L, and, since L is indecomposable, $P \neq L$. Moreover, since $g(P) = P$ for all $g \in G$, the coefficients of P belong in C by separability. Finally, by proposition 1. the solution space of P is the sum of the solutions spaces of the $g_i(Q)$. Moreover, for all $i \in \{0, \dots, k-1\}$ all solutions of $g_i(Q)$ are liouvillian, hence all solutions of P are liouvillian.

In [4], the authors give an algorithm to compute right factors of linear difference operator. This algorithm is based upon the following idea :

1. constructing a family of associated linear difference operators $(L_m)_{1 \leq m < n}$
2. for each m, computing the hypergeometric solutions of L_m.

Hypergeometric solutions of L_m give then candidates for the order m right factors of L_m.

If the coefficients of L lie in $k = C(z)$, where C is not necessarily algebraically closed, the coefficients of L_m lie in k. Moreover, for computing right factors of L with coefficients in k, one just need to search hypergeometric solutions *over* k of L_m, which avoid computations in extensions of C (see [8]).

Note that the fact that L has a right factor in $k[E; \sigma]$ with a full space of liouvillian solutions does not imply that all right factor of L with coefficients in k have a full space of liouvillian solutions. However there exists a factorization $L = Q_1 \dots Q_l$ of L in $k[E; \sigma]$ such Q_l has only liouvillian solutions, and, by theorem 1, for any factorization $L = P_1 \dots P_k$ of L into irreducible factors, $k = l$ and there exists $i \in \{1, \dots, k\}$ such that P_i is equivalent to Q_l, hence has only liouvillian solutions.

6.3 Full Algorithm

We can now describe our algorithm for computing liouvillian solutions of an ordinary linear difference operator.

Let L be such an operator and $\sigma(X) = A_L X$ the associated system.

First step. By using our decomposition algorithm of subsection 4.2, put $\sigma(X) = A_L X$ in the form liouvillian solutions

$$\sigma(X) = \begin{pmatrix} A_{L_1} & & \\ & \ddots & \\ & & A_{L_p} \end{pmatrix} X \tag{9}$$

where $\sigma(X) = A_{L_i} X$ is the companion system of an indecomposable operator of order n_i for all $i \in \{1, \dots, p\}$.

The operator L is the left least common multiple of L_1, $\sigma^{-n_1}(L_2)$, $\dots$, $\sigma^{-n_1+\dots+n_{p-1}}(L_p)$. Hence by proposition 5, we just need to compute a basis of the space of liouvillian solutions of each system $\sigma(X) = A_{L_i} X$ to obtain a basis of solutions of the space of liouvillian solutions of L.

Let $\sigma(X) = A_{L_i} X$. If the system is of order 1, its solution space is trivially generated by an hypergeometric solution.

If not, $\sigma(X) = A_{L_i} X$ is either irreducible, or reducible and indecomposable.

In the first case, we know by corollary 1 that if L_i has a liouvillian solution, the iterated system $\sigma^{n_i}(X) = (\prod_{n_i}^{\sigma} A_{L_i})X$ must be diagonalizable. This gives us the way to follow.

Second step. 1. Compute the iterated system $\sigma^{n_i}(X) = (\prod_{n_i}^{\sigma} A_{L_i})X$. Then compute its Eigenring and try to factorize $\sigma^{n_i}(X) = (\prod_{n_i}^{\sigma} A_{L_i})X$ by using the decomposition Eigenring of subsection 4.2.

If $\sigma^{n_i}(X) = (\prod_{n_i}^{\sigma} A_{L_i})X$ is diagonalizable this way, all solutions of $\sigma^{n_i}(X) = (\prod_{n_i}^{\sigma} A_{L_i})X$ are liouvillian and one can compute a basis of solutions of this system as explained in corollary 1.

2. Assume that it is not the case.

If L_i has a liouvillian solutions, by proposition 7, for all $L_i = P_1 \dots P_k$ factorization of L_i into irreducible linear difference operators with coefficients in $C(z)$, there exists $i \in \{1, \dots, k\}$ such that P_i has only liouvillian solutions.

Search now if L_i has such a factorization.

Proceed by induction on n. One can search a right factor P of L_i with coefficients in $C(z)$ of minimal order as explained in section 6.2. Since P is of minimal order, it is irreducible in $k[E;\sigma]$.

If $P = L_i$, i.e. L_i is irreducible, this part of the algorithm end and L_i has no liouvillian solution. Otherwise, put L_i in the form $\widetilde{L_i}P$ where P is as above. Test then if all the solutions of P are liouvillian by applying recursively our algorithm for computing such solutions.

If not, search if $\widetilde{L_i}$ has a right factor all of whose solutions are liouvillian, and so on.

This part of the algorithm end when either we obtain a factorization $L_i = P_1 \dots P_k$ of L_i where no P_i has liouvillian solution, or we obtain a decomposition $L_i = \widetilde{L_i}P_1 \dots P_k$ where P_1 has a full set of liouvillian solutions. In the first case, L_1 has no liouvillian solutions. In the second case, we know by theorem 1 that P_1 similar to a right factor Q_1 of L. Moreover, one can compute this factor as explain in [7].

Put L in the form $L = QQ_1$ and compute recursively a basis of the space of liouvillian solutions of Q. Corollary 2 allows then to compute a basis of the space of liouvillian solutions of L from the liouvillian solutions of Q and Q_1.

6.4 Examples

Example 1. Let L be the operator $E^2 + \frac{1}{n-1}E - \frac{n^2}{n-1}$.

A computation with SHASTA shows that the Eigenring of the associated system is trivial.

The second iterated system associated to L has for matrix of coefficients

$$\Pi_2^\sigma A_L = \sigma(A_L)A_L = \begin{pmatrix} \frac{n^2}{n-1} & -\frac{1}{n-1} \\ -\frac{n}{n-1} & -\frac{n^2+n-1}{n-1} \end{pmatrix}$$

A new computation shows that this system has a dimension two Eigenring whose matrix $B_1 = Id$ and

$$B_2 = \begin{pmatrix} \frac{1}{n-1} & -\frac{1}{n-1} \\ \frac{n}{n-1} & -\frac{n}{n-1} \end{pmatrix}$$

are a basis.

The matrix B_2 has two Eigenvalues $\lambda_0 = 0$ and $\lambda_1 = 1$ of order 1 each. By our decomposition algorithm, we find

$$P = \begin{pmatrix} 1 & -\frac{1}{n} \\ \frac{n}{n-1} & 0 \end{pmatrix}$$

such that

$$\sigma^2(P)(\Pi_2^\sigma A_L)P^{-1} = \begin{pmatrix} n+1 & 0 \\ 0 & n+2 \end{pmatrix} \quad \text{and} \quad \sigma(P)AP^{-1} = \begin{pmatrix} 0 & -1 \\ -(n+1) & 0 \end{pmatrix}$$

Let $B = \sigma(P)AP^{-1}$. Define a sequence of matrix $X(n)$ by $X(0) = Id$ and $X(n+1) = BX(n)$. By induction one can verify that for all $p \in \mathbb{N}$,

$$X(2p) = \begin{pmatrix} 1...(2p-1) & 0 \\ 0 & 1...(2p) \end{pmatrix} \quad \text{and} \quad X(2p+1) = \begin{pmatrix} 0 & 1...(2p) \\ 1...(2p+1) & 0 \end{pmatrix}$$

Finally, $P^{-1}X$ is a solution matrix of $\sigma(X) = A_L(X)$. The first rows of this matrix give us a basis of solutions $\{x_1, x_2\}$ of L, where, for all $p \in \mathbb{N}$

$$\begin{cases} x_1(2p) = 1 \dots (2p-1) \\ x_2(2p) = 1 \dots 2(p-1) \end{cases} \quad \text{and} \quad \begin{cases} x_1(2p+1) = 1 \dots (2p-1) \\ x_2(2p+1) = \quad 1 \dots (2p) \end{cases}$$

Example 2.Let L be the operator $E^2 - (n+1)E + n$.

A computation with SHASTA shows that the operator and the associated second iterated system both have trivial Eigenring.

If L has liouvillian solution, he then must have a right factor of order 1 *with coefficients in* $\mathbb{Q}(z)$.

A computation with SHASTA shows that the constant sequence $x_1 = 1$ is a hypergeometric solution of L, hence that L admits $L - 1$ as a right factor. By Euclidean division, $L = (E - n) * (E - 1)$.

Let $L_2 = E - n$; L_2 is of order 1 and the sequence $y = ((n-1)!)_{n \in \mathbb{N}}$ is an hypergeometric section of L_2.

We apply now the variations of the parameter. Let $c \in \mathcal{S}$; $L_1(c1) = y$ if and only if $\sigma(c) - c = y$, i.e. if and only if $c(n+1) = c(n) + (n-1)!$ for all $n \in \mathbb{N}$. It follows that $x_1 = 1$ and $x_2 = (\sum_{1 \leq k \leq n-1} (k-1)!)_{n \in \mathbb{N}}$ are a basis of the space of the liouvillian solutions of L.

References

1. S.A. Abramov and M. Bronstein. On solutions of linear functional systems. In *Proceedings of ISSAC'2001*, page in press. ACM Press, 2001.
2. M.A. Barkatou. Rational solutions of matrix difference equations : The problem of equivalence and factorisation. In *Proceedings of ISSAC* 99, 1999.
3. Raphaël Bomboy. *Réductibilité et résolubilité des équations aux différences finies*. PhD thesis, Université de Nice-Sophia Antipolis, 2001.
4. Manuel Bronstein and Marko Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157:3–33, 1996.
5. P.A. Hendriks and M.F. Singer. Solving difference equations in finite terms. *Journal of Symbolic Computation*, 27:239–259, 1999.
6. Serge Lang. *Algebra*. Addison-Wesley Publishing Company, 3 edition, 1993.
7. Oystein Ore. Theory of non-commutative polynomials. *Annals of math.*, 1933.
8. Marko Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation*, 14:243–264, 1992.
9. Michael F. Singer. Personnal communication.
10. Michael F. Singer. Testing reducibility of linear differential operator : A group theoretic perspective. *Applicable Algebra in Engineering, Communication and Computing*, 7:77–104, 1996.
11. Marius van der Put and Michael F. Singer. *Galois Theory of Difference Equations*. Number 1666 in Lecture Notes in Mathematics. Springer, 1997.
12. Mark van Hoeij. Finite singularities and hypergeometric solutions of linear recurrence equations. *J. Pure Appl. Algebra,*, 139:109–131, 1999.