COMPLEXITY OF QUANTIFIER ELIMINATION
IN THE THEORY OF ORDINARY DIFFERENTIAL EQUATIONS

D.Yu.Grigor'ev

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

Introduction

Let a formula of the first-order theory of ordinary differential equations be given

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

where $Q_1, \dots, Q_n$ are quantifiers (either universal or existential), Ω is a quantifier-free formula containing as atomic subformulas of the kind $(f_i = 0)$, $1 \leqslant i \leqslant N$. Here $f_i \in \mathbb{Z}\{u_1, \dots, u_n, v_1, \dots, v_m\}$ are differential polynomials (relatively to differentiating over variable X), indeterminates $u_1, \dots, u_n$ are connected, $v_1, \dots, v_m$ are free (remind, see e.g. [7, 9], that the differential ring $\mathbb{Z}\{u_1, \dots, u_n, v_1, \dots, v_m\}$ is generated as a polynomial ring over $\mathbb{Z}[X]$ by the derivatives $u_s, u_s^{(1)}, u_s^{(2)}, \dots ; v_t, v_t^{(1)}, v_t^{(2)}, \dots$ for $1 \leqslant s \leqslant n$, $1 \leqslant t \leqslant m$). Denote by $ord_{u_s}(f_i)$ the maximal order of derivatives $u_s, u_s^{(1)}, u_s^{(2)}, \dots$ of the indeterminate u_s, occuring in the differential polynomial f_i. Suppose that $ord_{u_s}(f_i) \leqslant r$, $ord_{v_t}(f_i) \leqslant r$ for all $1 \leqslant s \leqslant n$, $1 \leqslant t \leqslant m$, then one can consider f_i as a (usual) polynomial from a ring $\mathbb{Z}[X, u_1, u_1^{(1)}, \dots, u_1^{(r)}, \dots, u_n, u_n^{(1)}, \dots, u_n^{(r)}, v_1, v_1^{(1)}, \dots, v_1^{(r)}, \dots, v_m, v_m^{(1)}, \dots, v_m^{(r)}]$. Assume also that the degree $deg(f_i)$ of the polynomial f_i as an element of the latter ring (relatively to all the indeterminates) is less than d, and finally, that the absolute value of any (integer) coefficient of the polynomial f_i does not exceed 2^M.

In [7] a quantifier elimination method in the first-order theory of ordinary differential equations is described, which allows for a given formula of the kind (1) to produce equivalent to it quantifier-free formula. Here and further we consider the equivalence of the formulas over the differential closure of the quotient field $\mathbb{Z}\langle v_1, \ldots, v_m \rangle$ of the ring $\mathbb{Z}\{v_1, \ldots, v_m\}$ (see [7 , 9]). However, the working time of the method from [9] is nonelementary (in Kalmar sense), in particular, it cannot be bounded from above by any finite tower of exponential functions (one can consider the working time on RAM or on any other polynomially equivalent computational model, e.g. Turing machine). The main result of the present paper is the following theorem, in which a quantifier elimination algorithm is designed with an elementary complexity bound (see also [3]).

THEOREM. There is an algorithm which for a given formula of the kind (1) of the first-order theory of ordinary differential equations produces an equivalent to it quantifier-free formula of this theory of the form

$$\bigvee_{1 \le i \le \mathcal{N}} \left(\mathop{\&}_{1 \le j \le \mathcal{K}} (g_{i,j} = 0) \,\&\, (g_{i,0} \ne 0) \right) \qquad (2)$$

where $g_{i,j} \in \mathbb{Z}\{v_1, \ldots, v_m\}$ are differential polynomials, within time polynomial in $M(Nd)^{m^n c^{r 2^n}}$ for a suitable constant $c > 1$. Moreover, for the parameters of the polynomials $g_{i,j}$ hold the following bounds: $\mathrm{ord}_{v_t}(g_{i,j}) \le r 2^n$; $\mathcal{N}, \mathcal{K}, \deg(g_{i,j}) \le (Nd)^{O(m^n c^{r 2^n})} = \mathcal{M}$ and the absolute value of every (integer) coefficient of a polynomial $g_{i,j}$ is less than $2^{M\mathcal{M}}$.

The method from [9] contains two subroutines, transforming a system of differential equations in a certain disjunction of systems. The first subroutine is applied in the case, when informally speaking, for some distinguished indeterminate its derivative of the maximal order occurs at least in two polynomials. As a result of executing the first subroutine each obtained system has at most one polynomial containing this derivative. The second subroutine consists in splitting a system and decreasing the order of the distinguished indeterminate. Just executing the first subroutine leads in [9] to nonelementary complexity bound. In the present paper transforming (instead of the first subroutine) to a disjunction of systems such that each of then contains at most one polynomial, in which occurs the derivative of the maximal order of the distinguished indeterminate is going in a quite another way, based on the constructing the greatest common divisor of a family of one-variable polynomials with parametric coefficients (lemma 1 in section 1), apparently, interesting itself. The proof of lemma 1 is similar to the construction from [2], but on the other hand the direct application of the result from [2] (see also

[4]) yields a worse complexity bound than in lemma 1. In section 2 a modification of the subroutine from [9] of splitting a system and decreasing the order of the distinguished indeterminate is exposed, then a quantifier elimination algorithm and its complexity analysis are exhibited.

In [9], moreover a quantifier elimination method for the first-order theory of partially differential equations is described. It would be interesting to clarify, whether there exists such a method with elementary complexity? This problem is connected (see [9]) with estimating in an effective version of Hilbert's theorem on Idealbasis.

1. Constructing the greatest common divisor of a family of one-variable polynomials with parametric coefficients

We present the main result of this section (lemma 1) in a more general form than it is necessary for the main theorem, namely for the polynomials with the coefficients from a field F finitely generated over a prime subfield (cf. [1, 2, 4, 5]).

Thus $F=H(T_1,\dots,T_e)[\eta]$ where either $H=\mathbb{Q}$ or $H=\mathbb{F}_p$, i.e. H is a prime subfield, $T_1,\dots,T_e$ are algebraically independent over the field H, an element η is algebraic separable over the field $H(T_1,\dots,T_e)$, let $\varphi(Z)\in H(T_1,\dots,T_e)[Z]$ be its minimal polynomial. Each polynomial $f\in F[X_1,\dots,X_n]$ can be uniquely (up to a factor from H^*) represented in a form $f=\sum_{0\leq i<\deg_Z(\varphi);i_1,\dots,i_n}(a_{i,i_1,\dots,i_n}/b)\eta^i X_1^{i_1}\cdots X_n^{i_n}$, where $a_{i,i_1,\dots,i_n}, b\in H(T_1,\dots,T_e]$ and $\deg(b)$ is the least possible. Define the degree $\deg_{T_1,\dots,T_e}(f)=\max_{i,i_1,\dots,i_n}\{\deg_{T_1,\dots,T_e}(a_{i,i_1,\dots,i_n}), \deg_{T_1,\dots,T_e}(b)\}$.

The size $l(\alpha)$ for $\alpha\in H$ is defined as its bit-size in the case $H=\mathbb{Q}$ and as $\log_2(p)$ when $H=\mathbb{F}_p$. Denote by $l(f)$ the maximum of the sizes of all the coefficients (from the field H) of the polynomials $a_{i,i_1,\dots,i_n}, b$ at the monomials of variables $T_1,\dots,T_e$.

For the functions $g_1>0,\ g_2>0,\ \dots,\ g_s>0$ we write $g_1\leq \mathcal{P}(g_2,\dots,g_s)$ if for a suitable polynomial P an inequality $g_1\leq P(g_2,\dots,g_s)$ is valid.

Consider some polynomials $h_0,h_1,\dots,h_K\in F[X_1,\dots,X_n,Y]$ and assume that the following bounds are true:

$$\deg_{T_1,\dots,T_e,Z}(\varphi)<d_1;\ \deg_{X_1,\dots,X_n,Y}(h_i)<d_0;\ \deg_{T_1,\dots,T_e}(h_i)<d_2;\ l(\varphi)\leq M_1;\ l(h_i)\leq M_2 \quad (3)$$

for every $0 \leqslant i \leqslant K$. Introduce a notation $h_i = \sum_j h_{i,j} Y^j$ where the polynomials $h_{i,j} \in F[X_1, \ldots, X_n]$. Denote by $\bar{F}$ an algebraic closure of the field F.

LEMMA 1. There is an algorithm which for given polynomials $h_0, h_1, \ldots, h_K$ yields such two families of polynomials $g_{q,t} \in F[X_1, \ldots, X_n]$, $\varphi_q \in F_1[X_1, \ldots, X_n, Y]$ for $1 \leqslant q \leqslant N_1$, $0 \leqslant t \leqslant N_2$ that

a) quasiprojective varieties $\mathcal{V}_q = \{x \in \bar{F}^n : g_{q,1}(x) = \ldots = g_{q,N_2}(x) = 0;\ g_{q,0}(x) \neq 0\}$ for $1 \leqslant q \leqslant N_1$ form a decomposition of an open (in Zariski topology) set $\bar{F}^n \setminus \{x \in \bar{F}^n : h_{i,j}(x) = 0$ for all $1 \leqslant i \leqslant K$ and $j\}$;

b) for each $1 \leqslant q \leqslant N_1$ the following two varieties coincide:

$$\{(x,y) \in \bar{F}^n \times \bar{F} = \bar{F}^{n+1} : h_1(x,y) = \ldots = h_K(x,y) = 0;\ h_0(x,y) \neq 0\} \cap (\mathcal{V}_q \times \bar{F}) = \{(x,y) \in \bar{F}^{n+1} : \varphi_q(x,y) = 0\} \cap (\mathcal{V}_q \times \bar{F})$$

, and besides the leading coefficient $lc_Y(\varphi_q)$ is distinguished from zero everywhere on $\mathcal{V}_q$.

The running time of the algorithm can be estimated by a certain polynomial in $K, M_1, M_2, (d_1 d_2)^e, d_0^{n+e}$. Finally, the following bounds on the parameters of the polynomials are fulfilled:

$$
\begin{gathered}
\deg_{X_1,\ldots,X_n,Y}(\varphi_q),\ \deg_{X_1,\ldots,X_n}(g_{q,t}) \leqslant \mathcal{P}(d_0); \\
\deg_{T_1,\ldots,T_e}(\varphi_q),\ \deg_{T_1,\ldots,T_e}(g_{q,t}) \leqslant d_2 \mathcal{P}(d_1, d_0) \\
l(\varphi_q),\ l(g_{q,t}) \leqslant (M_1 + M_2 + (e+n)\log d_2)\mathcal{P}(d_1, d_0);\ N_1, N_2 \leqslant K\mathcal{P}(d_0^n).
\end{gathered}
\tag{4}
$$

REMARK. 1) The property b) shows that one can consider φ_q as a kind of the greatest common divisor of the polynomials $h_1, \ldots, h_K$ (under the condition $h_0 \neq 0$) considered in a variable Y on the quasiprojective variety $\mathcal{V}_q$;

2) The properties a), b) are still correct if to replace $\bar{F}$ by an arbitrary algebraically closed field containing F.

Proof of Lemma 1. For any $1 \leqslant i \leqslant K$, $0 \leqslant j < d_0$ consider a quasiprojective variety $\mathcal{U}_{i,j} = \{x \in \bar{F}^n : h_{1,d_0-1}(x) = \ldots = h_{1,0}(x) = h_{2,d_0-1}(x) = \ldots = h_{2,0}(x) = \ldots = h_{i,d_0-1}(x) = \ldots = h_{i,j+1}(x) = 0;\ h_{i,j}(x) \neq 0\}$. Obviously $\bigcup_{i,j} \mathcal{U}_{i,j} = \bar{F}^n \setminus \{x \in \bar{F}^n : h_{i,j}(x) = 0$ for all $1 \leqslant i \leqslant K$ and $j\}$. Introduce a notation $\tilde{h}_{i,j} = \sum_{0 \leqslant \beta \leqslant j} h_{i,\beta} Y^\beta$. The system under consideration

$$h_1 = \ldots = h_K = 0; \quad h_0 \neq 0 \tag{5}$$

is equivalent to a disjunction (over all $1 \leq i \leq K$, $0 \leq j < d_0$) of the following systems $\tilde{h}_{i,j} = h_{i+1} = \ldots = h_K = h_{1,d_0-1} = \ldots = h_{1,0} = h_{2,d_0-1} = \ldots = h_{2,0} = \ldots = h_{i,d_0-1} = \ldots = h_{i,j+1} = 0;\ h_0 h_{i,j} \neq 0$. Fix for the time being $1 \leq i \leq K$, $0 \leq j \leq d_0$ and consider a system

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

Introduce new variables Y_1, Y_0 . For every point $x = (x_1, \ldots, x_n)$ an element y satisfies the system $(6)_x$ (which is obtained from the system (6) by substituting the coordinates $x_1, \ldots, x_n$ instead of $X_1, \ldots, X_n$ respectively) iff there exists y_1 such that $\tilde{h}_{i,j}(x,y) = h_{i+1}(x,y) = \ldots = h_K(x,y) = y_1 h_0(x,y) - 1 = 0$. Consider the following homogeneous relatively to the variables Y_1, Y, Y_0 polynomials: $\bar{h}_\ell(X_1, \ldots, X_n, Y_1, Y, Y_0) = Y_0^{\deg_Y(h_\ell)} h_\ell(X_1, \ldots, X_n, Y/Y_0)$ for $i < \ell \leq K$; $\bar{h}_i(X_1, \ldots, X_n, Y_1, Y, Y_0) = Y_0^j \tilde{h}_{i,j}(X_1, \ldots, X_n, Y/Y_0)$; $\bar{h}_0(X_1, \ldots, X_n, Y_1, Y, Y_0) = Y_0^{\deg_Y(h_0)+1}(Y_1/Y_0\, h_0(X_1, \ldots, X_n, Y/Y_0) - 1)$.
Notice, besides, that for arbitrary point $x \in \mathcal{U}_{i,j}$ the systems $(5)_x$ and $(6)_x$ are equivalent.

Consider some field F_1, a point $x = (x_1, \ldots, x_n) \in \bar{F}_1^n$ and a homogeneous system of equations (in variables Y_1, Y, Y_0):

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

Suppose that $h_{i,j}(x) \neq 0$. Then the system $(6)_x$ has a finite number of solutions. If $y \in \bar{F}_1$ is a solution of $(6)_x$ then a point $(1/h_0(x,y) : y : 1) \in \mathbb{P}^2(\bar{F}_1)$ of the projective space is a solution of the system $(7)_x$. Conversely, if $(y_1 : y : y_0) \in \mathbb{P}^2(\bar{F}_1)$ is a solution of $(7)_x$ and $y_0 \neq 0$ then y/y_0 is a solution of $(6)_x$ and apart from that $y_1/y_0 = 1/h_0(x, y/y_0)$; if $y_0 = 0$ then $y = 0$ since $lc_Y(\tilde{h}_{ij}) = h_{ij}$. Thus, the system $(7)_x$ has a finite number of solutions in $\mathbb{P}^2(\bar{F}_1)$, and moreover all these solutions, may be except (1:0:0), correspond bijectively to the solutions of the system $(6)_x$ (provided that $h_{i,j}(x) \neq 0$).

In the sequel we need a certain construction from [8]. Let $g_0, \ldots, g_{t-1} \in F_1[Y_0, \ldots, Y_m]$ be homogeneous polynomials of degrees $\gamma_0 \geq \ldots \geq \gamma_{t-1}$ respectively. Introduce the variables $U_0, \ldots, U_m$ algebraically independent over the field $F_1(Y_0, \ldots, Y_m)$ and a polynomial $g_t = Y_0 U_0 + \ldots + Y_m U_m \in F_1(U_0, \ldots, U_m)[Y_0, \ldots, Y_m]$, its degree $\gamma_t = 1$. Set $D = (\sum_{1 \leq \ell \leq \min\{t-1, m\}} (\gamma_\ell - 1)) + \gamma_0$. Consider a linear over $F_1(U_0, \ldots, U_m)$ mapping $\mathfrak{A}: \mathcal{H}_0 \oplus \cdots \oplus \mathcal{H}_t \to \mathcal{H}$ where $\mathcal{H}_\ell$ (respectively $\mathcal{H}$) is a space of homogeneous in the variables $Y_0, \ldots, Y_m$ polynomials over the field $F_1(U_0, \ldots, U_m)$ of the degree $D - \gamma_\ell$ (respectively D) for $0 \leq \ell \leq t$, namely $\mathfrak{A}(f_0, \ldots, f_t) = f_0 g_0 + \ldots + f_t g_t$. Fix some numeration of monomials of degrees $D - \gamma_0, \ldots, D - \gamma_t, D$,respectively and write down the operator $\mathfrak{A}$ in the coordinates corresponding to this numeration, we obtain the matrix A of size $\binom{m+D}{m} \times \sum_{0 \leq \ell \leq t} \binom{m + D - \gamma_\ell}{m}$. The matrix A can be represented in a form $A = (A^{(num)}, A^{(for)})$ where the submatrix $A^{(num)}$ (called a numerical part of A) contains $\sum_{0 \leq \ell \leq t-1} \binom{m + D - \gamma_\ell}{m}$ columns and its entries belong to F_1 ; the submatrix $A^{(for)}$ (called a formal part of A) contains $\binom{m+D-1}{m}$ columns, and its entries are linear forms in the variables $U_0, \ldots, U_m$ over F_1 .

PROPOSITION 1. ([8]). a) A system $g_0 = \ldots = g_{t-1} = 0$ has a finite number of solutions in $\mathbb{P}^m(\bar{F}_1)$ iff the rank $rg(A) = \binom{m+D}{m}$;

denote $r = \binom{m+D}{m}$ and assume in the items b), c), d) that $rg(A) = r$;

b) all $r \times r$ minors of the matrix A generate a principal ideal, whose generator $R \in F_1[U_0, \ldots, U_m]$ is also their greatest common divisor;

c) homogeneous relatively to the variables $U_0, \ldots, U_m$ form R equals to the 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, moreover $(\xi_0^{(\varkappa)} : \ldots : \xi_m^{(\varkappa)}) \in \mathbb{P}^m(\bar{F}_1)$ is a solution of the system $g_0 = \ldots = g_{t-1} = 0$ and the number of occurences in the product R of the forms proportional to $L_\varkappa$ coincides with the multiplicity of the solution $(\xi_0^{(\varkappa)} : \ldots : \xi_m^{(\varkappa)})$ of the system $g_0 = \ldots = g_{t-1} = 0$ $(1 \leq \varkappa \leq D_1)$;

d) let Δ be a nonsingular $r \times r$ submatrix of the matrix A , containing $rg(A^{(num)})$ columns in the numerical part $A^{(num)}$ (one can easily see that such a submatrix exists), then $\det(\Delta)$ coincides with R up to a factor from F_1^* , besides the degree $\deg(R) = D_1 = r - rg(A^{(num)})$.

Let us apply the described construction to a system $(7)_{(X_1, \ldots, X_n)}$ taking $F_1 = F(X_1, \ldots, X_n)$, $m = 2$, we get a matrix A with the entries from the ring $F[X_1, \ldots, X_n, U_1, U, U_0]$. According to proposition 1a) the rank $rg(A_x) = r = \binom{D+2}{2}$ for any point x , provided that

$h_{i,j}(x) \neq 0$ (recall that r is the number of the rows of A).

Define a variant of Gaussian algorithm (VGA) as a succession of pairs of indices $(\alpha_0, \beta_0), (\alpha_1, \beta_1), \dots, (\alpha_\rho, \beta_\rho)$, herein $\alpha_\lambda \neq \alpha_\gamma, \beta_\lambda \neq \beta_\gamma$ for $\lambda \neq \gamma$. VGA determines a succession of matrices $A^{(0)} = A, A^{(1)}, \dots, A^{(\rho+1)}$. Introduce the notation $A^{(\ell)} = \left(a^{(\ell)}_{\alpha,\beta}\right)$, then $a^{(\ell+1)}_{\alpha,\beta} = a^{(\ell)}_{\alpha,\beta} - a^{(\ell)}_{\alpha_\ell,\beta}\, a^{(\ell)}_{\alpha,\beta_\ell} / a^{(\ell)}_{\alpha_\ell,\beta_\ell}$ for $\alpha \neq \alpha_0, \dots, \alpha_\ell$ distinguished from $\alpha_0, \dots, \alpha_\ell$ and $a^{(\ell+1)}_{\alpha_s,\beta} = a^{(\ell)}_{\alpha_s,\beta}$ for $0 \leqslant s \leqslant \ell$, apart from that, the leading entry $a^{(\ell)}_{\alpha_\ell,\beta_\ell} \neq 0$ for all $0 \leqslant \ell \leqslant \rho$. Then $a^{(\ell)}_{\alpha,\beta_s} = 0$ for every $0 \leqslant s \leqslant \ell - 1$ unless $\alpha = \alpha_t$ for a certain $0 \leqslant t \leqslant s$. Provided that $\alpha \neq \alpha_0, \dots, \alpha_{\ell-1}$ and $\beta \neq \beta_0, \dots, \beta_{\ell-1}$ denote by $\Delta^{(\ell)}_{\alpha,\beta}$ the determinant of $(\ell+1) \times (\ell+1)$ submatrix of the matrix A formed by the rows $\alpha_0, \dots, \alpha_{\ell-1}, \alpha$ and the columns $\beta_0, \dots, \beta_{\ell-1}, \beta$. It is well known that $a^{(\ell)}_{\alpha,\beta} = \Delta^{(\ell)}_{\alpha,\beta} / \Delta^{(\ell-1)}_{\alpha_{\ell-1},\beta_{\ell-1}}$ (see e.g. [6]).

We produce a sequence of VGA $\Gamma_1, \Gamma_2, \dots$ and a corresponding sequence of linearly independent over F polynomials $P_1, P_2, \dots \in F[X_1, \dots, X_n][U_1, U, U_0]$. Moreover, VGA Γ_s is applicable correctly to a matrix $A_{\tilde{x}}$ for any point $\tilde{x}$ from (possibly empty) quasi-projective variety $\mathcal{W}_s = \{x \in \bar{F}^n : 0 = P_t(x, U_1, U, U_0) \in \bar{F}[U_1, U, U_0]$ for all $1 \leqslant t < s$ and $0 \neq P_s(x, U_1, U, U_0)\}$. Besides $\bigcup_s \mathcal{W}_s \supset \mathcal{U}_{i,j}$ (see the beginning of the proof of lemma 1).

Considering a current VGA Γ_t we utilize the introduced above notations (in particular, applying Γ_t to A yields a succession $A^{(0)} = A, A^{(1)}, \dots$). Assume that $\Gamma_1, \dots, \Gamma_s$; $P_1, \dots, P_s$ are already produced $(s \geqslant 0)$. Then as Γ_{s+1} we take VGA satisfying the condition that for every $\ell \geqslant 0$ the index β_ℓ of the leading entry $(\alpha_\ell, \beta_\ell)$ of the matrix $A^{(\ell)}$ is the least possible such that $\beta_\ell > \beta_{\ell-1}$ and the polynomials $P_1, \dots, P_s, \prod_{0 \leqslant t \leqslant \ell} \Delta^{(t)}_{\alpha_t,\beta_t}$ are linearly independent over F. Assume that it is impossible to continue the succession $(\alpha_0, \beta_0), \dots, (\alpha_{\rho_{s+1}}, \beta_{\rho_{s+1}})$ with fulfilment of the formulated condition. Then we take this succession as VGA Γ_{s+1} and set the polynomial

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

If each entry of A is linearly dependent over F with $P_1, \dots, P_s$ then we terminate the process of producing $\Gamma_1, \dots, \Gamma_s$ without producing Γ_{s+1}.

Observe that if $\rho_{s+1} < r - 1$ then $\mathcal{W}_{s+1} \cap \mathcal{U}_{i,j} = \emptyset$. Indeed, let a point $x \in \mathcal{W}_{s+1} \cap \mathcal{U}_{i,j}$. By induction on $0 \leqslant \ell \leqslant \rho_{s+1}$ we deduce the equality $\left(a^{(\ell+1)}_{\alpha,\beta}\right)_x = \left(\Delta^{(\ell+1)}_{\alpha,\beta}\right)_x / \left(\Delta^{(\ell)}_{\alpha_\ell,\beta_\ell}\right)_x = 0$

for any $\beta_\ell < \beta < \beta_{\ell+1}$ and $\alpha \neq \alpha_0, \dots, \alpha_\ell$ since $(\Delta^{(\ell)}_{\alpha_\ell, \beta_\ell})_x \neq 0$ for $x \in \mathcal{W}_{s+1}$ (see (8)), and on the other hand $(\Delta^{(\ell+1)}_{\alpha,\beta})_x = 0$, otherwise we could take $\beta_{\ell+1} \leq \beta$, that contradicts to the choice of $\beta_{\ell+1}$. This implies that $(a^{(\ell+1)}_{\alpha,\beta})_x = 0$ when $\beta < \beta_{\ell+1}$ and $\alpha \neq \alpha_0, \dots, \alpha_\ell$, taking into account that the executed elementary transformations with the rows in VGA keep this property. Analogously $(a^{(\rho_{s+1}+1)}_{\alpha,\beta})_x = 0$ for $\beta > \beta_{\rho_{s+1}}$ and $\alpha \neq \alpha_0, \dots, \alpha_{\rho_{s+1}}$. Therefore, $rg(A_x) = \rho_{s+1} + 1 < r$ that contradicts to the relation $x \in \mathcal{U}_{i,j}$ and to proposition 1a) (see the system $(7)_x$).

Now we show the inclusion $\mathcal{U}_{i,j} \subset \bigcup_s \mathcal{W}_s$. Let $x \in \mathcal{U}_{i,j}$, then $rg(A_x) = r$, hence $(a_{\alpha,\beta})_x \neq 0$ for suitable α, β. Suppose that $x \notin \bigcup_s \mathcal{W}_s$, this means that $0 = P_1(x, U_1, U, U_0) = P_2(x, U_1, U, U_0) \cdots$, therefore the entry $a_{\alpha,\beta}$ cannot be linearly dependent with the polynomials $P_1, P_2, \dots$ that contradicts to the condition of terminating the process of producing $\Gamma_1, \Gamma_2, \dots$

Let us prove that for any point $x \in \mathcal{W}_{s+1} \cap \mathcal{U}_{i,j}$ the polynomial R_x, corresponding to the matrix A_x according to proposition 1b), coincides with the minor $\delta_1 \Delta_{s+1}(x) = \delta_1 \Delta^{(r-1)}_{\alpha_{r-1}, \beta_{r-1}}(x) \neq 0$ (here and further $\delta_1 \in F^*$, $\bar{\delta}_1, \bar{\delta}_2, \dots \in \bar{F}^*$), arising from VGA Γ_{s+1}. Indeed, consider such a unique λ that the cell $(\alpha_{\lambda-1}, \beta_{\lambda-1})$ is located in the numerical part $A^{(num)}$ and the cell $(\alpha_\lambda, \beta_\lambda)$ is located in the formal part $A^{(for)}$, then $rg(A^{(num)}) = \lambda$ since $(a^{(\lambda)}_{\alpha,\beta})_x = 0$ for any $\beta < \beta_\lambda$ and $\alpha \neq \alpha_0, \dots, \alpha_{\lambda-1}$ by virtue of the proved above. Hence $\delta_1 \Delta_{s+1}(x) = R_x$ in force of proposition 1d), besides $r - \lambda = deg_{U_1, U, U_0}(\Delta_{s+1})$, denote $D_2 = r - \lambda$.

Represent $\Delta_{s+1} = \sum_{0 \leq \omega \leq D_2} E^{(\omega)}_{s+1} U_0^{D_2 - \omega}$ where $E^{(\omega)}_{s+1}(X_1, \dots, X_n) \in F[X_1, \dots, X_n, U_1, U]$. Introduce quasiprojective varieties $\mathcal{W}^{(\omega)}_{s+1} = \{x \in \mathcal{W}_{s+1} : 0 = E^{(0)}_{s+1}(x) = \dots = E^{(\omega-1)}_{s+1}(x) \in \bar{F}[U_1, U];\ 0 \neq E^{(\omega)}_{s+1}(x)\}$. Then $\mathcal{W}^{(\omega_1)}_{s+1} \cap \mathcal{W}^{(\omega_2)}_{s+1} = \emptyset$ for $\omega_1 \neq \omega_2$ and $\mathcal{W}_{s+1} = \bigcup_{0 \leq \omega \leq D_2} \mathcal{W}^{(\omega)}_{s+1}$. For any point $x \in \mathcal{W}_{s+1} \cap \mathcal{U}_{i,j}$, proposition 1c) and the proved above entail the equality $\Delta_{s+1}(x) = \prod_{\varkappa} L_\varkappa^{c_\varkappa}$ where linear forms $L_\varkappa = \zeta_1^{(\varkappa)} U_1 + \zeta^{(\varkappa)} U + \zeta_0^{(\varkappa)} U_0$ correspond bijectively to the solutions $(\zeta_1^{(\varkappa)} : \zeta^{(\varkappa)} : \zeta_0^{(\varkappa)}) \in \mathbb{P}^2(\bar{F})$ of the system $(7)_x$, therefore for each point $x \in \mathcal{W}^{(\omega)}_{s+1} \cap \mathcal{U}_{i,j}$ the form $E^{(\omega)}_{s+1}(x) \mid \Delta_{s+1}(x)$ coincides with the product $\bar{\delta}_1 \prod_\mu L_\mu^{c_\mu}$ of all linear forms L_μ, for which $\zeta_0^{(\mu)} = 0$. Then $\zeta^{(\mu)} = 0$ for every such index μ according to the proved before proposition 1, hence $E^{(\omega)}_{s+1}(x) = \bar{\delta}_2 U_1^\omega$.

Write $E^{(\omega_1)}_{s+1} = \sum_{0 \leq \gamma \leq \omega_1} E^{(\omega_1)}_{s+1,\gamma} U_1^{\omega_1 - \gamma} U^\gamma$ where $E^{(\omega_1)}_{s+1,\gamma} \in$

$F[X_1,\dots,X_n]$, then $E^{(\omega)}_{s+1}(x)=E^{(\omega)}_{s+1,0}(x)\,U_1^{\omega}$ for $x\in\mathcal{W}^{(\omega)}_{s+1}\cap\mathcal{U}_{i,j}$. Then $\Delta_{s+1}(x)/E^{(\omega)}_{s+1}(x)$ coincides with the product $\bar\delta_3\prod_\gamma L_\gamma^{c_\gamma}$ of all linear forms L_γ, for which $\zeta_0^{(\gamma)}\neq 0$, when $x\in\mathcal{W}^{(\omega)}_{s+1}\cap\mathcal{U}_{i,j}$, in particular a relation $E^{(\omega)}_{s+1}(x)\,|\,E^{(\omega_1)}_{s+1}(x)$ is valid in the ring $\bar F[U_1,U]$ for arbitrary $\omega_1\geqslant\omega$. Therefore $E^{(\omega_1)}_{s+1,\gamma}(x)=0$ if $\omega_1-\gamma<\omega$, thus $\Delta_{s+1}(x)/E^{(\omega)}_{s+1}(x)=$

$$\frac{1}{E^{(\omega)}_{s+1,0}(x)}\sum_{\omega\leqslant\omega_1\leqslant D_2}U_0^{D_2-\omega_1}\sum_{0\leqslant\gamma\leqslant\omega_1-\omega}E^{(\omega_1)}_{s+1,\gamma}(x)\,U_1^{\omega_1-\gamma-\omega}U^{\gamma}\in\bar F[U_1,U,U_0].$$

So, a polynomial $(\Delta_{s+1}(x)/E^{(\omega)}_{s+1}(x))\,(0,-1,Y)\in\bar F[Y]$ coincides with the product $\bar\delta_4\prod_\gamma(Y-y_\gamma)^{c_\gamma}$, where $y_\gamma=\zeta^{(\gamma)}/\zeta_0^{(\gamma)}$ ranges over all the solutions of the system $(6)_x$ (see the claim proved before proposition 1), for each point $x\in\mathcal{W}^{(\omega)}_{s+1}\cap\mathcal{U}_{i,j}$.

For the fixed indices i,j,m,s denote the quasiprojective variety $\mathcal{Y}^{(1)}_q=\mathcal{W}^{(\omega)}_{s+1}\cap\mathcal{U}_{i,j}$ (this yields the polynomials $g^{(1)}_{q,t_1},g^{(2)}_{q,t_2}\in F[X_1,\dots,X_n]$ such that $\mathcal{Y}^{(1)}_q=\{x\in\bar F^n:\ \&_{t_1}(g^{(1)}_{q,t_1}(x)=0)\ \&\ \bigvee_{t_2}(g^{(2)}_{q,t_2}(x)\neq 0)\}$; fixing a certain t_3 we obtain pairwise disjunctive quasiprojective varieties $\mathcal{Y}_q=\{x\in\bar F^n:\&_{t_1}(g^{(1)}_{q,t_1}(x)=0)\ \&\ \&_{t_2<t_3}(g^{(2)}_{q,t_2}(x)=0)\ \&\ (g^{(2)}_{q,t_3}(x)\neq 0)\}$ and the required in lemma 1a) polynomials $g_{q,t}$). Thereupon set a polynomial $\varphi_q=\sum_{\omega\leqslant\omega_1\leqslant D_2}Y^{D_2-\omega_1}E^{(\omega_1)}_{s+1,\omega_1-\omega}(-1)^{\omega_1-\omega}\in F[X_1,\dots,X_n,Y]$. Then for $x\in\mathcal{Y}_q$ the equality $\varphi_q(x)=(E^{(\omega)}_{s+1,0}(x)\,\Delta_{s+1}(x)/E^{(\omega)}_{s+1}(x))\,(0,-1,Y)$ is true, this implies the required in lemma 1b) coincidence of the varieties

$\{(x,y)\in\bar F^{n+1}:h_1(x,y)=\dots=h_K(x,y)=0,\ h_0(x,y)\neq 0\}\cap(\mathcal{Y}_q\times\bar F)=$

$\{(x,y):\tilde h_{i,j}(x,y)=h_{i+1}(x,y)=\dots=h_K(x,y)=0;\ h_0(x,y)\neq 0\}\cap(\mathcal{Y}_q\times\bar F)=$

$\{(x,y):\varphi_q(x,y)=0\}\cap(\mathcal{Y}_q\times\bar F)$. Moreover, the leading coefficient $lc_Y(\varphi_q)=E^{(\omega)}_{s+1,0}$ does not vanish anywhere on $\mathcal{Y}_q$. Evidently $\bigcup_q\mathcal{Y}_q=\{x\in\bar F^n:h_{i,j}(x)\neq 0$ for some $1\leqslant i\leqslant K$ and $j\}$.

It remains to check the bounds (4) and the running time of the algorithm. Taking into account that Δ_{s+1} is a minor of the matrix A, the polynomial P_{s+1} (see (8)) is a product of not more than $r\leqslant\mathcal{P}(D)\leqslant\mathcal{P}(d_0)$ minors of A and involving bounds (3) one can deduce the following bounds: $\deg_{X_1,\dots,X_n,U_1,U,U_0}(\Delta_{s+1})$,

$\deg_{X_1,\dots,X_n,U_1,U,U_0}(P_{s+1}),\ \deg_{X_1,\dots,X_n}(g_{q,t}),\ \deg_{X_1,\dots,X_n,Y}(\varphi_q)\leqslant\mathcal{P}(d_0);$

$\deg_{T_1,\dots,T_e}(\Delta_{s+1}),\ \deg_{T_1,\dots,T_e}(P_{s+1}),\ \deg_{T_1,\dots,T_e}(g_{q,t}),\ \deg_{T_1,\dots,T_e}(\varphi_q)\leqslant d_2\,\mathcal{P}(d_1,d_0);$

$l(\Delta_{s+1}),\ l(P_{s+1}),\ l(g_{q,t}),\ l(\varphi_q)\leqslant(M_1+M_2+(e+n)\log d_2)\,\mathcal{P}(d_1,d_0).$

Since $P_1,P_2,\dots$ are linearly independent over F, one concludes that the number of them does not exceed $\mathcal{P}(d_0^n)$, hence $1 \leqslant q \leqslant N_1 \leqslant K\mathcal{P}(d_0^n)$, $0 \leqslant t \leqslant N_2 \leqslant K\mathcal{P}(d_0^n)$; the bounds (4) are ascertained. From (4) one can infer $\mathcal{P}(K, M_1, M_2, (d_1 d_2)^e d_0^{n+e})$ bound on the running time of the algorithm, because this is a bound on bit-sizes of all the intermediate polynomials in the calculations, and also a bound on the number of executed with them arithmetic operations, that completes the proof of lemma 1.

2. Splitting subroutine and quantifier elimination algorithm

Before describing the splitting subroutine, we ascertain the following lemma 2 allowing under relevant conditions to decrease the order of a system of differential equations. Let $g_0, g_1, \ldots, g_\gamma, f_0, f_1, \ldots, f_K \in \mathbb{Q}\{u, u_1, \ldots, u_n\}$ be differential polynomials. Assume that the bounds $ord_u(g_\beta) \leqslant r-t$; $ord_u(f_i) \leqslant r$; $ord_{u_j}(g_\beta), ord_{u_j}(f_i) \leqslant R$; $deg(g_\beta), deg(f_i) < d$; $l(g_\beta), l(f_i) \leqslant M$

are valid for any $0 \leqslant \beta \leqslant \gamma$, $0 \leqslant i \leqslant K$, $1 \leqslant j \leqslant n$ where deg (here and further) denotes the degree relatively to all the indeterminates $X, u, u^{(1)}, \ldots, u^{(r)}, u_1, \ldots, u_1^{(R)}, \ldots, u_n, \ldots, u_n^{(R)}$.

LEMMA 2. For given $g_0, \ldots, g_\gamma, f_0, \ldots, f_K$ one can produce such differential polynomials $\hat{f}_0, \hat{f}_1, \ldots, \hat{f}_K \in \mathbb{Q}\{u, u_1, \ldots, u_n\}$ that a system

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

is equivalent in the ring $\mathbb{Q}\{u, u_1, \ldots, u_n\}$ to a system $g_0 = g_1 = \ldots = g_\gamma = \hat{f}_1 = \ldots = \hat{f}_K = 0$; $\hat{f}_0 \frac{\partial g_0}{\partial u^{(r-t)}} \neq 0$. Besides, the following bounds: $ord_u(\hat{f}_i) \leqslant r-t$; $ord_{u_j}(\hat{f}_i) \leqslant R+t$; $deg(\hat{f}_i) \leqslant \mathcal{P}(d,t)$; $l(\hat{f}_i) \leqslant (M + nR + r)\mathcal{P}(d,t)$ are true for any $0 \leqslant i \leqslant K$, $1 \leqslant j \leqslant n$. Finally, the time of producing $\hat{f}_0, \ldots, \hat{f}_K$ can be estimated by $\mathcal{P}(K, M, (dt)^{n(R+t)+r})$.

Proof. Observe that for every $s \geqslant 1$ a derivative $g_0^{(s)} = u^{(r-t+s)}\left(\frac{\partial g_0}{\partial u^{(r-t)}}\right) - Q_s$, where a differential polynomial $Q_s \in \mathbb{Q}[X, u, \ldots, u^{(r-t+s-1)}, u_1, \ldots, u_1^{(R+s)}, \ldots, u_n, \ldots, u_n^{(R+s)}]$. Obviously, $deg(g_0^{(s)}) < d$; $l(g_0^{(s)}) \leqslant M + O(s \log d)$.

Define a weight of a monomial $X^\beta \prod_{l \leqslant r} (u^{(l)})^{d_l} \prod_{s,j} (u_j^{(s)})^{\beta_{j,s}}$ as $wgt = \sum_{r-t+1 \leqslant l \leqslant r} d_l (l - r + t)$, the weight of a differential polynomial is defined as the maximum of the weights of its monomials. Evidently, $wgt(g_0^{(s)}) \leqslant s$.

Assume by recursion that for a certain $0 \leqslant s < t$ differential polynomials $f_{i,s} \in \mathbb{Q}[X, u, u^{(1)}, \ldots, u^{(r-s)}, u_1, \ldots, u_1^{(R+t)}, \ldots, u_n, \ldots, u_n^{(R+t)}]$ are already produced such that the system (9) is equivalent to a system $g_0 = g_1 = \ldots = g_\gamma = f_{1,s} = \ldots = f_{K,s} = 0$; $f_{0,s} \frac{\partial g_0}{\partial u^{(r-t)}} \neq 0$. For the base of the recursion $(s=0)$ we set $f_{i,0} = f_i$. Let $wgt(f_{i,s}) \leqslant W_s$; $deg(f_{i,s}) < D_s$; $l(f_{i,s}) \leqslant M_s$. Fix some $0 \leqslant i \leqslant K$. Obviously $deg_{u^{(r-s)}}(f_{i,s}) \leqslant W_s/(t-s)$. Substitute in $f_{i,s}$ instead of $u^{(r-s)}$ a quotient of differential polynomials $Q_{t-s} / \left(\frac{\partial g_0}{\partial u^{(r-t)}}\right)$ and in the obtained expression eliminate a denominator multiplying the expression on $\left(\frac{\partial g_0}{\partial u^{(r-t)}}\right)^{deg_{u^{(r-s)}}(f_{i,s})}$, as a result we get a differential polynomial $f_{i,s+1} \in \mathbb{Q}[X, u, \ldots, u^{(r-s-1)}, u_1, \ldots, u_n^{(R+t)}]$. Clearly a system $g_0 = \ldots = g_\gamma = f_{1,s+1} = \ldots = f_{K,s+1} = 0$; $f_{0,s+1}\left(\frac{\partial g_0}{\partial u^{(r-t)}}\right) \neq 0$ is equivalent to $g_0 = \ldots = g_\gamma = f_{1,s} = \ldots = f_{K,s} = 0$; $f_{0,s}\left(\frac{\partial g_0}{\partial u^{(r-t)}}\right) \neq 0$ and hence is equivalent to (9). Finally, set $\hat{f}_i = f_{i,t}$.

Taking into account inequality $wgt(Q_s) \leqslant t - s = wgt(u^{(r-s)})$ one can deduce that after the described substitution the weight does not increase, in other words $W_{s+1} \leqslant W_s$. Moreover $deg(f_{i,s+1}) \leqslant D_s + d \cdot deg_{u^{(r-s)}}(f_{i,s}) \leqslant D_s + d\frac{W_s}{t-s}$. Besides $l(f_{i,s+1}) \leqslant M_s + (M + O(s \log d))(W_s/(t-s)) + (n(R+t)+r)\log(D_{s+1})$. Since $wgt(f_i) \leqslant W_0 < dt$, we conclude that $deg(\hat{f}_i) = O(d^2 t \log t)$; $l(\hat{f}_i) = O(Mdt\log t + dt^2 \log d \log t + (n(R+t)+r)t \cdot \log(dt))$. Finally, the algorithm produces $f_{i,s+1}$ starting with $f_{i,s}$ in time $\mathcal{P}(M_{s+1}, D_{s+1}^{n(R+t)+r})$. Lemma 2 is proved.

Now we proceed to describing a splitting subroutine of a system of the kind

$$g = h_1 = \ldots = h_\ell = 0; \quad h_0 \neq 0 \tag{10}$$

where $g, h_i \in \mathbb{Q}[X, u, \ldots, u^{(r)}, u_1, \ldots, u_n^{(R)}]$, apart from that $0 \leqslant ord_u(g) = p < r$. Write $g = \sum_{0 \leqslant \alpha \leqslant \gamma} g_\alpha (u^{(p)})^\alpha$, herein $ord_u(g_\alpha) \leqslant p-1$.

The system (10) is equivalent to the dijunction of the following formulas (11), (12) (we call this equivalence a splitting of the system (10) and g a splitted polynomial):

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

$$(g_0 = \dots = g_\gamma = h_1 = \dots = h_\ell = 0) \& (h_0 \neq 0). \tag{12}$$

Let differential polynomials $f_0, \dots, f_K \in \mathbb{Q}[X, u, \dots, u^{(r)}, u_1, \dots, u_n^{(R)}]$ satisfy the following bounds: $deg(f_i) < d$, $\ell(f_i) \leqslant M$ for every $0 \leqslant i \leqslant K$. Denote $f_i = \sum_s f_{i,s} (u^{(r)})^s$ where $ord_u(f_{i,s}) \leqslant r-1$. Consider a formula

$$\Omega_1 = ((f_1 = \dots = f_K = 0) \& (f_0 \neq 0)) \tag{13}$$

Our nearest goal is to design an algorithm producing a quantifier-free formula equivalent to a formula $\exists u(\Omega_1)$. Apply to (13) lemma 1, taking the derivative $u^{(r)}$ as the variable Y and $X, u, \dots, u^{(r-1)}, u_1, \dots, u_n^{(R)}$ as $X_1, \dots, X_n$ respectively. It yields differential polynomials $g_{q,t} \in \mathbb{Q}[X, u, \dots, u^{(r-1)}, u_1, \dots, u_n^{(R)}]$, $\varphi_q \in \mathbb{Q}[X, u, \dots, u^{(r-1)}, u^{(r)}, u_1, \dots, u_n^{(R)}]$ such that formula (13) is equivalent to the disjunction of the following formulas (14), (15):

$$\bigvee_q (\underset{t \geqslant 1}{\&} (g_{q,t} = 0) \& (\varphi_q = 0) \& (g_{q,0} \neq 0)) \tag{14}$$

$$\underset{i \geqslant 1; s}{\&} (f_{i,s} = 0) \& (f_0 \neq 0) \tag{15}$$

To any system $\underset{t \geqslant 1}{\&} (g_{q,t} = 0) \& (\varphi_q = 0) \& (g_{q,0} \neq 0)$ (from (14)) the algorithm applies the splitting subroutine, considering this system as (10) and an arbitrary $g_{q,t}$ as a splitted polynomial, provided that $ord_u(g_{q,t}) \geqslant 0$. Thereupon the algorithm applies repeatedly the splitting subroutine to all the obtained systems of the kind (12) taking them as the system (10) (without taking φ_q as a splitted polynomial). In a similar way the algorithm applies the splitting subroutine to the system (15) taking it as (10) and an arbitrary polynomial among $\{f_{i,s}\}_{i \geqslant 1; s}$ as a splitted one, provided that the indeterminate u occurs in it, and continues applying repeatedly the splitting subroutine to all the obtained systems of the kind (12) taking them as (10).

Observe that the algorithm is unable at some step to apply the splitting subroutine to a certain obtained system of the kind (12) iff either the system is of the form $\Omega_2 = \underset{t \geqslant 1; E}{\&} (g_{q,t,E} = 0) \& (\varphi_q = 0) \& (g_{q,0} \neq 0)$ (i.e. it arises from (14)) where $g_{q,t} = \sum_E g_{q,t,E} u^{\varepsilon_0} (u^{(1)})^{\varepsilon_1} \dots (u^{(r-1)})^{\varepsilon_{r-1}}$, herein $g_{q,t,E} \in \mathbb{Q}[X, u_1, \dots, u_n^{(R)}]$ and $E = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{r-1})$ is a multiindex, or the system arises from (15) and is of the form $\Omega_3 = \underset{i \geqslant 1; s; E}{\&} (f_{i,s,E} = 0) \& (f_0 \neq 0)$.

We claim that a formula $\exists u\,(\Omega_2)$ is equivalent to the following disjunction

$$\bigvee_{E_0}\Big(\underset{t\geq 1;E}{\&}(g_{q,t,E}=0)\,\&\,(g_{q,0,E_0}\neq 0)\Big) \tag{16}$$

Consider some $u_1,\ldots,u_n$ and denote by $K=\mathbb{Q}\langle u_1,\ldots,u_n\rangle$ the differential field generated by them. Let (16) be true. Take $u,u^{(1)},\ldots,u^{(r-1)}$ to be algebraically independent over the field K, then $g_{q,0}(X,u,u^{(1)},\ldots,u^{(r-1)},u_1,\ldots,u_n^{(R)})\neq 0$ hence $0\neq lc_{u^{(r)}}(\varphi_q)\in K[u,u^{(1)},\ldots,u^{(r-1)}]$ by virtue of lemma 1b) and involving remark 2) just after lemma 1. Consider an irreducible over the field $K(u,u^{(1)},\ldots,u^{(r-1)})$ divisor $\tilde{\varphi}_q\in K[u,\ldots,u^{(r-1)},u^{(r)}]$ of the polynomial φ_q. Then take u satisfying the single relation $\tilde{\varphi}_q(u,u^{(1)},\ldots,u^{(r-1)},u^{(r)})=0$ (so, u is an element of the differential factor-ring $K\{u\}/(\tilde{\varphi}_q)$ without divisors of zero, see [7]). The equality $0=\varphi_q(u,u^{(1)},\ldots,u^{(r-1)},u^{(r)})\in K\{u\}/(\tilde{\varphi}_q)$ proves the claim.

Analogously and even easier, a formula $\exists u\,(\Omega_3)$ is equivalent to the following disjunction

$$\bigvee_{E_0}\Big(\underset{i\geq 1;S;E}{\&}(f_{i,S,E}=0)\,\&\,(f_{0,E_0}\neq 0)\Big) \tag{17}$$

For every obtained (after executing splitting subroutine at some step) formula of the kind (11) the algorithm applies lemma 2 to each its disjunctive term (for a given β we take $g_0=\dfrac{\partial^\beta g}{\partial (u^{(p)})^\beta}$, see (9)). It yields the differential polynomials $\hat{h}_{0,\beta},\hat{h}_{1,\beta},\ldots,\hat{h}_{l,\beta}\in\mathbb{Q}[X,u,u^{(1)},\ldots,u^{(p)},u_1,\ldots,u_n^{(R+r-p)}]$ such that (11) is equivalent to the following disjunction

$$\bigvee_{0\leq\beta\leq\gamma-1}\Big(\Big(g=\frac{\partial g}{\partial u^{(p)}}=\ldots=\frac{\partial^\beta g}{\partial (u^{(p)})^\beta}=\hat{h}_{1,\beta}=\ldots=\hat{h}_{l,\beta}=0\Big)\,\&\,\Big(\hat{h}_{0,\beta}\frac{\partial^{\beta+1} g}{\partial (u^{(p)})^{\beta+1}}\neq 0\Big)\Big). \tag{18}$$

To any disjunctive term from the formular (18) the described process is again applied taking this term as a formula of the kind (13) etc. It completes the description of the algorithm producing a quantifier-free formula equivalent to a formula $\exists u\,(\Omega_1)$ (see (13)). Notice that the terminal systems (in which the indeterminate u does not occur) are of the form (16) or (17).

Now we estimate the number of systems obtained by the described above algorithm from (13) and their parameters. Observe that for any intermediate system, occuring in it differential polynomials belong to a ring $\mathbb{Q}[X,u,\dots,u^{(\rho)},u_1^{(1)},\dots,u_1^{(R+r-\rho)},\dots,u_n,\dots,u_n^{(R+r-\rho)}]$ for some ρ, hence the polynomials occuring in systems of forms (16), (17) belong to $\mathbb{Q}[X,u_1,\dots,u_1^{(R+r)},\dots,u_n,\dots,u_n^{(R+r)}]$ From system (13) lemma 1 yields $Kd^{c_1(nR+r)}$ disjunctive terms in formulas (14), (15) (here and below $c_1,c_2,\dots$ are suitable constants). The degree of each polynomial occuring in (14), (15) is less than d^{c_2} by lemma 1. The subroutine splitting disjunctive terms in (14), (15) produces $Kd^{c_3(nR+r)}$ systems of kinds (11), (12). For any disjunctive term from (11) lemma 2 gives a system (18) with the polynomials of degrees less than $(d(r-\rho))^{c_4}$.

Basing on these speculations one can prove by induction on $0\leqslant\rho\leqslant r$ that after repeatedly applying the described process yields in the whole not more than $K(dr)^{c_5^{\rho}(nR+r)}$ intermediate systems of the form $\tilde g_{1,\rho}=\dots=\tilde g_{\tilde s,\rho}=0,\ \tilde g_{0,\rho}\neq 0$ where $\tilde g_{\alpha,\rho}\in\mathbb{Q}[X,u,u^{(1)},\dots,u^{(r-\rho)},u_1,\dots,u_1^{(R+\rho)},\dots,u_n,\dots,u_n^{(R+\rho)}]$, besides $\tilde s\leqslant K(dr)^{c_5^{\rho}(nR+r)}$, $deg(\tilde g_{\alpha,\rho})\leqslant(dr)^{c_6^{\rho}}$, $\ell(\tilde g_{\alpha,\rho})\leqslant(M+nR)(dr)^{c_6^{\rho}}$. Thus, the formula $\exists u(\Omega_1)$ (see (13)) is equivalent to a disjunction of $Kd^{c_7^{r}nR}$ systems of the kind $g_1=\dots=g_s=0,\ g_0\neq 0$ (see (16), (17)), where $g_\alpha\in\mathbb{Q}[X,u_1,\dots,u_1^{(R+r)},\dots,u_n,\dots,u_n^{(R+r)}]$, moreover $s\leqslant Kd^{c_7^{r}nR}$, $deg(g_\alpha)\leqslant d^{c_7^{r}}$, $\ell(g_\alpha)\leqslant(M+nR)d^{c_8^{r}}$. The time required to produce this quantifier-free disjunction is less than $\mathcal{P}(KMd^{c_9^{r}nR})$.

Describe now a procedure reducing a quantifier-free formula of the kind Ω, see (1) in the introduction, to disjunctive normal form. We utilize the notations from (1) and consider $\{f_1,\dots,f_N\}$ occuring in Ω as (usual) polynomials in $(n+m)(r+1)+1$ variables. For any subset $I\subset\{1,\dots,N\}$ we name $\mathcal{B}=\mathop{\&}_{i\in I}(f_i=0)\mathop{\&}_{i\in\{1,\dots,N\}\setminus I}(f_i\neq 0)$ an elementary $\{f_1,\dots,f_N\}$-formula. Corollary 1 to theorem 2 [6] implies a bound $(\sum_{i\in I} deg\, f_i)^{(n+m)(r+1)+1}<(dN)^{(n+m)(r+1)+1}$ on the number of elementary $\{f_1,\dots,f_N\}$-formulas, determining nonempty quasiprojective varieties (in a space $\bar F_1^{(n+m)(r+1)+1}$ for arbitrary algebraically closed field $\bar F_1$), such elementary formulas we call nontrivial. One can find all of them successively. Assuming that for some $0\leqslant t<N$ all nontrivial elementary $\{f_1,\dots,f_t\}$-formulas $\mathcal{B}_1=\mathop{\&}_{i\in I_1}(f_i=0)\mathop{\&}_{i\in\{1,\dots,t\}\setminus I_1}(f_i\neq 0)$ are found, one tests, which among two elementary $\{f_1,\dots,f_t,f_{t+1}\}$-formulas $\mathcal{B}_1\,\&\,(f_{t+1}=0)$ and $\mathcal{B}_1\,\&\,(f_{t+1}\neq 0)$ are nontrivial involving the algorithm from [1] (see also [2, 4, 5]). Thus, one can list all nontrivial elementary $\{f_1,\dots,f_N\}$-formulas in time $\mathcal{P}(M,N^{(n+m)r},d^{(n+m)^2r^2})$ ([1]).

Next, for each nontrivial elementary $\{f_1,\dots,f_N\}$-formula $\mathcal{B}$ the procedure detects, whether it is consistent with Ω, replacing in Ω every atomic subformula $(f_i=0)$ by its truth value from $\mathcal{B}$. The obtained formula is true iff $\mathcal{B}$ is consistent with Ω . Then Ω is equivalent to the disjunction of all the consistent with Ω nontrivial elementary $\{f_1,\dots,f_N\}$ -formulas.

The quantifier elimination algorithm repeatedly applies to (1) alternatively described two procedures of eliminating one quantifier (see (13) and after it) and reducing a quantifier-free formula to disjunctive normal form and yields formula (2). The bounds on parameters of formula (2) and on the working time of the algorithm (see the theorem) one can prove by induction on n .

References

1. A.L.Chistov, D.Yu.Grigor'ev. Solving systems of algebraic equations in subexponential time I, II. - Preprints LOMI, E-9-83, E-10-83, Leningrad, 1983.
2. 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.
3. D.Yu.Grigor'ev. Complexity of quantifier elimination in the theory of ordinary differential equations. - Proc.VIII All-Union conf. Math.Logic, Moscow, 1986, p.46 (in Russian).
4. D.Yu.Grigor'ev. Computational Complexity in Polynomial Algebra. - Proc.International Congress of Mathematicians, 1987, Berkeley.
5. D.Yu.Grigor'ev, A.L.Chistov. Fast decomposition of polynomials into irreducible ones and the solution of systems of algebraic equations. - Soviet Math.Dokl., 1984, v.29, p.380-383.
6. J.Heintz. Definability and fast quantifier elimination in algebraically closed fields. - Theor.Comput.Sci., 1983, v.24, p.239-278.
7. E.R.Kolchin. Differential algebra and algebraic groups. - Academic Press, 1973.
8. D.Lazard. Resolution des systemes d'equations algebriques. - Theor. Comput.Sci., 1981, v.15, p.77-110.
9. A.Seidenberg. An elimination theory for differential algebra. - Univ.of Calif.Press, 1956, v.3, N 2, p.31-66.