*ACM Communications in Computer Algebra, Vol. 48, No. 4, Issue 190, December 2014*

# On Solution Spaces of Products of Linear Differential or Difference Operators

Sergei A. Abramov *
Computing Centre
of the Russian Academy of Sciences
Vavilova 40, Moscow, 119333
Russia
sergeyabramov@mail.ru

Moulay A. Barkatou
Institut XLIM, DMI,
Université de Limoges; CNRS
123, Av. A. Thomas, 87060 Limoges
France
moulay.barkatou@unilim.fr

**Abstract**

We consider linear ordinary differential or difference systems of the form $L(y) = 0$ where $L$ is an operator with matrix coefficients, the unknown vector $y$ has $m$ components $y_1, \ldots, y_m$, $m \geqslant 1$. The matrix coefficients are of size $m \times m$, their entries belong to a differential or difference field $K$ of characteristic 0. For any such a system the solution space $V_L$ is considered, and the components of each solution are in a fixed appropriate differential or difference extension of $K$ (e.g., in the universal Picard-Vessiot extension). We prove that $\dim V_{LM} = \dim V_L + \dim V_M$ for arbitrary operators $L$ and $M$ of the considered form, and discuss some algorithms based on this property of operators. In particular, we propose an algorithm to compute $\dim V_L$, as well as a new algorithm having a low complexity for recognizing unimodular operators and constructing the inverse of a unimodular operator.

## 1 Introduction

Linear ordinary differential and difference systems with variable coefficients appear in various areas of mathematics. In this paper we discuss some questions related to the dimension of solution spaces of such systems. First we detail the differential case, then we consider specific features of difference systems.

Let $K$ be a differential field of characteristic 0 with a derivation $\partial = '$. The ring of $m \times m$ matrices with entries belonging to a ring $R$ is denoted by $\mathrm{Mat}_m(R)$. Let $K[\partial]$ denote the ring of differential operators with coefficients in $K$. Any non-zero element $L \in \mathrm{Mat}_m(K[\partial])$ can be represented as a differential operator with matrix coefficients in $\mathrm{Mat}_m(K)$:

$$L = A_r\partial^r + A_{r-1}\partial^{r-1} + \cdots + A_0, \tag{1}$$

where the coefficients $A_0, A_1, \ldots, A_r$ belong to $\mathrm{Mat}_m(K)$, and where $A_r$ (the *leading matrix* of $L$) is non-zero. The number $r$ is the *order* of $L$ (we write $r = \operatorname{ord} L$). The corresponding differential system $L(y) = 0$ is given by

$$A_r y^{(r)} + A_{r-1} y^{(r-1)} + \cdots + A_0 y = 0, \tag{2}$$

where $y$ is an unknown $m-$dimensional vector with components $y_1, \ldots, y_m$. When the operator $L$ is of full rank, i.e., the equations of the corresponding system (2) are linearly independent over $K[\partial]$, the solution space $V_L$ is of finite dimension. In the *scalar case*, i.e., the case where $m = 1$, any non-zero scalar equation

*Supported in part by the Russian Foundation for Basic Research, project no. 13-01-00182-a. The first author thanks also Department of Mathematics and Informatics of XLIM Institute of Limoges University for the hospitality during his visits.

$L(y) = 0$, has in appropriate extensions of $K$ a solution space $V_L$ whose dimension is equal to $\operatorname{ord} L$. Moreover, if for scalar operator $L, M \in K[\partial]$ we consider the equation $LM(y) = 0$, where $LM$ is the product of the operators $L$ and $M$ then we have

$$\dim V_{LM} = \dim V_L + \dim V_M. \tag{3}$$

The equality (3) is a direct consequence of the equality $\operatorname{ord}(LM) = \operatorname{ord} L + \operatorname{ord} M$.

In the case of a system of differential equations the situation is not so simple. If the leading matrix of $L$ is invertible then $\dim V_L = m \operatorname{ord} L$ in an appropriate differential extension of $K$. However, if this matrix is not invertible then $\dim V_L < m \operatorname{ord} L$. Nevertheless, equality (3) holds for any $L, M \in \operatorname{Mat}_m(K[\partial])$ and an elementary proof is given in Section 3. Equality (3) is a generalization of the following fact that we proved in [2]: By differentiating one of the equations in a full rank system, one increases the dimension of the solution space by one.

In the general case $\operatorname{ord}(LM) \leqslant \operatorname{ord} L + \operatorname{ord} M$, and it may happen that $\operatorname{ord}(LM) < \operatorname{ord} L + \operatorname{ord} M$, due to the existence of zero divisors in the ring of matrices. It is even possible that $\operatorname{ord}(LM) = 0$ while both operators $L$ and $M$ are of positive order. This is the case for example when $L$ is an invertible in $\operatorname{Mat}_m(K[\partial])$ and $M$ is its inverse, i.e., $LM = ML = I_m$ where $I_m$ is the unit $m \times m$-matrix. Invertible operators are also called unimodular operators. It can be shown by different ways that an operator $L \in \operatorname{Mat}_m(K[\partial])$ is unimodular if and only if $\dim V_L = 0$.

In Section 4 we propose an algorithm to compute $\dim V_L$, as well as algorithms for recognizing unimodular operators and constructing their inverses.

These algorithms are based on the algorithm RR (Row-Reduction) by B.Beckermann, H.Cheng, and G.Labahn from [8, Thm. 2.2] (see also [6, Sect. 2.1]). The complexity measured as the number of field operations in $K$ in the worst case of each of those algorithms is the same as of algorithm RR, i.e.,

$$\Theta(m^{\omega+1} r^2), \tag{4}$$

where $r = \operatorname{ord} L$, and $2 < \omega \leqslant 3$ is the matrix multiplication exponent. To verify these new algorithms we suppose that the field $K$ is constructive and, in particular that there exists an algorithm for zero testing in $K$.

Section 5 is devoted to the difference case. First we give an elementary proof that for any difference field of characteristic 0 there exists a difference extension such that the needed statements on the dimension of solution spaces of first-order systems hold. (The proof of existence of the universal difference extension given in [15] is quite non-trivial). Then we prove the properties analogous to the ones established in the differential case. We define, prove the existence, and give an algorithm to construct a strongly row-reduced form of a full-rank difference operator. In comparison with the row-reduced form which was considered in [8], this new form has some additional useful properties. An algorithm to compute $\dim V_L$ for a full-rank difference operator $L$ as well as algorithms for recognizing unimodular operators and constructing their inverses are also described. (In [2, Appx.] only an incomplete sketch of an algorithm to compute $\dim V_L$ in the difference case was given.)

## 2 Preliminaries

The notation $M^T$ is used for the transpose of a matrix (vector) $M$. If $F$ is a differential field with derivation $\partial$ then $\operatorname{Const}(F) = \{c \in F \mid \partial c = 0\}$ is the *constant field* of $F$.

### 2.1 Differential Adequate Field Extension

Let $K$ be a differential field of characteristic 0 with derivation $\partial = '$.

**Definition 1** *An* adequate differential extension $\Lambda$ *of* $K$ *is a differential field extension* $\Lambda$ *of* $K$ *such that any differential system*

$$\partial y = Ay, \tag{5}$$

*with* $A \in \mathrm{Mat}_m(K)$ *has in* $\Lambda^m$ *a solution space of dimension* $n$ *over* $\mathrm{Const}\,(\Lambda)$.

If $\mathrm{Const}\,(K)$ is algebraically closed then there exists a unique (up to a differential isomorphism) adequate differential extension $\Lambda$ such that $\mathrm{Const}\,(\Lambda) = \mathrm{Const}\,(K)$ which is called the *universal differential field extension* of $K$ [16, Sect. 3.2]. For any differential field $K$ of characteristic 0 there exists a differential extension whose constant field is algebraically closed. Indeed, this is the algebraic closure $\bar{K}$ with the derivation obtained by extending the derivation of $K$ in the natural way. In this case $\mathrm{Const}\,(\bar{K}) = \overline{\mathrm{Const}\,(K)}$ (see [16, Exercises 1.5, 2:(c),(d)]). Existence of the universal differential extension for $\bar{K}$ implies that there exists an adequate differential extension for $K$, i.e., for an arbitrary differential field of characteristic zero.

In the sequel, we denote by $\Lambda$ a fixed adequate differential extension of $K$. Concerning the solution spaces of systems of the form (2), we suppose that the solutions are in $\Lambda^m$.

In addition of the first-order systems of the form (5), we also consider the differential systems of the form (2) of arbitrary order $r \geqslant 1$.

**Remark 1** *If* $A_r$ *is invertible in* $\mathrm{Mat}_m(K)$ *then system (2) is equivalent to the first-order system having* $mr$ *equations:*

$$\partial Y = AY, \tag{6}$$

*with*

$$A = \begin{pmatrix} 0 & I_m & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & I_m \\ \hat{A}_0 & \hat{A}_1 & \dots & \hat{A}_{r-1} \end{pmatrix}, \tag{7}$$

*where* $\hat{A}_k = -A_r^{-1}A_k$, $k = 0, 1, \dots, r-1$, *and*

$$Y = (y_1 \dots, y_m,\, y_{m+1}, \dots, y_{rm})^T \tag{8}$$

*with*

$$(y_1 \dots, y_m,\, y_{m+1}, \dots, y_{rm}) = \left(y_1 \dots, y_m,\, y_1' \dots, y_m', \dots,\, y_1^{(r-1)}, \dots, y_m^{(r-1)}\right).$$

*Therefore if the leading matrix of system (2) is invertible then the dimension of the solution space of this system is equal to* $mr$.

Operator (1) can be represented as a matrix in $\mathrm{Mat}_m(K[\partial])$:

$$\begin{pmatrix} L_{11} & \dots & L_{1m} \\ \dots & \dots & \dots \\ L_{m1} & \dots & L_{mm} \end{pmatrix}, \tag{9}$$

$L_{ij} \in K\,[\partial]$, $i, j = 1, \dots, m$, with $\max_{i,j} \mathrm{ord}\, L_{ij} = r$. We say that the operator $L \in \mathrm{Mat}_m(K\,[\partial])$ (as well as the system $L(y) = 0$) is of *full rank*, if the rows

$$\ell_i = (L_{i1}, \dots, L_{im}), \quad i = 1, \dots, m, \tag{10}$$

of matrix (9) are linearly independent over $K\,[\partial]$.

System (2) can be also written as a system of $m$ scalar linear equations

$$L_1(y_1, \dots, y_m) = 0, \quad \dots, \quad L_m(y_1, \dots, y_m) = 0, \tag{11}$$

with

$$L_i(y_1, \ldots, y_m) = \sum_{j=1}^{m} L_{ij}(y_j), \tag{12}$$

where $L_{ij}$, $i, j = 1, \ldots, m$, are as in (9).

The matrix $A_r$ is the leading matrix of both the system $L(y) = 0$ and operator $L$, regardless of the representation form.

### 2.2 Unimodular Factors and Algorithm RR

We use the notation

$$[M]_{i,*}\,, \;\; 1 \leqslant i \leqslant m,$$

for the $1 \times m$-matrix which is the $i$-th row of an $m \times m$-matrix $M$.

**Definition 2** *Let a full-rank operator $L \in \mathrm{Mat}_m(K[\partial])$ be of the form (1). If $1 \leqslant i \leqslant m$ then define $\alpha_i(L)$ as the maximal integer $k$, $0 \leqslant k \leqslant r$, such that $[A_k]_{i,*}$ is a nonzero row. The matrix $M \in \mathrm{Mat}_m(K)$ such that $[M]_{i,*} = [A_{\alpha_i(L)}]_{i,*}$, $i = 1, 2, \ldots, m$, is the* row frontal matrix *of $L$. The vector $(\alpha_1(L), \ldots, \alpha_m(L))$ is the* row-order *of $L$. (We will write simply $(\alpha_1, \ldots, \alpha_m)$, when it is clear which operator is considered.)*

**Definition 3** *An operator $U \in \mathrm{Mat}_m(K[\partial])$ is* unimodular *(or* invertible*) if there exists $\bar{U} \in \mathrm{Mat}_m(K[\partial])$ such that $\bar{U}U = U\bar{U} = I_m$. An operator in $\mathrm{Mat}_m(K[\partial])$ is* row-reduced *if its row frontal matrix is invertible.*

The following proposition is a consequence of [8, Thm. 2.2]:

**Proposition 1** *If $L \in \mathrm{Mat}_m(K[\partial])$ is of full rank then there exists a unimodular operator $U \in \mathrm{Mat}_m(K[\partial])$ such that the operator*

$$\breve{L} = UL \tag{13}$$

*is row-reduced and* $\operatorname{ord} \breve{L} \leqslant \operatorname{ord} L$.

Suppose that the field $K$ is *constructive*, i.e., there exist algorithms to execute the field operations and an algorithm for zero testing in $K$. In this case the proof of mentioned Theorem 2.2 from [8] gives an algorithm for constructing $U, \breve{L}$. This algorithm "...closely follows the one in [7, Eqn. (12)], for ordinary matrix polynomials, and is similar to that of [4] in case of skew polynomials" ([8, Rem. 2.3 ]). A detailed description of this algorithm is given in [6, Sect. 2.1]. We will refer to this algorithm as RR (Row-Reduction).

We describe briefly algorithm RR. Suppose that it is checked whether the rows of the row frontal matrix of $L$ are linearly dependent over $K$. If they are not then $U = I_m$, $\breve{L} = L$, and the algorithm stops. Otherwise, let coefficients

$$v_1, \ldots, v_m \in K \tag{14}$$

of the dependence be found. From the rows of (9) corresponding to nonzero coefficients, we select a row with the maximal component of the row-order. Let it be the $i$-th row, so $\alpha_i = \max_{\substack{1 \leqslant j \leqslant m \\ v_j \neq 0}} \alpha_j$. The row $\ell_i$ of (9) is replaced by

$$v_1 \partial^{\alpha_i - \alpha_1} \ell_1 + \cdots + v_{i-1} \partial^{\alpha_i - \alpha_{i-1}} \ell_{i-1} + v_i \ell_i + v_{i+1} \partial^{\alpha_i - \alpha_{i+1}} \ell_{i+1} + \cdots + v_m \partial^{\alpha_i - \alpha_m} \ell_m,$$

and $\alpha_i$ is decreased. This transformation of $L$ is equivalent to the left multiplication by a unimodular $W \in \mathrm{Mat}_m(K[\partial])$. Let the recursive application of RR to the operator $WL$ give $\tilde{U}$, $\tilde{L}$, then return $U = \tilde{U}W$, $\breve{L} = \tilde{L}$ and stop.

The recursion is correct due to decreasing of the sum of the row-order components. In[8, 6], it was shown that the complexity of RR measured as the number of the field operations in $K$ in the worst case is given by (4).

**Remark 2** *The full version of the algorithm from [8, 6] allows one to solve a more general problem: given an operator $L \in \mathrm{Mat}_m(K\,[\partial])$, to construct $U, \breve{L} \in \mathrm{Mat}_m(K\,[\partial])$ such that $U$ is unimodular while $\breve{L}$ represented in form (9) has $k$ zero rows, $0 \leqslant k \leqslant m$, and the row frontal matrix of $\breve{L}$ is of rank $m-k$ over $K$. An operator $L$ is of full rank if and only if $k = 0$.*

### 2.3 Differentiating an Equation of a Full Rank System

**Theorem 1** *([2]) Let a system of the form (11) be of full rank. Let the system*

$$L_1(y_1, \ldots, y_m) = 0, \;\; \ldots, \;\; L_{m-1}(y_1, \ldots, y_m) = 0, \;\; \tilde{L}_m(y_1, \ldots, y_m) = 0, \tag{15}$$

*be such that its first $m-1$ equations are as in system (11) while the $m$-th equation is the result of differentiating the $m$-th equation of (11), i.e., the equation $\tilde{L}_m(y_1, \ldots, y_m) = 0$ is equivalent to the equation $(L_m(y_1, \ldots, y_m))' = 0$. Then the dimension of the solution space of (15) exceeds that of (11) by 1.*

The following remark was also given in [2]:

**Remark 3** *Theorem 1 is valid for the case of a full-rank inhomogeneous system as well. That is a system of form $L(y) = b$, with $L \in \mathrm{Mat}_m(K\,[\partial])$ of full rank and $b \in K^m$. First of all note that this system has at least one solution in $\Lambda^m$ since by adding to $y$ a $(m+1)$-st component with value 1, one can transform the given system into a homogeneous system with a matrix belonging to $\mathrm{Mat}_{m+1}(K)$. The set of solutions in $\Lambda^m$ of $L(y) = b$ is an affine space over the $\mathrm{Const}\,(\Lambda)$ and is given by $V_L + f$ where $V_L \subset \Lambda^m$ is the solution space of the homogeneous system $L(y) = 0$ and $f \in \Lambda^m$ is a particular solution of $L(y) = b$. When we differentiate the $m$-th equation of the system $L(y) = b$ we get a new system $\tilde{L}(y) = \tilde{b}$ where the operator $\tilde{L}$ corresponds to system (15). By Theorem 1 $\dim V_{\tilde{L}} = \dim V_L + 1$.*

### 2.4 The Dimension of the Solution Space of a Given Full Rank System

The following theorem was derived in [2] as a consequence of Theorem 1:

**Theorem 2** ([2]) *Let $L \in \mathrm{Mat}_m(K\,[\partial])$ be row-reduced, and $\alpha = (\alpha_1, \ldots, \alpha_m)$ its row-order. Then $\dim V_L = \sum_{i=1}^{m} \alpha_i$.*

In Section 2.2 we discussed algorithm RR to convert a given full-rank operator $L$ into an operator $\breve{L}$ such that $V_L = V_{\breve{L}}$ and $\breve{L}$ is row-reduced. If the field $K$ is constructive then by Theorem 2 we are able to compute algorithmically the dimension of the solution space of a given full-rank system.

**Remark 4** *A unimodular $U$ and a row-reduced $\breve{L}$ in (13) are not in general unique. However, it follows from Theorem 2 that the sum of components of the row-order $(\alpha_1, \ldots, \alpha_m)$ is invariant for all possible $\breve{L}$.*

## 3 Products of Operators

**Theorem 3** *Let $L, M \in \mathrm{Mat}_m(K\,[\partial])$ be of full rank. Then $\dim V_{LM} = \dim V_L + \dim V_M$.*

Proof. Four auxiliary statements can be easily proved.

(A) *The product of two full-rank operators is again a full-rank operator.* (Indeed, let $u$ be a row-vector with coefficient from $K[\partial]$ and suppose that $uLM = 0$. Then necessarily $uL = 0$, because otherwise, $M$ would not be of full rank. As $L$ is of full-rank and $uL = 0$, we must have $u = 0$.)

(B) *Let $\Lambda$ be an adequate differential extension of $K$ and $\Omega$ be a differential field extension of $\Lambda$. Let a full-rank operator $P \in \mathrm{Mat}_m(K[\partial])$ and $z \in \Omega^m$ be such that $P(z) = 0$. Then $z \in \Lambda^m$.* (By Proposition 1 there exists an operator $U$ such that the row frontal matrix of $UP$ is invertible; then multiplying $UP$

from the left by an operator of the form $\mathrm{diag}(\partial^{l_1},\dots,\partial^{l_m})$ gives an operator $\tilde{P}$ with an invertible leading matrix. Since $\tilde{P}(z)=0$, we have $z\in\Lambda^m$.)

(C) *For a full-rank operator $P$ the value* $\dim V_P$ *is finite.* (Again, $P$ is a right factor of an operator $Q$ with invertible leading matrix. $Q$ can be converted into a first-order system of the form (5).)

(D) *Let $L,M\in\mathrm{Mat}_m(K[\partial])$ be of full rank, and $L(z)=0$ for some $z\in\Lambda^m$. Then the equation $M(y)=z$ has at least one solution belonging to $\Lambda^m$.* (By Remark 3, the equation $M(y)=z$ has a solution in $\Omega^m$ where $\Omega$ is an adequate extension of $\Lambda$. By (B), we have $y\in\Lambda^m$ since any such $y$ satisfies $LM(y)=0$.)

Now we can prove our theorem. The product $LM$ is of full rank too by (A). Hence, by (C), the $V_{LM}$ is of finite dimension over $\mathrm{Const}\,(\Lambda)$. Observe that $V_M$ is a subspace of $V_{LM}$ and let $W$ be any subspace of $V_{LM}$ such that $V_{LM}=V_M\oplus W$. We will prove that $W$ is isomorphic to $V_L$. Indeed, for each $w\in W$, $M(w)$ belongs to $V_L$ and if $M(w)=0$ then $w=0$ (since $W\cap V_M=\{0\}$). Hence the operator $M$ induces an injective $\mathrm{Const}\,(\Lambda)-$linear map $\varphi$ from $W$ into $V_L$. We will prove now that this map is also surjective: Given $z\in V_L$, the equation $M(y)=z$ has (at least) one solution $y\in\Lambda^m$ by (D). Now, such an element $y$ belongs to $V_{LM}$ so it can be written as $y=v+w$ where $v\in V_M$ and $w\in W$. One has $M(w)=M(y)=z$. This proves that $\varphi$ is surjective, and concludes the proof of our theorem. □

Note that different proofs of the latter theorem are possible. The proof presented above is elementary (it only uses basic techniques).

An adequate differential extension of $K$ is not in general unique, and we can consider $V_L,V_M,\dots$ only after fixing such an extension $\Lambda$. Those solution spaces are considered as subspaces of the space $\Lambda^m$ over $\mathrm{Const}\,(\Lambda)$. Theorems 2 and 3 hold for *any* adequate differential extension $\Lambda$ of $K$. In particular, the values $\dim V_L,\dim V_M,\dots$ do not depend on the choice of an adequate differential extension $\Lambda$ of $K$.

**Remark 5** *If we consider solutions whose components belong to an arbitrary differential extension then the statement of Theorem 3 is in general incorrect (as well as the statement of Theorem 1). Let $K=\mathbb{C}(x)$, $L=\partial=\frac{d}{dx}$, $M=\partial-\frac{1}{x}$, and $LM=\partial^2-\frac{1}{x}\partial+\frac{1}{x^2}$. If we consider only solutions belonging to $\mathbb{C}(x)$ or even to $\mathbb{C}((x))$ then the solution spaces of both $M$, $LM$ are one dimensional (they are spanned by $x$), but the solution space of $LM(y)=0$ is two dimensional if we consider solutions in the universal differential extension: in this case the solution space of $LM(y)=0$ is spanned by $x$, $x\ln x$.*

# 4 The inverse operator

Algorithms for recognizing invertibility of a matrix whose entries belong to a constructive field $K$, and for computing the inverse matrix are well known. In this section we describe analogous algorithms for matrices whose entries belong to $K[\partial]$.

## 4.1 Unimodularity of an Operator and the Dimension of its Solution Space

**Proposition 2** *Let $L$ be a full-rank operator belonging to* $\mathrm{Mat}_m(K[\partial])$, $\mathrm{ord}\,L=r$. *We have*

*(i) If the leading matrix of $L$ is invertible then* $\dim V_L=mr$ *otherwise* $\dim V_L<mr$.

*(ii) $L$ is unimodular if and only if* $\dim V_L=0$.

Proof. (i) Follows from Proposition 1 and Theorem 2.

(ii) Let $L^{-1}$ be the inverse of $L$. Then the equality $L(y)=0$ implies $y=0$. Therefore $\dim V_L=0$. If $\dim V_L=0$ then by Theorem 2 the representation $UL=\breve{L}$ described in Proposition 1 has to be such that the row-order of $\breve{L}$ is $(0,\dots,0)$. This implies that $\mathrm{ord}\,\breve{L}=0$, i.e. $\breve{L}$ is an invertible matrix in $\mathrm{Mat}_m(K)$. This gives $L^{-1}=(\breve{L})^{-1}U$. □

**Remark 6** *It follows that if an operator $L \in \mathrm{Mat}_m(K[\partial])$ has a left inverse $\bar{L}$ then $L$ is unimodular: $\bar{L}L = L\bar{L} = I_m$. Indeed, by Theorem 3*

$$\dim V_{L\bar{L}} = \dim V_L + \dim V_{\bar{L}} = \dim V_{\bar{L}L} = \dim V_{I_m} = 0,$$

*and the operator $L\bar{L}$ is unimodular by Proposition 2(ii). Thus there exists the inverse of this operator: $L\bar{L}(L\bar{L})^{-1} = I_m$. It follows that $\bar{L}(L\bar{L})^{-1}$ is a right inverse of $L$. Now we can use the standard proof of the fact that if an operator $L$ has both left and right inverses $L_l^{-1}$, $L_r^{-1}$ then these inverses are equal: $L_l^{-1} = L_l^{-1}LL_r^{-1} = L_r^{-1}$. The case when an operator $L$ has a right inverse can be similarly considered.*

### 4.2 Recognizing Invertibility of an Operator and Computing the Inverse Operator

**Proposition 3** *Let $L \in \mathrm{Mat}_m(K[\partial])$ have an invertible row frontal matrix. Then $L$ is unimodular if and only if* $\operatorname{ord} L = 0$.

Proof. By Theorem 2 and Proposition 2(ii). □

Algorithm RR allows one to compute a unimodular $U \in \mathrm{Mat}_m(K[\partial])$ such that the operator $\breve{L} = UL$ has an invertible row frontal matrix. Proposition 3 implies that $L$ is unimodular if and only if $\breve{L}$ is an invertible matrix in $\mathrm{Mat}_m(K)$. In this case $(\breve{L})^{-1}UL = I_m$, i.e., $(\breve{L})^{-1}U$ is the inverse of $L$. Hence the following theorem holds (taking into account Remark 2, we need not assume that $L$ is of full rank):

**Theorem 4** *Let $K$ be constructive and $L \in \mathrm{Mat}_m(K[\partial])$. One can recognize algorithmically whether $L$ is unimodular or not, and compute the inverse operator if it is.*

The algorithm is as follows:

*By algorithm* RR*, compute a unimodular $U$ such that the operator $\breve{L} = UL$ represented in the form (9) has $k$ zero rows, $0 \leqslant k \leqslant m$, and the row frontal matrix of $\breve{L}$ is of rank $m-k$ over $K$. The operator $L$ is of full rank if and only if $k = 0$, and is unimodular if and only if $\breve{L}$ is an invertible matrix in* $\mathrm{Mat}_m(K)$. *In the latter case $(\breve{L})^{-1}U$ is the inverse for $L$.*

### 4.3 Complexity comparison

There exists a number of algorithms for solving quite general problems and which can be used in particular for solving the problem considered in Section 4.2. The algorithm proposed in Section 4.2 serves especially to solve the problem of recognizing unimodularity of an operator $L$ and computing the inverse operator, if $L$ is unimodular. Its complexity (the number of operations in $K$ in the worst case) to the best of our knowledge is lower than the complexity of other algorithms when used to solve the formulated problem.

For example, for solving the problem considered in Section 4.2, algorithms to construct the Jacobson and Hermite forms of a given operator can be used. Recall that for a full-rank operator $L \in \mathrm{Mat}_m(K[\partial])$ there exist unimodular $S, T \in \mathrm{Mat}_m(K[\partial])$ such that $SLT = \mathrm{diag}(1, \ldots, 1, p)$, where $p$ is a monic (the leading coefficient of $p$ is equal to 1) scalar operator from $K[\partial] \setminus \{0\}$. In this case $\mathrm{diag}(1, \ldots, 1, p)$ is the *Jacobson form* of $L$ ([9, Chap. 8, Thm. 1.1]). It is clear that if as before $V_L$ is the space of solutions of $L$ in an adequate differential extension $\Lambda$ of $K$ then $\dim V_L = \operatorname{ord} p$, and $L$ is unimodular if and only if $p = 1$ (thus we get again that $L$ is unimodular if and only if $\dim V_L = 0$). Therefore using an algorithm for constructing the Jacobson form we can at least check the unimodularity of an operator. The Jacobson form of $L$ can be constructed by numerous algorithms. A polynomial-time deterministic algorithm was proposed by J.Middeke ([14]). Its complexity is considered in [14] as a function of three variables, and two of them are our $m, r$ (in [14] another notation is used). The value of the third variable is in the worst case $mr$, and for the complexity as a function of the variables $m, r$ one can derive the estimate $\Theta(m^9 r^9)$ from the asymptotic estimate given in [14, Sect. 6]. On the other hand, the algorithms proposed in Section 4.2 have the same complexity as the algorithm RR, i.e., $\Theta(m^{\omega+1} r^2)$.

A full-rank operator can be represented also in the Hermite normal form (the definition can be found, e.g., in [12, Sect. 1]): $H = UL$, where $U$ is unimodular. The Hermite form of a unimodular matrix is the identity, the transformation matrix $U$ is the inverse. The algorithm of M.Giesbreht and M.Kim in [12] works for both differential and difference cases. The complexity estimate for this algorithm given in [12, Thm. 5.5] is $O(m^7 r^3 \log(mr))$ (in our notation). It looks like this estimate is exact. So, again, the complexity $\Theta(m^{\omega+1} r^2)$ looks better.

Of course, the algorithms from [14, 12] solve more general problems, and our algorithms have some advantages only for recognizing invertibility of an operator and computing the inverse operator.

**Remark 7** *In [11], M.Giesbrecht and A.Heinle proposed a Las Vegas type algorithm for the Jacobson form which is polynomial-time in the degree of the entries as well as in the coefficient size (degree and bit-length), if the coefficients are rational functions of $x$. The algorithm in [13] by V.Levandovskyy and K.Schindelar is useful for practical Jacobson form computation, even though it is not polynomial-time.*

### 4.4 An Additional Trick

Searching for coefficients (14) of a linear dependence is equivalent to solving a homogeneous system of linear algebraic equations with coefficients in $K$. If we obtain $s$ linearly independent solutions of the linear algebraic system then it is possible to use all of them, which gives an decreasing of the sum of the row-order components at least by $s$. To do that, we first represent the $s$ dependencies as rows of an $s \times m$ matrix $V$, and use the first row of $V$ to decrease an $\alpha_i$, $1 \leqslant i \leqslant m$. We then transform $V$ by eliminating the $i$-th element in its rows having the numbers $2, 3, \ldots, s$, using the $i$-th element of the first row as pivot. After this elimination, each remaining row of $V$ contains the coefficients of a linear dependence of the rows $1, \ldots, i-1, i+1, \ldots, m$ of the frontal row matrix. So we may perform $s$ similar steps. This is a modification of the trick proposed originally in [4] for the EG-eliminations algorithm ([1]). The trick does not decrease complexity but can be useful to practice.

## 5 The Difference Case

### 5.1 Difference Rings and Fields; Adequate Difference Extensions

A *difference ring* is a commutative ring $K$ with multiplicative identity, together with an automorphism $\sigma$. The *constant ring* of $K$ is then $\mathrm{Const}\,(K) = \{c \in K \mid \sigma c = c\}$. If, in addition, $K$ is a field then $K$ is a *difference field*. In this case $\mathrm{Const}\,(K)$ is a subfield of $K$ (the *constant field* of $K$).

Let $K$ be a difference field of characteristic 0 with an automorphism $\sigma$, and $\Lambda$ be a difference ring extension of $K$. Then the ring $\Lambda$ is an *adequate difference extension* if $\mathrm{Const}\,(\Lambda)$ is a field and the dimension of the solution space over $\mathrm{Const}\,(\Lambda)$ (considered as a subspace of $\Lambda^m$) of an arbitrary system

$$\sigma y = Ay, \tag{16}$$

with an invertible $A \in \mathrm{Mat}_m(K)$, is equal to $m$. Note that in the differential case the invertibility of $A$ in (5) is not needed; this peculiarity of the difference case requires some additional efforts. We will discuss this in the two following sections.

If $\mathrm{Const}\,(K)$ is algebraically closed then there exists a unique (up to a difference isomorphism) adequate extension $\Lambda$ such that $\mathrm{Const}\,(\Lambda) = \mathrm{Const}\,(K)$ which is called the *universal difference Picard-Vessiot ring extension* of $K$ (see [15, Sect. 1.4]). In the general case, an adequate difference extension can be easily constructed, e.g., as described in the following proposition (the equality $\mathrm{Const}\,(\Lambda) = \mathrm{Const}\,(K)$ is not guaranteed any longer).

**Proposition 4** *Let $K$ with an automorphism $\sigma$ be a difference field of characteristic 0. Then there exists an adequate difference ring extension of $K$.*

PROOF. Let $G$ be the ring of double-sided sequences whose elements belong to $K$, with componentwise addition and multiplication. Let $\tau$ be the automorphism of this ring defined by $\tau\left((a_i)_{-\infty<i<\infty}\right) = (b_i)_{-\infty<i<\infty}$ with $b_i = a_{i+1}$, $i \in \mathbb{Z}$. Then $G$ together with $\tau$ is a difference ring, and $g \in \mathrm{Const}\,(G)$ if and only if $g = (\dots, f, f, f, \dots)$, $f \in K$. Define the monomorphism $\varphi : K \to G$ by $\varphi a = (\sigma^i a)_{-\infty<i<\infty}$ for an arbitrary $a \in K$. Define additionally an automorphism $\tilde{\sigma}$ of $\mathrm{Im}(\varphi)$ as follows: if $g = \varphi a$ then $\tilde{\sigma} g = \varphi \sigma a$. One can see that $\tau$ and $\tilde{\sigma}$ coincide on $\mathrm{Im}(\varphi)$. Since $K$ with $\sigma$ and $\mathrm{Im}(\varphi)$ with $\tilde{\sigma}$ are isomorphic as difference fields, we can consider $G$ with $\tau$ as a difference ring extension of $K$ with $\sigma$. We can set $\Lambda = G$ and write $\sigma$ for $\tau$.

Set $e_j = (\underbrace{0, \dots, 0}_{j-1}, 1, \underbrace{0, \dots, 0}_{n-j})^T$, $j = 1, \dots, n$, and define sequences $s_1, \dots, s_n$ whose components belong to $K^n$, by $s_j = (f_{ji})_{-\infty<i<\infty}$, where

$$f_{ji} = \begin{cases} (\sigma^{i-1}A)(\sigma^{i-2}A)\dots Ae_j & \text{if } i \geqslant 0, \\ (\sigma^{-i}A^{-1})(\sigma^{-i+1}A^{-1})\dots(\sigma^{-1}A^{-1})e_j & \text{if } i < 0, \end{cases}$$

$j = 1 \dots, n$, $i = 0, \pm 1, \pm 2, \dots$ Then $\varphi s_1, \dots, \varphi s_n$ form a basis for the solution space of system (16) over the field $\mathrm{Const}\,(\Lambda)$. □

**Remark 8** *The latter proposition shows that an adequate difference ring extension exists for any difference field $K$ of characteristic zero. The claim is not true for difference field (rather than ring) extensions: a well-known example due to Franke ([10]) is the scalar equation $\sigma y = -y$ which has no non-zero solution if* $\mathrm{Const}\,(K)$ *is algebraically closed.*

In the sequel we denote by $\Lambda$ a fixed adequate difference ring extension of $K$. We set also $\Delta = \sigma - 1$.

### 5.2 Strongly Row Reduced Form of a Full Rank Difference Operator

A difference operator can be considered as a matrix in $\mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$. An operator is of full rank if the rows of the corresponding matrix are linearly independent over $K[\sigma, \sigma^{-1}]$. Let $L \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ then $L$ can be expanded as

$$L = A_l\sigma^l + A_{l-1}\sigma^{l-1} + \dots + A_t\sigma^t, \tag{17}$$

where $A_t, A_{t+1}, \dots, A_l \in \mathrm{Mat}_m(K)$, and matrices $A_l, A_t$ (the leading and *trailing* matrices of the system) are non-zero. We set $\deg L = l$, $\mathrm{val}\, L = t$ and $\mathrm{ord}\, L = \deg L - \mathrm{val}\, L$.

We define the row-order $(\alpha_1, \dots, \alpha_m)$ of (17) similarly to the differential case: if $1 \leqslant i \leqslant m$ then $\alpha_i$ is the maximal integer $k$, $t \leqslant k \leqslant l$, such that $[A_k]_{i,*}$ is a nonzero row.

By definition, the row frontal matrix of $L$ is the leading matrix of $PL$ where

$$P = \mathrm{diag}(\sigma^{l-\alpha_1}, \sigma^{l-\alpha_2}, \dots, \sigma^{l-\alpha_m}).$$

**Definition 4** *An operator $L$ in $Mat_m(K\left[\sigma, \sigma^{-1}\right])$ is* strongly row-reduced *if its row frontal and trailing matrices are both invertible.*

**Proposition 5** *Let $L \in \mathrm{Mat}_m(K\left[\sigma, \sigma^{-1}\right])$ be of full rank, then there exists a unimodular operator $U$ such that the operator*

$$\breve{L} = UL \tag{18}$$

*is strongly row-reduced and $\mathrm{ord}\,\breve{L} \leqslant \mathrm{ord}\, L$ (such an operator $\breve{L}$ is a* strongly row-reduced *form of the original operator $L$).*

PROOF. It has been proved (see [1, 4]) that for any full-rank operator $L$ of form (17) there exists a unimodular operator $G \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ such that the product $GL$ is an operator which has an invertible trailing matrix, $\operatorname{ord} GL \leqslant \operatorname{ord} L$. We can apply the difference version (replacing $\partial$ by $\Delta$) of algorithm RR to $GL$. This gives an operator $\breve{L}$ with invertible row frontal matrix. Each step of the considered version of algorithm RR does not change the rank of the trailing matrix. The claim follows. □

**Remark 9** *The original difference version of the algorithm RR proposed in [8] does not guarantee the invertibility of the trailing matrix of* $\breve{L}$. *Note that a strongly reduced row form can be also defined for an operator of arbitrary rank: the operator as an element of* $\mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ *has* $k$ *zero rows, the row frontal and trailing matrices are of rank* $m-k$. *(It follows also from [1, 4] that in the general case for any operator* $L$ *of form (17) there exists a unimodular operator* $G \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ *such that the product* $GL$ *has* $k$ *zero rows, and its trailing matrix is of rank* $m-k$. *We can apply the mentioned difference version of* RR *to* $GL$.*)*

By definition, if $L$ is of full rank then the system $L(y) = 0$ is of full rank too, and the order of the system $L(y) = 0$ coincides with $\operatorname{ord} L$. Consider a system of order $r \geqslant 1$ which has the form $L(y) = 0$ with $L$ as in (17). If $A_l, A_t$ are invertible then the system $L(y) = 0$ is equivalent to the first-order system having $mr$ equations: $\sigma Y = AY$, where $A$ is as in (7) with $\hat{A}_k = -A_l^{-1} A_{k+t}$, $k = 0, 1, \ldots, r-1$. The matrix $A$ is invertible since $\det A = -\det \hat{A}_0 = \det A_l^{-1} \det A_t \neq 0$. Let $V_L$ be the set of the solutions of $L(y) = 0$ belonging to $\Lambda^m$. We consider this set as a linear space over the field $\mathrm{Const}\,(\Lambda)$. It follows that if both the leading and trailing matrices of $L \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ are invertible and $\operatorname{ord} L = r$ then $\dim V_L = rm$.

The proof of Theorem 3 given in Section 3 is valid for the difference case after replacing derivation $\partial$ by an automorphism $\sigma$. (In part (B) of the proof we can consider $U$ such that $UP$ is strongly row-reduced, then multiplying $UP$ from the left by an operator of form $\operatorname{diag}(\Delta^{l_1}, \ldots, \Delta^{l_m})$ gives an operator $\tilde{P}$ with invertible leading and trailing matrices.) Thus we have the following theorem:

**Theorem 5** *Let* $L, M \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ *be of full rank. Then* $\dim V_{LM} = \dim V_L + \dim V_M$.

### 5.3 The Dimension of the Solution Space of a Full Rank Difference System

**Theorem 6** *Let a full-rank operator* $L \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ *be strongly row-reduced, and* $\alpha = (\alpha_1, \ldots, \alpha_m)$ *be the row-order of* $L$, $t = \operatorname{val} L$. *Then* $\dim V_L = \sum_{i=1}^m \alpha_i - mt$.

PROOF. Let $l = \deg L$, $r = \operatorname{ord} L = l - t$. If we left multiply $L$ by

$$\operatorname{diag}(\Delta^{l-\alpha_1}, \Delta^{l-\alpha_2}, \ldots, \Delta^{l-\alpha_m}),$$

then we increase by Theorem 5 the dimension of the solution space by $ml - \sum_{i=1}^m \alpha_i(L)$, and the resulting full-rank operator has a leading matrix which coincides with the row frontal matrix of $L$, and a trailing matrix which coincides with the trailing matrix of $L$. The dimension of the solution space of the obtained operator is $mr = ml - mt$ by the last paragraph of Section 5.2. □

We can similarly prove that for any full-rank operator $L \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$, there exists an operator $R$ such that $RL$ has invertible both the leading and trailing matrices, and $\operatorname{ord} RL \leqslant \operatorname{ord} L$. Note that earlier it was known only that one can construct an operator $R$ such that $RL$ has invertible leading and trailing matrices, with $\operatorname{ord} RL = \operatorname{ord} L + 1$ in the general case (see, e.g., [5, Sect. 3.5]).

Theorem 6 and the difference version of algorithm RR (as that version was explained in the proof of Proposition 5) give an algorithm to compute $\dim V_L$ for any full-rank operator $L$.

**Remark 10** *A unimodular* $U$ *and a strongly row-reduced* $\breve{L}$ *in (18) are not in general uniquely defined. However, it follows from Theorem 6 that the sum of components of the row-order* $(\alpha_1, \ldots, \alpha_m)$ *is invariant for all possible* $\breve{L}$.

If $K$ is constructive, and $L \in \mathrm{Mat}_m(K[\sigma, \sigma^{-1}])$ then one can recognize algorithmically whether $L$ is unimodular or not, and compute the inverse operator if it is. The algorithm is the same as that given in Section 4.1 for the differential case. The complexity measured as the number of the field operations in $K$ in the worst case of this computation is equal to $\Theta(m^{\omega+1}r^2)$, where $\omega$ is the matrix multiplication exponent.

## Acknowledgments

The authors are thankful to M. Petkovšek and D. Trushin for useful discussions.

## References

[1] S.A. Abramov. EG–eliminations. *J. of Difference Equations and Applications*, 5(4-5): 393–433, 1999.

[2] S.A. Abramov, M.A. Barkatou. On the dimension of solution spaces of full-rank linear differential systems. *CASC 2013, LNCS 8136*, Springer, Heidelberg, 1–9, 2013.

[3] S.A. Abramov, M.A. Barkatou, D.E. Khmelnov. On full-rank differential systems with power series coefficients. *J. of Symbolic Computation*, accepted.

[4] S.A. Abramov, M. Bronstein. On solutions of linear functional systems. *Proc. ISSAC'2001*: 1–6, 2001.

[5] S.A. Abramov, D.E. Khmelnov. Linear differential and difference Systems: $\mathrm{EG}_\delta$- and $\mathrm{EG}_\sigma$-eliminations. *Programming and Computer Software*, 39(2): 91–109, 2013. Translated from from *Programmirovanie*, 39(2) (in Russian), 2013.

[6] M.A. Barkatou, C. El Bacha, G. Labahn, E. Pflügel. On simultaneously row and column reduction of higher-order linear differential systems. *J. of Symbolic Comput.*, 49(1): 45–64, 2013.

[7] B. Beckermann, G. Labahn. Recursiveness in matrix rational interpolation problems. *J. of Computational and Applied Mathematics*, 77: 5–34, 1997.

[8] B. Beckermann, H. Cheng, G. Labahn. Fraction-free row reduction of matrices of Ore polymomials. *J. of Symbolic Comput.*, 41(5): 513–543, 2006.

[9] P.M. Cohn. Free Rings and their Relations. Academic Press, London & New York, 1971.

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

[11] M. Giesbrecht, A. Heinle. A Polynomial-Time Algorithm for the Jacobson Form of a Matrix of Ore Polynomials. *CASC 2012, LNCS 7442*. Springer, Heidelberg: 117–128, 2012.

[12] M. Giesbrecht, M. Sub Kim. Computation of the Hermite form of a Matrix of Ore Polynomials. *J. of Algebra*. 376: 341–362, 2013.

[13] V. Levandovskyy, K. Schindelar. Computing diagonal form and Jacobson normal form of a matrix using Grobner bases. *J. of Symbolic Computation*, 46(5): 595–608, 2011.

[14] J. Middeke. A Polynomial-Time Algorithm for the Jacobson Form for Matrices of Differential Operators. *Tech. Report No. 08-13 in RISC Report Series*, 2008.

[15] M. van der Put, M.F. Singer. Galois Theory of Difference Equations. *Lectures Notes in Mathematics 1666*, Springer-Verlag, Berlin Heidelberg, 1997.

[16] M. van der Put, M.F. Singer. Galois Theory of Linear Differential Equations. *Grundlehren der mathematischen Wissenschaften, 328*, Springer, Heidelberg, 2003.