**Linear difference operators with coefficients in the form of infinite sequences**

©2021 S. A. Abramov[a,*,1], M. A. Barkatou[b,**], M. Petkovšek[c,***,2]

[a] *Dorodnicyn Computing Centre, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences;* Vavilova str., 40, Moscow, 119333, Russia;

[b] *University of Limoges ; CNRS ; XLIM UMR 7252 ; MATHIS 123, Av. A. Thomas, 87060 Limoges cedex, France;*

[c] *University of Ljubljana, Faculty of Mathematics and Physics, Jadranska 19, SI-1000 Ljubljana, Slovenia*

[*] *e-mail: sergeyabramov@mail.ru*

[**] *e-mail: moulay.barkatou@unilim.fr*

[***] *e-mail: Marko.Petkovsek@fmf.uni-lj.si*

**Abstract**

Some properties of linear difference operators whose coefficients have the form of infinite two-sided sequences over a field of characteristic zero are considered. In particular, it is found that such operators are deprived of some properties that are natural for differential operators over differential fields. In addition, we discuss questions of the decidability of certain problems arising in connection with the algorithmic representation of infinite sequences.

**Key words:** linear difference equations, infinite sequences in the role of coefficients, annihilating operators, solution spaces, divisibility, common multiples of operators, undecidable problems.

# 1 Introduction

The need to consider linear difference operators with coefficients in the form of sequences (or equivalence classes of sequences) arises, in particular, in connection with the universal Picard-Vessiot extensions of difference fields [8, 5]. As has been noticed already in [4], one has to consider *difference-ring*

[1]Supported in part by the Russian Foundation for Basic Research, project no. 19-01-00032-a.

[2]Supported in part by the Ministry of Education, Science and Sport of Slovenia research programme P1-02.

extensions of difference fields. In the context of such extensions, questions arise naturally about properties of operators with such coefficients.

In [5, Appx. A], it is found that some properties that are natural for differential operators over differential fields ([9]) are not satisfied in the case of difference operators over rings – in particular, over rings of sequences. Additionally, we point out undecidability of a number of problems related to linear difference operators with sequences as coefficients.

The rest of the paper is organized as follows. Sect. 2 contains some preliminary information. In Sect. 3 we consider the question whether for any $m$ linearly independent sequences there exists an operator of order $m$ whose solution space is generated by these sequences. It is shown that for any $m$ there are $m$ linearly independent sequences such that any operator annihilating these sequences has an infinite-dimensional solution space. In the same section it is shown that the space of solutions of the least common left multiple of operators $L_1$, $L_2$ can be infinite-dimensional while the solution spaces of $L_1$ and $L_2$ have finite dimension. The final Sect. 4 discusses the use of computable sequences (for each such sequence, an algorithm is known that computes elements from their indices) as operator coefficients. A number of questions of decidability of certain problems arising in connection with the algorithmic representation of infinite sequences is investigated: the problem of testing invertibility of an operator, testing divisibility of one operator by another, and testing existence of a nonzero common left multiple of two given operators.

A preliminary version of this work was presented as [2].

# 2 Preliminaries

Below, $R = \mathbb{Q}^{\mathbb{Z}}$ stands for the ring of two-sided sequences having rational-number terms, with addition and multiplication defined termwise, and $\sigma$ is the shift automorphism on $R$ acting by $\sigma c = d$ with $d(k) = c(k+1)$ for all $k \in \mathbb{Z}$. Clearly, the ring of constants of $R$ is the field $\mathbb{Q}$. By $\mathbf{1}$ we denote the sequence in $R$ all of whose terms are equal to 1. For $k, m \in \mathbb{Z}$ with $m \geq 1$

we define two-sided sequences $\delta_k, \omega_m \in R$ by

$$\begin{aligned}\delta_k(n) &= \begin{cases} 1, & n = k, \\ 0, & \text{otherwise}, \end{cases} \\ \omega_m(n) &= \begin{cases} 1, & n \equiv m \pmod{m+1}, \\ 0, & \text{otherwise}; \end{cases}\end{aligned}$$

here $\delta_k(n)$ is the well-known Kronecker delta.

The ring $R[\sigma]$ is the ring of linear difference operators with coefficients in $R$. The *order* of $L \in R[\sigma]$ denoted by $\operatorname{ord} L$ is the non-negative integer equal to the degree of the (skew) polynomial $L$ in $\sigma$ (cf. [7, 3]); conventionally $\operatorname{ord} 0 = -\infty$. For $L \in R[\sigma]$, we denote the $\mathbb{Q}$-linear space of all $f \in R$ s.t. $L(f) = 0$ by $V_L$.

# 3 Dimension of solution spaces of operators in $R[\sigma]$

## 3.1 A useful lemma

**Lemma 1** *Let $m$ be a positive integer. The sequence $\omega_m$ is such that if $L$ is an operator with $\operatorname{ord} L \leq m$, then the equality $L(\omega_m) = 0$ implies that $\dim V_L = \infty$.*

*Proof.* Let $L$ be of the form

$$L = a_m(n)\sigma^m + \cdots + a_1(n)\sigma + a_0(n) \in R[\sigma].$$

If $L(\omega_m) = 0$ then for all $n \in \mathbb{Z}$

$$\begin{aligned} 0 &= \sum_{i=0}^{m} a_i(n)\omega_m(n+i) = \sum_{i=0}^{m} a_i(n) \begin{cases} 1, & n+i \equiv m \pmod{m+1} \\ 0, & \text{otherwise} \end{cases} \\ &= \sum_{i=0}^{m} \begin{cases} a_i(n), & n \equiv m-i \pmod{m+1} \\ 0, & \text{otherwise} \end{cases} = a_{i_n}(n) \end{aligned} \tag{1}$$

where $i_n$ is the unique $i \in \{0, 1, \ldots, m\}$ such that $n \equiv m - i \pmod{m+1}$. Hence for all $n \in \mathbb{Z}$ and $i \in \{0, 1, \ldots, m\}$ we have the implication

$$n \equiv m - i \pmod{m+1} \implies a_i(n) = 0.$$

Now let $c(n)$ be an arbitrary sequence from $R$ and $g(n) \in R$ be the sequence for which

$$g(n) \;=\; \begin{cases} c(n), & n \equiv m \pmod{m+1}, \\ 0, & \text{otherwise.} \end{cases}$$

Note that the set (parameterized by $c(n) \in R$) of all such $g(n)$ is an infinite-dimensional subspace of the $\mathbb{Q}$-linear space $R$. Then by (1)

$$\sum_{i=0}^{m} a_i(n)g(n+i) \;=\; \sum_{\substack{0\le i\le m\\ n+i\equiv m \ (\mathrm{mod}\ m+1)}} a_i(n)g(n+i) \;=\; a_{i_n}(n)g(n+i_n) \;=\; 0,$$

so $L(g) = 0$ for all such $g$, implying that $\dim \ker L = \infty$. □

Recall that in the differential case we can find a differential operator $L$ annihilating elements $f_1, \ldots, f_m$ of a differential field, such that the dimension of the solution space of $L$ is equal to the maximum number of elements from among $f_1, ..., f_m$ that are linearly independent over constants of the differential field under consideration.

**Example 1** Let $m = 2$. Then $\omega_2(3k) = \omega_2(3k+1) = 0$, $\omega_2(3k+2) = 1$ for all $k \in \mathbb{Z}$. If $L = a_2(n)\sigma^2 + a_1(n)\sigma + a_0(n)$ annihilates $\omega_2(n)$ then

$$a_0(3k+2) = a_1(3k+1) = a_2(3k) = 0.$$

Such an operator $L$ annihilates also any sequence $g_s(n)$ such that $g_s(3k) = g_s(3k+1) = 0$, $g_s(3k+2) = k^s$. Note that sequences $g_s(n)$ for $s \in \mathbb{Z}$ are linearly independent over the constants.

## 3.2 Annihilating operators in $R[\sigma]$

**Proposition 1** *For any positive integer $m$ there exist $f_1, \ldots, f_m \in R$ such that if for some $L \in R[\sigma]$ with $\operatorname{ord} L \le m$ the equalities*

$$L(f_i) = 0$$

*hold for $i = 1, \ldots, m$, then $\dim V_L = \infty$.*

*Proof.* This is a consequence of Lemma 1: Any $f_1, \ldots, f_m \in R$ such that $f_1 = \omega_m$ possess the formulated property. □

The following example shows that there are other (but similar) ways for constructing $f_1, \ldots, f_m$ beside the one used in the proof of Proposition 1.

**Example 2** Consider two sequences $f_1, f_2$ where

$$f_1(4k) = 0, \;\; f_1(4k+1) = f_1(4k+2) = f_1(4k+3) = 1,$$

$$f_2(4k+1) = 0, \;\; f_2(4k) = f_2(4k+2) = f_2(4k+3) = 1, \quad k = 0, \pm 1, \pm 2, \ldots$$

If $L = a\,\sigma^2 + b\,\sigma + c$ annihilates $f_1$ and $f_2$ then

$$\begin{gathered} b(4k) = c(4k) = -a(4k), \\ b(4k+1) = -a(4k+1), \;\; c(4k+1) = 0, \\ a(4k+2) = 0, \;\; c(4k+2) = -b(4k+2), \\ b(4k+3) = -c(4k+3) = a(4k+3). \end{gathered}$$

This implies that $L(y) = 0$ for any sequence $y$ which satisfies

$$\begin{gathered} y(4k+1) = y(2) - y(4k), \\ y(4k+2) = y(4k+3) = y(2), \end{gathered}$$

while $y(2), y(4k)$ can be arbitrary constants for all $k$.

Note that an even stronger form of the statement of Lemma 1 is possible:

**Lemma** 1* *There exist sequences, say $c$, such that if an operator $L$ annihilates $c$ then* $\dim V_L = \infty$.

Indeed, let $c(n)$ be equal to 1 if $n = k^2$ for some integer $k$, and 0 otherwise. Using the same idea as in the proof of Lemma 1, it is possible to show that if $L(c) = 0$, $\operatorname{ord} L = m$, then $L$ annihilates any sequence $d$ such that the inequality $d(n) \neq 0$ implies that $n = k^2, \; k > \sqrt{m}$.

The general consideration is the following: Let $\nu$ be a sequence of positive integers $\nu(0), \nu(1), \ldots$ such that $\nu(k+1) - \nu(k)$ tends to infinity with $k$, e.g., $\nu(k) = k^2$ or $\nu(k) = 2^k$. Define $c \in R$ by $c(n) = 1$ if $\exists_{k \geq 1}\colon |n| = \nu(k)$, and $c(n) = 0$, otherwise. Then the distance between two consecutive 1's in $c$ increases and tends to $\infty$, which is not the case for sequences $\omega_m$. – Accordingly, the statement of Proposition 1 can be strengthened as well.

Recall that in the differential case we can find an operator $L$, $\operatorname{ord} L \leq m$, annihilating given $f_1, \ldots, f_m$ such that the dimension of the solution space of $L$ is equal to the number of linearly independent elements from $f_1, \ldots, f_m$.

## 3.3 Least common left multiple of operators in $R[\sigma]$

**Definition 1** We define $\mathrm{lclm}\,(L_1, L_2)$ as the set of all operators $L$ such that

- $L$ is not zero,
- $L$ is a common left multiple of $L_1$ and $L_2$,
- there is no operator $M$ such that $M$ is not zero, $M$ is a common left multiple of $L_1$ and $L_2$, and $\mathrm{ord}\, M < \mathrm{ord}\, L$. $\square$

**Remark 1** It can happen that $L$ does not belong to $\mathrm{lclm}\,(L, L)$. For example, let $L := a\sigma + \mathbf{1}$, where $a = \omega_1$. Let $f = \sigma(a)$. Then $fa = 0$, so $fL = fa\sigma + f = f$ is a left multiple of $L$. Since $\mathrm{ord}\, f = 0$ is the lowest possible order for a nonzero operator, $f$ belongs to $\mathrm{lclm}\,(L, L)$, but $L$ itself does not because $\mathrm{ord}\ L = 1$. It is easy to see that $L$ is invertible in $R[\sigma]$ and $L^{-1} = -a\sigma + 1$ (since $\sigma(a)a = a\sigma(a) = 0$). This implies that $\mathbf{1} \in \mathrm{lclm}\,(L, L)$.

Note that it is also possible that for two given operators $L_1, L_2 \in R[\sigma]$, their only common multiple is 0.

**Example 3** Consider the following operators $L_1$ and $L_2$ of order zero: $L_1$ is the sequence $c = \omega_1$, and $L_2$ is the sequence $d = \sigma\omega_1$. Then their only common multiple is the zero sequence.

Indeed, assume that $M_1L_1 = M_2L_2$ where $M_1$ is an operator whose $i$-th term is of the form $a_i\sigma^i$, and $M_2$ an operator whose $i$-th term is of the form $b_i\sigma^i$ where $a_i$ and $b_i$ are arbitrary sequences. Then the $i$-th term of $M_1L_1 = M_1c$ is of the form $a_i(\sigma^i c)\sigma^i = a_i(n)c(n+i)\sigma^i$, and the $i$-th term of $M_2L_2 = M_2d$ is of the form $b_i(\sigma^i d)\sigma^i = b_i(n)d(n+i)\sigma^i$. For each $i$ and $n$, (exactly) one of $c(n+i)$, $d(n+i)$ is zero. If $M_1L_1 = M_2L_2$ then $a_i(n)c(n+i) = b_i(n)d(n+i) = 0$ for all $i$ and $n$, hence $a_i(\sigma^i c) = b_i(\sigma^i d)$ for all $i$, therefore $M_1L_1 = M_2L_2 = 0$.

**Proposition 2** *There exist first-order operators $L_1, L_2$ such that*

(i) $\dim V_{L_1} = \dim V_{L_2} = 1$,

(ii) *there exists a second-order common multiple $L$ of $L_1, L_2$,*

(iii) *for any common multiple $A$ of $L_1, L_2$ such that* $\mathrm{ord}\, A \leq 2$, *the relation* $\dim V_A = \infty$ *holds.*

*Proof.* (i),(iii): Set

$$L_1 = \sigma - b(n), \quad L_2 = \sigma - 1, \tag{2}$$

where $b(3k) = 1$, $b(3k+1) = b(3k+2) = -1$. Then $V_{L_1}$ and $V_{L_2}$ are one-dimensional: $V_{L_1}$ is generated by the sequence $s(n)$ such that $s(3k) = s(3k+1) = -1$, $s(3k+2) = 1$, while $V_{L_2}$ is generated by the sequence $\mathbf{1}$. If $V_{L_1}, V_{L_2} \subseteq V_A$ for some operator $A$, then $V_A$ contains $f(n) = (s(n) + \mathbf{1}(n))/2 = \omega_2(n)$. By Lemma 1, if $\operatorname{ord} A \leq 2$ then $\dim V_A = \infty$. Thus, (i) and (iii) are proven.

(ii): It is easy to check that

$$\big((1 - b(n))\sigma + b(n+1) - 1\big)L_1 = \big((1 - b(n))\sigma + b(n)(b(n+1) - 1)\big)L_2. \tag{3}$$

It is evident that each of the left- and right-hand sides of (3) is a non-zero least common multiple of $L_1, L_2$. $\square$As a consequence, we have that for $L \in \operatorname{lclm}(L_1, L_2)$ the equality

$$V_L = V_{L_1} + V_{L_2} \tag{4}$$

does not hold in general.

Recall that in the differential case, when $L_1, L_2$ the operators over a differential field $\mathbb{K}$ the equality (4) holds if we consider solutions from the Picard-Vessiot extension of $\mathbb{K}$. Similarly, this holds also for the case of differential systems, see [1]. The equality (4) takes place in the scalar difference case when the coefficients belong to a difference field possessing some special properties [6].

**Remark 2** The statement of Proposition 2 as well as its consequence that the equality (4) is in general not satisfied, hold if one considers solutions as sequences having their elements in any extension of the field $\mathbb{Q}$. Indeed, the leading and trailing coefficients of operators (2) do not vanish and solution spaces of $L_1$ and $L_2$ are one-dimensional, while the solution space of $\operatorname{lclm}(L_1, L_2)$ has infinite dimension.

# 4 On some undecidable problems

## 4.1 A consequence of a classical Turing's result

Below, we prove undecidability of some problems related to the operators having coefficients in $R$. The proofs are in general based on the consequence of classical Turing's result on undecidability of the well-known halting problem [10]:

*Let $M$ be a set containing at least two elements and such that there is an algorithm to test the equality of any two given elements from $M$. Then there is no algorithm to answer the question whether a given computable sequence (one-sided: $c(0), c(1), \dots,$ or two-sided: $\dots, c(-1), c(0), c(1), \dots$) is such that each of its elements is equal to a given $u \in M$; the same for the case of a sequence having no element being equal to a given element of $M$.*

## 4.2 Testing for invertibility and divisibility of operators in $R[\sigma]$

The problem of representing infinite sequences is an important one in computer algebra. A general formula for the $n$-th element of a sequence is not always available and may even not exist. Another way to represent a sequence is the algorithmic one, where a sequence is given by an algorithm for computing its elements from their indices. We will call such sequences *computable*. The algorithmic representation of a concrete sequence is not, of course, unique. This non-uniqueness is one of the reasons for the undecidability of the zero-testing problem for such computable sequences.

**Lemma 2** *Testing for an arbitrary computable sequence $c \in R$ and a positive integer $r$ the truth of the statement*

$$\mathbf{P}(c, r) = \exists_{k \in \mathbb{Z},\, k \geq 0} \forall_{n \in \mathbb{Z}} \colon (c(n)c(n+r)c(n+2r) \cdots c(n+kr) = 0\,)$$

*is algorithmically undecidable.*

Proof. Define the sequence $a(n)$ as follows. For $n \geq 0$ we set

$$a(n) \;=\; \begin{cases} c(0) & \text{if } \; n = 0, \\ 0, & \text{if } \; n > 0 \;\text{ and }\; c(n) = 0, \\ a(n-1), & \text{otherwise.} \end{cases} \tag{5}$$

For $n < 0$ we set $a(n) = 0$. The condition that $c$ is a computable sequence implies that the sequence $a$ is computable too. The sequence $a$ is such that if there is no zero element in

$$c(0), c(1), c(2), \dots \tag{6}$$

then $\forall_{n\in\mathbb{Z},n\geq 0}$: $a(n)\neq 0$, hence also $\forall_{n,k\in\mathbb{Z},n,k\geq 0}$: $a(n)a(n+r)\cdots a(n+kr)\neq 0$. On the other hand, if $c(m)=0$ for some $m\geq 0$, then we have

$$\forall_{k\geq\lceil\frac{m}{r}\rceil,\,n\in\mathbb{Z}}\colon\,(a(n)a(n+r)\cdots a(n+kr)=0)$$

since the product $a(n)a(n+kr)$ is the zero sequence. Thus, $\mathbf{P}(a,r)$ is true if and only if there is at least one zero element in (6).

If an algorithm $\mathcal{A}$ allows us to test for the truth of $\mathbf{P}$ for any sequence from $R$ and any positive integer $r$ then using this algorithm we could test for the existence of a zero element in a given sequence of the form (6): one could apply $\mathcal{A}$ to the sequence

$$\tilde{c}(n) \;=\; \begin{cases} c(n) & \text{if } \; n\geq 0,\\ 0, & \text{otherwise.}\end{cases}$$

The sequence (6) has a zero element if and only if $\mathbf{P}(\tilde{c},r)$ is true ($r$ can be an arbitrary positive integer). However testing for the existence of a zero element in an arbitrary computable sequence is undecidable (see Sect. 4.1), therefore $\mathcal{A}$ cannot exist. $\square$

**Proposition 3** *Let $r$ be a nonnegative integer. There exists no algorithm for testing for an arbitrary $L\in R[\sigma]$, $\operatorname{ord} L=r$, whether $L$ is invertible in $R[\sigma]$.*

*Proof.* If $r=0$ then $L$ is a sequence from $R$. The sequence is invertible if and only if the sequence does not contain zeros. There is no algorithm to test this property.

Let $r>0$. Consider the set of operators of the form

$$1-c(n)\sigma^r, \tag{7}$$

where $c\in R$ is such that $c(0)=1$ and thus $c$ is a nonzero sequence. The order of each $L$ of the form (7) is $r$. If the inverse $L^{-1}$ for $L$ exists then there exists $k\geq 1$ such that $L^{-1}$ has the form

$$1+c(n)\sigma^r+c(n)c(n+r)\sigma^{2r}+\cdots+c(n)c(n+r)c(n+2r)\ldots c(n+(k-1)r)\sigma^{(k-1)r},$$

with

$$\forall_{n\in\mathbb{Z}}\colon(\,c(n)c(n+r)c(n+2r)\ldots c(n+kr)=0\,). \tag{8}$$

Therefore, $L$ of the form (7) is invertible if and only if (8) holds. So, if we have an algorithm for testing invertibility then we can use it for testing validity of (8). By Lemma 2, the problem is undecidable. $\square$

**Remark 3** Let $r$ be a nonnegative integer number. Then there exists an invertible operator of order $r$ in $R[\sigma]$. Indeed, if $r = 0$ then $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$. Otherwise, $(\mathbf{1} - \delta_0(n)\sigma^r)(\mathbf{1} + \delta_0(n)\sigma^r) = \mathbf{1}$.

**Proposition 4** *Let $s, r$ be nonnegative integer numbers. There exists no algorithm for testing for arbitrary $L_1, L_2 \in R[\sigma]$, $\operatorname{ord} L_1 = s$, $\operatorname{ord} L_2 = r$ whether $L_1$ is right-divisible by $L_2$ in $R[\sigma]$ or not.*

*Proof.* If such an algorithm existed then one could use it to test for invertibility of a given $L \in R[\sigma]$ of order $r$. Indeed, take any operator $M$ of order $s$, for example, $M = \sigma^s$. It is evident that $L$ is invertible if and only if $M$ and $M + 1$ are both right-divisible by $L$. So, if one can test for divisibility then one can test for invertibility. But by Proposition 3, the latter problem is undecidable. □

## 4.3 On testing for existence of a nonzero common multiple

Below, we discuss the problem of possibility or impossibility of algorithms for testing for existence of a nonzero common multiple for given $L_1, L_2 \in R$.

Notice that the impossibility of a general algorithm for testing for existence of a common nonzero multiple can be proven easily by considering the case of zero-order operators, i.e., the case of sequences.

**Proposition 5** *There is no algorithm for testing for existence of a non-zero common multiple of two given sequences $a, b \in R$.*

*Proof.* First, we prove that there is no algorithm for testing the relation

$$\forall_{n \in \mathbb{Z}} \colon (a(n)b(n) = 0) \tag{9}$$

for given computable sequences $a, b$. Indeed, if we had an algorithm for testing this relation, this would make it possible to test algorithmically whether the sequence $a$ is identically zero. If we take $b$ such that $b(n) = 1$ for all $n$, then (9) holds if and only if $a$ is identically zero.

Now we show that the problem of testing the existence of a nonzero common multiple is undecidable even in the case of zero-order operators, i.e. when the operators $L_1, L_2$ are some sequences $a$ and $b$. It is easy to see that $a$ and $b$ have a non-zero common multiple if and only if (9) does not hold. In fact, the proof of the absence of a non-zero common multiple in the case (9) is similar to the proof from Example 3. If for some $n$ the product $a(n)b(n)$ is not equal to zero, then $a(n)b(n)$ is a non-zero common multiple. $\square$

This implies that an algorithm for testing for existence of a non-zero common multiple of given arbitrary operators $L_1$, $L_2$ is not possible. We will prove a stronger statement:

**Proposition 6** *Let $r, s$ be nonnegative integers. Then there is no algorithm for testing the existence of a non-zero common multiple of given operators $L_1, L_2 \in R[\sigma]$ of the form*

$$L_1 = a_r\sigma^r + a_{r-1}\sigma^{r-1} + \dots, \quad L_2 = b_s\sigma^s + b_{s-1}\sigma^{s-1} + \dots, \tag{10}$$

*with nonzero sequences $a_r, b_s$.*

The proof is based on the following lemma.

**Lemma 3** *Let $a, b$ be nonzero sequences and $r, s$ nonnegative integer numbers, $r \geq s$. Then $a\sigma^r$, $b\sigma^s$ have a nonzero left common multiple if and only if there exists an integer $m$ such that*

$$a(m) \neq 0, \quad b(m + r - s) \neq 0. \tag{11}$$

*Proof*:

$\Longrightarrow$ : Let $Ua\sigma^r = Wb\sigma^s$ where both sides are nonzero operators. Let $u = \operatorname{ord} U$, $w = \operatorname{ord} W$. Clearly

$$u + r = w + s. \tag{12}$$

Let $c\sigma^u$ and $d\sigma^w$ be the leading terms of $U$ and $W$, respectively. The nonzero sequences $c(n)a(n + u)$ and $d(n)b(n + w)$ are equal. This implies that the equality

$$c(n - u)a(n) = d(n - u)b(n + w - u)$$

holds for all $n$. By (12), the latter equality can be represented as

$$c(n - u)a(n) = d(n - u)b(n + r - s).$$

Since the left and right sides of the latter equality are nonzero sequences, there exists an integer $m$ such that

$$c(m - u)a(m) = d(m - u)b(m + r - s) \neq 0.$$

This implies that $a(m) \neq 0,\ b(m+r-s) \neq 0$.

$\Longleftarrow$ : If $m$ exists then we set $U := \frac{1}{a(m)}\delta_m(n)$ and $W := \frac{1}{b(m+r-s)}\delta_m(n)\sigma^{r-s}$. We obtain

$$Ua\sigma^r = Wb\sigma^s = \delta_m(n)\sigma^r.$$

□

*Proof* of Proposition 6: First, we prove the following: Let $t$ be a nonnegative integer. There is no algorithm $\mathcal{A}_t$ for testing for arbitrary $a, b \in R$ whether there exists an $m \in \mathbb{Z}$ such that $a(m)b(m+t) \neq 0$. We show that if $\mathcal{A}_t$ existed then one could use this algorithm for testing whether a given sequence

$$c = c(0),\ c(1),\ c(2),\ \ldots \tag{13}$$

at least one nonzero element. However, the latter problem is undecidable (see Section 4.1), and this will imply nonexistence of $\mathcal{A}_t$.

Let $c$ be as in (13). We define two-sided sequences $a$ and $b$ as follows:

$$a(n) = \begin{cases} c(n), & n \geq 0, \\ 0, & n < 0, \end{cases}, \qquad b(n) = \begin{cases} c(n-t), & n \geq t, \\ 0, & n < t. \end{cases}$$

Then

$$b(n+t) = \begin{cases} c(n), & n \geq 0, \\ 0, & n < 0 \end{cases}, \qquad a(n)b(n+t) = \begin{cases} c(n)^2, & n \geq 0, \\ 0, & n < 0. \end{cases}$$

It follows that the two-sided sequence $a(n)b(n+t)$ contains a nonzero element iff the one-sided sequence $c^2$ contains a nonzero element, and this is true iff the one-sided sequence $c$ contains a nonzero element.

The sequences $a, b$ are computable and nonzero. It is easy to see that there exists $m \in \mathbb{Z}$ such that $a(m)b(m+t) \neq 0$ if and only if $c(m-2) \neq 0$. So, if the algorithm $\mathcal{A}_t$ existed then for any sequence $c$ one can test algorithmically the existence of a nonzero element in $c$. But this problem is undecidable, as it follows from the statement from Sect. 4.1. This implies that the algorithm $\mathcal{A}_t$ does not exist for any nonnegative $t$. By Lemma 3 this means that the statement of Proposition 6 holds. □

# 5 Conclusion

Difference equations are the foundation on which modern numerical methods are built. The article presents results which indicate that difference equations with coefficients in the form of sequences are complicated objects that require very careful handling.

# References


[1] Abramov S., Barkatou M., Petkovšek M. Matrices of Scalar Differential Operators: Divisibility and Spaces of Solutions. *Computational Mathematics and Mathematical Physics* **60**, no 1, 109–118 (2020).

[2] Abramov S., Barkatou M., Petkovšek M. On infinite sequences and difference operators. *Materials of 4-th international conference "Computer algebra"*, Moscow: MAX Press, 19–22 (2021).

[3] Bronstein M., Petkovšek M. An introduction to pseudo-linear algebra. *Theor. Comput. Sci.* **157**, 3–33 (1996).

[4] Franke C.H. Picard-Vessiot theory of linear homogeneous difference equations. *Trans. Amer. Math. Soc.* **108**, 491–515 (1963).

[5] Hendriks P., Singer M. Solving difference equation in finite terms. *J. Symbolic Comput.* **27**(3): 239–259 (1999).

[6] van Hoeij M. Finite singularities and hypergeometric solutions of linear recurrence equations. *J. Pure Appl. Algebra* **139**, 109–131 (1999).

[7] Ore O. Theory of non-commutative polynomials. *Annals of Mathematics* **34**, 480–508 (1933).

[8] van der Put M., Singer M. F. *Galois Theory of Difference Equations.* LNM **1666**, Springer-Verlag, Berlin, 1997.

[9] van der Put M., Singer M. F. *Galois Theory of Linear Differential Equations.* Grundlehren der mathemat. Wissenschaften, **328**, Springer-Verlag, Berlin, 2003.

[10] Turing A. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, Series 2, **42**, 230–265 (1936).