JEMS

Michael Wibmer

Skolem–Mahler–Lech type theorems and Picard–Vessiot theory

Abstract. We show that three problems involving linear difference equations with rational function coefficients are essentially equivalent. The first problem is the generalization of the classical Skolem–Mahler–Lech theorem to rational function coefficients. The second problem is whether or not for a given linear difference equation there exists a Picard–Vessiot extension inside the ring of sequences. The third problem is a certain special case of the dynamical Mordell–Lang conjecture.

   This allows us to deduce solutions to the first two problems in a particular but fairly general special case.

Keywords. Linear difference equations, Picard–Vessiot theory, Skolem–Mahler–Lech theorem, dynamical Mordell–Lang conjecture

1. Introduction

Let k be a field of characteristic zero and

$$E: \quad \sigma^n(y) + h_{n-1}\sigma^{n-1}(y) + \cdots + h_0 y = 0$$

a linear difference equation with rational function coefficients $h_{n-1}, \ldots, h_0 \in k(z)$. We shall be concerned with the following two problems:

Problem SML. Let $f: \mathbb{N} \to k$ be a sequential solution of E, that is,

$$f(i+n) + h_{n-1}(i)f(i+n-1) + \cdots + h_0(i)f(i) = 0 \quad \text{for } i \gg 0.$$

Is the set $\{i \in \mathbb{N} \mid f(i) = 0\}$ a finite union of arithmetic progressions?

Problem PV. Does there exist a Picard–Vessiot extension of $k(z)$ for E inside the ring of k-valued sequences?

As we shall see shortly, these two problems are intimately connected. If the difference equation E has constant coefficients, i.e., if $h_{n-1}, \ldots, h_0 \in k$, then the answer to Problem SML is affirmative. This result is known as the Skolem–Mahler–Lech theorem. The

M. Wibmer: Lehrstuhl für Mathematik (Algebra), RWTH Aachen, 52056 Aachen, Germany;
e-mail: michael.wibmer@matha.rwth-aachen.de

reader is referred to the introduction of [Bel06] for proper attributions and more background on this celebrated theorem. Using p-adic techniques it has recently been shown in [BBY12] that the answer is also affirmative if $h_{n-1}, \dots, h_1 \in k[z]$ are polynomials and $h_0 \in k \smallsetminus \{0\}$ is a non-zero constant. Here we will give a new proof of this result based on Picard–Vessiot theory and a special case of the dynamical Mordell–Lang conjecture established by J. Bell [Bel06]. We also explain how a certain special case of the dynamical Mordell–Lang conjecture would imply an affirmative solution to problems SML and PV in general. We solve Problem PV affirmatively under the restriction $h_{n-1}, \dots, h_1 \in k[z]$ and $h_0 \in k \smallsetminus \{0\}$.

2. Picard–Vessiot theory and preliminaries

We start by recalling the basic definitions from Picard–Vessiot theory, the Galois theory of linear difference equations. The standard reference for this is [vdPS97]. We will also use some standard notations from difference algebra, see [Coh65] or [Lev08].

   All rings are assumed to be commutative. We set $\mathbb{N} := \{0, 1, 2, \dots\}$. A *difference ring*, or σ-*ring* for short, is a ring R equipped with a ring endomorphism $\sigma \colon R \to R$. A morphism of difference rings is a morphism of rings that commutes with σ. A σ-*field* is a σ-ring whose underlying ring is a field. The difference field we shall be most interested in is the field $K = k(z)$ of rational functions in the variable z over a field k of characteristic zero, equipped with the automorphism σ defined by $\sigma(h(z)) = h(z + 1)$ for $h \in k(z)$. For a difference ring R the *constants* of R are $R^\sigma := \{r \in R \mid \sigma(r) = r\}$. Note that in our example, $K^\sigma = k$.

   Instead of a linear difference equation of order n, as in the introduction, we shall consider the slightly more general situation of a square first order system $\sigma(y) = Ay$ where $A \in \mathrm{GL}_n(K)$ and y is a vector of length n.

Definition 2.1. Let K be a σ-field and $A \in \mathrm{GL}_n(K)$. A K-σ-algebra is called a *Picard–Vessiot ring* for $\sigma(y) = Ay$ if

 (i) R is generated by a fundamental solution matrix for $\sigma(y) = Ay$, i.e., there exists $Y \in \mathrm{GL}_n(R)$ such that $\sigma(Y) = AY$ and $R = K[Y_{ij}, 1/\det(Y)]$,
(ii) R is σ-*simple*, i.e., R has no non-trivial σ-ideals.

It is a characteristic feature of the Galois theory of linear difference equations that the Picard–Vessiot ring is usually not an integral domain, in contrast to the case of linear differential equations (see e.g. [vdPS03].) However, like any Noetherian σ-simple σ-ring R, a Picard–Vessiot ring has a certain simple algebraic structure (see [vdPS97, Cor. 1.16, p. 12] or [Wib10, Prop. 1.1.2, p. 2]). Namely, there exist orthogonal idempotents $e_0, \dots, e_{l-1} \in R$ such that

  (i) $R = e_0 R \oplus \cdots \oplus e_{l-1} R$,
 (ii) $\sigma(e_0) = e_1, \sigma(e_1) = e_2, \dots, \sigma(e_{l-1}) = e_0$,
(iii) the ring $e_i R$ is σ^l-simple and an integral domain for $i = 0, \dots, l-1$.

We will call the integer l the *period* of R. It is precisely this simple algebraic structure of the Picard–Vessiot ring that is at the core of the connection between Picard–Vessiot theory and Problem SML. In fact we will see (Proposition 3.5) that in many cases the period of the Picard–Vessiot ring is a bound for the period of the arithmetic progressions appearing in Problem SML.

It is sometimes more convenient or even necessary (e.g. for Galois correspondence) to work with the total ring of fractions of the Picard–Vessiot ring rather than with the Picard–Vessiot ring itself. If L is the total ring of fractions of a Noetherian σ-simple σ-ring then there exist orthogonal idempotents $e_0, \ldots, e_{l-1} \in L$ such that

(i) $L = e_0 L \oplus \cdots \oplus e_{l-1} L$,
(ii) $\sigma(e_0) = e_1, \sigma(e_1) = e_2, \ldots, \sigma(e_{l-1}) = e_0$,
(iii) $e_i L$ is a field for $i = 0, \ldots, l - 1$.

Conversely, if L is a σ-ring satisfying the above three properties then L is a Noetherian σ-simple σ-ring such that every non-zero divisor is invertible. We will call such σ-rings σ-*pseudo fields*.

Definition 2.2. Let K be a σ-field and $A \in \mathrm{GL}_n(K)$. A σ-pseudo field extension L of K is called a *Picard–Vessiot extension* for $\sigma(y) = Ay$ if

(i) L is generated by a fundamental solution matrix for $\sigma(y) = Ay$, i.e., there exists $Y \in \mathrm{GL}_n(L)$ such that $\sigma(Y) = AY$ and $L = K(Y_{ij})$ (to be precise, this notation means that L is the total ring of fractions of $K[Y_{ij}]$),
(ii) $L^\sigma = K^\sigma$.

It is easy to see that a Picard–Vessiot ring always exists for a given equation $\sigma(y) = Ay$, $A \in \mathrm{GL}_n(K)$: Consider the universal solution ring $U = K[Z_{ij}, 1/\det Z]$ where Z is an $n \times n$-matrix of indeterminates. We consider U as a K-σ-algebra by setting $\sigma(Z) = AZ$. Then any quotient of U modulo a maximal element in the set of all σ-ideals of U is a Picard–Vessiot ring.

Under the assumption that $\sigma \colon K \to K$ is surjective and K^σ is algebraically closed it is shown in [vdPS97] that a Picard–Vessiot ring for a given linear system $\sigma(y) = Ay$ is unique up to K-σ-isomorphisms. Moreover, the total ring of fractions of a Picard–Vessiot ring is a Picard–Vessiot extension. Under the additional hypothesis that K is perfect it is also shown that $K[Y_{ij}, 1/\det(Y)] \subset L$ is a Picard–Vessiot ring for $\sigma(y) = Ay$ if L is a Picard–Vessiot extension for $\sigma(y) = Ay$ with fundamental solution matrix $Y \in \mathrm{GL}_n(L)$.

If K^σ is not algebraically closed, a Picard–Vessiot extension for $\sigma(y) = Ay$ might or might not exist. However, if $K = k(z)$ with $\sigma(z) = z + 1$ then one can show that there always exists a Picard–Vessiot extension (Proposition 2.4).

Let K be a σ-field and R a K-σ-algebra. An element $f \in R$ is called σ-*finite* (over K) if f satisfies a linear σ-equation over K. This is equivalent to saying that f is contained in a finite-dimensional K-vector subspace of R which is stable under σ. For later reference we note the following simple fact:

Lemma 2.3. *Let R be a Picard–Vessiot ring for some equation $\sigma(y) = Ay$ over some σ-field K. Then every element of R is σ-finite over K.*

Proof. Let $Y \in \mathrm{GL}_n(R)$ be a fundamental solution matrix for $\sigma(y) = Ay$. Then the finite-dimensional K-vector subspace of R generated by all Y_{ij} and $\det(Y)$ is stable under σ. The claim follows because sums and products of σ-finite elements are σ-finite. $\qquad\square$

Let k be a field of characteristic zero. We define the ring Seq_k of k-valued sequences as in [vdPS97, Example 1.3, p. 4]: Two sequences $f, g\colon \mathbb{N} \to k$ are identified if $f(i) = g(i)$ for all $i \gg 0$. Addition and multiplication are defined componentwise. We shall be rather careless about the distinction between an element $f \in k^{\mathbb{N}}$ and its equivalence class in Seq_k. In particular, the equivalence class of f will often be denoted by $(f(0), f(1), \ldots)$. We consider Seq_k as a σ-ring by shifting to the left, that is,

$$\sigma(f) = (f(1), f(2), \ldots).$$

For $f \in \mathrm{Seq}_k$ the set $\{i \in \mathbb{N} \mid f(i) = 0\}$ is strictly speaking not well-defined. However, if we identify two subsets M_1, M_2 of $\mathbb{N}$ if the difference $M_1 \smallsetminus M_2$ (or equivalently $M_2 \smallsetminus M_1$) is finite, then $\{i \in \mathbb{N} \mid f(i) = 0\}$ yields a well-defined equivalence class. We will usually consider subsets of $\mathbb{N}$ modulo this equivalence relation.

By an *arithmetic progression* we mean a subset of $\mathbb{N}$ of the form $j + \mathbb{N}l$ with $j, l \in \mathbb{N}$. In particular, the one-element set $\{j\}$ is considered to be an arithmetic progression. Therefore the property of a subset of $\mathbb{N}$ to be a finite union of arithmetic progressions passes down to equivalence classes. The integer l is called the *period* of the arithmetic progression $j + \mathbb{N}l$.

One advantage of the ring Seq_k compared to $k^{\mathbb{N}}$ is that we can consider $k(z)$ as a subring of Seq_k. In fact, the map

$$k(z) \to \mathrm{Seq}_k, \quad h \mapsto (h(0), h(1), h(2), \ldots),$$

is a morphism of difference rings, i.e., Seq_k is a $k(z)$-σ-algebra. (The expression $(h(0), h(1), h(2), \ldots)$ is well-defined because a rational function has only finitely many poles.)

For a given linear system $\sigma(y) = Ay$ with $A \in \mathrm{GL}_n(K)$ where $K = k(z)$, $\sigma(z) = z + 1$ it seems quite natural to ask whether or not there exists a Picard–Vessiot extension for $\sigma(y) = Ay$ inside Seq_k. The fact that $(\mathrm{Seq}_k)^{\sigma} = k = K^{\sigma}$ seems to speak in favor of an affirmative answer. In [vdPS97, Prop. 4.1, p. 45] it is shown, under the assumption that k is algebraically closed, that there always exists a Picard–Vessiot ring inside Seq_k. This is not sufficient to deduce the existence of a Picard–Vessiot extension inside Seq_k because a non-zero divisor in the Picard–Vessiot ring could be a zero divisor in Seq_k.

The following proposition removes the restriction of k being algebraically closed.

Proposition 2.4. *Let k be a field of characteristic zero and $A \in \mathrm{GL}_n(k(z))$. Then there exists a Picard–Vessiot ring for $\sigma(y) = Ay$ inside Seq_k. Moreover there exists a Picard–Vessiot extension for $\sigma(y) = Ay$.*

Proof. It is easy to construct a fundamental solution matrix Y for $\sigma(y) = Ay$ inside Seq_k: If we choose $i_0 \in \mathbb{N}$ large enough then $A(i)$ is defined and $\det(A)(i)$ is non-zero for every $i \geq i_0$. Set $Y(i_0)$ to be the identity matrix and recursively define $Y(i + 1) =$

$A(i)Y(i)$ for $i \geq i_0$. Then $Y \in \mathrm{GL}_n(\mathrm{Seq}_k)$ and $\sigma(Y) = AY$. We have to show that $R := k(z)[Y_{ij}, 1/\det(Y)] \subset \mathrm{Seq}_k$ is σ-simple.

Let $\bar{k}$ denote an algebraic closure of k. We know from [vdPS97, Prop. 4.1, p. 45] that $\bar{R} := \bar{k}(z)[Y_{ij}, 1/\det(Y)]$ is a Picard–Vessiot ring for $\sigma(y) = Ay$ over $\bar{k}(z)$. Since the natural map $\mathrm{Seq}_k \otimes_k \bar{k} \to \mathrm{Seq}_{\bar{k}}$ is injective, also $R \otimes_k \bar{k} \to \bar{R}$ is injective. Therefore $\bar{R} = R \otimes_k \bar{k}$. A non-trivial σ-ideal $\mathfrak{a}$ of R would give rise to a non-trivial σ-ideal $\mathfrak{a} \otimes_k \bar{k}$ of $\bar{R}$. Consequently, R must be σ-simple, i.e., R is a Picard–Vessiot ring for $\sigma(y) = Ay$.

The total quotient ring L of R is a σ-pseudo field, generated by a fundamental solution matrix for $\sigma(y) = Ay$. It remains to see that $L^\sigma = k$. So let $g \in L^\sigma$. The set $\{f \in R \mid fg \in R\}$ is a non-zero σ-ideal of R. Because R is σ-simple, this ideal must contain 1, i.e., $g \in R^\sigma$. But $R^\sigma = k$ because $(\mathrm{Seq}_k)^\sigma = k$. $\qquad\square$

A Picard–Vessiot ring or a Picard–Vessiot extension for a linear equation $\sigma(y) = Ay$ over $K = k(z)$ need not be unique up to K-σ-isomorphisms if $k = K^\sigma$ is not algebraically closed. However, inside Seq_k there only exists one Picard–Vessiot ring:

Remark 2.5. Let k be a field of characteristic zero and $A \in \mathrm{GL}_n(k(z))$. The Picard–Vessiot ring $R \subset \mathrm{Seq}_k$ for $\sigma(y) = Ay$ is set-theoretically unique. In fact, if $Y \in \mathrm{GL}_n(\mathrm{Seq}_k)$ is any fundamental solution matrix for $\sigma(y) = Ay$ then $R = k(z)[Y_{ij}, 1/\det(Y)]$.

Proof. Let $Y' \in \mathrm{GL}_n(R) \subset \mathrm{GL}_n(\mathrm{Seq}_k)$ be a fundamental solution matrix for $\sigma(y) = Ay$. Then $Y' = YC$ for some matrix $C \in \mathrm{GL}_n((\mathrm{Seq}_k)^\sigma) = \mathrm{GL}_n(k)$. (Simply compute $\sigma(Y^{-1}Y')$.) Therefore $R = k(z)[Y'_{ij}, 1/\det(Y')] = k(z)[Y_{ij}, 1/\det(Y)]$. $\qquad\square$

3. Dynamical Mordell–Lang and main results

Let $\sigma \colon X \dashrightarrow X$ be a rational map on a variety X. Let U be the largest open subset such that σ is defined on U. For $x \in X$ we say that the orbit $\mathcal{O}_\sigma(x)$ is defined if $x \in U$, $\sigma(x) \in U$, …. The *dynamical Mordell–Lang conjecture* is a fundamental problem in algebraic dynamics:

Problem DML. Let X be a variety over a field of characteristic zero equipped with a rational map $\sigma \colon X \dashrightarrow X$. Let $x \in X$ be such that $\mathcal{O}_\sigma(x)$ is defined and let Y be a closed subvariety of X. When is the set $\{i \in \mathbb{N} \mid \sigma^i(x) \in Y\}$ a finite union of arithmetic progressions?

Several special cases of the dynamical Mordell–Lang conjecture have already been established. We refer the reader to [BGT10] and [GT09] for an overview. The most relevant special case for us is due to J. Bell [Bel06] and solves the case when X is affine and $\sigma \colon X \to X$ is an everywhere defined invertible morphism.

Now we are prepared to prove our main result:

Theorem 3.1. *Let k be a field of characteristic zero and $A \in \mathrm{GL}_n(k(z))$. Set $X = \mathbb{A}^1_k \times \mathrm{GL}_{n,k}$ and define a rational map $\sigma \colon X \dashrightarrow X$ by*

$$\sigma(b, B) = (b + 1, A(b)B).$$

Then the following statements are equivalent:

(i) *For every* $x = (b, B) \in X(k)$ *with* $b \in \mathbb{N}$ *and* $\mathcal{O}_\sigma(x)$ *defined and every closed subvariety* $Y \subset X$, *the set* $\{i \in \mathbb{N} \mid \sigma^i(x) \in Y\}$ *is a finite union of arithmetic progressions.*

(ii) *There exists a point* $x = (b, B) \in X(k)$ *with* $b \in \mathbb{N}$ *and* $\mathcal{O}_\sigma(x)$ *defined such that for every closed subvariety* $Y \subset X$ *the set* $\{i \in \mathbb{N} \mid \sigma^i(x) \in Y\}$ *is a finite union of arithmetic progressions.*

(iii) *There exists a Picard–Vessiot extension of* $k(z)$ *for* $\sigma(y) = Ay$ *inside* Seq_k.

Proof. We start by showing that (iii) implies (i): Let $x = (b, B) \in X(k)$ be such that $b \in \mathbb{N}$ and $\mathcal{O}_\sigma(x)$ is defined. We can define a map ψ from $k[X] = k[z, Z_{ij}, 1/\det(Z)]$ to Seq_k by setting

$$\psi(f) := (*, \ldots, *, f(x), f(\sigma(x)), f(\sigma^2(x)), \ldots)$$

where $f(x)$ is on position $b \in \mathbb{N}$. Then ψ is a morphism of $k[z]$-algebras and extends to a morphism $\psi \colon k(z)[Z_{ij}, 1/\det(Z)] \to \mathrm{Seq}_k$ of $k(z)$-algebras. As in the remark after Definition 2.2 we consider $U = k(z)[Z_{ij}, 1/\det(Z)]$ as a $k(z)$-σ-algebra by virtue of $\sigma(Z) = AZ$. As $\sigma(x) = (b + 1, A(b)B)$, $\sigma^2(x) = (b + 2, A(b + 1)A(b)B), \ldots$ for $f = f(z, Z) \in U$ we have

$$\begin{aligned}
\psi(\sigma(f)) &= \psi(f(z + 1, A(z)Z)) \\
&= (*, \ldots, *, f(b + 1, A(b)B), f(b + 2, A(b + 1)A(b)B), \ldots) \\
&= (*, \ldots, *, f(\sigma(x)), f(\sigma^2(x)), \ldots) = \sigma(\psi(f)).
\end{aligned}$$

So $\psi \colon U \to \mathrm{Seq}_k$ is a morphism of $k(z)$-σ-algebras.

By Proposition 2.4 there exists a Picard–Vessiot ring $R \subset \mathrm{Seq}_k$ for $\sigma(y) = Ay$. Because $\psi(Z) \in \mathrm{GL}_n(\mathrm{Seq}_k)$ is a fundamental solution matrix for $\sigma(y) = Ay$ it follows from Remark 2.5 that $\psi(U) = R$. As explained in Section 2, the ring R is of the form $R = e_0 R \oplus \cdots \oplus e_{l-1} R$ where

(i) $e_j^2 = e_j$ for $j = 0, \ldots, l - 1$,
(ii) $e_j e_k = 0$ for $j \neq k$,
(iii) $\sigma(e_0) = e_1, \sigma(e_1) = e_2, \ldots, \sigma(e_{l-1}) = e_0$

and $e_j R$ is an integral domain for $j = 0, \ldots, l - 1$. The unique set $e_0, \ldots, e_{l-1}$ of elements of Seq_k satisfying properties (i), (ii) and (iii) consists of the indicator functions of the arithmetic progressions $j + \mathbb{N}l$, $j = 0, \ldots, l - 1$. So after possibly renumbering the e_j's we can assume that e_j is the indicator function of $j + \mathbb{N}l$ for $j = 0, \ldots, l - 1$.

By assumption there exists a Picard–Vessiot extension $L|k(z)$ for $\sigma(y) = Ay$ inside Seq_k. Let $Y \in \mathrm{GL}_n(L)$ be a fundamental solution matrix for $\sigma(y) = Ay$. Then it follows again from Remark 2.5 that $R = k(z)[Y_{ij}, 1/\det(Y)] \subset L$. So $L = k(z)(Y_{ij})$ is the total ring of fractions of R.

Let $g \in R$. Clearly, every non-zero element of $e_j R$ is invertible in $e_j L$. Because $e_j L$ lives inside Seq_k this implies that either $e_j g$ is zero or $e_j g$ is (eventually) non-zero on

every element of $j + \mathbb{N}l$. In summary, this shows that for every element $g = e_0 g + \cdots + e_{l-1} g \in R$ the set $\{i \in \mathbb{N} \mid g(i) = 0\}$ is a finite union of arithmetic progressions of period l.

We have to show that $\{i \in \mathbb{N} \mid \sigma^i(x) \in Y\}$ is a finite union of arithmetic progressions for every closed subvariety $Y \subset X$. The case when $Y = \mathbb{V}(f)$ ($f \in k[X]$) is a hypersurface follows from the above result because $\psi(f) \in R$ and

$$\{i \in \mathbb{N} \mid \sigma^i(x) \in Y\} = \{i \in \mathbb{N} \mid f(\sigma^i(x)) = 0\} = \{i \in \mathbb{N} \mid \psi(f)(i + b) = 0\}.$$

The general case follows from the hypersurface case because every closed subvariety is a finite intersection of hypersurfaces, and the intersection of two finite unions of arithmetic progressions is again a finite union of arithmetic progressions. This finishes the proof that (iii) implies (i).

The implication (i)⟹(ii) is immediate because the set of $b \in \mathbb{N}$ which are zeros of a denominator appearing in an entry of A is finite.

So it only remains to prove that (ii) implies (iii). Let $x = (b, B) \in X(k)$ be such that $b \in \mathbb{N}$ and $\mathcal{O}_\sigma(x)$ is defined. As in the first part of the proof, we obtain a $k(z)$-σ-morphism $\psi: U \to \mathrm{Seq}_k$. We know from Proposition 2.4 that there exists a Picard–Vessiot ring for $\sigma(y) = Ay$ inside Seq_k and it follows from Remark 2.5 that $\psi(U)$ is that Picard–Vessiot ring. To construct a Picard–Vessiot extension inside Seq_k it suffices to show that every non-zero divisor of $\psi(U)$ is a non-zero divisor (i.e., a unit) in Seq_k. So let $f' \in U$ be such that $\psi(f')$ is a non-zero divisor in $\psi(U)$. Suppose for a contradiction that $\psi(f')$ is a zero divisor in Seq_k.

There exists a $p \in k[z] \smallsetminus \{0\}$ such that $f = pf'$ lies in $k[z, Z_{ij}, 1/\det(Z)] = k[X]$. Because $\psi(f')$ is a non-zero divisor in $\psi(U)$ and $\psi(p)$ is a unit in $\psi(U)$, $\psi(f)$ is a non-zero divisor in $\psi(U)$. Because $\psi(f')$ is a zero divisor in Seq_k, $\psi(f)$ is a zero divisor in Seq_k. This means that $\psi(f)$ assumes the value zero an infinite number of times.

By assumption the set $\{i \in \mathbb{N} \mid \sigma^i(x) \in \mathbb{V}(f)\} = \{i \in \mathbb{N} \mid \psi(f)(i + b) = 0\}$ is a finite union of arithmetic progressions. Thus there exists an infinite arithmetic progression $j + \mathbb{N}l$ with $l \geq 2$ such that $\psi(f)$ vanishes on $j + \mathbb{N}l$. But then $\psi(f)\sigma(\psi(f)) \cdots \sigma^{l-1}(\psi(f)) = 0$. Replacing l with a smaller integer if necessary, we can assume that $\sigma(\psi(f)) \cdots \sigma^{l-1}(\psi(f)) \in \psi(U)$ is non-zero. This contradicts the fact that $\psi(f)$ is a non-zero divisor in $\psi(U)$. □

Let k be a field of characteristic zero and consider a linear difference equation

$$E: \quad \sigma^n(y) + h_{n-1}\sigma^{n-1}(y) + \cdots + h_0 y = 0$$

over $K = k(z)$ where $\sigma(z) = z + 1$. If $h_0 = 0$ then E is equivalent to a linear difference equation of order strictly smaller than n. So we can assume that h_0 is non-zero. The equation E is equivalent to an $n \times n$ first order system $\sigma(y) = A(E)y$ where

$$A(E) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -h_0 & -h_1 & \cdots & -h_{n-2} & -h_{n-1} \end{pmatrix}.$$

An element f in some K-σ-algebra is a solution of E if and only if

$$\begin{pmatrix} f \\ \sigma(f) \\ \vdots \\ \sigma^{n-1}(f) \end{pmatrix}$$

is a solution of $\sigma(y) = A(E)y$. Note that $A(E) \in \mathrm{GL}_n(K)$ because $h_0 \neq 0$.

Corollary 3.2. *Let k be a field of characteristic zero and*

$$E : \ \sigma^n(y) + h_{n-1}\sigma^{n-1}(y) + \cdots + h_0 y = 0$$

a linear difference equation over $K = k(z)$ with $h_0 \neq 0$. If the equivalent conditions of Theorem 3.1 are satisfied for $A = A(E)$ then for every solution $f \in k^{\mathbb{N}}$ of E, the set $\{i \in \mathbb{N} \mid f(i) = 0\}$ is a finite union of arithmetic progressions.

Proof. Let $R \subset \mathrm{Seq}_k$ denote the Picard–Vessiot ring for $\sigma(y) = A(E)y$. In the proof of Theorem 3.1 we have seen that for every element $g \in R$ the set $\{i \in \mathbb{N} \mid g(i) = 0\}$ is a finite union of arithmetic progressions. Therefore it suffices to see that (the equivalence class of) f lies in R. But this follows from the simple algebraic fact that

$$\begin{pmatrix} f \\ \sigma(f) \\ \vdots \\ \sigma^{n-1}(f) \end{pmatrix}$$

must be a k-linear combination of the columns of a fundamental solution matrix $Y \in \mathrm{GL}_n(R)$. $\qquad\square$

The following result has recently been proved in [BBY12]. The methods and ideas used there (namely a p-adic analytic arc lemma and Strassman's theorem) are very similar to the methods used in [Bel06] to prove a special case of the dynamical Mordell–Lang conjecture (when X is affine and σ an everywhere defined automorphism). Here we actually deduce the result of [BBY12] from [Bel06].

Corollary 3.3 ([BBY12, Theorem 1.2]). *Let k be a field of characteristic zero and*

$$E : \ \sigma^n(y) + h_{n-1}(z)\sigma^{n-1}(y) + \cdots + h_0(z)y = 0$$

a linear difference equation over $k(z)$ such that $h_{n-1}, \ldots, h_1 \in k[z]$ and $h_0 \in k \smallsetminus \{0\}$. Then for every solution $f \in k^{\mathbb{N}}$ of E, the set $\{i \in \mathbb{N} \mid f(i) = 0\}$ is a finite union of arithmetic progressions.

Proof. The assumptions imply that $A(E)$ is in $\mathrm{GL}_n(k[z])$ and that the rational map $\sigma : X \dashrightarrow X$ of Theorem 3.1 is an everywhere defined automorphism. Thus the validity of (i) (or (ii)) of Theorem 3.1 follows from [Bel06] and we can conclude via Corollary 3.2. $\qquad\square$

Corollary 3.4. *Let k be a field of characteristic zero and let $A \in k[z]^{n \times n}$ be such that $\det(A) \in k \smallsetminus \{0\}$. Then there exists a Picard–Vessiot extension for $\sigma(y) = Ay$ inside Seq_k.*

Proof. The assumptions imply that the rational map $\sigma : X \dashrightarrow X$ of Theorem 3.1 is an everywhere defined automorphism. Thus the validity of (i) (or (ii)) of Theorem 3.1 follows again from [Bel06]. □

In the classical case of the Skolem–Mahler–Lech theorem, i.e., for constant coefficients, there has been a vital interest in finding effective versions of the theorem, i.e., in bounding the data defining the finite union of arithmetic progressions in terms of the data of the difference equation. See e.g. [ESS02] or [AV11] and the references given there. In this context it seems worthwhile to note the following fact:

Proposition 3.5. *Let k be a field of characteristic zero and*

$$E : \sigma^n(y) + h_{n-1}(z)\sigma^{n-1}(y) + \cdots + h_0(z)y = 0$$

a linear difference equation over $k(z)$ such that $h_0 \neq 0$ and the equivalent statements of Theorem 3.1 are satisfied, e.g., $h_{n-1}, \ldots, h_1 \in k[z]$ and $h_0 \in k \smallsetminus \{0\}$. Then for every solution $f \in k^{\mathbb{N}}$ of E, the set $\{i \in \mathbb{N} \mid f(i) = 0\}$ is a finite union of arithmetic progressions of period less than or equal to the period of the Picard–Vessiot ring $R \subset \mathrm{Seq}_k$ associated to $A(E)$.

Proof. This is clear from Corollary 3.2 and the proof of the implication (iii)⇒(i) in Theorem 3.1. □

We note that if k is algebraically closed, then the Picard–Vessiot ring is unique up to $k(z)$-σ-isomorphisms. So its period is an abstract algebraic invariant of the difference equation E, a priori not related to sequences at all. This period is also given by the number of connected components of the Galois group [vdPS97, Prop. 1.20, p. 15]. Corollary 4.13 in [CHS08] gives yet another way of computing it.

If k is not algebraically closed, one can replace the period of $R \subset \mathrm{Seq}_k$ by the m-invariant of any Picard–Vessiot ring (see [CHS08, Prop. 4.9]).

The following simple example shows that the period l of the Picard–Vessiot ring of $A(E)$ is not the optimal bound to write the set of zeros of any solution of E as a finite union of arithmetic progressions of period l. However, the period of the Picard–Vessiot ring is the optimal bound to write the set of zeros of any sequence that can be obtained from solutions of E by taking sums and products as a finite union of arithmetic progressions of period l.

Example 3.6. We consider the Fibonacci recurrence $\sigma^2(y) - \sigma(y) - y = 0$ over $\mathbb{C}(z)$. The associated matrix equation is

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

Let $\alpha_1 = (1 + \sqrt{5})/2$ and $\alpha_2 = (1 - \sqrt{5})/2$ be the two solutions of the associated characteristic polynomial $t^2 - t - 1 = 0$. Then $f_1 := (\alpha_1^n)_{n \in \mathbb{N}}$ and $f_2 := (\alpha_2^n)_{n \in \mathbb{N}}$ are two $\mathbb{C}$-linearly independent solutions in $\mathrm{Seq}_{\mathbb{C}}$. The matrix

$$Y = \begin{pmatrix} f_1 & f_2 \\ \sigma(f_1) & \sigma(f_2) \end{pmatrix} = \begin{pmatrix} f_1 & f_2 \\ \alpha_1 f_1 & \alpha_2 f_2 \end{pmatrix}$$

is a fundamental solution matrix for equation (1). It follows that $R = \mathbb{C}(z)[f_1, f_2] \subset$ Seq_k is the Picard–Vessiot ring of equation (1). Because $f_1 f_2 = ((-1)^n)_{n\in\mathbb{N}}$, there are two idempotent elements $(f_1 f_2 + 1)/2 = (1, 0, 1, \ldots)$ and $(f_1 f_2 - 1)/2 = (0, 1, 0, \ldots)$ in R. Consequently, the period of R is greater than or equal to two. (It is not too hard to work out that $(f_1 f_2 + 1)(f_1 f_2 - 1)$ is the only algebraic relation between f_1, f_2 so that the period of R is precisely two.)

On the other hand, any solution of the Fibonacci recurrence assumes the value zero only a finite number of times.

4. Three equivalent conjectures

In this last section we show that the three problems SML, PV and a certain special case of DML are equivalent when considered "globally", i.e., without fixing the equation.

Theorem 4.1. *Let k be a field of characteristic zero. The following statements are equivalent:*

(i) *For every $A \in \mathrm{GL}_n(k(z))$ the rational map $\sigma: X \dashrightarrow X$ on $X = \mathbb{A}_k^1 \times \mathrm{GL}_{n,k}$ defined by $\sigma(b, B) = (b+1, A(b)B)$ has the following property: For every closed subvariety $Y \subset X$ and every $x \in X(k)$ with $\mathcal{O}_\sigma(x)$ defined the set $\{i \in \mathbb{N} \mid \sigma^i(x) \in Y\}$ is a finite union of arithmetic progressions.*

(ii) *For every solution $f \in k^{\mathbb{N}}$ of a linear difference equation*

$$\sigma^n(y) + h_{n-1}\sigma^{n-1}(y) + \cdots + h_0 y = 0$$

with $h_{n-1}, \ldots, h_0 \in k(z)$ the set $\{i \in \mathbb{N} \mid f(i) = 0\}$ is a finite union of arithmetic progressions.

(iii) *For every $A \in \mathrm{GL}_n(k(z))$ there exists a Picard–Vessiot extension of $k(z)$ for $\sigma(y) = Ay$ inside Seq_k.*

Proof. The implication (i)⇒(iii) is immediate from Theorem 3.1. To show (iii)⇒(i) let $A \in \mathrm{GL}_n(k(z))$ and let $x = (b, B) \in X(k)$ be such that $\mathcal{O}_\sigma(x)$ is defined. Moreover let $Y \subset X$ be a closed subvariety.

Set $\widetilde{A}(z) = A(z + b) \in \mathrm{GL}_n(k(z))$ and $\widetilde{x} = (0, B) \in X$. Let $\widetilde{\sigma}: X \dashrightarrow X$ be defined by $\widetilde{A}$ and let $\widetilde{Y}$ be the subvariety of X defined by the equations $f(z+b, Z)$ where $f(z, Z)$ is a defining equation of Y. Then $\widetilde{\sigma}^i(\widetilde{x}) = (i, A(b+i-1)\cdots A(b)B)$ for $i \geq 0$. In particular, $\mathcal{O}_{\widetilde{\sigma}}(\widetilde{x})$ is defined. Moreover, $\sigma^i(x) = (b+i, A(b+i-1)\cdots A(b)B)$ lies in Y if and only if $\widetilde{\sigma}^i(\widetilde{x})$ lies in $\widetilde{Y}$. By assumption, statement (iii) of Theorem 3.1 is satisfied for $\widetilde{A}$. So it follows from the implication (iii)⇒(i) of Theorem 3.1 applied to the $\sim$-setting that

$$\{i \in \mathbb{N} \mid \sigma^i(x) \in Y\} = \{i \in \mathbb{N} \mid \widetilde{\sigma}^i(\widetilde{x}) \in \widetilde{Y}\}$$

is a finite union of arithmetic progressions.

To show (iii)⇒(ii) one can assume that $h_0 \neq 0$. Then the claim follows from Corollary 3.2.

Finally, we show that (ii) implies (iii). We already know (Proposition 2.4) that there exists a Picard–Vessiot ring R for $\sigma(y) = Ay$ inside Seq_k. So we only have to show that every non-zero divisor of R is invertible in Seq_k. Let $g \in R$ be a non-zero divisor in R and suppose for a contradiction that g is not invertible in Seq_k. This means that g assumes the value zero an infinite number of times. As noted in Lemma 2.3, the element $g \in \mathrm{Seq}_k$ satisfies a linear difference equation with coefficients in $k(z)$. So by (ii) there must exist an arithmetic progression $j + \mathbb{N}l$ with $l \geq 2$ such that g vanishes on $j + \mathbb{N}l$. But then $g\sigma(g)\cdots\sigma^{l-1}(g) = 0$. Replacing l with a smaller integer if necessary, we can assume that $\sigma(g)\cdots\sigma^{l-1}(g)$ is non-zero. This contradicts the assumption that g is a non-zero divisor in R. $\qquad\square$

References

[AV11]   Amoroso, F., Viada, E.: On the zeros of linear recurrence sequences. Acta Arith. **147**, 387–396 (2011)   Zbl 1271.11015   MR 2776095

[Bel06]   Bell, J. P.: A generalised Skolem–Mahler–Lech theorem for affine varieties. J. London Math. Soc. (2) **73**, 367–379 (2006)   Zbl 1147.11020   MR 2427064

[BGT10]   Bell, J. P., Ghioca, D., Tucker, T. J.: The dynamical Mordell–Lang problem for étale maps. Amer. J. Math. **132**, 1655–1675 (2010)   Zbl 1230.37112   MR 2766180

[BBY12]   Bell, J. P., Burris, S. N., Yeats, K.: On the set of zero coefficients of a function satisfying a linear differential equation. Math. Proc. Cambridge Philos. Soc. **153**, 235–247 (2012)   Zbl 1264.11005   MR 2981925

[CHS08]   Chatzidakis, Z., Hardouin, C., Singer, M. F.: On the definitions of difference Galois groups. In: Model Theory with Applications to Algebra and Analysis, Vol. 1, London Math. Soc. Lecture Note Ser. 349, Cambridge Univ. Press, Cambridge, 73–109 (2008)   Zbl 1234.12005   MR 2441376

[Coh65]   Cohn, R. M.: Difference Algebra. Wiley, New York (1965)   Zbl 0141.01002   MR 0205987

[ESS02]   Evertse, J.-H., Schlickewei, H. P., Schmidt, W. M.: Linear equations in variables which lie in a multiplicative group. Ann. of Math. (2) **155**, 807–836 (2002)   Zbl 1026.11038   MR 1923966

[GT09]   Ghioca, D., Tucker, T. J.: Periodic points, linearizing maps, and the dynamical Mordell–Lang problem. J. Number Theory **129**, 1392–1403 (2009)   Zbl 1186.14047   MR 2521481

[Lev08]   Levin, A.: Difference Algebra. Algebra Appl. 8, Springer, New York (2008)   Zbl 1209.12003   MR 2428839

[vdPS97] van der Put, M., Singer, M. F.: Galois Theory of Difference Equations. Lecture Notes in Math. 1666, Springer, Berlin (1997)   Zbl 0930.12006   MR 1480919

[vdPS03] van der Put, M., Singer, M. F.: Galois Theory of Linear Differential Equations. Grundlehren Math. Wiss. 328, Springer, Berlin (2003)   Zbl 1036.12008   MR 1960772

[Wib10]   Wibmer, M.: Geometric difference Galois theory. PhD thesis, Heidelberg (2010). http://www.ub.uni-heidelberg.de/archiv/10685   Zbl 1287.12003