DOI 10.1007/s10958-018-3868-z
Journal of Mathematical Sciences, Vol. 232, No. 2, July, 2018

SYSTEMS WITH PARAMETERS, OR EFFICIENTLY SOLVING SYSTEMS OF POLYNOMIAL EQUATIONS: 33 YEARS LATER. I

A. L. Chistov*

UDC 513.6, 518.5

Consider a system of polynomial equations with parametric coefficients over an arbitrary ground field. We show that the variety of parameters can be represented as a union of strata. For values of parameters from each stratum, the solutions of the system are given by algebraic formulas depending only on this stratum. Each stratum is a quasiprojective algebraic variety with degree bounded from above by a subexponential function in the size of the input data. Also, the number of strata is subexponential in the size of the input data. Thus, here we avoid double exponential upper bounds on the degrees and solve a long-standing problem. Bibliography: 11 *titles.*

Introduction

Let k be an arbitrary field of characteristic exponent p containing sufficiently many elements. Denote by $\overline{k}$ an algebraic closure of k. Let ν be a nonnegative integer. Let $a_1, \ldots, a_\nu$ be a family of independent variables (or parameters) over k. Denote by $\mathbb{A}^\nu(\overline{k})$ the affine space of parameters with the coordinate functions $a_1, \ldots, a_\nu$ (in a more general situation, one can consider an algebraic variety of parameters $\mathcal{V} \subset \mathbb{A}^\nu(\overline{k})$, but this case can easily be reduced to the special case of $\mathcal{V} = \mathbb{A}^\nu(\overline{k})$).

In this paper, we consider the problem of solving systems of polynomial equations with parametric coefficients from $k[a_1, \ldots, a_\nu]$. At the output, we obtain solutions depending on these parameters; precise statements are given below, see Theorems 1 and 2. To obtain the required results, we rely on our algorithms from [2, 3, 7] for solving usual systems of polynomial equations. They have the best known complexity bounds in the general case. But it turns out that they are not sufficiently explicit for the aims of the present paper. So, in this paper we significantly revise the algorithms from [2, 3, 7] and give a new, probably more clear and succinct, background for them (although the main ideas remain the same). Actually, in this paper, as the special case $\nu = 0$ of our main result on systems with parameters, we obtain improved and more explicit versions of the algorithms from [2, 3, 7] for solving systems of polynomial equations. Also, we give a self-contained background for these new versions. Now, for the reader's convenience, we would like to list the improvements in these new versions of the algorithms for solving polynomial systems as compared with [2, 3, 7].

1) We consider separable bases of transcendence of the fields of rational functions of irreducible components of the variety of solutions, see Lemma 7 in Sec. 4[1].
2) A more explicit reduction to the zero-dimensional case is described. Everything is reduced to the computation of some determinants and resultants (which, of course, are also determinants).

*St. Petersburg Department of Steklov Institute of Mathematics, St. Petersburg, Russia, e-mail: alch@pdmi.ras.ru.

[1]Sometimes, in this first part of the paper, mainly when surveying the results, we use references to lemmas, sections, and so on from the next part (or parts; this depends on the circumstances) of the paper. In all the parts, the numeration of the theorems (respectively, lemmas, sections, and so on) continues from this first one.

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 462, 2017, pp. 122–166. Original article submitted August 15, 2017.

3) We suggest a new explicit construction of generic points of irreducible components of the variety of solutions. The coordinates of these generic points are represented as quotients of some partial derivatives, see Secs. 3 and 6.
4) We suggest a new explicit and clear construction of systems of polynomial equations giving irreducible components of the variety of solutions, see (xii) below. This construction is valid even for arbitrary equidimensional algebraic varieties, see (xi) below and Lemma 8 in Sec. 4.
5) We obtain a decomposition of the variety of solutions into a union of equidimensional algebraic varieties. In nonzero characteristic, we obtain an explicit decomposition of the variety of solutions into a union of equidimensional algebraic varieties defined over the fields k^{1/p^r} where r is a nonnegative integer, see (v) below.
6) We obtain an explicit criterion to decide whether linear forms $Y_0, \ldots, Y_s$ give a separable basis of transcendence $Y_1/Y_0, \ldots, Y_s/Y_0$ of the field of rational functions of every irreducible component of dimension s of the variety of solutions of the original system, see Lemma 15 in Sec. 6.
7) More presice estimates for the degrees, lengths of coefficients, and running time of the algorithm are given. For example, we use D'_{n-s}, D_{n-s} (see below) in place of d^{n-s}, cf. [2, 3, 7].
8) Only polynomials in one variable are to be factored into irreducibles, i.e., it suffices to have factorization algorithms only for one-variable polynomials.
9) We have fixed an inaccuracy in Lemma 2.11 of [2] (one should delete this lemma from that paper), see Remark 8 in Sec. 4. Actually, this correction is simple, and it is made in [7, p. 221], but one cannot find it in English. Still, it is strange that nobody (to the author's knowledge) has noticed this inaccuracy.

Now we return to systems with parameters. Let $m, n \geq 1$ be integers. Let $f_0, \ldots, f_{m-1} \in k[a_1, \ldots, a_\nu, X_0, \ldots, X_n]$ be polynomials homogeneous with respect to $X_0, \ldots, X_n$. Assume that

$$\deg_{X_0,\ldots,X_n} f_i = d_i \leq d, \quad \deg_{a_1,\ldots,a_\nu} f \leq d' \tag{1}$$

for some integers $d_0 \geq d_1 \geq \ldots \geq d_{m-1} \geq 0$ and $d, d' \geq 2$.

Hence each polynomial f_i can be represented in the form

$$f_i = \sum_{\substack{i_1,\ldots,i_\nu \geq 0,\ i_1+\ldots+i_\nu \leq d',\\ j_0,\ldots,j_n \geq 0,\ j_0+\ldots+j_n = d_i}} f_{i,i_1,\ldots,i_\nu,j_0,\ldots,j_n} a_1^{i_1} \cdot \ldots \cdot a_\nu^{i_\nu} X_0^{j_0} \cdot \ldots \cdot X_n^{j_n}, \tag{2}$$

where $0 \leq i \leq m-1$, all $i_1, \ldots, i_\nu$, $j_0, \ldots, j_n$ are integers, and $f_{i,i_1,\ldots,i_\nu,j_0,\ldots,j_n} \in k$.

Let $a^* = (a_1^*, \ldots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$. Denote by $V_{a^*} \subset \mathbb{P}^n(\overline{k})$ the variety of all solutions of the system of polynomial equations

$$f_0(a_1^*, \ldots, a_\nu^*, X_0, \ldots, X_n) = \ldots = f_{m-1}(a_1^*, \ldots, a_\nu^*, X_0, \ldots, X_n) = 0 \tag{3}$$

(if $\nu = 0$, then $\mathbb{A}^\nu(\overline{k}) = \{()\}$ is a one-element set; if $a^{(0)} = () \in \mathbb{A}^\nu(\overline{k})$, then the sequence $a_1^{(0)}, \ldots, a_\nu^{(0)}$ is empty and we assume that $f_i(a_1^{(0)}, \ldots, a_\nu^{(0)}, X_0, \ldots, X_n) = f_i$ for all i; we adopt a similar convention also for other polynomials with parametric coefficients in the case where $\nu = 0$).

For every point $a^* \in \mathbb{A}^\nu(\overline{k})$, for every integer s, where $0 \leq s \leq n$, denote by $V_{a^*,s}$ the union of all irreducible components W of the variety V_{a^*} such that $\dim W = s$. For example, $V_{a^*,s} = \varnothing$ if $n > m$ and $s < n - m$.

Let c and c' be integers such that $-1 \le c \le n$ and $0 \le c' \le \max\{0, c\}$. Put $V_{a^*}^{(c',c)} = \bigcup\limits_{c' \le s \le c} V_{a^*,s}$. Thus $V_{a^*}^{(c',c)}$ is the union of all irreducible components W of the variety V_{a^*} such that $c' \le \dim W \le c$. In particular, $V_{a^*}^{(0,n)} = V_{a^*}$, $V_{a^*}^{(0,0)} = V_{a^*,0}$, and $V_{a^*}^{(0,-1)} = \varnothing$.

Denote by $\mathcal{U}_c$ the subset of all $a^* \in \mathbb{A}^\nu(\overline{k})$ such that $\dim V_{a^*} \le c$. One can prove that it is a subset of $\mathbb{A}^\nu(\overline{k})$ open in the Zariski topology. Hence if $a^* \in \mathcal{U}_c$, then $V_{a^*} = V_{a^*}^{(0,c)}$. If $a^* \in \mathcal{U}_{-1}$, then $V_{a^*} = \varnothing$.

Consider the problem of representing the set of parameters

$$\mathcal{U}_c = \bigcup_{\alpha \in A} \mathcal{W}_\alpha \tag{4}$$

as a union of finitely many (i.e., $\#A < +\infty$) quasiprojective algebraic varieties $\mathcal{W}_\alpha$ satisfying the following properties. For every $\alpha \in A$, for all $a^* = (a_1^*, \dots, a_\nu^*) \in \mathcal{W}_\alpha$, the subvariety of solutions $V_{a^*}^{(c',c)}$ is given uniformly, i.e., by some algebraic formulas (similarly to [2], see below for details) everywhere defined on $\mathcal{W}_\alpha$ and depending on $a_1^*, \dots, a_\nu^*$ as on parameters.

For an arbitrary polynomial $f \in k[a_1, \dots, a_\nu, X_0, \dots, X_n]$ and a point $a^* = (a_1^*, \dots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$, we write $f(a^*, X_0, \dots, X_n) = f(a_1^*, \dots, a_\nu^*, X_0, \dots, X_n)$ and use other similar notation.

Denote by k_{a^*} the field generated over k by the coordinates of the point a^*, i.e., $k_{a^*} = k(a_1^*, \dots, a_\nu^*)$ (if $\nu = 0$, we assume that $k_{a^*} = k$ for $a^* \in \mathbb{A}^\nu(\overline{k})$; recall that $\#\mathbb{A}^\nu(\overline{k}) = 1$ for $\nu = 0$). Thus all the polynomials $f_i(a^*, X_0, \dots, X_n)$ lie in $k_{a^*}[X_0, \dots, X_n]$.

Let $\mathcal{Z}(f_i(a^*, X_0, \dots, X_n),\ 0 \le i \le m-1)$ denote the set of all common zeros of the polynomials under consideration in $\mathbb{P}^n(\overline{k})$. Then $V_{a^*} = \mathcal{Z}(f_i(a^*, X_0, \dots, X_n),\ 0 \le i \le m-1)$. We will also use other similar notation.

Remark 1. In what follows, we assume that $d_{m-1} \ge 1$. Let us show that this involves no loss of generality. Indeed, assume that there are $q \ge 1$ polynomials f_i with $d_i = 0$. Then for each i with $\deg_{X_0,\dots,X_n} f_i = d_i = 0$, it suffices to replace the polynomial f_i by the family of polynomials $\{X_j f_i\}_{0 \le j \le n}$ and m by $m + qn$. After that, for every $a^* \in \mathbb{A}^\nu(\overline{k})$ the newly obtained system (3) is equivalent to the original system (3).

Now we are going to give a precise meaning to the uniformity of algebraic formulas related to (4). Namely, the following properties hold.

(i) For every $\alpha \in A$, the variety $\mathcal{W}_\alpha$ is nonempty. For all α_1, $\alpha_2 \in A$, if $\alpha_1 \ne \alpha_2$ then $\mathcal{W}_{\alpha_1} \cap \mathcal{W}_{\alpha_2} = \varnothing$, i.e., these varieties $\mathcal{W}_\alpha$ are pairwise disjoint; thus we will call them strata, and the union (4) will be called a stratification.

(ii) One can represent $\mathcal{W}_\alpha$ in the form

$$\mathcal{W}_\alpha = \mathcal{W}_\alpha^{(1)} \setminus \bigcup_{2 \le \beta \le \mu_\alpha} \mathcal{W}_\alpha^{(\beta)}$$

where $\mathcal{W}_\alpha^{(\beta)} = \mathcal{Z}(\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)})$, $1 \le \beta \le \mu_\alpha$, is the set of all common zeros of the polynomials $\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)} \in k[a_1, \dots, a_\nu]$ in the affine space $\mathbb{A}^\nu(\overline{k})$ and $m_{\alpha,\beta} \ge 1$ is an integer.

Let $\alpha \in A$ be arbitrary. Let s be an arbitrary integer such that $c' \le s \le c$ (if $c = -1$, then there are no such integers s).

(iii) If $V_{a^*,s} = \varnothing$ for some $a^* \in \mathcal{W}_\alpha$, then $V_{a^*,s} = \varnothing$ for all $a^* \in \mathcal{W}_\alpha$ (if $s \ne n$, then the last implication follows also from (iv)).

If $m-1<n$, then we put $d_i=1$ for $m-1\le i\le n$ (but in this case, the polynomials f_i are not defined for these i). Set

$$D'_{n-s}=d_0d_1\cdot\ldots\cdot d_{n-s-1},\quad 0\le s\le n-1,$$

and $D'_{n-s}=1$ if $s=n$.

Put $\rho_s=0$ if $p=1$, and $\rho_s=\log_p D'_{n-s}$ otherwise.

In what follows, all the constants in $O(\ldots)$ are absolute.

Let $\mathcal{I}_\varkappa$ be a finite subset of $k\setminus\{0\}$ with the number of elements $\#\mathcal{I}_\varkappa=\varkappa+1$. Let s be an integer, $0\le s\le n-1$. Put

$$\mathcal{M}_\varkappa=\Big\{\sum_{0\le i\le n}\gamma^iX_i\,:\,\gamma\in\mathcal{I}_\varkappa\Big\},\quad \mathcal{M}'_{s,\varkappa}=\Big\{\sum_{s+1\le i\le n}\gamma^{i-s-1}X_i\,:\,\gamma\in\mathcal{I}_\varkappa\Big\}. \tag{5}$$

These are finite sets of linear forms with coefficients from k.

Put $\varkappa_{1,s}=2(n-s)D'_{n-s}+s$ and $\varkappa_{2,s}=(n-s)D'_{n-s}(D'_{n-s}-1)/2$. For every s, where $0\le s\le n-1$, set

$$\mathcal{L}_s=\mathcal{M}_{\varkappa_{1,s}},\qquad \mathcal{L}'_s=\mathcal{M}'_{s,\varkappa_{2,s}}.$$

In (iv)–(xii) below, we assume additionally that s is arbitrary such that $c'\le s\le\min\{c,n-1\}$. For every such s there are linear forms $Y_0,\ldots,Y_s\in\mathcal{L}_s$ and $Y_{s+1}\in\mathcal{L}'_s$ (depending on α and s; we will also write $Y_i=Y_{s,i}$ if the dependence on s is important, so $(Y_{s,0},\ldots,Y_{s,s+1})\in\mathcal{L}_s^{s+1}\times\mathcal{L}'_s$) satisfying the following properties.

(iv) For every $a^*\in\mathcal{W}_\alpha$, the intersection $V_{a^*,s}\cap\mathcal{Z}(Y_0,\ldots,Y_s)$ is empty in $\mathbb{P}^n(\overline{k})$.

(v) The linear forms $Y_0,\ldots,Y_{s+1}$ are linearly independent. For every integer r, $0\le r\le\rho_s$, there is a nonzero polynomial $\Phi_{\alpha,s,r}\in k[a_1,\ldots,a_\nu,Y_0,\ldots,Y_{s+1}]$ homogeneous with respect to $Y_0,\ldots,Y_{s+1}$ such that for every $a^*\in\mathcal{W}_\alpha$

$$0\le\deg_{Y_0,\ldots,Y_{s+1}}\Phi_{\alpha,s,r}=\deg_{Y_{s+1}}\Phi_{\alpha,s,r}(a^*,Y_0,\ldots,Y_{s+1})\le D'_{n-s}/p^r,$$

the leading coefficient $\mathrm{lc}_{Y_{s+1}}\Phi_{\alpha,s,r}$ lies in $k[a_1,\ldots,a_\nu]$, and

$$\prod_{0\le r\le\rho_s}\Phi^{1/p^r}_{\alpha,s,r}(a^*,Y_0^{p^r},\ldots,Y_{s+1}^{p^r})$$

is a nonzero polynomial from $\overline{k}[Y_0,\ldots,Y_{s+1}]$ of minimum degree vanishing on the projective algebraic variety $V_{a^*,s}$. Furthermore,

$$\deg V_{a^*,s}=\sum_{0\le r\le\rho_s}\deg_{Y_{s+1}}\Phi_{\alpha,s,r}.$$

Finally, denote by $\Delta_{\alpha,s,r}$ the discriminant of the polynomial $\Phi_{\alpha,s,r}$ with respect to Y_{s+1} (by definition, $\Delta_{\alpha,s,r}=1$ if $\deg_{Y_{s+1}}\Phi_{\alpha,s,r}=0$). Then for every $a^*\in\mathcal{W}_\alpha$, the polynomial $\Delta_{\alpha,s,r}(a^*,Y_0,\ldots,Y_s)$ is nonzero.

Denote by $V_{a^*,s,r}$, $0\le r\le\rho_s$, the union of all components E irreducible over $\overline{k}$ of the algebraic variety $V_{a^*,s}$ such that $\Phi_{\alpha,s,r}(a^*,Y_0^{p^r},\ldots,Y_{s+1}^{p^r})$ vanishes on E. Thus we have $V_{a^*,s}=\bigcup\limits_{0\le r\le\rho_s}V_{a^*,s,r}$, and if $r_1\ne r_2$ then the varieties V_{a^*,s,r_1} and V_{a^*,s,r_2} do not have common irreducible components.

The algebraic variety $V_{a^*,s,r}$ is defined over the field $k_{a^*}^{1/p^r}$.

(vi) Let Z be a new variable. There is a finite (or empty) family of polynomials $H_j\in k[a_1,\ldots,a_\nu,Z]$, $j\in J_{\alpha,s,r}$, satisfying the following properties. The inequalities

$$1\le\deg_Z H_j\le D'_{n-s}/p^r$$

hold. Denote by Δ_j the discriminant of the polynomial H_j with respect to Z. Then $\Delta_j(a^*)\ne0$ for every $a^*\in\mathcal{W}_\alpha$. Denote by Ξ_{j,a^*} the family of roots from $\overline{k}$ of the

separable polynomial $H_j(a^*, Z)$. We assume that the sets of indices $J_{\alpha,s,r}$ are pairwise disjoint.

(vii) There is a family of polynomials $\Phi_j \in k[a_1, \dots, a_\nu, Z, Y_0, \dots, Y_{s+1}]$, $j \in J_{\alpha,s,r}$, and polynomials $\lambda_{\alpha,s,r,0}, \lambda_{\alpha,s,r,1} \in k[a_1, \dots, a_\nu]$ satisfying the following properties. For every $a^* \in \mathcal{W}_\alpha$, the polynomials Φ_j are homogeneous with respect to $Y_0, \dots, Y_{s+1}$, the degrees satisfy the inequalities $\deg_Z \Phi_j < \deg_Z H_j$, the leading coefficient $\mathrm{lc}_{Y_{s+1}} \Phi_j$ lies in $k[a_1, \dots, a_\nu]$, all the polynomials $\Phi_j(a^*, \xi, Y_0, \dots, Y_{s+1})$, $\xi \in \Xi_{j,a^*}$, $j \in J_{\alpha,s,r}$, are irreducible over $\overline{k}$ in the ring $\overline{k}[X_0, \dots, X_n]$ (in particular, they have degree ≥ 1), $\lambda_{\alpha,s,r,0}(a^*) \neq 0$, $\lambda_{\alpha,s,r,1}(a^*) \neq 0$, and

$$\Phi_{\alpha,s,r}(a^*, Y_0, \dots, Y_{s+1}) = \frac{\lambda_{\alpha,s,r,0}(a^*)}{\lambda_{\alpha,s,r,1}(a^*)} \prod_{\substack{j \in J_{\alpha,s,r}, \\ \xi \in \Xi_{j,a^*}}} \Phi_j(a^*, \xi, Y_0, \dots, Y_{s+1}).$$

Hence $1 \leq \deg_{Y_0,\dots,Y_{s+1}} \Phi_j \leq \deg_{Y_0,\dots,Y_{s+1}} \Phi_{\alpha,s,r} \leq D'_{n-s}/p^r$.

(viii) For every $a^* \in \mathcal{W}_\alpha$, for every r, where $0 \leq r \leq \rho_s$, the irreducible components over $\overline{k}$ of the projective algebraic variety $V_{a^*,s,r}$ are in a natural one-to-one correspondence with the pairs (ξ, j) where $\xi \in \Xi_{j,a^*}$, $j \in J_{\alpha,s,r}$. Denote by $W_{j,a^*,\xi}$ the irreducible (over $\overline{k}$) component of the algebraic variety $V_{a^*,s,r}$ corresponding to the pair (ξ, j). We have $\deg W_{j,a^*,\xi} = \deg_{Y_{s+1}} \Phi_j$.

(ix) Let Y and Z be variables, $t_1, \dots, t_s$ be a family of algebraically independent elements over $\overline{k}$, j be a index from $J_{\alpha,s,r}$, and θ be an algebraic element over $\overline{k}(t_1, \dots, t_s)$ such that $\Phi_j(a^*, \xi, 1, t_1^{p^r}, \dots, t_s^{p^r}, \theta^{p^r}) = 0$. Then there are polynomials

$$G_j \in k[a_1, \dots, a_\nu, t_1, \dots, t_s], \quad G_{j,i} \in k[a_1, \dots, a_\nu, Z, t_1, \dots, t_s, Y], \quad 0 \leq i \leq n,$$

satisfying the following properties. The polynomial $G_j(a^*, t_1, \dots, t_s)$ is nonzero for every $a^* \in \mathcal{W}_\alpha$, the inequalities $\deg_Z G_{j,i} < \deg_Z H_j$, $\deg_Y G_{j,i} < \deg_{Y_{s+1}} \Phi_j$ hold, and all degrees $\deg_{t_1,\dots,t_s} G_j$, $\deg_{t_1,\dots,t_s} G_{j,i}$ are bounded from above by $(D'_{n-s}/p^r)^{O(1)}$. Furthermore, there is a $\overline{k}$-isomorphism of fields

$$\overline{k}(W_{j,a^*,\xi}) \to \overline{k}(t_1, \dots, t_s)[\theta]$$

such that $Y_i/Y_0 \mapsto t_i$, $1 \leq i \leq s$, $Y_{s+1}/Y_0 \mapsto \theta$,

$$(X_i/Y_0)^{p^r} \mapsto G_{j,i}(a^*, \xi, t_1^{p^r}, \dots, t_s^{p^r}, \theta^{p^r}) / G_j(a^*, t_1^{p^r}, \dots, t_s^{p^r}), \quad 0 \leq i \leq n.$$

Hence this isomorphism gives a generic point of the algebraic variety $W_{j,a^*,\xi}$. The projective algebraic variety $W_{j,a^*,\xi}$ is defined over the field $k_{a^*}^{1/p^r}[\xi]$ (it is well known that in this case $\xi^{1/p^r} \in k_{a^*}^{1/p^r}[\xi]$).

(x) Moreover, there are polynomials

$$G_{\alpha,s,r} \in k[a_1, \dots, a_\nu, t_1, \dots, t_s], \quad G_{\alpha,s,r,i} \in k[a_1, \dots, a_\nu, t_1, \dots, t_s, Y], \quad 0 \leq i \leq n,$$

satisfying the following properties. Put

$$d_j = \deg_Z H_j, \quad d'_j = \deg_{Y_0,\dots,Y_{s+1}} \Phi_j, \quad d_{\alpha,s,r,i} = \deg_Y G_{\alpha,s,r,i}.$$

For every i, $0 \leq i \leq n$, we have $\deg_Y G_{\alpha,s,r,i} < \deg_{Y_0,\dots,Y_{s+1}} \Phi_{\alpha,s,r}$,

$$\deg_{t_1,\dots,t_s} G_{\alpha,s,r,i} < 2(D'_{n-s})^2, \quad \deg_{t_1,\dots,t_s} G_{\alpha,s,r} < 2(D'_{n-s})^2.$$

Put $\Phi'_j = \Phi_j(a_1, \dots, a_\nu, Z, 1, t_1, \dots, t_s, Y)$. For every $j \in J_{s,r}$, we have

$$(\mathrm{lc}_{Y s+1} \Phi_j)^{\max\{d_{\alpha,s,r,i} - d'_j + 1, 0\}} G_{\alpha,s,r,i} = A'_j \Phi'_j + G'_{j,i},$$

where $A'_j, G'_{j,i} \in k[a_1, \dots, a_\nu, Z, t_1, \dots, t_s, Y]$ and $\deg_Y G'_{j,i} = d'_{j,i} < d'_j$. Furthermore, $(\mathrm{lc}_Z H_j)^{\max\{d'_{j,i} - d_j + 1, 0\}} G'_{j,i} = A_j H_j + G_{j,i}$ where $A_j \in k[a_1, \dots, a_\nu, Z, t_1, \dots, t_s, Y]$. Finally,

$$G_j = (\mathrm{lc}_{Y_{s+1}} \Phi_j)^{\max\{d_{\alpha,s,r,i} - d'_j + 1, 0\}} \cdot (\mathrm{lc}_Z H_j)^{\max\{d'_{j,i} - d_j + 1, 0\}} \cdot G_{\alpha,s,r}.$$

Therefore, if $s = 0$, then by (ix) for every $a^* \in \mathcal{W}_\alpha$, for all $j \in J_{\alpha,0,r_0}$, $\xi \in \Xi_{a^*,j}$, $0 \le r \le \rho_0$,

$$W_{j,a^*,\xi} = \mathcal{Z}(G_{j,i}(a^*, \xi) Y_0^{p^r} - G_j(a^*) X_i^{p^r},\ 0 \le i \le n).$$

If $s = n - 1$, then for every $a^* \in \mathcal{W}_\alpha$, for all $j \in J_{\alpha,n-1,r}$, $\xi \in \Xi_{a^*,j}$, $0 \le r \le \rho_{n-1}$, obviously, $W_{j,a^*,\xi} = \mathcal{Z}(\Phi_j(a^*, \xi, Y_0^{p^r}, \dots, Y_{s+1}^{p^r}))$ and $V_{a^*,s,r} = \mathcal{Z}(\Phi_{\alpha,s,r}(a^*, Y_0^{p^r}, \dots, Y_{s+1}^{p^r}))$.

Let $Y^{(i)}$, $0 \le i \le \varkappa_{2,s}$, be all pairwise distinct linear forms from $\mathcal{L}'_s$. Note that for every $Y^{(i)} \in \mathcal{L}'_s$, the linear forms $Y_0, \dots, Y_s, Y^{(i)}$ are linearly independent over k. Let t be an element algebraically independent over k. One can extend the ground field k to $k(t)$. In (xi) and (xii) below, we assume that $0 \le s \le n - 2$.

(xi) There are polynomials $\Psi_{\alpha,s,r,i_1,i_2} \in k[a_1, \dots, a_\nu, t, Y_0, \dots, Y_s, Z]$, $0 \le i_1 \le \varkappa_{2,s}$, $s + 2 \le i_2 \le n$, homogeneous with respect to $Y_0, \dots, Y_s, Z$ and satisfying the following properties. For every $a^* \in \mathcal{W}_\alpha$, for $0 \le i_1 \le \varkappa_{2,s}$, $s + 2 \le i_2 \le n$, the polynomial $\Psi_{\alpha,s,r,i_1,i_2}(a^*, t, Y_0, \dots, Y_s, Z)$ is nonzero and such that

$$\Psi_{\alpha,s,r,i_1,i_2}(a^*, t^{p^r}, Y_0^{p^r}, \dots, Y_s^{p^r}, (Y^{(i_1)} + tX_{i_2})^{p^r})$$

vanishes on the algebraic variety $V_{a^*,s,r}(\overline{k(t)})$. Furthermore, for all s, r, the variety $V_{a^*,s,r}$ coincides with the set

$$\mathcal{Z}\left(\Psi_{\alpha,s,r,i_1,i_2}\left(a^*, t^{p^r}, Y_0^{p^r}, \dots, Y_s^{p^r}, (Y^{(i_1)} + tX_{i_2})^{p^r}\right), \forall\, i_1, i_2\right) \cap \mathbb{P}^n(\overline{k}). \tag{6}$$

The leading coefficient $\mathrm{lc}_Z \Psi_{\alpha,s,r,i_1,i_2}$ lies in $k[a_1, \dots, a_\nu]$, and for every $a^* \in \mathcal{W}_\alpha$ we have $(\mathrm{lc}_Z \Psi_{\alpha,s,r,i_1,i_2})(a^*) \ne 0$. The degrees satisfy the inequalities

$$\deg_t \Psi_{\alpha,s,r,i_1,i_2} \le \deg_Z \Psi_{\alpha,s,r,i_1,i_2} \le \deg_{Y_{s+1}} \Phi_{\alpha,s,r} \le D'_{n-s}/p^r.$$

Let us write

$$\Psi_{\alpha,s,r,i_1,i_2} = \sum_{0 \le i_3 \le \deg_t \Psi_{\alpha,s,r,i_1,i_2}} \Psi_{\alpha,s,r,i_1,i_2,i_3} t^{i_3}$$

where $\Psi_{\alpha,s,r,i_1,i_2,i_3} \in k[a_1, \dots, a_\nu, Y_0, \dots, Y_s, Y^{(i_1)}, X_{i_2}]$ (note that now the linear forms $Y_0, \dots, Y_s, Y^{(i_1)}, X_{i_2}$ are linearly independent over k). Then (since the set (6) coincides with $V_{a^*,s,r}$) we have

$$\mathcal{Z}\left(\Psi_{\alpha,s,r,i_1,i_2,i_3}\left(a^*, Y_0^{p^r}, \dots, Y_s^{p^r}, (Y^{(i_1)})^{p^r}, X_{i_2}^{p^r}\right), \forall\, i_1, i_2, i_3\right) = V_{a^*,s,r}.$$

Thus we obtain a system of polynomial equations with the set of zeros $V_{a^*,s,r}$. This system consists of at most $(n - s - 1)n(D'_{n-s})^3/(2p^r)$ homogeneous equations of degree at most D'_{n-s}.

(xii) For every $j \in J_{\alpha,s,r}$, $0 \le r \le \rho_s$, there are polynomials

$$\Psi_{j,i_1,i_2} \in k[a_1, \dots, \quad a_\nu, Z, t, Y_0, \dots, Y_s, Z_1],$$

$0 \le i_1 \le \varkappa_{2,s}$, $s + 2 \le i_2 \le n$, homogeneous with respect to $Y_0, \dots, Y_s, Z_1$ and satisfying the following properties. The inequalities $\deg_Z \Psi_{j,i_1,i_2} < \deg_Z H_j$ hold. For every $a^* \in \mathcal{W}_\alpha$, for every $\xi \in \Xi_{a^*,j}$, for $0 \le i_1 \le \varkappa_{2,s}$, $s + 2 \le i_2 \le n$, the polynomial $\Psi_{j,i_1,i_2}(a^*, \xi, t, Y_0, \dots, Y_s, Z)$ is nonzero and such that

$$\Psi_{j,i_1,i_2}(a^*, \xi, t^{p^r}, Y_0^{p^r}, \dots, Y_s^{p^r}, (Y^{(i_1)} + tX_{i_2})^{p^r})$$

vanishes on the algebraic variety $W_{j,a^*,\xi}(\overline{k(t)})$. Furthermore, the variety $W_{j,a^*,\xi}$ coincides with the set

$$\mathcal{Z}\left(\Psi_{j,i_1,i_2}\left(a^*,\xi,t^{p^r},Y_0^{p^r},\dots,Y_s^{p^r},(Y^{(i_1)}+tX_{i_2})^{p^r}\right),\forall\, i_1,i_2\right)\cap\mathbb{P}^n(\overline{k}). \tag{7}$$

The leading coefficient $\mathrm{lc}_Z\Psi_{j,i_1,i_2}$ lies in $k[a_1,\dots,a_\nu]$, and for every $a^*\in\mathcal{W}_\alpha$ we have $(\mathrm{lc}_Z\Psi_{j,i_1,i_2})(a^*)\neq 0$. The inequalities

$$\deg_t\Psi_{j,i_1,i_2}\le\deg_Z\Psi_{j,i_1,i_2}\le\deg_{Y_{s+1}}\Phi_j\le D'_{n-s}/p^r$$

hold.

Let us write $\Psi_{j,i_1,i_2}=\sum\limits_{0\le i_3\le\deg_t\Psi_{j,i_1,i_2}}\Psi_{j,i_1,i_2,i_3}t^{i_3}$ where

$$\Psi_{j,i_1,i_2,i_3}\in k[a_1,\dots,a_\nu,Z,Y_0,\dots,Y_s,Y^{(i_1)},X_{i_2}].$$

Then (since the set (7) coincides with $W_{j,a^*,\xi}$) we have

$$\mathcal{Z}\left(\Psi_{j,i_1,i_2,i_3}\left(a^*,\xi,Y_0^{p^r},\dots,Y_s^{p^r},(Y^{(i_1)})^{p^r},X_{i_2}^{p^r}\right),\forall\, i_1,i_2,i_3\right)=W_{j,a^*,\xi}.$$

Thus we obtain a system of polynomial equations with the set of zeroes $W_{j,a^*,\xi}$. This system consists of at most $(n-s-1)n(D'_{n-s})^3/(2p^r)$ homogeneous equations of degree at most D'_{n-s}.

Let $a^*\in\mathcal{W}_\alpha$. By definition, put $c_\alpha=\max\{\dim V_{a^*}^{(c',c)},c'-1\}$. Hence c_α depends only on α and does not depend on the choice of the point a^*.

(xiii) There are an integer c'_α and homogeneous polynomials $q_{\alpha,i,i_1}\in k[X_0,\dots,X_n]$, for $1\le i\le n-c'_\alpha$, $0\le i_1\le m-1$, satisfying the following properties. The inequalities $c'-1\le c'_\alpha\le c_\alpha$ hold. Put

$$h_{\alpha,i}=\sum_{0\le i_1\le m-1}q_{\alpha,i,i_1}f_{i_1},\quad 1\le i\le n-c'_\alpha.$$

Set $d^{(i)}=\deg_{X_0,\dots,X_n}h_{\alpha,i}$ for all i. Then $d^{(i)}\le d_{i-1}$, and for all i_1 we have

$$\deg_{X_0,\dots,X_n}q_{\alpha,i,i_1}=d^{(i)}-d_{i_1}$$

provided that $q_{\alpha,i,i_1}\neq 0$.

For every $a^*\in\mathcal{W}_\alpha$, put $h_{a^*,i}=\sum\limits_{0\le i_1\le m-1}q_{\alpha,i,i_1}f_{i_1}(a^*,X_0,\dots,X_n)$. Then

$$\mathcal{Z}(h_{a^*,1},\dots,h_{a^*,n-c'_\alpha})=V_{a^*}^{(c',c)}\cup E_{a^*,c'}$$

where $E_{a^*,c'}$ is a projective algebraic variety with $\dim E_{a^*,c'}\le c'-1$. Furthermore, for every integer c'' such that $c'_\alpha<c''\le c$,

$$\mathcal{Z}(h_{a^*,1},\dots,h_{a^*,n-c''})=V_{a^*}^{(c'',c)}\cup E_{a^*,c''},$$

where $E_{a^*,c''}$ is a projective algebraic variety such that $\dim E_{a^*,c''}=c''$ and each irreducible (over $\overline{k}$) component of $E_{a^*,c''}$ is not an irreducible component of V_{a^*}.

Note that if $E_{a^*,c'}=\varnothing$, then $V_{a^*}^{(c',c)}=V_{a^*}$. Furthermore, one can easily deduce from (xiii) that $h_{a^*,i}\neq 0$ for every i, $1\le i\le c'_\alpha$, and every $a^*\in\mathcal{W}_\alpha$.

For every integer s such that $0\le s\le n-1$, put

$$D_{n-s}=\binom{d_0+\ldots+d_{n-s-1}+1}{n-s}$$

(this is a binomial coefficient). If $s=n$, put $D_{n-s}=1$. Also set $D_{n+1}=D_n$.

The (bitwise) length of an integer $z \in \mathbb{Z}$ is defined by the formula $\mathrm{l}(z) = 1 + [\log_2(|z| + 1)]$ (here $[\ldots]$ stands for the integral part of a real number). If $f_i \in \mathbb{Z}[a_1, \ldots, a_\nu, X_0, \ldots, X_n]$, then, by definition, the length of integer coefficients of the polynomial f_i is equal to

$$\mathrm{l}(f_i) = \max_{\substack{i_1,\ldots,i_\nu,\\ j_0,\ldots,j_n}} \mathrm{l}(f_{i,i_1,\ldots,i_\nu,j_0,\ldots,j_n}),$$

see (2). The lengths of integer coefficients of other polynomials with integer coefficients are defined in a similar way.

In the statements of Theorems 1 and 2 below, we assume that the field k has sufficiently many elements. More precisely, it suffices that $\#k \geq D_{n-c'}^C$ for some absolute constant $C > 0$ (it can be easily computed if necessary).

Now we are able to state our main result.

Theorem 1. *Let polynomials $f_0, \ldots, f_{m-1} \in k[a_1, \ldots, a_\nu, X_1, \ldots, X_n]$, integers c, c', and a Zariski-open set $\mathcal{U}_c$ be as above. Then there is a stratification* (4) *satisfying properties* (i)–(xiii) *and such that*

(a) *the number of elements $\#A$ and all the integers μ_α, $m_{\alpha,\beta}$ are bounded from above by $(d')^\nu D_{n-c'}^{O(\nu)}$ with an absolute constant in $O(\nu)$;*

(b) *the degrees in $a_1, \ldots, a_\nu$ of all polynomials $\psi_{\alpha,1}^{(\beta)}, \ldots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)}$ are bounded from above by $d' D_{n-c'}^{O(1)}$ with an absolute constant in $O(1)$;*

(c) *for every s such that $c' \leq s \leq \min\{c, n-1\}$, the degrees in $a_1, \ldots, a_\nu$ of all polynomials $\Phi_{\alpha,s,r}$, H_j, Φ_j, $\lambda_{\alpha,s,r,0}, \lambda_{\alpha,s,r,1}$, G_j, $G_{j,i}$, $G_{\alpha,s,r}$, $G_{\alpha,s,r,i}$, $\Psi_{\alpha,s,r,i_1,i_2}$, Ψ_{j,i_1,i_2}, $j \in J_{\alpha,s,r}$, $0 \leq r \leq \rho_s$, are bounded from above by $d' D_{n-s}^{O(1)}$ with an absolute constant in $O(1)$.*

Consider also the following property.

(ł) *The field k is $\mathbb{Q}$, and in* (2)*, for $0 \leq i \leq m-1$, we have*

$$f_i \in \mathbb{Z}[a_1, \ldots, a_\nu, X_0, \ldots, X_n]$$

and $\mathrm{l}(f_i) \leq M$ for some real number $M \geq 1$.

Further, for every $\varkappa \geq 0$ we take $\mathcal{I}_\varkappa = \{1, 2, \ldots, \varkappa + 1\}$.

Then, additionally,

(d) *under condition* (ł)*, the coefficients from k of all polynomials from* (b) *and* (c) *actually belong to $\mathbb{Z}$. The lengths of integer coefficients of all polynomials from* (b) *are bounded from above by*

$$(M + c^2 + \nu \log_2 d') D_{n-c'}^{O(1)} \tag{8}$$

with an absolute constant in $O(1)$. The lengths of integer coefficients of all polynomials from (c) *are bounded from above by*

$$(M + c^2 + \nu \log_2 d') D_{n-s}^{O(1)} \tag{9}$$

with an absolute constant in $O(1)$.

Under condition (ł), we will also give good estimates for all lengths $\mathrm{l}(h_{\alpha,i})$.

Note that if $c = -1$, only the stratification (4) itself and the polynomials $h_{\alpha,1}, \ldots, h_{\alpha,n+1}$ (from (xiii)) appear in the statement of Theorem 1, there are no other objects in this case.

Let $c = n$. Then $V_{a^*,n} = \mathbb{P}^n(\overline{k})$ for some $a^* \in \mathcal{W}_\alpha$ if and only if $c_\alpha = c'_\alpha = n$ (since $h_{a^*,i} \neq 0$ for $1 \leq i \leq n - c'_\alpha$, see (xiii)), i.e., if and only if no polynomials $h_{\alpha,i}$ correspond to α.

Let $c' \leq s \leq \min\{c, n-1\}$. Then $V_{a^*,s} = \varnothing$ if and only if $\Phi_{\alpha,s,r} \in k[a_1, \ldots, a_\nu]$ for $0 \leq r \leq \rho_s$, i.e., if and only if $J_{s,r} = \varnothing$ for $0 \leq r \leq \rho_s$.

Note also that one can write A as a disjoint union $A = \bigcup_{c'-1 \le i \le c} A_i$ such that for every $\alpha \in A_i$, for every $a^* \in \mathcal{W}_\alpha$, we have $\dim V_{a^*} = i$ if $c' \le i \le c$, and $\dim V_{a^*} \le i$ if $i = c' - 1$.

For the problem under consideration, all previously known bounds on the degrees were double exponential, cf. [1, 9].

We mention again that the algorithm from [2, Chap. 2] can be viewed as an analog of the construction of the present paper for $\nu = 0$ (in this case, one can omit a^* in the notation).

Remark 2. We need to state also a modified version of Theorem 1 for the case of a covering instead of a stratification, i.e., when condition (i) does not necessarily hold.

Namely, *if in the statement of Theorem* 1 *one replaces* "(i)–(xiii)" *by* "(ii)–(xiii)"*, then one can claim additionally in* (a) *that* $\mu_\alpha = 2$ *for every* $\alpha \in A$.

A similar remark is true for Theorem 1 of [6], see the introduction of [6]. It is important in the present paper.

In the next Theorem 2, we make Theorem 1 effective, in the sense that we suggest an algorithm for constructing a stratification (4) (and also a corresponding covering, see Remark 2) and all related objects in time subexponential in the size of the input data. But first we need to give explicitly the field k.

We assume that the field k is finitely generated over the subfield k_0 where $k_0 = \mathbb{Q}$ if $p = 1$ and $k_0 = \mathbb{F}_{p^\epsilon}$ is a finite field of order p^ϵ if $p > 1$. In the latter case, ϵ is a positive integer and the field $\mathbb{F}_{p^\epsilon}$ is given by a basis with a multiplication table over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Set $k_1 = \mathbb{Z}$ if $p = 1$ and $k_1 = k_0$ if $p > 1$. If $\mathrm{char}(k_0) = p > 1$ and $z \in k_0$, then, by definition, the length of z is $\mathrm{l}(z) = \epsilon(1 + [\log_2(p-1)])$.

We assume that $k = k_0(\tau_1, \dots, \tau_l)[\tau_{l+1}]$ where l is a nonnegative integer and $\tau_1, \dots, \tau_l$ are algebraically independent elements over the field k_0. Furthermore, there is a nonzero polynomial $\varphi \in k_1[\tau_1, \dots, \tau_l, Z]$ such that $\deg_Z \varphi \ge 1$, $\mathrm{lc}_Z \varphi = 1$, the polynomial φ is irreducible in the ring $k_0(\tau_1, \dots, \tau_l)[Z]$, and $\varphi(\tau_1, \dots, \tau_{l+1}) = 0$. We assume that $\deg_{\tau_1,\dots,\tau_l,Z} \varphi < d''$ for some integer $d'' \ge 2$. If $\mathrm{char}(k) = 0$, then, additionally, $\mathrm{l}(\varphi) \le M_1$ where $M_1 \ge 1$. If $\mathrm{char}(k) > 0$, put $M_1 = \epsilon(1 + [\log_2(p-1)])$.

If $\mathrm{char}(k) = 0$, then for any polynomial g with integer coefficients, the length of integer coefficients (or of coefficients from k_1, or just the length of coefficients if this will not lead to an ambiguity) of g is defined to be the maximum of the lengths of integer coefficients of g.

If $\mathrm{char}(k) > 0$, then for any polynomial g with coefficients in k_0, the length of coefficients from k_1 (or just the length of coefficients if this will not lead to an ambiguity) of g is defined by the formula $\mathrm{l}(g) = \epsilon(1 + [\log_2(p-1)])$.

Let $z \in k_0(\tau_1, \dots, \tau_l)[\tau_{l+1}]$ be an arbitrary element. Then we represent it as

$$z = (1/z^{(0)}) \sum_{0 \le i < \deg_Z \varphi} z_i \tau_{l+1}^i$$

where $z^{(0)}, z_i \in k_1[\tau_1, \dots, \tau_l]$, $z^{(0)} \ne 0$, and the greatest common divisor of all elements $z^{(0)}, z_0, \dots, z_{\deg_Z \varphi - 1}$ is 1 in the ring $k_1[\tau_1, \dots, \tau_l]$. In the case where $\mathrm{char}(k) = p > 0$, the element $z^{(0)}$ is uniquely defined up to a nonzero factor from k_0. If $\mathrm{char}(k) = 0$, then $z^{(0)}$ is uniquely defined up to a factor ± 1. In any case, if we fix $z^{(0)}$ then all z_i are uniquely defined. To fix $z^{(0)}$, we will assume that the iterated leading coefficient satisfies the condition

$$\mathrm{lc}_{\tau_1} \mathrm{lc}_{\tau_2} \dots \mathrm{lc}_{\tau_l}(z^{(0)}) = \begin{cases} 1 & \text{if } \mathrm{char}(k) = p > 0, \\ > 0 & \text{if } \mathrm{char}(k) = 0. \end{cases}$$

We define the degree $\deg_{\tau_1,\dots,\tau_l} z = \max\limits_{0 \le i < \deg_Z \varphi} \{\deg_{\tau_1,\dots,\tau_l} z^{(0)}, \deg_{\tau_1,\dots,\tau_l} z_i\}$ and the length of coefficients $\mathrm{l}(z) = \max\limits_{0 \le i < \deg_Z \varphi} \{\mathrm{l}(z^{(0)}), \mathrm{l}(z_i)\}$.

By definition, the degree $\deg_{\tau_1,\ldots,\tau_l}(f_i)$ of the polynomial f_i is the maximum of

$$\deg_{\tau_1,\ldots,\tau_l}(f_{i,i_1\ldots,i_\nu,\,j_0,\ldots,j_n})$$

over all indices $i_1\ldots,i_\nu$, $j_0,\ldots,j_n$. The degrees in $\tau_1,\ldots,\tau_l$ of other polynomials with coefficients in k are defined in a similar way.

Let us return to the case of arbitrary characteristic. In this paper, we will assume that $f_{i,i_1\ldots,i_\nu,j_0,\ldots,j_n} \in k_1[\tau_1,\ldots,\tau_{l+1}]$ for all $i,i_1,\ldots,i_\nu,\,j_0,\ldots,j_n$.

We assume that for $0 \le i \le m-1$, we have $\deg_{\tau_1,\ldots,\tau_l} f_i < d'''$ for some integer $d''' \ge 2$ and $\mathrm{l}(f_i) \le M_2$ where $M_2 \ge 1$. Thus we can take $M_2 = \epsilon(1+[\log_2(p-1)])$ if $\mathrm{char}(k) > 0$.

In [2, 3], in the case of nonzero characteristic, the role of the field k_0 is played by a finite field H. Then, in order to apply the algorithms from [2, 3] for solving systems of polynomial equations, the field H must have sufficiently many elements (for example, we assume that $Z_1,\ldots,Z_{n-m+2} \in H[X_0,\ldots,X_n]$, see the statement of the main theorem of Chap. II in [2] and Theorem 1 in [3]). Thus we extend the finite field H if necessary, see Remark 1 in [3]. Actually, the estimates on the lengths of coefficients from H (or $\widetilde{H}$ in the notation of [3]) give bounds on the number of elements of the extended field H, although we do not emphasize this in [2, 3] (since for the number of elements of H, even better bounds can be obtained in nonzero characteristic).

In the last two papers, we obtain systems of polynomial equations giving the irreducible components of the variety of solutions and generic points of these irreducible components. In [2], we also discuss how to return from these systems and generic points involving the extended field H to those with the original field H if $l > 0$. Note that in the case $l = 0$, there is no such reduction for systems of polynomial equations giving the irreducible components: we need to extend H (if the number of elements of H is small) to obtain such systems of equations with the required bound on their size, see the remark at the end of [2].

By Remark 1 of [3], if $l > 0$, then, alternatively, one can choose linear forms $Z_1,\ldots,Z_{n-m+2}$ with coefficients in $H[T_1,\ldots,T_l]$ (in [3], the elements $T_1,\ldots,T_l$ play the role of $\tau_1,\ldots,\tau_l$) and do not extend the field H. But in [2, 3] we do not give explicit estimates on the degrees in $T_1,\ldots,T_l$ of all objects (it is especially interesting for systems of polynomial equations giving the irreducible components) in this case. Of course, the running time of the algorithms from [2, 3] remains the same for this alternative choice of linear forms.

In this paper, to take into account all cases, we use a slightly more general approach to representing elements from the ground field k.

Assume that $\mathrm{char}(k) > 0$. Then if $l > 0$, put

$$\epsilon(\varkappa) = \min\left\{b \in \mathbb{Z} : \binom{b+l}{b}\epsilon\log_2 p \ge \log_2(\varkappa+1)\ \&\ b \ge 0\right\},\quad 0 \le \varkappa \in \mathbb{Z}. \tag{10}$$

In this case, according to (10), we choose and fix $\mathcal{I}_\varkappa$ to be a subset of the set of polynomials from $k_0[\tau_1,\ldots,\tau_l]$ of degree at most $\epsilon(\varkappa)$.

For every s, $0 \le s \le n-1$, set $\epsilon_s = 0$ if $\epsilon(\varkappa_{1,s}) = 0$, and $\epsilon_s = 1$ if $\epsilon(\varkappa_{1,s}) \ge 1$.

If $l = 0$ or $\mathrm{char}(k) = 0$, then set $\epsilon_s = 0$ for all s.

Recall that we assume that the field k has sufficiently many elements, see above. Hence if $l = 0$, then the field $k_0[\tau_1]$ has sufficiently many elements.

Put

$$D = \max_{c'-1 \le s \le c}\{D_{n-s}^{s+\nu+l+2}\}.$$

Thus D depends on c, c'. Obviously, $D \le d^{(n+1)(c+\nu+l+2)}$ (this estimate does not depend on c').

Theorem 2. *Under the conditions described above, one can construct a stratification* (4) *satisfying properties* (i)–(xiii) (*respectively, a covering* (4) *satisfying properties* (ii)–(xiii)) *and*

all the related objects from (iv)–(xiii)*, see assertions* (a)–(c) *of Theorem* 1 (*respectively, of the modified version of Theorem* 1*, see Remark* 2)*. Furthermore, the following assertions hold.*

(a) *All polynomials* $\psi_{\alpha,1}^{(\beta)},\dots,\psi_{\alpha,m_{\alpha,\beta}}^{(\beta)}$ *from assertion* (b) *of Theorem* 1 (*respectively, of the modified version of Theorem* 1) *belong to* $k_1[\tau_1,\dots,\tau_{l+1},a_1,\ \dots,a_\nu]$*. The degrees in* $\tau_1,\dots,\tau_l$ *of all these polynomials are bounded from above by*

$$(d'''+c^2\epsilon_{c'}+(d'')^2)D_{n-c'}^{O(1)}. \tag{11}$$

If $\mathrm{char}(k)=0$*, then the lengths of integer coefficients of all these polynomials are bounded from above by*

$$(M_1+M_2d''+c^2+\nu\log_2 d'+(l+1)\log_2(d''d'''))D_{n-c'}^{O(1)}. \tag{12}$$

(b) *For every* s*,* $c'\le s\le\min\{c,n-1\}$*, the coefficients from* k *of all polynomials from assertion* (c) *of Theorem* 1 (*respectively, of the modified version of Theorem* 1) *actually belong to* $k[\tau_1,\dots,\tau_{l+1}]$*. The degrees in* $\tau_1,\dots,\tau_l$ *of all these polynomials are bounded from above by*

$$(d'''+c^2\epsilon_s+(d'')^2)D_{n-s}^{O(1)}. \tag{13}$$

If $\mathrm{char}(k)=0$*, then the lengths of integer coefficients of all these polynomials are bounded from above by*

$$(M_1+M_2d''+c^2+\nu\log_2 d'+(l+1)\log_2(d''d'''))D_{n-s}^{O(1)}. \tag{14}$$

(c) *The running time of this algorithm for constructing a stratification* (4) *(respectively, a covering* (4)*) is polynomial in* D*,* $(d')^\nu$*,* $(d'')^{l+1}$*,* $(d''')^{l+1}$*,* M_1*,* M_2*, and* m*.*

Remark 3. In the case of zero characteristic, one can modify the construction of a stratification (4) (respectively, a covering (4)) as follows. The linear forms $Y_{s,i}$, $0\le i\le s+1$, can be replaced by some linear forms $Y_{\alpha,s,i}\in\mathbb{Z}[X_0,\dots,X_n]$, with lengths of integer coefficients bounded from above by $O(\log_2 D_{n-s})$ for $0\le i\le s+1$ (now, the condition $(Y_{\alpha,s,0},\dots,Y_{\alpha,s,s+1})\in\mathcal{L}_s^{s+1}\times\mathcal{L}_s'$ does not necessarily hold).

In the case of nonzero characteristic and $l>0$, the linear forms $Y_{s,i}$, $0\le i\le s+1$, can be replaced by some linear forms $Y_{\alpha,s,i}\in k_0[\tau_1,\dots,\tau_l][X_0,\dots,X_n]$ (they are linear forms in $X_0,\dots,X_n$) with degrees in $\tau_1,\dots,\tau_l$ at most $\epsilon(\varkappa)$ where $\varkappa$ is bounded from above by $O(\log_2 D_{n-s})$ for $0\le i\le s+1$.

Then for the ground field of arbitrary characteristic, one can also replace c^2 by c in (8), (9), (11)–(14), and all the assertions of Theorems 1 and 2 remain true. But we will not prove these new versions of Theorems 1 and 2 in the present paper (we leave this to an interested reader; this is not very difficult).

Note also that if $n-c>C_1\log_2 n$ for an absolute constant $C_1>0$, then, obviously, one can omit $c^2, c^2\epsilon_{c'}, c^2\epsilon_s$ in (8), (9), (11)–(14).

Remark 4. A small correction to [6]. In this paper, we consider a ground field k with at least $2d^2+1$ elements. But, in fact, for the construction described in [6], the field k must contain at least d^{C_2} elements for an absolute constant $C_2>0$. On the other hand, one can remove all restrictions on the number of elements $\#k$ in [6], replacing there the field k by $k(t)$ where t is a transcendental element over k (this requires only minor modifications of the construction described in [6]).

1. Solving linear systems with parametric coefficients

It is known that one can apply the Gaussian elimination algorithm for solving linear systems in such a way that at each step, all the entries of the matrix being transformed are quotients of some minors of the original extended matrix of the linear system under consideration. This gives an algorithm corresponding to a computation forest for solving linear systems with good estimates on the degrees in the parameters.

Still, here we describe a modification of this algorithm in a form convenient for our purposes. Consider a linear system

$$\sum_{1\le j\le m} a_{i,j}X_j = a_{i,m+1}, \quad 1\le i\le n, \tag{15}$$

where $a_{i,j}\in\overline{k}$. Denote by A the extended matrix $(a_{i,j})_{1\le i\le n,\,1\le j\le m+1}$ of this linear system.

We will use recursion on r, where $0\le r\le \min\{n,m\}-1$.

(**) Assume that indices $1\le i_1<\ldots<i_r\le n$, $1\le j_1<\ldots<j_r\le m+1$ are constructed and $\det((a_{i_\alpha,j_\beta})_{1\le\alpha,\beta\le r})\ne 0$.

Our aim is to construct i_{r+1}, j_{r+1} such that property (**) is fulfilled for $r+1$ in place of r or to establish that there is no such pair i_{r+1}, j_{r+1}. For convenience, we may assume without loss of generality (only in the description of the recursion step) that $i_\alpha=\alpha$, $j_\beta=\beta$ for $1\le\alpha,\beta\le r$.

Denote by $\widetilde{A}_r$ the adjoint matrix to $A_r=(a_{\alpha,\beta})_{1\le\alpha,\beta\le r}$. Put $\delta_r=\det(A_r)\ne 0$. Let E_w be the identity matrix of order w where $w\ge 1$. Put

$$G'_r=\begin{pmatrix}\widetilde{A}_r, & 0\\ 0, & \delta_r E_{n-r}\end{pmatrix},\quad A'_r=G'_rA=\begin{pmatrix}\delta_r E_r, & B_r\\ \delta_r C_r, & \delta_r D_r\end{pmatrix},$$

$$G_r=\begin{pmatrix}\widetilde{A}_r, & 0\\ -C_r\widetilde{A}_r, & \delta_r E_{n-r}\end{pmatrix},\quad A''_r=G_rA=\begin{pmatrix}\delta_r E_r, & B_r\\ 0, & F_r\end{pmatrix}.$$

Here B_r, C_r, D_r, F_r are uniquely defined matrices with entries in k. Note that all entries of the matrix F_r are (up to a sign) some minors of order $r+1$ of the matrix A.

Now, if $F_r=0$, then there does not exist a required pair i_{r+1}, j_{r+1}. In this case, put $\rho=r$, $G=G_\rho$, $A''=A''_\rho$. We have $\rho=\mathrm{rank}(A)$.

If

$$F_r=(f_{r,i,j})_{r+1\le i\le n,\,r+1\le j\le m+1}\ne 0,$$

then put $j_{r+1}=\min\{j\,:\,\exists i\,(f_{r,i,j}\ne 0)\}$, $i_{r+1}=\min\{i\,:\,f_{r,i,j_{r+1}}\ne 0\}$, and $J_r=\{(i,j)\,:\,((r+1\le j<j_{r+1})\&(r+1\le i\le n))\vee((j=j_{r+1})\&(r+1\le i<i_{r+1}))\}$. Then $f_{r,i,j}=0$ for all $(i,j)\in J_r$.

Thus, one can eventually transform the matrix A to the canonical trapezoidal form A'' (up to a permutation of rows and columns of the matrix A'') with $F_\rho=0$, applying a nondegenerate transformation of rows of A. This transformation is the multiplication of A by the matrix $G=(g_{i,j})_{1\le i,j\le n}$ from the left. Therefore, one can construct a fundamental family of solutions of the linear system (15) (or to establish that this system have no solutions). Note also that the indices $j_1,\ldots,j_\rho$ are the smallest possible such that property (**) holds. This follows immediately from the described recursive construction.

Now we change the notation. In what follows, we will assume that

$$a=\{a_{i,j}\}_{1\le i\le n,\,1\le j\le m+1}$$

is a family of algebraically independent parameters over the field k. Let the affine space $\overline{k}^{(m+1)n}$ have the coordinate functions from the family a. We will denote by $a^*=\{a^*_{i,j}\}_{1\le i\le n,\,1\le j\le m+1}$ an element of $\overline{k}^{(m+1)n}$. Denote by $\mathfrak{A}$ the ring of polynomials over k with respect to all variables

from the family a. For every $\psi \in \mathfrak{A}$, we will denote by $\deg_a \psi$ the degree of ψ with respect to all variables from the family a. Now, all the matrices $A, A_r, G'_r, A'_r, G_r, A''_r, B_r, C_r, D_r, G$ introduced above have entries in $\mathfrak{A}$, all the elements δ_r, $g_{i,j}$ are polynomials from $\mathfrak{A}$. Denote by $\delta'_1, \ldots, \delta'_\mu$ all pairwise distinct elements of the family $\{f_{r,i,j}\}$, $(i,j) \in J_r$, $1 \le r \le \rho$. Then each δ'_i is a minor of the matrix A (up to a sign). We will write $G(a^*) = G|_{a=a^*} = (g_{i,j}(a^*))_{1 \le i,j \le n}$ and use other similar notation.

We have proved the following lemma.

Lemma 1. *If $k = \overline{k}$, then the described construction defines a function*

$$\bigcup_{n,m \ge 1} \overline{k}^{(m+1)n} \to \bigcup_{n \ge 1} \overline{k}^{n^2},$$

$$a^* \mapsto G(a^*) \quad \text{if and only if} \quad a^* \in \mathcal{Z}(\delta'_1, \ldots, \delta'_\mu) \setminus \mathcal{Z}(\delta_1 \cdot \ldots \cdot \delta_\rho).$$

This function is an algorithm corresponding to a computation forest $\{T_{m,n}\}_{m,n \ge 1}$. Each tree $T_{m,n}$ is a computation tree over k of level at most $\min\{m+1, n\}$ with the input parameters from the family a. For every leaf $v \in L(T_{m,n})$, the output corresponding to v is a matrix G with entries in $\mathfrak{A}$ such that $\deg_a g_{i,j} \le \min\{m+1, n\} - 1$ for all i, j. The quasiprojective algebraic variety $\mathcal{W}_v \subset \overline{k}^{(m+1)n}$ corresponding to the leaf v has the form

$$\mathcal{W}_v = \mathcal{Z}(\delta'_1, \ldots, \delta'_\mu) \setminus \mathcal{Z}(\delta_1 \cdot \ldots \cdot \delta_\rho),$$

where $\rho = \mathrm{rank} A(a^*)$. Besides, the indices $1 \le i_1 < \ldots < i_\rho \le n$, $1 \le j_1 < \ldots < j_\rho \le m+1$ correspond to the leaf v, and $\mathrm{rank}(A_r(a^*)) = \rho$. For every $a^* \in \mathcal{W}_v$, the matrix $G(a^*)A(a^*)$ has the canonical trapezoidal form (see above) up to a permutation of rows and columns.

Now, we would like to deduce some consequences from [8]. They are closely related to solving linear systems. But first we introduce some notation. Let K be an arbitrary field. We will denote by $M_{n,m}(K)$ the set of all matrices with entries in K with n rows and m columns.

Lemma 2. *Let k, K be fields and $K \supset k$. Let $m, n, r \ge 1$ be integers such that $r \le \min\{m, n\}$. Assume that the field k contains at least $\min\{(m-r)r, (n-r)r\} + 1$ elements. Then there are matrices $B_i = (b_{i,\alpha,\beta})_{1 \le \alpha \le r,\, 1 \le \beta \le n} \in M_{r,n}(k)$, $0 \le i \le (n-r)r$, and $C_j = (c_{j,\alpha,\beta})_{1 \le \alpha \le m,\, 1 \le \beta \le r} \in M_{m,r}(k)$, $0 \le j \le (m-r)r$, satisfying the following property.*

Let $A = (a_{i,j})_{1 \le i \le n, 1 \le j \le m} \in M_{n,m}(K)$ be an arbitrary matrix. Then $\mathrm{rank}(A) \ge r$ if and only if there are indices i and j, where $0 \le i \le (n-r)r$ and $0 \le j \le (m-r)r$, such that $\det(B_i A C_j) \ne 0$.

Or, equivalently, all minors of order r of the matrix A are zeros if and only if

$$\det(B_i A C_j) = 0$$

for all i, j.

Proof. In [8], a family of matrices $D_j \in M_{m-r,m}(k)$, $0 \le j \le (m-r)r$, is constructed satisfying the following property.

- For every matrix $Q \in M_{r,m}(K)$ with $\mathrm{rank}(Q) = r$ there is j, $0 \le j \le (m-r)r$, such that $\det \begin{pmatrix} Q \\ D_j \end{pmatrix} \ne 0$.

Let us construct a matrix $D'_j \in M_{r,m}(k)$ such that $\delta_j = \det \begin{pmatrix} D'_j \\ D_j \end{pmatrix} \ne 0$. Denote by $\widetilde{D}_j$ the adjoint matrix to the square matrix $\begin{pmatrix} D'_j \\ D_j \end{pmatrix}$. Let us represent it in the form $\widetilde{D}_j = (C_j, C'_j)$ where $C_j \in M_{m,r}(k)$, $C'_j \in M_{m,m-r}(k)$. Then $\begin{pmatrix} Q \\ D_j \end{pmatrix} \widetilde{D}_j = \begin{pmatrix} Q_1, & Q_2 \\ 0, & \delta_j E_{m-r} \end{pmatrix}$ for some

matrices Q_1, Q_2. Hence $Q_1 = QC_j$ and $\det(QC_j) \neq 0$. We will also write $C_j = C_j^{(r,m)}$, $0 \leq j \leq (m-r)r$.

Hence $\operatorname{rank}(A) \geq r$ if and only if there is j, $0 \leq j \leq r(m-r)$, such that $\operatorname{rank}(AC_j) = r$. Denote by $(AC_j)^t$ the transpose of the matrix AC_j. Then, by what is proved above (with n in place of m), there is i, $0 \leq i \leq r(n-r)$, such that $\det((AC_j)^t C_i^{(r,n)}) \neq 0$. Hence one can take $B_i = (C_i^{(r,n)})^t$ for $0 \leq i \leq r(n-r)$. The lemma is proved. □

Remark 5. One can use Lemma 2 in Sec. 3 of [6]. Namely, there we mentioned the following: *"Applying a result of* [8]*, one can replace the minors* Δ_i *by their linear combinations and in what follows assume without loss of generality that* $m_3 = d^{O(1)}$*."*

These minors Δ_i are from formula (20) of [6]. Actually, to get $m_3 = d^{O(1)}$, one should apply Lemma 2 three times: first to $\Delta_1, \ldots, \Delta_{m_1}$, then to $\Delta_{m_1+1}, \ldots, \Delta_{m_2}$, and, finally, to $\Delta_{m_2+1}, \ldots, \Delta_{m_3}$.

After that, one can simplify the construction of $\psi^{(1)}$ and $\psi^{(2)}$. Namely, one can put

$$\psi^{(1)} = \mathrm{G\,C\,D}_{Y_1,X,v_3,\ldots,v_n}\Big(\sum_{1\leq i\leq m_1} Y_1^i \widetilde{\Delta}_i, f(X,0)\Big) \in k[v][X], \tag{16}$$

$$\psi^{(2)} = \mathrm{G\,C\,D}_{Y_2,Y_3,X,v_3,\ldots,v_n}\Big(\psi^{(1)}, \sum_{\substack{m_1<i_2\leq m_2,\\ m_2<i_3\leq m_3}} Y_2^{i_2} Y_3^{i_3} \widetilde{\Delta}_{i_2} \widetilde{\Delta}_{i_3}\Big) \in k[v][X]. \tag{17}$$

One should not introduce the function $\varkappa$ in Sec. 3 of [6]. Of course, the number of minors Δ_i linearly independent over $\overline{k}$ is bounded from above by $D_n^{O(1)}$. We tried to use this fact and defined the function $\varkappa$. But this may seem slightly obscure (when one constructs the corresponding computation forest) and requires additional explanations. For instance, one can apply Lemma 1 to justify the construction involving the function $\varkappa$. Still, it is better to apply Lemma 2 in [6].

Of course, to obtain the main result of [6], one can proceed in a simpler way. Namely, let $Z_1, \ldots, Z_{m_3}$ be new variables. Then in formula (16) for $\psi^{(1)}$ (with arbitrary m_1, we do not use Lemma 2), it suffices to replace $Y_1, X, v_3, \ldots, v_n$ by $Z_1, \ldots, Z_{m_1}, X, v_3, \ldots, v_n$ and Y_1^i by Z_i. In formula (17) for $\psi^{(2)}$ (with arbitrary m_2, m_3), it suffices to replace $Y_2, Y_3, X, v_3, \ldots, v_n$ by $Z_{m_1+1}, \ldots, Z_{m_3}, X, v_3, \ldots, v_n$ and $Y_2^{i_2} Y_3^{i_2}$ by $Z_{i_2} Z_{i_3}$. But here there are too many variables Z_i if we wish to construct a stratification from Theorem 1 of [6] in subexponential time.

2. Multivalued computation trees and forests

In [5], computation trees and forests are introduced. According to Sec. 1 of [5] (we use the notation from there),

(∗) for every vertex v of a computation tree T, for every point $a^* = (a_1^*, \ldots, a_\nu^*) \in \mathcal{W}_v$ there is at most one son w of v such that $\mathcal{A}_w(a_1^*, \ldots, a_\nu^*) = \text{true}$.

In [5], property (∗) is stated in an equivalent form, see formula (3) in Sec. 1 of that paper.

The definition of a multivalued computation tree is the same as in [5] with only one difference: property (∗) does not necessarily hold. Thus, for a multivalued computation tree, all the objects introduced in [5] are defined. In [5] (see formula (5) at the end of Sec. 1 there),

$$\mathcal{S}(T) = \bigcup_{v\in L(T)} \mathcal{W}_v \tag{18}$$

is a stratification of a constructive set $\mathcal{S}(T)$, i.e., $\mathcal{W}_{v_1} \cap \mathcal{W}_{v_2} = \varnothing$ for all pairwise distinct $v_1, v_2 \in L(T)$. Now, for a multivalued computation tree, (18) is a covering of the set $\mathcal{S}(T)$.

Similarly to [5] (we leave the details to the reader), a subtree of a multivalued computation tree is defined. Any such subtree is a multivalued computation tree. A multivalued computation tree T is irredundant if and only if for any subtree T' of T such that $T' \neq T$, we have $\mathcal{S}(T') \neq \mathcal{S}(T)$. If T is a computation tree in the sense of [5], then T is irredundant if and only if $T = \mathrm{IRD}(T)$, see Sec. 2 of [5].

For any multivalued computation tree T there is an irredundant subtree T' of T with $\mathcal{S}(T') = \mathcal{S}(T)$, but this subtree is generally not unique.

Similarly to [5], one can define full signatures, signatures, and labels corresponding to multivalued computation trees and their vertices (we leave the details to the reader).

Let $a'_1, \ldots, a'_\varkappa$ be parameters algebraically independent over k and $c_1, \ldots, c_\nu \in k[a'_1, \ldots, a'_\varkappa]$. In [5], at the end of Sec. 2, the computation tree $T(c)$ and the incomplete tree $T'(c)$ corresponding to a computation tree T and a family of elements $c = \{c_i\}_{1 \leq i \leq \nu}$ are defined (actually, $T(b)$ and $T'(b)$ are defined there, but for convenience here we replace the notation b by c and μ by $\varkappa$). The tree $T(c)$ has the family of input parameters $a'_1, \ldots, a'_\varkappa$. Now assume that T is a multivalued computation tree. Then, replacing everywhere in the definitions of $T(c)$ and $T'(c)$ in [5] a computation tree T by a multivalued computation tree T, we obtain (by definition) the multivalued computation tree $T(c)$ and the incomplete multivalued tree $T'(c)$ corresponding to a multivalued computation tree T and a family of elements c. Roughly speaking, to obtain $T'(c)$, one should substitute $c_1, \ldots, c_\nu$ for $a_1, \ldots, a_\nu$ everywhere in the objects related to T. After that, in order to define $T(c)$, one glues a new root to $T'(c)$.

Let us replace computation trees by multivalued computation trees everywhere in the definition of a computation forest. Then we obtain the definition of a multivalued computation forest. Thus, a multivalued computation forest is a family $\{T_\sigma\}_{\sigma \in \Sigma}$ of multivalued computation trees.

In [5, Sec. 3], a function $\mathfrak{F} : \mathcal{S}(T) \to \mathcal{K}$ corresponding to a computation forest T is defined.

Now let T be a multivalued computation forest. Let us replace a computation forest by a multivalued computation forest (for which we use here the same notation T) in the definition of this function $\mathfrak{F}$ from [5, Sec. 3]. Then we obtain (in place of a function $\mathfrak{F}$) a binary relation $\mathfrak{F} \subset \mathcal{S}(T) \times \mathcal{K}$ corresponding to the multivalued computation forest T. Here $\mathfrak{F}$ can be regarded as a multivalued function. We will write $\mathfrak{F} = \mathfrak{F}(T)$.

By definition, the binary relation $\mathfrak{F}(T)$ is an algorithm corresponding to the multivalued computation forest T. An arbitrary binary relation $\mathfrak{Q}$ is an algorithm corresponding to a multivalued computation forest if and only if there is a multivalued computation forest T such that $\mathfrak{Q} = \mathfrak{F}(T)$.

As we have noted in [5], in practice, an algorithm corresponding to a computation forest T arises from some algorithm in the usual sense. The latter has the set of inputs $\mathcal{S}(T)$, its outputs belong to $\mathcal{K}$, and it computes the function $\mathfrak{F}(T)$.

In a similar way, in practice, an algorithm corresponding to a multivalued computation forest, say $T = \{T_\sigma\}_{\sigma \in \Sigma}$, arises from a multi-output algorithm. In the latter, at some steps some objects are chosen (for example, linear forms or some matrices from given finite sets, see the next sections). One considers all possible choices. But some of them give outputs (with a prescribed signature, see [5] for details), and others not. Thus the outputs of this algorithm depend on the choice of these objects. One obtains a multivalued function from the domain of inputs of this algorithm to the range of outputs, or, which is the same, a binary relation $\mathfrak{Q}$ (such that $\mathfrak{Q} = \mathfrak{F}(T)$).

Let us fix $\sigma \in \Sigma$. Assume that a step of the multi-output algorithm under consideration containing a choice of objects corresponds to a vertex v' of the tree T_σ. Then all sons v of v' are in a one-to-one correspondence with all possible choices of these objects. Denote by $L(v, T_\sigma)$ the set of leaves w of the computation tree T_σ such that w is a descendant of v.

Then the choice of objects corresponding to v does not give any required output if and only if $\mathcal{W}_w = \varnothing$ for every $w \in L(v, T_\sigma)$. Here is a somewhat informal explanation of this fact: this multi-output algorithm solves some problem (e.g., determines all solutions of a system of polynomial equations), and each its output from $\mathcal{K}$ gives a solution of this problem. There are no other outputs.

Often, an algorithm $\mathfrak{Q}$ corresponding to a multivalued computation forest determines an algorithm in the usual (or classical) sense. Namely, assume that $\mathfrak{Q}$ arises from a multi-output algorithm. In this multi-output algorithm, some objects are chosen. In the corresponding classical algorithm, these objects are enumerated until the first object that gives an output appears (of course, one should specify the method of enumerating; note also that there can be many steps with enumeration). The latter algorithm computes a function (in the usual sense) $\mathfrak{Q}' : \mathcal{S}(T) \to \mathcal{K}$, which is a restriction of the binary relation $\mathfrak{Q}$.

Conversely, let us be given an algorithm with enumerations in the usual sense computing a function $\mathfrak{Q}' : \mathcal{S} \to \mathcal{K}$. Then it determines a multi-output algorithm $\mathfrak{Q} : \mathcal{S} \to \mathcal{K}$. To define $\mathfrak{Q}$, one should use all possible choices of the objects under consideration instead of enumerating them. Thus, here again $\mathfrak{Q}'$ is a restriction of the binary relation $\mathfrak{Q}$.

We will say that an algorithm with enumerations (in the usual sence) computing a function $\mathfrak{Q}'$ corresponds to a multivalued computation forest T if and only if the related multi-valued function $\mathfrak{Q}$ is an algorithm corresponding to a computation forest T. We will say that an algorithm with enumerations (in the usual sence) corresponds to a multivalued computation forest if there is a multivalued computation forest T such that this algorithm corresponds to T.

Similarly to [5, Sec. 3], one can define the composition $T_2 \circ T_1$ of multivalued computation forests T_1 and T_2. It is defined if and only if the composition of binary relations $\mathfrak{F}(T_2) \circ \mathfrak{F}(T_1)$ is defined. Moreover, in this case we have $\mathfrak{F}(T_2 \circ T_1) = \mathfrak{F}(T_2) \circ \mathfrak{F}(T_1)$.

Similarly to [5, Sec. 3], one can define the N-tuple $\langle T_1, \dots, T_N \rangle$ of multivalued computation forests $T_1, \dots, T_N$. Thus $\langle T_1, \dots, T_N \rangle$ is a multivalued computation forest.

Now we are going to state an analog of Theorem 1 of [5] for multivalued computation trees. This analog is Theorem 3, see below. It can be regarded as a fundamental result in the theory of multivalued computation trees and forests.

But first we need to strengthen Lemma 5 from Sec. 6 of [6]. In that paper, for a quasiprojective algebraic variety $V \subset \mathbb{A}^\mu(\overline{k})$, we use the following notation: $D_a(V)$ is the degree (see Sec. 6 of [6] for details) of the union of all irreducible components of V of dimension a where $0 \le a \le \mu$; for an integer $D \ge 2$, put $\delta_1(V, D) = \sum\limits_{0 \le a \le \mu} D_a(V) D^a$ and $\delta(V, D) = \sum\limits_{0 \le a \le \mu} D_a(V)(D^{a+1} - 1)/(D - 1)$.

In the statement of the following lemma there are two bounds on degrees, D_1 and D, in place of only one bound D in Lemma 5 of [6]. Nevertheless, assertions (b)–(d) of this lemma coincide with the corresponding assertions (b)–(d) of Lemma 5 of [6].

Lemma 3. *Let V be a quasiprojective algebraic variety in $\mathbb{A}^\mu(\overline{k})$. Let $\{\mathcal{W}_\gamma\}_{\gamma \in \Gamma}$ be a family of quasiprojective algebraic varieties in $\mathbb{A}^\mu(\overline{k})$. Assume that for every $\gamma \in \Gamma$,*

$$\mathcal{W}_\gamma = \mathcal{Z}(\psi_{\gamma,1}, \dots, \psi_{\gamma,\mu_{\gamma,1}}) \setminus \mathcal{Z}(\psi_{\gamma,\mu_{\gamma,1}+1}, \dots, \psi_{\gamma,\mu_{\gamma,2}}) \subset \mathbb{A}^\mu(\overline{k})$$

for some polynomials $\psi_{\gamma,i} \in \overline{k}[b_1, \dots, b_\mu]$ such that $\deg_{b_1,\dots,b_\mu} \psi_{\gamma,i} \le D_1$ for $1 \le i \le \mu_{\gamma,1}$ and $\deg_{b_1,\dots,b_\mu} \psi_{\gamma,i} \le D$ for $\mu_{\gamma,1} + 1 \le i \le \mu_{\gamma,2}$, for some integers $D_1 \ge D \ge 2$. Assume that $\bigcup\limits_{\gamma \in \Gamma} \mathcal{W}_\gamma \supset V$. Then there is a family of quasiprojective algebraic varieties $\{\mathcal{W}_\beta\}_{\beta \in B}$ satisfying the following properties.

(a) *For every* $\beta \in B$,

$$\mathcal{W}_\beta = \mathcal{Z}(\psi^{(1)}_{\beta,1}, \ldots, \psi^{(1)}_{\beta,\mu_{\beta,1}}) \setminus \bigcup_{2 \le j \le m_\beta} \mathcal{Z}(\psi^{(j)}_{\beta,1}, \ldots, \psi^{(j)}_{\beta,\mu_{\beta,j}}) \subset \mathbb{A}^\mu(\overline{k})$$

for an integer $m_\beta \ge 2$ *and some polynomials* $\psi^{(j)}_{\beta,i} \in \overline{k}[b_1, \ldots, b_\mu]$ *such that*

$$\deg_{b_1,\ldots,b_\mu} \psi^{(1)}_{\beta,i} \le D_1$$

for $1 \le i \le \mu_{\beta,1}$ *and* $\deg_{b_1,\ldots,b_\mu} \psi^{(j)}_{\beta,i} \le D$ *for* $1 \le i \le \mu_{\beta,j}$, $2 \le j \le m_\beta$.

(b) *For every* $\beta \in B$, *the integer* m_β *is bounded from above by* $\delta_1(V, D)$.

(c) $\{V \cap \mathcal{W}_\beta\}_{\beta \in B}$ *is a stratification of the algebraic variety* V, *i.e.,* $\bigcup_{\beta \in B} (V \cap \mathcal{W}_\beta) = V$, *and* $(V \cap \mathcal{W}_{\beta_1}) \cap (V \cap \mathcal{W}_{\beta_2}) = \varnothing$ *for all pairwise distinct* β_1, β_2.

(d) *For every* $\beta \in B$ *there is* $\gamma \in \Gamma$ *such that* $\mathcal{W}_\beta \subset \mathcal{W}_\gamma$.

(e) *The number of elements* $\#B$ *does not exceed* $\delta(V, D)$.

Proof. The proof coincides with the proof of Lemma 5 in Sec. 6 of [6]. □

Theorem 3. *Let* T *be a multivalued computation tree with input parameters* $a_1, \ldots, a_\nu$ *over the ground field* k *and* $l(T) = w$. *Assume that for every vertex* v *of* T, *the condition* $\mathcal{A}_v$ *has the form*

$$(\varphi_{v,1} = 0) \wedge \ldots \wedge (\varphi_{v,\mu_{v,1}} = 0) \wedge ((\varphi_{v,\mu_{v,1}+1} \ne 0) \vee \ldots \vee (\varphi_{v,\mu_{v,2}} \ne 0)), \tag{19}$$

where $\wedge$, $\vee$ *denote the logical conjunction and disjunction,* $\varphi_{v,\beta} \in k[a_1, \ldots, a_\nu]$, $1 \le \beta \le \mu_{v,2}$, *are polynomials for some integers* $\mu_{v,2} \ge \mu_{v,1} \ge 0$, *and* $\deg_{a_1,\ldots,a_\nu} \varphi_{v,\beta} \le d$ *for* $\mu_{1,v} < \beta \le \mu_{2,v}$ (*see* (19)) *for an integer* $d \ge 2$. *Let* $\mathcal{S}(T) = \bigcup_{1 \le j \le N} S_j$ *where* S_j *are quasiprojective algebraic varieties in* $\mathbb{A}^\nu(\overline{k})$. *Then there is an irredundant multivalued subtree* T' *of the tree* T *such that* $\mathcal{S}(T') = \mathcal{S}(T)$ *and*

$$\#L(T') \le \sum_{1 \le j \le N} \delta(S_j, wd).$$

In particular, if $\mathcal{S}(T) = \mathbb{A}^\nu(\overline{k})$, *then*

$$\#L(T') \le \frac{(wd)^{\nu+1} - 1}{wd - 1}.$$

Proof. Let us apply Lemma 3 with $\mu = \nu$, $V = S_j$ for every j, $D = wd$, $\Gamma = L(T)$. Then first we obtain a stratification of each variety S_j, and then, by assertion (d) of the lemma, a covering of each variety S_j. This gives a covering $\{\mathcal{W}_v\}_{v \in \Gamma'}$ of $\mathcal{S}(T) = \bigcup_{1 \le j \le N} S_j$ with $\Gamma' \subset \Gamma$ and $\#\Gamma' \le \sum_{1 \le j \le N} \delta(S_j, wd)$. Now let T' be the minimal multivalued subtree of T such that $L(T') = \Gamma'$. For this subtree T', the assertion of the theorem holds. The theorem is proved. □

As an example, observe that the covering from the modified version of Theorem 1 of [6] (see Remark 2 in the introduction) can be obtained using a multivalued computation forest. We leave the details to the reader.

3. The case of a finite number of solutions in the projective space

First, we consider the case $c = 0$. Now, for every $a^* \in \mathcal{U}_c$ the system (3) has a finite (or empty) set of solutions in $\mathbb{P}^n(\overline{k})$. Put $B = \overline{k}[a_1, \ldots, a_\nu]$. Let $Y_0, Y_1, \ldots, Y_n \in B[X_0, \ldots, X_n]$ be arbitrary linear forms in $X_0, \ldots, X_n$ with coefficients in B. Let $U_0, U_1, \ldots, U_n$ be new variables. Put $f_m = U_0 Y_0 + U_1 Y_1 + \ldots + U_n Y_n$.

Let $\deg_{X_0,\dots,X_n} f_i = d_i$ for $0 \le i \le m-1$. Put $d_m = 1$. Recall that $d_0 \ge d_1 \ge \ldots \ge d_{m-1} \ge 1$, see Remark 1 in the introduction. Let $D' = d_0 + \sum\limits_{1 \le i \le \min\{m-1,n\}} (d_i - 1)$. Let $\mathcal{H}_i$, $1 \le i \le m$, (respectively, $\mathcal{H}$) be the $B[U_0,\dots,U_n]$-module of all polynomials $g \in B[U_0,\dots,U_n][X_0,\dots,X_n]$ homogeneous with respect to $X_0,\dots,X_n$ of degree $\deg_{X_0,\dots,X_n} g = D' - d_i$ (respectively, $\deg_{X_0,\dots,X_n} g = D'$). Then $\mathcal{H}_i$ (respectively, $\mathcal{H}$) is a free $B[U_0,\dots,U_n]$-module of rank $\gamma_i = \binom{D'-d_i+n}{n}$ (respectively, $\gamma = \binom{D'+n}{n}$). Consider the homomorphism of free $B[U_0,\dots,U_n]$-modules

$$\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \ldots \oplus \mathcal{H}_m \to \mathcal{H}, \quad (g_0,\dots,g_m) \mapsto g_0 f_0 + \ldots + g_m f_m. \tag{20}$$

Let us choose a basis of each module $\mathcal{H}_i$ (respectively, $\mathcal{H}$) consisting of monomials in $X_0,\dots,X_n$ with coefficients 1 of degree $D' - d_i$ (respectively, D'). Then the homomorphism (20) is given in these bases by a matrix $\mathcal{A}$ with γ rows and $\sum\limits_{0 \le i \le m} \gamma_i$ columns. One can represent $\mathcal{A}$ in the form $\mathcal{A} = (\mathcal{A}', \mathcal{A}'')$ where $\mathcal{A}'$ is a submatrix of $\mathcal{A}$ consisting of the first $\sum\limits_{0 \le i \le m-1} \gamma_i$ columns. Then the entries of $\mathcal{A}'$ are elements of B, and the entries of $\mathcal{A}''$ are linear forms in $U_0,\dots,U_n$ with coefficients in B.

For every $a^* \in \mathbb{A}^\nu(\overline{k})$, let $\mathcal{A}(a^*) = \mathcal{A}|_{a_1=a_1^*,\dots,a_\nu=a_\nu^*}$ be the result of substituting a_i^* for a_i, $1 \le i \le \nu$, in $\mathcal{A}$. The matrices $\mathcal{A}'(a^*)$, $\mathcal{A}''(a^*)$ are defined in a similar way. Thus $\mathcal{A}'(a^*)$ is a matrix with entries in k_{a^*}, all entries of the matrix $\mathcal{A}''(a^*)$ are linear forms in $U_0,\dots,U_n$ with coefficients from k_{a^*}, and $\mathcal{A}(a^*) = (\mathcal{A}'(a^*), \mathcal{A}''(a^*))$. Denote by Δ_{a^*} the greatest common divisor in the ring $k_{a^*}[U_0,\dots,U_n]$ of all minors of order γ of the matrix $\mathcal{A}(a^*)$ (it is uniquely defined up to a nonzero factor from k_{a^*}).

Let us state a result from [10, 11].

Lemma 4. *Let $a^* \in \mathbb{A}^\nu(\overline{k})$. Let V_{a^*} be the set of all solutions (or roots) of the system (3) in $\mathbb{P}^n(\overline{k})$. Then the following assertions hold.*

(a) *If $\#V_{a^*} = +\infty$ (or, which is the same, $\dim V_{a^*} > 0$), then $\Delta_{a^*} = 0$.*

(b) *If $\#V_{a^*} < +\infty$, then*

$$\Delta_{a^*} = \lambda \prod_{\eta=(\eta_0:\ldots:\eta_n)\in V_{a^*}} \Big(\sum_{0 \le i \le n} U_i Y_i(\eta_0,\dots,\eta_n) \Big)^{e_\eta},$$

where $e_\eta \ge 1$ is the multiplicity of a root η of the system (3), $0 \ne \lambda \in \overline{k}$, and all η_i lie in $\overline{k}$, $0 \le i \le n$ (note that here the linear forms $\sum\limits_{0 \le i \le n} U_i Y_i(\eta_0,\dots,\eta_n) \in \overline{k}[U_0,\dots,U_n]$, $\eta \in V_{a^*}$, are not necessarily pairwise distinct, since Y_i are arbitrary).

(c) *Assume that $\#V_{a^*} < +\infty$ and for every solution $\eta = (\eta_0 : \ldots : \eta_n) \in V_{a^*}$ we have $\sum\limits_{0 \le i \le n} U_i Y_i(\eta_0,\dots,\eta_n) \ne 0$. Then $\deg_{U_0,\dots,U_n} \Delta_{a^*} = \gamma - \operatorname{rank} \mathcal{A}'(a^*)$.*

Proof. If $Y_i = X_i$ for all i, this is proved in [10, 11]. The case of arbitrary Y_i can be easily reduced to the special case of $Y_i = X_i$, $0 \le i \le n$, using a nondegenerate linear transformation of linear forms and a substitution (we leave the details to the reader). □

Recall that the finite sets of linear forms $\mathcal{L}_0 = \mathcal{M}_{\varkappa_{1,0}}$, $\mathcal{L}_0' = \mathcal{M}'_{0,\varkappa_{2,0}}$ are defined in the introduction. Also, recall that $\varkappa_{1,0} = 2nD_n'$ and $\varkappa_{2,0} = nD_n'(D_n' - 1)/2$.

Lemma 5. *Let $a^* \in \mathcal{U}_0$. Then there is a pair of linear forms $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}_0'$ such that for every $\eta \in V_{a^*}$ we have $Y_0(\eta) \ne 0$ and for any two distinct $\eta_1, \eta_2 \in V_{a^*}$ we have $(Y_1/Y_0)(\eta_1) \ne (Y_1/Y_0)(\eta_2)$.*

Proof. This is straightforward, cf. [2]. □

Let us weaken Theorem 1 (respectively, the modified version of Theorem 1) for $c = 0$ as follows. In its statement replace "(i)–(xiii)" by "(i)–(ix)" (respectively, "(ii)–(xiii)" by "(ii)–(ix)"), and in assertion (c) omit "$\Psi_{\alpha,s,r,i_1,i_2}$, Ψ_{j,i_1,i_2}". Now we are going to construct a multivalued computation forest T_0, to prove the weakened Theorem 1 (respectively, the weakened modified version of Theorem 1) for $c = 0$. Consider the system (3) with $a^* \in \mathcal{U}_0$. First, we will describe an algorithm (with enumerations, see Sec. 2) for solving this system. It follows the method from [10, 11] with some modifications. After that, we will see that it is an algorithm corresponding to a multivalued computation forest in the sense of Sec. 2.

Let $Y_0, Y_1 \in k[X_0, \dots, X_n]$ be arbitrary linear forms. Put $Y_i = 0$ for $2 \le i \le n$. Our aim is to find the polynomial Δ_{a^*}, see Lemma 4. Let us construct the matrix $\mathcal{A} = (\mathcal{A}', \mathcal{A}'')$, see above. Then, using Lemma 1, we construct a matrix $\mathcal{G}$ such that $\mathcal{G}\mathcal{A}'(a^*)$ has the canonical trapezoidal form up to a permutation of rows and columns. Let $\mathcal{G}\mathcal{A}'(a^*) = \begin{pmatrix} \mathcal{A}_1 \\ 0 \end{pmatrix}$ where $\operatorname{rank}(\mathcal{A}_1) = \operatorname{rank}(\mathcal{A}'(a^*))$ is equal to the number of rows of $\mathcal{A}_1$. Hence, after a permutation of rows and columns of the matrix $\mathcal{G}\mathcal{A}(a^*)$, this matrix has the form $\begin{pmatrix} \mathcal{A}_1, & \mathcal{A}_2 \\ 0, & \mathcal{A}_3 \end{pmatrix}$ where all entries of the matrices $\mathcal{A}_2$, $\mathcal{A}_3$ are linear forms from $k_{a^*}[U_0, U_1]$ and $\operatorname{rank}(\mathcal{A}_3) = \gamma - \operatorname{rank}(\mathcal{A}'(a^*))$.

Now we apply Lemma 2 to the matrix $\mathcal{A}_3$ (in place of A). By this lemma, we obtain a family of matrices C_j, $0 \le j \le N$, with entries in k such that $\mathcal{A}_3 C_j$ is a square matrix for every j. We enumerate the matrices C_j for $j = 1, 2, \dots, N$. If $\det(\mathcal{A}_3 C_j) = 0$ for every j, then $\operatorname{rank}(A) < \gamma$ and $\Delta_{a^*} = 0$.

Let $\det(\mathcal{A}_3 C_{j_0}) \ne 0$ for some j_0 and $\det(\mathcal{A}_3 C_j) = 0$ for $1 \le j < j_0$. Then, by Lemma 4(c), we have $\Delta_{a^*} = \det(\mathcal{A}_3 C_{j_0})$ (up to a nonzero factor from k_{a^*}; we will assume without loss of generality that this factor is equal to 1). Thus we have computed the nonzero polynomial $\Delta_{a^*} \in k_{a^*}[U_0, U_1]$.

Remark 6. Assume that $\nu = 0$, $a^{(0)} \in \mathbb{A}^\nu(\overline{k})$, $Y_0 \ne 0$. By definition, put $\widetilde{\Delta}_{k;X_0,\dots,X_n;f_0,\dots,f_{m-1};Y_0,Y_1} = \Delta_{a^{(0)}}$ where $\Delta_{a^{(0)}}$ is uniquely defined by the described construction.

Under these conditions, we also introduce the notation

$$\Delta_{k;X_0,\dots,X_n;f_0,\dots,f_{m-1};Y_0,Y_1} = \begin{cases} \Delta_{a^{(0)}}/\operatorname{lc}_{U_0}(\Delta_{a^{(0)}}) & \text{if} \quad \Delta_{a^{(0)}} \ne 0, \\ 0 & \text{if} \quad \Delta_{a^{(0)}} = 0. \end{cases}$$

It will be used in the next sections.

Let $a^* \in \mathcal{U}_0$. Now we enumerate the pairs of linear forms $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}_0'$. Put $Y_i = 0$ for $2 \le i \le n$ and compute the corresponding polynomial Δ_{a^*} as described.

If $\Delta_{a^*} = 0$, then the pair of linear forms does not satisfy the assertion of Lemma 5, and we proceed to the next pair $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}_0'$.

If $\Delta_{a^*} \ne 0$ and U_1 divides Δ_{a^*}, then $Y_0(\eta) = 0$ for some $\eta \in V_{a^*}$. In this case, we proceed to the next pair $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}_0'$.

Finally, by Lemmas 5 and 4, we will find (Y_0, Y_1) such that $\Delta_{a^*} \ne 0$ and U_1 does not divide Δ_{a^*}. In this case, we apply the result of [6, Sec. 2] and construct separable polynomials

$$\Delta_{a^*,j} = \operatorname{SQF}_{j,Z}(\Delta_{a^*}(Z, -1)) \in k_{a^*}[Z], \quad 1 \le j \le \deg_{U_0} \Delta_{a^*},$$

giving the square-free decomposition of the polynomial $\Delta_{a^*}(Z, -1)$ in the sense of (21), see below. For every j, we have $0 \le \deg_Z \Delta_{a^*,j} \le (\deg_{U_0} \Delta_{a^*})/j$.

Recall that the integer ρ_0 is defined in the introduction, see (iv) with $s = 0$. If the characteristic exponent p is equal to 1, then, by definition, $B_0 = \{1, \dots, \deg_Z \Delta_{a^*}(Z, -1)\}$, $B_1 = \varnothing$. If $p > 1$, then $B_r = \{jp^r : 1 \le j \le (\deg_Z \Delta_{a^*}(Z, -1))/p^r\}$ for every integer $r \ge 0$, see [6, Sec. 2]. By definition, put $r(j) = r$ if and only if $j \in B_r \setminus B_{r+1}$.

In this notation, the polynomial

$$\prod_{0\le r\le\rho_0}\prod_{j\in B_r\setminus B_{r+1}}\Delta_{a^*,j}^{j/p^r}(Z^{p^r})=\lambda'_{a^*}\Delta_{a^*}(Z,-1), \tag{21}$$

where $0\ne\lambda'_{a^*}\in k_{a^*}$, and the polynomials $\Delta_{a^*,j}(Z^{p^{r(j)}})$, $1\le j\le\deg_{U_0}\Delta_{a^*}$, are pairwise relatively prime, see [6, Sec. 2]. Put

$$g_{a^*,r}=\prod_{j\in B_r\setminus B_{r+1}}\Delta_{a^*,j}\in k_{a^*}[Z],\quad 0\le r\le\rho_0.$$

Therefore, every polynomial $g_{a^*,r}\in k_{a^*}[Z]$ is separable. Note that

$$\sum_{0\le r\le\rho_0}\deg_Z g_{a^*,r}=\#\{(Y_1/Y_0)(\eta)\,:\,\eta\in V_{a^*}\} \tag{22}$$

(we leave the details to the reader).

Let t be a transcendental element over k. Let us extend the ground field k to $k(t)$. For every i, $0\le i\le n$, we apply the described construction to $k(t)$, Y_0, Y_1+tX_i in place of k, Y_0, Y_1 with the same j_0 fixed earlier (i.e., we do not enumerate the matrices C_j again; also, the system (3) remains the same). Put $\tau_r=t^{p^r}$. We obtain polynomials $\Delta_{a^*,i}\in k_{a^*}[t,U_0,U_1]$ and $g_{a^*,r,i}\in k_{a^*}[\tau_r,Z]$ in place of Δ_{a^*} and $g_{a^*,r}$, respectively, $0\le r\le\rho_0$. We have

$$\sum_{0\le r\le\rho_0}\deg_Z g_{a^*,r,i}=\#\{((Y_1+tX_i)/Y_0)(\eta)\,:\,\eta\in V_{a^*}\}. \tag{23}$$

Lemma 6. *In the notation of Lemma* 4 (b), *let* $e_\eta=p^{r_\eta}e'_\eta$ *where* r_η, e'_η *are integers,* $0\le r_\eta\le\rho_0$, $e'_\eta\ge 1$, $\mathrm{GCD}\,(e'_\eta,p)=1$ *for every* $\eta\in V_{a^*}$. *Assume that* U_1 *does not divide* Δ_{a^*}. *Then the pair of linear forms* $(Y_0,Y_1)\in\mathcal{L}_0\times\mathcal{L}'_0$ *satisfies the assertion of Lemma* 5 *if and only if one of the following equivalent conditions holds*:

(a) $\sum\limits_{0\le r\le\rho_0}\deg_Z g_{a^*,r,i}=\sum\limits_{0\le r\le\rho_0}\deg_Z g_{a^*,r}$ *for all* i,

(b) $\deg_Z g_{a^*,r,i}=\deg_Z g_{a^*,r}$ *for all* i,r,

(c) *for every* r, $0\le r\le\rho_0$, *the polynomial* $g_{a^*,r}(Z^{p^r})$ *coincides with*

$$\prod_{\eta\in V_{a^*},\,r_\eta=r}(Z-(Y_1/Y_0)(\eta))^{p^r}$$

up to a nonzero factor from $\overline{k}$, *and for all* i, $0\le i\le n$, *and* r, $0\le r\le\rho_0$, *the polynomial* $g_{a^*,r,i}(Z^{p^r})$ *coincides with*

$$\prod_{\eta\in V_{a^*},\,r_\eta=r}(Z-(Y_1/Y_0)(\eta)-t(X_i/Y_0)(\eta))^{p^r}$$

up to a nonzero factor from $\overline{k}(\tau_r)$.

Proof. Obviously, (c) implies (b) and (b) implies (a). Let us prove that (a) implies (c). For every $\eta\in V_{a^*}$, denote by e''_η (respectively, $e''_{\eta,i}$) the multiplicity of the root $Z=(Y_1/Y_0)(\eta)$ (respectively, $Z=((Y_1/Y_0)+t(X_i/Y_0))(\eta)$) of the polynomial $\Delta_{a^*}(Z,-1)\in k_{a^*}[Z]$ (respectively, $\Delta_{a^*,i}(t,Z,-1)\in k_{a^*}(t)[Z]$). Then $e''_\eta\ge e''_{\eta,i}\ge e_\eta$ for any η and i. Therefore, by (22) and (23),

$$\sum_{0\le r\le\rho_0}\deg_Z g_{a^*,r}=\sum_{\eta\in V_{a^*}}1/e''_\eta\le\sum_{\eta\in V_{a^*}}1/e''_{\eta,i}=\sum_{0\le r\le\rho_0}\deg_Z g_{a^*,r,i}. \tag{24}$$

If $e''_\eta > e_\eta$ for some η, then there is an element $\eta^{(1)} \in V_{a^*}$ such that $(Y_1/Y_0)(\eta^{(1)}) = (Y_1/Y_0)(\eta)$ but $(X_i/Y_0)(\eta^{(1)}) \neq (X_i/Y_0)(\eta)$ for some i, $0 \leq i \leq n$. Hence, in this case there is i, $0 \leq i \leq n$, such that $e''_\eta > e''_{\eta,i}$.

Therefore, in (24) the equality takes place for every i, $0 \leq i \leq n$, if and only if $e_\eta = e''_\eta$ for every $\eta \in V_{a^*}$. This immediately implies (c). The lemma is proved. □

Assume that a pair (Y_0, Y_1) satisfies the assertion of Lemma 5. Let $\mathrm{lc}_Z(g_{a^*,r,i})$ be the leading coefficient of the polynomial $g_{a^*,r,i}$ with respect to Z. Then $g_{a^*,r,i}/\mathrm{lc}_Z(g_{a^*,r,i}) \in k_{a^*}[\tau_r, Z]$, since the roots of this polynomial are integral over $k_{a^*}[\tau_r]$. Thus, applying Lemma 2 of [6], we can replace $g_{a^*,r,i}$ by a polynomial coinciding with $g_{a^*,r,i}/\mathrm{lc}_Z(g_{a^*,r,i})$ up to a nonzero factor from k_{a^*}. Hence in what follows we may assume without loss of generality that $\mathrm{lc}_Z(g_{a^*,r,i}) \in k_{a^*}$.

Now, for every r and for every i, the polynomial $g_{a^*,r,i}(0, Z)$ coincides with $g_{a^*,r}$ up to a nonzero factor from k_{a^*}. Let $\mu_{a^*,r} = \mathrm{lc}_Z g_{a^*,r}$ (respectively, $\mu_{a^*,r,i} = \mathrm{lc}_Z g_{a^*,r,i}$, $0 \leq i \leq n$). Replacing $g_{a^*,r}$ by $\left(\prod\limits_{0\leq j\leq n} \mu_{a^*,r,j}\right) g_{a^*,r}$ and each polynomial $g_{a^*,r,i}$ by

$$\mu_{a^*,r} \left(\prod_{0\leq j\neq i\leq n} \mu_{a^*,r,j}\right) g_{a^*,r,i},$$

we will assume without loss of generality that $g_{a^*,r,i}(0, Z) = g_{a^*,r}$ for every i.

If $\deg_Z g_{a^*,r} = 0$, put $J_{a^*,r} = \varnothing$ and $V_{a^*,0,r} = \varnothing$. Let $\deg_Z g_{a^*,r} > 0$. Then let $J_{a^*,r}$ be a one-element set. Put $H_{a^*,j} = g_{a^*,r}$ for $j \in J_{a^*,r}$. We assume that the sets $J_{a^*,r}$ are pairwise disjoint. Now we are going to define and compute the variety $V_{a^*,0,r}$ in the case under consideration. Thus in what follows, unless otherwise stated, we assume in the proof that $\deg_Z g_{a^*,r} > 0$.

For every r, $0 \leq r \leq \rho_0$, we construct a polynomial $Q \in k_{a^*}[Y, Z]$ such that $g_{a^*,r} = (Z - Y)Q + g_{a^*,r}(Y)$. For every root ξ of the polynomial $g_{a^*,r}$, we have $(Z - \xi)Q(\xi, Z) = 0$. Put $g'_{a^*,r} = \frac{d}{dZ}(g_{a^*,r}) = Q(Z, Z)$.

For every i, we have $g_{a^*,r,i} = g_{a^*,r} + \sum\limits_{j\geq 0} g_{a^*,r,i,j}\tau_r^j \in k_{a^*}((\tau_r))[Z]$ where $g_{a^*,r,i,j} \in k_{a^*}[Z]$. Now we apply the Hensel lifting to the polynomial $g_{a^*,r,i}$ and the decomposition $g_{a^*,r,i}(0, Z) = (Z - \xi)Q(\xi, Z)$ and obtain a root $Z = \xi_i \in k_{a^*}[[\tau_r]]$ of this polynomial $g_{a^*,r,i}$ such that $\xi_i(0) = \xi_i|_{\tau_r=0} = \xi$. Furthermore,

$$\frac{d}{d\tau_r}(\xi_i)\Big|_{\tau_r=0} = -\left(\frac{\partial g_{a^*,r,i}}{\partial \tau_r}\right) \Big/ \left(\frac{\partial g_{a^*,r,i}}{\partial Z}\right)\Big|_{\tau_r=0, Z=\xi} = -g_{a^*,r,i,1}(\xi)/g'_{a^*,r}(\xi).$$

By Lemma 4, the root ξ_i is actually a linear polynomial in τ_r and

$$\xi_i = \xi - \tau_r \frac{g_{a^*,r,i,1}(\xi)}{g'_{a^*,r}(\xi)}, \quad 0 \leq i \leq n.$$

Recall that now $\mu_{a^*,r} = \mathrm{lc}_Z g_{a^*,r} = \mathrm{lc}_Z g_{a^*,r,i}$ for all i. Let $\delta_{a^*,r}$ be the discriminant of the polynomial $g_{a^*,r}$. There are polynomials $A, B \in k_{a^*}[Z]$ such that $\deg_Z A < \deg_Z g_{a^*,r}$, $\deg_Z B < \deg_Z g'_{a^*,r}$, and $-g_{a^*,r,i,1}\delta_{a^*,r} = Ag'_{a^*,r} + Bg_{a^*,r}$ (actually, the coefficients of A and B are polynomials in the coefficients of $g_{a^*,r,i,1}$, $g'_{a^*,r}$, $g_{a^*,r}$). Put $A = \delta_{a^*,r,i}$. Then one can write $-g_{a^*,r,i,1}(\xi)/g'_{a^*,r}(\xi) = \delta_{a^*,r,i}(\xi)/\delta_{a^*,r}$.

If $J_{a^*,r} = \varnothing$, then put $\delta_{a^*,r} = 1$ and $\delta_{a^*,r,i} = 0$ for $0 \leq i \leq n$.

Denote by $\Xi_{a^*,r}$ the set of roots of $g_{a^*,r}$. Let $\xi \in \Xi_{a^*,r}$. Put $W_{a^*,r,\xi} = \{(\eta_0 : \ldots : \eta_n)\}$ where $\eta_i^{p^r} = \delta_{a^*,r,i}(\xi)/\delta_{a^*,r}$ for $0 \le i \le n$. Set

$$V_{a^*,0,r} = \bigcup_{\xi \in \Xi_{a^*,r}} W_{a^*,r,\xi}$$

for every r, $0 \le r \le \rho_0$, such that $\deg_Z g_{a^*,r} > 0$, and $V_{a^*,0,r} = \varnothing$ for every r, $0 \le r \le \rho_0$, such that $\deg_Z g_{a^*,r} = 0$.

Now we are going to prove a modified version of the weakened Theorem 1 (see Remark 2 in the introduction) for the case $c = 0$.

Let $\mu = \gamma_0 + \ldots + \gamma_{m-1}$ and $b = \{b_i\}_{1 \le i \le \mu}$ be a family of algebraically independent elements over k. First we assume that

($\mathfrak{g}$) $\mu = \nu$, the elements a_i and b_i coincide for $0 \le i \le \mu$, and $b_1, \ldots, b_\mu$ is the family of all coefficients of the polynomials $f_0, \ldots, f_{m-1}$, i.e., the family of coefficients of these polynomials has the maximum possible transcendence degree over k.

So, now $d' = 1$.

Under condition ($\mathfrak{g}$), the described construction defines a multivalued function (or a binary relation)

$$\mathfrak{F} : \bigcup_{n, d_0, \ldots, d_{m-1}} \overline{k}^{\gamma_0 + \ldots + \gamma_{m-1}} \to \mathcal{K},$$

$$a^* \mapsto \left(\{g_{a^*,r}\}_{0 \le r \le \rho_0},\ \{\delta_{a^*,i}\}_{\substack{0 \le r \le \rho_0, \\ 0 \le i \le n}} \right),$$

which is an algorithm corresponding to a multivalued computation forest $T_0 = \{T_{0,n,d_0,\ldots,d_{m-1}}\}$ in the sense of Sec. 2 (recall that $\mathcal{K}$ is a universal range of values of algorithms corresponding to multivalued computation forests, see [5] and Sec. 2). Recall that all polynomials $g_{a^*,r}$, $\delta_{a^*,r,i}$ depend on the pair of linear forms (Y_0, Y_1) and the matrix C_{j_0}, see above.

Thus $\mathfrak{F} = \mathfrak{F}(T_0)$. The level $l(T_{0,n,d_0,\ldots,d_{m-1}})$ of each multivalued computation tree is $D_n^{O(1)}$. For every vertex v of the tree $T_{0,n,d_0,\ldots,d_{m-1}}$, we have

$$\mathcal{W}_v = \mathcal{Z}(\psi_{v,1}, \ldots, \psi_{v,\mu_{v,1}}) \setminus \mathcal{Z}(\psi_{v,\mu_{v,1}+1}, \ldots, \psi_{v,\mu_{v,2}}),$$

where all polynomials $\psi_{v,j}$ lie in $k[a_1, \ldots, a_\nu]$ and have degrees bounded from above by $\binom{n+D'}{n}^{O(1)}$. Let $A = L(T_{0,n,d_0,\ldots,d_{m-1}})$ be the set of leaves of the tree $T_{0,n,d_0,\ldots,d_{m-1}}$.

Now, for every $\alpha \in A$, $0 \le r \le \rho_0$, $0 \le i \le n$, polynomials $g_\alpha, r \in k[a_1, \ldots, a_\nu, Z]$, $\delta_{\alpha,r,i} \in k[a_1, \ldots, a_\nu, Z]$ are computed at the vertex α. They satisfy the following properties: $\deg_Z g_{\alpha,r} \le D_n/p^r$, $\deg_Z \delta_{\alpha,r,i} < \deg_Z g_{\alpha,r}$; the degrees in $a_1, \ldots, a_\nu$ of $g_{\alpha,r}$, $\delta_{\alpha,r,i}$ are bounded from above by $\binom{n+D'}{n}^{O(1)}$; and for every $a^* \in \mathcal{W}_\alpha$, we have $\deg_Z g_{\alpha,r} = \deg_Z g_{\alpha,r}(a^*, Z)$,

$$g_{\alpha,r}(a^*, Z) = g_{a^*,r}, \quad \delta_{\alpha,r,i}(a^*, Z) = \delta_{a^*,r,i}$$

for all i, r. Denote by $\delta_{\alpha,r}$ the discriminant of the polynomial $g_{\alpha,r}$ with respect to Z. Then $\delta_{\alpha,r}(a^*) = \delta_{a^*,r} \ne 0$ for all $a^* \in \mathcal{W}_\alpha$ and $0 \le r \le \rho_0$.

Let $d'_r = \deg_Z g_{\alpha,r}$. Put $\Phi_{\alpha,0,r} = Y_0^{d'_r} g_{\alpha,r}(a_1, \ldots, a_\nu, Y_1/Y_0)$. Let $J_{\alpha,0,r}$ be a one-element set if $\deg_Z g_{\alpha,r} > 0$, and $J_{\alpha,0,r} = \varnothing$ if $\deg_Z g_{\alpha,r} = 0$. We will assume without loss of generality that for every α the sets $J_{\alpha,0,r}$, $0 \le r \le \rho_0$, are pairwise disjoint. Furthermore, we will assume without loss of generality that $J_{\alpha,0,r} = J_{a^*,r}$ for every $a^* \in \mathcal{W}_\alpha$.

Put $H_j = g_{\alpha,r}$, $\lambda_{\alpha,0,r,1} = \mathrm{lc}_Z g_{\alpha,r}$, $\lambda_{\alpha,0,r,0} = 1$, and $\Phi_{\alpha,0,j} = Y_1 - ZY_0$ for every $j \in J_{\alpha,r}$, $0 \le r \le \rho_0$, see (v) and (vi) in the introduction.

Now we have $\Xi_{j,a^*} = \Xi_{a^*,r}$ and $W_{j,a^*,\xi} = W_{a^*,r,\xi}$ for every $j \in J_{\alpha,0,r}$, $a^* \in \mathcal{W}_\alpha$, see (vii) in the introduction.

Set $G_j = \delta_{\alpha,r}$ and $G_{j,i} = \delta_{\alpha,r,i}$ for $j \in J_{\alpha,0,r}$, $0 \le r \le \rho_0$, $0 \le i \le n$, see (ix) in the introduction.

The above definitions and the described construction imply the weakened modified version of Theorem 1 for $c = 0$ if condition $(\mathfrak{g})$ is fulfilled.

Therefore, by Theorem 3, the weakened modified version of Theorem 1 holds for $c = 0$ and for arbitrary $a_1, \dots, a_\nu$ and d' (when condition $(\mathfrak{g})$ is not necessarily fulfilled).

Assume that condition $(\mathfrak{g})$ does not necessarily hold. Denote by f the family of coefficients from $k[a_1, \dots, a_\nu]$ of all the polynomials $f_0, \dots, f_{m-1}$. Then, by Theorem 3 applied to the tree $T_{0,d_0,\dots,f_{m-1}}(f)$ (see the definition of this tree in Sec. 2), we obtain the weakened Theorem 1 for $c = 0$.

4. The general case. Preliminaries

Let s be an integer, $0 \le s \le n-1$. Recall that the finite sets of linear forms $\mathcal{M}_\varkappa$, $\mathcal{M}'_{s,\varkappa}$ are defined in the introduction, see (5). Let D be an integer, $D \ge 2$, and $\varkappa_3 = 2(n-s)D + s$, $\varkappa_4 = (n-s)D(D-1)/2$. Assume that the sets $\mathcal{M}_{\varkappa_3}$, $\mathcal{M}'_{s,\varkappa_4}$ exist (i.e., the field k contains sufficiently many elements). First of all, we need the following general result.

Lemma 7. *Let $V \subset \mathbb{P}^n(\overline{k})$ be a nonempty projective algebraic variety such that the dimension of each irreducible component of V is s and $\deg V \le D$. Then there is an element $(Y_0, \dots, Y_{s+1}) \in \mathcal{M}^{s+1}_{\varkappa_3} \times \mathcal{M}'_{s,\varkappa_4}$ satisfying the following properties.*

(a) *$V \cap \mathcal{Z}(Y_0, \dots, Y_s) = \varnothing$ in $\mathbb{P}^n(\overline{k})$, and there are $\lambda_1, \dots, \lambda_s \in \overline{k}$ such that the intersection $V \cap \mathcal{Z}(Y_1 - \lambda_1 Y_0, \dots, Y_s - \lambda_s Y_0)$ is transversal at each point. This implies that the morphism*

$$\pi_s : V \to \mathbb{P}^s(\overline{k}), \quad (X_0 : \dots : X_n) \mapsto (Y_0 : \dots : Y_s),$$

is finite dominant separable (or, which is the same by definition, the restriction of π_s to each irreducible component of V is a finite dominant separable morphism). Moreover, $\deg \pi_s = \deg V = \#(V \cap \mathcal{Z}(Y_1, \dots, Y_s)) = \#\pi_s^{-1}((1 : \lambda_1 : \dots : \lambda_s))$.

(b) *Let $\Phi_s \in \overline{k}[Y_0, \dots, Y_s, Z]$ be a nonzero polynomial of the smallest degree such that the polynomial $\Phi_s(Y_0, \dots, Y_{s+1})$ vanishes on V. Denote by $\Delta_s \in \overline{k}[Y_0, \dots, Y_s]$ the discriminant of Φ_s with respect to Z. Then $\deg_{Y_0,\dots,Y_s,Z} \Phi_s = \deg_Z \Phi_s = \deg V$ and $\Delta_s \ne 0$.*

Proof. (a) We will use induction on s. The base $s = 0$ is trivial. Let $s \ge 1$. There is a linear form $Y_0 \in \mathcal{M}_{\varkappa_3}$ such that $\dim V \cap \mathcal{Z}(Y_0) = s-1$. Note that for arbitrary $\mu_1, \dots, \mu_n \in \overline{k}$, for any pairwise distinct linear forms $L_1, \dots, L_n \in \mathcal{M}_{\varkappa_3} \setminus \{Y_0\}$, the linear forms $L_1 - \mu_1 Y_0, \dots, L_n - \mu_n Y_0$ are linearly independent over $\overline{k}$. For every irreducible (over $\overline{k}$) component E of V, choose a smooth point ξ_E of the algebraic variety V such that $\xi_E \in E \setminus \mathcal{Z}(Y_0)$. Thus the number of all chosen points ξ_E is at most D by the Bézout theorem. For every $L \in \mathcal{M}_{\varkappa_3}$, for every point ξ_E there is an element $\lambda_{L,E} \in \overline{k}$ such that $(L - \lambda_{L,E} Y_0)(\xi_E) = 0$.

For every point ξ_E there are at most $n - s$ pairwise distinct linear forms $L \in \mathcal{M}_{\varkappa_3} \setminus \{Y_0\}$ such that $L - \lambda_{L,E} Y_0$ vanishes on the tangent space of the algebraic variety V at the point ξ_E. Furthermore, for every irreducible (over $\overline{k}$) component E' of the algebraic variety $V \cap \mathcal{Z}(Y_0)$ there are at most $(n-1) - (s-1)$ linear forms $L \in \mathcal{M}_{\varkappa_3}$ such that L vanishes on E'.

Therefore, there is a linear form $Y_s \in \mathcal{M}_{\varkappa_3} \setminus \{Y_0\}$ such that $Y_s - \lambda_{Y_s,E} Y_0$ does not vanish on the tangent space of any chosen point ξ_E and Y_s does not vanish on any irreducible component E' of the algebraic variety $V \cap \mathcal{Z}(Y_0)$. Thus $\dim V \cap \mathcal{Z}(Y_0, Y_s) = s - 2$.

Furthermore, the intersection $E \cap \mathcal{Z}(Y_s - \lambda_{Y_s,E} Y_0)$ is transversal at each point ξ_E. Consider the morphism $\pi' : V \to \mathbb{P}^1(\overline{k})$, $(X_0 : \dots : X_n) \mapsto (Y_0 : Y_s)$. Denote by V' the set of points

$\xi \in V$ such that $d_\xi \pi' = 0$ or ξ is not a smooth point of V. The differential $d_{\xi_E}\pi'$ is not zero for every point ξ_E. Therefore, $\dim V' \leq s-1$.

Let E'' be an arbitrary irreducible (over $\overline{k}$) component of V' such that $\dim E'' = s-1$. We claim that there is at most one element $\mu \in \overline{k}$ such that E'' is an irreducible component of $V \cap \mathcal{Z}(Y_s - \mu Y_0)$. Indeed, otherwise $E'' \subset V \cap \mathcal{Z}(Y_0, Y_s)$. Since $\dim V \cap \mathcal{Z}(Y_0, Y_s) \leq s-2$, we obtain a contradiction.

Thus, there is $\lambda_s \in \overline{k}$ such that each irreducible component of $V \cap \mathcal{Z}(Y_s - \lambda_s Y_0)$ is not an irreducible component of V'. This implies that the intersection $V \cap \mathcal{Z}(Y_s - \lambda_s Y_0)$ is transversal, i.e., for every irreducible (over $\overline{k}$) component E''' of this intersection there is a smooth point $\xi \in E'''$ such that ξ is a smooth point of V and the intersection of the tangent spaces of V and $\mathcal{Z}(Y_s - \lambda_s Y_0)$ at ξ is transversal. Also, this implies that $\deg V = \deg V \cap \mathcal{Z}(Y_s - \lambda_s Y_0)$. Let us identify $\mathcal{Z}(Y_s - \lambda_s Y_0)$ with $\mathbb{P}^{n-1}(\overline{k})$. Now, replacing $(\mathbb{P}^n(\overline{k}), V, Y_0, \mathcal{M}_{\varkappa_3})$ by

$$(\mathbb{P}^{n-1}(\overline{k}), V \cap \mathcal{Z}(Y_s - \lambda_s Y_0), Y_0, \mathcal{M}_{\varkappa_3} \setminus \{Y_s\}),$$

we prove (a) applying the inductive assumption.

(b) There is a linear form $Y_{s+1} \in \mathcal{M}'_{s,\varkappa_4}$ such that

$$\#(Y_{s+1}/Y_0)(V \cap \mathcal{Z}(Y_1 - \lambda_1 Y_0, \ldots, Y_s - \lambda_s Y_0)) = \deg V.$$

By the Bézout theorem, for this linear form Y_{s+1} assertion (b) holds (we leave the details to the reader). The lemma is proved. □

Remark 7. Let V be a projective algebraic variety from the statement of Lemma 7 and $Y_0, \ldots, Y_s \in \overline{k}[X_0, \ldots, X_n]$ be arbitrary linear forms. Now, $V \cap \mathcal{Z}(Y_0, \ldots, Y_s) = \varnothing$ in $\mathbb{P}^n(\overline{k})$ if and only if the morphism π_s is finite dominant (this is well known). We would like to emphasize again that if the morphism π_s is finite dominant separable, then assertion (a) of Lemma 7 is fulfilled automatically. The proof of the last fact is straightforward using the Bézout theorem.

Let V be a projective algebraic variety from the statement of Lemma 7. Assume that $Y_0, \ldots, Y_s \in k[X_0, \ldots, X_n]$ are linear forms such that $V \cap \mathcal{Z}(Y_0, \ldots, Y_s) = \varnothing$ in $\mathbb{P}^n(\overline{k})$ and $Y_0, \ldots, Y_s, X_{s+1}, \ldots, X_n$ are linearly independent over k. Let t be a transcendental element over k.

Assume that $s \leq n-1$. Let $Y \in k[X_0, \ldots, X_n]$ be a linear form such that $Y_0, \ldots, Y_s, Y$ are linearly independent over k. Denote by $\Phi_Y \in \overline{k}[Y_0, \ldots, Y_s, Z]$ the nonzero polynomial of the smallest degree (in $Y_0, \ldots, Y_s, Z$) such that $\mathrm{lc}_Z \Phi_Y = 1$ and the polynomial $\Phi_Y(Y_0, \ldots, Y_s, Y)$ vanishes on the algebraic variety V. If $s = n-1$, then, obviously, $V = \mathcal{Z}(\Phi_Y(Y_0, \ldots, Y_s, Y))$ in $\mathbb{P}^n(\overline{k})$.

Let $s \leq n-2$. Let $Y \in \mathcal{M}'_{s,\varkappa_4}$ and i be an integer such that $s+2 \leq i \leq n$. Denote by $\Phi_{Y,i} \in \overline{k}[t, Y_0, \ldots, Y_s, Z]$ the nonzero polynomial of the smallest degree (in $t, Y_0, \ldots, Y_s, Z$) such that $\mathrm{lc}_Z \Phi_{Y,i} = 1$ (see Remark 7) and the polynomial

$$\Phi_{Y,i}(t, Y_0, \ldots, Y_s, Y + tX_i)$$

vanishes on the algebraic variety V. Let $\widetilde{\Phi} \in \overline{k}[t, Y_0, \ldots, Y_s, Z]$ be a polynomial such that $\mathrm{lc}_Z \widetilde{\Phi} \in \overline{k}$ and the square-free parts of the polynomials $\widetilde{\Phi}$ and $\Phi_{Y,i}$ coincide (i.e., they have the same sets of factors irreducible over $\overline{k}$). Then, for brevity, we will say that *the polynomial* $\widetilde{\Phi}$ *satisfies the property of the square-free part minimality for the ground field* k*, the algebraic variety* V*, and the linear forms* $Y_0, \ldots, Y_s, Y, X_i$.

Let $\widetilde{\Phi}_{Y,i} \in \overline{k}[t, Y_0, \ldots, Y_s, Z]$ be a polynomial satisfying the property of the square-free part minimality for the ground field k, the algebraic variety V, and the linear forms $Y_0, \ldots, Y_s, Y, X_i$.

Assume additionally that $\mathrm{lc}_Z\widetilde{\Phi}_{Y,i}=1$. Let us represent this polynomial in the form

$$\widetilde{\Phi}_{Y,i}(t,Y_0,\dots,Y_s,Y+tX_i)=\sum_{0\le j\le \deg_Z\widetilde{\Phi}_{Y,i}}\widetilde{\Phi}_{Y,i,j}t^j$$

where $\widetilde{\Phi}_{Y,i,j}\in\overline{k}[Y_0,\dots,Y_s,Y,X_i]$ (note that now the linear forms $Y_0,\dots,Y_s,Y,X_i$ are linearly independent over $\overline{k}$).

Lemma 8. *Let V be a nonempty projective algebraic variety from the statement of Lemma 7. Assume that $Y_0,\dots,Y_s\in k[X_0,\dots,X_n]$ are linear forms such that $V\cap\mathcal{Z}(Y_0,\dots,Y_s)=\varnothing$ in $\mathbb{P}^n(\overline{k})$ and $Y_0,\dots,Y_s,X_{s+1},\dots,X_n$ are linearly independent over k. Assume that $\deg_Z\widetilde{\Phi}_{Y,i}\le\widetilde{D}$. Let $0\le s\le n-2$. Then, in the above notation,*

$$V=\mathcal{Z}(\widetilde{\Phi}_{Y,i,j},\ Y\in\mathcal{M}'_{\varkappa_4},\ s+2\le i\le n,\ 0\le j\le\deg_Z\widetilde{\Phi}_{Y,i}),\tag{25}$$

i.e., the variety V is the set of all common zeros in $\mathbb{P}^n(\overline{k})$ of the system of homogeneous polynomial equations $\widetilde{\Phi}_{Y,i,j}=0$ for all Y, i, j. The number of equations in this system is bounded from above by $(n-s-1)\widetilde{D}(1+(n-s)D(D-1)/2)$. The degrees of these equations are bounded from above by $\widetilde{D}$.

Proof. Let V_1 be the projective algebraic variety from the right-hand side of (25). Obviously, $V\subset V_1$. We need to prove that $V\supset V_1$. Let $\xi=(\xi_0:\ldots:\xi_n)\in V_1$ and $\xi_i\in\overline{k}$ for all i. Performing if necessary a permutation of the linear forms $Y_0,\dots,Y_s$, we will assume without loss of generality that $Y_0(\xi)\ne0$. Put $\xi'=(1:(Y_1/Y_0)(\xi):\ldots:(Y_s/Y_0)(\xi))\in\mathbb{P}^s(\overline{k})$ and $\Xi=\pi_s^{-1}(\xi')$. Thus $\#\Xi\le D$. There is a linear form $Y_\xi\in\mathcal{M}'_{\varkappa_4}$ such that $\#(Y_\xi/Y_0)(\Xi)=\#\Xi$.

By Remark 7 and the properties of $\Phi_{Y,i}$ and $\widetilde{\Phi}_{Y,i}$, there is a point $\xi^{(i)}\in\Xi$ such that $(Y_\xi/Y_0)(\xi^{(i)})+t(X_i/Y_0)(\xi^{(i)})=(Y_\xi/Y_0)(\xi)+t(X_i/Y_0)(\xi)$ for $s+2\le i\le n$. This implies that $(Y_\xi/Y_0)(\xi^{(i)})=(Y_\xi/Y_0)(\xi)$ and $(X_i/Y_0)(\xi^{(i)})=(X_i/Y_0)(\xi)$ for $s+2\le i\le n$. By the choice of Y_ξ, we have $\xi^{(i_1)}=\xi^{(i_2)}$ for $s+2\le i_1,i_2\le n$. Put $\xi''=\xi^{(s+2)}\in V$. Then we have $(Y_i/Y_0)(\xi)=(Y_i/Y_0)(\xi'')$ for $1\le i\le s$, $(Y_\xi/Y_0)(\xi)=(Y_\xi/Y_0)(\xi'')$ and $(X_i/Y_0)(\xi)=(X_i/Y_0)(\xi'')$ for $s+2\le i\le n$. But the linear forms $Y_0,\dots,Y_s,Y_\xi,X_{s+2},\dots,X_n$ are linearly independent over k. This implies that $\xi=\xi''\in V$. The last two assertions of the lemma about estimates on the number of equations and the degrees are obvious. The lemma is proved. □

Let c be an enteger, $-1\le c\le n$. Now we are going to describe some preliminary algorithm (with enumerations, see Sec. 2). For brevity, write $f_{a^*,i}=f_i(a^*,X_0,\dots,X_n)$, $0\le i\le m-1$. Applying Lemma 3 from Sec. 1 to the family of polynomials $X_j^{d_0-d_i}f_{a^*,i}$, $0\le j\le n$, $0\le i\le m-1$, we find a maximal subfamily $\{X_{j_\gamma}^{d_0-d_{i_\gamma}}f_{a^*,i_\gamma}\}$, $1\le\gamma\le N$, of this family linearly independent over k. Then $N\le\binom{n+d}{n}$. Put $I_{a^*}=\{i_\gamma:1\le\gamma\le N\}$. Then, obviously, $\mathcal{Z}(f_{a^*,0},\dots,f_{a^*,m-1})=\mathcal{Z}(f_{a^*,i},\ i\in I_{a^*})$. Thus, replacing if necessary the family of polynomials $f_{a^*,0},\dots,f_{a^*,m-1}$ by $\{f_{a^*,i}\}_{i\in I_{a^*}}$, in what follows we will assume without loss of generality that $m\le\binom{n+d}{n}$. If $a^*\in\mathcal{U}_c$, then, obviously, $m\ge n-c$.

If $c=n$, then properties (α_{n-c}) and (β_{n-c}) are trivially fulfilled, see below. Further in this section, we assume that $c<n$.

Assume that $c=-1$. Then put $Y_i=X_i$ for $0\le i\le n$.

Assume that $0\le c\le n-1$. We assume that the field k contains sufficiently many elements, and hence the set of linear forms $\mathcal{L}_c$ (defined in the introduction) exist.

Let $a^*\in\mathcal{U}_c$. Using an enumeration and the construction of Sec. 3, we find an element $(Y_0,\dots,Y_c)\in\mathcal{L}_c^{c+1}$ (it depends on a^*) such that $V_{a^*}\cap\mathcal{Z}(Y_0,\dots,Y_c)=\varnothing$, see Lemma 7(a).

Put $Y_i = X_i$ for $c+1 \le i \le n$. Then the linear forms $Y_0, \dots, Y_n$ are linearly independent over k.

Now let us return to the case $-1 \le c \le n-1$. Our aim is to construct polynomials $h_{a^*,1}, \dots, h_{a^*,n-c}$ satisfying the following properties.

(α_{n-c}) For every i, $1 \le i \le n-c$,

$$h_{a^*,i} = f_{a^*,i-1} + \sum_{i \le w \le m-1} q_{a^*,i,w} f_{a^*,w},$$

where $q_{a^*,i,w} \in k[X_0, \dots, X_n]$ are homogeneous polynomials of degrees $\deg_{X_0,\dots,X_n} q_{a^*,i,w} = d_w - d_{i-1}$.

(β_{n-c}) $\dim \mathcal{Z}(h_{a^*,1}, \dots, h_{a^*,n-c}) = c$.

Hence $V_{a^*,c}$ is a union of some irreducible components of the algebraic variety

$$\mathcal{Z}(h_{a^*,1}, \dots, h_{a^*,n-c}).$$

Remark 8. Let $\nu = 0$ (so a^* can be omitted in the notation). In [2, Chap. 2, Sec. 3], the construction of $h_1, \dots, h_{n-c}$ (in that paper, the notation m in place of $n-c$ is used) with "inessential components" (see Lemma 2.11 in [2]) is inaccurate. One should delete this lemma. But the required correction is short and simple. It is given in the thesis [7, p. 221] (note that the case where $d_i = d$ for all i is considered in [7] and [2], and then there are simplifications). In this paper, we follow [7] with small modifications in this place.

Assume that $1 \le j \le n-c+1$. Consider the following property:

(γ_{j-1}) $\mathcal{Z}(h_{a^*,1}, \dots, h_{a^*,j-1}) \cap \mathcal{Z}(Y_0, Y_1, \dots, Y_{n-j+1}) = \varnothing$ in $\mathbb{P}^n(\overline{k})$.

(Here, if $j = 1$, then the sequence $h_{a^*,1}, \dots, h_{a^*,j-1}$ is empty and $\mathcal{Z}(h_{a^*,1}, \dots, h_{a^*,j-1}) = \mathbb{P}^n(\overline{k})$.) Note that if properties (α_{n-c}) and (γ_{n-c}) hold, then (α_{n-c}) and (β_{n-c}) are also satisfied.

Let $1 \le j \le n-c$. Assume that polynomials $h_{a^*,1}, \dots, h_{a^*,j-1}$ satisfying properties (α_{j-1}) and (γ_{j-1}) have been constructed recursively (for the recursion base $j = 1$, nothing has been constructed). We are going to construct a polynomial $h_{a^*,j}$ such that properties (α_j), (γ_j) hold.

By (γ_{j-1}), we have $\dim \mathcal{Z}(h_{a^*,1}, \dots, h_{a^*,j-1}, Y_0, Y_1, \dots, Y_{n-j}) = 0$. Hence

$$E_{j-1} = \mathcal{Z}(h_{a^*,1}, \dots, h_{a^*,j-1}, Y_0, Y_1, \dots, Y_{n-j})$$

is a finite set. We have $E_{j-1} \cap V_{a^*} = \varnothing$, since $n-j \ge c$ and $V_{a^*} \cap \mathcal{Z}(Y_0, \dots, Y_c) = \varnothing$. Therefore, by property (α_{j-1}), also

$$E_{j-1} \cap \mathcal{Z}(f_{a^*,j-1}, \dots, f_{a^*,m-1}) = \varnothing.$$

Now we will find recursively indices $j-1 \le j_1 < \dots < j_{m'} \le m$ such that $m' \le \#E_{j-1} \le D'_{j-1}$ (the integer D'_{j-1} is defined in the introduction) and

$$E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_{m'}}) = \varnothing.$$

Namely, let $1 \le i \le m-2$ and $E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_{i-1}}) \ne \varnothing$. Then we set

$$j_i = \sup\{w : E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_{i-1}}, f_{a^*,w}, f_{a^*,w+1}, \dots, f_{a^*,m-1}) = \varnothing\}.$$

We use the construction of Sec. 3 to find the index j_i. Obviously,

$$E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_{i-1}}) \ne E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_i}).$$

If $E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_i}) = \varnothing$, then put $m' = i$, and the required indices are constructed.

Let t be a transcendental element over k. Set $q_{j,i} = 0$ if $j \le i \le m-1$ and $i \notin \{j_1, \dots, j_{m'}\}$. Put

$$q_{j,j_w} = \sum_{1 \le u \le j} t^{j(w-1)+u} Y_{n-j+u}^{d_{j-1}-d_{j_w}}, \quad 1 \le w \le m', \tag{26}$$

and

$$\widetilde{h}_{a^*,j} = \sum_{j \le w \le m-1} q_{j,w} f_{a^*,w} \in \overline{k}[t, X_0, \ldots, X_n]. \tag{27}$$

Then $0 \neq \widetilde{h}_{a^*,j}(\eta) \in \overline{k}[t]$ for every $\eta \in E_{j-1}$. We have $\deg_t \widetilde{h}_{a^*,j} \le jm' \le jD'_{j-1}$.

Set $\beta_j = jm' D'_{j-1}$. Recall that $\mathcal{I}_{\beta_j}$ denotes a subset of $k \setminus \{0\}$ with $\#\mathcal{I}_{\beta_j} = \beta_j + 1$. It follows that there is an element $t_{a^*,j} \in \mathcal{I}_{\beta_j}$ such that $\widetilde{h}_{a^*,j}(t_{a^*,j}, \eta_0, \ldots, \eta_n) \neq 0$ for every $\eta = (\eta_0 : \ldots : \eta_n) \in E_{j-1}$. Put $h_{a^*,j} = \widetilde{h}_{a^*,j}(t_{a^*,j}, X_0, \ldots, X_n)$ and $q_{a^*,j,w} = q_{j,w}|_{t=t_{a^*,j}}$ for all w. Then properties (α_j), (γ_j) hold.

One can find a required element $t_{a^*,j}$ enumerating the elements $t' \in \mathcal{I}_{\beta_j}$ and deciding whether

$$\mathcal{Z}(h_{a^*,1}, \ldots, h_{a^*,j-1}, \widetilde{h}_{a^*,j}(t', X_0, \ldots, X_n), Y_0, \ldots, Y_{n-j}) = \varnothing$$

using the construction of Sec. 3. The recursion for obtaining $h_{a^*,1}, \ldots, h_{a^*,n-c}$ is completely described. Note that simultaneously we obtain all the polynomials $q_{a^*,j,w}$ and all the elements $t_{a^*,j} \in \mathcal{I}_{\beta_j}$.

Translated by A. L. Chistov.

REFERENCES

1. A. Ayad, "Complexity of solving parametric polynomial systems," *Zap. Nauchn. Sem. POMI*, **387**, 5–52 (2011).
2. A. L. Chistov, "Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time," *J. Sov. Math.*, **34**, No. 4, 1838–1882 (1986).
3. A. L. Chistov, "An improvement of the complexity bound for solving systems of polynomial equations," *Zap. Nauchn. Sem. POMI*, **390**, 299–306 (2011).
4. A. L. Chistov, "A bound for the degree of a system of equations determining the variety of reducible polynomials," *St. Petersburg Math. J.*, **24**, No. 3, 513–528 (2013).
5. A. L. Chistov, "Computations with parameters: a theoretical background," *J. Math. Sci.*, **215**, No. 6, 769–781 (2016).
6. A. L. Chistov, "Efficient absolute factorization of polynomials with parametric coefficients," *J. Math. Sci.*, **224**, No. 2, 360–384 (2017).
7. A. L. Chistov, "Efficient algorithms for factorization of polynomials and their applications," *Doctor of Sciences Thesis*, Leningrad (1987).
8. A. L. Chistov, H. Fournier, L. Gurvits, and P. Koiran, "Vandermonde matrices, NP-completeness, and transversal subspaces," *Found. Comput. Math.*, **3**, No. 4, 421–427 (2003).
9. D. Lazard and F. Rouillier, "Solving parametric polynomial systems", *J. Symbolic Comput.*, **42**, No. 6, 636–667 (2007).
10. D. Lazard, "Résolution des systémes d'équations algébriques," *Theoret. Comput. Sci.*, **15**, 77–110 (1981).
11. D. Lazard, "Commutative algebra and computer algebra", *Lect. Notes Comput. Sci.*, **144**, 40–48 (1983).