ISSN 0965-5425, Computational Mathematics and Mathematical Physics, 2020, Vol. 60, No. 1, pp. 109–118. © Pleiades Publishing, Ltd., 2020.

Matrices of Scalar Differential Operators: Divisibility and Spaces of Solutions

S. A. Abramov[a,*], M. A. Barkatou[b,], and M. Petkovšek[c,***]**

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

[b] *University of Limoges, CNRS, XLIM UMR 7252, Limoges cedex, 87060 France*

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

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

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

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

Received July 31, 2019; revised August 15, 2019; accepted September 18, 2019

Abstract—We investigate the connection between divisibility of full-rank square matrices of linear scalar differential operators over some differential field K, and the solution spaces of these matrices over the universal Picard–Vessiot extension of K. We establish some properties of the solution spaces of the greatest common right divisor and the least common left multiple of such matrices.

Keywords: computer algebra algorithms, differential operator matrices, divisibility of square matrices of differential operators, solution space, greatest common right divisor, least common left multiple

DOI: 10.1134/S0965542520010030

1. INTRODUCTION

In [9, p. 82] it is shown that if R is a principal right ideal ring then so is the ring $\mathbf{M}_m(R)$ of square matrices of size m with entries in R (the same holds for principal left ideal ring). This is enough for the existence of the (right and left) greatest common divisor and least common multiple for any pair (A, B) of matrices of this type (even if they are not of full rank). This is in particular the case for $R = K[\partial]$ the ring of scalar linear differential operators over a given differential field K. Later, in [5, Section 9.3], algorithms for finding the greatest common right divisor (gcrd) and the least common left multiple (lclm) of Ore operator matrices were given in the same way as it has been done earlier for matrices of polynomials [6]. Those algorithms are based originally on the algorithm FF [5]. A simplified version of FF is the RowReduction algorithm presented in [4],—for short, we will use the abbreviation RR in the sequel.

However, as far as we know, the relations between the divisibility properties of differential operator matrices (i.e., of matrices of scalar differential operators) and their spaces of solutions were not investigated in detail in those publications. In the present paper, we are interested in studying such relationships in the case of differential full-rank operator matrices over a differential field K of characteristic zero. We assume that $\mathrm{Const}(K)$, the constant field of K, is algebraically closed and we fix a *universal Picard–Vessiot extension* Λ of K [14]. With each differential operator matrix $A \in \mathbf{M}_m(K[\partial])$ we associate its solution space V_A over Λ (that is the set of vector-column $y = (y_1, \ldots, y_m)^{\mathrm{T}} \in \Lambda^m$ satisfying $A(y) = 0$).

Note that the solution space of a full-rank operator matrix is finite-dimensional over $\mathrm{Const}(K)$, as it follows from [2]. We prove that for any given finite set $F \subset \Lambda^m$ there exists an operator matrix whose solution space is generated by F (the entries of that matrix are, in general, in Λ, not necessarily in K). We use this first result and some matrix divisibility properties to prove that for any full-rank matrices $A, B \in \mathbf{M}_m(K[\partial])$ we have $V_A + V_B = V_{\mathrm{lclm}(A,B)}$. It seems that this has so far been explicitly stated and proved in the scalar case, i.e. $m = 1$, but even there the proof is nontrivial (see the comment to [11, Lemma 1] where it is noted that the proof can be based on [10, Lemma A.6]).

So again, although the definition and computation of gcrd and lclm of operator matrices are not new—as we have noted, a very similar exposition can be found in [5], [9]—the connection to solution spaces does not appear to have been studied so far.

We would like to note that some of the statements of our paper can be proved in a different way with the methods of differential algebra, in particular by using some statements from [12]. Our current proofs are quite elementary, and from them the algorithms of interest to us can often be extracted with little or no additional effort.

2. PRELIMINARIES: OPERATOR MATRICES

Let (K,∂) be a differential field of characteristic 0 with an algebraically closed constant field $\mathrm{Const}(K) = \{c \in K \mid \partial c = 0\}$. We denote by Λ a fixed *universal Picard–Vessiot differential extension field* of K (see [14, Section 3.2]). This is a differential extension Λ of K with $\mathrm{Const}(\Lambda) = \mathrm{Const}(K)$ such that any linear differential equation of order n with coefficients in K has a fundamental set of solutions in Λ.

Let m be a positive integer, L an operator matrix from $K[\partial]^{n\times m}$. We denote by V_L the $\mathrm{Const}(\Lambda)$-vector space of solutions of L (i.e., solutions of the equation $L(y) = 0$) belonging to Λ^m. Its dimension will be denoted by $\dim V_L$.

The rows of an operator matrix $C \in K[\partial]^{n\times m}$ having indices $i_1,\dots,i_s$, $s \le n$, are said to be independent over $K[\partial]$, if the equality $f_1C_{i_1,*} + \dots + f_sC_{i_s,*} = 0$ with $f_1,\dots,f_s \in K[\partial]$, implies that $f_1 = \dots = f_s = 0$. Here $C_{i,*}$, for $1 \le i \le n$, denotes the $1\times m$ matrix which is the ith row of C.

Analogously, one can define the independence of columns, but then $f_1, f_2, \dots$ must be used as right factors. For a matrix C we can define the *row rank* as the maximal number of independent rows of the matrix and its *column rank* as the maximal number of its independent columns. For any matrix those two ranks are equal [8, Ch. 8.1, Theorem 1.1] (note that if $f_1, f_2, \dots$ were used as the left coefficients of the columns of C then the claim about equality of the two ranks would not hold). We will use below the term *rank* for this number. A matrix from $K[\partial]^{n\times m}$ is said to be of *full rank* if its rank is equal to $\min\{n,m\}$.

Let R be a ring. Denote

—by $\mathbf{M}_m(R)$ the matrix ring $R^{m\times m}$,

—by $\mathbf{M}_m$ the matrix ring $K[\partial]^{m\times m} = \mathbf{M}_m(K[\partial])$,

—by $\mathrm{ord}\,M$ the *order* of a given matrix $M \in \mathbf{M}_m$, i.e., the maximum of the orders of its entries,

—by $\mathbf{\Phi}_m$ the multiplicative semigroup of all full-rank matrices from $\mathbf{M}_m$, and,

—by $\mathbf{\Upsilon}_m$ the group of unimodular (i.e., invertible) matrices from $\mathbf{M}_m$.

Evidently, $\mathbf{\Upsilon}_m \subset \mathbf{\Phi}_m$.

In the following proposition, we recall two results that will be used later and whose proof is based on [2, Theorem 2] (remark however that (2) can also be proven using [13, Theorem 3]).

Note that the first Eq. (1) can serve as a replacement for the equality $\mathrm{ord}\,AB = \mathrm{ord}\,A + \mathrm{ord}\,B$ valid for scalar operators A and B, but not in the general case of operator matrices (due to existence of zero divisors in $\mathbf{M}_m(K)$).

Proposition 1. *Let $A, B \in \mathbf{\Phi}_m$. Then*

(i) [3, Theorem 3] *We have the equality*

$$\dim V_{AB} = \dim V_A + \dim V_B. \tag{1}$$

(ii) [3, Proposition 2(ii)] *We have the equivalence*

$$A \in \mathbf{\Upsilon}_m \Leftrightarrow V_A = 0. \tag{2}$$

Remark 1. If we consider only solutions belonging to a subfield F of Λ then (1) does not hold in general even in the scalar case. Indeed, take $m = 1$, $K = F = \overline{\mathbb{Q}}(x)$, $A = x\partial - 1$, $B = x^2\partial + 1$. The solution space $\mathrm{Sol}_F A$ of A whose elements belong to F is generated over constants by x, and $\mathrm{Sol}_F B = \mathrm{Sol}_F AB = 0$; so $\dim \mathrm{Sol}_F AB = 0$ while $\dim \mathrm{Sol}_F A + \dim \mathrm{Sol}_F B = 1 + 0 = 1$.

We assume that the field K is *computable*, i.e., there exist algorithms to execute the field operations and an algorithm for zero testing in K. The following known algorithms are important in the context of our paper:

$\mathbf{A}_1$: Given $C \in K[\partial]^{n\times m}$, the algorithm RowReduction from [5] (*algorithm RR* in the sequel) allows one in particular to find a matrix $U \in \mathbf{\Upsilon}_m$ such that the number of nonzero rows of UC is equal to the rank of C, and those rows are the first rows of UC. Since U is unimodular, the nonzero rows of UC are independent over $K[\partial]$ ([4], [5]).

$\mathbf{A}_2$: Given $A \in \mathbf{\Phi}_m$, the algorithm from [2] can be used to compute $\dim V_A$.

$\mathbf{A}_3$: Given $A \in \mathbf{\Phi}_m$, the algorithm discussed in [1, 3] allows one to test whether A is unimodular, and to construct A^{-1} if the answer is positive.

The following lemma will also be useful in the sequel:

Lemma 1 ([5]). *Let $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$. Let*

$$C = \begin{pmatrix} A \\ B \end{pmatrix} \in K[\partial]^{2m\times m}.$$

Then one can construct $U \in \mathbf{\Upsilon}_{2m}$ such that the first m rows of UC are independent over $K[\partial]$ while its last m rows are zero.

The matrix U can be constructed by the algorithm RR (see $\mathbf{A}_1$).

3. THE GREATEST COMMON RIGHT DIVISOR

Definition 1. Let $A, B, D \in \mathbf{M}_m$. Then

—D is a right divisor of A (we write $D\big|_r A$) if there exists $Q \in \mathbf{M}_m$ such that $A = QD$,

—D is a common right divisor of A, B if $D\big|_r A$ and $D\big|_r B$.

Lemma 2. *Let $A \in \mathbf{\Phi}_m$, $Q, D \in \mathbf{M}_m$ and $A = QD$. Then $Q, D \in \mathbf{\Phi}_m$.*

Proof. First, if $Q \notin \mathbf{\Phi}_m$ then there exist $f_1,\dots,f_m \in K$, such that $\exists_{i,1\le i\le m} f_i \ne 0$ and $f_1Q_{1,*} + \dots + f_mQ_{m,*} = 0$. The equality $A = QD$ implies that $f_1A_{1,*} + \dots + f_mA_{m,*} = 0$, and $A \notin \mathbf{\Phi}_m$.

Second, if $D \notin \mathbf{\Phi}_m$ then there exist $f_1,\dots,f_m \in K$, such that $\exists_{i,1\le i\le m} f_i \ne 0$ and $D_{*,1}f_1 + \dots + D_{*,m}f_m = 0$. The equality $A = QD$ implies that $A_{*,1}f_1 + \dots + A_{*,m}f_m = 0$, and $A \notin \mathbf{\Phi}_m$.

Lemma 3. *Let $A, B \in \mathbf{M}_m$. Then*

(i) *$V_D \subseteq V_A \cap V_B$ for any common divisor D of A, B.*

(ii) *If $A \in \mathbf{\Phi}_m$ then there exists a common right divisor $D \in \mathbf{\Phi}_m$ of A and B such that $V_D = V_A \cap V_B$.*

(iii) *If $A \in \mathbf{\Phi}_m$, D is as in* (ii) *and $V_A = V_D$ then $D = TA$ with $T \in \mathbf{\Upsilon}_m$.*

Proof. (i) This follows from $A = Q_1D$, $B = Q_2D$ for some $Q_1, Q_2 \in \mathbf{M}_m$. We have $V_D \subseteq V_A$ and $V_D \subseteq V_B$.

(ii) Let $D \in \mathbf{\Phi}_m$ be the $m\times m$ matrix consisting of the nonzero rows of the $2m\times m$ matrix UC, where U, C are as in Lemma 1. Then $V_D = V_A \cap V_B$. Indeed, $V_C = V_A \cap V_B$ and $V_C = V_{UC}$ since U is unimodular; observe that $V_{UC} \subset \Lambda^m$ and $V_{UC} = V_D$. In addition, $D\big|_r A$, $D\big|_r B$, i.e., there exist $Q_1, Q_2 \in \mathbf{M}_m$ such that $A = Q_1D$, $B = Q_2D$. Indeed, we have $C = U^{-1}(UC)$. Remove from U^{-1} the columns having indices corresponding to zero rows of UC, i.e., the last m columns. Denote the resulting $2m\times m$ matrix by $\tilde{U}$. Then

$$C = \tilde{U}D. \tag{3}$$

We can represent $\tilde{U}$ in the block form:

$$\tilde{U} = \begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix}, \tag{4}$$

$Q_1, Q_2 \in \mathbf{M}_m$. Then (3) gives us $A = Q_1D$, $B = Q_2D$. By Lemma 2, $D \in \mathbf{\Phi}_m$.

(iii) Let $D \in \mathbf{\Phi}_m$ be constructed as in (ii). As $A = QD$ for some $Q \in \mathbf{\Phi}_m$, it follows from (1) that $\dim V_Q = \dim V_A - \dim V_D = 0$, hence $Q \in \mathbf{\Upsilon}_m$ by (2) and $D = TA$ with $T = Q^{-1} \in \mathbf{\Upsilon}_m$.

Lemma 4. *Let $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$. Then $A\big|_r B \Leftrightarrow V_A \subseteq V_B$.*

Proof. ($\Rightarrow$) $B = QA$ for some $Q \in \mathbf{\Phi}_m$, so each solution of A is a solution of B.

($\Leftarrow$) Let D be a common right divisor of A and B such that $V_D = V_A \cap V_B$ (Lemma 3(ii)). Then $V_D = V_A$ and by Lemma 3(iii) we get $D = TA$ with $T \in \mathbf{\Upsilon}_m$, and $(TA)\big|_r B$, i.e., $(QT)A = B$ with $QT \in \mathbf{M}_m$. So, $A\big|_r B$.

Proposition 2. Let $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$. *Then there exists a common right divisor D of A, B such that any other common right divisor of A, B is a right divisor of D. Such a common right divisor D is defined uniquely up to a left factor from $\mathbf{\Upsilon}_m$.*

Proof. Let D be as in Lemma 3(ii). Let $\tilde{D}$ be another right common divisor of A, B. By Lemma 2, $\tilde{D} \in \mathbf{\Phi}_m$. By Lemmas 3(i), 4, we have $\tilde{D}\big|_r D$.

Now, let D and $\tilde{D}$ be such that $V_D = V_{\tilde{D}} = V_A \cap V_B$. By Lemma 4($\Leftarrow$), $D\big|_r \tilde{D}$ and $\tilde{D}\big|_r D$, i.e., $\tilde{D} = QD$ and $D = \tilde{Q}\tilde{D}$ for some $Q, \tilde{Q} \in \mathbf{\Phi}_m$. By $\dim V_D = \dim V_{\tilde{D}}$ and (1) we get $\dim V_Q = \dim V_{\tilde{Q}} = 0$. By (2), $Q, \tilde{Q} \in \mathbf{\Upsilon}_m$.

Definition 2. The greatest common right divisor of $A, B \in \mathbf{\Phi}_m$, denoted by $\mathrm{gcrd}(A, B)$, is a right divisor D of A, B such that any other common right divisor of A, B is a right divisor of D.

By Proposition 2 for any $A, B \in \mathbf{\Phi}_m$ the greatest common right divisor $\mathrm{gcrd}(A, B)$ is defined uniquely up to a left factor from $\mathbf{\Upsilon}_m$. Thus, $\mathrm{gcrd}(A, B)$ is actually a set of matrices. Instead of $D \in \mathrm{gcrd}(A, B)$, we will write $D = \mathrm{gcrd}(A, B)$ if D belongs to this set.

From the proof of Lemma 3(ii) we have

Proposition 3. *For any $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$ we can construct algorithmically $D = \mathrm{gcrd}(A, B)$ belonging to $\mathbf{\Phi}_m$ and $Q_1 \in \mathbf{\Phi}_m$, $Q_2 \in \mathbf{M}_m$ such that $A = Q_1 D$, $B = Q_2 D$. For V_D, the equality $V_D = V_A \cap V_B$ holds.*

Lemma 5. *Let $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$ and $D = \mathrm{gcrd}(A, B) \in \mathbf{\Phi}_m$. Then we can construct algorithmically $G, H \in \mathbf{M}_m$ such that $GA + HB = D$.*

Proof. Let U, as in Lemma 1, be a $2m \times m$ matrix such that

$$U\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} D \\ 0 \end{pmatrix}.$$

Write

$$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix},$$

where $U_{ij} \in \mathbf{M}_m$. Take $G = U_{11}$ and $H = U_{12}$.

Definition 3. Two operator matrices $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$ are right coprime if $D = \mathrm{gcrd}(A, B) \in \mathbf{\Upsilon}_m$. In other words, A and B are right coprime if $V_A \cap V_B = \{0\}$.

Remark 2. If A and B are right coprime then $\mathrm{gcrd}(A, B) = I_m$, the identity matrix.

Proposition 4. *Two operator matrices $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$ are right coprime if and only if there exist $G, H \in \mathbf{M}_m$ such that $GA + HB = I_m$.*

Proof. If $GA + HB = I_m$ then the only common solution of A and B is 0.

4. DIVISIBILITY OF OPERATOR MATRICES

Let $A \in \mathbf{\Phi}_m$, $B \in \mathbf{M}_m$. Suppose that we want to test whether $A\big|_r B$, and if this relation holds then to construct $Q \in \mathbf{M}_m$ such that $B = QA$.

This can be done algorithmically:

(1) Let $D = \mathrm{gcrd}(A, B)$ and $A = Q_1 D$, $B = Q_2 D$ for $Q_1 \in \mathbf{\Phi}_m$, $Q_2 \in \mathbf{M}_m$ (Prop. 3). Note that $A\big|_r B$ holds if and only if $Q_1 \in \mathbf{\Upsilon}_m$.

(2) Use algorithm $\mathbf{A}_3$ to test whether $Q_1 \in \mathbf{\Upsilon}_m$. If the answer is negative then $A\big|_r B$ does not hold;

(3) otherwise compute Q_1^{-1} by algorithm $\mathbf{A}_3$. We get $B = QA$ with $Q = Q_2 Q_1^{-1} \in \mathbf{M}_m$.

Remark 3. This algorithm generalizes the algorithm from [1] for inverting matrices: $A \in \mathbf{M}_m$ is invertible (unimodular) if and only if $A\big|_r I_m$ where I_m is the identity matrix; the equality $I_m = QA$ implies that $A^{-1} = Q$.

5. THE LEAST COMMON LEFT MULTIPLE

Definition 4. Let $A, B, M \in \mathbf{\Phi}_m$. Then

—M is a left multiple of A if $A\big|_r M$,

—M is a common left multiple of A and B if $A\big|_r M$, $B\big|_r M$.

Lemma 6. *Let $A, B \in \mathbf{\Phi}_m$, then there exists a common left multiple M of A, B.*

Proof. Let U, C be as in Lemma 1. The last m rows of the matrix U form a $m \times 2m$ matrix P such that $PC = 0$. Let $P = (P_1\ P_2)$, where P_1, P_2 are $m \times m$ matrices. Now

$$P_1 A + P_2 B = 0. \tag{5}$$

Suppose that P_1 is not of full rank. Then there exists $W \in \mathbf{\Upsilon}_m$ such that the first row of WP_1 is zero. In this case the first row of $WP_2 B$ is also zero, and since B is of full rank, the first row of WP_2 is zero. Hence the first row of WP is zero, which implies that the rows of P are linearly dependent, but this does not hold since the rows of U are linearly independent. So, $P_1 \in \mathbf{\Phi}_m$, and similarly $P_2 \in \mathbf{\Phi}_m$. Thus $P_1 A$ (as well as $P_2 B$) is a common left multiple of A and B.

Proposition 5. *Let $A, B \in \mathbf{\Phi}_m$, then there exists a common left multiple M of A, B such that any other common left multiple of A, B is a left multiple of M. Such a common left multiple M is defined uniquely up to a left factor from $\mathbf{\Upsilon}_m$.*

Proof. By Lemma 6, the set of common left multiples is not empty. Let M be a common left multiple of A, B with the minimal dimension, and let $\tilde{M}$ be an arbitrary common left multiple of A, B. Then $D = \mathrm{gcrd}(M, \tilde{M})$ is also a common left multiple of A, B, $\dim V_D = \dim V_M$, and $V_D \subseteq V_M$, hence (as these are finite-dimensional spaces) $V_D = V_M$. But $V_D \subseteq V_{\tilde{M}}$ as well, so $V_M \subseteq V_{\tilde{M}}$. By Lemma 4, $M\big|_r \tilde{M}$.

Definition 5. The least common left multiple of $A, B \in \mathbf{\Phi}_m$, denoted by $\mathrm{lclm}(A, B)$, is a left multiple M of A, B such that any other common left multiple of A, B is a left multiple of M.

By Proposition 5, for any $A, B \in \mathbf{\Phi}_m$ their least common left multiple is defined uniquely up to a left factor from $\mathbf{\Upsilon}_m$. Thus, $\mathrm{lclm}(A, B)$ is actually a set of matrices. Instead of $M \in \mathrm{lclm}(A, B)$, we write $M = \mathrm{lclm}(A, B)$ if M belongs to this set.

Proposition 6 ([5, Section 9.3]). *Let $A, B \in \mathbf{\Phi}_m$, then the common left multiple of A, B described in the proof of Lemma 6 is* $\mathrm{lclm}(A, B)$.

Thus, for any $A, B \in \mathbf{\Phi}_m$ the operator $L = \mathrm{lclm}(A, B) \in \mathbf{\Phi}_m$ can be constructed algorithmically, as well as $P_1, P_2 \in \mathbf{\Phi}_m$ such that $P_1 A = P_2 B = L$.

Proposition 7. *Let $A, B, L \in \mathbf{\Phi}_m$ such that $V_L = V_A + V_B$. Then $L = \mathrm{lclm}(A, B)$.*

Proof. We see that $V_A, V_B \subseteq V_L$. By Lemma 4, L is a left common multiple of A, B. Let $M \in \mathbf{\Phi}_m$ be another left common multiple of A and B. Then $V_M \supseteq V_A + V_B = V_L$. This implies that $L\big|_r M$. Thus $L = \mathrm{lclm}(A, B)$.

The converse, i.e., $L = \mathrm{lclm}(A, B) \Rightarrow V_L = V_A + V_B$ will be proved later: see Theorem 1.

Example 1. Consider the three operator matrices belonging to $\mathbb{C}(x)[\partial]^{2\times 2}$ with $\partial = \frac{d}{dx}$.

$$A = \begin{pmatrix} \partial & 0 \\ -x & 1 \end{pmatrix}, \quad B = \begin{pmatrix} \partial - \frac{1}{x} & 0 \\ -x & 1 \end{pmatrix}, \quad \text{and} \quad L = \begin{pmatrix} \partial^2 & 0 \\ -x & 1 \end{pmatrix}.$$

One can directly check that V_A is generated by $(1, x)^{\mathrm{T}}$, V_B is generated by $(x, x^2)^{\mathrm{T}}$ and $V_L = V_A + V_B$. Thus $L = \operatorname{lclm}(A, B)$ by Proposition 7; we have

$$L = \begin{pmatrix} \partial & 0 \\ 0 & 1 \end{pmatrix} A = \begin{pmatrix} \partial + \frac{1}{x} & 0 \\ 0 & 1 \end{pmatrix} B.$$

6. A MATRIX HAVING A GIVEN SPACE OF SOLUTIONS

Let (K, ∂) be as before a differential field, and denote by $\mathscr{C}$ its constant field. Let n be a positive integer and $f_1, \ldots, f_n$ be n elements in K. We denote by $Wr(f_1, \ldots, f_n)$ their Wronskian, that is the determinant of the Wronskian matrix

$$\begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ \partial(f_1) & \partial(f_2) & \cdots & \partial(f_n) \\ \vdots & \vdots & \ddots & \vdots \\ \partial^{n-1}(f_1) & \partial^{n-1}(f_2) & \cdots & \partial^{n-1}(f_n) \end{pmatrix}.$$

Recall that $f_1, \ldots, f_n$ are linearly dependent over $\mathscr{C}$ if and only if $Wr(f_1, \ldots, f_n) = 0$ (for a proof, see [14, p. 9, Lemma 1.12]). We also recall that given n elements $f_1, \ldots, f_n \in K$ that are linearly independent over $\mathscr{C}$, there exists an operator $N \in K[\partial]$ of order n such that the space V_N of solutions of N is generated over $\mathscr{C}$ by the family $f_1, \ldots, f_n$. Such an operator N can be obtained as

$$N = \begin{vmatrix} f_1 & f_2 & \cdots & f_n & \partial^0 \\ \partial(f_1) & \partial(f_2) & \cdots & \partial(f_n) & \partial^1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \partial^n(f_1) & \partial^n(f_2) & \cdots & \partial^n(f_n) & \partial^n \end{vmatrix}.$$

We are going to extend this result to the case where $f_1, \ldots, f_n$ are column vectors in K^m where m is an arbitrary positive integer.

For $f_1, \ldots, f_n \in K^m$, we will denote by $\langle f_1, \ldots, f_n \rangle$ the $\mathscr{C}$-vector space generated by $f_1, \ldots, f_n$. If $F \in K^{m\times n}$ then we will write $\langle F \rangle$ for the $\mathscr{C}$-vector space generated by the columns of F.

Lemma 7. *Let r be a positive integer and $u_1, \ldots, u_r$ be $\mathscr{C}$-linearly independent elements of K. Then for all $v_1, \ldots, v_r$ in K there exists an operator $\ell \in K[\partial]$ of order at most $r - 1$ such that $\ell(u_j) = v_j$ for $j = 1, \ldots, r$.*

Proof. Let $W = Wr(u_1, \ldots, u_r)$. The matrix W is invertible, since $u_1, \ldots, u_r$ are $\mathscr{C}$-linearly independent. We search for $\ell = \sum_{i=0}^{r-1} a_i \partial^i$ where the a_i are elements of K to be determined so that $\ell(u_j) = v_j$ for $j = 1, \ldots, r$. This yields the system of linear algebraic equations

$$W^T \begin{pmatrix} a_0 \\ \vdots \\ a_{r-1} \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix}.$$

Proposition 8. *Let m and n be positive integers, and let $f_1, \ldots, f_n$ be $\mathscr{C}$-linearly independent column vectors belonging to K^m. Then there exists $N \in \mathbf{\Phi}_m$ of order at most n, such that $V_N = \langle f_1, \ldots, f_n \rangle$.*

Proof. We will proceed by induction on m. The result is true for $m = 1$. Let $m \geq 2$ and suppose that the result is true for any family of vectors belonging to K^{m-1}. Consider $f_1, \ldots, f_n \in K^m$ and denote by $F = (f_{ij})$

the $m \times n$ matrix whose columns are $f_1, \dots, f_n$. Let $r = \dim\langle f_{11}, f_{12}, \dots, f_{1n}\rangle$. We have $0 \le r \le n$ ($r = 0$ means the first row of F is zero). Without loss of generality we can assume that $f_{1,j} = 0$ for $j > r$. We denote by $\tilde{F}$ the submatrix of F, obtained by deleting the first row and the r first columns of F. We then can apply the induction hypothesis to the $n - r$ columns of $\tilde{F}$: there exists $\tilde{N} \in \mathbf{\Phi}_{m-1}$ of order at most $n - r$, $V_{\tilde{N}} = \langle \tilde{F}\rangle$. Put $M = \operatorname{diag}(1, \tilde{N}) \in \mathbf{\Phi}_m$. It is clear that $\operatorname{ord} M \le n - r$ and $V_M = \langle f_{r+1}, \dots, f_n\rangle$. If $r = 0$ then we are done because we can take $N = M$.

Suppose that $r \ge 1$ and let $\ell_{11} \in K[\partial]$ denote the monic scalar operator of order r whose solution space is generated by the family $\{f_{11}, \dots, f_{1r}\}$. By Lemma 7, we know that for each $i = 2, \dots, m$ there exists a scalar differential operator $\ell_{i1} \in K[\partial]$ of order at most $r - 1$ such that $\ell_{i1}(f_{1j}) = f_{ij}$ for $j = 1, \dots, r$. Let R be the following full rank $m \times m$ matrix

$$R = \begin{pmatrix} \ell_{11} & 0 & 0 & \dots & 0 \\ -\ell_{21} & 1 & 0 & \dots & 0 \\ -\ell_{31} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\ell_{m1} & 0 & 0 & \dots & 1 \end{pmatrix}.$$

One can check that $V_R = \langle f_1, \dots, f_r\rangle$. Now we claim that $N := MR$ has the requested properties, namely N is of full rank, $\operatorname{ord} N \le n$ and $V_N = \langle f_1, \dots, f_n\rangle$. Indeed, one can check easily that $f_1, \dots, f_n$ belong to V_N. This is clear for $f_1, \dots, f_r$ as they are solutions of R. As for $f_{r+1}, \dots, f_n$, we note that they are fixed by R, i.e., $R(f_j) = f_j$ for $j = r + 1, \dots, f_n$ (since they have their first component equal to zero), hence $N(f_j) = MR(f_j) = M(f_j) = 0$. We conclude by noting that $\dim V_N = \dim V_M + \dim V_R = n$.

Note that a similar result, whose proof uses the notion of Dieudonné determinant, can be found in [7, Lemma 1.41]. However, our proof of Proposition 8 is completely different, more elementary and constructive.

Remark 4. The operator matrix $N = (\ell_{ij})$ constructed in the above proof is a lower triangular matrix belonging to $\mathbf{\Phi}_m$ of order at most n such that $\sum_{i=1}^{m} \operatorname{ord}(\ell_{ii}) = n$ and its off-diagonal entries are of order at most $n - 1$. This can be proven by a double induction on m and n. Indeed, it suffices to observe that N can be partitioned into four blocs

$$N = MR = \begin{pmatrix} 1 & 0 \\ 0 & \tilde{N} \end{pmatrix} \begin{pmatrix} \ell_{11} & 0 \\ -\tilde{\ell} & 1 \end{pmatrix} \begin{pmatrix} \ell_{11} & 0 \\ -\tilde{N}\tilde{\ell} & \tilde{N} \end{pmatrix},$$

where $\tilde{\ell} = (\ell_{21}, \dots, \ell_{m1})^{\mathrm{T}}$ and $V_{\tilde{N}} = \langle f_{r+1}, \dots, f_n\rangle$.

By construction, we have $\operatorname{ord} \ell_{11} = r$, $\operatorname{ord} \tilde{\ell} \le r - 1$ and by induction $\tilde{N}$ is a lower triangular operator matrix of order at most $n - r$ whose off-diagonal elements are of order at most $n - r - 1$ and the sum of the orders of its diagonal entries is $n - r$. We conclude by remarking that $\operatorname{ord} \tilde{N}\tilde{\ell} \le n - r + r - 1 = n - 1$.

Example 2. Consider the differential field $K = \mathbb{Q}(x)$ equipped with the derivation $\partial = \frac{d}{dx}$.

(1) Let us apply the method described in the above proof to the family $\{f_1, f_2\}$ where $f_1 = (1, x)^{\mathrm{T}}$ and $f_2 = (x, x^2)^{\mathrm{T}}$. The first components of f_1, f_2 are linearly independent over $\mathscr{C}$, since $f_{11} = 1$, $f_{12} = x$. Thus, we take $\ell_{11} := \operatorname{lclm}(\partial, \partial - 1/x) = \partial^2$; then we look for ℓ_{21} of order 0 such that $\ell_{21}(1) = x$ and $\ell_{21}(x) = x^2$ and get $\ell_{21} = x$. Hence, we obtain

$$R = \begin{pmatrix} \ell_{11} & 0 \\ -\ell_{21} & 1 \end{pmatrix} = \begin{pmatrix} \partial^2 & 0 \\ -x & 1 \end{pmatrix}, \quad V_R = \langle f_1, f_2\rangle.$$

(2) Consider a third column vector $f_3 = (0, x^3)^{\mathrm{T}}$ and apply our method to the family $\{f_1, f_2, f_3\}$. The matrix F is given by

$$F = \begin{pmatrix} 1 & x & 0 \\ x & x^2 & x^3 \end{pmatrix}.$$

Here $r = 2$ and $\tilde{F} = (x^3)$. Thus, $\tilde{N} = (\partial - 3/x)$ and R is as in item 1. Hence

$$N = \operatorname{diag}(1, \tilde{N})R = \begin{pmatrix} 1 & 0 \\ 0 & \partial - 3/x \end{pmatrix}\begin{pmatrix} \partial^2 & 0 \\ -x & 1 \end{pmatrix} = \begin{pmatrix} \partial^2 & 0 \\ -x\partial + 2 & \partial - 3/x \end{pmatrix}.$$

Example 3.

(1) Now, instead of the three previous vectors, consider the columns of the matrix

$$G = PF = \begin{pmatrix} x & x^2 & x^3 \\ 1 & x & 0 \end{pmatrix},$$

where P is the following permutation matrix

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

For G, we have $r = \dim\left\langle x, x^2, x^3 \right\rangle = 3$ so we take

$$\ell_{11} := \operatorname{lclm}\left(\partial - \frac{1}{x}, \partial - \frac{2}{x}, \partial - \frac{3}{x}\right) = \partial^3 - 3x^{-1}\partial^2 + 6x^{-2}\partial - 6x^{-3}.$$

Now we should find $\ell_{21} = a_0 + a_1\partial + a_2\partial^2$ such that $\ell_{21}(x) = 1$, $\ell_{21}(x^2) = x$ and $\ell_{21}(x^3) = 0$. For this we have to solve the following linear system

$$\begin{pmatrix} x & 1 & 0 \\ x^2 & 2x & 2 \\ x^3 & 3x^2 & 6x \end{pmatrix}\begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 1 \\ x \\ 0 \end{pmatrix}.$$

We find $a_0 = 0$, $a_1 = 1$, $a_2 = -x/2$. Hence $\ell_{21} = -\frac{x}{2}\partial^2 + \partial$. This yields the matrix operator

$$R = \begin{pmatrix} \ell_{11} & 0 \\ -\ell_{21} & 1 \end{pmatrix} = \begin{pmatrix} \partial^3 - \frac{3}{x}\partial^2 + \frac{6}{x^2}\partial - \frac{6}{x^3} & 0 \\ \frac{x}{2}\partial^2 - \partial & 1 \end{pmatrix}$$

which satisfies $V_R = \langle g_1, g_2, g_3 \rangle$. It follows that the operator

$$N' = PRP = \begin{pmatrix} 1 & \frac{x}{2}\partial^2 - \partial \\ 0 & \partial^3 - \frac{3}{x}\partial^2 + \frac{6}{x^2}\partial - \frac{6}{x^3} \end{pmatrix}$$

satisfies $V_{N'} = \langle f_1, f_2, f_3 \rangle$.

(2) Since $V_N = V_{N'}$, we should have $N' = TN$ for some $T \in \boldsymbol{\Upsilon}_2$. This is indeed the case, with

$$T = \begin{pmatrix} \frac{x^2}{2} & \frac{1}{2}(x\partial + 1) \\ x\partial & \partial^2 \end{pmatrix}.$$

7. THE SOLUTION SPACE OF $\operatorname{lclm}(A, B)$

Theorem 1. *Let $A, B, L \in \boldsymbol{\Phi}_m$. Then $V_L = V_A + V_B$ if and only if $L = \operatorname{lclm}(A, B)$.*

Proof. The “only if” condition was proved in Proposition 7. Now suppose that $L = \mathrm{lclm}(A, B)$ and let $f_1, \ldots, f_n \subset \Lambda^m$ be a basis for $V_A + V_B$. By Proposition 8, there exists an operator matrix $N \in \mathbf{\Phi}_m(\Lambda)$ such that $V_N = V_A + V_B$. By Lemma 4, the matrix N is a common left multiple of A and B if one considers them as matrices over Λ. Thus $L\big|_r N$ and $V_L \subseteq V_A + V_B$. Taking into account that $V_A, V_B \subseteq V_L$ we obtain $V_L = V_A + V_B$.

Corollary 1. $\dim V_{\mathrm{lclm}(A,B)} = \dim V_A + \dim V_B - \dim V_{\mathrm{gcrd}(A,B)}$.

Example 4. Consider the two operators

$$A = \begin{pmatrix} \partial^2 & 0 \\ -x & 1 \end{pmatrix}, \quad B = \begin{pmatrix} \partial - 1/x & 0 \\ -x\partial + 2 & \partial - 3/x \end{pmatrix}.$$

One has

$$V_A = \left\langle (1, x)^{\mathrm{T}}, (x, x^2)^{\mathrm{T}} \right\rangle, \quad V_B = \left\langle (x, x^2)^{\mathrm{T}}, (0, x^3)^{\mathrm{T}} \right\rangle, \quad V_A \cap V_B = \left\langle (x, x^2)^{\mathrm{T}} \right\rangle.$$

Let $L = \mathrm{lclm}(A, B)$ and $D = \mathrm{gcrd}(A, B)$. Then

$$V_L = \left\langle (1, x)^{\mathrm{T}}, (x, x^2)^{\mathrm{T}}, (0, x^3)^{\mathrm{T}} \right\rangle, \quad V_D = \left\langle (x, x^2)^{\mathrm{T}} \right\rangle.$$

The operators L and D can be constructed using the method in Section 6:

$$L = \begin{pmatrix} \partial^2 & 0 \\ -x\partial + 2 & \partial - 3/x \end{pmatrix}, \quad D = \begin{pmatrix} \partial - \dfrac{1}{x} & 0 \\ -x & 1 \end{pmatrix}.$$

Remark 5. If instead of considering solutions in Λ^m we consider only the solutions in F^m where F is a field such that $K \subset F \subset \Lambda$ then the statement of Theorem 1 is not in general correct (compare with Remark 1). Indeed, the solution space of $L = \mathrm{lclm}(A, B)$ in F^m can be larger than the sum of the solution spaces of A and B over F as illustrated by the following example.

Example 5. Consider the field $K = \overline{\mathbb{Q}}(x)$ equipped with the derivation $\partial = x\dfrac{d}{dx}$. Let $f \in \overline{\mathbb{Q}}(x)$ be a nonconstant rational function and consider the following operators in $K[\partial]$:

$$A = \partial^2, \quad B = (1 + \partial(f))\partial^2 - \partial^2(f)\partial.$$

One has

$$L = \mathrm{lclm}(A, B) = \partial^2(f)\partial^3 - \partial^3(f)\partial^2.$$

The solution spaces having components in Λ are, respectively,

$$V_A = \langle 1, \log x \rangle, \quad V_B = \langle 1, \log x + f(x) \rangle, \quad V_L = \langle 1, f(x), \log x \rangle$$

while the solution spaces having components in K are, respectively,

$$\mathrm{Sol}_K(A) = \langle 1 \rangle, \quad \mathrm{Sol}_K(B) = \langle 1 \rangle, \quad \mathrm{Sol}_K(L) = \langle 1, f(x) \rangle.$$

8. RIGHT AND LEFT DIVISIONS

In previous sections, we discussed right division: A is the right factor in the product QA. Left division $B = AQ$ may also be of interest. The algorithms described above can be used for left division if we consider adjoint matrices. For a scalar operator $L = a_k\partial^k + \ldots + a_1\partial + a_0 \in K[\partial]$ its adjoint operator has the form $L^* = (\partial^*)^k a_k + \ldots + \partial^* a_1 + a_0$ with $\partial^* = -\partial$. For an $m \times m$ matrix

$$\begin{pmatrix} L_{11} & \ldots & L_{1m} \\ \vdots & \ddots & \vdots \\ L_{m1} & \ldots & L_{mm} \end{pmatrix},$$

its adjoint is the $m \times m$ matrix

$$\begin{pmatrix} L_{11}^* & \dots & L_{m1}^* \\ \vdots & \ddots & \vdots \\ L_{1m}^* & \dots & L_{mm}^* \end{pmatrix}.$$

It is significant that $(M_1M_2)^* = M_2^*M_1^*$, and $M^{**} = M$. Hence $B = AQ \Leftrightarrow B^* = Q^*A^*$. For example, we can apply the algorithm described in Section 4 to A^*, B^*. We can observe that B is left divisible by A if and only if B^* is right divisible by A^*, and if $B^* = QA^*$ then $B = AQ^*$.

ACKNOWLEDGMENTS

The authors would like to thank Michael F. Singer for his valuable advice.

FUNDING

Abramov's research was supported in part by the Russian Foundation for Basic Research, project no. 19-01-00032-a. Petkovšek's research was supported in part by the Ministry of Education, Science, and Sport of Slovenia research program P1-0294.

REFERENCES

1. S. Abramov, "On the differential and full algebraic complexities of operator matrices transformations," in *Proceedings of CASC'2016, Lecture Notes in Computer Science* (Springer, Heidelberg, 2016), Vol. 9890, pp. 1–14.
2. S. Abramov and M. Barkatou, "On the dimension of solution spaces of full rank linear differential systems," in *Computer Algebra in Scientific Computing: Proceedings of the 15th International Workshop, CASC'2013, Berlin, Germany, September 2013, Lecture Notes in Computer Science* (Springer, Heidelberg, 2013), pp. 1–9.
3. S. Abramov and M. Barkatou, "On solution spaces of products of linear differential or difference operators," ACM Commun. Comput. Algebra **48** (4), 155–165 (2014).
4. M. Barkatou, C. El Bacha, G. Labahn, and E. Pflügel, "On simultaneous row and column reduction of higher-order linear differential systems," J. Symb. Comput. **49** (1), 45–64 (2013).
5. B. Beckermann, H. Cheng, and G. Labahn, "Fraction-free row reduction of matrices of Ore polynomials," J. Symb. Comput. **41** (5), 513–543 (2006).
6. B. Beckermann and G. Labahn, "Fraction-free computation of matrix rational interpolants and matrix GCDs," SIAM J. Matrix Anal. Appl. **22** (1), 114–144 (2000).
7. S. Carpentier, PhD Thesis (Massachusetts Institute of Technology, 2017). https://dspace.mit.edu/handle/1721.1/112909
8. P. M. Cohn, *Free Rings and Their Relations* (Academic, London, 1971).
9. J. C. McConnell and J. C. Robson, *Noncommutative Noetherian Rings*, rev. ed. (Am. Math. Soc., Providence, RI, 2001).
10. P. A. Hendriks and M. F. Singer, "Solving difference equations in finite terms," J. Symb. Comput. **27** (3), 239–259 (1999).
11. M. van Hoeij, "Finite singularities and hypergeometric solutions of linear recurrence equations," J. Pure Appl. Algebra **139** (1–3), 109–131 (1999).
12. E. R. Kolchin, *Differential Algebra and Algebraic Groups* (Academic, New York, 1973).
13. M. Miyake, "Remarks on the formulation of the Cauchy problem for general system of ordinary differential equations," Tôhoku Math. J. **32** (1), 79–89 (1980).
14. M. van der Put and M. F. Singer, *Galois Theory of Linear Differential Equations* (Springer, Berlin, 2003).