COMPLEXITY OF COMPUTING THE CHARACTERS AND THE GENRE OF A SYSTEM OF EXTERIOR DIFFERENTIAL EQUATIONS

D.Yu.Grigor'ev

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

Let a system $\{\sum_J A_{J,i}[dX_{j_1},\ldots,dX_{j_m}]=0\}_{m,i}$ of exterior differential equations be given, where $A_{J,i}$ are polynomials in n variables $X_1,\ldots,X_n$ of degrees less than d and skew-symmetric relatively to multiindices $J=(j_1,\ldots,j_m)$, the square brackets denote the exterior product of the differentials $dX_{j_1},\ldots,dX_{j_m}$. E.Cartan introduced the characters and the genre h of the system. Cauchy-Kovalevski theorem guarantes the existence of an integral manifold (and even of the general form) with the dimension less or equal to h satisfying the given system. An algorithm for computing the characters and the genre is designed with the running time polynomial in $\mathcal{L},(dn)^{n^2}$, herein $\mathcal{L}$ denotes the bit-size of the system. The algorithm involves the subexponential-time procedures for finding the irreducible components of an algebraic variety and for linear projecting a variety due to the author jointly with A.Chistov.

Introduction

Utilized below notions and statements about the systems of exterior differential equations and about integral manifolds satisfying the systems one can find in [1]. In [1] the genre of a system is defined (see also section 1 below). This definition entails that in principle one can reduce computing the genre to quantifier elimination in a certain formula of the first-order theory of algebraically closed fields (see e.g. [3]). Somewhat modified algorithm computing the genre is designed below in section 2, it has the complexity (see the theorem at the end of section 2) considerably less than the procedure from [1]. The algorithm is based on the lemma from section 1 giving an additional information on the structure of ordinary and regular points (see [1]), which has apparently an independent interest.

As in [2, 3, 4] we fix a ground field F of the following kind. Let $F = \mathbb{Q}(\delta_1, \dots, \delta_e)[\eta]$ where the elements $\delta_1, \dots, \delta_e$ are algebraically independent over the field $\mathbb{Q}$ of rational numbers and η is an algebraic element over the field $\mathbb{Q}(\delta_1, \dots, \delta_e)$, denote by $\varphi(Z) \in \mathbb{Q}[\delta_1, \dots, \delta_e][Z]$ a minimal polynomial of η. An arbitrary polynomial $f \in F[X_1, \dots, X_n]$ can be written uniquely (up to a factor ± 1) in the form as follows: $f = \sum_{i_1, \dots, i_n, i} (a_{i_1, \dots, i_n, i}/b)\, \eta^i X_1^{i_1} \dots X_n^{i_n}$, where $0 \leqslant i < \deg_Z(\varphi)$, the polynomials $a_{i_1, \dots, i_n, i}, b \in \mathbb{Z}[\delta_1, \dots, \delta_e]$, herein the degree $\deg_{\delta_1, \dots, \delta_e}(b)$ is the least possible and the (integer) coefficients of the polynomial b are reciprocately prime in community. Denote the degree $\deg_{\delta_1, \dots, \delta_e}(f) = \max_{i_1, \dots, i_n, i} \{\deg_{\delta_1, \dots, \delta_e}(a_{i_1, \dots, i_n, i}), \deg_{\delta_1, \dots, \delta_e}(b)\}$. At last define the size $l(f)$ of coefficients as the maximal bit-size among all (integer) coefficients of the polynomials $a_{i_1, \dots, i_n, i}, b$. It completes the description of the field F and the auxiliary parameters. By $\overline{F}$ we denote an algebraic closure of the field F.

So, let a system of exterior differential equations be given (cf. [1])

$$f_i^{(0)}(X_1, \dots, X_n) = 0; \quad 1 \leqslant i \leqslant K_0 \tag{1}$$

$$f_i^{(m)} \equiv \frac{1}{m!} \sum_J A_{J,i} [dX_{j_1}, \dots, dX_{j_m}] = 0; \quad 1 \leqslant m \leqslant R, \quad 1 \leqslant i \leqslant K_m. \tag{2}$$

Here $f_i^{(0)}, A_{J,i} \in F[X_1, \dots, X_n]$ are polynomials; the square brackets in (2) denote the exterior product of the differentials of the variables $dX_{j_1}, \dots, dX_{j_m}$; a multiindex $J = (j_1, \dots, j_m)$ where $1 \leqslant j_1, \dots, j_m \leqslant n$, moreover the coefficients $A_{J,i}$ are skew-symmetric relatively to the multiindices J. One can assume w.l.o.g. the system (1), (2) to be differentially closed, i.e. the exterior differential of the left part of any equation (1), (2) is the left part of a certain equation (2) (provided that this exterior differential does not vanish identically). One can also suppose w.l.o.g. that $R \leqslant n$ since for $m > n$ an equation (2) vanishes trivially ([1]). Denote $K = \sum_{0 \leqslant m \leqslant n} K_m$.

Remind ([1]) that a smooth manifold is called an integral manifold satisfying the system (1), (2) if firstly, any its point satisfies the system (1) and secondly, the coordinates of a tangent to the manifold vector of the general form in a point, being plugged instead of differentials $dX_1, \dots, dX_n$, satisfy the system (2).

We assume the following bounds on the parameters of the system (1), (2) to be valid for $m \geqslant 0$ (cf. [2, 3, 4]):

$$deg_{X_1,\dots,X_n}(f_i^{(m)}) < d;\; deg_{\delta_1',\dots,\delta_e'}(f_i^{(m)}) < d_2;\; deg_{\delta_1,\dots,\delta_n,Z}(\varphi) < d_1;\; \ell(f_i^{(m)}), \ell(\varphi) \leqslant M. \qquad (3)$$

In sequel we need the subexponential-time algorithms for decomposing variety (here and below a variety means an algebraic variety over an algebraically closed field [5, 6]) into irreducible components (see proposition 1 below) and for linear projecting a variety (see proposition 2 below). Thus, let $g_1,\dots,g_K \in F[X_1,\dots,X_n]$ be some polynomials satisfying the bounds similar to (3). Consider the variety $W=\{(x_1,\dots,x_n)\in \overline{F}^n : g_1(x_1,\dots,x_n)=\dots=g_K(x_1,\dots,x_n)=0\}$ of all common roots of the polynomials. The variety $W=\bigcup_\alpha W_\alpha$ is uniquely decomposable into a union of its irreducible (over the field F) components W_α [5, 6] . The algorithm from [2] yields each component W_α in two following manners: by a general point of W_α (in other words, by a special representation of the field $F(W_\alpha)$ of rational functions on W_α) and by a certain system of equations with the variety of common roots coinciding with W_α (we say in the latter case that the system of equations determines the variety W_α).

For a closed (here and below the Zariski topology [5, 6] is meant) defined and irreducible over F variety $\mathcal{W} \subset \overline{F}^n$ with the dimension $dim(\mathcal{W}) = n-m$ its general point is a fields isomorphism as follows:

$$F(T_1,\dots,T_{n-m})[\theta] \simeq F(\mathcal{W}) = F(X_1,\dots,X_n) \qquad (4)$$

where the elements $T_1,\dots,T_{n-m}$ are algebraically independent over the field F , the element θ is algebraic over the field $F(T_1,\dots,T_{n-m})$, let $\Phi(Z)\in F[T_1,\dots,T_{n-m}][Z]$ be its minimal polynomial; $X_1,\dots,X_n$ are considered here as coordinate functions on $\mathcal{W}$. Under the action of isomorphism (4) $\theta \simeq \sum_{1\leqslant i\leqslant n} c_i X_i$ for suitable integers $0 \leqslant c_i \leqslant deg_Z(\Phi)$ and $T_j \simeq X_{i_j}$ for $1\leqslant j \leqslant n-m$ and appropriate indices $1\leqslant i_1<\dots<i_{n-m}\leqslant n$. The algorithm represents isomorphism (4) by the polynomial Φ , indices $i_1,\dots,i_{n-m}$, integers c_i and the expressions $X_i = X_i(T_1,\dots,T_{n-m},\theta)\in F(T_1,\dots,T_{n-m})[\theta]$ (for simplicity of notations we identify X_i with its image in the field $F(T_1,\dots,T_{n-m})[\theta]$ under isomorphism (4), this does not lead to misunderstanding).

PROPOSITION 1 ([2], see also [3, 4]). One can design an algorithm which for a given system $g_1 = \ldots = g_K = 0$ yields all the irreducible components W_α. For each component W_α the algorithm yields its general point (keep for it the same notations as in (4)) and besides, some polynomials $\Psi_{\alpha,s} \in F[X_1, \ldots, X_n]$, $1 \leqslant s \leqslant N$ such that $W_\alpha = \{x \in \overline{F}^n : \Psi_{\alpha,s}(x) = 0,\ 1 \leqslant s \leqslant N\}$. Furthermore, the following bounds are true for all indices j, s:

$$deg_Z(\Phi) \leqslant deg(W_\alpha) \leqslant d^m; \quad N \leqslant m^2 d^{4m}; \quad deg_{X_1,\ldots,X_n}(\Psi_{\alpha,s}) \leqslant d^{2m};$$

$$deg_{\delta_1,\ldots,\delta_e,T_1,\ldots,T_{n-m}}(\Phi),\ deg_{\delta_1,\ldots,\delta_e,T_1,\ldots,T_{n-m}}(X_j),\ deg_{\delta_1,\ldots,\delta_e}(\Psi_{\alpha,s}) \leqslant$$

$$\leqslant d_2 (d^n d_1)^{O(1)};\ \ell(\Phi), \ell(X_j), \ell(\Psi_{\alpha,s}) \leqslant (M + e d_2)(d^n d_1)^{O(1)}.$$

Finally, the algorithm works within time polynomial in $M, K, (d^n d_1 d_2)^{n+e}$.

Now we proceed to linear projecting algorithm of a variety. Let a polynomial $g_0 \in F[X_1, \ldots, X_n]$ satisfy the bounds similar to (3). Consider a projection $\pi : \overline{F}^n \longrightarrow \overline{F}^m$ defined by a formula $\pi(X_1, \ldots, X_n) = (X_1, \ldots, X_m)$. Denote a quasiprojective variety [6] $W' = \{x \in W : g_0(x) \neq 0\}$.

PROPOSITION 2 ([3], see also [4]). One can design an algorithm which for a given family $g_0, g_1, \ldots, g_K$ yields a linear projection $\pi(W') \subset \overline{F}^m$, namely suitable polynomials $g_{\lambda,\sigma} \in F[X_1, \ldots, X_m]$ such that $\pi(W') = \bigcup_\lambda V_\lambda$ where $V_\lambda = \{x \in \overline{F}^m : g_{\lambda,\sigma}(x) = 0$ for all $\sigma > 0$ and $g_{\lambda,0}(x) \neq 0\} \neq \emptyset$, and apart from that the closure $\overline{V_\lambda} = \{x \in \overline{F}^m : g_{\lambda,\sigma}(x) = 0$ for all $\sigma > 0\}$ is irreducible. Moreover, the following bounds are valid:

$$deg_{X_1,\ldots,X_n}(g_{\lambda,\sigma}) \leqslant d^{O((n-m)n)}; \quad deg_{\delta_1,\ldots,\delta_e}(g_{\lambda,\sigma}) \leqslant d_2 (d^{(n-m)n} d_1)^{O(1)};$$

$$\ell(g_{\lambda,\sigma}) \leqslant (M + e d_2)(d^{(n-m)n} d_1)^{O(1)}; \quad \lambda, \sigma \leqslant d^{O((n-m)n)}.$$

Finally, the algorithm runs within time polynomial in $M, K, (d^{(n-m)n} d_1 d_2)^{n+e}$.

1. Polar system. Ordinary and regular points

Let us carry out some auxiliary construction (cf. [1]). Denote $W^{(0)} = \{x \in \overline{F}^n : f_i^{(0)}(x) = 0,\ 1 \leqslant i \leqslant K\}$ the variety determined by the system (1). For $1 \leqslant m \leqslant R$ consider the variety $W^{(m)} \subset \overline{F}^{n(m+1)}$ in the space with the coordinates $X_1, \ldots, X_n, X_1^{(1)}, \ldots, X_n^{(1)}, \ldots, X_1^{(m)}, \ldots, X_n^{(m)}$ determined by the equations (1) and in addition by the equations

$$\sum_J A_{J,i} X_{j_1}^{(\ell_1)} \dots X_{j_t}^{(\ell_t)} = 0 \tag{5}$$

for all $1 \leqslant t \leqslant m$, $1 \leqslant i \leqslant k_t$ and all possible $1 \leqslant \ell_1 < \dots < \ell_t \leqslant m$ (which are fixed for a given equation); herein multiindex $J=(j_1,\dots,j_t)$ (see (2)).

For $1 \leqslant m \leqslant R$ consider a projection $\pi^{(m)}: \overline{F}^{n(m+1)} \to \overline{F}^{nm}$ along the coordinates $X_1^{(m)},\dots,X_n^{(m)}$. Then $\pi^{(m)}(W^{(m)}) = W^{(m-1)}$, since the inclusion $\pi^{(m)}(W^{(m)}) \subset W^{(m-1)}$ is obvious and if a point $(x_1,\dots,x_n,\dots, x_1^{(m-1)},\dots,x_n^{(m-1)}) \in W^{(m-1)}$ then the point $(x_1,\dots,x_n,\dots,x_1^{(m-1)},\dots,x_n^{(m-1)},0,\dots,0) \in W^{(m)}$.

Let $W^{(0)} = \bigcup_\alpha W_\alpha^{(0)}$ be the decomposition of $W^{(0)}$ into a union of its irreducible (here and below the components defined and irreducible over the field F are meant) components, then the variety $\widetilde{W}_\alpha^{(0)} \subset W_\alpha^{(0)}$ consisting of all nonsingular points ([6]) of $W_\alpha^{(0)}$ is open and dense in $W_\alpha^{(0)}$. The points from $\widetilde{W}_\alpha^{(0)}$ are called here ordinary of the component $W_\alpha^{(0)}$ (cf. [1]).

Assume that by induction on m are defined already for some $1 \leqslant m \leqslant R$ for every irreducible component $W_\beta^{(m-1)}$ of the variety $W^{(m-1)}$ an open (may be empty) subvariety $\widetilde{W}_\beta^{(m-1)} \subset W_\beta^{(m-1)}$ of the ordinary points of $W_\beta^{(m-1)}$ and besides, for each irreducible component $W_\gamma^{(m-2)}$ of the variety $W^{(m-2)}$ an open subvariety $\widetilde{\widetilde{W}}_\gamma^{(m-2)} \subset \widetilde{W}_\gamma^{(m-2)} \subset W_\gamma^{(m-2)}$ of the regular points of $W_\gamma^{(m-2)}$. The conjunction of all the equations of the form (5) in which $\ell_t = m$ (for all $1 \leqslant t \leqslant m$) can be considered as a linear system of the form $\mathcal{A}\mathcal{X} = 0$ (it is called the polar system, see [1]), where $\mathcal{X}$ is the vector with the coordinates being the variables $X_1^{(m)},\dots,X_n^{(m)}$ and $\mathcal{A} = \mathcal{A}^{(m)}$ is a matrix over the ring $F[X_1,\dots,X_n,\dots,X_1^{(m-1)},\dots,X_n^{(m-1)}]$. Observe that for any point $y \in W^{(m-1)}$ an intersection $W^{(m)} \cap (\{y\} \times \overline{F}^n) = \{(y,x) \in \overline{F}^{n(m+1)} : \mathcal{A}(y)x = 0\}$ where the matrix $\mathcal{A}(y)$ is obtained from $\mathcal{A}$ by plugging the coordinates of the point y instead of the variables $X_1,\dots,X_n,\dots,X_1^{(m-1)},\dots,X_n^{(m-1)}$, respectively.

Fix an irreducible component V of the variety $W^{(m-1)}$. For any irreducible component $W_\alpha^{(m)}$ of the variety $W^{(m)}$ its projection $\pi^{(m)}(W_\alpha^{(m)})$ is also irreducible ([5]), therefore $\pi^{(m)}(W_\alpha^{(m)}) \subset W_\beta^{(m-1)}$ for an appropriate (not necessary unique) irreducible component $W_\beta^{(m-1)}$ of the variety $W^{(m-1)}$. Further we consider the components $W_\alpha^{(m)}$ of the variety $W^{(m)}$ for which $\pi^{(m)}(W_\alpha^{(m)}) \subset V$.

For almost all the points $y \in V$ the rank $rg(\mathcal{A}(y)) = r$ equals to a certain integer r ([5]), hence for every point $y_1 \in V$ an inequality $rg(\mathcal{A}(y_1)) \leqslant r$ holds, taking into account that the set of all the points satisfying the latter condition is closed and on the other hand V is irreducible. Consider some $r\times r$ submatrix of the matrix $\mathcal{A}$ without vanishing its determinant Δ identically on V. Then an open dense in V subset $V_\Delta = V\cap\{y:\Delta(y)\neq 0\}$ is irreducible ([5]). An isomorphism of quasiprojective varieties $W^{(m)}\cap(V_\Delta\times\overline{F}^n)\simeq V_\Delta\times\overline{F}^{n-r}$ is valid, since for each point $y\in V_\Delta$ a solution of the linear system $(\mathcal{A}(y))\mathcal{X}=0$ is obtained by arbitrary assigning values of $(n-r)$ coordinates not belonging to $r\times r$ submatrix under consideration with the determinant Δ, after that r coordinates corresponding to this submatrix are expressed uniquely ([6]). The variety $V_\Delta\times\overline{F}^{n-r}$ is irreducible as the product of irreducible varieties ([5, 6]). Therefore there exists such an irreducible component $U=W^{(m)}_{\alpha_0}$ of the variety $W^{(m)}$ that $W^{(m)}_{\alpha_0}\supset W^{(m)}\cap(V_\Delta\times\overline{F}^n)$.

For any $r\times r$ submatrix of the matrix $\mathcal{A}$ without vanishing its determinant Δ_1 identically on V holds an inclusion $U\supset W^{(m)}\cap(V_{\Delta_1}\times\overline{F}^n)$ taking into account that U is closed and contains an open dense subset $W^{(m)}\cap(V_{\Delta\Delta_1}\times\overline{F}^n)=W^{(m)}\cap(V_{\Delta_1}\times\overline{F}^n)\cap\{(y,x):\Delta(y)\neq 0\}$ of the irreducible set $W^{(m)}\cap(V_{\Delta_1}\times\overline{F}^n)$ (cf. above). Observe that $\pi^{(m)}(U)\subset V$, indeed $\pi^{(m)}(U)\subset W^{(m-1)}_\beta$ for a suitable irreducible component $W^{(m-1)}_\beta$ of the variety $W^{(m-1)}$ (see above), then $W^{(m-1)}_\beta$ contains the open dense subset V_Δ of the irreducible component V, hence $W^{(m-1)}_\beta=V$.

Consider a closed set $U'=U\cap(\{y:\underset{\gamma}{\&}(\Delta_\gamma(y)=0)\}\times\overline{F}^n)$, where Δ_γ ranges over determinants of all $r\times r$ submatrices of the matrix $\mathcal{A}$, evidently $U'\subsetneqq U$, therefore $U\setminus U'=W^{(m)}\cap\bigcup_\gamma(V_{\Delta_\gamma}\times\overline{F}^n)$ (see above) is an open dense subset of the set U. Remark that $\bigcup_\gamma V_{\Delta_\gamma}=\{y\in V: rg(\mathcal{A}(y))=r\}$. If for an irreducible component $W^{(m)}_\alpha\neq U$ of the variety $W^{(m)}$ such that $\pi^{(m)}(W^{(m)}_\alpha)\subset V$ holds $W^{(m)}_\alpha\not\subset\{y:\underset{\gamma}{\&}(\Delta_\gamma(y)=0)\}\times\overline{F}^n$, then a set $W^{(m)}_\alpha\cap(\bigcup_\gamma\{y:\Delta_\gamma(y)\neq 0\}\times\overline{F}^n)=W^{(m)}_\alpha\cap\bigcup_\gamma(V_{\Delta_\gamma}\times\overline{F}^n)\subset U\setminus U'$ is an open dense subset of the variety $W^{(m)}_\alpha$, this implies an inclusion $U\supset W^{(m)}_\alpha$ (cf. above), whence get a contradiction, so $W^{(m)}_\alpha\subset\{y:\underset{\gamma}{\&}(\Delta_\gamma(y)=0)\}\times\overline{F}^n$. Thus, there is exactly one irreducible component U of the variety $W^{(m)}$ among such components $W^{(m)}_\alpha$ that $\pi^{(m)}(W^{(m)}_\alpha)\subset V$, for which $U\supset W^{(m)}\cap\bigcup_\gamma(V_{\Delta_\gamma}\times\overline{F}^n)$, moreover for any such component $W^{(m)}_\alpha\neq U$ holds $W^{(m)}_\alpha\cap\bigcup_\gamma(V_{\Delta_\gamma}\times\overline{F}^n)=\emptyset$.

Thereupon consider an irreducible closed set $V\times\{0\}\subset W^{(m)}$. Since U contains an open dense in $V\times\{0\}$ subset $\bigcup_\gamma(V_{\Delta_\gamma}\times\{0\})$, one infers an inclusion $U\supset V\times\{0\}$, therefore $\pi^m(U)=V$.

An ordinary point $y\in\widetilde{V}\subset V$ is called a regular point of V if $rg(\mathcal{A}(y))=r$, in other words the variety of all regular points of the irreducible component V equals to $\tilde{\tilde{V}} = \tilde{V} \cap (\bigcup_{\delta} V_{\Delta\delta})$. Furthermore, the points from the set $\tilde{U} = U \cap (\tilde{\tilde{V}} \times \overline{F}^{n})$ are called ordinary of the irreducible component U. Provided that $\tilde{V}$ is an open dense set in V, the set $\tilde{\tilde{V}}$ is also an open dense subset of V and $\tilde{U}$ is an open dense subset of U. Considering all the irreducible components of the variety $W^{(m-1)}$ completes the inductive step in defining the sets $\tilde{\tilde{W}}_{\beta}^{(m-1)}$ and $\tilde{W}_{\alpha}^{(m)}$.

As a result the following lemma is proved supplying us with more information about the structure of the varieties of ordinary and regular points than in [1], basing on which an algorithm computing the genre of the system (1), (2) will be designed in section 2.

LEMMA. For each irreducible component $W_{\alpha}^{(0)}$ of the variety $W^{(0)} \subset \overline{F}^{n}$ (determined by the system (1)) there is a unique chain of varieties $W_{\alpha}^{(0)}, W_{\alpha}^{(1)}, \ldots, W_{\alpha}^{(R)}$ (after an appropriate renumerating lower indices), herein $W_{\alpha}^{(m)}$ is an irreducible component of the variety $W^{(m)} \subset \overline{F}^{n(m+1)}$ and besides $\pi^{(m)}(W_{\alpha}^{(m)}) = W_{\alpha}^{(m-1)}$ for $1 \leqslant m \leqslant R$. For any point $y \in W_{\alpha}^{(m-1)}$ the inverse image $(\pi^{(m)})^{-1}(y) \cap W^{(m)}$ is a linear space with the dimension greater or equal to $n-(s_{0,\alpha}+\ldots+s_{m-1,\alpha})$ for suitable nonnegative integers $s_{0,\alpha}, s_{1,\alpha}, \ldots,$ moreover for almost all the points $y \in W_{\alpha}^{(m-1)}$ holds $(\pi^{(m)})^{-1}(y) \cap W^{(m)} = (\pi^{(m)})^{-1}(y) \cap W_{\alpha}^{(m)}$ and $\dim((\pi^{(m)})^{-1}(y) \cap W_{\alpha}^{(m)}) = n-(s_{0,\alpha}+\ldots+s_{m-1,\alpha})$. The sets, respectively, of all regular and ordinary points $\tilde{\tilde{W}}_{\alpha}^{(m-1)} \subset \tilde{W}_{\alpha}^{(m-1)} \subset W_{\alpha}^{(m-1)}$ of the component $W_{\alpha}^{(m-1)}$ are both open dense in $W_{\alpha}^{(m-1)}$, apart from that for every point $y \in \tilde{\tilde{W}}_{\alpha}^{(m-1)}$ the dimension of an inverse image $(\pi^{(m)})^{-1}(y) \cap W^{(m)} = (\pi^{(m)})^{-1}(y) \cap W_{\alpha}^{(m)}$ equals to $n-(s_{0,\alpha}+\ldots+s_{m-1,\alpha})$, furthermore $\tilde{W}_{\alpha}^{(m)} = (\pi^{(m)})^{-1}(\tilde{\tilde{W}}_{\alpha}^{(m-1)}) \cap W_{\alpha}^{(m)}$. Lastly, for each irreducible component $W_{\beta}^{(m)} \neq W_{\alpha}^{(m)}$ of the variety $W^{(m)}$ such that $\pi^{(m)}(W_{\beta}^{(m)}) \subset W_{\alpha}^{(m-1)}$ the following is true: for any point $y \in \pi^{(m)}(W_{\beta}^{(m)})$ the dimension $\dim((\pi^{(m)})^{-1}(y) \cap W^{(m)}) > n-(s_{0,\alpha}+\ldots+s_{m-1,\alpha})$.

Note that $\dim(W_{\alpha}^{(m)}) - \dim(W_{\alpha}^{(m-1)}) = n-(s_{0,\alpha}+\ldots+s_{m-1,\alpha})$ ([5]).

Only the statement of lemma about nonnegativity of integers $s_{0,\alpha}$, $s_{1,\alpha}, \ldots$ is not yet proved. One can deduce it from the observation that the matrix $\mathcal{A} = \mathcal{A}^{(m)}$ considered earlier, contains all the rows of the matrix $\mathcal{A}^{(m-1)}$ considered at the previous step of induction (and besides, may be some other rows, see (5)), because of that $s_{0,\alpha}+\ldots+s_{m-1,\alpha} = \max_{y \in W_{\alpha}^{(m-1)}} \operatorname{rg}(\mathcal{A}^{(m)}(y)) \geqslant \max_{z \in W_{\alpha}^{(m-2)}} \operatorname{rg}(\mathcal{A}^{(m-1)}(z)) = s_{0,\alpha}+\ldots+s_{m-2,\alpha}$.

Remind (see [1]) that the largest such integer h_{α}, for which $s_{0,\alpha}+\ldots+s_{h_{\alpha}-1,\alpha} \leqslant n-h_{\alpha}$ is called the genre of the system (1), (2) relatively to the irreducible component $W_{\alpha}^{(0)}$. A number $s_{m,\alpha}$ is called m-th character of the system relatively to $W_{\alpha}^{(0)}$ (cf. [1]).

The (global) genre of the system (1), (2) can be defined as $h = \max_{\alpha}\{h_\alpha\}$. Recall also (see [1]) that through any regular point of the irreducible component $W_\alpha^{(0)}$ passes at least one $\varkappa$-dimensional integral manifold satisfying the system (1), (2) for arbitrary $\varkappa \leqslant h_\alpha$ (in fact, see [1], Cauchy-Kovalevski theorem allows to prove a stronger result on the existence of integral manifolds).

2. Algorithm computing the characters and the genre and its complexity analysis.

Now we proceed to describing an algorithm computing the characters and the genre of the system (1), (2). Firstly, find irreducible components $W_\beta^{(m)}$ of the closed variety $W^{(m)}$ with the aid of proposition 1 for $0 \leqslant m \leqslant R$. Thereupon the algorithm for each component $W_\beta^{(m)}$ yields its projection $\pi^{(m)}(W_\beta^{(m)})$ basing on proposition 2. After that for every component $W_\alpha^{(0)}$ the algorithm finds successively $W_\alpha^{(1)}, W_\alpha^{(2)}, \ldots, W_\alpha^{(R)}$, so that $\pi^{(m)}(W_\alpha^{(m)}) = W_\alpha^{(m-1)}$ for all $1 \leqslant m \leqslant R$ (in force of lemma, $W_\alpha^{(m)}$ is determined uniquely by $W_\alpha^{(m-1)}$). Finally, one computes successively $s_{0,\alpha}, s_{1,\alpha}, \ldots, s_{R,\alpha}$ and then h_α (see the note just after lemma).

The algorithm has to test a coincidence $\pi^{(m)}(W_\alpha^{(m)}) = W_\alpha^{(m-1)}$ of the varieties. For this purpose one could again use directly proposition 1, but this would lead to a worse complexity bound than in the procedure described below. Let $U = W_\beta^{(m)}$ be an irreducible component of the variety $W^{(m)}$. We show that a coincidence $\pi^{(m)}(U) = W_\alpha^{(m-1)}$ is equivalent to an inclusion $\pi^{m}(U) \supset W_\alpha^{(m-1)}$ and also is equivalent to an inclusion $\overline{\pi^{(m)}(U)} \supset W_\alpha^{(m-1)}$. Indeed, suppose the opposite, let $\overline{\pi^{(m)}(U)} \supset W_\alpha^{(m-1)}$ and $\pi^{(m)}(U) \not\subset W_\alpha^{(m-1)}$. Then $\pi^{(m)}(U) \subset V$ for a certain irreducible component $V = W_\gamma^{(m-1)} \neq W_\alpha^{(m-1)}$ of the variety $W^{(m-1)}$, hence $V = \overline{V} \supset \overline{\pi^{(m)}(U)} \supset W_\alpha^{(m-1)}$, we get a contradiction. Thus, $\pi^{(m)}(U) \subset W_\alpha^{(m-1)}$ this entails the coincidence $\overline{\pi^{(m)}(U)} = W_\alpha^{(m-1)}$ and so $U = W_\alpha^{(m)}$, taking into account the inclusion $\overline{\pi^{(m)}(U)} \supset W_\alpha^{(m-1)}$ (see the proof of lemma).

In order to check the inclusion $\overline{\pi^{(m)}(U)} \supset W_\alpha^{(m-1)}$ recall that proposition 1 allows to produce a general point of the irreducible variety $W_\alpha^{(m-1)}$, i.e. a fields isomorphism of the following form:

$$F(T_1, \ldots, T_q)[\theta] \simeq F(W_\alpha^{(m-1)}) = F(X_1, \ldots, X_n, X_1^{(1)}, \ldots, X_n^{(1)}, \ldots, X_1^{(m-1)}, \ldots, X_n^{(m-1)}) \qquad (6)$$

where $q = \dim(W_\alpha^{(m-1)})$ and let T_j, Φ, c_i play the similar role as in (4). Besides, proposition 1 allows to produce a system of polynomials

$\varphi_{d,j}^{(m-1)} \in F[X_1,\dots,X_n,X_1^{(1)},\dots,X_n^{(m-1)}]$ determining the variety $W_d^{(m-1)}$. Analogous representation (by a general point and by a determining system of polynomials) the algorithm produces also for the irreducible component U. Basing on proposition 2 the algorithm yields the projection $\pi^{(m)}(U)$ in the following form: $\pi^{(m)}(U) = \bigcup_\lambda U_\lambda$, where $\emptyset \neq U_\lambda = \{y \in \overline{F}^{nm} : g_{\lambda,\sigma}(y) = 0$ for all $\sigma > 0$ and $g_{\lambda,0}(y) \neq 0\}$, herein $g_{\lambda,\sigma} \in F[X_1,\dots,X_n,X_1^{(1)},\dots,X_n^{(m-1)}]$ are suitable polynomials.

Thus, the inclusion $\overline{\pi^{(m)}(U)} \supset W_d^{(m-1)}$ is equivalent to a statement that for a certain index λ an inclusion $\overline{U_\lambda} \supset W_d^{(m-1)}$ is true. The latter inclusion holds iff plugging images of the coordinate functions $X_1,\dots,X_n,X_1^{(1)},\dots,X_n^{(m-1)}$ in the field $F(T_1,\dots,T_q)[\theta] \simeq F(T_1,\dots,T_q)[Z]/(\Phi)$ under the action of isomorphism (6) into the polynomials $g_{\lambda,\sigma}$ instead of corresponding variables, one obtains zero elements of the field $F(T_1,\dots,T_q)[\theta]$ for all $\sigma>0$ (see [2]), taking into account the irreducibility of $\overline{U_\lambda} = \{y \in \overline{F}^{nm} : g_{\lambda,\sigma}(y)=0$ for all $\sigma > 0\}$. Testing the inclusion $\overline{\pi^{(m)}(U)} \supset W_d^{(m-1)}$ and so the coincidence $\pi^{(m)}(U) = W_d^{(m-1)}$ completes describing the algorithm computing the characters and the genre of the system (1), (2).

In conclusion we proceed to the complexity analysis of the algorithm. According to (3) and to proposition 1 the algorithm finds the irreducible components $W_\beta^{(m-1)}$ of the variety $W^{(m-1)}$ within time $(M\kappa((dR)^{nR} d_1 d_2)^{nR+e})^{O(1)}$. Moreover (see proposition 1), for the parameters of the general point (6) and of the polynomials $\varphi_{d,j}^{(m-1)}$ the following bounds are valid (for simplicity of notations we omit indices denoting by X an arbitrary coordinate functions):

$$\deg_Z(\Phi) \leq (d+R)^{nR}; \quad \deg_{X_1,\dots,X_n,X_1^{(1)},\dots,X_n^{(m-1)}}(\varphi_{d,j}^{(m-1)}) < (d+R)^{2nR};$$

$$\deg_{\delta_1,\dots,\delta_e,T_1,\dots,T_q}(\Phi), \deg_{\delta_1,\dots,\delta_e,T_1,\dots,T_q}(X), \deg_{\delta_1,\dots,\delta_e}(\varphi_{d,j}^{(m-1)}) < d_2((dR)^{nR} d_1)^{O(1)};$$

$$l(\Phi), l(X), l(\varphi_{d,j}^{(m-1)}) \leq (M+ed_2)((dR)^{nR} d_1)^{O(1)}$$

and the number of the polynomials $\varphi_{d,j}^{(m-1)}$ does not exceed $(nR)^2(d+R)^{4nR}$. By virtue of proposition 2 for yielding the projection $\pi^{(m)}(W_\beta^{(m)})$, i.e. the polynomials $g_{\lambda,\sigma}$, and also for plugging the images of coordinate functions under isomorphism (6) into the polynomials $g_{\lambda,\sigma}$, the algorithm suffices time $(M\kappa((dR)^{n^3R^2} d_1 d_2)^{nR+e})^{O(1)}$. Furthermore, the following bounds are true: $\deg_{X_1,\dots,X_n,X_1^{(1)},\dots,X_n^{(m-1)}}(g_{\lambda,\sigma}) < (dR)^{O(n^3R^2)}$; $\deg_{\delta_1,\dots,\delta_e}(g_{\lambda,\sigma}) < d_2((dR)^{n^3R^2} d_1)^{O(1)}$; $l(g_{\lambda,\sigma}) \leq (M+ed_2)((dR)^{n^3R^2} d_1)^{O(1)}$.

Remind (see above) that $R \leqslant n$. Thus, the following theorem, being the main result of the paper, is proved.

THEOREM. One can compute the characters $s_{0,\alpha}, s_{1,\alpha}, \dots, s_{R,\alpha}$, the genre h_α , the global genre $h = \max_\alpha \{h_\alpha\}$ of the system (1), (2), besides, the specified in lemma chains of the varieties $W_\alpha^{(0)}, W_\alpha^{(1)}, \dots, W_\alpha^{(R)}$ within time $(M\kappa((dR)^{n^3R^2}d_1d_2)^{nR+e})^{O(1)} \leqslant (M\kappa((dn)^{n^5}d_1d_2)^{n^2+e})^{O(1)}$.

References

1. E.Cartan. Les systèmes différentiels extérieurs et leurs applications géometriques. - Paris, Hermann, 1945.
2. A.L.Chistov, D.Yu.Grigor'ev. Subexponential-time solving systems of algebraic equations. I, II. - Preprints LOMI E-9-83, E-10-83, Leningrad, 1983.
3. A.L.Chistov, D.Yu.Grigor'ev. Complexity of quantifier elimination in the theory of algebraically closed fields. - Lect.Notes Comput. Sci., 1984, v.176, p.17-31.
4. D.Yu.Grigor'ev. Computational complexity in polynomial algebra. - Proc.Int.Congr.Math., Berkeley, 1986.
5. D.Mumford. Algebraic geometry. - Springer, 1976.
6. I.R.Shafarevich. Basic algebraic geometry. - Springer, 1974.