Докл. Акад. Наук СССР
Том 306 (1989), № 1

Soviet Math. Dokl.
Vol. 39 (1989), No. 3

# COMPLEXITY OF COMPUTING THE GENUS OF A SYSTEM OF EXTERIOR DIFFERENTIAL EQUATIONS

UDC 518.5

D. YU. GRIGOR'EV

In [1] the notion of genus of a system of exterior differential equations was introduced; from its definition one sees that computing the genus reduces, in principle, to quantifier elimination in a certain formula of the first order theory of algebraically closed fields (see [5]). However, if one follows directly this method of computing the genus, the estimate obtained for the running time of the algorithm is considerably larger than in the algorithm described below. This algorithm is based on some properties (see the lemma below) of the varieties of ordinary and regular points and the varieties defined by polar systems [1]; it also employs subexponential complexity algorithms for finding the irreducible components of algebraic varieties [2]–[4]. Recall that it was proved in [1], on the basis of the Cauchy-Kovalevskaya theorem, that there exist integral varieties, satisfying the given system of exterior differential equations, of arbitrary dimension not exceeding the genus.

So suppose we have a system of exterior differential equations (cf. [1]) of the form

$$f_i^{(0)}(X_1,\dots,X_n)=0, \qquad 1\le i\le k; \tag{1}$$

$$f_i^{(m)} \equiv \frac{1}{m!}\sum_J A_{J,i}\,dX_{j_1}\wedge\cdots\wedge dX_{j_m}=0, \qquad 1\le m\le n,\ 1\le i\le k. \tag{2}$$

Here $f_i^{(0)}, A_{J,i}\in \mathbf{Q}[X_1,\dots,X_n]$ are polynomials of degrees $\deg(f_i^{(0)})=\deg_{X_1,\dots,X_n}(f_i^{(0)})$, $\deg(A_{J,i})<d$; the multi-index $J=(j_1,\dots,j_m)$, where $1\le j_1,\dots,j_m\le n$, and the coefficients $A_{J,i}$ are skew-symmetric with respect to the multi-indices $J$.

For a rational number $p/q\in\mathbf{Q}$, we denote by $l(p/q)=\log_2(|pq|+1)+1$ its size in bits. By $l(f_i^{(0)})$ we denote the maximum of the sizes in bits of the coefficients of $f_i^{(0)}$. Suppose that $l(f_i^{(0)}), l(A_{J,i})\le M$ for some natural number $M$. Then the size in bits of the system (1), (2) may be estimated as $Mk(nd)^n$ (see [2]–[4]).

**1.** We introduce the following auxiliary constructions (cf. [1]). Denote by $W^{(0)}\subset \mathbf{C}^n$ the algebraic variety defined by the system (1). For any $1\le m\le n$, denote by $W^{(m)}\subset \mathbf{C}^{n(m+1)}$ the variety, in the space with coordinates $X_1,\dots,X_n, X_1^{(1)},\dots,X_n^{(1)},\dots,X_1^{(m)},\dots,X_n^{(m)}$ defined by (1) and the equations

$$\sum_J A_{J,i}X_{j_1}^{(l_1)}\cdots X_{j_t}^{(l_t)}=0, \qquad 1\le t\le m,\ 1\le i\le k, \tag{3}$$

for all $1\le l_1<\cdots<l_t\le m$ (fixed for a given equation); here the multi-index $J=(j_1,\dots,j_t)$ (see (2)).

Consider the projection $\pi^{(m)}\colon \mathbf{C}^{n(m+1)}\to\mathbf{C}^{nm}$ along the coordinates $X_1^{(m)},\dots,X_n^{(m)}$ for $1\le m\le n$. Then $\pi^{(m)}(W^{(m)})=W^{(m-1)}$.

Nonsingular points of the variety $W^{(0)}$ [7] will be called its *ordinary points*, and the set of them will be denoted by $\widetilde{W}^{(0)}\subset W^{(0)}$ (cf. [1]). Let $W^{(0)}=\bigcup_\alpha W_\alpha^{(0)}$ be

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 58A15; Secondary 14A10, 68Q40.

the decomposition of $W^{(0)}$ into irreducible components (here and below we mean irreducible components over $\mathbf{Q}$ [6]). Then $\widetilde{W}_\alpha^{(0)} = \widetilde{W}^{(0)} \cap W_\alpha^{(0)}$ is an open dense subset of $W_\alpha^{(0)}$ (here and below we consider the Zariski topology [6], [7]).

Suppose that we have already defined, by induction on $m$, the (open in $W^{(m-1)}$) variety $\widetilde{W}^{(m-1)} \subset W^{(m-1)}$ of ordinary points, and also the (open in $W^{(m-2)}$ variety $\widetilde{\widetilde{W}}^{(m-2)} \subset \widetilde{W}^{(m-2)}$ of regular points (cf. [1]) for some $1 \le m \le n$. The collection of all equations of system (3) in which $l_t = m$ (for all $1 \le t \le m$) may be considered as a linear system of the form $\mathscr{A}\mathscr{Z} = 0$ (it is called a *polar system*; see [1]), where $\mathscr{Z}$ is a vector of the variables $X_1^{(m)}, \dots, X_n^{(m)}$ and $\mathscr{A} = \mathscr{A}^{(m)}$ is a matrix over the ring $\mathbf{Q}[X_1, \dots, X_n, \dots, X_1^{(m-1)}, \dots, X_n^{(m-1)}]$. Note that, for any point $y \in W^{(m-1)}$, $W^{(m)} \cap (\{y\} \times \mathbf{C}^n) = \{(y,x)\colon \mathscr{A}(y)x = 0\}$, where the matrix $\mathscr{A}(y)$ is obtained from $\mathscr{A}$ by substituting the coordinates of $y$ for the variables $X_1, \dots, X_n, \dots, X_1^{(m-1)}, \dots, X_n^{(m-1)}$.

Fix an irreducible component $V$ of $W^{(m-1)}$. For any irreducible component $W_\alpha^{(m)}$ of $W^{(m)}$, its projection $\pi^{(m)}(W_\alpha^{(m)})$ is also irreducible [6], hence $\pi^{(m)}(W_\alpha^{(m)}) \subset W_\beta^{(m-1)}$ for some (possibly nonunique) irreducible component $W_\beta^{(m-1)}$ of $W^{(m-1)}$. Below, we consider those components $W_\alpha^{(m)}$ of $W^{(m)}$ for which $\pi^{(m)}(W_\alpha^{(m)}) \subset V$.

If, for almost all points $y \in V$ (see [6]), $\operatorname{rank}(\mathscr{A}(y)) = r$, then, for any $y_1 \in V$, $\operatorname{rank}(\mathscr{A}(y_1)) \le r$. Consider an $r \times r$ submatrix of the matrix $\mathscr{A}$ with determinant $\Delta$ not identically equal to zero on $V$. Then the open and dense in $V$ subset $V_\Delta = V \cap \{y\colon \Delta(y) \ne 0\}$ is irreducible [6]. There is an isomorphism of quasiprojective varieties $W^{(m)} \cap (V_\Delta \times \mathbf{C}^n) \simeq V_\Delta \times \mathbf{C}^{n-r}$, due to the fact that, for $y \in V_\Delta$, a solution of the linear system $(\mathscr{A}(y))\mathscr{Z} = 0$ is obtained by fixing arbitrarily the values of the $n-r$ coordinates outside the considered submatrix with determinant $\Delta$, and the $r$ coordinates corresponding to that submatrix are then uniquely determined [7]. The variety $V_\Delta \times \mathbf{C}^{n-r}$ is irreducible as a product of irreducible ones [6], [7]. Therefore we can find an irreducible component $U = W_{\alpha_0}^{(m)}$ of $W^{(m)}$ such that $W_{\alpha_0}^{(m)} \supset W^{(m)} \cap (V_\Delta \times \mathbf{C}^n)$.

For any $r \times r$ submatrix of $\mathscr{A}$ with determinant $\Delta_1$ not identically equal to zero on $V$ we have $U \supset W^{(m)} \cap (V_{\Delta_1} \times \mathbf{C}^n)$, since $U$ is closed and contains an open dense subset $W^{(m)} \cap (V_{\Delta\Delta_1} \times \mathbf{C}^n) = W^{(m)} \cap (V_{\Delta_1} \times \mathbf{C}^n) \cap \{(y,x)\colon \Delta(y) \ne 0\}$ of the irreducible set $W^{(m)} \cap (V_{\Delta_1} \times \mathbf{C}^n)$ (see above). Note that $\pi^{(m)}(U) \subset V$; in fact, $\pi^{(m)}(U) \subset W_\beta^{(m-1)}$ for some irreducible component $W_\beta^{(m-1)}$ of $W^{(m-1)}$ (see above); then $W_\beta^{(m-1)}$ contains a dense open subset $V_\Delta$ of the irreducible component $V$, and, consequently, $W_\beta^{(m-1)} = V$.

The set $U' = U \cap (\{y\colon \&_\gamma(\Delta_\gamma(y) = 0)\} \times \mathbf{C}^n)$, where $\Delta_\gamma$ runs over the determinants of all $r \times r$ submatrices of $\mathscr{A}$, is closed; clearly $U' \subsetneq U$, and hence $U \setminus U' = W^{(m)} \cap \bigcup_\gamma (V_{\Delta_\gamma} \times \mathbf{C}^n)$ (see above) is an open dense subset of $U$. If, for some irreducible component $W_\alpha^{(m)} \ne U$ of $W^{(m)}$ such that $\pi^{(m)}(W_\alpha^{(m)}) \subset V$, $W_\alpha^{(m)} \not\subset \{y\colon \&_\gamma(\Delta_\gamma(y) = 0)\} \times \mathbf{C}^n$, then

$$W_\alpha^{(m)} \cap \left( \bigcup_\gamma \{y\colon \Delta_\gamma(y) \ne 0\} \times \mathbf{C}^n \right) = W_\alpha^{(m)} \cap \bigcup_\gamma (V_{\Delta_\gamma} \times \mathbf{C}^n) \subset U \setminus U'$$

is an open dense subset of $W_\alpha^{(m)}$ and, consequently, $U \supset W_\alpha^{(m)}$ (cf. above); we arrive at a contradiction, hence $W_\alpha^{(m)} \subset \{y\colon \&_\gamma(\Delta_\gamma(y) = 0)\} \times \mathbf{C}^n$. Thus there is exactly one

irreducible component $U$ of $W^{(m)}$, among the components $W_\alpha^{(m)}$ with $\pi^{(m)}(W_\alpha^{(m)}) \subset V$, for which $U \supset W^{(m)} \cap \bigcup_\gamma (V_{\Delta_\gamma} \times \mathbf{C}^n)$; moreover, for any of those $W_\alpha^{(m)} \neq U$, $W_\alpha^{(m)} \cap \bigcup_\gamma (V_{\Delta_\gamma} \times \mathbf{C}^n) = \varnothing$.

Consider, further, the irreducible closed set $V \times \{0\} \subset W^{(m)}$. Since $U$ contains the open and dense in $V \times \{0\}$ set $\bigcup_\gamma (V_{\Delta_\gamma} \times \{0\})$, we see that $U \supset V \times \{0\}$, which implies that $\pi^{(m)}(U) = V$.

We define the set of regular points of $V$ as $\widetilde{\widetilde{V}} = \widetilde{V} \cap (\bigcup_\gamma V_{\Delta_\gamma})$. Further, we call the points of $\widetilde{U} = U \cap (\widetilde{\widetilde{V}} \times \mathbf{C}^n)$ *ordinary* (cf. [1]). Consideration of all irreducible components of $W^{(m-1)}$ completes the inductive step in the definition of $\widetilde{\widetilde{W}}^{(m-1)}$ and $\widetilde{W}^{(m)}$. We have thus proved

LEMMA. *For each irreducible component $W_\alpha^{(0)}$ of the variety $W^{(0)} \subset \mathbf{C}^n$ (defined by system (1)), there exists a uniquely determined sequence of varieties $W_\alpha^{(0)}$, $W_\alpha^{(1)}, \ldots, W_\alpha^{(n)}$ (after a suitable renumbering of the subscripts) such that $W_\alpha^{(m)}$ is an irreducible component of $W^{(m)} \subset \mathbf{C}^{n(m+1)}$ and $\pi^{(m)}(W_\alpha^{(m)}) = W_\alpha^{(m-1)}$ for $1 \leq m \leq n$. For each point $y \in W_\alpha^{(m-1)}$, the inverse image $(\pi^{(m)})^{-1}(y) \cap W^{(m)}$ is a plane of dimension not less than $n-(s_{0,\alpha}+\cdots+s_{m-1,\alpha})$; moreover, for almost all $y \in W_\alpha^{(m-1)}$ we have $(\pi^{(m)})^{-1}(y) \cap W^{(m)} = (\pi^{(m)})^{-1}(y) \cap W_\alpha^{(m)}$ and $\dim((\pi^{(m)})^{-1}(y) \cap W_\alpha^{(m)}) = n - (s_{0,\alpha} + \cdots + s_{m-1,\alpha})$ for some nonnegative integers $s_{0,\alpha}, s_{1,\alpha}, \ldots$. The respective sets $\widetilde{\widetilde{W}}_\alpha^{(m-1)} \subset \widetilde{W}_\alpha^{(m-1)} \subset W_\alpha^{(m-1)}$ of regular and ordinary points of $W_\alpha^{(m-1)}$ are open and dense in $W_\alpha^{(m-1)}$ and, for any $y \in \widetilde{\widetilde{W}}_\alpha^{(m-1)}$, the inverse image $(\pi^{(m)})^{-1}(y) \cap W^{(m)} = (\pi^{(m)})^{-1}(y) \cap W_\alpha^{(m)}$ has dimension $n-(s_{0,\alpha}+\cdots+s_{m-1,\alpha})$; moreover, $\widetilde{W}_\alpha^{(m)} = (\pi^{(m)})^{-1}(\widetilde{\widetilde{W}}_\alpha^{(m-1)}) \cap W_\alpha^{(m)}$. Finally, for each irreducible component $W_\beta^{(m)} \neq W_\alpha^{(m)}$ of $W^{(m)}$ such that $\pi^{(m)}(W_\beta^{(m)}) \subset W_\alpha^{(m-1)}$, the following holds: for any $y \in \pi^{(m)}(W_\beta^{(m)})$,*

$$\dim((\pi^{(m)})^{-1}(y) \cap W^{(m)}) > n - (s_{0,\alpha} + \cdots + s_{m-1,\alpha}).$$

We remark that $\dim(W_\alpha^{(m)}) - \dim(W_\alpha^{(m-1)}) = n - (s_{0,\alpha} + \cdots + s_{m-1,\alpha})$ (see [6]).

Recall (see [1]) that the greatest $h_\alpha$ such that $s_{0,\alpha}+\cdots+s_{h_\alpha-1,\alpha}) \leq n-h_\alpha$ is called the *genus of the system* (1), (2) *relative to the irreducible component* $W_\alpha^{(0)}$. The number $s_{m,\alpha}$ is called the *mth character of the system relative to* $W_\alpha^{(0)}$, the (global) genus of system (1), (2) may be defined as $h = \max_\alpha \{h_\alpha\}$.

**2.** We now turn to a description of the algorithm for computing the genus, and also the characters, of system (1), (2). First we find, by means of the methods of [2] and [3] (see also [4]), the irreducible components $W_\beta^{(m)}$ of the closed varieties $W^{(m)}$. Then, for each component $W_\alpha^{(0)}$, we consecutively find $W_\alpha^{(1)}, \ldots, W_\alpha^{(n)}$ so that $\pi^{(m)}(W_\alpha^{(m)}) = W_\alpha^{(m-1)}$ for all $1 \leq m \leq n$ (in virtue of the lemma, $W_\alpha^{(m)}$ is uniquely determined by $W_\alpha^{(m-1)}$). Finally, we consecutively compute $s_{0,\alpha}, s_{1,\alpha}, \ldots, s_{n-1,\alpha}$ and then $h_\alpha$ (see the remark after the lemma).

The algorithm should verify the equality $\pi^{(m)}(W_\alpha^{(m)}) = W_\alpha^{(m-1)}$. To this end we could again apply the methods of [2]–[5] and construct the projection $\pi^{(m)}(W_\alpha^{(m)})$; however, the time estimate we would get is considerably greater than in the procedure given below. Note that, in virtue of what has been proved above, for any irreducible component $W_\beta^{(m)}$ of $W^{(m)}$, the equality $\pi^{(m)}(W_\beta^{(m)}) = W_\alpha^{(m-1)}$ is tantamount to the

fact that

$$\overline{\pi^{(m)}(W_\beta^{(m)})} \subset W_\alpha^{(m-1)} \quad \text{and} \quad \dim \overline{\pi^{(m)}(W_\beta^{(m)})} = \dim W_\alpha^{(m-1)}.$$

Just as in the proof of Lemma 2 in [5] (cf. also [3]), the algorithm constructs a general point of the closed irreducible set $V = \overline{\pi^{(m)}(W_\beta^{(m)})}$, i.e. an isomorphism of fields of the form

$$\mathbf{Q}(T_1, \dots, T_q)[\theta] \simeq \mathbf{Q}(V) = \mathbf{Q}(X_1, \dots, X_n, X_1^{(1)}, \dots, X_n^{(m-1)}), \tag{4}$$

where $q = \dim \overline{\pi^{(m)}(W_\beta^{(m)})}$, the elements $T_1, \dots, T_q$ are algebraically independent over $\mathbf{Q}$, the element $\theta$ is algebraic over the field $\mathbf{Q}(T_1, \dots, T_q)$, and

$$\Phi(Z) = \mathbf{Q}[T_1, \dots, T_1][Z]$$

is its minimal polynomial, $\mathbf{Q}(V)$ being the field of rational functions on $V$; here $X_1, \dots, X_n, X_1^{(1)}, \dots, X_n^{(m-1)}$ are coordinate functions.

The methods of [2] and [3] (see also [4]) allow us to construct polynomials $\Psi_{\alpha,j}^{(m-1)} \in \mathbf{Q}[X_1, \dots, X_n, X_1^{(1)}, \dots, X_n^{(m-1)}]$ such that the variety $\{y \in \mathbf{C}^{nm} \colon \&_j(\Psi_{\alpha,j}^{(m-1)}(y) = 0)\}$ of their common zeros coincides with $W_\alpha^{(m-1)}$. Then the inclusion $V \subset W_\alpha^{(m-1)}$ is tantamount to the fact that substituting into $\Psi_{\alpha,j}^{(m-1)}$ the images in $\mathbf{Q}(T_1, \dots, T_q)[\theta]$ under the isomorphism (4) of the coordinate functions $X_1, \dots, X_n, X_1^{(1)}, \dots, X_n^{(m-1)}$ yields the zero element of $\mathbf{Q}(T_1, \dots, T_q)[\theta]$ for all $j$ (see [2] and [3]). Given an irreducible component $W_\alpha^{(m-1)}$, this allows us to find $W_\alpha^{(m)}$ among the irreducible components of $W^{(m)}$, which completes the description of the algorithm.

We now estimate the running time of the algorithm. The estimates of [2]–[4] (see also Theorem 1, the remark that follows it and the proof of Lemma 2 in [5]) imply the following estimates for the parameters of general points (see (4)), the polynomials $\Psi_{\alpha,j}^{(m-1)}$ and the time needed for constructing them (to simplify the notation, we identify here the coordinate functions $X_1, \dots, X_n, X_1^{(1)}, \dots, X_n^{(m-1)}$ with their images in $\mathbf{Q}(T_1, \dots, T_q)[\theta]$ under the isomorphism (4) and we drop the indices, writing $X$ for any coordinate function):

$$\deg_Z(\Phi) \le (d+n)^{n^2};$$

$$\deg_{T_1,\dots,T_q}(\Phi), \deg_{X_1,\dots,X_n,X_1^{(1)},\dots,X_n^{(m-1)}}(\Psi_{\alpha,j}^{(m-1)}) \le (dn)^{O(n^2)};$$

$$l(\Phi), l(X), l(\Psi_{\alpha,j}^{(m-1)}) \le M(dn)^{O(n^2)};$$

the number of the polynomials $\Psi_{\alpha,j}^{(m-1)}$ does not exceed $n^4(d+n)^{4n^2}$. The time needed for constructing the general points and the polynomials $\Psi_{\alpha,j}^{(m-1)}$, and also for verifying the inclusion $\overline{\pi^{(m)}(W_\alpha^{(m)})} \subset W_\alpha^{(m-1)}$, may be estimated as $(Mk(dn)^{n^4})^{O(1)}$.

We have thus proved the following

THEOREM. *The characters $s_{0,\alpha}, s_{1,\alpha}, \dots, s_{n-1,\alpha}$, the genus $h_\alpha$ (and thereby the global genus $h = \max_\alpha\{h_\alpha\}$) of the system (1), (2) of exterior differential equations, and also the sequences of varieties $W_\alpha^{(0)}, W_\alpha^{(1)}, \dots, W_\alpha^{(n)}$ of the lemma, can be found in time $(Mk(dn)^{n^4})^{O(1)}$.*

Leningrad Branch
Steklov Mathematical Institute
Academy of Sciences of the USSR

Received 2/DEC/87

## BIBLIOGRAPHY

1. Élie Cartan, *Les systèmes différentiels extérieurs et leurs applications géométriques*, Actualités Sci. Indust., no. 994, Hermann, Paris, 1946.

2. D. Yu. Grigor'ev, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 20–79; English transl. in J. Soviet Math. **34** (1986), no. 4.

3. A. L. Chistov, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 124–188; English transl. in J. Soviet Math. **34** (1986), no. 4.

4. D. Yu. Grigor'ev and A. L. Chistov, Dokl. Akad. Nauk SSSR **275** (1984), 1302–1306; English transl. in Soviet Math. Dokl. **29** (1984).

5. D. Yu. Grigor'ev, Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), 1106–1120; English transl. in Math. USSR Izv. **29** (1987).

6. Armand Borel, *Linear algebraic groups*, Benjamin, New York, 1969.

7. I. R. Shafarevich, *Basic algebraic geometry*, "Nauka", Moscow, 1972; English transl., Springer-Verlag, 1974.

Translated by W. LISIECKI