J. Symbolic Computation (1999) **27**, 239–259
Article No. jsco.1998.0251
Available online at http://www.idealibrary.com on IDEAL

Solving Difference Equations in Finite Terms

PETER A. HENDRIKS[†] AND MICHAEL F. SINGER[‡§¶]

[†]*Department of Mathematics, University of Groningen, P.O. Box 800, 9700 AV Groningen, The Netherlands*
[‡]*Department of Mathematics, Box 8205, North Carolina State University, Raleigh, NC 27695-8205, U.S.A.*

We define the notion of a Liouvillian sequence and show that the solution space of a difference equation with rational function coefficients has a basis of Liouvillian sequences iff the Galois group of the equation is solvable. Using this we give a procedure to determine the Liouvillian solutions of such a difference equation.

1. Introduction

One of the main results in the Galois theory of linear differential equations is that the Galois group of an equation $L(y) = 0$ has a solvable subgroup of finite index iff the equation can be solved in terms of Liouvillian functions, that is, in terms of functions built up from the coefficients of $L(y)$ iterating field operations, differentiation, integration, exponentials of integrals and taking roots of polynomials (see Kaplansky (1976), Kolchin (1948), Kolchin (1976), Magid (1994)). Furthermore, much work has been devoted to developing algorithms to decide if a linear differential equation has Liouvillian solutions and, if so, find them (see Singer (1997) for a history of this problem).

In this paper we consider difference equations with rational function coefficients. Formally, this is done by considering fields of the form $\mathcal{C}(x)$, $\mathcal{C} \subset \mathbf{C}$, the complex numbers, with an automorphism defined by $\phi(x) = x + 1$ and equations of the form $L(y) = \phi^n(y) + a_{n-1}\phi^{n-1}(y) + \cdots + a_0 y = 0$. One can associate to any such equation a "splitting ring", called the Picard–Vessiot ring, that contains $\mathcal{C}(x)$ as well as a basis for the solution space of $L(y) = 0$. The group of $\mathcal{C}(x)$-automorphisms of this ring that commute with ϕ is called the Galois group of $L(y) = 0$. We show that $L(y) = 0$ can be solved in terms of "Liouvillian sequences" (see Section 3.2 for a definition) iff the Galois group is a solvable group and give an algorithm to find all such solutions. The notion of *solvable in terms of Liouvillian sequences* generalizes the notion of *solvable in hypergeometric closed form* of Petkovsek *et al.* (1996, p. 141). The algorithm presented here generalizes algorithms that find hypergeometric solutions (e.g. HYPER in Petkovsek (1992), Petkovsek *et al.* (1996)), or the algorithm presented in van Hoeij (1998a,b).

The paper is organized as follows. In Section 2, we review the basics of the Galois theory of difference equations. In Section 3 we discuss rings of sequences, define Liouvillian

[§]The preparation was partially supported by NSF Grants CCR-93222422 and CCR-9731507.
[¶]E-mail: singer@math.ncsu.edu, http://www.math.ncsu.edu/∼singer

0747–7171/99/030239 + 21 $30.00/0

sequences and give the Galois theoretic characterization of solvability in terms of Liouvillian sequences. In Section 4 we study equations of the form $\phi^m - a$. An understanding of these equations and their Galois groups is the key to the algorithm for finding Liouvillian solutions of equations $L(y) = 0$. In Section 5, we present this algorithm. The paper ends with two appendices. The first appendix discusses properties of the Casoratian determinant, the difference analogue of the Wronskian determinant. The second appendix shows the equivalence between systems $\phi(Y) = AY,\ A \in \mathrm{GL}_n(k)$ and equations $L(y) = 0$ with coefficients in k where k is a difference field containing an element a such that $\phi^n(a) \neq a$ for all $n \in \mathbf{Z} - \{0\}$, where $\mathbf{Z}$ is the integers.

2. Galois Theory

In this section we will review the basic notions from the Galois theory of difference equations that are needed in the rest of the paper. A complete treatment can be found in van der Put and Singer (1997).

Let k be a difference field of characteristic 0, that is, a field k with an automorphism ϕ. Let $\mathcal{C} = \{c \in k \mid \phi(c) = c\}$ be the field of constants of k. We shall consider systems of difference equations of the form

$$\phi(Y) = AY \tag{2.1}$$

where $A \in \mathrm{GL}_n(k)$. If R is a difference ring[†] extension of k, a *fundamental matrix* for (2.1) is an element $U = (u_{ij}) \in \mathrm{GL}_n(R)$ such that $\phi(U) = AU$. A difference ring extension R of k is called a *Picard–Vessiot extension of k for* (2.1) if R is a simple difference ring (i.e. the only ϕ-invariant ideals are (0) and R) and $R = k[u_{11}, \ldots, u_{nn}, (\det\ U)^{-1}]$ where $U \in \mathrm{GL}_n(R)$ is a fundamental matrix for (2.1). When $\mathcal{C}$ is algebraically closed, the Picard–Vessiot extension R or k for (2.1) exists and is unique up to k-difference isomorphism (Proposition 1.9 of van der Put and Singer (1997)).

Let R be a Picard–Vessiot extension of k. The group of k-difference automorphisms $\mathrm{Gal}(R/k)$ has a natural structure of a linear algebraic group defined over $\mathcal{C}$ (Theorem 1.13 of van der Put and Singer (1997)). The set of solutions V in R^n of (2.1) is an n-dimensional vector space over $\mathcal{C}$ that is left invariant by $\mathrm{Gal}(R/k)$ and so yields a representation $\mathrm{Gal}(R/k) \to \mathrm{GL}_n(\mathcal{C})$.

Let $\phi(Y) = AY,\ \phi(Y) = BY$ with $A, B \in \mathrm{GL}_n(k)$ be two systems. Let R_A and R_B be the corresponding Picard–Vessiot extensions and let V_A and V_B be the corresponding solution spaces. We say the two systems are equivalent if there exists a $T \in \mathrm{GL}_n(k)$ such that $B = \phi(T)AT^{-1}$. In this case, if $U \in \mathrm{GL}_n(R_A)$ is a fundamental matrix for $\phi(Y) = AY$, then TU is a fundamental matrix for $\phi(Y) = BY$. Therefore, we can identify the two Picard–Vessiot rings $R_A = R_B = R$ and the two spaces V_A and V_B are isomorphic as $\mathrm{Gal}(R/k)$-modules. Conversely, if R_A and R_B are k-isomorphic as difference rings and V_A and V_B are isomorphic as Gal-modules, then the two systems are equivalent.

When $k = \mathcal{C}(x)$, $\mathcal{C}$ algebraically closed and $\phi(x) = x + 1$ the following results contain the essential facts concerning Galois groups that we shall use in the rest of the paper (cf. Propositions 1.20 and 1.21 of van der Put and Singer (1997)). The following notation is used. If X is a variety defined over a field k_0 and S is any ring containing k_0, we denote by $X(S)$ the points of X with coefficients in S. We say that a subvariety $Y \subset X$ is a k_0-*subvariety* (or in the case of an algebraic subgroup, a k_0-*subgroup*) if Y is defined by equations whose coefficients lie in k_0.

[†]All rings in this paper are assumed (except when otherwise noted) to be commutative with an identity.

THEOREM 2.1. *Let $k = \mathcal{C}(x)$, $\mathcal{C}$ algebraically closed and $\phi(x) = x + 1$. Let G be the Galois group of the Picard–Vessiot extension for (2.1). Then*

(1) *G/G^0 is a finite cyclic group where G^0 is the identity component of G.*
(2) *There exists a $B \in G(k)$ such that (2.1) and $\phi(Y) = BY$ are equivalent.*

It is conjectured that every linear algebraic group G with G/G^0 finite cyclic is the Galois group of a system (2.1) over $\mathcal{C}(x)$. In Hendriks (1998, 1996), it is shown that this conjecture is true for $n = 1, 2$ by giving explicit examples. In van der Put and Singer (1997), this conjecture is shown to be true for connected G and further partial results are given. The following result gives a theoretical characterization of the Galois group.

THEOREM 2.2. *Let $k = \mathcal{C}(x)$, $\mathcal{C}$ algebraically closed and $\phi(x) = x + 1$. Let G be an algebraic subgroup of GL_n defined over $\mathcal{C}$ and let (2.1) be a system with $A \in G(k)$. Then*

(1) *the Galois group of (2.1) over k is a subgroup of $G(\mathcal{C})$, and*
(2) *the Galois group of (2.1) over k is G iff for any $T \in G(k)$ and any proper $\mathcal{C}$-subgroup H of G one has that $\phi(T)AT^{-1} \notin H(k)$.*

We will also work with difference operators $L = \phi^m + a_{m-1}\phi^{m-1} + \cdots + a_0$ and scalar equations $L(y) = \phi^m(y) + a_{m-1}\phi^{m-1}(y) + \cdots + a_0 y = 0,\ a_i \in k$.[†] Given such an equation, one can form the system $\phi(Y) = A_L Y$ where

$$A_L = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -a_0 & -a_1 & \dots & \dots & -a_{m-1} \end{pmatrix}.$$

One easily sees that y is a solution of $L(y) = 0$ iff $(y, \phi(y), \dots, \phi^{m-1}(y))^T$ is a solution of $\phi(Y) = A_L Y$. We call the matrix A_L *the companion matrix of the equation $L(y) = 0$* and the system $\phi(Y) = A_L Y$ *the companion system*. In Appendix B, we show that for a large class of the difference fields, any system $\phi(Y) = AY$ is equivalent to the companion system of a scalar equation. We define the Picard–Vessiot extension of k corresponding to L to be the Picard–Vessiot extension of the companion system and the Galois group of L to be the Galois group of this ring.

The set of linear difference operators, that is polynomials in ϕ, forms a noncommutative ring where $\phi a = \phi(a)\phi$ for all $a \in k$. This ring is both left and right Euclidean. One can define the notions of *left factor, right factor, least common left multiple (LCLM), greatest common right divisor (GCRD),* etc. in the usual way (see Bronstein and Petkovsek (1994, 1996)). We say that two operators L_1 and L_2 are equivalent if their companion systems are equivalent. One can verify that two operators L_1 and L_2 of the same orders n are equivalent iff there are two operators R, S of orders at most $n - 1$ such that R and L_2 have no nontrivial common right factors and $L_1 R = S L_2$ (cf. the similar notions for differential operators in Singer (1996)).

[†]Since ϕ is an automorphism of k, we can restrict our attention to operators L with $a_0 \neq 0$. Throughout this paper we shall assume that this is the case.

3. Sequence Spaces

3.1. the ring $\mathcal{S}$ of germs of sequences

Let $\mathcal{C} \subset \mathbf{C}$ be a field and let $\mathrm{Seq}_{\mathcal{C}}$ be the ring of sequences $\mathbf{a} = (\mathbf{a}(0), \mathbf{a}(1), \ldots)$, $\mathbf{a}(i) \in \mathcal{C}$ where addition and multiplication are defined coordinatewise. Let J be the ideal of all sequences with at most a finite number of nonzero terms and let $\mathcal{S}_{\mathcal{C}} = \mathrm{Seq}\,/J$ (cf. Chapter 4 of van der Put and Singer (1997)). We shall sometimes drop the subscript $\mathcal{C}$ and use the notation $\mathcal{S}$ when there is no confusion as to the field $\mathcal{C}$. We shall frequently identify a sequence $\mathbf{a}$ with its equivalence class in $\mathcal{S}$. The map $\phi(\mathbf{a}(0), \mathbf{a}(1), \ldots) = (\mathbf{a}(1), \mathbf{a}(2), \ldots)$ is well defined on $\mathcal{S}$ and defines an automorphism of $\mathcal{S}$ (note that ϕ has a nontrivial kernel on Seq).

Let $k_\infty = \mathbf{C}(\{x^{-1}\})$ be the fraction field of convergent series at infinity with automorphism $\phi(x^{-1}) = \frac{x^{-1}}{1+x^{-1}}$. We can embed k_∞ in $\mathcal{S}_{\mathbf{C}}$ by mapping $f \in k_\infty$ to the sequence $\mathbf{s}_f = (\mathbf{s}(0), \mathbf{s}(1), \ldots)$ where $\mathbf{s}(i) = f(i)$ for all but a finite number of i. By selecting a branch for $x^{-\frac{1}{m}}$ that is real and positive on the positive real axis and mapping $x^{-\frac{1}{m}}$ to the sequence defined by evaluating this branch at sufficiently large integers, we define an embedding of $\mathbf{C}(\{x^{-\frac{1}{m}}\})$ into $\mathcal{S}_{\mathbf{C}}$. This is a difference embedding where the automorphism on $\mathbf{C}(\{x^{-\frac{1}{m}}\})$ is defined by $\phi(x^{-\frac{1}{m}}) = x^{-\frac{1}{m}}/(1 + x^{-1})^{\frac{1}{m}}$. This allows us to embed the algebraic closure of k_∞ into $\mathcal{S}_{\mathbf{C}}$. Using this we can embed $\mathcal{C}(x) \subset k_\infty$ and its algebraic closure into $\mathcal{S}_{\tilde{\mathcal{C}}}$ where $\tilde{\mathcal{C}}$ is the algebraic closure of $\mathcal{C}$.

Let $\mathcal{C} \subset \mathbf{C}$ be an algebraically closed field and let $\mathcal{S} = \mathcal{S}_{\mathcal{C}}$. The following result (Proposition 4.1 of van der Put and Singer (1997)) allows one to assume that any Picard–Vessiot extension of $\mathcal{C}(x) \subset \mathcal{S}_{\mathcal{C}}$ also lies in $\mathcal{S}_{\mathcal{C}}$.

Proposition 3.1. *Let $\mathcal{C}$ be an algebraically closed field of characteristic zero and let $\mathcal{C} \subset k \subset \mathcal{S}$ be a difference field such that the algebraic closure of k also lies in $\mathcal{S}$ and is invariant under ϕ. Let $A \in \mathrm{GL}_n(k)$ and consider the equation $\phi(Y) = AY$. Let N be such that $A = (A(0), A(1), \ldots)$ considered as an element of $\mathrm{GL}_n(\mathcal{S})$ satisfies $A(m) \in \mathrm{GL}_n(\mathcal{C})$ for $m \geq N$. Define $Z = (Z_{ij}) \in \mathrm{GL}_n(\mathcal{S})$ by $Z(N) = id$ and $Z(m+1) = A(m)Z(m)$ for $m \geq N$. Then*

(1) *$\phi(Z) = AZ$ and $R = k\big[Z_{ij}, \frac{1}{\det(Z)}\big] \subset \mathcal{S}$ is the Picard–Vessiot ring for $\phi(Y) = AY$.*
(2) *Every $Y \in \mathcal{S}^n$ that is a solution of $\phi(Y) = AY$ is a $\mathcal{C}$-linear combination of the columns of Z.*

One of the striking differences between the theories of linear difference and linear differential equations is the phenomenon of interlacing which we define here.

Definition 3.2. (1) Let m be a positive integer and $0 \leq i \leq m-1$. We say that $\mathbf{b}$ is the ith m-interlacing of $\mathbf{a}$ with zeroes if $\mathbf{b}(mn+i) = \mathbf{a}(n)$ and $\mathbf{b}(r) = 0$ if $r \not\equiv i \mod m$.

(2) We define the interlacing $\mathbf{c}$ of sequences $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{m-1}$ to be the sum of sequences $\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{m-1}$ where each $\mathbf{b}_i$ is the ith m-interlacing of $\mathbf{c}_i$ with zeroes.

(3)We say that $\mathbf{a}$ is the ith m-section of $\mathbf{b}$ if $\mathbf{a}(mn+i) = \mathbf{b}(mn+i)$ and $\mathbf{a}(r) = 0$ if $r \not\equiv i \mod m$.

Remarks. (1) If $\mathbf{a}$ satisfies $L(y) = \phi^n(y) + a_{n-1}\phi^{n-1}(y) + \cdots + a_0 y = 0$ then the ith m-interlacing of $\mathbf{a}$ with zeroes satisfies $L_m^i(y) = \phi^{nm}(y) + \phi^{-i}\tau^{-1}(a_{n-1})\phi^{(n-1)m}(y) +$

$\cdots + \phi^{-i}\tau^{-1}(a_0)y = 0$, where $\tau(x) = mx$. In terms of operators, if $L = P(\phi)$ for some polynomial P with coefficients in k, then $L^i_m = (\phi^{-i}\tau^{-1}P)(\phi^m)$, where $\phi^{-i}\tau^{-1}P$ denotes the polynomial obtained by applying $\phi^{-i}\tau^{-1}$ to each coefficient of P.

(2) Concretely, if $\mathbf{v}$ is the interlacing of $\mathbf{a}, \mathbf{b}, \ldots, \mathbf{f}$, then $\mathbf{v} = (\mathbf{a}(0), \mathbf{b}(0), \ldots, \mathbf{f}(0), \mathbf{a}(1), \mathbf{b}(1), \ldots, \mathbf{f}(1), \ldots)$ and $(\mathbf{a}(0), 0, \ldots, 0, \mathbf{a}(1), 0, \ldots)$ is the zeroth m-section of $\mathbf{v}$, $(0, \mathbf{b}(0), \ldots, 0, 0, \mathbf{b}(1), 0, \ldots)$ is the first m-section of $\mathbf{v}$, etc.

(3) If k is a *differential* field and a is an element in an algebraic extension of k, then a satisfies a linear differential equation over k. In contrast, the difference field $\mathcal{C}(x)$, $\mathcal{C} \subset \mathbf{C}$ algebraically closed with $\phi(x) = x + 1$ has no proper difference extension fields of finite dimension (van der Put and Singer, 1997, Lemma 1.19). In fact, a sequence $\mathbf{a}$ satisfies both a linear difference and a polynomial equation over $\mathcal{C}(x)$ iff $\mathbf{a}$ is the interlacing of elements of $\mathcal{C}(x)$ (van der Put and Singer, 1997, Proposition 4.4).

3.2. The ring $\mathcal{L}$ of Liouvillian sequences

One defines the ring of Liouvillian sequences recursively. Let $k = \mathcal{C}(x)$, $\mathcal{C}$ an algebraically closed subfield of $\mathbf{C}$. Most of the results of this section are contained in Hendriks (1996).

Definition 3.3. The ring $\mathcal{L}$ of Liouvillian sequences is the smallest subring of $\mathcal{S}$ such that

(1) $k \subset \mathcal{L}$,
(2) $\mathbf{a} \in \mathcal{L}$ iff $\phi(\mathbf{a}) \in \mathcal{L}$,
(3) $\mathbf{a} \in k$ implies that $\mathbf{b} \in \mathcal{L}$ if $\phi(\mathbf{b}) = \mathbf{ab}$,
(4) $\mathbf{a} \in \mathcal{L}$ implies that $\mathbf{b} \in \mathcal{L}$ if $\phi(\mathbf{b}) = \mathbf{a} + \mathbf{b}$,
(5) $\mathbf{a} \in \mathcal{L}$ implies that $\mathbf{b} \in \mathcal{L}$ where for some m, i, $0 \leq i \leq m-1$, $\mathbf{b}$ is an ith $m-$interlacing of $\mathbf{a}$ with zeroes.

Remarks. (1) The sequences defined by equations of the form $\phi(y) = ay$, $a \in k$ are called *hypergeometric sequences* (cf. Petkovsek *et al.* (1996, 1992), van der Put and Singer (1997, Definition 4.2)). The sequences defined by equations of the form $\phi(y) = y + \mathbf{a}$, $\mathbf{a} \in \mathcal{S}$ are the *indefinite sums* of $\mathbf{a}$

(2) The interlacing of Liouvillian sequences is Liouvillian.

(3) Condition (2) above implies that we can replace condition (5) with the weaker condition $\mathbf{a} \in \mathcal{L}$ *implies that the zeroth* m*-interlacing of* $\mathbf{a}$ *is in* $\mathcal{L}$.

(4) Since $\mathbf{1} = (1, 1, \ldots) \in \mathcal{L}$, the ith m-interlacing of $\mathbf{1}$ with zeroes is in $\mathcal{L}$ for any m and i. Since $\mathcal{L}$ is a ring, we have that any section (cf. Definition 3.2) of an element of $\mathcal{L}$ is also in $\mathcal{L}$.

We will also say that a vector $Y_1 \in \mathcal{S}^n$ is the ith m-interlacing of a vector $Y_0 \in \mathcal{S}^n$ with zeroes if each component of Y_1 is the ith m-interlacing with zeroes of the corresponding component of Y_0. The above definition yields the following theorem

Theorem 3.4. *Suppose* $\mathbf{a} \in \mathcal{S}$. *The following are equivalent.*

(1) $\mathbf{a} \in \mathcal{L}$.
(2) *The sequence* $\mathbf{a}$ *satisfies a linear difference equation over* k *whose Galois group* G *is solvable.*

PROOF. Note that G/G^0 is cyclic so G is solvable iff G^0 is solvable.

(2) $\Rightarrow$ (1) Consider the system (2.1) with $A \in \mathrm{GL}_n(k)$. Let $V_A = \{Y \in \mathcal{S}^n \mid \phi(Y) = AY\}$ be the solution space for this system. We will prove that if the Galois group of this system is solvable then V_A is a subspace of $\mathcal{L}^n$. This statement is slightly more general than the (2) $\Rightarrow$ (1) part of the theorem.

Suppose now that the difference Galois group G is solvable and G/G^0 is finite cyclic of order m. We assume that $A \in G(k)$. This is without loss of generality since if $\phi(Y) = \tilde{A}Y$ is an equivalent system then $V_A \subset \mathcal{L}^n$ iff $V_{\tilde{A}} \subset \mathcal{L}^n$.

Let $B = \phi^{m-1}(A) \cdots \phi(A)A$. We then have $B \in G^0(k)$. We may further assume that B is an upper triangular matrix. If not, then by the Lie–Kolchin Theorem, there is a matrix $T \in \mathrm{GL}_n(\mathcal{C})$ such that $\tilde{B} = T^{-1}BT$ is upper triangular and we can continue with $\tilde{B}$ instead of B. Consider the system of difference equations $\phi^m(Y) = BY$. The solution space $V_B = \{Y \in \mathcal{S}^n \mid \phi^m(Y) = BY\}$ is an nm-dimensional $\mathcal{C}$-vector space and $V_A \subset V_B$. We will prove that $V_B \subset \mathcal{L}^n$. Let $\mathcal{S}_i = \{\mathbf{a} \in \mathcal{S} \mid a_j = 0 \text{ if } j \not\equiv i \bmod m\}$ for $i = 0, \ldots, m-1$. Then we have $\mathcal{S} = \mathcal{S}_0 \oplus \cdots \oplus \mathcal{S}_{m-1}$. Let $V_B^i = V_B \cap \mathcal{S}_i^n$ for $i = 0, \ldots, m-1$. We then have that V_B^i is an n-dimensional $\mathcal{C}$-vector space for $i = 0, \ldots, m-1$ and $V_B = V_B^0 \oplus \cdots \oplus V_B^{m-1}$.

Let $\tau : k \to k$ be the map defined by $x \mapsto mx$. Then $\tau \circ \phi^m = \phi \circ \tau$. Let $C = \tau(B) \in \mathrm{GL}_n(k)$. Note that C is also an upper triangular matrix. Consider the system $\phi(Y) = CY$. The solution space V_C is n-dimensional and one has that $Y_0 \in V_C$ iff $Y_1 \in V_B^0$, where Y_1 is the zeroth m-interlacing of Y_0 with zeroes. We will show by induction on n that there exists an upper triangular fundamental matrix $U = (u_{ij}) \in \mathrm{GL}_n(\mathcal{L})$ for the system $\phi(Y) = CY$.

If $n = 1$ then we are considering a single equation of the form $\phi(y) = \mathbf{a}y$. Since $\mathbf{a} \neq 0$, any nonzero solution $\mathbf{y}$ is invertible in $\mathcal{S}$. Furthermore, part (3) of the definition implies that such a $\mathbf{y} \in \mathcal{L}$. Since $\mathbf{y}^{-1}$ satisfies $\phi(z) = \mathbf{a}^{-1}z$, we have that $\mathbf{y}^{-1} \in \mathcal{L}$.

Now assume $n > 1$ and write $C = \begin{pmatrix} C_0 & D \\ 0 & C_1 \end{pmatrix}$ where $C_0 \in \mathrm{GL}_{n-1}(k)$ is upper triangular and $C_1 \in \mathrm{GL}_1(k)$. By induction we have that there exist $U_0 \in \mathrm{GL}_{n-1}(\mathcal{L})$ and $U_1 \in \mathrm{GL}_1(\mathcal{L})$ satisfying $\phi(U_i) = C_iU_i$. Let W be an $(n-1)\times 1$ matrix whose entries are to be determined and let $U = \begin{pmatrix} U_0 & U_0W \\ 0 & U_1 \end{pmatrix}$. A computation shows that a necessary and sufficient condition that U satisfy $\phi(Y) = CY$ is that W satisfy $\phi(W) = W + U_0^{-1}C_0^{-1}DU_1$. By our induction hypothesis, the entries of $Y_0^{-1}C_0^{-1}DY_1$ lie in $\mathcal{L}$. If $W = (w_1, \ldots, w_{n-1})^T$ then each w_i satisfies $\phi(w_i) = w_i + l_i$ for some $l_i \in \mathcal{L}$. Condition (4) of the definition of $\mathcal{L}$ insures that these equations have solutions in $\mathcal{L}$. Therefore $\phi(Y) = CY$ has a solution as desired.

(1) $\Rightarrow$ (2) We will prove this part of the theorem case-by-case.

(1) Suppose $\mathbf{a} \in k - \{0\}$. Then $\mathbf{a}$ satisfies the first-order linear difference equation $\phi(y) = (\phi(\mathbf{a})/\mathbf{a})y$. The difference Galois group of this equation is trivial.

(2) We have that $\mathbf{a} \in \mathcal{S} - \{0\}$ satisfies a linear difference equation iff $\phi(\mathbf{a})$ satisfies an equivalent equation of the same order. Hence the Galois groups associated to both equations coincide.

(3) Suppose $\mathbf{b} \in \mathcal{S} - \{0\}$ satisfies the first-order difference equation $\phi(y) = \mathbf{a}y$, where $\mathbf{a} \in k - \{0\}$. The difference Galois group G associated with this equation is an algebraic subgroup of $\mathrm{GL}_1(\mathcal{C}) = \mathcal{C}^*$ and so is solvable.

(4) Suppose L is an nth-order linear difference operator with coefficients in k such that $L(\mathbf{a}) = 0$. Let G be the difference Galois group associated to the equation $L(y) = 0$.

Let $\mathbf{b} \in \mathcal{S}$ satisfy $\phi(\mathbf{b}) - \mathbf{b} = \mathbf{a}$. Then $\tilde{L}(\mathbf{b}) = (L \circ (\phi - 1))(\mathbf{b}) = 0$. Hence $\mathbf{b}$ satisfies a difference equation order $n+1$ whose difference Galois group of $\tilde{L}$ is a subgroup of the semidirect product of G and $\mathcal{C}^n$ and so is solvable.

(5) Suppose $\mathbf{a} \in \mathcal{S}$ satisfies the difference equation $L(y) = \phi^n(y) + c_{n-1}\phi^{n-1}y + \cdots + c_0 y = 0$, with $c_{n-1}, \ldots, c_0 \in k, c_0 \neq 0$. Consider the associated system $\phi(Y) = CY$ where

$$C = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -c_0 & -c_1 & -c_2 & \ldots & -c_{n-1} \end{pmatrix}$$

is the companion matrix of L. Let $G \subset \mathrm{GL}_n$ be the difference Galois group of this system. Theorem 2.1 implies that there exists a matrix $T \in \mathrm{GL}_n(k)$ such that $B = \phi(T)CT^{-1} \in G(k)$. Now let $\mathbf{b}$ be the zeroth m-interlacing of $\mathbf{a}$ with zeroes. Then $\mathbf{b}$ satisfies the linear difference equation $\tilde{L}(y) = \phi^{nm}(y) + (\tau^{-1}c_{n-1})\phi^{(n-1)m}y + \cdots (\tau^{-1}c_0)y = 0$ where $\tau : k \to k$ is the map defined by $x \mapsto mx$. Note that $\tau^{-1} \circ \phi = \phi^m \circ \tau^{-1}$. The equation $\tilde{L}(y) = 0$ can be identified with the $nm \times nm$ system $\phi(Y) = \tilde{C}Y$ where

$$\tilde{C} = \begin{pmatrix} 0 & I & 0 & \ldots & 0 \\ 0 & 0 & I & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & I \\ \tau^{-1}(C) & 0 & 0 & \ldots & 0 \end{pmatrix} \in \mathrm{GL}_{nm}(k).$$

Let $\tilde{T} = \mathrm{diag}(\tau^{-1}T, \phi(\tau^{-1}T), \ldots, \phi^{m-1}(\tau^{-1}T)) \in \mathrm{GL}_{nm}(k)$. Then

$$\tilde{B} = \phi(\tilde{T})\tilde{C}\tilde{T}^{-1} = \begin{pmatrix} 0 & I & 0 & \ldots & 0 \\ 0 & 0 & I & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & I \\ \tau^{-1}(B) & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Therefore Theorem 2.1 implies that the difference Galois group $\tilde{G}$ of this latter equation is a subgroup of a cyclic extension of order m of m copies of G and so is also solvable.

We still must show that if $\mathbf{a}$ and $\mathbf{b}$ satisfy linear difference equations over k whose Galois groups are solvable then $\mathbf{ab}$ and $\mathbf{a} - \mathbf{b}$ also satisfy linear difference equation over k whose Galois groups are solvable. We give a constructive proof of this in Lemma A.8 of Appendix B. □

Remarks. One can define an *a priori* larger class of sequences, the *generalized Liouvillian sequences*. One says that a sequence $\mathbf{a}$ is a generalized Liouvillian sequence if there exists a sequence of rings $\mathcal{C}(x) = R_0 \subset \cdots \subset R_m \subset \mathcal{S}$ such that $\mathbf{a} \in R_m$ and for each $i = 0, \ldots, m, R_{i+1} = R_i(\ldots, \phi^{-1}(\mathbf{b}_i), \mathbf{b}_i, \phi(\mathbf{b}_i), \ldots)$ where either (1) $\phi(\mathbf{b}_i) = \mathbf{a}_i\mathbf{b}_i$ for some $\mathbf{a}_i \in R_i$, or (2) $\phi(\mathbf{b}_i) = \mathbf{a}_i + \mathbf{b}_i$ for some $\mathbf{a}_i \in R_i$, or (3) $\mathbf{b}_i$ is the interlacing of sequences in R_i. Clearly a Liouvillian sequence is generalized Liouvillian. We conjecture that a linear difference equation has a nonzero Liouvillian solution iff it has a nonzero generalized Liouvillian solution. This conjecture is motivated by the fact that in the definition of Liouvillian function using towers of fields, one allows at each stage the introduction of exponential of integrals, yet one can show that to solve a linear differen-

tial equations in terms of Liouvillian functions one only needs exponentials of algebraics (together with field theoretic operations and iterations of integration).

4. The Operator $\phi^m - a$

The key to understanding Liouvillian solutions of difference equations can be found in the structure of the solution space of the operator $\phi^m - a$. In this section we will investigate this operator. For the next result recall that a torus is a connected diagonalizable linear algebraic group. Throughout this section, k will denote the field $\mathcal{C}(x)$ where $\mathcal{C}$ is an algebraically closed subfield of $\mathbf{C}$ and $\phi(x) = x + 1$.

LEMMA 4.1. *(1) A necessary and sufficient condition that the Galois group of an* irreducible *mth-order system $\phi(Y) = AY$ is a finite cyclic extension of a torus is that $\phi(Y) = AY$ is equivalent to an equation*

$$\phi(Y) = BY = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 \\ a & 0 & 0 & \dots & 0 \end{pmatrix} Y \tag{4.1}$$

for some nonzero $a \in k$.

(2) A necessary and sufficient condition that the Galois group of an irreducible *difference operator L be a finite cyclic extension of a torus is that L be equivalent to an operator of the form $\phi^m - a$ for some nonzero $a \in k$.*

PROOF. (1) Assume that $\phi(Y) = AY$ is equivalent to (4.1). One sees that B^m lies in the diagonal subgroup of $\mathrm{GL}_m(k)$ so Theorem 2.1 implies that the identity component of the Galois group is a torus.

Now assume that the Galois group G is a finite cyclic extension of a torus and let V be the solution space of $\phi(Y) = AY$. Let $g \in G$ be an element whose image in G/G^0 generates this latter group and let $V = V_0 \oplus V_1 \oplus \cdots \oplus V_{t-1}$ where each V_i is a weightspace of G^0 of weight λ_i. Since V is irreducible and g permutes the V_i, we can assume that the $g(V_i) = V_{i+1 \bmod t}$. Let $v \in V_0$ be an eigenvector of g^t and let W be the span of $\{v, gv, \dots, g^{t-1}v\}$. Since W is G-invariant, we must have $t = m$ and $W = V$. Therefore we may assume that G is generated by the diagonal group G^0 and a matrix of the form

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

for some $c \in \mathcal{C}$. Theorem 2.1 implies that $\phi(Y) = AY$ is equivalent to a system $\phi(Y) = B_0 Y$ with B_0 a k-point of this group. After conjugation by a constant matrix if necessary,

we can assume that

$$B_0 = \begin{pmatrix} 0 & a_1 & 0 & \dots & 0 \\ 0 & 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & a_{m-1} \\ a_m & 0 & 0 & \dots & 0 \end{pmatrix}.$$

If $T = \operatorname{diag}(1, a_1, \phi(a_1)a_2, \dots, \phi^{m-2}(a_1)\phi^{m-3}(a_2)\cdots a_{m-1})$, then

$$B = \phi(T)B_0T^{-1} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 \\ a & 0 & 0 & \dots & 0 \end{pmatrix}$$

for some nonzero $a \in k$. This gives the conclusion of (1).

(2) This follows from applying (1) to the companion system of L. □

Remark. The proof of Lemma 4.1 demonstrates that, without the assumption of irreducibility, if $\phi(Y) = AY$ is equivalent to (4.1) (or L is equivalent to $\phi^m - a$) then the Galois group is a finite cyclic extension of a torus.

Corollary 4.2. *(1) A necessary and sufficient condition that the Galois group of a system $\phi(Y) = AY$ is a finite cyclic extension of a torus is that $\phi(Y) = AY$ is equivalent to an equation $\phi(Y) = BY$ where B is block diagonal with each block of the form given in (4.1).*

(2) A necessary and sufficient condition that the Galois group of a difference operator L be a finite cyclic extension of a torus is that L be equivalent to the least common left multiple of operators of the form $\phi^m - a$ for some nonzero $a \in k$.

Proof. (1) If $\phi(Y) = AY$ is equivalent to the system $\phi(Y) = BY$ of the prescribed form then some power of B is diagonal and so the identity component of the Galois group of B is a torus. Conversely, if the Galois group G is a finite cyclic extension of a torus, then it is *a fortiori* a completely reducible group. Therefore, after a possible change of basis, we can assume that G is in block diagonal form where each block is irreducible. Theorem 2.1 implies that $\phi(Y) = AY$ is equivalent to a system whose matrix is of the same form. An application of Lemma 4.1 to each block yields the conclusion of the first part of the corollary.

(2) From the above one sees that the Galois group of an operator of the form $\phi^m - a$ is a finite cyclic extension of a torus. If L is the least common left multiple of operators L_i of the prescribed form then its Galois group G leaves the solution space V_i of each L_i invariant. Furthermore, G has a faithful representation into $\mathrm{GL}(V)$ where $V = V_1 \oplus \cdots \oplus V_t$ such that the image in each $\mathrm{GL}(V_i)$ is a finite cyclic extension of a torus. Therefore G is a subgroup of the direct product of the groups that are finite cyclic extensions of tori and so we must have that G^0 is a torus. Therefore, G is a finite cyclic extension of a torus.

Conversely, if the Galois group of L is a finite extension of a torus, then as before it is completely reducible and we can write $V = V_1 \oplus \cdots \oplus V_t$ where each V_i is a G-irreducible module. Each V_i is the solution space of an operator L_i and L is the least common left

multiple of the L_i. Lemma 4.1 implies that each L_i is equivalent to an operator of the prescribed form. □

The following will allow us to characterize linear difference operators with Liouvillian solutions as well as being the basis for algorithms to determine if an operator has Liouvillian solutions.

COROLLARY 4.3. *Let L be an irreducible difference operator with coefficients in k. Then L is equivalent to an operator of the form $\phi^m - a,\ a \in k$ iff L has a nonzero solution in $\mathcal{S}$ that is the m-interlacing of hypergeometric sequences. Furthermore, if this is the case, then the solution space of L has a basis each of whose members is the interlacing of hypergeometric sequences.*

PROOF. Assume that L is equivalent to $\phi^m - a$. The solution space of L has a basis $\mathbf{b}_1, \ldots, \mathbf{b}_m$ where each $\mathbf{b}_i$ is the ith m-interlacing with zeroes of a nonzero solution of $\phi(y) - (\tau\phi^i(a))(y) = 0$. Concretely,

$$\begin{aligned}
\mathbf{b}_1 &= (1, 0, \ldots, 0, a(0), 0, \ldots, 0, a(m)a(0), 0, \ldots)\\
\mathbf{b}_2 &= (0, 1, \ldots, 0, 0, a(1), \ldots, 0, 0, a(m+1)a(1), \ldots)\\
&\vdots\ \vdots\ \vdots\\
\mathbf{b}_m &= (0, 0, \ldots, 1, 0, 0, \ldots, a(m-1), 0, 0, \ldots, a(2m-1)a(m-1), \ldots).
\end{aligned}$$

Since L is equivalent to $\phi^m - a$ there exist $c_0, \ldots, c_{m-1} \in k$ such that $z_i = c_0\mathbf{b}_i + c_1\phi(\mathbf{b}_i) + \cdots + c_{m-1}\phi^{m-1}(\mathbf{b}_i),\ i = 1, \ldots, m$ is a basis for the solution space of L. One easily sees that each z_i is the interlacing of hypergeometric sequences.

Conversely, assume that L has a nonzero solution $\mathbf{y}$ that is the interlacing of sequences defined by the equations $\phi(y) - a_i y = 0,\ i = 1, \ldots, m$. Then $\mathbf{y}$ is the sum of sequences $\mathbf{z}_i$ where for each i, $\mathbf{z}_i$ satisfies the equation $\phi^m\mathbf{z}_i - (\phi^{-i}\tau^{-1})(a_i)\mathbf{z}_i = 0$. Let $\tilde{L}$ be the least common left multiple of the $\phi^m - \phi^{-i}\tau^{-1}(a_i)$ and let $R \subset \mathcal{S}$ be the corresponding Picard–Vessiot extension. Note that $\mathbf{y}$ is in the solution space of $\tilde{L}$. Corollary 4.2.2 implies that the Galois group G of R is a finite cyclic extension of a torus. Since the vector space of solutions of L in R is nontrivial and L is irreducible, Corollary A.7 implies that R contains a full set of solutions of L. This furthermore implies that the Picard–Vessiot extension of L in $\mathcal{S}$ is contained in R. Therefore the Galois group of L is a quotient of G and so its identity component is a torus. Therefore the Galois group of L is a finite cyclic extension of a torus and another application of Corollary 4.2.2 yields the desired conclusion. □

As a final application of these ideas, we prove the following corollary although it is not used in the remainder of the paper.

COROLLARY 4.4. *If $L = \phi^n - a,\ a \in k$, then all irreducible factors of L have orders dividing n. Furthermore, L is reducible iff for some $m \neq n$ dividing n there exists and an $\bar{a} \in k$ such that $a = \bar{a}\phi^m(\bar{a}) \cdots \phi^{n-m}(\bar{a})$ in which case L has an irreducible factor of the form $\phi^m - \bar{a}$.*

PROOF. If A_L is the companion matrix of L, then $(A_L)^n$ is a diagonal matrix. Therefore the Galois group G of L is a subgroup of a $\mathbf{Z}/n\mathbf{Z}$-extension of the diagonal group

$D_n \subset \mathrm{GL}_n(\mathcal{C})$. If $D_G = G \cap D_n$, then one sees that $[G : D_G] = t$ divides n. Let V be the solution space of $L(y) = 0$. Corollary A.7 implies that G-irreducible subspaces of V correspond to irreducible factors of L. Let $W \subset V$ be a G-irreducible subspace of V and let $g \in G$ be an element whose image in G/D_G generates this latter group. As above one can show that W has a basis of the form $v, gv, \ldots, g^{m-1}v$ where each $g^i v$ lies in a weightspace of D_G. Let $\Psi : G \to \mathrm{GL}_m(\mathcal{C})$ be the representation obtained by restricting the elements of G to W. Using the above basis for W, we see that $\Psi(D_G)$ lies in the diagonal subgroup D_m of $\mathrm{GL}_m(\mathcal{C})$ and $[\Psi(G) : \Psi(G) \cap D_m] = m$. Since $[\Psi(G) : \Psi(D_G)]$ divides n and $[\Psi(G) : \Psi(D_G)] = [\Psi(G) : \Psi(G) \cap D_m][\Psi(G) \cap D_m : \Psi(D_G)]$ we have that m divides n. This proves the first claim of the Corollary.

To prove the second claim, we use the following calculations of Petkovsek (1992). Let $L_1 = \sum_{i=0}^{m} a_i \phi^i,\ a_m = 1$ be a monic irreducible factor of $L = \phi^n - a$. From the above, we know that $m|n$. We have that $\phi^n L_1 = \sum_{i=0}^{m} \phi^n(a_i)\phi^{n+i}$. Since $\phi^n \equiv a \pmod{L}$ (where $f \equiv g \pmod{L}$ means that L divides $f - g$ on the right) we have that $\phi^n L_1 \equiv \sum_{i=0}^{m} \phi^n(a_i)\phi^i(a)\phi^i \pmod{L}$. Since L_1 divides L on the right, we have that L_1 divides $\sum_{i=0}^{m} \phi^n(a_i)\phi^i(a)\phi^i$ on the right. Since these two operators have the same order, we can conclude that

$$a_i = \phi^n(a_i)\frac{\phi^i(a)}{\phi^m(a)}.$$

When $i = 0$, this equation yields the following difference equation for a

$$\phi^m(a) = \frac{\phi^n(a_0)}{a_0}a.$$

Since $m|n$, a solution of this equation is $b = a_0\phi^m(a_0)\cdots\phi^{n-m}(a_0)$. A calculation shows that $\phi^m(\frac{a}{b}) = \frac{a}{b}$. Since constants are the only rational function satisfying $\phi^m(f) = f$ we have that $a = cb$ for some $c \in \mathcal{C}$. Letting $\bar{a} = c^{m/n}a_0$ we have $a = \bar{a}\phi(\bar{a})\cdots\phi^{n-m}(\bar{a})$. Therefore

$$\begin{aligned}\phi^n - a &= \phi^n - \bar{a}\phi^m(\bar{a})\cdots\phi^{n-m}(\bar{a}) \\ &= \left(\phi^{n-m} + \sum_{i=1}^{n/m-1}\left(\prod_{j=1}^{i}\phi^{n-jm}(\bar{a})\right)\phi^{n-(i+1)m)}\right)(\phi^m - \bar{a}).\square\end{aligned}$$

5. Difference Equations with Liouvillian Solutions

The following characterizes linear difference equations having Liouvillian solutions. Let k be a field as in Section 3. We will further assume that $\mathcal{C}$ is a field in which the field operations can be effectively performed.

THEOREM 5.1. *Let L be a difference operator of order n with coefficients in k. Then $L(y) = 0$ has a nonzero Liouvillian solution iff $L(y) = 0$ has a nonzero solution that is the interlacing of m hypergeometric sequences where $1 \leq m \leq n$.*

PROOF. If $L(y) = 0$ has a nonzero solution that is the interlacing of hypergeometric sequences then it clearly has a Liouvillian solution.

Now assume that $L(y) = 0$ has a nonzero Liouvillian solution. Let V be the solution space of $L(y) = 0$ and let $W \subset V$ be the nonzero space of Liouvillian solutions of $L(y) = 0$. Theorem 3.4 implies that W lies in the solution space of an operator $\tilde{L}$ whose

Galois group is solvable (and so all solutions of $\tilde{L}$ are Liouvillian). Let L_W be the greatest common right divisor of L and L_W. The solution space of L_W is W. Since L_W divides $\tilde{L}$ on the right, its Galois group is solvable. Replacing L by L_W, we may assume that the Galois group of L is solvable. Since any factor of L also has solvable Galois group we may further assume that L is an irreducible operator with solvable Galois group.

The Lie–Kolchin theorem implies that the identity component G^0 of G has a nontrivial weightspace in V. Let V_0 be the sum of the weight spaces of G^0 in V. Since G permutes the weightspaces of G^0 and V is irreducible, we have that $V_0 = V$. In particular G^0 is diagonalizable and so is a torus. Therefore Corollary 4.2 implies that L is equivalent to an equation of the form $\phi^m - a$. Corollary 4.3 implies that $L(y) = 0$ has a nonzero solution that is the interlacing of $m \leq n$ hypergeometric sequences. □

The algorithm to decide if a linear operator L of order n with coefficients in $\mathcal{C}(z)$ has Liouvillian solutions and finding a basis for the set of such solutions depends on several subprocedures which we now state.

Lemma 5.2. *Let L be a linear difference operator with coefficients in k. One can decide if $L(y) = 0$ has hypergeometric solutions and, if so, find a set $\mathcal{H} = \{h_1, \ldots, h_t\} \subset \mathcal{C}(x)$ such that any hypergeometric solution of $L(y) = 0$ is a solution of $L_1(y) = 0$ where*

$$L_1 = \mathrm{LCLM}\{\phi - h\}_{h \in \mathcal{H}}.$$

Proof. An algorithm for this was presented in Petkovsek (1992) (see also Petkovsek *et al.* (1996)). Recent improvements (and other references) are contained in Abramov and Barkatou (1998) and van Hoeij (1998a,b). Note that these algorithms either produce (or can be modified to produce) an operator L_1 as above that divides L and a basis for the solution space of L_1. □

Lemma 5.3. *Let L be a linear difference operator of order n with coefficients in k. For each $m = 1, \ldots, n$ one can find a set $\mathcal{H}_m = \{h_1, \ldots, h_{t_m}\} \subset \mathcal{C}(x)$ such that any solution of $L(y) = 0$ that is an interlacing of m hypergeometric series is a solution of $L_m(y) = 0$ where*

$$L_m = \mathrm{LCLM}\{\phi^m - h\}_{h \in \mathcal{H}_m}.$$

Proof. When $m = 1$ this is just the procedure of Lemma 5.2. We shall show how to reduce the general case of Lemma 5.3 to the procedure of Lemma 5.2. Fix some m, $1 \leq m \leq n$. Let $P \in k[Z]$ be a polynomial of smallest degree such that $P(\phi^m)(y) = 0$ for all solutions of $L(y) = 0$. One can find such a polynomial by writing each of $y, \phi^m(y), \phi^{2m}(y), \ldots, \phi^{nm}(y)$ as k-linear combinations of $y, \phi(y), \ldots, \phi^{n-1}(y)$ (using $L(y) = 0$) and finding a k-linear dependence among these $n+1$ expressions in the n quantities $y, \phi(y), \ldots, \phi^{n-1}(y)$. Note that not only does every solution $\mathbf{a}$ of $L(y) = 0$ satisfy $P(\phi^m)(y) = 0$ but every ith m-section of $\mathbf{a}$ also satisfies $P(\phi^m)(y) = 0$. Therefore, if $L(y) = 0$ has a nonzero solution $\mathbf{u}$ that is the interlacing of m sequences $\mathbf{u}_0, \ldots, \mathbf{u}_{m-1}$ then each $\mathbf{u}_i$ satisfies $P_i(\phi)(\mathbf{u}_i) = 0$ where $P_i = \tau\phi^i P$. Now use the procedure of Lemma 5.2 to find, for each i, $0 \leq i \leq m-1$ a set $\mathcal{G}_i \subset k^*$ such that $\mathbf{v}$ is a hypergeometric solution of $P_i(\phi)(y) = 0$ iff $\mathbf{v}$ satisfies $L^i(y) = 0$ where $L^i = \mathrm{LCLM}\{\phi^m - h\}_{h \in \mathcal{G}_i}$. One then sees that the conclusion of the lemma is satisfied for $\mathcal{H} = \cup_{0 \leq i \leq m-1}\{\phi^{-i}\tau^{-1}(h) \mid h \in \mathcal{G}_i\}$. □

REMARKS. The solution space of L_m has a basis consisting of ith m-interlacings. Not all sums of these will appear as solutions of $L(y) = 0$. The proof of Lemma 5.3 shows that any solution of $L(y) = 0$ that is an interlacing of m hypergeometric sequences $\mathbf{u}_1, \ldots, \mathbf{u}_m$ where each $\mathbf{u}_i$ satisfies $L^i(y) = 0$, L^i as above. This observation can be used to improve the efficiency of the algorithm of Theorem 5.5. Nonetheless, we will use Lemma 5.3 as stated to simplify the presentation.

LEMMA 5.4. *Let L, L_1, L_2 be operators with coefficients in k of orders n, r and s and let $L = L_1 L_2$.*

(1) *If $\mathbf{y}_1, \ldots, \mathbf{y}_n$ is a basis of the solution space of L then one can effectively find constants $\{c_{ij}\}$ such that $\{\mathbf{z}_i = \sum_{1 \le j \le n} c_{ij} \mathbf{y}_j\}$ is a basis of the solution space of L_2.*
(2) *If $\mathbf{b}_1, \ldots, \mathbf{b}_r$ and $\mathbf{c}_1, \ldots, \mathbf{c}_s$ are bases for the solution space of L_1 and L_2 respectively, then one can express a basis for the solution space of L in terms of these using field operations, ϕ and indefinite summation.*

PROOF. (1) Let $c_1, \ldots, c_n$ indeterminates and let $\mathbf{z} = \sum_{1 \le i \le n} c_i \mathbf{y}_i$. We wish to determine conditions on the c_i such that $\mathbf{w} = L_2(\mathbf{z}) = 0$. Let N be an integer larger than the poles of the coefficients of L, L_1 and L_2. The conditions $\mathbf{w}(N) = 0, \ldots, \mathbf{w}(N + r) = 0$ give a system of linear equations $\mathbf{S}$ in the c_i. Since $L_1(\mathbf{w}) = 0$ and L_1 has order r, $\mathbf{z}$ is a solution of $L_2(\mathbf{z}) = 0$ iff the c_i satisfy $\mathbf{S}$. Therefore a basis for the solution space of $\mathbf{S}$ yields a basis for the solution space of L_2.

(2) This is done using the difference version of variation of parameters. We wish to find $\mathbf{d}_1, \ldots, \mathbf{d}_s$ that are linearly independent over $\mathcal{C}$ such that $L_2(\mathbf{d}_i) = \mathbf{b}_i$ for $i = 1, \ldots s$ and such that each $\mathbf{d}_i$ is expressed in terms of $\mathbf{b}_1, \ldots, \mathbf{b}_r, \mathbf{c}_1, \ldots, \mathbf{c}_s$ using field operations, ϕ and indefinite summation. One then has that $\{\mathbf{d}_1, \ldots, \mathbf{d}_s, \mathbf{c}_1, \ldots, \mathbf{c}_r\}$ is a basis for the solution space of L. It will be convenient to do this in terms of matrix equations.

Letting A be the companion matrix of L_2 and C be the matrix $(\phi^i(c_j))_{1 \le j \le s}^{0 \le i \le s-1}$, we have that $\phi(C) = AC$. Let B be the $s \times s$ matrix $(\mathbf{b}_{ij})$ where $\mathbf{b}_{ij} = \mathbf{0}$ if $1 \le i \le s-1$ and $\mathbf{b}_{sj} = \mathbf{b}_j$. One sees that solving the equations $L_2(\mathbf{d}_i) = \mathbf{b}_i$ is equivalent to solving the system

$$\phi(Y) = AY + B. \tag{5.1}$$

If U is an $s \times s$ matrix of indeterminates, then $Y = CU$ is a solution of equation (5.1) iff U satisfies $\phi(U) - U = (\phi(C))^{-1} B$. This latter equation is clearly solvable in the desired terms. □

The following theorem contains the algorithm to find all Liouvillian solutions of a linear difference equation.

THEOREM 5.5. *Let L be an operator with coefficients in k. One can find operators $H_1, \ldots, H_t, R$ with coefficients in k such that*

(1) *$L = RH_t \cdot \ldots \cdot H_1$;*
(2) *the solution space of each H_i is spanned by interlacings of hypergeometric sequences;*
(3) *any Liouvillian solution of $L(y) = 0$ is a solution of $H_t \cdot \ldots \cdot H_1(y) = 0$.*

Furthermore, one can find a basis of the solution space of each H_i consisting of interlacings of hypergeometric sequences and find a basis of the space of Liouvillian solutions of

L expressed in terms of these interlacings of hypergeometric series using field operations, ϕ, and indefinite summation.

PROOF. Let L have order n. For each integer m with $1 \leq m \leq n$, successively test to see if $\mathrm{GCRD}(L_m, L)$ is nontrivial where L_m is as defined in Lemma 5.3. If all of these are trivial then Lemma 5.3 and Theorem 5.1 imply that $L(y) = 0$ has no nonzero Liouvillian solutions. Otherwise, let m be the smallest integer such that $H_1 = \mathrm{GCRD}(L_m, L)$ is nontrivial. One can easily find a basis for the solution space of L_m consisting of interlacings of hypergeometric sequences and so, using Lemma 5.4.1, find such a basis for H_1. Let $L = \tilde{L}H_1$. Proceeding by induction on the order of the operator, we can write $\tilde{L} = RH_t \cdot \ldots \cdot H_2$ with the H_i satisfying the conclusion of the theorem. Applying Lemma 5.4 to bases of the solution spaces of $H_t \cdot \ldots \cdot H_2$ and H_1, yields a basis for the solution space of L of the prescribed form. □

REMARKS. (1) The algorithm by Hendriks (1998) allows one to determine the Galois group of a second-order operator and therefore to determine if $L(y) = 0$ has Liouvillian solutions. The algorithm will furthermore determine a basis for the space of Liouvillian solutions if any exist.

(2) In practice, one is given a linear operator L with coefficients in $\mathcal{C}_0(x)$ where $\mathcal{C}_0$ is a finitely generated extension of $\mathbf{Q}$. To find a basis for the space of Liouvillian solutions of $L(y) = 0$, one may need elements of an algebraic extension of $\mathcal{C}_0$. For example, if P is an irreducible polynomial over $\mathbf{Q}$ of degree n and $\{\alpha_1, \ldots, \alpha_n\}$ are its roots in $\mathbf{C}$, then the sequences $\mathbf{a}_1, \ldots, \mathbf{a}_n$ form a basis of the solutions space of $P(\phi)$ where e ach $\mathbf{a}_i$ satisfies $\phi(y) = \alpha_i y$. It would be useful to know, *a priori* the smallest extension $\mathcal{C}_1$ of $\mathcal{C}_0$ such that if $L(y) = 0$ has a nonzero solution that is the interlacing of hypergeometric sequences then it has a nonzero solution that is an interlacing of hypergeometric sequences defined over $\mathcal{C}_1(x)$.

(3) One can apply Theorem 5.1 to systems $\phi(Y) = AY$ by finding an equivalent linear operator (see Section 5). A direct proof avoiding cyclic vectors is not difficult once one has a version of Lemma 5.4 applicable to systems. Progress in this direction has been made in Abramov and Barkatou (1998) and van Hoeij (1998b).

Acknowledgements

We wish to thank J. Kovacic for making available his notes to us (Kovacic, 1996), M. Petkovsek for allowing us to use some of his ideas in Corollary 4.4 and the referees for suggestions to make the presentation clearer.

References

Abramov, S., Barkatou, M. (1998). Rational solutions of first order linear difference systems. Technical report, IMAC-LMC, Université de Grenoble I.

Bronstein, M., Petkovsek, M. (1994). On Ore rings, linear operators and factorization. *Program. Comput. Software*, **20**, 14–26.

Bronstein, M., Petkovsek, M. (1996). An introduction to pseudo linear algebra. *Theor. Computer Sci.*, **157**, 3–33.

Cohn, R. (1965). *Difference Algebra*. Tracts in Mathematics 17. New York, Interscience Press.

Hendriks, P. (1996). Algebraic aspects of linear differential and difference equations. Ph.D. thesis, Rijksuniversiteit Groningen.

Hendriks, P. A. (1998). An algorithm for determining the difference Galois group for second order linear difference equations. *J. Symb. Comp.*, **54**, 445–462.
Kaplansky, I. (1976). *An Introduction to Differential Algebra*, 2nd edn. Paris, Hermann.
Kolchin, E. R. (1948). Algebraic matric groups and the Picard–Vessiot theory of homogeneous linear ordinary differential equations. *Ann. Math.*, **49**, 1–42.
Kolchin, E. R. (1976). *Differential Algebra and Algebraic Groups*. New York, Academic Press.
Kovacic, J. (1996). Cyclic vectors and Picard–Vessiot theory. Technical report, Prolifics, Inc.
Magid, A. (1994). In *Lectures on Differential Galois Theory*. University Lecture Series. New York, American Mathematical Society.
Petkovsek, M. (1992). Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symb. Comput.*, **14**, 243–264.
Petkovsek, M., Wilf, H., Zeilberger, D. (1996). *A=B*. Wellsely, MA, A. K. Peters.
Singer, M. F. (1996). Testing reducibility of linear differential operators: a group theoretic perspective. *App. Algebra Eng. Commun. Comput.*, **7**, 77–104.
Singer, M. (1997). Direct and inverse problems in differential Galois theory. To appear in the *Collected Works of E. R. Kolchin*.
van Hoeij, M. (1998a). Finite singularities and hypergeometric solutions of linear recurrence equations. Technical report, Department of Mathematics, Florida State University.
van Hoeij, M. (1998b). Rational solutions of linear difference equations. In Gloor, O., ed. *Proceedings of ISSAC'98*, pp. 120–123. New York, ACM Press.
van der Put, M., Singer, M. F. (1997). *Galois Theory of Difference Equations*, LNM 1666, Heidelberg, Springer.

Appendix A. Linear Dependence and Casoratians

One of the key technical tools in the Picard–Vessiot theory of linear differential equations is the fact that elements in a differential field are linearly dependent over constants iff their Wronskian is zero. In the theory of linear difference equations one works with rings that have zero divisors and the corresponding fact using the Casoratian is no longer true in general . In this section we show how to get around this problem.

Let R be a difference ring with automorphism ϕ. If $y_1, \ldots, y_n \in R$, we define the *Casoratian matrix* $C(y_1, \ldots, y_n)$ to be $(\phi^i(y_j)_{i=0,\ldots,n-1}^{j=1,\ldots,n}$ and the *Casoratian determinant,* $\mathrm{Cas}(y_1, \ldots, y_n)$ to be $\det(C(y_1, \ldots, y_n))$ (cf. Cohn (1965)).

Example A.1. Let $\mathcal{S}$ be the difference ring of equivalence classes of sequences. Let $a = (a_i)$, where $a_i = 1$ if $4|i$ and 0 otherwise and let $b = (b_i)$ where $b_i = 1$ if $4|i-2$ and 0 otherwise. We then have $C(a, b) = 0$ but a and b are not linearly dependent over constants.

Lemma A.2. *Let (R, ϕ) be a simple difference ring and let $y_1, \ldots, y_t \in R$. The following are equivalent:*

(1) *$y_1, \ldots, y_t$ are linearly dependent over constants and*
(2) *the vectors $\mathcal{Y}_j = (\phi^i(y_j))_{-\infty<i<\infty}$, $j = 1, \ldots, t$ are linearly dependent over R.*

Proof. Assertion (2) follows easily from assertion (1).

Now assume that there exist $r_i \in R$, not all zero, such that $\sum r_i \mathcal{Y}_i = 0$. Among all such relations, select one with minimal support $S = \{i_1, \ldots, i_s\}$ (i.e. $r_i \neq 0$ implies $i \in S$). Without loss of generality, we may assume that $1 \in S$. Let

$$I = \left\{ r_1 \in R \mid \exists r_2, \ldots, r_t \in R, \sum r_i \mathcal{Y}_i = 0 \text{ and the support of the } r_i \subset S \right\}$$

One sees that I is a nonzero difference ideal so $1 \in I$. Therefore, there exist $r_1 = 1, r_2, \ldots, r_t \in R$ such that support$\{r_1, \ldots, r_t\} \subset S$ and

$$\phi^i(y_1) + \sum_{j=2}^{t} r_j \phi^i(y_j) = 0 \quad \forall i.$$

Applying ϕ and subtracting, we have

$$\sum_{j=2}^{t} (r_j - \phi(r_j))\phi^i(y_j) = 0 \quad \forall i.$$

Using the minimality of the support, we have that $r_j = \phi(r_j)$. □

LEMMA A.3. *Let (R, ϕ) be a difference ring and let $L(y) = \sum_{i=n}^{m} a_i \phi^i(y)$ with $a_i \in R$. Assume that a_n and a_m are invertible in R and that there exist $y_1, \ldots, y_t \in R$ such that $L(y_i) = 0$ for $i = 1, \ldots, t$. Let $r_i, \ldots, r_t \in R$ satisfy $\sum_{i=1}^{t} r_i \phi^j(y_i) = 0$ for $j = n, \ldots, m$. Then $\sum_{i=1}^{t} r_i \phi^j(y_i) = 0$ for $-\infty < j < \infty$.*

PROOF. For any $j > m$, there exist $a_{i,j} \in R$ such that $\phi^j(y_l) = \sum_{i=n}^{m-1} a_{i,j} \phi^i(y_l)$ for $l = 1, \ldots, t$. Therefore $\sum_l r_l \phi^i(y_l) = \sum_i a_{i,j} \sum_l r_l \phi^j(y_l) = 0$. A similar statement is true for $j < n$. □

We shall need some simple facts from linear algebra over a commutative ring with unit. If R is such a ring and A is an $n \times n$ matrix over R then one can define the determinant $\det(A)$ in the usual way. One has that $\det(A) = \det(A^t)$. Furthermore, if R is a field (or even an integral domain) then $\det(A) = 0$ iff the columns of A are linearly dependent over R. We shall need the following fact

LEMMA A.4. *Let $R = R_1 \oplus \cdots \oplus R_m$ where each R_i is an integral domain and let A be an $n \times n$ matrix with entries in R. The following are equivalent.*

(1) $\mathrm{Det}(A) = 0$.
(2) *For each $i = 1, \ldots, m$, there exists a nonzero $v_i \in R_i^n$ such that $Av_i = 0$.*
(3) *For each $i = 1, \ldots, m$, there exists a nonzero $v_i \in R_i^n$ such that $v_i^t A = 0$.*

PROOF. Let $1 = e_1 + \cdots + e_m$ where $e_i^2 = e_i \in R_i$. We then have $\det(A) = 0$ iff $\det(e_i A) = 0$ for all i. Since each R_i is an integral domain, we have that $\det(A) = 0$ iff there exists a nonzero $v_i \in R_i^n$ such that $Av_i = 0$ for all i. This shows that (1) is equivalent to (2) Since $\det(A) = \det(A^t)$, a similar argument replacing A with A^t shows that (1) is equivalent to (3). □

LEMMA A.5. *Let R be a Picard–Vessiot extension of a difference field k of characteristic zero with algebraically closed field of constants C. Let $L(y) = \sum_{i=n}^{m} a_i \phi^i(y)$ with $a_i \in k$, $a_n a_m \neq 0$ and let V be the solution space of $L(y) = 0$ in R. Then $\dim_C V \leq m - n$.*

PROOF. Corollary 1.16 of van der Put and Singer (1997) states that R may be written as $R = Re_1 \oplus \cdots \oplus Re_l$ where each $e_i^2 = e_i$, $e_1 + \cdots + e_n = 1$ and each Re_i is an integral domain. Let $v = (a_n, \ldots, a_m)^T$. Note that for each i, ve_i is nonzero.

Let $y_1, \ldots, y_t \in V$, $t = m - n + 1$. We may apply Lemma A.4 to the matrix $M = (\phi^i(y_j)_{i=n,\ldots,m}^{j=1,\ldots,t})$ and conclude that there exist $r_1, \ldots, r_t \in R$, not all zero, such that $M(r_1, \ldots, r_t)^T = 0$. Therefore $\sum_{j=1}^{t} r_j \phi^i(y_j) = 0$ for $i = n, \ldots, m$. Lemma A.3 implies that $\sum_{j=1}^{t} r_j \phi^i(y_j) = 0$ for $-\infty < i < \infty$. Lemma A.2 implies that the y_i are linearly dependent over $\mathcal{C}$. □

LEMMA A.6. *Let k be as above and let R be a Picard–Vessiot extension of k. Let G be the Galois group of R and let V be an n-dimensional G-invariant $\mathcal{C}$-space. Then V is the solution space of a linear difference equation of order n with coefficients in k.*

PROOF. Let $y_1, \ldots, y_t$ be a $\mathcal{C}$-basis of V and let $C = C(y_1, \ldots, y_t)$ be the Casoratian matrix. One sees that for each $\sigma \in G$ there exists a matrix $A_\sigma \in \mathrm{GL}_t(\mathcal{C})$ such that $\sigma(C) = CA_\sigma$.

We now claim that $\mathrm{Cas}(y_1, \ldots, y_t) = \det(C) \neq 0$. Assume that this is not the case. Lemma A.4 implies that there exist $r_1, \ldots, r_t \in R$, not all zero such that $(r_2, \ldots, r_t)C = 0$. Among all such, select one with the smallest support S and assume $r_1 \neq 0$. Let $I = \{r \in R | \exists\ r_2, \ldots, r_t$ such that $(r, r_2, \ldots, r_t)C = 0$ and support $(r_1, \ldots, r_t) \subset S\}$. I is a nonzero G-invariant ideal of R, so $1 \in I$ by Corollary 1.15 of van der Put and Singer (1997). Using the minimality of the support, we see that each r_j is G-invariant and so lies in k. Therefore there exist $r_2, \ldots, r_t \in k$ such that $y_i + r_2\phi(y_i) + \cdots, r_t\phi^{t-1}(y_i) = 0$ for each i. This means that the t independent elements $y_1, \ldots, y_t$ satisfy a linear difference equation over k of order at most $t-1$ contradicting Lemma A.5. This contradiction shows that $\mathrm{Cas}(y_1, \ldots, y_t) \neq 0$.

We now claim that $\mathrm{Cas}(y_1, \ldots, y_t)$ is invertible in R. Since

$$\sigma(\mathrm{Cas}(y_1, \ldots, y_t)) = \det(A_\sigma)\,\mathrm{Cas}(y_1, \ldots, y_t),$$

we have that $\mathrm{Cas}(y_1, \ldots, y_t)$ generates a G-invariant ideal. Therefore $1 \in (\mathrm{Cas}(y_1, \ldots, y_t))$.

One now readily sees that $L(y) = \mathrm{Cas}(Y, y_1, \ldots, y_t)/\mathrm{Cas}(y_1, \ldots, y_t)$ has coefficients in k and solution space equal to V. □

COROLLARY A.7. *Let k be as above and let L be a difference operator with coefficients in k. There is a bijective correspondence between the G-invariant subspaces of the solution space of L and the monic right factors of L.*

PROOF. We claim that the bijection is given by associating a monic factor to its solution space. Let L have order n and let V be the solution space of $L(y) = 0$. Let L_1 be a right factor of L of order m and write $L = L_2L_1$. The operator L_1 maps V into the solution space of L_2. Lemma A.5 implies that the kernel of L_1 has dimension at most m and the image has dimension at most $n-m$. Since these dimensions must sum to n, we have that the kernel of L_1 has dimension m and so is the full solution space of L_1. Clearly this space is invariant under the action of G. Now let W be a G-invariant subspace of V of dimension m. Lemma A.6 implies that W is the solution space of a monic operator L_W. We may write $L = QL_W + R$ where Q and R are operators with the order of R at most $m-1$. The operator R annihilates W and so Lemma A.5 implies that it must be zero. □

The following lemma completes the proof of Theorem 3.4.

LEMMA A.8. *Let k be a difference field with algebraically closed constants $\mathcal{C}$. Let R be a Picard–Vessiot ring with Galois group G. If $a, b \in R$ satisfy linear difference equations over k then so do $a-b$ and ab. Furthermore, these linear difference equations have Galois groups that are quotients of G.*

PROOF. Let a satisfy $L_a(y) = 0$ and b satisfy $L_b(y) = 0$ where L_a and L_b have orders n and m respectively.

$a - b$: The ring $k[\phi]$ of difference operators (where $\phi \circ u = \phi(u)\phi$ for $u \in k$) is a left and right Euclidean domain. We can therefore form the least common left multiple $\mathrm{LCLM}(L_a, L_b)$ of L_a and L_b. The space $V = \{u + v \mid L_a(u) = 0,\ L_b(v) = 0\}$ is a G-invariant $\mathcal{C}$-vector space of finite dimension, say t. Clearly, V contains $a - b$ and is a subspace of the solution space W of $\mathrm{LCLM}(L_a, L_b)$. Lemma A.6 implies that V is the solution space of a linear operator L_V of order t. Since L_a and L_b divide L_V on the right we have that $\mathrm{LCLM}(L_a, L_b)$ divides $L_V$on the right. Furthermore, since V is a subspace of W, L_V divides $\mathrm{LCLM}(L_a, L_b)$ on the right, so we have that V is the solution space of $\mathrm{LCLM}(L_a, L_b)$. Let $\phi(Y) = CY$ be the system associated to $\mathrm{LCLM}(L_a, L_b)$. This system has a fundamental matrix $Z = (z_{ij})$ with entries in R. Let $S = k[z_{ij}, 1/\det(Z)] \subset R$. Corollary 1.24 of van der Put and Singer (1997) implies that S is the Picard–Vessiot ring associated to the operator $\mathrm{LCLM}(L_a, L_b)$. Furthermore, Corollary 1.30 of van der Put and Singer (1997) implies that the Galois group is a quotient of G.

ab: Let U and V be difference indeterminates. Formally calculate $UV, \phi(UV), \ldots, \phi^N(UV)$ where $N = n \cdot m$. Each time $\phi^j(U), j \geq n$ (resp., $\phi^j(V), j \geq m$) occurs use the relation $L_a(U) = 0$ (resp., $L_b(V) = 0$) and replace this with a k-linear combination of the $U, \phi(U), \ldots, \phi^{n-1}(U)$ (resp., $V, \phi(V), \ldots, \phi^{m-1}(V)$). One then has $N + 1$ linear forms in the N expressions $\phi^i(U)\phi^j(V),\ 0 \leq i \leq n-1, 0 \leq j \leq m-1$. One must therefore have a k-linear relation among these and therefore among the $\phi^i(UV),\ i = 0, \ldots, N$. Among all such relations, select one where the highest power of ϕ appearing is minimal. We claim that this will yield a difference equation $L(y) = 0$ whose solution space is $W = span\{uv \mid L_a(u) = 0,\ L_b(v) = 0\}$.

Let $\tilde{L}$ be a nonzero operator of order smaller than the order of L. In $\tilde{L}(y) = 0$ replace y by UV and then replace each $\phi^j(U), j \geq n$ (resp., $\phi^j(V), j \geq m$) with a k-linear combination of the $U, \phi(U), \ldots, \phi^{n-1}(U)$ (resp., $V, \phi(V), \ldots, \phi^{m-1}(V)$) as above. The above construction insures that the resulting polynomial $P(U, V) \in k[\phi^i(U), \phi^j(V)]_{i=0,\ldots,n-1}^{j=0,\ldots,m-1}$ is nonzero. Let R be as in the hypotheses. In particular R contains full sets of solutions $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_m\}$ of $L_a(y) = 0$ and $L_b(y) = 0$ respectively such that the matrices $\mathcal{U} = (\phi^i(u_j))_{i=0,\ldots,n-1}^{j=1,\ldots,n}, \mathcal{V} = (\phi^i(v_j))_{i=0,\ldots,m-1}^{j=1,\ldots,m}$ are invertible in R. In the ring $R[\phi^i(U), \phi^j(V)]_{i=0,\ldots,n-1}^{j=0,\ldots,m-1}$, we consider the substitutions

$$\begin{pmatrix} U \\ \phi(U) \\ \vdots \\ \phi^{n-1}(U) \end{pmatrix} \mapsto \mathcal{U} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}, \qquad \begin{pmatrix} V \\ \phi(V) \\ \vdots \\ \phi^{m-1}(V) \end{pmatrix} \mapsto \mathcal{V} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix},$$

where the c_i and d_i are indeterminates. These substitutions are invertible so the resulting polynomial $\tilde{P}(c_i, d_j) \in R[c_i, d_j]$ is again nonzero. Therefore we can find $\tilde{c}_i$ and $\tilde{d}_j \in \mathcal{C}$ such that $\tilde{P}(\tilde{c}_i, \tilde{d}_j) \neq 0$. Therefore, for $\tilde{u} = \sum c_i u_i$ and $\tilde{v} = \sum d_i v_i$, we have that $\tilde{L}(\tilde{u}\tilde{v}) \neq 0$.

Therefore W lies in the solution space of no operator of order smaller than the order of L. Since W does lie in the solution space of L and is the solution space of some operator, we must have that W is the solution space of L.

The Picard–Vessiot extension corresponding to L lies in R and, as before, we see that the Galois group of L is a quotient of G. □

Remarks. (1) The above lemma implies that any element of R satisfies a linear difference equation over k. This follows by induction since the ring R is generated by solutions of linear difference equations and $w = 1/\det(Y)$ where Y is a fundamental matrix for a system $\phi(Y) = AY$ (note that w satisfies $\phi(w) = (1/\det A)w$).

(2) From the proof of the lemma one sees that if the field operations and ϕ are effective, then one can effectively construct the equations for ab and $a - b$ once one knows the equations for a and b. Furthermore, if a and b satisfy difference equations of orders n and m respectively, then ab and $a - b$ satisfy difference equations of order at most nm and $n + m$ respectively.

Appendix B. Systems and Scalar Equations

Let k be a difference field of characteristic zero with automorphism ϕ and constants $\mathcal{C}$. In this section we shall show the equivalence between systems $\phi(Y) = AY,\ A \in \mathrm{GL}_n(k)$ and nth-order linear homogeneous difference equations $L(y) = 0$. As in the differential case, this is done by proving a cyclic vector lemma for the appropriate modules.

Let Φ be an indeterminate. By a *difference module* M we mean a finite dimensional k-vector space M that is also a left $k[\Phi, \Phi^{-1}]$-module where $\Phi(am) = \phi(a)\Phi(m)$ and $\Phi^{-1}(am) = \phi^{-1}(a)\Phi^{-1}(m)$ for all $a \in k$, $m \in M$. We will show that, under suitable hypotheses, such a module contains a cyclic vector, that is, a vector v such that $\{v, \phi(v), \ldots, \phi^{n-1}(v)\}$ is a k-basis for M for some n. To do this we use the following lemma whose differential version appears in the unpublished notes of Kovacic (1996). The proof given here of this lemma is identical, *mutatis mutandis*, to the one appearing in that paper. The proof of the theorem is only slightly different from the corresponding differential result appearing in that paper.

Lemma B.1.

Let F be a nonzero element of the ring of difference polynomials $k\{y_1, \ldots, y_n\}$. Suppose that $\mathrm{ord}(F) = r - 1$ *and* $\deg(F) = s$. *If $\eta_1, \ldots, \eta_r \in k$ are linearly independent over $\mathcal{C}$, then there exist integers $0 \le c_{ij} \le s,\ (1 \le i \le n, 1 \le j \le r)$, such that $F(a_1, \ldots, a_n) \ne 0$ where $a_i = c_{i1}\eta_1 + \cdots + c_{ir}\eta_r$.*

Proof. Let $C_{ij},\ (1 \le i \le n, 1 \le j \le r)$ be indeterminates over k (in the ordinary, not difference, sense). Since the $\phi^{j-1}(y_i)$ are algebraically independent over k we may define a (nondifference) homomorphism $\psi : k[\phi^{j-1}(y_i)] \longrightarrow k[C_{ij}], (1 \le i \le n, 1 \le j \le r)$, by the formula $\psi(\phi^{j-1}(y_i)) = \sum_{t=1}^{r} C_{it}\phi^{j-1}\eta_t$. Let $G = \psi(F)$.

Since the η_i are linearly independent over $\mathcal{C}$, their Casoratian $\det(\phi^{j-1}(\eta_i))$ is not zero. Therefore ψ is an isomorphism and $\deg(G) = s$. We shall now use induction on nr to prove the conclusion. If $nr = 1$, then G is an ordinary polynomial in one variable of degree s. Since such a polynomial has at most s roots, there exists $0 \le c \le s$ such that $G(s) \ne 0$.

Now assume that $nr > 1$. Select a variable C_{uv} that appears in G, and think of G as a polynomial in C_{uv} with coefficients that are polynomials in the other variables. By

induction, there exist $0 \leq c_{ij} \leq s$ with $(i,j) \neq (u,v)$, that do not annihilate the leading coefficient of G. Substituting these into G, we get a polynomial in one variable C_{uv} and we can find a remaining c_{uv} to make $G(c) \neq 0$. Let $a_i = c_{i1}\eta_1 + \cdots + c_{ir}\eta_r$. Since $F(a_1, \ldots, a_n) = G(c) \neq 0$ we have proven the lemma. □

Recall that an element a of k is said to be *periodic (of period m)* if $\phi^m(a) = a$ for some positive integer m. If a is periodic of period m, then the symmetric functions of $a, \phi(a), \ldots, \phi^{m-1}(a)$ are left fixed by ϕ and so a is algebraic over the constants $\mathcal{C}$. Conversely, any element algebraic over $\mathcal{C}$ is periodic, so the periodic elements of k form the algebraic closure of $\mathcal{C}$ in k. Note that if a is not periodic, then for any m the elements $1, a, \ldots, a^{m-1}$ are linearly independent over $\mathcal{C}$.

THEOREM B.2. *Let k be a difference field of characteristic zero with constants $\mathcal{C}$. Assume that k contains an element that is not periodic. If M is a $k[\Phi, \Phi^{-1}]$-module, then M contains a cyclic vector.*

If $k = \mathcal{C}(x), \phi(x) = x + 1$ and $\{e_1, \ldots, e_n\}$ is a basis of M, then there exist integers $0 \leq c_{ij} \leq n$, $(1 \leq i \leq n, 1 \leq j \leq r)$, such that $v = \sum_{i=1}^{n} a_i e_i$ is a cyclic vector of M, where $a_i = \sum_{j=1}^{n} c_{ij} x^{j-1}$.

PROOF. Let $e_1, \ldots, e_n$ be a basis of M and let $\Phi(e_i) = \sum_{j=1}^{n} a_{ji} e_j$. With respect to this basis we may identify M with k^n and we then have for any $u = (u_1, \ldots, u_n)^T \in k^n$,

$$\Phi \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = A \begin{pmatrix} \phi(u_1) \\ \vdots \\ \phi(u_n) \end{pmatrix},$$

where $A = (a_{ji})$. Let $y_1, \ldots, y_n$ be indeterminates (in the difference sense) over k. Then $N = k < y_1, \ldots, y_n > \otimes_k M$ is a difference module over $k < y_1, \ldots, y_n >$ with basis $1 \otimes e_1, \ldots, 1 \otimes e_n$. With respect to this basis let $f = (y_1, \ldots, y_n)^T$. We then have that

$$\Phi^i(f) = \phi^{i-1}(A) \cdots \phi(A) A \begin{pmatrix} \phi^i(y_1) \\ \vdots \\ \phi^i(y_n) \end{pmatrix}. \tag{B.2}$$

We shall show that f is a cyclic vector for N and that we can specialize the y_i to get a cyclic vector for M. Let B be the matrix whose ith column is the right-hand side of equation (B.2). The determinant of B lies in the ring $k[\phi^i(y_j)], (0 \leq i \leq n-1,\ 1 \leq j \leq n)$. We shall show that $\det(B) \neq 0$. To see this replace each n-tuple $(\phi^{i-1}(y_1), \ldots, \phi^{i-1}(y_n))^T$ with $A^{-1}\phi(A^{-1}) \cdots \phi^{i-1}(A^{-1})(\phi^{i-1}(y_1), \ldots, \phi^{i-1}(y_n))^T$ in the polynomial $\det(B)$. The resulting polynomial is $\det(\phi^{i-1}(y_j))$. Since this polynomial is clearly nonzero, we must have $\det(B) \neq 0$. This implies that $f, \Phi(f), \ldots, \Phi^{n-1}(f)$ are linearly independent over $k < y_1, \ldots, y_m >$ and so f is a cyclic vector for N.

Let $a \in k$ be an element that is not periodic. In particular, $1, a, \ldots, a^{n-1}$ are linearly independent over $\mathcal{C}$. The difference polynomial $F = \det(B)$ is of degree n and order $n-1$, so Lemma B.1 implies that there exist integers $0 \leq c_{ij} \leq n$, $(1 \leq i \leq n, 1 \leq j \leq n)$, such that $F(a_1, \ldots, a_n) \neq 0$ where $a_i = c_{i1}1 + \cdots + c_{in}a^{n-1}$. Therefore $v = a_1 e_1 + \cdots + a_n e_n$ is a cyclic vector for M. When $k = \mathcal{C}(x)$, we can let $a = x$ and so conclude the final statement of the theorem. □

We are now in a position to describe the equivalence between first-order systems $\phi(Y) = AY$ of difference equations and nth-order linear scalar difference equations $L(y) = \phi^n(y) - a_{n-1}\phi^{n-1}(y) - \cdots - a_0 y = 0$. Given such a scalar equation we have already noted in Section 2 that one can form the system $\phi(Y) = A_L Y$ where A_L is the companion matrix of L.

Conversely, let k be a difference field of characteristic zero containing an element that is not periodic and let $\phi(Y) = AY$, $A \in \mathrm{GL}_n(k)$. Let k^o be the difference field whose underlying field is k and whose automorphism is ϕ^{-1}. Let M be the difference module $(k^o)^n$ over k^o defined by

$$\Phi \begin{pmatrix} u_1 \\ u_2 \\ \cdots \\ u_n \end{pmatrix} = A \begin{pmatrix} \phi^{-1}(u_1) \\ \phi^{-1}(u_2) \\ \cdots \\ \phi^{-1}(u_n) \end{pmatrix}.$$

Let $\mathbf{e} = \{e_1, \ldots, e_m\}$ be the usual basis of k^n and let $\mathbf{f} = \{v, \Phi(v), \ldots, \Phi^{n-1}(v)\}$ where v is a cyclic vector of M (over k^o). Note that with respect to $\mathbf{f}$, Φ has the matrix

$$B = \begin{pmatrix} 0 & 0 & 0 & \ldots & a_1 \\ 1 & 0 & 0 & \ldots & a_0 \\ 0 & 1 & 0 & \ldots & a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & a_{n-1} \end{pmatrix}$$

for some $a_i \in k$. If $w \in M$, we shall let $w_{\mathbf{e}}$ (resp. $w_{\mathbf{f}}$) be its vector of coordinates with respect to $\mathbf{e}$ (resp. $\mathbf{f}$). Let U be the change of basis matrix, i.e. $w_{\mathbf{f}} = U w_{\mathbf{e}}$ for all $w \in M$. We then have that $B = \phi^{-1}(U) A^T U^{-1}$ and so $B^T = \phi(V) A V^{-1}$, where $V = \phi^{-1}(U^T)^{-1}$. The matrix B^T is the companion matrix of a scalar equation $L(y) = 0$. Furthermore, Y is a solution of $\phi(Y) = AY$, iff $Z = VY$ is a solution of $\phi(Z) = B^T Z$. Therefore the system $\phi(Y) = AY$ is equivalent to the scalar equation whose companion matrix is B^T.

Originally Received 22 April 1998
Accepted 22 September 1998