21. A. L. Chistov, "Algorithm with polynomial complexity for factoring polynomials and finding components of varieties in subexponential time," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, **137**, 124-188 (1984).
22. D. Yu. Grigor'ev, "The complexity of solutions in the first-order theory of real closed fields," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, **174**, 53-100 (1988).
23. J. Renegar, "A faster PSPACE algorithm for deciding the existential theory of the reals," Techn. Rep. N 792, College of Engineering, Cornell University (1988).
24. S. Lang, Algebra, Addison-Wesley, Reading (1965).
25. N. G. Chebotarev, The Theory of Algebraic Functions, Moscow—Leningrad (1948).
26. M. Ben-Or, D. Kozen, and J. Reif, "The complexity of elementary algebra and geometry," in: Proc. Sixteenth ACM Symp. Theor. Comput., 459-464 (1984).
27. L. E. Heindel, "Integer arithmetic algorithms for polynomial real zero determination," J. Assoc. Comput. Mach., **18**, No. 4, 533-548 (1971).

COMPLEXITY OF QUANTIFIER ELIMINATION IN THE THEORY OF ORDINARY DIFFERENTIALLY CLOSED FIELDS

D. Yu. Grigor'ev

UDC 518.5

This article presents an algorithm for elimination of quantifiers in the theory of first-order ordinary differentially closed fields; the algorithm has elementary complexity. The previously known algorithm, due to A. Seidenberg, is of non-elementary complexity. In the description of the algorithm an important procedure is construction of a polynomial-time algorithm for finding the greatest common divisor of a family of polynomials in one variable with parametric coefficients. The GCD is itself a polynomial in several variables.

INTRODUCTION

Assume that we are given a formula in the theory of first-order ordinary differentially closed fields:

$$Q_1 u_1 \dots Q_n u_n (\Omega), \tag{1}$$

where $Q_1,\dots,Q_n$ are quantifiers (existential or universal) and Ω is a quantifier-free formula containing, as atomic subformulas, expressions of the form $(f_i = 0)$, $1 \le i \le N$. Here $f_i \in F\{u_1,\dots,u_n,v_1,\dots,v_m\}$ are differential polynomials (with differentiation by X) and the variables $u_1,\dots,u_n$ in formula (1) are bound, while $v_1,\dots,v_m$ are free. The field is $F = \mathbf{Q}(T_1,\dots,T_\varepsilon)[\eta]$, where $T_1,\dots,T_\varepsilon$ are algebraically independent over $\mathbf{Q}$, the element η is algebraic over the field $\mathbf{Q}(T_1,\dots,T_\varepsilon)$ and $\varphi(Z) \in \mathbf{Q}[T_1,\dots,T_\varepsilon][Z]$ is its minimal polynomial, i.e., $F \simeq \mathbf{Q}(T_1,\dots,T_\varepsilon)[Z]/(\varphi)$. By the (bit) size of a rational number p/q, where the integers $p,q \in \mathbf{Z}$ are relatively prime, we mean $l(p/g) = \log_2(|pq| + 1) + 1$ (see [2, 3, 8, 9, 10, 11]. For any polynomial $g \in F[Y_1,\dots,Y_k]$ we write $g = \sum_{j_1,\dots,j_k;\, 0 \le j < \deg_Z(\varphi)} (g_{j_1,\dots,j_k,j}/g_0)\eta^j Y_1^{j_1}\dots Y_k^{j_k}$, where $g_{j_1,\dots,j_k,j}, g_0 \in \mathbf{Q}[T_1,\dots,T_\varepsilon]$ and the degree $\deg_{T_1,\dots,T_\varepsilon}(g_0)$ is the smallest possible. We write $\deg_{T_1,\dots,T_\varepsilon}(g) = \max_{j_1,\dots,j_k,j} \{\deg_{T_1,\dots,T_\varepsilon}(g_{j_1,\dots,j_k,j}), \deg_{T_1,\dots,T_\varepsilon}(g_0)\}$ for the elements $T_1,\dots,T_\varepsilon$. Let $g_0 = \sum_{i_1,\dots,i_\varepsilon} g_0^{(i_1,\dots,i_\varepsilon)} T_1^{i_1}\dots T_\varepsilon^{i_\varepsilon}$, where $g_0^{(i_1,\dots,i_\varepsilon)} \in \mathbf{Q}$; we define (bit) sizes of coefficients $l(g_0) = \max_{i_1,\dots,i_\varepsilon} \{l(g_0^{(i_1,\dots,i_\varepsilon)})\}$ and $l(g) = \max_{j_1,\dots,j_k,j} \{l(g_{j_1,\dots,j_k,j}), l(g_0)\}$.

Translated from Zapiski Nauchnykh Seminarov Leingradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova, Vol. 176, pp. 53-67, 1989.

 0090-4104/92/5903-0814$12.50

A differential ring $F\{u_1,\ldots,u_n,v_1,\ldots,v_m\}$ (see [5, 7]) is generated as a ring of polynomials over F[X] by the derivatives $u_s,u_s^{(1)},u_s^{(2)},\ldots,v_t,v_t^{(1)},v_t^{(2)},\ldots$ for $1 \le s \le n$, $1 \le t \le m$, where $u_s^{(k)} = \frac{d^k u_s}{dx^k}$ (the elements of the field F are treated as constants, i.e., for any $\alpha \in F$ we have $\alpha^{(1)} = 0$). We denote by $\mathrm{ord}_{u_s}(f_i)$ the largest of the order of the derivatives $u_s,u_s^{(1)}$, $u_s^{(2)},\ldots$ of the variable u_s in the differential polynomial f_i. We assume that $\mathrm{ord}_{u_s}(f_i) \le r$; $\mathrm{ord}_{v_t}(f_i) \le r$ for all $1 \le s \le n$, $1 \le t \le m$; then f_i can be treated as an (ordinary) polynomial in the ring

$$F\left[x,u_1,u_1^{(1)},\ldots,u_1^{(r)},\ldots,u_n,u_n^{(1)},\ldots,u_n^{(r)},v_1,v_1^{(1)},\ldots,v_1^{(r)},\ldots,v_m,v_m^{(1)},\ldots,v_m^{(r)}\right].$$

We also assume that the degree $\deg(f_i)=\deg_{x,u_1,\ldots,u_1^{(r)},\ldots,v_m^{(1)},\ldots,v_m^{(r)}}(f_i)$ of the polynomial f_i as an element of this ring (with respect to all variables) is less than d; moreover, we assume $\deg_Z(\varphi) < d_1$, $\deg_{\tau_1,\ldots,\tau_\varepsilon}(\varphi)$, $\deg_{\tau_1,\ldots,\tau_\varepsilon}(f_i) < d_2$, and, finally, $l(\varphi),l(f_i) \le M$ for all $1 \le i \le N$.

For the functions $g_1 > 0,g_2 > 0,\ldots,g_s > 0$ we write $g_1 \le g_2\,\mathcal{P}(g_3,\ldots,g_s)$ if, for some polynomial P, we have $g_1 \le g_2 P(g_3\ldots g_s)$.

In [7] there is a description of a method for eliminating quantifiers in the theory of first-order ordinary differentially closed fields, which method makes it possible to use formulas of the form (1) to construct equivalent quantifier-free formulas. Here and below we take equivalence of formulas to mean over the differential closure of the field of fractions $F\langle u_1,\ldots,u_n, v_1,\ldots,v_m\rangle$ of the ring $F\{u_1,\ldots,u_n,v_1,\ldots,v_m\}$ (see [5, 7]). However, the time complexity of the method of [7] is non-elementary and, in particular, is not bounded above by any tower of exponents of fixed height. The fundamental result of the present paper is the following theorem, in which we construct an algorithm for quantifier elimination with elementary complexity (see also [1]).

THEOREM. A formula of the form (1) in the theory of first-order ordinary differential equations can be used to construct an equivalent quantifier-free formula of this theory in the form

$$\bigvee_{1\le i\le N}\Big(\&_{1\le j\le K}(g_{i,j}=0)\&(g_{i,0}\ne 0)\Big), \tag{2}$$

where $g_{i,j} \in F\{v_1,\ldots,v_m\}$ are differential polynomials; the execution time is polynomial in $M,((Nd)^{m^n}d_1d_2)^{cr2^n\varepsilon+m}$ for some constant $c > 1$. In addition, for the polynomials $g_{i,j}$ we have the following estimates: $\mathrm{ord}_{v_t}(g_{i,j}) \le r2^n$; $N,K,\deg(g_{i,j}) \le (Nd)^{m^n c r 2^n} = M$; $\deg_{\tau_1,\ldots,\tau_\varepsilon}(g_{i,j}) \le d_2\mathcal{P}(Md_1^{cr2^n})$ and for the sizes of the coefficients $l(g_{i,j}) \le (M+\varepsilon\log(d_2))\mathcal{P}(Md_1^{cr2^n})$.

The method of [7] contains two procedures that transform a system of differential equations into the disjunction of systems. The first of these methods is used when, for some distinguished variable, at least two polynomials of the system contain its derivative of maximum order. Application of the first procedure in each of the systems leaves no more than one polynomial containing this derivative. In the second procedure, the system is decomposed and the order of the distinguished variable is reduced if it occurs in a polynomial of the system. It is the first procedure of [7] that leads to the non-elementary complexity. In this paper we execute a transformation that leads to the disjunction of systems that each contain no more than one polynomial containing a derivative of maximal order of the distinguished variable; our method is completely different and is based on construction of the greatest common divisor of a family of polynomials in one variable with parametric coefficients (Lemma 1, §1); this GCD algorithm appears to be of independent interest. The proof of Lemma 1 is similar to the construction of [9] (see also [11]), but direct application of the results of [9] yields a worse complexity than Lemma 1. In §2 we present a modification of the procedure of [7] for splitting and reducing the order of the distinguished variable, an algorithm for quantifier elimination, and an analysis of the complexity of this algorithm.

In [7] there are also algorithms for quantifier elimination in the theory of higher-order differentially closed fields, but it is currently unknown whether there are algorithms of elementary complexity for this problem.

§1. FINDING THE GREATEST COMMON DIVISOR OF A FAMILY OF POLYNOMIALS WITH PARAMETRIC COEFFICIENTS

We present the fundamental result of this section (Lemma 1) in greater generality than required for proof of our theorem, namely, we present it for polynomials with coefficients in a field H that is finitely generated over a simple subfield that includes a field of nonzero characteristic (see [2, 3, 8, 9]).

Thus, $H = H_0(T_1,\dots,T_\varepsilon)[\eta]$, where either $H_0 = \mathbf{Q}$ (see below) or the finite field $H_0 = \mathbf{F}_p$ (here p is a prime number), i.e., H_0 is a prime subfield, $T_1,\dots,T_\varepsilon$ are algebraically independent over H_0, and the element η is algebraically separable over the field $H_0(T_1,\dots,T_\varepsilon)$; let $\varphi \in H_0(T_1,\dots,T_\varepsilon)[Z]$ be its minimial polynomial.

By the notation length $l(\alpha)$ for $\alpha \in \mathbf{F}_p$ we mean the number $\log_2(p)$. The degree and notation length for the coefficients are defined as in the introduction to this paper.

Consider the polynomials $h_0,h_1,\dots,h_k \in H[X_1,\dots,X_n,Y]$ and assume that (see below)

$$\begin{aligned} &\deg_Z(\varphi)<d_1;\deg_{X_1,\dots,X_n,Y}(h_i)<d_0;\deg_{T_1,\dots,T_\varepsilon}(h_i),\deg_{T_1,\dots,T_\varepsilon}(\varphi)<d_2;\\ &l(\varphi),l(h_i)\leqslant M \end{aligned} \tag{3}$$

for all $0 \le i \le k$. We write $h_i = \sum_j h_{i,j} Y^j$, where $h_{i,j} \in H[X_1,\dots,X_n]$. We denote the algebraic closure of the field H by $\bar{H}$.

LEMMA 1. For given $h_0,\dots,h_k$ we can construct two families of polynomials $g_{q,t} \in H[X_1,\dots,X_n]$, $\Psi_q \in H[X_1,\dots,X_n,Y]$ for $1 \le q \le N_1$, $0 \le t \le N_2$, with the following properties:

a) the quasiprojective varieties $\mathcal{V}_q = \{x \in \bar{H}^n: g_{q,1}(x)=\dots= g_{q,N_2}(x)=0, g_{q,0}(x)\neq 0\}$ $1 \le q \le N_1$, form a partition of the open set (in the Zariski topology — see, for example, [4]) $H^n\setminus\{x \in \bar{H}^n$: $h_{i,j}(x) = 0$ for all $1 \le i \le k$ and $j\}$;

b) for any $1 \le q \le N_1$ the following two varieties coincide: $\{(x,y)\in \bar{H}^n\times\bar{H}=\bar{H}^{n+1}: h_1(x,y)=\dots=h_k(x,y)=0; h_0(x,y)\neq 0\}\cap(\mathcal{V}_q\times\bar{H}) = \{(x,y)\in\bar{H}^{n+1}: \Psi_q(x,y)=0\}\cap(\mathcal{V}_q\times\bar{H})$. Moreover, the leading coefficient $lc_Y(\Psi_q) \in H[X_1,\dots,X_n]$ is nonzero everywhere on $\mathcal{V}_q$. The time required to construct the indicated families of polynomials is bounded by some polynomial of M, $(d_1d_2)^{\varepsilon+1}$, $d_0^{n+\varepsilon}$, and k. We have the following estimates for the parameters of the polynomials:

$$\begin{aligned} &\deg_{X_1,\dots,X_n,Y}(\Psi_q),\deg_{X_1,\dots,X_n}(g_{q,t})\leqslant \mathcal{P}(d_0);\\ &\deg_{T_1,\dots,T_\varepsilon}(\Psi_q),\deg_{T_1,\dots,T_\varepsilon}(g_{q,t})\leqslant d_2\mathcal{P}(d_1,d_0);\\ &l(\Psi_q),l(g_{q,t})\leqslant (M+(\varepsilon+n)\log(d_2))\mathcal{P}(d_1,d_0); N_1,N_2\leqslant \kappa\mathcal{P}(d_0^n). \end{aligned} \tag{4}$$

Remark. 1) Property b) shows that Ψ_q is the analog of the greatest common divisor of the polynomials $h_1,\dots,h_k$ (assuming $h_0 \neq 0$), treated as polynomials in the variable Y on the quasiprojective varieties $\mathcal{V}_q$.

2) Properties a) and b) hold for an arbitrary algebraically closed field (not only $\bar{H}$) containing H.

Proof of Lemma 1. For any $1 \le i \le k$, $0 \le j < d_0$, consider the quasiprojective variety $\mathcal{U}_{i,j} = \{x\in\bar{H}^n: h_{1,d_0-1}(x) = \dots=h_{1,0}(x)=h_{2,d_0-1}(x)=\dots=h_{2,0}(x)=\dots=h_{i,d_0-1}(x)=\dots=h_{i,i+1}(x)=0; h_{i,j}(x)\neq 0\}$. It is clear that $\bigcup_{i,j}\mathcal{U}_{i,j} = \bar{H}^n\setminus\{x\in\bar{H}^n: h_{i,j}(x) = 0$ for all $1 \le i \le k$ and $j\}$. We write $h_{i,j} = \sum_{0\le\beta\le j} h_{i,\beta}Y^\beta$. The system

$$h_1=\dots=h_k=0;\ h_0\neq 0 \tag{5}$$

is equivalent to the disjunction over all $1 \le i \le k$, $0 \le j < d_0$ of the following systems:

$$\begin{aligned} &\tilde{h}_{i,j} = h_{i+1}=\dots=h_k=h_{1,d_0-1}=\dots=h_{1,0}=h_{2,d_0-1}=\dots=h_{2,0}=\dots=h_{i-1,d_0-1}=\dots\\ &\dots=h_{i-1,0}=h_{i,d_0-1}=\dots=h_{i,j+1}=0; h_0h_{i,j}\neq 0. \end{aligned}$$

We temporarily fix $1 \le i \le k$, $0 \le j < d_0$, and consider the system

$$\tilde{h}_{i,j} = h_{i+1}=\dots=h_k=0;\ h_0\neq 0. \tag{6}$$

We now introduce new variables Y_1 and Y_0. For any point $x = (x_1,\dots,x_n)$ an element y satisfies system $(6)_x$ (which is obtained from (6) by substituting $x_1,\dots,x_n$ for $X_1,\dots,X_n$) if and only if there exists a y_1 such that $\tilde{h}_{i,j}(x,y)=h_{i+1}(x,y)=\dots=h_k(x,y)=y_1h_0(x,y)-1=0$. We now introduce polynomials that are homogeneous with respect to the variables Y_1, Y, and Y_0: $\bar{h}_l(X_1,\dots,X_n,Y_1,Y,Y_0) = Y_0^{\deg_Y(h_l)}h_l(X_1,\dots,X_n,Y/Y_0)$ for $i < l \le k$; $\bar{h}_i(X_1,\dots,X_n,Y_1,Y,Y_0) =$

$$\begin{aligned} &Y_0^j\tilde{h}_{i,j}(X_1,\dots,X_n,Y/Y_0);\ \bar{h}_0(X_1,\dots,X_n,Y_1,Y,Y_0) =\\ &Y_0^{\deg_Y(h_0)+1}((Y_1/Y_0)h_0(X_1,\dots,X_n,Y/Y_0)-1). \end{aligned}$$

We consider some field H_1, a point $x = (x_1,\dots,x_n) \in \bar{H}1^n$, and a homogeneous system of equations (in the variables Y_1, Y, and Y_0):

$$\bar{h}_i(x,Y_1,Y,Y_0) = \bar{h}_{i+1}(x,Y_1,Y,Y_0) = \dots = \bar{h}_\kappa(x,Y_1,Y,Y_0) = \bar{h}_0(x,Y_1,Y,Y_0) = 0. \qquad (7)_x$$

We assume that $h_{ij}(x) \neq 0$; then system $(6)_x$ has a finite number of solutions. If $y \in \bar{H}_1$ is a solution of system $(6)_x$, then the point $(1/h_0(x,y):y:1) \in \mathbf{P}^2(H_1)$ of the projective space is a solution of $(7)_x$. Conversely, if $(y_1:y:y_0) \in \mathbf{P}^2(\bar{H}_1)$ is a solution of $(7)_x$ and $y_0 \neq 0$, then y/y_0 is a solution of system $(6)_x$ and $y_1/y_0 = 1/h_0(x,y/y_0)$; if, however, $y_0 = 0$, then $y = 0$, since $lc_Y(\bar{h}_{i,j}) = h_{i,j}$. Thus, system $(7)_x$ has a finite number of solutions in $\mathbf{P}^2(\bar{H}_1)$, and, in this case, all of the solutions, except, perhaps, for (1:0:0), bijectively correspond to the solutions of system $(6)_x$ (under the assumption $h_{i,j}(x) \neq 0$).

Now, we require a construction from [6]. Let $g_0,\dots,g_{t-1} \in H_1[Y_0,\dots,Y_m]$ be homogeneous polynomials of degrees $\gamma_0 \geq \dots \geq \gamma_{t-1}$, respectively. We introduce variables $U_0,\dots,U_m$ that are algebraically independent over the field $H_1(Y_0,\dots,Y_m)$ and the polynomial $g_t = Y_0U_0 + \dots + Y_mU_m \in H_1(U_0,\dots,U_m)[Y_0,\dots,Y_m]$ with degree $\gamma_t = 1$. We set $D = \left(\sum_{1 \leq l \leq \min\{t-1,m\}} (\gamma_l - 1)\right) + \gamma_0$. Consider the linear (over the field $H_1(U_0,\dots,U_m)$) map $\mathcal{A}: \mathcal{H}_0 \oplus \dots \oplus \mathcal{H}_t \to \mathcal{H}$, where $\mathcal{H}_l$ (respectively, $\mathcal{H}$) is the space of homogeneous polynomials in $Y_0,\dots,Y_m$ over the field $H_1(U_0,\dots,U_m)$ of degree $D - \gamma_l$ (respectively, D) for $0 \leq l \leq t$; namely, $\mathcal{A}(f_0,\dots,f_t) = f_0g_0 + \dots + f_tg_t$. We fix some enumeration of the monomials of degrees $D - \gamma_0,\dots,D - \gamma_t, D$, respectively, and we write the operator $\mathcal{A}$ in coordinates corresponding to this enumeration; we thus obtain a $\binom{m+D}{m} \times \sum_{0 \leq l \leq t} \binom{m+D-\gamma_l}{m}$ matrix A. The matrix A can be represented in the form $A = (A^{(num)}, A^{(for)})$, where the submatrix $A^{(num)}$ is called the numerical part of the matrix A and contains $\sum_{0 \leq l \leq t-1} \binom{m+D-\gamma_l}{m}$ columns, whose elements belong to the field H_1; the submatrix $A^{(for)}$, which is called the formal part of the matrix A, contains $\binom{m+D-1}{m}$ columns, whose elements are linear forms in the variables $U_0,\dots,U_m$ over the field H_1. The following result was established in [6].

Proposition 1. a) The system $g_0 = \dots = g_{t-1} = 0$ has a finite number of solutions in $\mathbf{P}^m(\bar{H}_1)$ if and only if the rank $rg(A) = \binom{m+D}{m}$; we write $r = \binom{m+D}{m}$ and we assume in paragraphs b), c), and d) that $rg(A) = r$;

b) all $r \times r$ minors of the matrix A together generate, in the ring $H_1[U_0,\dots,U_m]$, a principal ideal, whose generator $R \in H_1[U_0,\dots,U_m]$ is also their greatest common divisor;

c) the form R, which is homogeneous with respect to $U_0,\dots,U_m$, factors into product $R = \prod_{1 \leq \varkappa \leq D_1} L_\varkappa$, where $L_\varkappa = \sum_{0 \leq \alpha \leq m} \xi_\alpha^{(\varkappa)} U_\alpha$ is a linear form, $(\xi_0^{(\varkappa)}:\dots:\xi_m^{(\varkappa)}) \in \mathbf{P}^m(\bar{H}_1)$ is a root of the system $g_0 = \dots = g_{t-1} = 0$, and the number of appearances of the form $L_\varkappa$ in the product R coincides with the multiplicity of the roots $(\xi_0^{(\varkappa)}:\dots:\xi_m^{(\varkappa)})$ of the system $g_0 = \dots = g_{t-1} = 0$ $(1 \leq \varkappa \leq D_1)$;

d) let Δ be a nonsingular $r \times r$ submatrix of the matrix A that contains $rg(A^{(num)})$ columns in the numerical part $A^{(num)}$ of the matrix A (it is not difficult to see that a matrix Δ with the properties given exists); then $\det(\Delta)$ coincides with R up to factors of H_1^* and $\deg_{U_0,\dots,U_m}(R) = D_1 = r - rg(A^{(num)})$.

It is natural to call the polynomial R the generalized U-resultant of the system $g_0 = \dots = g_{t-1} = 0$.

We now apply the construction we have described to $(7)_{(X_1,\dots,X_n)}$ and the field $H_1 = H(X_1,\dots,X_n)$; we obtain a matrix A with elements in the ring $H[X_1,\dots,X_n,U_1,U,U_0]$. By 1a), for any point x we have $rg(A_x) = r = \binom{D+2}{2}$ for $h_{i,j}(x) \neq 0$ (recall that r is the number of rows in the matrix A). We define a variant of Gauss' algorithm (VGA) as a sequence of pairs of indices $(\alpha_0,\beta_0),(\alpha_1,\beta_1),\dots,(\alpha_\rho,\beta_\rho)$, where $\alpha_\lambda \neq \alpha_\nu$, $\beta_\lambda \neq \beta_\nu$ for $\lambda \neq \nu$. The VGA determines a sequence of matrices $A^{(0)} = A$, $A^{(1)},\dots,A^{(\rho+1)}$. We write $A^{(l)} = (a_{\alpha,\beta}^{(l)})$; then $a_{\alpha,\beta}^{(l+1)} = a_{\alpha,\beta}^{(l)} - a_{\alpha_l,\beta}^{(l)} a_{\alpha,\beta_l}^{(l)} / a_{\alpha_l,\beta_l}^{(l)}$ for $\alpha \neq \alpha_0,\dots,\alpha_l$ and $a_{\alpha_s,\beta}^{(l+1)} = a_{\alpha_s,\beta}^{(l)}$ for $0 \leq s \leq l$; here the leading element $a_{\alpha_l,\beta_l}^{(l)} \neq 0$ for all $0 \leq l \leq \rho$. Then $a_{\alpha,\beta_s}^{(l)} = 0$, if $0 \leq s \leq l - 1$ and $\alpha \neq \alpha_0,\dots,\alpha_s$. Let $\Delta_{\alpha,\beta}^{(l)}$, where $\alpha \neq \alpha_0,\dots,\alpha_{l-1}; \beta \neq \beta_0,\dots,\beta_{l-1}$, denote the determinant of the $(l + 1) \times (l + 1)$ submatrix of A generated by the rows $\alpha_0,\dots,\alpha_{l-1},\alpha$ and the columns $\beta_0,\dots,\beta_{l-1},\beta$. Then, $a_{\alpha,\beta}^{(l)} = \Delta_{\alpha,\beta}^{(l)} / \Delta_{\alpha_{l-1},\beta_{l-1}}^{(l-1)}$ (see, for example, [4]).

We will construct a sequence of VGA's $\Gamma_1,\Gamma_2,\dots$, and a sequence of polynomials $P_1,P_2,\dots \in H[X_1,\dots,X_n][U_1,U,U_0]$ that are linearly independent over H. Here the algorithm Γ_s is properly applied to the matrix $A_{\tilde{x}}$ for any point $\tilde{x}$ in the

(possibly empty) quasiprojective variety $\mathcal{W}_S = \{x \in \bar{H}^n : 0 = P_t(x,U_1,U,U_0) \in \bar{H}[U_1,U,U_0]$ for all $1 \le t < s$ and $P_s(x,U_1, U,U_0) \neq 0\}$. Moreover, $\bigcup_S \mathcal{W}_S \supset \mathcal{U}_{i,j}$ (see the beginning of the proof of the lemma).

Discussions of the current VGA Γ_t require the notation introduced above (we apply Γ_t to the matrix A, obtaining the sequence $A^{(0)} = A, A^{(1)}, \ldots$). We assume that $\Gamma_1,\ldots,\Gamma_s; P_1,\ldots,P_s$ have already been constructed ($s \ge 0$). Then, as Γ_{s+1} we take a VGA in which, for any $l \ge 0$, the index of the column β_l of the leading element (α_l,β_l) of the matrix $A^{(l)}$ is the smallest such that $\beta_l > \beta_{l-1}$ and the polynomials $P_1,\ldots, P_s, \prod_{0 \le t \le l} \Delta^{(t)}_{\alpha_t,\beta_t}$ are linearly independent over H. Assume that we are unable to extend the sequence $(\alpha_0,\beta_0),\ldots,(\alpha_{\rho_{s+1}},\beta_{\rho_{s+1}})$ without violating the conditions that have been given. We take this sequence for the VGA Γ_{s+1} and we define the polynomial

$$P_{s+1} = \prod_{0 \le t \le \rho_{s+1}} \Delta^{(t)}_{\alpha_t,\beta_t}. \tag{8}$$

If each element of the matrix A is linearly dependent over H on $P_1,\ldots,P_s$, we can terminate the process of constructing $\Gamma_1,\ldots,\Gamma_s$ (in this case it is impossible to construct Γ_{s+1}).

We should note that if $\rho_{s+1} < r - 1$, then $\mathcal{W}_{s+1} \cap \mathcal{U}_{i,j} = \emptyset$. Indeed, let $x \in \mathcal{W}_{s+1} \cap \mathcal{U}_{i,j}$. Then, by induction on $0 \le l < \rho_{s+1}$, we find that in the matrix $(A^{(l)})_x$ we have $(a^{(l+1)}_{\alpha,\beta})_x = (\Delta^{(l+1)}_{\alpha,\beta})_x / (\Delta^{(l)}_{\alpha_l,\beta_l})_x = 0$ for $\beta_l < \beta < \beta_{l+1}$ and α is different from $\alpha_0,\ldots,\alpha_l$, since $(\Delta^{(l)}_{\alpha_l,\beta_l})_x \neq 0$ for $x \in \mathcal{W}_{s+1}$ (see (8)); on the other hand, $(\Delta^{(l+1)}_{\alpha,\beta})_x = 0$, since otherwise we might have $\beta_{l+1} \le \beta$, which contradicts the choice of β_{l+1}. It follows that $(a^{(l+1)}_{\alpha,\beta})_x = 0$ for $\beta < \beta_{l+1}$ and α different from $\alpha_0,\ldots,\alpha_l$, since elementary transformations we have performed preserve this property. Similarly, $(a^{(\rho_{s+1}+1)}_{\alpha,\beta})_x = 0$ for α different from $\alpha_0,\ldots,\alpha_{\rho_{s+1}}$. As a result, $\mathrm{rg}(A_x) = \rho_{s+1} + 1 < r$, which contradicts the fact that $x \in \mathcal{U}_{i,j}$ and assumption 1a) (see system $(7)_x$).

It is clear that $\mathcal{U}_{i,j} \subset \bigcup_S \mathcal{W}_S$, since, for $x \in \mathcal{U}_{i,j}$ we have $\mathrm{rg}(A_x) = r$. In particular, let $(a_{\alpha,\beta})_x \neq 0$ for some α,β, so if $x \notin \bigcup_S \mathcal{W}_S$, i.e., $0 = P_1(x,U_1,U,U_0) = P_2(x,U_1,U,U_0) = \ldots$, the element $a_{\alpha,\beta}$ might not be linearly dependent over H of the polynomials $P_1,P_2,\ldots$, which contradicts the condition for terminating the process of constructing $\Gamma_1,\Gamma_2,\ldots$.

We will show that for any point $x \in \mathcal{W}_{s+1} \cap \mathcal{U}_{i,j}$ the polynomials R_x corresponding under assumption 1b) to the matrix A_x coincide (up to factors of H^*) with the minor $\Delta_{s+1}(x) = \Delta_{\alpha_{\gamma-1},\beta_{\gamma-1}}(x) \neq 0$ corresponding to the VGA Γ_{s+1}. Indeed, assume that λ is such that the "cell" $(\alpha_{\lambda-1},\beta_{\lambda-1})$ is in the numerical part $A^{(\mathrm{num})}$ of the matrix A, and the "cell" $(\alpha_\lambda,\beta_\lambda)$ is in the formal part $A^{(\mathrm{for})}$; then $\mathrm{rg}(A_x^{(\mathrm{num})}) = \lambda$, since $(a_{\alpha,\beta}^{(\lambda)})_x = 0$ if $\beta < \beta_\lambda$ and α is different from $\alpha_0,\ldots,\alpha_{\lambda-1}$ (see below). Thus, $\Delta_{s+1}(x)$ coincides with R_x (up to factors from H^*), by assumption 1d); in addition $r - \lambda = \deg_{U_1,U,U_0}(\Delta_{s+1})$; we write $D_2 = r - \lambda$.

Now, we write $\Delta_{s+1} = \sum_{0 \le \hat{\omega} \le D_2} E^{(\hat{\omega})}_{s+1} U_0^{D_2 - \hat{\omega}}$, where $E^{(\omega)}_{s+1}(X_1,\ldots,X_n) \in F[X_1,\ldots,X_n,U_1,U]$. Also, we introduce the quasiprojective varieties $\mathcal{W}^{(\omega)}_{s+1} = \{x \in \mathcal{W}_{s+1} : 0 = E^{(0)}_{s+1}(x) = \ldots = E^{(\omega-1)}_{s+1}(x) \in \bar{H}[U_1,U];\ 0 \neq E^{(\omega)}_{s+1}(x)\}$. Then, $\mathcal{W}^{(\omega_1)}_{s+1} \cap \mathcal{W}^{(\omega_2)}_{s+1} = \emptyset$ for $\omega_1 \neq \omega_2$ and $\mathcal{W}_{s+1} = \bigcup_{0 \le \hat{\omega} \le D_2} \mathcal{W}^{(\hat{\omega})}_{s+1}$. Since, for $x \in \mathcal{W}_{s+1} \cap \mathcal{U}_{i,j}$, it follows from assumption 1c) and what we proved above that $\Delta_{s+1}(x) = \prod_x L_x^{c_x}$, where the linear forms $L_x = \zeta_1^{(x)} U_1 + \zeta^{(x)} U + \zeta_0^{(x)} U_0$ bijectively correspond to the solutions $(\zeta_1^{(x)} : \zeta^{(x)} : \zeta_0^{(x)}) \in \mathbf{P}^2(\bar{H})$ of system $(7)_x$, for $x \in \mathcal{W}^{(\omega)}_{s+1} \cap \mathcal{U}_{i,j}$ the form $E^{(\omega)}_{s+1}(x) \mid \Delta_{s+1}(x)$ coincides (up to factors from $\bar{H}^*$) with the product of all those L_μ for which $\zeta_0^{(\mu)} = 0$. Then $\zeta_0^{(\mu)} = 0$ for each index μ according to what was proved before Proposition 1, so $E_{s+1}{}^{(\omega)}(x)$ coincides with $U_1{}^\omega$ (up to factors from $\bar{H}^*$). We write $E^{(\omega_1)}_{s+1} = \sum_{0 \le \gamma \le \omega_1} E^{(\omega_1)}_{s+1,\gamma} U_1^{\omega_1 - \gamma} U^\gamma$, where $E^{(\omega_1)}_{s+1,\gamma} \in H[X_1,\ldots,X_n]$; then $E^{(\omega)}_{s+1}(x) = E^{(\omega)}_{s+1,0}(x) U_1^{\hat{\omega}}$ for $x \in \mathcal{W}^{(\omega)}_{s+1} \cap \mathcal{U}_{i,j}$. Further, $\Delta_{s+1}(x)/E_{s+1}{}^{(\omega)}(x)$ coincides (up to factors from $\bar{H}^*$) with product $\prod L_\nu^{c_\nu}$ of all those forms L_ν for which $\zeta_0^{(\nu)} \neq 0$ with $x \in \mathcal{W}^{(\omega)}_{s+1} \cap \mathcal{U}_{i,j}$; in particular, relation $E^{(\omega)}_{s+1}(x) \mid E^{(\omega_1)}_{s+1}(x)$ holds in the ring $\bar{H}[U_1,U]$ for any $\omega_1 \ge \omega$. Thus, $E_{s+1,\gamma}{}^{(\omega_1)}(x) = 0$ when $\omega_1 - \gamma < \omega$, so $\Delta_{s+1}(x)/E^{(\omega)}_{s+1}(x) = \frac{1}{E^{(\omega)}_{s+1,0}(x)} \sum_{\omega \le \omega_1 \le D_2} U_0^{D_2 - \omega_1} \sum_{0 \le \gamma \le \omega_1 - \omega} E^{(\omega_1)}_{s+1,\gamma}(x) U_1^{\omega_1 - \gamma - \omega} U^\gamma \in \bar{H}[U_1,U,U_0]$. As a result, the polynomial $(\Delta_{s+1}(x)/E^{(\omega)}_{s+1}(x))(0,-1,Y) \in \bar{H}[Y]$ coincides (up to factors from $\bar{H}^*$) with the product $\prod (Y - y_\nu)^{c_\nu}$, where $y_\nu = \zeta^{(\nu)}/\zeta_0^{(\nu)}$ runs through

the solutions of system $(6)_x$ (see the material above Proposition 1) for all $x \in \mathcal{V}^{(\omega)}_{s+1} \cap \mathcal{U}_{i,j}$.

For fixed i, j, m, and s, we write $\mathcal{V}^{(i)}_q = \mathcal{V}^{(\omega)}_{s+1} \cap \mathcal{U}_{i,j}$ (from which we obtain polynomials $g_{q,t_1}^{(1)}, g_{q,t_2}^{(2)} \in H[X_1,\ldots,X_n]$ such that $\mathcal{V}^{(i)}_q = \{x \in \overline{H}^n : \&_{t_1}(g^{(1)}_{q,t_1}(x)=0) \& \vee_{t_2}(g^{(2)}_{q,t_2}(x)\neq 0)\}$; fixing some t_3, we obtain pairwise disjoint quasiprojective varieties $\mathcal{V}_q = \{x \in \overline{H}^n : \&_{t_1}(g^{(1)}_{q,t_1}(x)=0) \& \&_{t_2<t_3}(g^{(2)}_{q,t_2}(x)=0) \& (g^{(2)}_{q,t_3}(x)\neq 0)\}$ and thus the polynomials $g_{q,t}$ required by Lemma 1a)). In addition, we set $\Psi_q = \sum_{\omega \le \omega_1 \le D_2} Y^{D_2-\omega_1} E^{(\omega_1)}_{s+1,\omega_1-\omega}(-1)^{\omega_1-\omega} \in H[X_1,\ldots,X_n,Y]$. Then, for $x \in \mathcal{V}_q$, we have $\Psi_q(x) = (E^{(\omega)}_{s+1,0}(x)\Delta_{s+1}(x) / E^{(\omega)}_{s+1}(x))(0,1,Y)$, from which we obtain the coincidence of the varieties

$$\{(x,y)\in\overline{H}^{n+1}: \Psi_q(x,y)=0\} \cap (\mathcal{V}_q \times \overline{H}) = \{(x,y): h_1(x,y)=\ldots=h_K(x,y)=0, h_0(x,y)\neq 0\} \cap$$
$$\cap (\mathcal{V}_q \times \overline{H}) = \{(x,y): h_{i,j}(x,y)=h_{i+1}(x,y)=\ldots=h_K(x,y)=0, h_0(x,y)\neq 0\} \cap (\mathcal{V}_q \times \overline{H}),$$

required by Lemma 1b). The equation $\bigcup_q \mathcal{V}_q = \{x \in \overline{H}^n : h_{i,j}(x) \neq 0$ for some $1 \le i \le k$ and $j\}$ is obvious. We should note that the leading coefficient $lc_Y(\Psi_q) = E_{s+1,0}^{(\omega)}$ is nonzero everywhere on $\mathcal{V}_q$.

It remains to estimate the sizes of the polynomials Ψ_q and $g_{q,t}$ determining the quasiprojective varieties $\mathcal{V}_q$, their number, and the time complexity of the algorithm. Since Δ_{s+1} is a minor of the matrix A (depending on i and j), and P_{s+1} is the product (see (8)) of no more than $\tau \le \mathcal{P}(D) \le \mathcal{P}(d_0)$ minors of the matrix A, it follows that (see (3)) $\deg_{x_1,\ldots,x_n,U_i,U_j,U_0}(\Delta_{s+1})$, $\deg_{x_1,\ldots,x_n,U_i,U_j,U_0}(P_{s+1})$, $\deg_{x_1,\ldots,x_n}(g_{q,t})$, $\deg_{x_1,\ldots,x_n,Y}(\Psi_q) \le d_2\mathcal{P}(d,d_0)$; $\deg_{\tau_1,\ldots,\tau_\varepsilon}(\Delta_{s+1})$ $\deg_{\tau_1,\ldots,\tau_\varepsilon}(P_{s+1})$, $\deg_{\tau_1,\ldots,\tau_\varepsilon}(g_{q,t})$, $\deg_{\tau_1,\ldots,\tau_\varepsilon}(\Psi_q) \le d_2\mathcal{P}(d,d_0)$; $l(\Delta_{s+1})$, $l(P_{s+1})$, $l(g_{q,t})$, $l(\Psi_q) \le (M+(\varepsilon+n)\log(d_2))\mathcal{P}(d_1,d_0)$ because of the size of the determinant (see [4] and also [2, 3, 9, 10, 11]). Since $P_1,P_2,\ldots$ are linearly independent over H, their number is no greater than $\mathcal{P}(d_0^n)$, so $1 \le q \le N_1 \le K\mathcal{P}(d_0^n)$, $0 \le t \le N_2 \le K\mathcal{P}(d_0^n)$, which proves (4). This implies a time estimate that is polynomial in $M, (d_1d_2)^{\varepsilon+1}, d_0^{n+\varepsilon}, K$, since it consititutes an estimate of the bit size of all intermediate polynomials and an estimate of the number of arithmetic operations executed on them; this completes the proof of Lemma 1.

§2. SPLITTING AND AN ALGORITHM FOR QUANTIFIER ELIMINATION

Before we describe procedures for splitting we establish the following lemma, which, under certain conditions, makes it possible for us to reduce the order of systems of differential equations. Let $g_0, g_1, \ldots, g_\gamma, f_0, f_1, \ldots, f_K \in F\{u, u_1, \ldots, u_n\}$ be differential polynomials. We assume that $ord_u(g_\beta) \le \tau - t$; $ord_u(f_i) \le \tau$; $ord_{u_j}(g_\beta)$, $ord_{u_j}(f_i) \le R$; $\deg(g_\beta)$, $\deg(f_i) < d$; $\deg_{\tau_1,\ldots,\tau_\varepsilon}(g_\beta)$, $\deg_{\tau_1,\ldots,\tau_\varepsilon}(f_i) < d_2$; $l(g_\beta)$, $l(f_i) \le M$ for all $0 \le \beta \le \gamma$, $0 \le i \le k$, $1 \le j \le n$, where (here and in the sequel) deg denotes the degree in all variables $X, u, u^{(1)}, \ldots, u^{(\tau)}, u_1, u_1^{(1)}, \ldots, u_1^{(R)}, \ldots, u_n, u_n^{(1)}, \ldots, u_n^{(R)}$.

LEMMA 2. Given $g_0,\ldots,g_\gamma,f_0,\ldots,f_k$, we can construct differential polynomials $\hat{f}_0, \hat{f}_1, \ldots, \hat{f}_K \in F\{u,u_1,\ldots,u_n\}$, such that the system

$$g_0 = g_1 = \ldots = g_\gamma = f_1 = \ldots = f_K = 0; \quad f_0 \frac{\partial g_0}{\partial u^{(\tau-t)}} \neq 0 \tag{9}$$

is equivalent in the ring $F\{u,u_1,\ldots,u_n\}$ to the system $g_0 = g_1 = \ldots = g_\gamma = \hat{f}_1 = \ldots = \hat{f}_K = 0$; $\hat{f}_0 \frac{\partial g_0}{\partial u^{(\tau-t)}} \neq 0$. In this case, $ord_u(\hat{f}_i) \le \tau - t$; $ord_{u_j}(\hat{f}_i) \le R+t$; $\deg(\hat{f}_i) \le \mathcal{P}(d,t)$; $\deg_{\tau_1,\ldots,\tau_\varepsilon}(\hat{f}_i) \le d_2\mathcal{P}(d,d_1,t)$; $l(\hat{f}_i) \le (M+nR+\tau+\varepsilon\log(d_2))\mathcal{P}(d,d_1,t)$ for all $0 \le i \le k$, $1 \le j \le n$. The time required to construct all $\hat{f}_0,\ldots,\hat{f}_k$ does not exceed some polynomial in $M, (dt)^{n(R+t)+\tau}, (d_2dd_1t)^{\varepsilon+1}, K$.

Proof. Note that the derivative $g_0^{(s)} = u^{(\tau-t+s)}\left(\frac{\partial g_0}{\partial u^{(\tau-t)}}\right) - Q_s$ for $s \ge 1$, where differential polynomial $Q_s \in F[X, u, \ldots, u^{(\tau-t+s-1)}, u_1, \ldots, u_1^{(R+s)}, \ldots, u_n, \ldots, u_n^{(R+s)}]$. It is clear that $\deg(g_0^{(s)}) < d$; $\deg_{\tau_1,\ldots,\tau_\varepsilon}(g_0^{(s)}) < d_2$; $l(g_0^{(s)}) \le M + O(s\log(d))$.

We define the weight of a monomial $X^\beta \prod_{\ell \le \tau}(u^{(\ell)})^{\alpha_\ell} \prod_{s,j}(u_j^{(s)})^{\beta_{j,s}}$ to be $wgt = \sum_{\tau-t+s\le\ell\le\tau} \alpha_\ell(\ell-\tau+t)$, and we define the weight of a differential polynomial to be the maximum of the weights of its monomials. Then $wgt(g_0^{(s)}) \le s$.

For a proof by induction, assume that for some $0 \le s < t$ we have constructed differential polynomials $f_{i,s} \in F[X, u, u^{(1)}, \ldots, u^{(\tau-s)}, u_1, \ldots, u_1^{(R+t)}, \ldots, u_n, \ldots, u_n^{(R+t)}]$, $0 \le i \le K$ such that system (9) is equivalent to system $g_0 = g_1 = \ldots = g_\gamma = f_{1,s} = \ldots = f_{K,s} = 0; f_{0,s}\left(\frac{\partial g_0}{\partial u^{(\tau-t)}}\right) \neq 0$. Initially, for $s = 0$ (the basis for the induction), we set $f_{i,0} = f_i$. Assume that $wgt(f_{i,s}) \le w_s$; $\deg(f_{i,s}) < D_s$; $\deg_{\tau_1,\ldots,\tau_\varepsilon}(f_{i,s}) < \delta_s$; $l(f_{i,s}) \le M_s$; $\deg_\eta(f_{i,s}) < \mathcal{A}_s$ (assume that in computing $f_{i,s}$ we give $f_{i,t}(\mathrm{mod}(\varphi))$ only at the very end, so here η figures as a variable — see the introduction). Fix some $0 \le i \le k$. It is clear that $\deg_{u^{(\tau-s)}}(f_{i,s}) \le w_s/(t-s)$. We replace

$u^{(r-s)}$ by the ratio of the differential polynomials $Q_{t-s} / \left(\frac{\partial g_0}{\partial u^{(r-t)}}\right)$, and then eliminate the denominator in the expression obtained by multiplying by the differential polynomial $\left(\frac{\partial g_0}{\partial u^{(r-t)}}\right)^{deg_{u^{(r-s)}}(f_{i,s})}$. We thus obtain the polynomial $f_{i,s+1} \in F[X, u, \ldots, u^{(r-s-1)}, u_1, \ldots, u_1^{(R+t)}, \ldots, u_n, \ldots, u_n^{(R+t)}]$. It is clear that the system $g_0 = \ldots = g_\gamma = f_{1,s} = \ldots = f_{k,s} = 0;\ f_{i,s+1}\left(\frac{\partial g_0}{\partial u^{(r-t)}}\right) \neq 0$ is equivalent to the system $g_0 = \ldots = g_\gamma = f_{1,s} = \ldots = f_{k,s} = 0;\ f_{0,s}\left(\frac{\partial g_0}{\partial u^{(r-t)}}\right) \neq 0$, and, consequently, to system (9). Since $wgt(Q_{t-s}) \leq t - s = wgt(u^{(r-s)})$, it is clear that with the substitution we have described the weight does not increase, i.e., $w_{s+1} \leq w_s$. Moreover,

$$deg(f_{i,s+1}) \leq d \cdot deg_{u^{(r-s)}}(f_{i,s}) + \mathcal{D}_s \leq d \cdot w_s/(t-s) + \mathcal{D}_s;\ \mathcal{D}_{s+1} \leq d d_1 + \mathcal{D}_s;\ deg_{T_1,\ldots,T_\varepsilon}(f_{i,s+1}) < d d_2 + \delta_s;\ l(f_{i,s+1}) \leq M_s + (M + O(s \log(d)))\, w_s/(t-s) + (n(R+t)+\tau)\log(\mathcal{D}_{s+1}) + O(\varepsilon \log(\delta_{s+1})).$$

Set $\hat{f}_i = f_{i,t}$. Since $wgt(f_i) \leq w_0 < dt$, we obtain (after giving $f_{i,t}(\mathrm{mod}(\varphi))$ $deg(\hat{f}_i) = O(d^2 t \log(t))$; $deg_{T_1,\ldots,T_\varepsilon}(\hat{f}_i) = O(d_1 d^2 t^2 d_2)$; $l(\hat{f}_i) = O((M dt \log(t) + dt^2 \log(d) \log(t) + (n(R+t)+\tau) t \log(dt) + \varepsilon t \log(dtd_2) + \log(d_1 dt))\, d d_1 t)$. The time required for construction of $f_{i,s+1}$, beginning with $f_{i,s}$, can be estimated as polynomial in $M_{s+1}, \mathcal{D}_{s+1}^{n(R+t)+\tau}, \delta_{s+1}^{\varepsilon}$. Lemma 2 is proved.

We now turn to a description of a procedure for splitting systems of differential equations. Let $g, h_i \in F[X, u, \ldots, u^{(r)}, u_1, \ldots, u_1^{(R)}, \ldots, u_n, \ldots, u_n^{(R)}]$ be differential polynomials satisfying the following constraints: $0 \leq ord_u(g) = p < r$, $0 \leq i \leq l$. We write $g = \sum_{0 \leq \alpha \leq \gamma} g_\alpha (u^{(p)})^\alpha$, where $ord_u(g_\alpha) \leq p - 1$. Consider the system

$$g = h_1 = \ldots = h_l = 0;\quad h_0 \neq 0. \tag{10}$$

System (10) is equivalent to the following disjunctive formulas (we call this equivalence a splitting of (10) and we call g a splitting polynomial):

$$\bigvee_{0 \leq \beta \leq \gamma - 1} \left(\left(g = \frac{\partial g}{\partial u^{(p)}} = \ldots = \frac{\partial^\beta g}{\partial (u^{(p)})^\beta} = h_1 = \ldots = h_l = 0 \right) \& \left(h_0 \frac{\partial^{\beta+1} g}{\partial (u^{(p)})^{\beta+1}} \neq 0 \right) \right) \tag{11}$$

$$(g_0 = \ldots = g_\gamma = h_1 = \ldots = h_l = 0) \& (h_0 \neq 0). \tag{12}$$

Assume that the differential polynomials $f_0, \ldots, f_k \in F[X, u_1, \ldots, u^{(r)}, u_1, \ldots, u_n^{(R)}]$ satisfy the following constraints: $deg(f_i) < d;\ deg_{T_1,\ldots,T_\varepsilon}(f_i) < d_2;\ l(f_i) \leq M, 0 \leq i \leq k$ (see the introduction). We write $f_i = \sum_s f_{i,s} (u^{(r)})^s$, where $ord(f_{i,s}) \leq r - 1$. Consider the formula

$$\Omega_1 = \left((f_1 = \ldots = f_k = 0) \& (f_0 \neq 0) \right). \tag{13}$$

Our immediate goal is to describe an algorithm that constructs a quantifier-free formula equivalent to the formula $\exists u(\Omega_1)$. We apply Lemma 1 to (13), using the derivative $u^{(r)}$ for the variable Y and $X, u, \ldots, u^{(r-1)}, u_1, \ldots, u_1^{(R)}, \ldots, u_n, \ldots, u_n^{(R)}$ for the variables $X_1, \ldots, X_n$, respectively. As a result, we obtain differential polynomials $g_{q,t} \in F[X, u, \ldots, u^{(r-1)}, u_1, \ldots, u_1^{(R)}, \ldots, u_n, \ldots, u_n^{(R)}]$, $\Psi_q \in F[u, \ldots, u^{(r-1)}, u^{(r)}, u_1, \ldots, u_1^{(R)}, \ldots, u_n, \ldots, u_n^{(R)}]$ such that formula (13) is equivalent to the following disjunctive formulas (we leave only those indices q for which $ord_u(\Psi_q) = r$):

$$\bigvee_q \left(\left(\&_{t \geq 1} (g_{q,t} = 0) \right) \& (\Psi_q = 0) \& (g_{q,0} \neq 0) \right) \tag{14}$$

$$\&_{i \geq 1; s} (f_{i,s} = 0) \& (f_0 \neq 0). \tag{15}$$

We apply the described splitting procedure to each of the disjunctive terms in (14) (for fixed q), treating this system as (10), and using, for a splitting polynomial q, an arbitrary polynomial $g_{q,t}$ ($t \geq 1$) for which $ord_u(g_{q,t}) \geq 0$, i.e., it contains u. We repeatedly apply the splitting procedure to all systems of the form (12) that we obtain, but we do not use Ψ_q as a splitting polynomial. We then apply the splitting procedure to system (15), like (14), taking one of the $\{f_{i,s}\}_{i \geq 1; s}$ containing u as the splitting polynomial and repeatedly apply the procedure to the systems of the form (12) that are obtained.

Note that the splitting procedure is not applied to systems of the form (12) that are obtained if and only if the obtained system is either of the form $\Omega_2 = \&_{t \geq 1; \gamma} (g_{q,t,\gamma} = 0) \& (\Psi_q = 0) \& (g_{q,0} \neq 0)$ (i.e., it is derived from (14)), where $g_{q,t,(R)} =$

$\sum_{\mathfrak{J}} g_{q,t,\mathfrak{J}} u^{j_0}(u^{(1)})^{j_1}\ldots(u^{(r-1)})^{j_{r-1}}$ and $g_{q,t,\mathfrak{J}} \in F[X,u_1,\ldots,u_1^{(R)},\ \ldots,u_n,\ldots,u_n]$ while $\mathfrak{J} = (j_0,j_1,\ldots,j_{r-1})$, or the system is derived from (15) and is of the form $\Omega_3 = \&_{i\geqslant 1;s;\mathfrak{J}}(f_{i,s,\mathfrak{J}}=0)\&(f_0\neq 0)$ when similar notation is used.

We will show that the formula $\exists u(\Omega_2)$ is equivalent to the following disjunction:

$$\bigvee_{\mathfrak{J}_0}\Big(\&_{t\geqslant 1,\mathfrak{J}}\big(g_{q,0,\mathfrak{J}_0}\neq 0\big)\Big). \tag{16}$$

We consider some $u_1,\ldots,u_n$ and we let $K = F\langle u_1,\ldots,u_n\rangle$ be the differential field generated by them. We assume that (16) is true. We choose $u,u^{(1)},\ldots,u^{(r-1)}$ to be algebraically independent over field K; then $g_{q,0}\big(X,u,u^{(1)},\ldots,u^{(r-1)},u_1,\ldots,u_1^{(R)},\ldots,u_n,\ldots,u_n^{(R)}\big)\neq 0$, so $0\neq lc_{u^{(r)}}(\Psi_q)\in K[u,u_1,\ldots,u^{(r-1)}]$, by Lemma 1b and Remark 2) on this lemma, and, finally, we choose u to satisfy the single equation $\widetilde{\Psi}_q(u,u^{(1)},\ldots,u^{(r-1)},u^{(r)})=0$, where $\widetilde{\Psi}_q\in K[u_1,\ldots,u^{(r-1)},u^{(r)}]$ is an irreducible (over the field $K(u,u^{(1)},\ldots,u^{(r-1)})$ divisor of the polynomial Ψ_q (i.e., u is a member of the differential quotient ring $K\{u\}/(\widetilde{\Psi}_q)$ without zero divisors (see [5, 7]). Then the u we have selected satisfies the equation $0=\Psi_q(u,u^{(1)},\ldots,u^{(r-1)},u^{(r)})\in K\{u\}/(\widetilde{\Psi}_q)$, so the formula $\exists u(\Omega_2)$ is true, i.e., there exists a u in the differential closure of the field K (see [5, 7]). Formula (16) obviously follows from the formula $\exists u(\Omega_2)$, which proves the required equivalence. Similarly, the formula $\exists u(\Omega_3)$ is equivalent to the disjunction

$$\bigvee_{\mathfrak{J}_0}\Big(\&_{i\geqslant 1;s,\mathfrak{J}}\big(f_{i,s,\mathfrak{J}}=0\big)\&\big(f_{0,\mathfrak{J}_0}\neq 0\big)\Big) \tag{17}$$

We apply Lemma 2 to each disjunctive term in any formula of the form (11) obtained after application of the splitting procedure (for given β we choose $g_0 = \partial^\beta g/\partial(u^{(p)})^\beta$; see (9)). As a result we obtain the differential polynomials $\hat{h}_{0,\beta}$, $\hat{h}_{1,\beta},\ldots,\hat{h}_{l,\beta}\in F[X,u,u^{(1)},\ldots,u^{(p)},u_1,\ldots,u_1^{(R+r-p)},\ldots,u_n,\ldots,u_n^{(R+r-p)}]$, so that (11) is equivalent to the disjunction

$$\bigvee_{0\leqslant\beta\leqslant\delta-1}\left(\left(g=\frac{\partial g}{\partial u^{(p)}}=\ldots=\frac{\partial^\beta g}{\partial(u^{(p)})^\beta}=\hat{h}_{1,\beta}=\ldots=\hat{h}_{l,\beta}=0\right)\&\left(\hat{h}_{0,\beta}\frac{\partial^{\beta+1}g}{\partial(u^{(p)})^{\beta+1}}\neq 0\right)\right) \tag{18}$$

We again apply the process we have described to each of the disjunctive terms of the formulas of the form (18) that are obtained, taking this disjunctive term as a formula of the form (13), etc. This completes the description of our algorithm for constructing quantifier-free formulas equivalent to the formula $\exists u(\Omega_1)$ (see (13)). We should note that the formulas we ultimately obtain (and which do not contain the variable u) are of the form (16) or (17).

We will now estimate the number of systems obtained from (13) and their sizes. Note that because, for any intermediate system, the differential polynomials that appear in such a system belong to the ring $F[X,u,\ldots,u^{(p)},u_1,\ldots,u_1^{(R+r-p)},\ldots,u_n,\ldots,u_n^{(R+r-p)}]$ for some p, the polynomials that appear in systems of the form (16) or (17) belong to the ring $F[X,u_1,\ldots,u_1^{(R+r)},\ldots,u_n,\ldots,u_n^{(R+r)}]$. From system (13) we obtain $kd^{c_1(nR+r)}$ disjunctive terms in formulas of the form (14) (as well as (15)), by Lemma 1 (here and below $c_1,c_2,\ldots$ are natural constants). The degree of each polynomial that appears in system (14) or (15) is no greater than d^{c_2}, while the degrees of these polynomials in the variables $T_1,\ldots,T_\varepsilon$ can be estimated as $d_2(dd_1)^{c_3}$, again by Lemma 1. By splitting disjunctive terms of formulas of the form (14) and (15) we obtain $kd^{c_4(nR+r)}$ systems of the form (11) and (12). We apply Lemma 2 to each disjunctive term of formulas of the form (11). We obtain a formula of the form (18) with polynomials of degrees less than $(d(r-p))^{c_5}$, degrees in $T_1,\ldots,T_\varepsilon$ less than $d_2(dd_1(r-p)^{c_6}$, and coefficients having dimensions less than $(M+(nR+r+\varepsilon)\log(d_4))(dd_1(r-p))^{c_6}$.

It is not difficult to use these considerations to prove by induction on $0\leq\rho\leq r$ that after ρ applications of the process there will be no more than $k(dr)^{c_7^\rho(nR+r)}$ intermediate systems of the form $\tilde{g}_{1,\rho}=\ldots=\tilde{g}_{s,\rho}=0$, $\tilde{g}_{0,\rho}\neq 0$, where $\tilde{g}_{\alpha,\rho}\in F[X,u,u^{(1)},\ldots,u^{(r-\rho)},u_1,\ldots,u_1^{(R+\rho)},\ldots,u_n,\ldots,u_n^{(R+\rho)}]$, and $s\leq k(dr)^{c_8^\rho(nR+r)}$; $\deg(\tilde{g}_{\alpha,\rho})<(dr)^{c_9^\rho}$; $\deg_{T_1,\ldots,T_\varepsilon}(\tilde{g}_{\alpha,\rho})<d_2(drd_1)^{c_9^\rho}$; $l(\tilde{g}_{\alpha,\rho})\leq(M+(nR+\varepsilon)\log(d_4))(drd_1)^{c_9}$. Thus, the formula $\exists u(\Omega_1)$ (see (13)) is equivalent to a disjunction of no more than $kd^{c_9^r nR}$ systems of the form (compare (16) and (17))

$$g_1=\ldots=g_s=0;\quad g_0\neq 0, \tag{19}$$

where $g_\alpha\in F[X,u_1,\ldots,u_1^{(R+r)},\ldots,u_n,\ldots,u_n^{(R+r)}]$; in this case $s\leq kd^{c_9^r nR}$; $\deg(g_\alpha)\leq d^{c_{10}^r}$; $\deg_{T_1,\ldots,T_\varepsilon}(g_\alpha)<d_2(dd_1)^{c_{10}}$; $lcg_\alpha)\leq(M+(nR+\varepsilon)\log(d_4))(dd_1)^{c_{10}^r}$. The time complexity for constructing the given quantifier-disjunction of systems of form (19) is polynomial in $M, d^{c_{11}^r(nR+\varepsilon)}, d_1^{c_{11}^r(\varepsilon+1)}, d_2^\varepsilon, k$.

We now turn to the description of a procedure that reduces a quantifier-free formula of the type Ω (see (1) in the introduction) to disjunctive normal form. We consider all of the $f_1,\ldots,f_n$ appearing in Ω as elements of the ring of polynomials $F[X,u_1,\ldots,u_1^{(\tau)},\ldots,u_n,\ldots,u_n^{(\tau)},v_1,\ldots,v_1^{(\tau)},\ldots,v_m,\ldots,v_m^{(\tau)}]$. For any set of indices $I \subset \{1,\ldots,N\}$, we will say that formula $\mathfrak{B}=\&_{i\in I}(f_i=0)\,\&\,\&_{i\in\{1,\ldots,N\}\setminus I}(f_i\neq 0)$ is an elementary $\{f_1,\ldots,f_N\}$-formula. It was shown in [4] that there are no more than $(\sum_{1\le i\le N}\deg(f_i))^{(n+m)r+1}<(dN)^{(n+m)r+1}$ elementary $\{f_1,\ldots,f_N\}$-formulas defining non-empty quasiprojective varieties $\bar{F}^{(n+m)r+1}$ (it is known that this property does not change when the field $\bar{F}$ is extended); such elementary formulas are said to be nontrivial. They can all be found by the following process (see also [9, 11]). We assume that for some $0 \le t < N$ all nontrivial elementary $\{f_1,\ldots,f_t\}$-formulas of the form $\mathfrak{B}_t=\&_{i\in I}(f_i=0)\,\&\,\&_{i\in\{1,\ldots,t\}\setminus I}(f_i\neq 0)$ have already been found. We will verify that each of the two elementary $\{f_1,\ldots,f_t,f_{t+1}\}$-formulas $\mathfrak{B}_t\&(f_{t+1}=0)$ and $\mathfrak{B}_t\&(f_{t+1}\neq 0)$ is nontrivial, using [2, 3] (see also [8, 9, 10]). Thus, we can construct all nontrivial elementary $\{f_1,\ldots,f_N\}$-formulas in time $\mathcal{P}(M,(d^{(n+m)r}d_1d_2N)^{(n+m)r+6})$ (see [2, 3]).

Then, for any nontrivial elementary $\{f_1,\ldots,f_N\}$-formula of the form $\mathfrak{B}$, the algorithm determines whether it is consistent with the formula Ω by replacing, in Ω, each atomic subformula $(f_i = 0)$ with its truth value from the formula B. The formula obtained by such substitution is true if and only if $\mathfrak{B}$ is consistent with Ω. The formula Ω is equivalent to the disjunction of all nontrivial elementary $\{f_1,\ldots,f_N\}$-formulas that are consistent with Ω. Eventually, at the end of this process, $\mathfrak{B}$ is replaced by the equivalent formula $\&_{i\in I}(f_i=0)\&(\prod_{i\in I}f_i\neq 0)$, which reduces it to the form (13) for further application of the algorithm for elimination of existential quantifiers.

Finally, the algorithm for elimination of quantifiers proceeds with alternate application of the two procedures we have described to formula (1): elimination of one quantifier and reduction of a quantifier-free formula of the form Ω (see (1)) to disjunctive normal form. As a result, we obtain a formula of the form (2). It is not difficult to estimate the size of formula (2) or the time complexity of the algorithm by induction on n, when we keep in mind that in each successive step of the algorithm for elimination of a quantifier we are led to a formula of the form (19), and we have established complexity estimates for formula (19).

LITERATURE CITED

1. D. Yu. Grigor'ev, "The complexity of eliminating quantifiers in the theory of ordinary differential equations," in: Abstracts of the Eighth All-Union Conf. on Math. Logic, Moscow (1986), p. 46.
2. D. Yu. Grigor'ev, "Factorization of polynomials over finite fields and solution of systems of algebraic equations," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, **137**, 20-79 (1984).
3. A. L. Chistov, "A polynomial complexity algorithm for factoring polynomials and finding components of varieties in subexponential time," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, **137**, 124-188 (1984).
4. J. Heintz, "Definability and fast quantifier elimination in algebraically closed fields," Theor. Comput. Sci., **24**, 239-278 (1983).
5. E. R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York (1973).
6. D. Lazard, "Resolution des systemes d'equations algebriques," Theor. Comput. Sci., **15**, 77-110 (1981).
7. A. Seidenberg, "An elimination theory for differential algebra," Univ. of Calif. Press, **3**, No. 2, 31-66 (1956).
8. D. Yu. Grigor'ev and A. L. Chistov, "Fast factoring of polynomials and solution of systems of algebraic equations," Dokl. Akad. Nauk SSSR, **275**, No. 6, 1302-1306 (1984).
9. D. Yu. Grigor'ev, "Complexity of decisions in the theory of first-order algebraically closed fields," Izv. Akad. Nauk SSSR, Ser. Mat., **50**, No. 5, 1106-1120 (1986).
10. N. N. Vorob'ev, Jr. and D. Yu. Grigor'ev, "Solution of polynomial inequalities over real closed fields in subexponential time," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, **174**, 3-36 (1988).
11. D. Yu. Grigor'ev, "Solution complexity in the theory of first-order real closed fields," Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst. Akad. Nauk SSSR, **174**, 53-100 (1988).