Journal of Mathematical Sciences, Vol. 70, No. 4, 1994

COMPLEXITY OF SOLUTION OF LINEAR SYSTEMS IN RINGS OF DIFFERENTIAL OPERATORS

D. Yu. Grigor'ev

UDC 518.5+512.46

Suppose given a $k_1 \times k_2$ system of linear equations over the Weyl algebra $\mathcal{A}_n = F[X_1,\dots,X_n,D_1,\dots,D_n]$ or over the algebra of differential operators $\mathcal{K}_n = F(X_1,\dots,X_n)[D_1,\dots,D_n]$, where the degree of each coefficient of the system is less than d. It is proved that if the system is solvable over $\mathcal{A}_n$ or $\mathcal{K}_n$, respectively, then it has a solution of degree at most $(k_1 d)^{2^{O(n)}}$.

Introduction

Let $\mathcal{A}_n = \mathcal{A}_n(F) = F[X_1,\dots,X_n,D_1,\dots,D_n]$ be the Weyl algebra over the field F ([6]); as is known, it is defined by the relations

$$X_iX_j = X_jX_i;\ D_iD_j = D_jD_i;\ X_iD_i = D_iX_i - 1;\ X_iD_j = D_jX_i \qquad i \neq j \tag{1}$$

One can also interpret the Weyl algebra as the algebra obtained from the polynomial algebra $F[X_1,\dots,X_n]$ by adjoining the differentiation operators $D_1,\dots,D_n$ with respect to the variables $X_1,\dots,X_n$, respectively. We denote by $\mathcal{K}_n = \mathcal{K}_n(F) = F(X_1,\dots,X_n)[D_1,\dots,D_n] \supset \mathcal{A}_n(F)$ the algebra of differential operators obtained from the field $F(X_1,\dots,X_n)$ of rational functions by adjoining the operators $D_1,\dots,D_n$ (cf. [6]).

An element $a \in \mathcal{A}_n$ can be represented uniquely in the form $a = \sum_{I,J} D_n^{i_n}\dots D_1^{i_1} X_n^{j_n}\dots X_1^{j_1}$, where $a_{I,J} \in F$, the multi-indices $I = (i_n,\dots,i_1), J = (j_n,\dots,j_1)$; any element $b \in \mathcal{K}$ can be represented uniquely in the form $b = a_1 c^{-1}$, where $a_1 \in \mathcal{A}_n, 0 \neq c \in F[X_1,\dots,X_n]$ and the degree $\deg(c)$ is the least possible. We define the degree $\deg(D_n^{i_n}\dots D_1^{i_1} X_n^{j_n}\dots X_1^{j_1}) = i_n+\dots+i_1+j_n+\dots+j_1$ according to the Bernshtein filtration (cf. [6]) and the degree $\deg(a) = \max_{a_{I,J}\neq 0} \deg(D_n^{i_n}\dots D_1^{i_1} X_n^{j_n}\dots X_1^{j_1})$; finally, $\deg(b) = \max(\deg(a_1), \deg(c))$.

The goal of the present paper is to estimate the complexity of the solution of the system of linear equations

$$\sum_{1\le l\le s} u_{k,l} V_l = w_k,\quad 1 \le k \le m \tag{2}$$

over the ring $\mathcal{A}_n$ (i.e., the coefficients $u_{k,l}$, $w_k \in \mathcal{A}_n$, and also the unknowns $V_l \in \mathcal{A}_n$) or, respectively, over the ring $\mathcal{K}_n$. Below in the formulation of the theorem and corollary $\mathcal{R}$ denotes either the ring $\mathcal{A}_n$ or the ring $\mathcal{K}_n$.

THEOREM. Let the system (2) be solvable in the ring $\mathcal{R}$ and $\deg(u_{k,l}), \deg(w_k) < d, 1 \le k \le m, 1 \le l \le s$. Then one can find a solution $V_1,\dots,V_s$ of (2) for which $\deg(V_l) \le (md)^{2^{O(n)}}, 1 \le l \le s$.

COROLLARY. Let the field F be defined effectively, for example, as a finitely generated extension of the field $\mathbb{Q}$ (cf. 2, 3, 5, 7]), and the bitwise size of any coefficient of the polynomials $u_{k,l}$, w_k be at most M. Then one can verify the solvability of (2) over the ring $\mathcal{R}$ and construct a solution (if the system is solvable) in polynomial time in M, $(md)^{2^{O(n)}}$, s.

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, Vol. 192, pp. 47-59, 1991.

One derives the corollary from the theorem by representing (2) as a system of linear equations over the field F in the case $\mathcal{R} = \mathcal{A}_n$ or over the field $F(X_1,\dots,X_n)$ in the case $\mathcal{R} = \mathcal{K}_n$, respectively, whose unknowns are the coefficients of the elements $V_1,\dots,V_s$ for monomials in $D_n,\dots,D_1,X_n,\dots,X_1$ or for monomials in $D_n,\dots,D_1$, respectively.

We note that in the case of a system (2) over the ring of polynomials $F[X_1,\dots,X_n]$ the estimate of the theorem is well-known [11]; however it is impossible to extend its proof from [11] directly to our case since the rings $\mathcal{A}_n$ and $\mathcal{K}_n$ are noncommutative. However the general approach of [11] is used below in proving the theorem.

We mention that in [3] an algorithm of polynomial complexity is constructed for finding the g.c.d. of a family of ordinary linear operators; this in particular implies the theorem for the case $\mathcal{R} = \mathcal{K}_1$. In [10] it is proved that in the polynomial ring $F[X_1,\dots,X_n]$ even for the special case of a system (2) of one equation $\sum_{1\le l\le s} u_l V_l = w$ (i.e., the problem of recognizing whether the polynomial w belongs to the ideal with generators $u_1,\dots,u_s$) the estimate given in the theorem is sharp in order. Thus, the estimate of the theorem is also sharp in order. Indeed let $u_l, w \in F[D_1,\dots,D_n] \subset \mathcal{A}_n$ and $\sum_{1\le l\le s} u_l V_l = w$; then when $\mathcal{R} = \mathcal{A}_n$ we represent $V_l = \sum_{I,J} V^{(l)}_{I,J} D_n^{i_n}\dots D_1^{i_1} X_n^{j_n}\dots X_1^{j_1}$ (cf. above), and then $\sum_{1\le l\le s} u_l \left(\sum_I V^{(l)}_{I,0} D_n^{i_n}\dots D_1^{i_1}\right) = w$, here the sum $\sum_I V^{(l)}_{I,0} D_n^{i_n}\dots D_1^{i_1}$ is taken over all pairs I, J in the representation of V_l, for which $J=0$; now when $\mathcal{R} = \mathcal{K}_n$ we represent $V_l = \sum_{I,J} V^{(l)}_{I,J} D_n^{i_n}\dots D_1^{i_1} X_n^{j_n}\dots X_1^{j_1} c^{-1}$, where $c = c_0 X_n^{j_n^{(0)}}\dots X_1^{j_1^{(0)}} + \tau \in F[X_1,\dots,X_n]$ and $0 \ne c_0 \in F$ is the coefficient of the polynomial c at some monomial $X_n^{j_n^{(0)}}\dots X_1^{j_1^{(0)}}$, then $c_0^{-1} \sum_{1\le l\le s} u_l \left(\sum_I V^{(l)}_{I,J^{(0)}} D_n^{i_n}\dots D_1^{i_1}\right) = w$, where the sum $\sum_I V^{(l)}_{I,J^{(0)}} D_n^{i_n}\dots D_1^{i_1}$ is taken over all pairs $I, J^{(0)}$ in the representation of V_l, for which $J^{(0)} = (j_n^{(0)},\dots,j_1^{(0)})$. Thus, we have shown that if the equation $\sum_{1\le l\le s} u_l V_l = w$ for u_l, $w \in F[D_1,\dots,D_n]$ is solvable in $\mathcal{R}$, then it has a solution $\tilde V_1,\dots,\tilde V_s \in F[D_1,\dots,D_n]$, where $\deg(\tilde V_l) \le \deg(V_l)$, $1 \le l \le s$, which by [10] proves the required sharpness of the estimate in order in the theorem.

We also mention that the nearly sharp estimate deg $\sum_{1\le l\le s} u_l V_l = 1$ established in [9] for the special case of recognition of an ideal being the unit ideal in a polynomial ring, i.e., the problem of solvability of the system $\deg(V_l) \le d^{O(n)}$ The author does not know whether an analogous result holds for the rings $\mathcal{A}_n$ and $\mathcal{K}_n$. A number of algorithmic problems in ideal theory in rings of differential operators are also posed in [8].

Sec. 1. Estimation of the Elements of a Quasi-Inverse Matrix Over the Weyl Algebra

Let the matrix $A = (a_{i,j})_{1\le i\le m-1, 1\le j\le m}$ have elements in the Weyl algebra, $a_{i,j} \in \mathcal{A}_n$, where $\deg(a_{i,j}) < d$.

LEMMA 1. There exists a vector $0 \ne b = (b_1,\dots,b_m) \in (\mathcal{A}_n)^m$, such that Ab = 0, where $\deg(b) \le 4n(m-1)d = N$.

Proof. We consider the linear space $\mathcal{B} \subset (\mathcal{A}_n)^m$ over F consisting of all vectors $c = (c_1,\dots,c_m)$, such that $\deg(c) \le N$. Then $\dim(\mathcal{B}) = \binom{N+2n}{2n} m$. For any vector $c \in \mathcal{B}$ one has $\deg(Ac) \le N+d$, i.e., $Ac \in \mathcal{T}$, where the space $\mathcal{T}$ consists of all vectors $e = (e_1,\dots,e_{m-1}) \in (\mathcal{A}_n)^{m-1}$, for which $\deg(e) \le N+d$, so $\dim(\mathcal{T}) = \binom{N+d+2n}{2n}(m-1)$.

We prove that $\binom{N+2n}{2n} m > \binom{N+d+2n}{2n}(m-1)$, from which the lemma will follow. Indeed $\binom{N+d+2n}{2n} / \binom{N+2n}{2n} = \frac{N+d+2n}{N+2n}\cdot\frac{N+d+2n-1}{N+2n-1}\cdots\frac{N+d+1}{N+1} < \left(\frac{N+d+1}{N+1}\right)^{2n}$. It suffices to verify that $\left(\frac{N+d+1}{N+1}\right)^{2n} < 1 + \frac{1}{m-1}$; it is easy to see that $\left(1+\frac{1}{m-1}\right)^{1/2n} > 1 + \frac{1}{2n(m-1)} + \frac{1}{2}\frac{1}{2n}\left(\frac{1}{2n}-1\right)\left(\frac{1}{m-1}\right)^2 > 1 + \frac{1}{4n(m-1)} > 1 + \frac{d}{N+1}$. The lemma is proved.

We call the $m\times m$ matrix $C = (c_{i,j})$ a right (respectively left) quasi-inverse to the matrix $B = (b_{i,j})$ if the matrix BC (resp. CB) is diagonal with nonzero elements on the diagonal.

LEMMA 2. If the $m \times m$ matrix B over the ring $\mathcal{A}_n$ has a right quasi-inverse over $\mathcal{A}_n$, then B also has a left quasi-inverse G over $\mathcal{A}_n$, while $\deg(G) \leq 4n(m-1)d$

Proof. We note first that there does not exist a vector $0 \neq b \in (\mathcal{A}_n)^m$, for which bB = 0, since $\mathcal{A}_n$ has no divisors of zero ([6]). We denote by $B^{(i)}$ the matrix obtained from B by removing the i-th column. By Lemma 1 one can find a vector $0 \neq g_i \in (\mathcal{A}_n)^m$, such that $g_i B^{(i)} = 0$ and $\deg(g_i) \leq N$. Then the matrix G whose rows are $g_1, \ldots, g_m$ is a left quasi-inverse to B. The lemma is proved.

For the algebra $\mathcal{A}_n$ one constructs the skew field of quotients $\mathcal{D}_n$ (cf. [6]), where any element of $\mathcal{D}_n$ can be represented in the form $a_1 b_1^{-1}$ and also in the form $b_2^{-1} a_2$ for suitable $a_1, b_1, a_2, b_2 \in \mathcal{A}_n$(cf. Lemma 1 for m = 2). $\mathcal{D}_n$ is also the skew field of quotients for the ring $\mathcal{K}_n$. A matrix over $\mathcal{A}_n$ (analogously over $\mathcal{K}_n$) has right and left quasi-inverses (cf. Lemma 2) if and only if it is nondegenerate as a matrix over $\mathcal{D}_n$, which is equivalent with its Dieudonne determinant being nonzero (cf. [1]). We define the rank r = rg(A) of the matrix A over $\mathcal{D}_n$ as the maximal size r of a nondegenerate submatrix. Below in the formulation of the lemma the $m_1 \times m_2$ matrix A of rank r over $\mathcal{D}_n$ is such that its $r \times r$ submatrix A_1 in the upper left corner is nondegenerate and the elements of A_1 belong to $\mathcal{A}_n$.

LEMMA 3. Let C_1 be a left quasi-inverse over $\mathcal{A}_n$ to A_1. Then one can find an $(m_1 - r) \times r$ matrix C_2 over $\mathcal{D}_n$, such that

$$\begin{pmatrix} C_1 & 0 \\ C_2 & E \end{pmatrix} A = \left(\begin{array}{c|c} \begin{matrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_r \end{matrix} & * \\ \hline 0 & 0 \end{array}\right),$$

E denoting the identity matrix here and below.

Proof. The matrix C_2 is defined by the condition that in the lower left corner of the product of matrices considered one has the zero matrix (it is obtained by suitable elementary row transformations, by addition of some combinations of the first r rows to the last $(m_1 - r)$ rows). Then in the product obtained the lower right submatrix is also equal to zero in view of the definition of rank, which proves the lemma.

Now we return to the system (2) over the ring $\mathcal{R}$ When $\mathcal{R} = \mathcal{A}_n$, we apply Lemma 3 to the $m \times s$ matrix $(u_{k,l})$ and get matrices C_1, C_2; making a suitable renumbering of the rows and columns we assume that in the upper left corner of $(u_{k,l})$ there is a nondegenerate submatrix of maximal size r. If the vector $(C_2\, E)(w_1, \ldots, w_m)^T$ is nonzero, the system (2) has no solutions. Now if $(C_2\, E)(w_1, \ldots, w_m)^T = 0$, then (2) is equivalent to a system of the following form (cf. Lemma 3):

$$a_k V_k + \sum_{r+1 \leq l \leq s} a_{k,l} V_l = b_k, \quad 1 \leq k \leq r. \tag{3}$$

By virtue of Lemma 2, $\deg(a_k), \deg(a_{k,l}), \deg(b_k) \leq 4nrd \leq 4nmd$. In the case when the ring $\mathcal{R} = \mathcal{K}_n$, the elements $u_{k,l} = u_{k,l}^{(1)} (u_{k,l}^{(2)})^{-1}$ for all $1 \leq k, l \leq r$, where $u_{k,l}^{(1)} \in \mathcal{A}_n, u_{k,l}^{(2)} \in F[X_1, \ldots, X_n]$, can be reduced to a common denominator u = g.c.d. $(\{u_{k,l}^{(2)}\}_{1 \leq k, l \leq r})$, i.e., $u_{k,l} = u_{k,l}^{(3)} u^{-1}$ for all k and l, where $u_{k,l}^{(3)} \in \mathcal{A}_n$ for $1 \leq k, l \leq r$. As above we apply Lemma 3 to the matrix $(u_{k,l}^{(3)})$ and reduce system (2) to a form analogous to (3). Here since $\deg(u_{k,l}^{(3)}) \leq dr^2 \leq dm^2$ for $1 \leq k, l \leq r$, one has $\deg(a_k), \deg(a_{k,l}), \deg(b_k) \leq 4nm^3 d$ by Lemma 2.

Remark. If initially one considers the system $\sum_{1 \leq l \leq s} V_l u_{k,l} = w_k, 1 \leq k \leq m$ instead of (2), then one should introduce a different multiplication of matrices $(a_{l,k})(b_{s,t}) = (\sum_i b_{i,t} a_{l,i})$.

Temporarily we fix $t+1 \le l \le s$. When $\mathcal{R} = \mathcal{A}_n$, in view of Lemma 1 one can find $h_1^{(l)}, \dots, h_t^{(l)}, h^{(l)} \in \mathcal{A}_n$, such that

$$a_k h_k^{(l)} + a_{k,l} h^{(l)} = 0, \quad 1 \le k \le t \tag{4}$$

where $\deg(h_1^{(l)}),\dots,\deg(h_t^{(l)}), \deg(h^{(l)}) \le 16 n^2 m^2 d$. Now we consider the case when $\mathcal{R} = \mathcal{K}_n$. Let $a \in \mathcal{K}_n$ be an element of the form $a_k, a_{k,l}$ and $a = a^{(1)}(a^{(2)})^{-1}$, where $a^{(1)} \in \mathcal{A}_n$, $a^{(2)} \in F[X_1,\dots,X_n]$. Using relations of the form $D_i (a^{(2)})^{-p} = (a^{(2)})^{-p} D_i - p (a^{(2)})^{-p-1}\left(\frac{\partial a^{(2)}}{\partial X_i}\right)$ several times we reduce a to the form $a = (a^{(2)})^{-4nm^3 d} a^{(3)}$ (cf. the estimates of deg(a) obtained above, where $a^{(3)} \in \mathcal{A}_n$ and $\deg(a^{(3)}) \le 16n^2m^6d^2 + 4nm^3 d \le 17 n^2 m^6 d^2$. We reduce all elements $a_k, a_{k,l}$ to the left common denominator $c \in F[X_1,\dots,X_n]$ and get representations $a_k = c^{-1}(a_k^{(3)})$, $a_{k,l} = c^{-1}(a_{k,l}^{(3)})$, where $\deg(a_k^{(3)}), \deg(a_{k,l}^{(3)}) \le 32 n^2 m^7 d^2$. Applying Lemma 1 to the matrix $\begin{pmatrix} a_1^{(3)} & & 0 & a_{1,l}^{(3)} \\ & \ddots & & \vdots \\ 0 & & a_t^{(3)} & a_{t,l}^{(3)} \end{pmatrix}$, we find $h_1^{(l)},\dots,h_t^{(l)}$, $h^{(l)} \in \mathcal{A}_n$, such that (4) holds and $\deg(h_1^{(l)}),\dots,\deg(h_t^{(l)}), \deg(h^{(l)}) \le 128 n^3 m^8 d^2$.

Sec. 2. Solution of Systems of Linear Equations Over the Weyl Algebra

Throughout this section $\mathcal{R} = \mathcal{A}_n$. The next lemma is an analog of the normalization lemma for the Weyl algebra. Below $g_1,\dots,g_t \in \mathcal{A}_n$ is a finite family of elements.

LEMMA 4. There is a nonsingular linear transformation over F of the 2n-dimensional space with basis $X_1, \dots, X_n$, $D_1, \dots, D_n$, under which $X_i \to \Gamma_{X_i} = \sum_j \gamma_{i,j}^{(1,1)} X_j + \sum_j \gamma_{i,j}^{(1,2)} D_j$; $D_i \to \Gamma_{D_i} = \sum_j \gamma_{i,j}^{(2,1)} X_j + \sum_j \gamma_{i,j}^{(2,2)} D_j$, so that $\Gamma_{D_i}\Gamma_{X_i} - \Gamma_{X_i}\Gamma_{D_i} = 1$, $\Gamma_{D_i}\Gamma_{X_j} = \Gamma_{X_j}\Gamma_{D_i}$ for $i \ne j$, $\Gamma_{X_i}\Gamma_{X_j} = \Gamma_{X_j}\Gamma_{X_i}$, $\Gamma_{D_i}\Gamma_{D_j} = \Gamma_{D_j}\Gamma_{D_i}$ (cf. (1)) and in addition for any $1 \le l \le t$ the leading coefficient $0 \ne lc_{D_n}(\tilde{g}_l)$ with respect to D_n belongs to F, where $\tilde{g}_l \in \mathcal{A}_n$ is obtained from g_l with the help of the linear transformation indicated, in order words $\tilde{g}_l = (lc_{D_n}(\tilde{g}_l)) D_n^{\deg(g_l)} + \tilde{\tilde{g}}_l$, where $\deg_{D_n}(\tilde{\tilde{g}}_l) < \deg(g_l)$.

Proof. We consider the matrix $\Gamma = \begin{pmatrix} \Gamma^{(1,1)} & \Gamma^{(1,2)} \\ \Gamma^{(2,1)} & \Gamma^{(2,2)} \end{pmatrix}$, whose rows correspond to linear forms $\Gamma_{X_1},\dots,\Gamma_{X_n}, \Gamma_{D_1},\dots,\Gamma_{D_n}$ in the order listed. Then the relations indicated in the formulation of the lemma are equivalent to Γ belonging to the symplectic group $Sp_{2n}(F)$ ([1, 4]), i.e., satisfying $\Gamma \begin{pmatrix} 0 & -E \\ E & 0 \end{pmatrix} \Gamma^T = \begin{pmatrix} 0 & -E \\ E & 0 \end{pmatrix}$. Let $g_l = \sum_{I,J} \alpha_{I,J} D_n^{i_n} \cdots D_1^{i_1} X_n^{j_n} \cdots X_1^{j_1} + \sum_1$, where all terms of highest degree $i_n + \dots + i_1 + j_n + \dots + j_1 = \deg(g_l)$ are gathered in the left summand, i.e., $\deg(\sum_1) < \deg(g_l)$. Then after performing the linear transformation the leading coefficient $lc_{D_n}(\tilde{g}_l)$ for $D_n^{\deg(g_l)}$ is equal to the expression $\sum_{I,J} \alpha_{I,J} (\gamma_{n,n}^{(2,2)})^{i_n} \cdots (\gamma_{1,n}^{(2,2)})^{i_1} (\gamma_{n,n}^{(1,2)})^{j_n} \cdots (\gamma_1^{(1,2)})^{j_1}$, which one can consider as a homogeneous polynomial in the elements of the last column of Γ. Since the sympletic group acts transitively on all vectors $F^{2n} \setminus \{0\}$ (cf. [4]), one can find a matrix $\Gamma \in Sp_{2n}(F)$ with arbitrarily preassigned nonzero last column. We choose a column such that all the homogeneous polynomials in its elements indicated are nonzero. Then such a matrix Γ satisfies the requirements of the lemma.

We apply Lemma 4 to the family (cf. (4)) of elements $h^{(l)}, t+1 \le l \le s$; the linear transformation Γ obtained preserves (1), so one can consider $\mathcal{A}_n$ as the Weyl algebra on $\Gamma_{X_1},\dots,\Gamma_{X_n}, \Gamma_{D_1},\dots,\Gamma_{D_n}$, and making a change of variables we shall assume that $0 \ne \alpha_l = lc_{D_n}(h^{(l)}) \in F$, $t+1 \le l \le s$. Then one can divide V_l (cf. (3)) from the left by $h^{(l)}$ with remainder (cf. (4)) with respect to D_n in the ring $\mathcal{A}_n$, i.e., $V_l = h^{(l)} \overline{\overline{V}}_l + \overline{V}_l$, where $\overline{\overline{V}}_l, \overline{V}_l \in \mathcal{A}_n$, while $\deg_{D_n}(\overline{V}_l) < \deg_{D_n}(h^{(l)})$. Namely, let $V_l^{(0)} = V_l = \sum_{0 \le i \le p} D_n^i v_i$; $h^{(l)} = \alpha_l D_n^{\mu} + \sum_{0 \le i < \mu} D_n^i h_{l,i}$, where $v_i, h_{l,i} \in \mathcal{A}_{n-1}[X_n]$; one can consider the last ring as a polynomial ring with coefficients from the algebra $\mathcal{A}_{n-1}$ in one variable X_n commuting with it. Let $V_l^{(1)}= V_l^{(0)}-\alpha_l^{-1}h^{(l)}D_n^{\rho-\mu}v_\rho$, so $\rho_1=\deg_{D_n}(V_l^{(1)})\le\rho-1$; in addition $V_l^{(2)}=V_l^{(1)}-\alpha_l^{-1}h^{(l)}D_n^{\rho_1-\mu}\,lc_{D_n}(V_l^{(1)})$, so $\rho_2=\deg_{D_n}(V_l^{(2)})\le\rho_1-1$, etc. By induction on j we prove that $\deg_{D_n}(V_l^{(j)})\le\rho-j$, if $\rho-j\ge\mu-1$; finally, we get $\overline{V}_l=V_l^{(j_0)}$ for suitable j_0 and $\deg_{D_n}(\overline{V}_l)<\deg_{D_n}(h^{(l)})=\mu\le 16n^2m^2d$ (cf. (4) and the estimates after it).

From (3) we subtract (4) multiplied on the right by $\overline{\overline{V}}_l$ for each $r+1\le l\le s$, respectively; we get as a result the following system of equations, which has a solution in $(\mathcal{A}_n)^s$ if and only if (3) and thus (2) have a solution:

$$a_k\overline{V}_k+\sum_{r+1\le l\le s}a_{k,l}\overline{V}_l=b_k,\quad 1\le k\le r. \tag{5}$$

Since $\deg_{D_n}(a_{k,l}\overline{V}_l)\le 4nmd+16n^2m^2d=N_0=(nmd)^{O(1)}$, one has $\deg_{D_n}(\overline{V}_k)\le\deg_{D_n}(a_k\overline{V}_k)\le N_0$ for $1\le k\le r$.

We write each $\overline{V}_j=\sum_{0\le i\le N_0}D_n^i\,\overline{v}_{j,i}$ for $1\le j\le s$ where $\overline{v}_{j,i}\in\mathcal{A}_{n-1}[X_n]$. Then one can replace (5) by an equivalent linear system in the variables $\overline{v}_{j,i}$, $1\le j\le s$, $0\le i\le N_0$ here each equality is replaced by (N_0+1) equalities, namely: if $a_k\overline{V}_k+\sum_{r+1\le l\le s}a_{k,l}\overline{V}_l=\sum_{0\le i\le N_0}D_n^i\sum_{0\le t\le N_0}\overline{a}_{k,i,t}\,\overline{v}_{k,t}+\sum_{0\le i\le N_0}D_n^i\sum_{r+1\le l\le s,}\ \sum_{0\le t\le N_0}\overline{a}_{k,l,i,t}\overline{v}_{l,t}$ and $b_k=\sum_{0\le i\le N_0}D_n^i\,\overline{b}_{k,i}$, where $\overline{a}_{k,i,t}$, $\overline{a}_{k,l,i,t}$, $\overline{b}_{k,i}\in\mathcal{A}_{n-1}[X_n]$, then $\sum_{0\le t\le N_0}\overline{a}_{k,i,t}\,\overline{v}_{k,t}+\sum_{r+1\le l\le s}\ \sum_{0\le t\le N_0}\overline{a}_{k,l,i,t}\,\overline{v}_{l,t}=\overline{b}_{k,i}$ for $0\le i\le N_0$. In addition deg $(\overline{a}_{k,i,t})$, $\deg(\overline{a}_{k,l,i,t})$, $\deg(b_{k,i})\le 4nmd$. Thus we have proved

LEMMA 5. The system (2) is equivalent to a linear system

$$\sum_{1\le l\le N_2}f_{k,l}Z_l=g_k,\quad 1\le k\le m(N_0+1)=N_3 \tag{6}$$

over the ring $\mathcal{A}_{n-1}[X_n]$, where $\deg(f_{k,l})$, $\deg(g_k)$, N_0, $N_3\le(nmd)^{O(1)}$, $N_2\le s(nmd)^{O(1)}$. Moreover, if (6) has a solution $Z_1,\dots,Z_{N_2}\in\mathcal{A}_{n-1}[X_n]$, such that $\deg(Z_l)\le N_1$ for $1\le l\le N_2$, then (2) has a solution $V_1,\dots,V_s\in\mathcal{A}_n$ for which $\deg(V_l)\le N_1+N_0$, $1\le l\le s$.

Thus, Lemma 5 lets one eliminate D_n and pass to the consideration of linear equations over the ring $\mathcal{A}_{n-1}[X_n]$. Now we shall similarly eliminate X_n. To begin we make the observation that Lemma 1 and hence also Lemma 2 are also valid for the ring $\mathcal{A}_{n-1}[X_n]$. One can verify this by following the proof of Lemma 1 and in addition derive it directly from Lemma 1 in the following way. Let A be an $(m-1)\times m$ matrix with elements from the ring $\mathcal{A}_{n-1}[X_n]$, so by Lemma 1 one can find a vector $0\ne b=(b_1,\dots,b_m)\in(\mathcal{A}_n)^m$, such that Ab = 0. We represent each element b_j, $1\le j\le m$ in the form $b_j=\sum_i b_{j,i}D_n^i$, where $b_{j,i}\in\mathcal{A}_{n-1}[X_n]$, while $\deg(b_{j,i})\le\deg(b_j)$ (cf. (1)). Let i_0 be the smallest index such that $b_{j,i_0}\ne 0$ for at least one j. Then $A(b_{1,i_0},\dots,b_{m,i_0})^T=0$, which proves the analog of Lemma 1 for the ring $\mathcal{A}_{n-1}[X_n]$. Applying the construction described above in Sec. 1 to (6) as to (2), we reduce (6) to trapezoidal form (cf. (3)):

$$p_kZ_k+\sum_{r_1+1\le l\le N_2}p_{k,l}Z_l=q_k,\ 1\le k\le r_1, \tag{3$'$}$$

where $p_k, p_{k,l}, q_k\in\mathcal{A}_{n-1}[X_n]$ and r_1 is the rank of the $N_3\times N_2$ matrix $(f_{k,l})$. By Lemma 2 and the observation made above, $\deg(p_k)$, $\deg(p_{k,l})$, $\deg(q_k)\le(nmd)^{O(1)}$.

Further, analogously to (4), in view of Lemma 1 and the observation made above, for each $r_1+1\le l\le N_2$ one can find $y_1^{(l)},\dots,y_{r_1}^{(l)},y^{(l)}\in\mathcal{A}_{n-1}[X_n]$, such that $\deg(y_k^{(l)}),\deg(y^{(l)})\le(nmd)^{O(1)}$ and

$$p_ky_k^{(l)}+p_{k,l}y^{(l)}=0,\ 1\le k\le r_1. \tag{4$'$}$$

Let $g_1',\dots,g_t'\in\mathcal{A}_{n-1}[X_n]$ be a finite family of elements. The next lemma is an analog of Lemma 4.

LEMMA 4′. There exists a nonsingular linear transformation over F of (2n — 1)-dimensional space under which $X_n \to X_n, X_i \to \Delta_{X_i} = X_i + \delta_i^{(1)} X_n, D_i \to \Delta_{D_i} = D_i + \delta_i^{(2)} X_n, 1 \le i \le n-1$, such that $0 \ne lc_{X_n}(\tilde{g}'_k) \in F$ for all $1 \le k \le t$, where $\tilde{g}'_k$ is obtained from g'_k with the help of the linear transformation indicated.

The proof is similar to the proof of Lemma 4. Let $g'_k = \sum_{I,J} \beta_{I,J}^{(k)} D_{n-1}^{i_{n-1}} \ldots D_1^{i_1} X_n^{j_n} X_{n-1}^{j_{n-1}} \ldots X_1^{j_1} + \sum_2$ where all terms of highest degree from g'_k are gathered into the left summand. Then $lc_{X_n}(\tilde{g}'_k) = \sum_{I,J} \beta_{I,J}^{(k)} (\delta_{n-1}^{(2)})^{i_{n-1}} \ldots (\delta_1^{(2)})^{i_1} (\delta_{n-1}^{(1)})^{j_{n-1}} \ldots (\delta_1^{(1)})^{j_1}$. One can find $\delta_1^{(1)}, \ldots, \delta_{n-1}^{(1)}, \delta_1^{(2)}, \ldots, \delta_{n-1}^{(2)} \in F$ such that the leading coefficients indicated are nonzero for all $1 \le k \le t$, which proves the lemma.

We apply Lemma 4′ to the family (cf. (4′)) of elements $y^{(l)}$, $r_1 - 1 \le l \le N_2$; the linear transformation Δ constructed obviously preserves (1), so one can again consider A_{n-1} as the Weyl algebra on $\Delta_{X_1}, \ldots, \Delta_{X_{n-1}}, \Delta_{D_1}, \ldots, \Delta_{D_{n-1}}$, and making a change of variables we shall assume that $0 \ne lc_{X_n}(y^{(l)}) \in F$, $r_1 + 1 \le l \le N_2$.

Similarly to the above, we divide Z_l (cf. (3′)) on the left by $y^{(l)}$ (cf. (4′)) with remainder with respect to X_n for $r_1+1 \le l \le N_2$ in the ring $A_{n-1}[X_n]$, and thus $Z_l = y^{(l)} \bar{Z}_l + \bar{\bar{Z}}_l$, where $deg_{X_n}(\bar{\bar{Z}}_l) < deg_{X_n}(y^{(l)}) \le (nmd)^{O(1)}$ (cf. (4′)). Then from (3′) we subtract (4′) multiplied on the right by $\bar{Z}_l$ for each $r_1+1 \le l \le N_2$ respectively. As a result we get the following system of linear equations which has a solution in $(A_{n-1}[X_n])^{N_2}$ if and only if (3′) and thus (6) have a solution:

$$p_k \bar{Z}_k + \sum_{r_1+1 \le l \le N_2} p_{k,l} \bar{Z}_l = q_k, \quad 1 \le k \le r_1 . \tag{5′}$$

Just as before we estimate $deg_{X_n}(\bar{Z}_k) \le deg_{X_n}(p_k \bar{Z}_k) \le \max_{r_1+1 \le l \le N_2} \{deg_{X_n}(p_{k,l}\bar{Z}_l)\} \le N_5 \le (nmd)^{O(1)}$. Similarly we write $\bar{Z}_j = \sum_{0 \le i \le N_5} X_n^i \bar{Z}_{j,i}$, where $\bar{Z}_{j,i} \in A_{n-1}$, and we replace each of the equations from (5′) by (N_5+1) linear equations in the variables $\bar{Z}_{j,i}$, $1 \le j \le N_2$, $0 \le i \le N_5$ over the ring A_{n-1} (cf. above). Analogously to Lemma 5 one proves the following:

LEMMA 5′. The system (6) is equivalent to a system of linear equations

$$\sum_j f'_{i,j} Y_j = h'_i \tag{6′}$$

over the ring A_{n-1}, where the number of equations and the degrees of all $f'_{i,j}$, h'_i are bounded by $(nmd)^{O(1)}$. In addition if (6′) has a solution $\{Y_j \in A_{n-1}\}$, where $deg(Y_j) \le N_4$ for some N_4 and all j, then (6) has a solution $\{Z_l \in A_{n-1}[X_n]\}$, for which $deg(Z_l) \le N_4 + N_5$, where $N_5 \le (nmd)^{O(1)}$.

To prove the theorem (cf. Introduction), arguing by induction on n one can assume that the theorem is proved for the ring $R = A_{n-1}$ and the system (6′) has a solution $\{Y_j \in A_{n-1}\}$ (if it is solvable over the ring A_{n-1}), such that $\deg(Y_j) \le (nmd)^{c_1 2^{c(n-1)}}$, where the constant c_1 is chosen from the estimates of Lemma 5′ and the constant c from the inductive hypothesis, while by increasing c one can assume that $2c_1 2^{c(n-1)} \le 2^{cn}$. Then it follows from Lemmas 5′ and 5 in succession that (6) and (2) have solutions of degrees at most $(ndm)^{2^{cn}}$, which proves the inductive hypothesis for the ring A_n and thus the theorem for the case of the ring $R = A_n$.

Sec. 3. Solution of Systems of Linear Equations Over the Algebra of Differential Operators

Now we return to consideration of the system (3) over the ring $R = \mathcal{K}_n$. For the element $g = g_1 g_2^{-1} \in \mathcal{K}_n$, where $g_1 = \sum_{0 \le i \le p} D_n^i g_{1,i} = \sum_I D_n^{i_n} \ldots D_1^{i_1} g_{1,I} \in A_n$; $g_{1,I} \in F[X_1, \ldots, X_n]$; $g_{1,i} \in A_{n-1}[X_n]$; $g_{1,p} \ne 0$; $g_2 \in F[X_1, \ldots, X_n]$, the leading coefficient $lc_{D_n}(g) = g_{1,p}\, g_2^{-1} \in \mathcal{K}_{n-1}(F(X_n))$. The next lemma is an analog of Lemma 4. Let $g^{(1)}, \ldots, g^{(t)} \in \mathcal{K}_n$ be a family of operators, $g^{(\ell)} g_2 \in \mathcal{A}_n$.

LEMMA 6. There is a nonsingular linear transformation over F of 2n-dimensional space under which the vector $(D_1, \ldots, D_n)^T \to \Omega(D_1, \ldots, D_n)^T$, where the $n \times n$ matrix $\Omega = (\omega_{i,j})$, the vector $(X_1, \ldots, X_n)^T \to (\Omega^{-1})^T (X_1, \ldots, X_n)^T$, in addition for any $1 \le l \le t$ the leading coefficient $0 \ne lc_{D_n}(\tilde{g}^{(\ell)}) \in F(X_1, \ldots, X_n)$, where $\tilde{g}(\ell)$ is obtained from $g^{(\ell)}$ with the help of the linear transformation indicated.

Proof. Obviously (1) is preserved under the linear transformation indicated. Let g_1 denote one of the elements $g^{(1)}g_2, \ldots, g^{(t)}g_2$; we use the notation introduced before the lemma and write $g_1 = \sum_{I_0} D_n^{i_n} \ldots D_1^{i_1} g_{1,I_0} + \Sigma_3$, where all terms from g_1 with maximal sum $i_n + \ldots + i_1$ are collected into the left summand. Then $lc_{D_n}(\tilde{g}_1) = \sum_{I} (\omega_{n,n})^{i_n} \ldots (\omega_{1,n})^{i_1} \tilde{g}_{1,I_0} \in F[X_1, \ldots, X_n]$. Since $\sum_{I_0} (\omega_{n,n})^{i_n} \ldots (\omega_{1,n})^{i_1} \tilde{g}_{1,I_0} \ne 0$ if and only if $\sum_{I_0} (\omega_{n,n})^{i_n} \ldots (\omega_{1,n})^{i_1} g_{1,I_0} \ne 0$, by considering the coefficient in the last polynomial of a monomial in the variables $X_1, \ldots, X_n$, which occurs in some polynomial g_{1,I_0}, it is easy to prove the existence of $\omega_{n,n}, \ldots, \omega_{1,n}$, for which this coefficient and hence the entire polynomial are different from zero. Consequently one can find a nonzero vector $\omega_{n,n}, \ldots, \omega_{1,n}$ for which the leading coefficients of all $g^{(1)}, \ldots, g^{(t)}$ are different from zero; we supplement it to a nonsingular matrix and this completes the proof of the lemma.

We apply Lemma 6 to the family of operators $h^{(\ell)}$, $r+1 \le \ell \le s$; the linear transformation obtained preserves (1) and in addition both the n-dimensional linear spaces generated by $D_1, \ldots, D_n$ and $X_1, \ldots, X_n$, respectively, so one can consider $\mathcal{K}_n$ as an algebra of operators on a vector of variables $(\Omega^{-1})^T (X_1, \ldots, X_n)$ and a vector of differential operators $\Omega(D_1, \ldots, D_n)$, and making a change of variables we shall assume that $0 \ne lc_{D_n}(h^{(\ell)}) \in F(X_1, \ldots, X_n)$, $r+1 \le \ell \le s$.

Then just as above in Sec. 2 one can divide V_ℓ (cf. (3)) on the left by $h^{(\ell)}$ with remainder with respect to D_n for $r+1 \le \ell \le s$ in the algebra $\mathcal{K}_n$, i.e., $V_\ell = h^{(\ell)} \hat{V}_\ell + \hat{V}_\ell$, where $\hat{V}_\ell, \hat{V}_\ell \in \mathcal{K}_n$ while $deg_{D_n}(\hat{V}_\ell) < deg_{D_n}(h^{(\ell)}) \le (nmd)^{O(1)}$. From (3) we subtract (4) multiplied on the right by $\hat{\hat{V}}_\ell$ for each $r+1 \le \ell \le s$, respectively; we get as a result the following system of equations, which has a solution in $(\mathcal{K}_n)^s$ if and only if (3) and thus (2) have a solution:

$$a_K \hat{V}_K + \sum_{r+1 \le \ell \le s} a_{K,\ell} \hat{V}_\ell = b_K, \quad 1 \le K \le r. \tag{7}$$

Similarly to Sec. 2 we establish the estimates $deg_{D_n}(\hat{V}_K) \le deg_{D_n}(a_K \hat{V}_K) \le max\{deg_{D_n}(a_{K,\ell} \hat{V}_\ell)\} \le \mathcal{N} \le (nmd)^{O(1)}$ for $1 \le K \le r$.

We write $\hat{V}_j = \sum_{0 \le i \le \mathcal{N}} D_n^i \hat{v}_{j,i}$ for $1 \le j \le s$, where $\hat{v}_{j,i} \in \mathcal{K}_{n-1}(F(X_n))$. Then one can replace (7) by an equivalent system of linear equations in the variables $\hat{v}_{j,i}$, $1 \le j \le s$, $0 \le i \le \mathcal{N}$, and here each of the equations of (7) is replaced by $(\mathcal{N}+1)$ equations. Namely, let a be one of the elements of the form $a_K, a_{K,\ell}$, and $\hat{V}$ be the corresponding element $\hat{V}_K, \hat{V}_\ell$, and $a = a^{(1)}(a^{(2)})^{-1}$, where $a^{(1)} \in \mathcal{A}_n$, $a^{(2)} \in F[X_1, \ldots, X_n]$ (cf. end of Sec. 1). Using the relation $(a^{(2)})^{-p} D_n = D_n (a^{(2)})^{-p} + p(a^{(2)})^{-p-1} \left(\frac{\partial a^{(2)}}{\partial X_n}\right)$ several times we reduce aD_n^i to the form $\sum_{0 \le t \le i} D_n^t \alpha_t (a^{(2)})^{-i-1}$, where $\alpha_t \in \mathcal{A}_{n-1}[X_n]$. Consequently, $a\hat{V} = \sum_{0 \le i,t \le \mathcal{N}} D_n^i \beta_{i,t} \hat{v}_t$, where $\beta_{i,t} \in \mathcal{K}_{n-1}(F(X_n))$, and here $deg(\beta_{i,t}) \le (\mathcal{N}+1) deg(a) \le (nmd)^{O(1)}$. Analogously to the proof of Lemma 5 in each of the equations of (7) we equate the coefficients of D_n^i for $0 \le i \le \mathcal{N}$ and we get the $\mathcal{N}+1$ equations required. Thus, we have proved

LEMMA 7. The system (2) is equivalent to a system of linear equations

$$\sum_{1 \le \ell \le \mathcal{N}_2} \beta_{K,\ell} Z_\ell = \alpha_K, \quad 1 \le K \le m(\mathcal{N}+1) = \mathcal{N}_3 \tag{8}$$

over the algebra $\mathcal{K}_{n-1}(F(X_n))$, where $\deg(\beta_{k,\ell}), \deg(\alpha_k), \mathcal{N}, \mathcal{N}_2, \mathcal{N}_3 \leq (nmd)^{O(1)}$. In addition, if system (8) has a solution $Z_1, \ldots, Z_{\mathcal{N}_2} \in \mathcal{K}_{n-1}(F(X_n))$, such that $\deg(Z_\ell) \leq \mathcal{N}_1$ for $1 \leq \ell \leq \mathcal{N}_2$, then (2) has a solution $V_1, \ldots, V_s \in \mathcal{K}_n(F)$, for which $\deg(V_\ell) \leq \mathcal{N}(\mathcal{N}_1 + 1)$, $1 \leq \ell \leq s$.

To prove the theorem (cf. Introduction), arguing by induction on n one can assume that (8) has a solution $Z_1, \ldots, Z_{\mathcal{N}_2} \in \mathcal{K}_{n-1}(F(X_n))$ (if it is solvable over the algebra $\mathcal{K}_{n-1}(F(X_n))$, such that $\deg(Z_\ell) \leq (nmd)^{c_2 2^{c_0(n-1)}}$, $1 \leq \ell \leq \mathcal{N}_2$, where the constant c_2 is chosen from the estimates of Lemma 7 and the constant c_0 from the inductive hypothesis, while by increasing c_0, one can assume that $2c_2 2^{c_0(n-1)} \leq 2^{c_0 n}$. Then it follows from Lemma 7 that system (2) has a solution of degree at most $(nmd)^{2^{c_0 n}}$, which proves the inductive hypothesis. We also note that the base of the induction for the field $\mathcal{K}_0(F(X_1, \ldots, X_n)) = F(X_1, \ldots, X_n)$ follows from the estimates on determinants over this field. This completes the proof of the theorem for the case of the ring $\mathcal{R} = \mathcal{K}_n(F)$.

REFERENCES

1. E. Artin, Geometric Algebra [Russian translation], Nauka, Moscow (1969).
2. D. Yu. Grigor'ev, "Decomposition of polynomials over a finite field and solution of systems of algebraic equations," Zapiski Nauchn. Semin. Leningr. Otdel. Mat. Inst., **137**, 20-79 (1984).
3. D. Yu. Grigor'ev, "Complexity of factorization and calculation of the g.c.d. of linear ordinary differential operators," Zap. Nauchn. Semin. Leningr. Otdel. Mat. Inst., **176**, 68-103 (1989).
4. J. Dieudonne, Geometry of the Classical Groups [Russian translation], Mir, Moscow (1974).
5. A. L. Chistov, "Algorithm of polynomial complexity for decomposing polynomials and finding components of a variety in subexponential time," Zap. Nauchn. Semin. Leningr. Otdel. Mat. Inst., **137**, 124-188 (1984).
6. J.-E. Björk, Rings of Differential Operators, North-Holland (1979).
7. D. Yu. Grigor'ev, "Computational complexity in polynomial algebra," in: Proc. Intern. Congress Math., Vol. 2, Berkeley (1986), pp. 1452-1460.
8. A. Galligo, "Some algorithmic questions on ideals of differential operators," Lect. Notes Comput. Sci., **204**, 413-421 (1985).
9. N. Fitch and A. Galligo, "Nullstellensatz effectif et conjecture de Serre (theoreme de Quillen-Suslin) pour le calcul formel," in: Seminaire "Structures algebriques ordonnees," Paris, VII (1988).
10. E. Mayr and A. Meyer, "The complexity of the word problem for commutative semigroups and polynomial ideals," Adv. Math., **46**, 305-329 (1982).
11. A. Seidenberg, "Constructions in algebra," Trans. Amer. Math. Soc., **197**, 273-313 (1974).