NC solving of a system of linear ordinary differential equations in several unknowns

D. Grigoriev

An NC algorithm is described for reducing a system of linear ordinary differential equations in several unknowns to the standard basis form

Introduction

We consider a problem of solvability of a system of linear ordinary differential equations in several unknowns

$$\sum_j L_{ij} u_j = b_i$$

where $b_i \in \mathbb{Q}(X)$ and $L_{ij} = \sum_k f_k \frac{d^k}{dx^k}$ are linear ordinary differential operators with the rational coefficients $f_k \in \mathbb{Q}(X)$. We consider a solvability of the system in the unknowns u_j in the differential closure of $\mathbb{C}(X)$ (in fact, as we deal with the linear operators it is equivalent to the solvability in Picard-Vessiot closure of $\mathbb{C}(X)$) (see [K]), in which any (resp. linear) ordinary differential equation has a solution. In other words, solvability in Picard-Vessiot closure means that the system cannot be brought to a contradiction by equivalent transformations over the ring $\mathcal{R} = \mathbb{C}(X)\left[\frac{d}{dX}\right]$ of the linear differential operators, or more precisely, that the ideal in the ring of differential polynomials in $\{u_j\}$, generated by the differential polynomials $\{\sum_j L_{ij} u_j - b_i\}$, differs from the unit one.

Remark that this problem is a particular case of the problem of solvability (over differential closure) of a system of non-linear ordinary differential equations in several unknowns (more general, a quantifier elimination problem for these systems), for which an algorithm with elementary complexity (more precisely, double-exponential) was designed in [G87]. In the present paper we deal with a linear fragment of this general problem and describe for it an algorithm with a considerably better (than for the general problem) complexity, namely from the complexity class NC, i.e. with polynomial time and polylog depth (parallel time), moreover the algorithm produces a "triangular" basis for the space of solutions of the system.

A close problem to the one under consideration is solving linear system over the ring $\mathcal{R}$ of differential operators for which an algorithm was designed in [G91] (even for the case of the differential operators with the coefficients in many variables from $\mathbb{Q}(X_1, \cdots, X_n)$). The problem considered in the present paper is more subtle from the point of view of the allowed transformations of a system since for the sake of equivalence we may not multiply the equations of the system by the differential operators, as we could do in the case of the linear systems over $\mathcal{R}$ (see [G91]).

Therefore, we need to carry out elementary transformations with the matrix over $\mathcal{R}$ of the system (see section 1 below), in order to reduce the matrix to a standard basis form which is a particular case of a differential standard basis [G], [O], [C] for partial differential operators. Since the ring $\mathcal{R}$ is non-commutative (some of its properties one can find in e.g. [B]), the difficulties arise in estimating the standard basis form of the matrix over $\mathcal{R}$ unlike the case of the matrices over the (euclidean) rings of integers or univariate polynomials, because for the latter one exploits the notion of the determinant. But still we are able (see lemma 4) to bound the size of a quasiinverse of a matrix over $\mathcal{R}$ (for an inversible matrix a similar bound follows from the bound in [O] obtained for a more general situation of nonlinear operators) and define the rank of a matrix over $\mathcal{R}$ (see [J], also Lemma 5 below). To replace the notion of the determinant we consider (see section 2 below) the order [R] of a system of linear differential operators, i.e. of a matrix over $\mathcal{R}$, being the dimension over $\mathbb{C}(X)$ of the factor of the free $\mathcal{R}$-module over the submodule generated by the rows of the matrix. We prove that the order is additive with respect to the product of the square matrices (Lemmas 6, 7). Relying on Lemma 7, on the analogue of Bezout's theorem for differential equations [R], [Ko] (see also Lemma 9 below) and on a bound on a quasiinverse (see Lemma 4 in section 1), we estimate in section 3 the size of the standard basis form of the matrix (see Lemma 10) using the construction of a minimal element in a module with respect to a non-archemedian form (the order). In the last section 4 we give an algorithm from NC for constructing the standard basis form of a matrix, applying the bounds achieved in section 3. This provides a desired algorithm from NC for testing solvability of a system of linear ordinary differential equations and producing a "triangular" basis for the space of solutions of a system (see the theorem at the end of the paper).

Let us underline that the main purpose of this paper is to describe an algorithm with the low complexity (NC) for an important problem in symbolic computations in systems of linear differential equations. The needed auxiliary bounds from sections 1,2 (unfortunately, nowhere written explicitely) could be obtained without difficulties by the experts in differential algebra and they are included to make the paper self-contained.

Mention also that the problem of solving a single linear ordinary differential equation in one unknown leads to the problem of factoring of the equation, for the latter problem an algorithm was proposed in [G88]. A slight generalization of this problem is solving a first-order system of linear ordinary differential equations, an algorithm for reducing a matrix of this system to the block-triangular form was exhibited in [G90]. A connection of the first-order linear systems with the general linear systems considered in the present paper, is discussed in section 4 below.

1. Transformations and the rank of matrices over the ring of linear differential operators.

Denote by $D = \frac{d}{dX}$, $\mathcal{R} = \mathbb{C}(X)[D]$, and by $\mathcal{F}$ a Picard-Vessiot closure (see [K]), i.e. any linear differential equation $L = \left(\sum_{0 \le i \le n} f_i D^i\right) u = 0$ with the coefficients $f_i \in \mathcal{F}$ and the leading coefficient $\ell c(L) = f_n \neq 0$ has n linearly independent over $\mathbb{C}$ solutions in $\mathcal{F}$, and furthermore, a subfield of constants of $\mathcal{F}$ (i.e. the elements $c \in \mathcal{F}$ such that $Dc = 0$) coincides with $\mathbb{C}$.

We consider a problem of solvability in $\mathcal{F}$ of a system of linear ordinary differential equations in several unknowns

$$\sum_{1\leq j\leq s} L_{ij}u_j = b_i, \quad 1\leq i\leq k \tag{1}$$

where $L_{ij}\in \mathbb{Q}(X)[D]$, $b_i\in\mathbb{Q}(X)$ and the solutions $u_1,\cdots,u_s$ should be in $\mathcal{F}^s$. For an operator $L=\sum_{0\leq i\leq n} f_iD^i\in\mathcal{R}$ with $\ell c(L)=f_n\neq 0$ denote $n=\text{ord } L$ and by $\deg L$ denote $\sum_{0\leq i\leq n}\deg_X f_i$. Consider $k\times s$ matrix $\mathcal{L}=(L_{ij})$, assume that ord $\mathcal{L}\leq r$, $\deg\mathcal{L}\leq d$, $\deg(b_i)\leq d$, i.e. ord $L_{ij}\leq r$, $\deg L_{ij}\leq d$ for all i,j. Assume also that the bit-size of each (rational) coefficient of L_{ij}, b_i does not exceed M.

Consider now $k\times s$ matrix $A=(A_{ij})$ with the entries $A_{ij}\in\mathcal{R}$, assume that ord $(A_{ij})\leq r$. As the ring $\mathcal{R}$ is left-euclidean, making elementary transformations over $\mathcal{R}$ with the rows, one can reduce A to the following standard basis form, see [J] (it is a particular case of a characteristic set [R] which is considered in [R] in nonlinear case, or of a differential standard basis [C], [G], [O])

$$Q=\begin{pmatrix} 0 & \dots & 0Q_{1p_1} & & & & & \\ 0 & \dots & \dots & 0Q_{2p_2} & & & & \\ 0 & \dots & \dots & \dots & 0Q_{3p_3} & * & & \\ \vdots & & & & & \ddots & & \\ 0 & \dots & \dots & \dots & \dots & \dots & 0Q_{\ell,p_\ell} & \dots \\ & & & \bigcirc & & & \bigcirc & \end{pmatrix} \tag{2}$$

where $p_1<p_2<\cdots<p_\ell$, all the rows starting with $(\ell+1)$-th vanish . Let us admit also as an elementary transformation the multiplication (from the left) of a row by a nonzero element from $\mathbb{C}(X)$. In other words, there is $k\times k$ matrix $B=(B_{ij})$ over $\mathcal{R}$ being a product of elementary matrices such that $BA=Q$. The rows of Q provide a triangular basis of a left $\mathcal{R}$-module $\mathcal{R}^kA\subset\mathcal{R}^s$ generated by the rows of the matrix A.

The next lemma and the corollary one can deduce from the results in [J].

LEMMA 1. *A square $k\times k$ matrix A over $\mathcal{R}$ is inversible from the left if and only if A equals to a product of elementary matrices.*

COROLLARY. *A square matrix is inversible from the left if and only if it is inversible from the right. The left inverse is unique and coincides with the right inverse. Thus, one could talk simply about inversible matrices.*

We say that $k \times s$ matrix A is quasiinversible from the left if there exists $s \times k$ matrix G over $\mathcal{R}$ such that $GA = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$ is a diagonal matrix with nonzero diagonal elements $C_1, \dots, C_s$ (in a similar way one could define quasiinversibility from the right).

LEMMA 2. *A is quasiinversible from the left iff the dimension $\dim_{\mathbb{C}(X)}(\mathcal{R}^s/\mathcal{R}^k A) < \infty$ of the factor-module is finite.*

Proof. If $GA = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$ and $\operatorname{ord} C_1 = r_1, \dots, \operatorname{ord} C_s = r_s$ then the vectors $\Pi(e_i^{(j)}) = \Pi(\underbrace{0, \cdots, 0, D^j}_{i}, 0, \cdots, 0) \in \mathcal{R}^s/\mathcal{R}^k A$ for $1 \le i \le s,\ 0 \le j < r_i$ constitute a generating set over $\mathbb{C}(X)$ of $\mathcal{R}$-module $\mathcal{R}^s/\mathcal{R}^k A$, where $\Pi : \mathcal{R}^s \to \mathcal{R}^s/\mathcal{R}^k A$, is the natural projection, hence $\dim_{\mathbb{C}(X)}(\mathcal{R}^s/\mathcal{R}^k A) \le r_1 + \dots + r_s$ (a better inequality see below in Lemmas 9, 10).

Let $\dim_{\mathbb{C}(X)}(\mathcal{R}^s/\mathcal{R}^k A) < \infty$. Then one can reduce A by elementary transformations of the rows to standard basis form (2) and if $\ell < s$ then the infinite family of vectors $\Pi(e_p^{(0)}),\ \Pi(e_p^{(1)}), \dots,$ where $1 \le p \le s$ is distinct from $p_1, \dots, p_\ell$, are independent over $\mathbb{C}(X)$ and we get a contradiction. Therefore, $\ell = s$. One can show that there exists $s \times k$ matrix G over $\mathcal{R}$ such that $GQ = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$ with nonzero $C_1, \dots, C_s$. Indeed, multiply the first row of Q by a suitable element $0 \ne \alpha_1 \in \mathcal{R}$ such that $\alpha_1 Q_{12} = \beta_1 Q_{22}$ for a certain $\beta_1 \in \mathcal{R}$ (this is possible since $\mathcal{R}$ is an Ore domain [B]), then subtract from the first row the second one multiplied by β_1, thereby we'll achieve vanishing the entry with the coordinates (1, 2). Continuing in a similar way, we'll make all the entries in the first row (except the diagonal entry) to be zeroes. Then we proceed to the second row and so on. As a result we'll get a diagonal matrix which shows that A is quasiinversible from the left.

Observe that when $\dim_{\mathbb{C}(X)}(\mathcal{R}^s/\mathcal{R}^k A) < \infty$, the latter dimension coincides with the order of the system $Au = 0$ [R]. In [R] the order was introduced for a prime ideal in the ring of differential polynomials, we use it for a linear ideal generated by the rows of A.

The next lemma was actually proved in [G91].

LEMMA 3. *A is quasiinversible from the left iff there does not exist a vector $0 \neq v \in \mathcal{R}^s$ such that $Av = 0$. For $(s-1) \times s$ matrix A one can select $0 \neq v \in \mathcal{R}^s$ such that $Av = O$ and ord $(v) \leq (s-1)r + 1$.*

Proof. If A is quasiinversible from the left and $GA = \begin{pmatrix} C_1 & & O \\ & \ddots & \\ O & & C_s \end{pmatrix}$ then $Av \neq 0$ for any $0 \neq v \in \mathcal{R}^s$ as $\mathcal{R}$ has no divisors of zero ([B]).

Conversely, let $Av \neq 0$ for any $0 \neq v \in \mathcal{R}^s$. Let us show that in the standard basis form (2) $\ell = s$. Suppose $\ell < s$. Consider the $\mathbb{C}(X)$-space $\mathcal{R}^{s;N}$ of the vectors $(\alpha_1, \ldots, \alpha_s) \in \mathcal{R}^s$ for which ord $(\alpha_1), \ldots,$ ord $(\alpha_s) < N$. Let ord $(Q_{ij}) \leq R$ for all i, j. Then the composition of the mapping $Q : v \to Qv$ with the restriction onto first ℓ coordinates (notice that others are zeroes, see (2)) maps $\bar{Q} : \mathcal{R}^{s;N} \to \mathcal{R}^{\ell;N+R}$. As $\dim_{\mathbb{C}(X)} \mathcal{R}^{s;N} = s\,N$, for $N = \left[\frac{\ell R}{s-\ell}\right] + 1$ we get that $\dim_{\mathbb{C}(X)} \mathcal{R}^{s;N} > \dim_{\mathbb{C}(X)} \mathcal{R}^{\ell;N+R}$ and therefore, there exists a vector $0 \neq v \in \mathcal{R}^{s;N}$ such that $Qv = 0$, hence $BAv = 0$ and thus $Av = 0$ since B is a product of elementary matrices (cf. Lemma 1). The obtained contradiction with the supposition justifies the equality $\ell = s$. Then one can show that A is quasiinversible from the left. This proves the first statement of the lemma. For the second statement follow the latter proof considering instead of $\bar{Q}$ the mapping $\bar{A} : \mathcal{R}^{s;M} \to \mathcal{R}^{s-1;M+\mathrm{ord}\,(A)}$ for $M = (s-1)\mathrm{ord}\ A + 1$.

The next lemma was proved in [G91].

LEMMA 4. *A square $s \times s$ matrix A is quasiinversible from the left iff A is quaisiinversible from the right. In this case there exists G for which $GA = \begin{pmatrix} C_1 & & O \\ & \ddots & \\ O & & C_s \end{pmatrix}$ with ord $(G) \leq (s-1)r + 1$.*

Proof. Let A be quasiinversible from the left. Then for an appropriate matrix B, being a product of elementary matrices, we have $BA = \begin{pmatrix} Q_{11} & Q_{12} & \\ & \ddots & \ddots \\ \bigcirc & & Q_{ss} \end{pmatrix}$ where $Q_{11} \cdots Q_{ss} \neq 0$ (see (2) and the proof of Lemma 2). Let us show that for any vector $0 \neq w \in \mathcal{R}^s$ holds $w\,A \neq 0$, this would imply that A is quasiinversible from the right because of Lemma 3. Assume that $0 = wA$. Then $0 = wA = (wB^{-1}Q)$ and we get a contradiction, which justifies that A is quasiinversible from the right.

In order to prove the necessary bound on G, consider for each $1 \leq j \leq s$ a matrix $A^{(j)}$ obtained from A by deleting its j-th column. Lemma 3 shows that there exists a vector $0 \neq g^{(j)} \in \mathcal{R}^s$ such that $g^{(j)} A^{(j)} = 0$ and ord $g^{(j)} \leq (s-1)r + 1$. As a matrix G take a matrix with j-th row equal to $g^{(j)}$.

Notice that when A is inversible, lemma 4 follows from the theorem 6 in [O], where a similar bound was proved for a much more general situation of an inversible nonlinear differential map.

Thus, for a square matrix A we can say that it is quasiinversible without specifying from the left or from the right. Notice (see also [G91]) that a square matrix A is quasiinversible iff its Dieudonné determinant ([A]) does not vanish.

Define the rank $rk(A)$ as a maximal ℓ such that there exists $\ell \times \ell$ quasiinversible submatrix of A (cf. [J]), the following lemma can be deduced from the results in [J].

Lemma 5. *$rk(A)$ coincides with*

a) ℓ in the standard basis form (2);

b) the maximal number of the columns of A being $\mathcal{R}$-linearly independent;

c) the maximal number of the rows of A being $\mathcal{R}$-linearly independent.

2. Some properties of the order of a system of linear differential operators.

For brevity we adopt the notation $\dim(\mathcal{R}^s/\mathcal{R}^k A) = \dim_{\mathbb{C}(X)}(\mathcal{R}^s/\mathcal{R}^k A)$.

Lemma 6. *For any $m \times k$ matrix B and $k \times s$ matrix A over $\mathcal{R}$*

$$\dim(\mathcal{R}^s/\mathcal{R}^m BA) \leq \dim(\mathcal{R}^k/\mathcal{R}^m B) + \dim(\mathcal{R}^s/\mathcal{R}^k A)$$

If A is quasiinversible from the right then this inequality turns to be the equality.

Proof. Consider the natural projections

$\Pi_1 : \mathcal{R}^s \to \mathcal{R}^s/\mathcal{R}^k A$, $\Pi_2 : \mathcal{R}^k \to \mathcal{R}^k/\mathcal{R}^m B$, $\Pi_3 : \mathcal{R}^s \to \mathcal{R}^s/\mathcal{R}^m BA$.

Let $u_1, \dots, u_\gamma \in \mathcal{R}^k$ be such that $\Pi_2(u_1), \dots, \Pi_2(u_\gamma)$ constitute a basis over $\mathbb{C}(X)$ of $\mathcal{R}^k/\mathcal{R}^m B$, and $v_1, \dots, v_\delta \in \mathcal{R}^s$ be such that $\Pi_1(v_1), \dots, \Pi_1(v_\delta)$ constitute a basis over $\mathbb{C}(X)$ of $\mathcal{R}^s/\mathcal{R}^k A$ (note that γ or δ could be infinite). Let us prove that $\Pi_3(v_1), \dots, \Pi_3(v_\delta)$, $\Pi_3(u_1 A), \dots, \Pi_3(u_\gamma A)$ generate $\mathcal{R}^s/\mathcal{R}^m BA$ over $\mathbb{C}(X)$ and constitute a basis when A is quasiinversible from the right. Indeed, let for some elements $f_1, \dots, f_\delta,\ g_1, \dots, g_\gamma \in \mathbb{C}(X)$ and a vector $(\beta_1, \dots, \beta_m) \in \mathcal{R}^m$ we have $f_1 v_1 + \cdots + f_\delta v_\delta + (g_1 u_1 + \cdots + g_\gamma u_\gamma)A = (\beta_1, \cdots, \beta_m)BA$, then $f_1 = \cdots = f_\delta = 0$. If A is quasiinversible from the right then $g_1 u_1 + \cdots + g_\gamma u_\gamma = (\beta_1, \cdots, \beta_m)B$ by virtue of Lemma 3, hence $g_1 = \cdots = g_\gamma = 0$.

On the other hand, for any vector $w \in \mathcal{R}^s$ there exist $f_1, \dots, f_\delta \in \mathbb{C}(X)$ and a vector $v \in \mathcal{R}^k$ for which $w = f_1 v_1 + \cdots + f_\delta v_\delta + vA$. Then $v = g_1 u_1 + \cdots + g_\gamma u_\gamma + uB$ for suitable $g_1, \dots, g_\gamma \in \mathbb{C}(X)$, $u \in \mathcal{R}^m$. Therefore $w = f_1 v_1 + \cdots + f_\delta v_\delta + g_1 u_1 A + \cdots + g_\gamma u_\gamma A + uBA$, i.e. $\dim(\mathcal{R}^s/\mathcal{R}^m BA) \le \gamma + \delta = \dim(\mathcal{R}^k/\mathcal{R}^m B) + \dim(\mathcal{R}^s/\mathcal{R}^k A)$.

In other terms we can reformulate what was proved above, saying that we have the following exact sequence of $\mathbb{C}(X)$-vector spaces

$$\mathcal{R}^k/\mathcal{R}^m B \xrightarrow{\alpha} \mathcal{R}^s/\mathcal{R}^m BA \xrightarrow{\pi} \mathcal{R}^s/\mathcal{R}^k A \to O$$

where $\alpha(v + \mathcal{R}^m B) = vA + \mathcal{R}^m BA$ and $\pi(w + \mathcal{R}^m BA) = w + \mathcal{R}^k A$. In the case of quasiinversible A the following sequence is exact:

$$O \to \mathcal{R}^k/\mathcal{R}^m B \xrightarrow{\alpha} \mathcal{R}^s/\mathcal{R}^m BA \xrightarrow{\pi} \mathcal{R}^s/\mathcal{R}^k A \to O$$

LEMMA 7. *If a matrix A is square then* $\dim(\mathcal{R}^s/\mathcal{R}^m BA) = \dim(\mathcal{R}^s/\mathcal{R}^m B) + \dim(\mathcal{R}^s/\mathcal{R}^s A)$

Proof. If A is quasiinversible (see Lemma 4) then we use Lemma 6.

If A is not quasiinversible then $\dim(\mathcal{R}^s/\mathcal{R}^m BA) \ge \dim(\mathcal{R}^s/\mathcal{R}^s A) = \infty$.

Remark that as in the following example $\dim\left(\mathcal{R}^2/\mathcal{R}^2\begin{pmatrix}1&1\\1&D\end{pmatrix}\right)=1$, $\dim\left(\mathcal{R}/\mathcal{R}^2\begin{pmatrix}1\\1\end{pmatrix}\right)=0$ and for the product of these matrices $\dim\left(\mathcal{R}/\mathcal{R}^2\begin{pmatrix}2\\1+D\end{pmatrix}\right)=0$, the inequality in Lemma 6 for rectangular matrices could be strict.

LEMMA 8. *a) For a triangular $k\times s$ (where $k\geq s$) matrix* $C=\begin{pmatrix}C_1 & & *\\ & \ddots & \\ \bigcirc & & C_s\end{pmatrix}$ *we have* $\dim(\mathcal{R}^s/\mathcal{R}^kC)=ord\ C_1+\cdots+ord\ C_s$, *provided that* $C_1\cdots C_s\neq 0$.

b) $\dim(\mathcal{R}^s/\mathcal{R}^kA)<\infty$ *iff* $\ell=s$ *in the standard basis form (2). In this case* $\dim(\mathcal{R}^s/\mathcal{R}^kA)=ord\ Q_{11}+\cdots+ord\ Q_{ss}$.

c) When A is a square matrix then $\dim(\mathcal{R}^s/\mathcal{R}^sA)=\dim(\mathcal{R}^s/A\mathcal{R}^s)$, *where in the right side of the equality we regard $\mathcal{R}^s$ as a right $\mathcal{R}$-module.*

d) A square matrix A is inversible iff $\dim(\mathcal{R}^s/\mathcal{R}^sA)=0$.

Proof. a) Is obvious.

b) The first statement one can find in the proof of Lemma 3. The second statement follows from a) and the equality $\dim(\mathcal{R}^s/\mathcal{R}^kA)=\dim(\mathcal{R}^s/\mathcal{R}^kQ)$.

c) Because of Lemma 4 both left and right sides of the equality are finite or infinite simultaneously. Assume they are both finite. Then $BA=\begin{pmatrix}Q_{11} & & *\\ & \ddots & \\ \bigcirc & & Q_{ss}\end{pmatrix}$ (see (2)) where B is a product of elementary matrices and $Q_{11}\cdots Q_{ss}\neq 0$ (see b)). For any $s\times s$ elementary matrix G we have $\dim(\mathcal{R}^s/\mathcal{R}^sG)=\dim(\mathcal{R}^s/G\mathcal{R}^s)=0$, hence by Lemma 7 the same is true for any inversible matrix (cf. Lemma 1), thus $\dim(\mathcal{R}^s/\mathcal{R}^sB)=\dim(\mathcal{R}^s/B\mathcal{R}^s)=0$. a) implies that for the triangular matrix

$Q=\begin{pmatrix}Q_{11} & & *\\ & \ddots & \\ \bigcirc & & Q_{ss}\end{pmatrix}$ the equalities $\dim(\mathcal{R}^s/\mathcal{R}^sQ)=\dim(\mathcal{R}^s/Q\mathcal{R}^s)=\text{ord }Q_{11}+\cdots+\text{ord }Q_{ss}$ hold, then Lemma 7 entails c).

d) follows from b) and Lemma 1.

The following lemma was proved in [R], p. 135 (see also [Ko]) in a more general form for the order of a prime ideal in the ring of differential polynomials.

LEMMA 9. *If $k \times s$ matrix A is quasiinversible from the left then* $\dim(\mathcal{R}^s/\mathcal{R}^k A) \leq \max_i \{ord\ a_{i1}\} + \cdots + \max_i \{ord\ a_{is}\}$.

3. <u>Bounds on the standard basis form of a matrix over the ring of differential operators.</u>

In this section we'll estimate ord (Q), ord (B) in the standard basis form (2) relying on the results on the order from the section 2.

Take any $s \times s$ permutation matrix P, mapping $P(p_1) = 1, \ldots, P(p_\ell) = \ell$, then $BAP = \begin{pmatrix} Q_{1p_1} & & & \\ & \ddots & & \\ & & Q_{\ell p_\ell} & \cdots \\ \bigcirc & & & \bigcirc \end{pmatrix}$. Represent $AP = (A_1 A_2)$ where $k \times \ell$ submatrix A_1 consists of the first ℓ columns of AP, then by Lemma 5 $rkA = rkA_1 = \ell$. Complete A_1 by $(k-\ell)$ columns of the type $(0, \ldots, 0, 1, 0, \ldots, 0)^T$ to $k \times k$ quasiinversible matrix $(A_1 A_3)$. Then

$$B(A_1 A_3) = \begin{pmatrix} Q_{1p_1} & & & \\ & \ddots & & \\ & & Q_{\ell p_\ell} & \\ & \bigcirc & & * \end{pmatrix}$$

Making several elementary transformations with the rows having indices bigger than ℓ, reduce the matrix at the right side to the triangular form

$$B_0(A_1 A_3) = \begin{pmatrix} Q_{1p_1} & & & * & & \\ & \ddots & & & & \\ & & Q_{\ell p_\ell} & & & \\ & & & Q^{(0)}_{\ell+1,\ell+1} & & \\ & \bigcirc & & & \ddots & \\ & & & & & Q^{(0)}_{kk} \end{pmatrix}$$

herewith $B = \binom{B_1}{B_2}$ where B_1 is $\ell \times k$ submatrix, $B_0 = \binom{B_1}{B_3}$ and $\dim(\mathcal{R}^k/\mathcal{R}^k B) = \dim(\mathcal{R}^k/\mathcal{R}^k B_0) = 0$ (see Lemma 8 d)).

Moreover, making some elementary transformations with the rows, one can assume w.l.o.g. that ord $(Q_{ip_i}) <$ ord (Q_{jp_j}), ord $(Q^{(0)}_{ij}) <$ ord $(Q^{(0)}_{jj})$ for all $i < j$.

By Lemmas 6, 7, 9 ord $(Q_{1p_1}) + \cdots$ord $(Q_{\ell p_\ell})$ + ord $(Q^{(0)}_{\ell+1,\ell+1}) + \cdots +$ ord $(Q^{(0)}_{kk})$ $= \dim(\mathcal{R}^k/\mathcal{R}^k A_1 A_3) \leq \max_i\{\text{ord } A_{ip_1}\} + \cdots + \max_i\{\text{ord } A_{ip_\ell}\} \leq \ell r$, hence ord (Q_{i,p_j}), ord $(Q_{ij}^{(0)}) \le \ell r$. By Lemma 4 there exists $k \times k$ matrix G over $\mathcal{R}$ such that $(A_1 A_3)\, G =$ $\begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_k \end{pmatrix}$

where $C_1 \cdots C_k \ne 0$ and ord $(G) \le (k-1)r+1$, hence ord $(C_i) \le kr+1$. As $B_0 \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_k \end{pmatrix}$ $= \begin{pmatrix} Q_{1p_1} & & * \\ & \ddots & \\ & & \ddots \\ \bigcirc & & Q_{kk}^{(0)} \end{pmatrix} G$, we conclude that ord $(B_0) \le (\ell + k - 1)r + 1$.

Observe that $B_0 A$ has the standard basis form similar to (2) (with the same "diagonal" entries $Q_{1p_1}, \dots, Q_{\ell,p_\ell}$ and perhaps different other entries as we achieved the conditions ord $Q_{ip_j} <$ ord Q_{jp_j}, ord $(Q_{ij}^{(0)}) <$ ord $(Q_{jj}^{(0)}),\ i < j$)

$$B_0 A = \begin{pmatrix} 0 & \dots & 0\, Q_{1p_1} & & & & * & \\ 0 & \dots & \dots & 0\, Q_{2p_2} & & & & \\ \vdots & & & & \ddots & & & \\ 0 & \dots & \dots & \dots & \dots & 0\, Q_{\ell p_\ell} & & \\ & & & & \bigcirc & & & \bigcirc \end{pmatrix}$$

since $rkA = \ell$. Therefore ord $(Q) \le (\ell + k)r + 1$. Let us summarize the proved in the present section in the following lemma.

LEMMA 10. *There exists an inversible matrix B such that $BA = Q$ has the standard basis form (2) and moreover ord $(B) \le (s + k - 1)r + 1$, ord $(Q) \le (s + k)r + 1$.*

4. NC algorithm for finding standard basis form of a matrix over the ring of differential operators.

Let us design an algorithm which finds the standard basis form of a matrix in NC, i.e. polynomial time and with polylogarithmic depth (parallel complexity).

Join to the matrix A the unit matrix and denote the resulting $k \times (s + k)$ matrix by $\bar{A} = (AE)$. Obviously $rk\bar{A} = k$ (see Lemma 5). Therefore, the standard basis form of $\bar{A}$

equals to

$$B_1\bar{A} = \begin{pmatrix} 0 & \dots & 0\,Q_{1p_1} & & & & & \\ \vdots & & & \ddots & & & & \\ 0 & \dots & \dots & \dots & 0\,Q_{\ell p_\ell} & * & & \\ \vdots & & & & & \ddots & & \\ 0 & \dots & \dots & \dots & \dots & \dots & 0\,Q_{kp_k} & \dots \end{pmatrix} = \bar{Q} \quad (\text{see } (2))$$

where $\dim(\mathcal{R}^k/\mathcal{R}^k B_1) = 0$ (see Lemma 8).

For each $1 \le m \le s+k$ and $0 \le j \le (s+2k)r+1$ the algorithm tests, whether there exists a vector $w = (w_1, \dots, w_k)$ with ord $(w) \le (s+2k-1)r+1$ (cf. Lemma 10) such that the vector $w\bar{A} = (\underbrace{0, \dots, 0, v}_{m}, \dots)$ where ord $v = j$ and the leading coefficient $\ell c(v) = 1$. The latter condition can be written as a linear system $\mathcal{T}_{m,j}$ over $\mathbb{Q}(X)$ with $k((s+2k-1)r+2)$ unknowns being the coefficients of $w_1, \dots, w_k$ in the powers of $1, D, \dots, D^{(s+2k-1)r+1}$ and with at most $(s+k)((s+2k)r+1)$ equations. As the entries of this linear system are the rational functions from $\mathbb{Q}(X)$ with the degrees in X not exceeding d and with the size of rational coefficients at most M, the algorithm can solve $\mathcal{T}_{m,j}$ in time $(Mdskr)^{0(1)}$ with the depth (parallel complexity) $\log^{0(1)}(Mdskr)$ using [M].

As the rows of the matrix $\bar{Q}$ constitute a (triangular) basis of the left $\mathcal{R}$-module $\mathcal{R}^k\bar{A}$, the system $\mathcal{T}_{m,j}$ could be solvable only for $m = p_1, \dots, p_k$. For each of these $m = p_i$ take the minimal such j_i for which $\mathcal{T}_{p_i,j_i}$ is solvable. Lemma 10 implies that $\mathcal{T}_{p_i,j}$ is solvable for $j =$ ord Q_{i,p_i}, hence $j_i \le$ ord Q_{i,p_i}. Take a solution $W^{(i)} = (w_1^{(i)}, \dots, w_k^{(i)})$ for $\mathcal{T}_{p_i,j_i}$, and denote by W $k \times k$ matrix with i-th row to be $W^{(i)}$. Then

$$W\bar{A} = \begin{pmatrix} 0 & \dots & 0\,\widetilde{Q}_{1p_1} & & \\ \vdots & & & * & \\ 0 & \dots & \dots & 0\,\widetilde{Q}_{kp_k} & \dots \end{pmatrix} = \widetilde{Q}$$

where ord $\widetilde{Q}_{i,p_i} = j_i$.

Let us prove that $\dim(\mathcal{R}^k/\mathcal{R}^k W) = 0$. Denote by $\bar{A}_0, \bar{Q}_0, \widetilde{Q}_0$ the $k \times k$ matrices obtained from $\bar{A}, \bar{Q}, \widetilde{Q}$ respectively, by taking the submatrices formed by the columns $p_1, \dots, p_k$. Then $B_1\bar{A}_0 = \bar{Q}_0$, $W\bar{A}_0 = \widetilde{Q}_0$.

Lemmas 7, 8 a) entail $0 = \dim(\mathcal{R}^k/\mathcal{R}^k B_1) = \text{ord } Q_{1,p_1} + \cdots + \text{ord } Q_{k,p_k} - \dim(\mathcal{R}^{s+k}/\mathcal{R}^k \bar{A}) \geq \text{ord } \widetilde{Q}_{1,p_1} + \cdots + \text{ord } \widetilde{Q}_{k,p_k} - \dim(\mathcal{R}^{s+k}/\mathcal{R}^k \bar{A}) = \dim(\mathcal{R}^k/\mathcal{R}^k W) \geq 0$, therefore $\dim(\mathcal{R}^k/\mathcal{R}^k W) = 0$ and moreover $\text{ord } \widetilde{Q}_{i,p_i} = \text{ord } Q_{i,p_i}$, $1 \leq i \leq k$. As WA has a desired standard basis form (see (2)), we get the following lemma

Lemma 11. *There is an NC-algorithm, so running in time $(Md\,skr)^{0(1)}$ with a depth (parallel complexity) $\log^{0(1)}(Md\,skr)$, which produces an inversible over $\mathcal{R}$ $k \times k$ matrix*

$$W \text{ such that } WA = \begin{pmatrix} 0 \ \dots \ 0 \ \widetilde{Q}_{1p_1} & & \\ \vdots & & * \\ 0 \ \dots & \dots & 0 \ \widetilde{Q}_{\ell p_\ell} \\ & \bigcirc & \bigcirc \end{pmatrix} \text{ has the standard basis form.}$$

Now we get a criterium for solvability of a system (1). Namely, apply Lemma 11 to $k \times (s+1)$ matrix $A = (L_{ij}\ b_i)_{1 \leq i \leq k,\ 1 \leq j \leq s}$, so the last column is $\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$. Then the system (1) has a solution in the field $\mathcal{F}$ iff and only if $p_\ell \leq s$ (in other words $p_\ell \neq s+1$) and the standard basis form provides a "triangular" basis of the space of solutions of (1). Let us summarize the obtained above in the following main result of the paper.

Theorem. *One can test solvability of a system (1) of linear differential equations in several unknowns in the Picard-Vessiot closure $\mathcal{F}$ and find a "triangular" basis of the space of solutions of (1) in NC complexity class, so with the time $(Md\,skr)^{0(1)}$ and with a depth (parallel time) $\log^{0(1)}(Md\,skr)$.*

Observe that the space of solutions of a homogeneous system (1), so when $b_1 = \cdots = b_k = 0$, has a finite dimension (over $\mathbb{C}(X)$) if and only if $p_1 = 1, \dots, p_\ell = \ell$ and $\ell = s$ (for $k \times s$ matrix $A = (L_{ij})$, see above). In this case the standard basis form WA of the system can be rewritten in the common first-order matrix form $DY = HY$ (cf. [G90]) where the vector Y has coordinates $u_1, Du_1, \dots, D^{j_1-1}u_1, u_2, \dots, D^{j_2-1}u_2, \dots, u_s, \dots, D^{j_s-1}u_s$ and $j_i = \text{ord } \widetilde{Q}_{i,p_i}$, $1 \leq i \leq s$, one could easily get the matrix H over $\mathbb{Q}(X)$ from the matrix WA.

Acknowledgements. The author would like to thank Mike Singer for the attention to the paper.

REFERENCES

[A] Artin, E., Geometric algebra, Interscience Publ., 1957.

[B] Björk, J.-E., Rings of differential operators, North-Holland, 1979.

[C] Carro-Ferro, G., *Groebner bases and differential ideals*, Lect. Notes Comput. Sci., 356 (1987), pp. 129–140.

[G] Galligo, A., *Some algorithmic questions on ideals of differential operators*, Lect. Notes Comput. Sci., 204 (1985), pp. 413–421.

[G87] Grigoriev, D., *Complexity of quantifier elimination in the theory of ordinary differential equations*, Lect. Notes Comput. Sci., 378 (1989), pp. 11–25.

[G88] Grigoriev, D., *Complexity of factoring and GCD calculating of ordinary linear differential operators*, J. Symb. Comput., 10, N1 (1990), pp. 7–37.

[G90] Grigoriev, D., Complexity of irreducibility testing for a system of linear ordinary differential equations, Proc. Int. Symp. on Symb. Algebr. Comput., ACM (1990) Japan, pp. 225–230.

[G91] Grigoriev, D., Complexity of solving systems of linear equations over the rings of differential operators, Proc. Int. Symp. Eff. Meth. in Algebraic Geometry (1990) Italy; in Progr. in Math., Birkhäuser, v.94, 1991, pp. 195–202 .

[J] Jacobson, N., *Pseudo-linear transformations*, Ann. Math., 38, N2 (1937), pp. 484–507.

[K] Kaplansky, I., An introduction to differential algebra, Hermann, Paris, 1957.

[Ko] Kolchin, E., Differential algebra and algebraic groups, Academic Press, 1973.

[M] Mulmuley, K., *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field*, Proc. 18 STOC ACM (1986), pp. 338–339.

[O] Ollivier, F., *Standard bases of differential ideals*, Lect. Notes Comput. Sci., 508 (1991), pp. 304–321.

[R] Ritt, J.F., Differential algebra, Amer. Math. Soc. Colloq. Publ., vol. 33, NY, 1950.

Departments of Computer Science and Mathematics
Pennsylvania State University
University Park, PA 16802 USA
e-mail: dima@math.psu.edu