

# Complexity of Irreducibility Testing for a System of Linear Ordinary Differential Equations

D. Yu. Grigoriev

Leningrad Department of Mathematical V. A. Steklov  
Institute of Academy of Sciences of the USSR  
Fontanka 27, Leningrad, 191011, USSR

## Abstract

Let a system of linear ordinary differential equations of the first order  $Y' = AY$  be given, where  $A$  is  $n \times n$  matrix over a field  $F(X)$ , assume that the degree  $\deg_X(A) < d$  and the size of any coefficient occurring in  $A$  is at most  $M$ . The system  $Y' = AY$  is called reducible if it is equivalent (over the field  $\bar{F}(X)$ ) to a system  $Y'_1 = A_1 Y_1$  with a matrix  $A_1$  of the form

$$A_1 = \begin{pmatrix} A_{1,1} & 0 \\ A_{2,1} & A_{2,2} \end{pmatrix}$$

An algorithm is described for testing irreducibility of the system with the running time  $\exp(M(d2^n)^{d2^n})$ .

## Introduction

Let a system of linear ordinary differential equations of the first order be given

$$Y' = AY \tag{1}$$

where  $A = (a_{i,j}/a)$  is a  $n \times n$  matrix over a field  $F(X)$  and the polynomials  $a_{i,j}$ ,  $a \in F[X]$ , here a field  $F = \mathbb{Q}(\delta_1, \dots, \delta_e)[\eta]$  where the elements  $\delta_1, \dots, \delta_e$  are algebraically independent over  $\mathbb{Q}$ , the element  $\eta$  is algebraic over the field  $\mathbb{Q}(\delta_1, \dots, \delta_e)$  and  $\varphi(Z) \in \mathbb{Q}[\delta_1, \dots, \delta_e][Z]$  is its minimal polynomial, lastly  $Y = (y_1, \dots, y_n)^T$  is the vector of unknowns. For a rational number  $\alpha/\beta \in \mathbb{Q}$ , where  $\alpha, \beta$  are reciprocally prime, define its bit-size as  $l(\alpha/\beta) = \lceil \log_2(|\alpha\beta| + 2) \rceil$ . Define bit-size  $l(\varphi)$  as the maximal of bit-sizes of all rational coefficients occurring in  $\varphi$  (cf. [CG 83], [Gr 86]). Assume that the degrees  $\deg_Z(\varphi) < d_1$ ,  $\deg_{\delta_1, \dots, \delta_e}(\varphi) < d_0$  and  $l(\varphi) \leq M$ , then we say that  $\varphi$  satisfies  $(d_1, d_0, M)$ -bound.

We suppose furthermore that the elements  $a_{i,j}$ ,  $a$  satisfy  $(d, d_0, M)$ -bound.

An algebraic closure  $\bar{F}$  is regarded in sequel as a field of constants. One can deem that the field  $\bar{F}$  is embedded in the field  $\mathbb{C}$ . Denote by  $G = \text{Gal}(A/\bar{F}(X))$  the differential Galois group of system (1) (see e. g. [Ka 57]). Let  $V$  be a space of all solutions of system (1). It is well known that  $V$  is  $n$ -dimensional space over the field  $\bar{F}$ ; moreover if the vectors  $v_1, \dots, v_s \in V$  are linearly independent over  $\bar{F}$  then  $v_1, \dots, v_s$  are also linearly independent over an arbitrary field ([CL 55]). The group  $G$  acts on the vectors from  $V$  componentwise. A subspace (here and further all the subspaces are considered over the field  $\bar{F}$ )  $W \subset V$  is called invariant if  $W$  is invariant under the action of  $G$ . We write the vectors from  $V$  as columns.

**Lemma 1** *A subspace  $W \subset V$  of dimension  $k$  is invariant iff there exists  $(n-k) \times n$  matrix  $B$  of the rank  $(n-k)$  with the entries from the field  $\bar{F}(X)$  such that  $BW = 0$  (we call  $B$  an annihilating matrix for  $W$ ).*

**PROOF:** Assume the existence of the required matrix  $B$ . Consider a subspace  $W' = \{w \in V | Bw = 0\}$ . Then  $W' \subset W$  and  $W'$  is invariant, on the other hand  $\dim(W') \leq k$  since  $\text{rk}(B) = n - k$ , therefore  $W' = W$  and  $W$  is invariant.

Conversely, suppose that  $W$  is invariant. Following Proposition 1.5 ([BBH 88]) consider  $n \times k$  matrix  $\Omega$  with the columns constituting a certain basis of the space  $W$ . Pick out some nonsingular  $k \times k$  submatrix  $\omega$  of the matrix  $\Omega$ . For every element  $g \in G$  there exists nonsingular  $k \times k$  matrix  $C_g$  with the entries from  $\bar{F}$  such that the action of  $g$  on  $\Omega$  coincides with the right multiplying on  $C_g$ , i. e.  $g \times \Omega = \Omega C_g$ , henceforth  $g \times \omega = \omega C_g$ . Therefore

$$\begin{aligned} g \times (\Omega \omega^{-1}) &= (g \times \Omega)(g \times \omega^{-1}) \\ &= \Omega C_g C_g^{-1} \omega^{-1} \\ &= \Omega \omega^{-1}, \end{aligned}$$

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

thus all the entries of the matrix  $\Omega\omega^{-1}$  belong to  $\bar{F}(X)$ . Henceforth, there exists  $(n-k) \times n$  matrix  $B$  over the field  $\bar{F}(X)$  of the rank  $(n-k)$ , such that  $B\Omega\omega^{-1} = 0$ , q. e. d.

System (1) is said to be equivalent to a system  $Y'_1 = A_1 Y_1$  if there exists a nonsingular  $n \times n$  matrix  $B_1$  over  $\bar{F}(X)$  such that for the space  $V_1$  of the solutions to the system  $Y'_1 = A_1 Y_1$  holds  $V_1 = B_1 V$ ; then  $A_1 = B'_1 B_1^{-1} + B_1 A B_1^{-1}$ . One can show that an invariant  $k$ -dimensional subspace  $W \subset V$  exists iff there is a system  $Y'_1 = A_1 Y_1$  equivalent to (1) such that the matrix  $A_1$  has a block-lowertriangular form

$$A_1 = \begin{pmatrix} A_{1,1} & 0 \\ A_{2,1} & A_{2,2} \end{pmatrix} \quad (2)$$

where  $A_{2,2}$  is  $k \times k$  matrix. Indeed, if  $A_1$  has a form (2) then we can consider  $k$ -dimensional space  $\tilde{W}_1$  of the solutions of the system  $\tilde{Y}'_1 = A_{2,2} \tilde{Y}_1$ . Then the space  $W_1$  consisting of all the vectors with  $n$  coordinates, obtained from the vectors of the space  $\tilde{W}_1$  by padding zeroes as the first  $(n-k)$  coordinates, is a subspace  $W_1 \subset V_1$ . Furthermore, for  $(n-k) \times n$  matrix  $B_0 = (E0)$ , where  $E$  is unit  $(n-k) \times (n-k)$  matrix, holds  $B_0 W_1 = 0$ , whence Lemma 1 implies that  $W_1$  is an invariant  $k$ -dimensional subspace. Then  $W = B_1^{-1} W_1 \subset V$  is an invariant  $k$ -dimensional subspace.

Conversely, let  $W \subset V$  be an invariant  $k$ -dimensional subspace and  $B$  be an annihilating  $(n-k) \times n$  matrix. Consider an arbitrary nonsingular  $n \times n$  matrix  $B_1$  of the form  $B_1 = \begin{pmatrix} B \\ B_2 \end{pmatrix}$  with the entries from  $\bar{F}(X)$ . Then the space  $B_1 W \subset B_1 V = V_1$  is contained in the subspace of the vectors with vanishing first  $(n-k)$  coordinates. Since the derivative  $(B_1 W)'$  is also contained in the latter subspace, the matrix  $A_1$  has the form (2) that was to be proved. System (1) is called *irreducible* iff  $V$  has no proper invariant subspace.

The main statement of the paper is the following

**Theorem** *There is an algorithm recognizing irreducibility of a system (1) and constructing an annihilating matrix  $B$ , provided (1) is reducible, such that*

$$\deg_X(B) \leq N \leq \exp((M + d_0 e)(d2^n)^{O(d2^n)} d_1^{O(2^n)}).$$

Moreover, the algorithm produces a field

$$F_1 \simeq \mathbb{Q}(\delta_1, \dots, \delta_e)[Z]/(\varphi_1) \supset F$$

being a finite extension of  $F$ , by means of specifying an irreducible polynomial  $\varphi_1 \in \mathbb{Q}[\delta_1, \dots, \delta_e][Z]$ , such that every entry of  $B$  belongs to  $F_1(X)$ . Besides,  $\varphi_1$  and  $B$  satisfy  $(d_1(Ndn)^{O(n^2)}, d_0((Ndn)^{n^2} d_1)^{O(1)}, (M +$

$d_0 e)((Ndn)^{n^2} d_1)^{O(1)})$  - bounds. Furthermore, the running time of the algorithm does not exceed a suitable polynomial in  $M, ((Ndn)^{n^2} d_1 d_0)^{n^2 + e}$ .

REMARK:

1. By virtue of the shown beforehand one can yield a system  $Y'_1 = A_1 Y_1$  equivalent to (1) whose matrix  $A_1$  has the form (2) with the bounds on  $A_1$  and time-bounds as in the theorem.
2. The theorem generalizes the result [Gr 90] where an algorithm for factoring a linear differential operator is designed, for the case of a system of linear differential equations of the first order. Similar to [Gr 90] one can produce a system  $Y'_0 = A_0 Y_0$  equivalent to (1) having a block-lowertriangular form

$$A_0 = \begin{pmatrix} A_{1,1} & & & \\ A_{2,1} & A_{2,2} & & 0 \\ \vdots & & \ddots & \\ A_{s,1} & \dots & & A_{s,s} \end{pmatrix}$$

where  $s$  is the maximal possible, i. e. for each  $1 \leq i \leq s$  the system  $Y'_i = A_{i,i} Y_i$  of the size  $k_i$  is irreducible. Observe that the set of integers  $\{k_1, \dots, k_s\}$  is uniquely determined, since these numbers are the dimensions of the factors of Jordan-Gölder tower of  $G$ -module  $V$  ([La 65]).

Notice that if system (1) is irreducible then it satisfies, in particular, the Siegel normality condition ([BBH 88]), which was involved by him for yielding the families of algebraically independent numbers.

Briefly about the further contents of the paper. In section 1 the problem of estimating the degree of an annihilating matrix  $\deg_X(B)$  (see Lemma 1) is reduced to the same problem in one-dimensional case  $\dim(W) = 1$  involving the construction of the exterior  $k$ -th power of system (1). In section 2 a bound on  $\deg_X(B)$  is ascertained for one-dimensional case based on the bounds for the factors of a linear ordinary differential operator achieved in sections 1, 2 ([Gr 90]). In the last section 3 a reduction of recognizing irreducibility of system (1) to solving an appropriate system of polynomial equations of a special form, regarded in section 3 ([Gr 90]) by designing an algorithm for factoring a linear differential operator is made.

## 1 Reduction of estimating the degree of annihilating matrix to one-dimensional case

We describe the construction of  $p$ -th exterior power  $\wedge^p(A)$  of system (1),  $1 \leq p \leq n$ , namely a system

of linear differential equations of the first order, with the space of solutions being isomorphic to  $\bigwedge^p(V)$ . System  $\bigwedge^p(A)$  has a size  $\binom{n}{p}$ , the vector of unknowns  $Z = (\{z_I\}_{I=(i_1, \dots, i_p)})^T$  where  $z_I$  can be written in a form  $z_I = y_{i_1} \wedge \dots \wedge y_{i_p}$ ,  $1 \leq i_1 < \dots < i_p \leq n$  (recall that  $Y = (y_1, \dots, y_n)^T$  is the vector of unknowns of system (1)). Denote by  $A^{(i)}$   $i$ -th row of the matrix  $A$ . Calculate the derivative  $z'_I = y'_{i_1} \wedge y_{i_2} \wedge \dots \wedge y_{i_p} + y_{i_1} \wedge y'_{i_2} \wedge \dots \wedge y_{i_p} + \dots + y_{i_1} \wedge \dots \wedge y'_{i_p} = (A^{(i_1)}Y) \wedge y_{i_2} \wedge \dots \wedge y_{i_p} + y_{i_1} \wedge (A^{(i_2)}Y) \wedge \dots \wedge y_{i_p} + \dots + y_{i_1} \wedge \dots \wedge (A^{(i_p)}Y) = \sum_J \alpha_{I,J} z_J$ . Here in the last equality the usual rule of signs alternating by permutation of multipliers in the exterior product is applied. Then we set a matrix of the system  $\bigwedge^p(A)$  to be equal to  $(\alpha_{I,J})_{I,J}$ .

One can show that the space of solutions of the system  $\bigwedge^p(A)$  coincides with  $\bigwedge^p(V)$ . Indeed, it suffices to check up that any vector from  $\bigwedge^p(V)$  satisfies the system  $\bigwedge^p(A)$ , since  $\dim \bigwedge^p(V) = \binom{n}{p}$ . Let  $u_1, \dots, u_p \in V$  and consider  $n \times p$  matrix  $U$  whose columns are  $u_1, \dots, u_p$ , denote its rows by  $u^{(1)}, \dots, u^{(n)}$ . Then the coordinate of the vector  $u_1 \wedge \dots \wedge u_p \in \bigwedge^p(V)$ , corresponding to  $z_I$  equals to  $\det(u^{(i_1)}, \dots, u^{(i_p)})$ . Taking into account an equality  $(\det(u^{(i_1)}, \dots, u^{(i_p)}))' = \det((u^{(i_1)})', u^{(i_2)}, \dots, u^{(i_p)}) + \det(u^{(i_1)}, (u^{(i_2)})', \dots, u^{(i_p)}) + \dots + \det(u^{(i_1)}, \dots, (u^{(i_p)})') = \det(A^{(i_1)}U, u^{(i_2)}, \dots, u^{(i_p)}) + \det(u^{(i_1)}, A^{(i_2)}U, \dots, u^{(i_p)}) + \dots + \det(u^{(i_1)}, \dots, A^{(i_p)}U)$ , we deduce the required statement. Observe that the matrix  $(\alpha_{I,J})$  satisfies  $(d, d_0, M + \log_2 p)$ -bound.

**Lemma 2** *Let  $W \subset V$  be an invariant subspace for system (1). Then  $\bigwedge^p(W) \subset \bigwedge^p(V)$  is also an invariant subspace for the system  $\bigwedge^p(A)$ .*

**PROOF:** One can assume w. l. o. g. (permuting columns and rows in the initial matrix  $A$  if necessary) that the columns  $B_{k+1}, \dots, B_n$  of the annihilating matrix  $B$  of the subspace  $W$  constitute a basis over the field  $\bar{F}(X)$  of the space of all its columns. Then for the rows  $\Omega^{(j)}$ ,  $k+1 \leq j \leq n$  of the matrix  $\Omega$  (see the proof of Lemma 1) hold  $\Omega^{(j)} = \sum_{1 \leq i \leq k} p_{j,i} \Omega^{(i)}$  for the suitable  $p_{j,i} \in \bar{F}(X)$ . Therefore the rows of  $\binom{n}{p} \times \binom{k}{p}$  matrix  $\bigwedge^p(\Omega)$ , whose columns being the exterior products of all possible subsets of  $p$  columns among the columns of the matrix  $\Omega$ , are linear over  $\bar{F}(X)$  combinations of the rows of the matrix  $\bigwedge^p(\Omega)$  which correspond to the coordinates  $z_I$  for all  $I = (i_1, \dots, i_p)$  where  $1 \leq i_1 < \dots < i_p \leq k$ . Henceforth, there exists an annihilating  $(\binom{n}{p} - \binom{k}{p}) \times \binom{n}{p}$  matrix  $\bar{B}$  with the entries from  $\bar{F}(X)$  with the rank  $\binom{n}{p} - \binom{k}{p}$  such that  $\bar{B} \bigwedge^p(\Omega) = 0$ , i. e.  $\bar{B} \bigwedge^p(W) = 0$ . This and Lemma 1 entail that  $\bigwedge^p(W)$  is invariant, q. e. d.

**REMARK:** In the case  $p = k$   $(\binom{n}{k} - 1) \times \binom{n}{k}$  matrix  $\bar{B}$  has the rank  $\binom{n}{k} - 1$ , therefore for each pair

$1 \leq i \leq k$ ,  $k+1 \leq j \leq n$  one can find a linear over  $\bar{F}(X)$  combination of the rows of  $\bar{B}$  which equals to a vector with exactly two nonlinear coordinates, corresponding to the multiindices  $(1, \dots, k)$  and  $(1, \dots, i-1, i+1, \dots, k, j)$ . Then the quotient of these two coordinates equals to  $p_{j,i}$ . Henceforth, for estimating  $\deg_X(p_{j,i})$  it suffices to estimate  $\deg_X(\bar{B})$ . On the other hand as an annihilating matrix for  $W$  one can take  $(n-k) \times n$ -matrix  $((p_{j,i})_{k+1 \leq j \leq n, 1 \leq i \leq k} E)$  where  $E$  is the unit  $(n-k) \times (n-k)$  matrix. Thus, we have reduced the problem of estimating the degree (with respect to  $X$ ) of an annihilating matrix to the problem of estimating  $\deg_X(\bar{B})$  for annihilating matrix of one-dimensional subspace  $\bigwedge^k(W)$ .

## 2 A bound on the degree of an annihilating matrix in one-dimensional case

Assume in this section that  $\dim W = 1$  and  $0 \neq (w_1, \dots, w_n)^T \in W$ . For any  $g \in G$  holds  $g \times w = c_g w$  for an appropriate  $c_g \in \bar{F}$ , therefore  $w'_i/w_i \in \bar{F}(X)$ ,  $1 \leq i \leq n$  (see [Si 81], also [Gr 90]). On the other hand for each  $1 \leq i \leq n$  one can easily yield a linear ordinary differential operator  $R_i \in F[X, \frac{d}{dX}]$ , such that  $R_i w_i = 0$  (cf. [Gr 90]). Indeed, it is possible to express successively the derivatives

$$w'_i = A^{(i)} w, w''_i = (A^{(i)})' w + A^{(i)} A w, \dots$$

So the  $s$ -th derivative

$$w_i^{(s)} = \mathcal{A}^{(s)} w, s \geq 1$$

for the suitable vectors  $\mathcal{A}^{(s)} \in (F(X))^n$  and  $\mathcal{A}^{(s)}$  satisfies  $(sd, sd_0, (M + ed_0 + \log n)(sdd_1)^{O(1)})$ -bound (cf. [CG 83]). Henceforth, there exists a vector

$$0 \neq r = (r_0, \dots, r_n) \in (F[X])^{n+1},$$

for which  $\sum_{0 \leq s \leq n} r_s \mathcal{A}^{(s)} = 0$  and  $r$  satisfies  $(dn^2, d_0 n^2, (M + ed_0)(dd_1 n)^{O(1)})$ -bound. Then we set

$$R_i = \sum_{0 \leq s \leq n} r_s \frac{d^s}{dX^s}.$$

Whence in force of Lemma 6 ([Gr 90]) for the rational function  $w'_i/w_i$  the following bounds are fulfilled:  $\deg_X(w'_i/w_i), \sum_{\gamma \in \bar{F}} \exp(l(\text{res}_\gamma(w'_i/w_i))) \leq N_0 \leq \exp((M + ed_0)((dn)^{dn^2} d_1^n)^{O(1)})$ , where  $l(\text{res}_\gamma(w'_i/w_i))$  denotes the bit-size (see beginning of the introduction)

of the residue in the point  $\gamma \in \bar{F}$  of the rational function  $w'_i/w_i$ , herewith the bit-size is considered in a relevant field  $\bar{F}$ , produced in Lemma 6 ([Gr 90]), being a finite extension of  $F$ , such that  $\text{res}_\gamma(w'_i/w_i) \in \bar{F}$  for all  $1 \leq i \leq n$ ,  $\gamma \in \bar{F}$ ; finally, the summation ranges over all the points  $\gamma \in \bar{F}$ .

Moreover, for a decomposition in a sum of partial fractions

$$w'_i/w_i = q_i + \sum_j m_{i,j}(X - \beta_{i,j})^{-1} + S_i,$$

where  $q_i \in \bar{F}[X]$  and in  $S_i$  occur only the powers  $(X - \beta)^{-\kappa}$  with  $\kappa \geq 2$ , hold the bounds  $\deg(q_i)$ ,  $\sum_j \exp(l(m_{i,j})) \leq N_0$  (see [Si 81], [Gr 90]). Lemma 1 implies that  $w_{i_1}/w_{i_2} \in \bar{F}(X)$  for all  $1 \leq i_1, i_2 \leq n$ . Therefore  $w_{i_1}/w_{i_2} = \exp \int (\sum_{j_1} m_{i_1,j_1}(X - \beta_{i_1,j_1})^{-1} - \sum_{j_2} m_{i_2,j_2}(X - \beta_{i_2,j_2})^{-1}) = \prod_{j_1} (X - \beta_{i_1,j_1})^{m_{i_1,j_1}} \prod_{j_2} (X - \beta_{i_2,j_2})^{-m_{i_2,j_2}}$ .

If  $\beta_{i_1,j_1} = \beta_{i_2,j_2}$  for some  $j_1, j_2$  then the number  $m_{i_1,j_1} - m_{i_2,j_2}$  is an integer. Henceforth,  $\deg_X(w_{i_1}/w_{i_2}) \leq 2N_0$ . Thus, the following Lemma is proved.

**Lemma 3** *Let  $W \subset V$  be one-dimensional invariant subspace for system (1). There exists an annihilating  $(n-1) \times n$  matrix  $\bar{B}$  of the rank  $n-1$  over the field  $\bar{F}(X)$  such that*

$$\deg_X(\bar{B}) \leq \exp((M + ed_0)((dn)^{dn^2} d_1^n)^{O(1)}).$$

**Corollary** *Let  $W \subset V$  be  $k$ -dimensional invariant subspace for system (1). There exists an annihilating  $(n-k) \times n$  matrix  $B$  of the rank  $n-k$  over  $\bar{F}(X)$  such that  $\deg_X(B) \leq \exp((M + ed_0)((d2^n)^{d2^{2n}} d_1^{2^n})^{O(1)})$ .*

The corollary follows from Lemmas 2, 3 with the help of the remark after Lemma 2, taking into account the inequality  $\binom{n}{k} < 2^n$ .

### 3 Recognizing irreducibility of a linear system

Fix a certain  $1 \leq k < n$  and find out, whether there exists an invariant subspace  $W \subset V$  of the dimension  $k$ . One can deem w. l. o. g. that a corresponding annihilating matrix  $B$  (after an appropriate columns permutating) has a trapezium form

$$\begin{pmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_{n-k} \end{pmatrix} \begin{pmatrix} (b_{i,j}) \end{pmatrix} \quad (3)$$

where  $b_i, b_{i,j} \in \bar{F}[X]$  and  $\deg_X(b_i), \deg_X(b_{i,j}) \leq N$ , where  $N$  satisfies a bound of the same type as in the

corollary to Lemma 3. Then in  $n \times k$  matrix  $\Omega = (w_{i,j})$  of the rank  $k$  its  $k \times k$  submatrix, consisting of the last  $k$  rows, is nonsingular (see the introduction). Thus, the existence of the subspace  $W \subset V$  is equivalent to the existence of an annihilating matrix  $B$  of the form (3). Later on we reformulate the latter condition in terms of solvability of a suitable system of polynomial equations and inequalities.

We assume for conveniency of notations that  $\deg_X(b_i) = N$ ,  $\deg_X(b_{i,j}) \leq 2N$ ,  $1 \leq i \leq n-k$ ,  $n-k+1 \leq j \leq n$  and that the leading coefficients  $lc_X(b_i) = 1$ ,  $1 \leq i \leq n-k$  multiplying if necessary the rows of the matrix  $B$  by appropriate monomials in the variable  $X$ . Write down  $b_i = X^N + \sum_{0 \leq s < N} b_i^{(s)} X^s$ ,  $b_{i,j} = \sum_{0 \leq s < 2N} b_{i,j}^{(s)} X^s$ ,  $1 \leq i \leq n-k < j \leq n$  where  $b_i^{(s)}, b_{i,j}^{(s)}$  are some indeterminates. Introduce one more indeterminate  $c$  and impose on it the requirement  $a(c) \neq 0$  (see (1)). Then (considering  $c$  as an element of the field  $\bar{F}$ , we'll do it sometimes and sometimes we consider  $c$  as an indeterminate, it would not confuse us) the point  $c$  is regular for system (1), and one write a regular solution  $y = \sum_{i \geq 0} y^{(i)}(X - c)^i$ , where  $y^{(i)} \in \bar{F}^n$  and the vector  $y^{(0)} \neq 0$  can be chosen in an arbitrary way ([CL 55]). Represent the matrix  $A = \sum_{i \geq 0} A^{(i)}(X - c)^i$  where the entries of  $A^{(i)}$  belong to the field  $F(c)$  and satisfy  $(di, d_0 id_1^{O(1)}(M + ed_0 + d + n)id_1^{O(1)})$ -bounds. Furthermore

$$y^{(i)} = i^{-1} \sum_{0 \leq j \leq i-1} A^{(j)} y^{(i-j-1)} = P^{(i)} y^{(0)}$$

where  $P^{(i)}$  is a matrix over  $F(c)$  with the entries satisfying  $(di, d_0 id_1^{O(1)}, (M + ed_0 + d + n)(id_1)^{O(1)})$ -bounds, this can easily be proved by induction on  $i$ .

Introduce, lastly more  $kn$  indeterminates  $y_{1,1}^{(0)}, \dots, y_{1,n}^{(0)}, \dots, y_{k,1}^{(0)}, \dots, y_{k,n}^{(0)}$  for the coordinates of the vectors  $y_1^{(0)}, \dots, y_k^{(0)}$  respectively, and for each of these vectors  $y_j^{(0)}$  the algorithm yields  $n$  first terms of expanding in series of a solution  $z_j = \sum_{i \geq 0} y_j^{(i)}(X - c)^i$  of system (1). Impose the condition of linear independence over  $\bar{F}$  of the vectors  $y_1, \dots, y_k$ . This is equivalent (taking into account that  $c$  is a regular point for system (1), see [CL 55]) to the condition that  $n \times k$  matrix, constituted from the vectors  $y_1^{(0)}, \dots, y_k^{(0)}$ , has the rank  $k$  (the algorithm tests the latter condition looking over all  $k \times k$  submatrices of this matrix). Let  $y_1, \dots, y_k$  span over  $\bar{F}$  a subspace  $W$ .

Finally, we have to impose the condition  $BW = 0$ . For the time being fix some row  $B^{(m)}$ ,  $1 \leq m \leq n-k$  of the matrix  $B$ . The algorithm produces a linear ordinary differential operator  $0 \neq Q_m \in F[b_m^{(0)}]$ ,

$\dots, b_{m,n-k+1}^{(N-1)}, b_{m,n-k+1}^{(0)}, \dots, b_{m,n-k+1}^{(2N)}, \dots, b_{m,n}^{(0)}, \dots, b_{m,n}^{(2N)}][X, \frac{d}{dX}]$  of the order at most  $n$ , such that for any solution  $y = (y_1, \dots, y_n)^T$  of system (1) holds  $Q_m(B^{(m)}y) = 0$ . Indeed, expressing successively the derivatives  $(B^{(m)}y)' = (B^{(m)})'y + B^{(m)}Ay$ ,  $(B^{(m)}y)'' = ((B^{(m)})' + B^{(m)}A)'y + ((B^{(m)})' + B^{(m)}A)Ay$ , ... we conclude that  $s$ -th derivative  $(B^{(m)}y)^{(s)} = t^{(s)}y$ ,  $s \geq 1$  for a suitable vector  $t^{(s)} \in (F[b_m^{(0)}, \dots, b_m^{(N-1)}, b_{m,n-k+1}^{(0)}, \dots, b_{m,n-k+1}^{(2N)}, \dots, b_{m,n}^{(0)}, \dots, b_{m,n}^{(2N)}](X))^n$  satisfying the following bounds:

$$\deg_X(t^{(s)}) \leq N + ds,$$

$$\deg_{b_m^{(0)}, \dots, b_m^{(2N)}}(t^{(s)}) \leq 1,$$

$$\deg_{\delta_1, \dots, \delta_e}(t^{(s)}) \leq d_0 s d_1^{O(1)},$$

$$l(t^{(s)}) \leq (M + ed_0 + \log N + d + n)(d_1 s)^{O(1)}$$

which one can ascertain by induction on  $s$ . There exist polynomials  $q_m^{(0)}, \dots, q_m^{(n)} \in F[b_m^{(0)}, \dots, b_m^{(N-1)}, b_{m,n-k+1}^{(0)}, \dots, b_{m,n-k+1}^{(2N)}, \dots, b_{m,n}^{(0)}, \dots, b_{m,n}^{(2N)}][X]$  such that  $\sum_{0 \leq s \leq n} q_m^{(s)} t^{(s)} = 0$ , then set an operator  $Q_m = \sum_{0 \leq s \leq n} q_m^{(s)} \frac{d^s}{dX^s}$  and applying the well known bounds on the size of the determinant (see e. g. [CG 83]) we get the following bounds:

$$\deg_X(Q_m) \leq (N + dn)n, \deg_{b_m^{(0)}, \dots, b_m^{(2N)}}(Q_m) \leq n,$$

$$\deg_{\delta_1, \dots, \delta_e}(Q_m) \leq d_0 n^2 d_1^{O(1)},$$

$$l(Q_m) \leq (M + ed_0 + \log N + d)(nd_1)^{(1)}.$$

Impose also the requirement that the point  $c$  is a regular for the operators  $Q_1, \dots, Q_{n-k}$ , namely write down the inequalities  $lc_{\frac{d}{dX}}(Q_m)(c) \neq 0, 1 \leq m \leq n - k$ .

Thereupon the algorithm yields the first  $n$  terms of the expansions of each of regular functions

$$B^{(m)}y_j = \sum_{i \geq 0} \xi_{j,i}^{(m)}(X - c)^i, 1 \leq m \leq n - k, 1 \leq j \leq k,$$

where  $\xi_{j,i}^{(m)} \in F[b_m^{(0)}, \dots, b_m^{(N-1)}, b_{m,n-k+1}^{(0)}, \dots, b_{m,n-k+1}^{(2N)}, \dots, b_{m,n}^{(0)}, \dots, b_{m,n}^{(2N)}][y_{j,1}^{(0)}, \dots, y_{j,n}^{(0)}](c)$  for  $i < n$  satisfy the following bounds:

$$\deg_{b_m^{(0)}, \dots, b_m^{(2N)}}(\xi_{j,i}^{(m)}) \leq 1,$$

$$\deg_{y_{j,1}^{(0)}, \dots, y_{j,n}^{(0)}}(\xi_{j,i}^{(m)}) \leq 1,$$

$$\deg_c(\xi_{j,i}^{(m)}) \leq N + dn,$$

$$\deg_{\delta_1, \dots, \delta_e}(\xi_{j,i}^{(m)}) \leq d_0 n d_1^{O(1)},$$

$$l(\xi_{j,i}^{(m)}) \leq (M + ed_0 + d + N)(d_1 n)^{O(1)}$$

taking into account obtained beforehand bounds for the entries of the matrices  $P^{(i)}$ . Observe that if the equalities  $\xi_{j,i}^{(m)} = 0$  are fulfilled for all  $0 \leq i < n$  then  $B^{(m)}y_j = 0$ , since the point  $c$  is regular for the operator  $Q_m$  (see [CL 55] and also the corollary to Lemma 7 in [Gr 90]). Thus the following Lemma is proved similar to Lemma 8 in [Gr 90]).

**Lemma 4** System (1) has an invariant  $k$ -dimensional subspace  $W \subset V$  of solutions iff there exists an annihilating matrix  $B$  of the form (3) (after a suitable columns permutation) over the ring  $\bar{F}[X]$  of the degree at most  $2N$ , besides that there exists  $n \times k$  matrix  $(y_1^{(0)}, \dots, y_k^{(0)})^T$  over the field  $\bar{F}$  with the rank  $k$  and lastly there exists a point  $c \in \bar{F}$ , such that  $a(c) \neq 0$ ,  $lc_{\frac{d}{dX}}(Q_m)(c) \neq 0, 1 \leq m \leq n - k$  for which the following equalities are valid:

$$\xi_{j,i}^{(m)} = 0, 1 \leq m \leq n - k, 1 \leq j \leq k, 0 \leq i < n \quad (4)$$

To the system (4) we apply the same procedure as in [Gr 90] was applied to system 6, taking into account that system (4) is linear with respect to the family of all the indeterminates  $b_m^{(s)}, b_{m,i}^{(s)}$  and considering the indeterminates  $y_{j,i}^{(0)}, c$  as the parameters. The procedure from [Gr 90] allows to solve system (4) in a parametrical form, and after that to find out, whether among its solutions there is one satisfying the inequalities contained in the formulation of Lemma 4. One can complete the proof of the Theorem (see the introduction) by the same complexity analysis of the algorithm as in [Gr 90].

## References

- [BBH 88] Beukers, F., Brownawell, D. and Heckman, G., *Siegel Normality*, Ann. Math. **127** (1988), pp. 279-308.
- [CG 83] Chistov, A. L. and Grigoriev, D. Yu., *Subexponential-time Solving Systems of Algebraic Equations*, volumes I and II (1983), Preprints LOMI E-9-83 and E-10-83, Leningrad.
- [CL 55] Coddington, E. and Levinson, N., *Theory of Ordinary Differential Equations*, McGraw-Hill, New York (1955).
- [Gr 86] Grigoriev, D. Yu., *Computational Complexity in Polynomial Algebra*, Proceedings of the International Congress of Mathematicians, volume 2, Berkeley (1986), pp. 1452-1460.
- [Gr 90] Grigoriev, D. Yu., *Complexity of Factoring and Calculating the GCD of Linear Differential Operators*, J. Symbol. Comput. (1990), to appear.
- [Ka 57] Kaplanski, I., *An Introduction to Differential Algebra*, Hermann, Paris (1957).

- [La 65] Lang, S., *Algebra*, Addison-Wesley, Reading (1965).
- [Si 81] Singer, M., *Liouvillean Solutions of  $n$ -th Order Homogeneous Linear Differential Equations*, Amer. J. Math. **103** (1981), pp. 661-682.