SPb. Math. Society Preprint 2004-07 16 Oct 2004

Polynomial–time computation of the degree of a dominant morphism in zero–characteristic I

Alexander L. Chistov

St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia
14th line 39, St. Petersburg 199178, Russia,
e-mail: labta@iias.spb.su or sliss@iias.spb.su

2004

Abstract

Consider a projective algebraic variety W which is an irreducible component of a set of all common zeroes of a family of homogeneous polynomials of degrees less than d in $n+1$ variables in zero–characteristic. We show how to compute the degree of a dominant rational morphism from W to W'. The morphism is given by homogeneous polynomials of degree d'. This algorithms is deterministic and polynomial in $(dd')^n$ and the size of input.

Introduction

Let k be a field of zero–characteristic with algebraic closure $\overline{k}$. Let $X_0, X_1, \ldots$ be independent variables over k. In the algorithms we shall suppose that k is finitely generated over the field of rational numbers $\mathbb{Q}$. Denote by $\mathbb{P}^n(\overline{k})$ the projective space over the field $\overline{k}$ with coordinates $X_0, \ldots, X_n$. We shall suppose that $\mathbb{P}^n(\overline{k})$ is defined over k. For arbitrary homogeneous polynomials $g_1, \ldots, g_m \in \overline{k}[X_0, \ldots, X_n]$ denote by $\mathcal{Z}(g_1, \ldots, g_m)$ the set of all common zeroes of polynomials $g_1, \ldots, g_m$ in $\mathbb{P}^n(\overline{k})$. The similar notations will be used for the sets of zeroes of ideals and polynomials with other fields of coefficients in affine and projective spaces (this will be seen from the context).

Let $V \subset \mathbb{P}^n(\overline{k})$ be a projective algebraic variety which is a set of all common zeroes of a family of homogeneous polynomials in $n+1$ variables of degrees less than d with coefficients from a field k. Let W be a defined over k and irreducible over k component of V and W is given by its point which belongs to only one irreducible over k component of V, see [8], Theorem 1 and also below for details. Let $e_0, \ldots, e_r \in k[X_0, \ldots, X_n]$, be homogeneous polynomials such that $\deg e_i = d' \geq 1$ for every nonzero e_i, $0 \leq i \leq r$. We shall suppose in what follows that $\dim W \cap \mathcal{Z}(e_0, \ldots, e_r) < \dim W$. Let

$$p : W \setminus \mathcal{Z}(e_0, \ldots, e_r) \to \mathbb{P}^r, \quad (X_0 : \ldots : X_n) \mapsto (e_0 : \ldots : e_r) \tag{1}$$

be the regular morphism. Set $W' = \overline{p(W \setminus \mathcal{Z}(e_0, \ldots, e_r)}$ (here and below in the similar situations the bar denotes closure with respect to the Zariski topology). Hence W' is irreducible over k closed subvariety of $\mathbb{P}^r(\overline{k})$. Note that one can consider the rational morphism $W \to \mathbb{P}^r(\overline{k})$ of projective algebraic varieties given by the same rule but to be more accurate in what follows we deal with regular morphisms of quasiprojective algebraic varieties. Denote by

$$p' : W \setminus \mathcal{Z}(e_0, \ldots, e_r) \to W'$$

the dominant morphism induced by p. Suppose that $\dim W = \dim W'$ (we can verify this fact using [6], see below). Then we construct an algorithm to compute the degree $\deg p'$ within the time polynomial in $(dd')^n$ and the size of input. Even more general results are obtained, see Theorem 1.

Notice that the probabilistic algorithm polynomial in $(dd')^n$ and the size of input for computing the degree of a dominant morphism is easy in arbitrary characteristic of the ground field. The difficulties arise when one consider the most important model of deterministic computations with bitwise complexity, cf. the Introduction of [6].

In [6] we described an algorithm to decide whether a morphism p is dominant. The considered algorithm is polynomial in $(dd')^n$ and the size of input. We shall apply this algorithm as a base in the present paper. But computing the degree of a dominant morphism is a much more difficult problem than ones considered in [6]. Now we use essentially the results of [8] and [7].

For every $0 \leq s \leq n$ denote by V_s the union of all the irreducible components of dimension $n-s$ of V. According to [8], Theorem 1 one can construct within the time polynomial in d^n and the size of input for every $0 \leq s \leq n$ a zero–dimensional or empty projective algebraic variety $V_{s,0}$ such that all the points of $V_{s,0}$ are smooth points of dimension $n-s$ of V and the irreducible over k components of V_s and $V_{s,0}$ are in the one–to–one correspondence by the

rule $W \mapsto W \cap V_{s,0}$, see the details in [8]. So we shall assume that all $V_{s,0}$, $0 \le s \le n$, are constructed. For every $z \in V_{s,0}$ denote by W_z the uniquely defined irreducible over k component of V such that $z \in W_z$. We shall use also Theorem 2 from [8] which allow us to decide within the time polynomial in d^n and the size of input whether two (or more) given points are from the same irreducible over k (or irreducible over $\overline{k}$) component of V, see the details in the cited theorem. On the other hand we need to attract [7]. We discuss the results of this paper and deduce from them some new corollaries in Section 1.

Notice also one correction in the statement of Lemma 2 from [8]. One needs to replace there "a solution from $\mathbb{A}^{4n+4}(\overline{k}_4)$ ..." by "a solution from $\mathbb{A}^{4n+4}(\overline{k}_4)$ giving a point from $V_s^4(\overline{k}_4)$ ...". The proof is without changes. To find such a solution in the algorithm for Theorem 1 [8] one needs only to apply the results of [7]. It can be done directly, or one can use there Theorem 2 Section 1 of the present paper replacing all the inequalities of system (7) [8] by nonstrict.

Now we proceed to the precise statements. Let homogeneous polynomials $f_1, \ldots, f_m \in k[X_0, \ldots, X_n]$ be given, $n \ge 1$, $m \ge 1$. Consider the closed algebraic set or algebraic variety (in this paper we do not distinguish these two concepts)

$$V = \{(x_0 : \ldots : x_n) : \ f_i(x_0, \ldots, x_n) = 0, \ x_i \in \overline{k}, \ \forall 1 \le i \le m\} \subset \mathbb{P}^n(\overline{k}) \, .$$

This is a set of all common zeros of polynomials $f_1, \ldots, f_m$ in $\mathbb{P}^n(\overline{k})$, where $\overline{k}$ is an algebraic closure of k. Hence $V = \mathcal{Z}(f_1, \ldots, f_m)$. Let $r \ge 0$ be an integer and $e_0, \ldots, e_r \in k[X_0, \ldots, X_n]$ be homogeneous polynomials such that the degree $\deg_{X_0,\ldots,X_n} e_j = d'$ if $e_j \ne 0$ for every $0 \le j \le r$.

Now let the field $k = \mathbb{Q}(t_1, \ldots, t_l, \theta)$ where $t_1, \ldots, t_l$ are algebraically independent over the field $\mathbb{Q}$ and θ is algebraic over $\mathbb{Q}(t_1, \ldots, t_l)$ with the minimal polynomial $F \in \mathbb{Q}[t_1, \ldots, t_l, Z]$ and leading coefficient $\mathrm{lc}_Z F$ of F is equal to 1. We shall represent each polynomial $f = f_i$ (and similarly e_j) in the form

$$f = \frac{1}{a_0} \sum_{i_0,\ldots,i_n} \sum_{0 \le j < \deg_Z F} a_{i_0,\ldots,i_n,j} \theta^j X_0^{i_0} \cdots X_n^{i_n} \, ,$$

where $a_0, a_{i_0,\ldots,i_n,j} \in \mathbb{Z}[t_1, \ldots, t_l]$, $\mathrm{G\,C\,D}_{\,i_0,\ldots,i_n,j}(a_0, a_{i_0,\ldots,i_n,j}) = 1$. Define the length $\mathrm{l}(a)$ of an integer a by the formula $\mathrm{l}(a) = \min\{s \in \mathbb{Z} : \ |a| < 2^{s-1}\}$. The length of coefficients $\mathrm{l}(f)$ of the polynomial f is defined to be the maximum of lengths of coefficients from $\mathbb{Z}$ of polynomials $a_0, a_{i_0,\ldots,i_n,j}$ and the degree

$$\deg_{t_\gamma}(f) = \max_{i_0,\ldots,i_n,j} \{\deg_{t_\gamma}(a_0), \deg_{t_\gamma}(a_{i_0,\ldots,i_n,j})\} \, ,$$

where $1 \le \gamma \le l$. In the similar way we shall define degrees and lengths of integer coefficients of other polynomials, in particular $\deg_{t_\gamma} F$ and $\mathrm{l}(F)$ are defined. We shall suppose that we have the following bounds:

$$\begin{aligned}
&\deg_{X_0,\ldots,X_n}(f_i) < d, \ \deg_{t_\gamma}(f_i) < d_2, \ \mathrm{l}(f_i) < M, \\
&\deg_{X_0,\ldots,X_n}(e_j) = d' \text{ or } e_j = 0, \ \deg_{t_\gamma}(e_j) < d_2', \ \mathrm{l}(e_j) < M', \\
&\deg_Z(F) < d_1, \ \deg_{t_\gamma}(F) < d_1, \ \mathrm{l}(F) < M_1 \, .
\end{aligned}$$

for all $1 \le i \le m$, $0 \le j \le r$, $1 \le \gamma \le l$. The size $\mathrm{L}(f)$ of the polynomial f is defined to be the product of $\mathrm{l}(f)$ to the number of all the coefficients from $\mathbb{Z}$ of

f in the dense representation. We have

$$\mathrm{L}(f_i) < (\binom{d+n}{n} d_1 + 1) d_2^l M$$

Similarly $\mathrm{L}(F) < d_1^{l+1} M_1$.

REMARK 1 *Unless we state otherwise, in what follows we suppose l to be fixed. The working time of the algorithm from Theorem 1, see below, is essentially the same as for solving systems of polynomial equations with a finite set of solutions in the projective space. So this theorem can be formulated also in the case when l is not fixed, see [2]. Notice that the constants $O(\ldots)$, see Theorem 1 and lemmas below, in the estimate of the lengths of integer coefficients of linear forms L'_j, L_j are absolute; they does not depend on l.*

We shall represent a point $z \in V$ with coordinates from a finite extension of k as follows. An index $0 \le i_0 \le n$ is known such that $X_{i_0}(z) \neq 0$ and an isomorphism of fields

$$k(z) = k((X_1/X_{i_0})(z), \ldots, (X_n/X_{i_0})(z)) = k[\eta] \simeq k[Z]/(\Phi) \tag{2}$$

is given where $\eta = \sum_{0 \le i \le n} c_i (X_i/X_{i_0})(z)$, the coefficients $c_i \in \mathbb{Z}$ are given and $\Phi \in k[Z]$ is minimal polynomial of η over k with leading coefficient $\mathrm{lc}_Z \Phi = 1$ (so the point z is defined up to a conjugation over k).

Let $a \in k[\eta]$ be an arbitrary element. Then $a = A(\eta)$ for the uniquely defined polynomial $A \in k[Z]$ such that $\deg_Z A < \deg_Z \Phi$. The length of integer coefficients $\mathrm{l}(a)$, the the size $\mathrm{L}(a)$ and the degrees $\deg_{t_\alpha} a$, $1 \le \alpha \le l$, of a are defined by the formulas

$$\mathrm{l}(a) = \mathrm{l}(A), \quad \mathrm{L}(a) = \mathrm{L}(A), \quad \deg_{t_\alpha} a = \deg_{t_\alpha} A.$$

Let us define the size of the point z to be $\mathrm{L}(\Phi) + \sum_{0 \le i \le n} \mathrm{L}(X_i/X_{i_0})$.

Let $W_1, W_2 \subset \mathbb{P}^n(\overline{k})$ be two quasiprojective algebraic varieties defined over k. Let W_3 be a defined over k and irreducible over k component of $W_1 \cap W_2$. We shall say that the intersection $W_1 \cap W_2$ is transversal at W_3 if and only if there is a point $x \in W_3$ such that x is a smooth point of every W_i, $i = 1, 2$, and the intersection of tangent spaces $T_{x,W_1} \cap T_{x,W_2}$ of W_1 and W_2 at the point x is transversal, i.e., $\dim(T_{x,W_1} \cap T_{x,W_2}) = n - \dim(T_{x,W_1}) - \dim(T_{x,W_2})$. We shall say that the intersection $W_1 \cap W_2$ is transversal if and only if it is transversal at every its defined over k and irreducible over k component. In the similar way one defines transversality for intersection of a finite number of algebraic varieties.

Suppose that the dimension $\dim W = \dim W'$. Denote by $W'' \subset W'$ the subset of all points $z \in W'$ such that the number of elements $\#p^{-1}(z) \neq \deg p'$ or z is a singular point of W'. Then since the set of all singular points of W' is closed and by Lemma 2, see below, W'' is closed with respect to the Zariski topology in W' and $W'' \neq W'$. Denote by W''' the closure in the Zariski topology of all points $z \in W'$ such that $\dim p^{-1}(z) > 0$. So $W''' \subset W''$.

Denote by $W^{(4)}$ the closure in the Zariski topology of the union of all irreducible components E of $p^{-1}(W''')$ such that the dimension of closure $\dim \overline{p(E)} < \dim E$. Therefore, the closure

$$\overline{p(W^{(4)} \setminus \mathcal{Z}(e_0, \ldots, e_r))} = W'''.$$

Further, $p^{-1}(W''') \neq W \setminus \mathcal{Z}(e_0,\ldots,e_r)$. Hence $\dim W^{(4)} = \dim p^{-1}(W''') \leq \dim(W)-1$ and $\dim W''' \leq \dim(W)-2$. Denote by $p^{(4)} : W^{(4)} \setminus \mathcal{Z}(e_0,\ldots,e_r) \to W'''$ the restriction of p'. By the theorem about dimension of fibers, see [11], for every $z \in W'''$ the dimension of every irreducible component (if it exists, $(p^{(4)})^{-1}(z)$ may be empty) of $(p^{(4)})^{-1}(z)$ is at least 1. Hence the quasiprojective algebraic variety $W^{(4)} \setminus \mathcal{Z}(e_0,\ldots,e_r)$ is exactly the set of all points $x \in W \setminus \mathcal{Z}(e_0,\ldots,e_r)$ such that for every irreducible component E of the fiber $p^{-1}p(x)$ if $x \in E$ then $\dim E > 0$.

THEOREM 1 *Let the field k, the algebraic variety V and the polynomials F, $f_1,\ldots,f_m$ and $e_0,\ldots,e_r$ be given as above. Let a point $x^{(0)} \in V$ be given and $x^{(0)}$ belong to only one irreducible over k component W of V. Let W' be as above, see (1). Then one can compute* $\dim W$ *and* $\dim W'$. *Suppose that* $\dim W = \dim W' = n-s$ *where* $0 \leq s \leq n$. *Then the following assertions holds.*

(a) One can compute the degree $\deg p'$ *of the morphism* $p' : W \setminus \mathcal{Z}(e_0,\ldots,e_r) \to W'$ *induced by (1).*

(b) More precisely, one can compute indices $0 \leq i_0 < \ldots < i_{n-s} \leq r$ such that e_{i_0} does not vanish on W and the family $e_{i_1}/e_{i_0},\ldots,e_{i_{n-s}}/e_{i_0}$ is a basis of transcendency of the field of rational functions $k(W)$ over k. We shall suppose for convenience of notation that $i_j = j$ for all j. Denote by $\rho : W \setminus \mathcal{Z}(e_0,\ldots,e_{n-s}) \to \mathbb{P}^{n-s}(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (e_0 : \ldots : e_{n-s})$ the regular dominant morphism. Then one can construct a point $z' = (1 : z'_1 : \ldots : z'_{n-s}) \in \mathbb{P}^{n-s}(\overline{k})$ such that all z'_j are integers with lengths $O(n \log d + (n-s)\log(d'))$; the number of elements (here and below # denotes the number of elements of a set) $\#\rho^{-1}(z') = \deg \rho$; the number of elements $\#p(\rho^{-1}(z')) = (\deg \rho)/(\deg p')$; all the points of $\rho^{-1}(z')$ are smooth points of V; all the points of $p(\rho^{-1}(z'))$ are smooth points of W'. Further, one can construct the sets $\rho^{-1}(z')$ and $p(\rho^{-1}(z'))$. For an arbitrary $z^{(1)} \in p(\rho^{-1}(z'))$ the number of elements $\#(p')^{-1}(z^{(1)}) = \deg p'$, cf. Lemma 2, Section 2, and every point from $(p')^{-1}(z^{(1)})$ belongs to the unique irreducible over k component of V, i.e., only to W.

(c) One can compute the degree $\deg W'$. *More precisely, one can construct linear forms $L'_0, L'_{s+1}, L'_{s+2}, \ldots, L'_n \in k[X_0,\ldots,X_r]$ satisfying the following properties. Set $e'_j = L'_j(e_0,\ldots,e_r)$, $j \in \{0, s+1,\ldots,n\}$. Then*

$$\#\big((W \setminus \mathcal{Z}(e_0,\ldots,e_r)) \cap \mathcal{Z}(e'_{s+1},\ldots,e'_n)\big) = \deg(p')\deg W', \quad (3)$$

$$(W \setminus \mathcal{Z}(e_0,\ldots,e_r)) \cap \mathcal{Z}(e'_0,e'_{s+1},\ldots,e'_n) = \emptyset, \quad (4)$$

$$(W \setminus \mathcal{Z}(e_0,\ldots,e_r)) \cap \mathcal{Z}(e'_{s+1},\ldots,e'_n) \cap (\overline{V \setminus W}) = \emptyset, \quad (5)$$

$$\#\big(W' \cap \mathcal{Z}(L'_{s+1},\ldots,L'_n)\big) = \deg W'. \quad (6)$$

Hence, (3), (6) and Lemma 2, see below, imply that for every point $x' \in W' \cap \mathcal{Z}(L'_{s+1},\ldots,L'_n)$ the number of elements $\#(p')^{-1}(x') = \deg p'$. Therefore, each point of the intersection in the right part of (6) is a smooth points of W', and this intersection is transversal at each its point. Further, again by Lemma 2 each point x of the intersection in the right part of (3) is a smooth point of the varieties W, $\mathcal{Z}(e'_{s+1}),\ldots,\mathcal{Z}(e'_n)$ simultaneously and the intersection of tangent spaces of these $n-s+1$ projective algebraic

varieties at x is transversal, i.e., is $\{0\}$. Besides that, (4), (3), (6) and Lemma 2 imply

$$W' \cap \mathcal{Z}(L'_0, L'_{s+1}, \ldots, L'_n) = \emptyset. \tag{7}$$

The constructed linear forms $L'_0, L'_{s+1}, L'_{s+2}, \ldots, L'_n$ have integer coefficients of length

$$O(n \log d + (n-s)\log(d')).$$

One can construct also all the points from the intersections in the right parts of (6), (3).

(d) *Let us identify the set of $(n-s+1)$–tuples of linear forms from $\overline{k}[X_0, \ldots, X_r]$ with $\mathbb{A}^{(r+1)(n-s+1)}(\overline{k})$. Then by Lemma 2 the set $\mathcal{U}'_0$ of all $(L''_0, L''_{s+1}, L''_{s+2}, \ldots, L''_n) \in \mathbb{A}^{(r+1)(n-s+1)}(\overline{k})$ satisfying (3), (4), (5), (6) in place of $(L'_0, L'_{s+1}, L'_{s+2}, \ldots, L'_n)$ is a nonempty open in the Zariski topology subset of $\mathbb{A}^{(r+1)(n-s+1)}(\overline{k})$. Let $\mathfrak{l}' \subset \mathbb{A}^{(r+1)(n-s+1)}(\overline{k})$ be a line such that $\mathfrak{l}' \cap \mathcal{U}'_0 \neq \emptyset$. Then the number of elements $\#(\mathfrak{l} \setminus \mathcal{U}'_0)$ is bounded from above by a polynomial in $d^n (d')^{n-s}$.*

(e) *More than that, one can construct linear forms $L'_0, L'_{s+1}, \ldots, L'_n$ from (c) satisfying additionally the condition*

$$\dim(\, W^{(4)} \setminus \mathcal{Z}(e_0, \ldots, e_r)\,) \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_i) \leq n - i - 1, \tag{8}$$

in $\mathbb{P}^n(\overline{k})$ for every $s+1 \leq n-1$.

(f) *Let $L'_{s+1}, L'_{s+2}, \ldots, L'_n \in \overline{k}[X_0, \ldots, X_r]$ be arbitrary linear forms satisfying (3), (6) and (8) for all $s+1 \leq i \leq n-1$. Then for every $s+1 \leq i \leq n$ the dimensions*

$$\dim W \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_i) \setminus \mathcal{Z}(e_0, \ldots, e_r) = n - i, \tag{9}$$

$$\dim W'' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_i) \leq n - i - 1 \tag{10}$$

(here and below in the present paper we suppose that an algebraic variety is empty if and only if its dimension is negative; we do not fixe the special negative value for the dimension of an empty set). Hence

$$W'' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n) = \emptyset, \tag{11}$$

$$(\, W^{(4)} \setminus \mathcal{Z}(e_0, \ldots, e_r)\,) \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_{n-1}) = \emptyset \tag{12}$$

in $\mathbb{P}^r(\overline{k})$ and $\mathbb{P}^n(\overline{k})$ respectively Further, each irreducible component of $(\, W \setminus \mathcal{Z}(e_0, \ldots, e_r)\,) \cap \mathcal{Z}(e'_{s+1})$ is not an irreducible component of $W^{(4)} \setminus \mathcal{Z}(e_0, \ldots, e_r)$, each irreducible component of $W' \cap \mathcal{Z}(L'_{s+1})$ is not an irreducible component of W''. Finally, if (5) holds then each irreducible component of $(W \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e'_{s+1})$ is not an irreducible component $(\overline{V \setminus W}) \setminus \mathcal{Z}(e_0, \ldots, e_r)$.

The working time of the algorithm from (a)–(c) and (e) is polynomial in d^n, $(d')^n$, d_1, d_2, d'_2, M, M', M_1, m, r, N and the size $\mathrm{L}(x^{(0)})$ of the point $x^{(0)}$.

REMARK 2 *Let us identify $\mathbb{P}^n(\overline{k}) = \mathcal{Z}(X_{n+1}) \subset \mathbb{P}^{n+1}(\overline{k})$. Hence $V \subset \mathbb{P}^{n+1}(\overline{k})$. Replacing if necessary n by $n+1$ and $\mathbb{P}^n(\overline{k})$ by $\mathbb{P}^{n+1}(\overline{k})$ we shall*

suppose without loss of generality that $s \geq 1$. Besides that, we can suppose that $f_1, \ldots, f_m$ are linearly independent over k.

REMARK 3 *One can combine conditions (3), (4) and (5) in the one equivalent*

$$\#\big(W \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_n) \setminus (\mathcal{Z}(e'_0) \cup \overline{V \setminus W}) \big) = \deg(p') \deg W'.$$

1 Preliminaries

We shall use in this paper the technique from [3], [5], [6], [7]. Namely, we apply Newton–Puiseux expansions and the Newton–Puiseux algorithm for constructing roots of a polynomial in the field of fractional power series in one variable, we apply infinitesimals, standard parts, constructing real structures.

Now we need to discuss the results from [7] to deduce some corollaries. Consider a bounded closed real algebraic variety V which is a set of all common zeroes of a family of polynomial $f_1, \ldots, f_m \in k_0[X_1, \ldots, X_n]$ of degrees less than d with coefficients from a real ordered field k_0. Let $R = \widetilde{k_0}$ be a real closure of k_0. The real field k_0 is finitely generated over $\mathbb{Q}$ and is given is similarly to k from the Introduction. The nonhomogeneous polynomials f_i, F (now F corresponds to k_0) have the same bounds for degrees and lengths of coefficients as in the Introduction. Additionally we suppose that for an element $a \in k_0$ one can decide whether $a > 0$ whithin the polynomial time in the size of a.

Consider a triangulation of V. Consider the cycles with coefficients from $\mathbb{Z}/2\mathbb{Z}$ of all dimensions of the triangulation of V which are sums of maximal (by inclusion in the triangulation) simplices. The main result here is Theorem 1 [7] which allows to construct within the time polynomial in d^n and the size of input a finite subset S of V which has a nonempty intersection with any considered cycle of any triangulation of V. The number of elements of S is bounded from above by a polynomial in d^n. The most part of [7] is devoted to the proof of Theorem 1. The case of an arbitrary real algebraic variety is reduced to the considered using the Alexandrov compactification.

Now let $n \geq 1$ and $s \geq 1$ be integers and $g_1, \ldots g_s \in k_0[X_1, \ldots, X_n]$ be some polynomials which have the estimations for degrees and sizes of integer coefficients similar to ones for $f_1, \ldots, f_m$ from the Introduction. Consider a basic semialgebraic set (an arbitrary semialgebraic set can be represented as a union of basic ones)

$$U = \{x \in R^n : f_1(x) = \ldots = f_m(x) = 0 \,\&\, g_1(x) > 0 \,\&\, \ldots \,\&\, g_s(x) > 0\}. \quad (13)$$

Let $2^{u-1} < n \leq 2^u$ for an integer u. Let $s \leq s' 2^u < s + 2^u$ and $s' \in \mathbb{Z}$. If $s < 2^u$ set $g_j = 1$ for all $s + 1 \leq j \leq 2^u$. Set $s_j = s'j$ for $j = 0, \ldots, 2^u - 1$ and $s_{2^u} = \max\{s, 2^u\}$. Let $Z_{j,i}$, $1 \leq j \leq 2^{u-i}$, $0 \leq i \leq u$, be new variables. Consider the real algebraic variety $U_1 \subset \mathbb{A}^{n+2^{u+1}-1}$ which is the set of all common zeroes of polynomials $\prod_{s_{j-1}+1 \leq i \leq s_j} g_i - Z_{j,0}$, $1 \leq j \leq 2^u$; $f_1, \ldots, f_m$, and $Z_{j,i} Z_{2j-1,i-1} Z_{2j,i-1} - 1$, $1 \leq j \leq 2^{u-i}$, $1 \leq i \leq u$, (so in the case when $s < 2^u$ the polynomials $1 - Z_{j,0}$, $s + 1 \leq j \leq 2^u$, belong to the considered family). Denote by

$$\widetilde{\pi} : R^{n+2^{u+1}-1} \to R^n,$$
$$(X_1, \ldots, X_n; Z_{j,i}, 1 \leq j \leq 2^{u-i}, 0 \leq i \leq u) \mapsto (X_1, \ldots, X_n)$$

the linear projection. Then the set U coincides with $\widetilde{\pi}(U_2)$ where U_2 is a union of some connected components of U_1

Let $W \subset R^n$ be an arbitrary set. By definition the family of all irreducible (over R) components of W is $W \cap W'_\alpha$, $\alpha \in A$, where W'_α, $\alpha \in A$, is the family of all the irreducible (over R) components of the closure of W in R^n with respect to the Zariski topology. In this paper and [7] *by connected components of semialgebraic sets we mean semialgebraic connected components of these sets,* see the definition in [1].

Denote by $\dot{U}^{(v)}$ the set of all smooth points of dimension v of U and by $U^{(v)}$ the closure of $\dot{U}^{(v)}$ in U with respect to the topology of the real ordered field R. Therefore, $\dot{U}^{(v)} = \bigcup_{j \in J_v} \dot{U}_j^{(v)}$, where $\dot{U}_j^{(v)}$ are all the pairwise distinct irreducible over R components of $\dot{U}^{(v)}$. Denote by $U_j^{(v)}$ the closure of $\dot{U}_j^{(v)}$ in U with respect to the topology of the real field R. Hence $U^{(v)} = \bigcup_{j \in J_v} U_j^{(v)}$, and every $U_j^{(v)}$ is a semialgebraic set. Now applying Corollary 2 and Remark 2 from [7] to the real algebraic variety U_1 we get the following result.

PROPOSITION 1 *(cf. Theorem 2 [7]) Consider a basic semialgebraic set (13). Then one can construct a finite set S of points of U which has a non–empty intersection with every connected component of every $U_j^{(v)}$ for every $j \in J_v$, $0 \leq v \leq n$. The number of points of S is bounded from above by a polynomial in $((1 + s/n)d)^n$. The working time of the algorithm for constructing S is polynomial in $((1 + s/n)d)^n$, d_1, d_2, M, M_1, m.*

So Proposition 1 is an almost immediate consequence of Theorem 1 [7]. In the given here Proposition 1 we remove inaccuracies from [7]. Namely, we slightly modify the construction introducing the variables $Z_{i,j}$ before the statement. Let U_i, $i \in I$, be the family of all irreducible components of U (or alternatively of all the connected components of all irreducible components of U). Let $U_i^{(v)}$ be the closure in the topology of the real ordered field of the set of all points which are smooth points of dimension v of U_i and U simultaneously. Hence $U^{(v)} = \cup_{i \in I} U_i^{(v)}$. Therefore, each connected component of every $U_i^{(v)}$ is a union of some connected components of some sets $U_j^{(v)}$, $j \in J_v$ (we leave the details to the reader). Hence if one adds in the statement Theorem 2 [7] add "and U simultaneously" this theorem becomes a consequence of Proposition 1. On the other hand, one needs to add "and U simultaneously" since it may happen that a connected component c' of an irreducible component W' of U is contained in a connected component c'' of an irreducible component W'' of U and $\dim c' < \dim c''$. One need to exclude all such connected components c' since they do not correspond to the considered cycles with maximal simlices of the Alexandrov compactification of U_1, see [7] for details.

Now let $q_1, \ldots, q_{s_1} \in k_0[X_1, \ldots, X_n]$ be some polynomials which have estimations for degrees and sizes of integer coefficients similar to ones for $f_1, \ldots, f_m$, see the Introduction and [7]. Let α_i denotes $=$ or $\geq$ or $>$ for every $1 \leq i \leq s_1$. Consider a semialgebraic set

$$U' = \{\, x \in R^n \,:\, q_1(x)\alpha_1 0 \quad \& \ldots \& \quad q_{s_1}(x)\alpha_{s_1} 0 \,\}. \tag{14}$$

Let $j \in J_v$, $0 \leq v \leq n$ in the previous notation. Let $\mathcal{C}'_{j,v}$ be the set of all connected components of $U_j^{(v)} \cap U'$ in the notation of Proposition 1. For every

$c \in \mathcal{C}'_{j,v}$ denote by $\overline{c}$ the closure in R^n with respect to the topology of the real field R of c. For $c', c'' \in \mathcal{C}'_{j,v}$ set $c' \sim c''$ if and only if there are $c_1, \ldots, c_\nu \in \mathcal{C}_{j,v}$, $\nu \geq 2$, such that $c_1 = c'$, $c_\nu = c''$ and $\overline{c_i} \cap \overline{c_{i+1}} \neq \emptyset$ for every $1 \leq i \leq \nu - 1$. Denote by $\overline{\mathcal{C}}_{j,v}$ the set of classes of equivalence of $\mathcal{C}'_{j,v}$ by this relation $\sim$. Set $\mathcal{C}''_{j,v} = \{\cup c : c \in \overline{\mathcal{C}}_{j,v}\}$ (here $\cup c$ is the union of the sets which are the elements of c), i.e., for every $\widetilde{c} \in \mathcal{C}''_{j,v}$ there is $c' \in \mathcal{C}'_{j,v}$ such that $\widetilde{c} = \cup_{c'' \sim c'} c''$. Notice that if U is a closed real algebraic variety in R^n and all α_i are $=$ or $\geq$ then $\mathcal{C}''_{j,v} = \mathcal{C}'_{j,v}$.

COROLLARY 1 *In the previous notation one can construct a finite set S' of points of $U \cap U'$ which has a non–empty intersection with every $c \in \mathcal{C}''_{j,v}$ for every $i \in J_v$, $0 \leq v \leq n$. The number of points of S' is bounded from above by a polynomial in $((1 + (s + s_1)/n)d)^n$. The working time of the algorithm for constructing S' is polynomial in $((1 + (s + s_1)/n)d)^n$, d_1, d_2, M, M_1, m.*

PROOF Let $\varepsilon > 0$ be an infinitesimal with respect to the field k_0. Consider the field $k_0(\varepsilon)$ as a ground field. Let $\widetilde{R(\varepsilon)}$ be a real closure of $R(\varepsilon)$. Let us replace in (14) each equation $q_i = 0$ (respectively inequality $q_i \geq 0$) by the conjugation $q_i + \varepsilon > 0$ and $\varepsilon - q_i > 0$ (respectively $q_i + \varepsilon > 0$). Denote by U'_ε the obtained open in the topology of the real field $\widetilde{R(\varepsilon)}$ semialgebraic set. Applying Proposition 1 to the set $U \cap U'_\varepsilon$ one constructs the finite set of points S'_ε. Let $c \in C''_{j,v}$. Then one sees that $c \subset \cup_{\gamma \in \Gamma} c_\gamma$ where c_γ, $\gamma \in \Gamma$ are all the connected components of the intersection $U^{(v)} \cap U'_\varepsilon$ such that $c_\gamma \cap c \neq \emptyset$. For every $z \in \widetilde{R(\varepsilon)}^n$ that is not infinitely large with respect to R the standard part $\mathrm{st}_\varepsilon(z) \in R^n$ is defined ($\mathrm{st}_\varepsilon(z)$ is the element which is infinitely close to z with respect to R). Then one sees $\mathrm{st}_\varepsilon(\cup_{\gamma \in \Gamma} c_\gamma) \supset c$. On the other hand, each semalgebraic set has only a finite number of connected components. Hence according to the given definitions $\mathrm{st}_\varepsilon(c_\gamma) = \cup_{1 \leq i \leq \mu} c_{\gamma,i}$ where $c_{\gamma,i}$ are some connected components of $U^{(v)} \cap U'$ (here μ depends on γ). Besides that, for all $1 \leq i < j \leq \mu$ there are $1 \leq i_1, \ldots, i_\omega \leq \mu$ such that $i = i_1$, $j = i_\omega$ and $\overline{c_{\gamma,i_u}} \cap \overline{c_{\gamma,i_{u+1}}} \neq \emptyset$ for $1 \leq u \leq \omega - 1$. Thus, $\mathrm{st}_\varepsilon(\cup_{\gamma \in \Gamma} c_\gamma) = c$. Therefore, $\mathrm{st}_\varepsilon(S'_\varepsilon) \cap c \neq \emptyset$ by Proposition 1. Now using the algorithm from [3], [5] we construct the set $\mathrm{st}_\varepsilon(S'_\varepsilon)$. Put $S' = \mathrm{st}_\varepsilon(S'_\varepsilon)$. The constructed set S' satisfies the required properties. The estimate for the working time of the algorithm for constructing S' follows immediately from the ones of the applied algorithms. The corollary is proved.

The real structure on the field k is an embedding $k \to K[\sqrt{-1}]$ where K is a real ordered field, see [4]. If k is supplied with a real structure then the absolute value $|a|$ of an element $a \in k$ is defined in the natural way. Using the algorithm from [4] one can construct within the polynomial time a real structure on k such that K is a finite extension of k, the field K is given similarly to k_0, and

(A) for every element $a \in K$ one can decide whether $a > 0$ within the time polynomial in d_1, M_1, and the size $\mathrm{L}(a)$ of the element a.

We shall use many times Proposition 1 [6], for solving systems of polynomial equations and inequalities with squares of absolute values and infinitesimals within polynomial time without references to this proposition.

Now we shall change slightly the conditions of Proposition 1 [6]. Consider inequalities in $X_1, \ldots, X_n$ of the type $A \geq 0$ where $A = \sum_{1 \leq i \leq r} a_i |A_i|^2$, $a_i \in K$,

and A_i is a superposition of polynomials with coefficients from k and functions $B \mapsto |B|^2$ for every i The upper bound for the degree of A can be easily defined if we set $\deg |B|^2 = 2 \deg B$.

Set

$$U'' = \{ \ x \in \overline{k}^n \ : \ q_1(x)\alpha_1 0 \quad \& \ \ldots \ \& \quad q_{s_1}(x)\alpha_{s_1} 0 \ \} \tag{15}$$

Suppose that in (15) all α_i are $=$ or $\geq$ and that all the inequalities $q_j \geq 0$ have the considered form $A \geq 0$. For each equation $q_j = 0$ from (15) assume that either it has the form $A = 0$ where A is as above, or $q_j \in k[X_1, \ldots, X_n]$ (it will be sufficient for our aims). Let $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ be polynomials. Suppose that $f_1, \ldots, f_m$, $g_1, \ldots, g_{s_1}$ satisfy the similar inequalities for degrees and lengths of coefficients as the polynomials $f_1, \ldots, f_m$ from the Introduction do. Let $V = \mathcal{Z}(f_1, \ldots, f_m) \subset \mathbb{A}^n(\overline{k})$, cf. the Introduction.

THEOREM 2 *Under the formulated conditions denote by $\mathcal{C}$ the set of all connected components of $W \cap U''$, where W runs over all irreducible over $\overline{k}$ components W of V. Then one can construct a finite set S'' of points of $V \cap U''$ which has a nonempty intersection with every connected component $c \in \mathcal{C}$. The number of points of S'' is bounded from above by a polynomial in $((1+s_1/n)d)^n$. The working time of the algorithm for constructing S'' is polynomial in $((1 + s_1/n)d)^n$, d_1, d_2, M, M_1, m.*

PROOF Each system of equations and inequalities with squares of absolute values over $\overline{k}$ is equivalent to the system of equations and inequalities over $\widetilde{K}$ with twice as much of variables. Hence it is sufficient to apply Corollary 1. The corollary is proved.

REMARK 4 *Since k (respectively k_0) is an arbitrary finitely generated over $\mathbb{Q}$ field (respectively finitely generated over $\mathbb{Q}$ real ordered field) Corollary 1 and Theorem 2 are valid also if one replaces the field of coefficients k (respectively k_0) by an extension of k (respectively k_0) by an algebraic element over k (respectively k_0) of degree polynomial in $d^n d_1 d_2$ and a fixed number of infinitesimals.*

In the proof of the following simple proposition we describe a usefull algorithm of reduction to general position, cf. also "the good properties" from [5], [6]. In what follows we shall refer to it as to *the algorithm of reduction to integer coefficients.*

PROPOSITION 2 *Let $\mathcal{U}_i \subset \overline{k}^N$ and $\nu_i \geq 1$, $1 \leq i \leq w$ be integers. Suppose that for every $z \in \mathcal{U}_i$ for every line $\mathfrak{l} \subset \overline{k}^N$ through z the number of elements $\#(\mathfrak{l} \setminus \mathcal{U}_i) \leq \nu_i$ for every $1 \leq i \leq w$. Suppose that one can decide for a given point $z \in \overline{k}$ whether $z \in \mathcal{U}_i$, $1 \leq i \leq w$. Suppose that a point $x_i \in \mathcal{U}_i$ is given for every $1 \leq i \leq w$. Then one can construct a point $x' = (x'_1, \ldots, x'_N) \in \bigcap_{1 \leq i \leq w} \mathcal{U}_i$ such that all x'_i, $1 \leq i \leq N$, are integers of length $O(\log(1 + \sum_{1 \leq i \leq w} \nu_i))$.*

PROOF Let $w = 1$. Set $x^{(0)} = x_1$. Let $0 \leq j < N$ be an integer. Suppose that we have constructed a point $x^{(j)} = (x_1^{(j)}, \ldots, x_N^{(j)}) \in \mathcal{U}_1$ such that all $x_i^{(j)}$, $1 \leq i \leq j$, are integers of length $O(\log(1 + \nu_1))$. Then considering the line $\mathfrak{l}$ parallel to $(j+1)$th coordinate axe such that $x^{(j)} \in \mathfrak{l}$ we construct a point $x^{(j+1)}$. Finally we set $x' = x^{(N)}$. The proposition is proved for $w = 1$.

Let $w > 1$. Suppose that we have already constructed a point $z^{(j)} = (z_1^{(j)}, \ldots, z_N^{(j)}) \in \bigcap_{1 \leq i \leq j} \mathcal{U}_i$ for some $1 \leq j < w$ such that all $z_i^{(j)}$, $1 \leq i \leq N$,

are integers of length $O(\log(1+\sum_{1\le i\le j}\nu_i))$. Considering a line through $z^{(j)}$ and x_{j+1} we construct a point $y^{(j+1)}\in\bigcap_{1\le i\le j+1}\mathcal{U}_i$. Applying the algorithm for the case $w=1$ to the set $\bigcap_{1\le i\le j+1}\mathcal{U}_i$ and its point $y^{(j+1)}$ we construct a point $z^{(j+1)}$. Finally we set $x'=z^{(w)}$. The proposition is proved.

2 The first auxiliary algorithm for Theorem 1

We shall suppose in this section that $\dim W=\dim W'=n-s$ and the transcendency degree of the family of rational functions $e_i/e_0\in k(W)$, $1\le i\le n-s$, is $n-s$. In particular, e_0 is not vanishing on W.

For an arbitrary projective algebraic variety $V'\subset\mathbb{P}^n(\overline{k})$ we shall denote by $\mathrm{con}(V')$ in what follows the affine algebraic variety in $\mathbb{A}^{n+1}(\overline{k})$ which is the set of zeroes of the homogeneous ideal of V'.

Let $\varepsilon_i>0$, $1\le i\in\mathbb{Z}$, be an infinitesimal with respect to the field $k_{i-1}=k(\varepsilon_1,\dots,\varepsilon_{i-1})$. One can supply the algebraic closure $\overline{k_i}$ with a real structure, which extends the one of k $\overline{k_i}$ with a real structure, which extends the one of k see [4], [5].

Let $L_0,\dots,L_{n+1}$ be linear forms from Theorem 1 [8] for the projective algebraic variety $V\cup\mathcal{Z}(e_0)=\mathcal{Z}(f_1e_0,\dots,f_me_0)$. Hence $W\cap\mathcal{Z}(L_0,L_{s+1},\dots,L_n)=\emptyset$ in $\mathbb{P}^n(\overline{k})$, $W\not\subset\mathcal{Z}(L_0)$ and $W\cap\mathcal{Z}(L_{s+1},\dots,L_n)\cap\mathcal{Z}(e_0)=\emptyset$. In what follows we fix $L_1,\dots,L_{n+1}$. On the other hand, for a given point $x^*\in\mathbb{P}^n(\overline{k})$ we shall choose L_0 such that additionally $L_0(x^*)\ne 0$.

Now we are going to describe the first auxiliary algorithm. In the input of this algorithm one has a point $x^*\in W$ that is a smooth point of V and $(L_0e_0)(x^*)\ne 0$. In output one has a point $x^{**}=x^{(n)}\in W(\overline{k(\varepsilon_2)})$ satisfying conditions (a)–(d) with $v=n$, see below. In this auxiliary algorithm for $s\le v\le n$ one constructs recursively points $x^{(v)}\in V(\overline{k(\varepsilon_2)})$ and the integers $s+1\le i_{v,v+1}<\ldots<i_{v,n}\le n$ satisfying the following properties:

(a) $(e_0L_0)(x^{(v)})\ne 0$,

(b) $\sum_{0\le i\le n}|(X_i/L_0)(x^{(v)})-(X_i/L_0)(x^*)|^2\le\varepsilon_1$,

(c) $L_i(x^{(v)})=L_i(x^*)-\mu_i\varepsilon_2L_0(x^*)$, $s+1\le i\le n$, where μ_i are integers (depending on v) with lengths $O(n\log d+(n-s)\log d')$.

Further, denote for brevity $\iota_\alpha=i_{v,\alpha}$, $v+1\le\alpha\le n$ when v is fixed. Set $\widetilde{e}_0=1$ if $v=s$, and $\widetilde{e}_0=e_0$ if $s+1\le v\le n$. Denote by

$$\pi_v\,:\,W\setminus\mathcal{Z}(L_0\widetilde{e}_0,L_0e_1,\dots,L_0e_{v-s},L_{\iota_{v+1}}\widetilde{e}_0,\dots,L_{\iota_n}\widetilde{e}_0)\to\mathbb{P}^{n-s}(\overline{k}),$$
$$(X_0:\ldots:X_n)\mapsto(L_0\widetilde{e}_0:L_0e_1:\ldots:L_0e_{v-s}:L_{\iota_{v+1}}\widetilde{e}_0:\ldots:L_{\iota_n}\widetilde{e}_0)$$

the regular morphism. Then

(d) the differential $d_{x^{(v)}}\pi_v$ of the morphism π_v at the point $x^{(v)}$ is an isomorphism and hence π_v is a dominant morphism.

We shall say that a point $y\in W$ (which may have coordinates in any extension of $\overline{k(\varepsilon_2)}$ supplied with the corresponding real structure) satisfies condition (a) (respectively (b), (c), (d)) if and only if condition (a) (respectively (b), (c), (d)) holds with y in place of $x^{(v)}$.

Denote $k'_\beta = k(\varepsilon_2, \ldots, \varepsilon_\beta) \subset k_\beta$ where $2 \le \beta \in \mathbb{Z}$ is fixed (for estimation of the complexity of the algorithm). Let a point $\widetilde{x}_v \in V(\overline{k'_\beta})$. Suppose that $\widetilde{x}_v$ satisfies (a), (b), (d). Let $\mathfrak{l} \subset \mathbb{P}^{n-s}(\overline{k'_\beta})$ be an arbitrary line containing the point $\pi_s(\widetilde{x}_v)$ and C_1 be the (unique by the implicit function theorem) defined and irreducible over $\overline{k'_\beta}$ component of $\pi_s^{-1}(\mathfrak{l})$ such that $\widetilde{x}_v \in C_1$. Then there is at most a polynomial in $d^n(d')^{n-s}$ number of points $x' \in C_1$ such that at least one of conditions (a), (d) is not satisfied for x'. On the other hand, see, e.g., Proposition 6 [5], for every point $z \in \mathbb{P}^{n-s}(\overline{k'_\beta})$ that is infinitely close to $\pi_s(x^*)$ with respect to the field k there is a point $x'' \in \pi_s^{-1}(z)$ such that x'' is infinitely close to x^* with respect to the field k. Hence, cf. the algorithm of reduction to integer coefficients, Proposition 2, enumerating $\mu_i = 0, 1, \ldots$, for every $s+1 \le i \le n$ and solving systems of polynomial equations and inequalities with squares of absolute values one can replace subsequently the coordinates $L_i(x^{(v)})$ of $\pi_s(\widetilde{x}_v)$ by by $L_i(x^*) - \varepsilon_2 \mu_i L_0(x^*)$, where μ_i are integers with lengths $O(n \log d + (n-s)\log d')$, and construct a point $x^{(v)}$ satisfying all the conditions (a)–(d). So it is sufficient to construct a point $\widetilde{x}_v$.

The base of the recursion is $v = s$. In this case obviously $i_{s,\alpha} = \alpha$ for all $s+1 \le \alpha \le n$. Let $\mathfrak{l} \subset \mathbb{P}^{n-s}(\overline{k})$ be a line containing the points $\pi_s(x^*)$ and $(1 : 0 : \ldots : 0)$ (this line is unique if these two points do not coincide). By Theorem 1 [8] for every point $y \in \pi_s^{-1}((1 : 0 : \ldots : 0))$ the differential $d_y\pi_s$ is an isomorphism. Let $x^* = (x_0^* : \ldots : x_n^*)$ where all $x_i^* \in \overline{k}$ and $L_0(x_0^*, \ldots, x_n^*) = 1$. Let us construct solving a system of polynomial equations and using Theorem 2 [8] all the points from $\mathrm{con}(W)$ satisfying the system

$$\left\{ \begin{array}{ll} f_i = 0, & 1 \le i \le m, \\ L_i = L_i(x_0^*, \ldots, x_n^*), & s+1 \le i \le n, \\ L_0 = 1 + \varepsilon_2 & \end{array} \right. \tag{16}$$

(the set of these points is finite). After that we choose among the constructed solutions of system (16) a point $(\widetilde{x}_{s,0}, \ldots, \widetilde{x}_{s,n}) \in \mathbb{A}^{n+1}(\overline{k'_2})$ such that $\sum_{0 \le i \le n} |\widetilde{x}_{s,i} - x_i^*|^2 \le \varepsilon_1$ and denote $\widetilde{x}_s = (\widetilde{x}_{s,0} : \ldots : \widetilde{x}_{s,n})$. So the point $\widetilde{x}_s \in \pi_s^{-1}(\mathfrak{l})$ is infinitely close to x^*. Hence $\widetilde{x}_s$ is a smooth point of V and satisfies conditions (a), (b), (d). Therefore, one can construct also $x^{(s)}$.

Now suppose that $s \le v \le n-1$ and the point $x^{(v)}$ is constructed. Our aim is to construct $x^{(v+1)}$ and all $i_{v+1,\alpha}$, $v+2 \le \alpha \le n$. Let Z_i, $s \le i \le v+1$, T_i, $v+1 \le i \le n$, be new variables. Let $\mathbb{A}^{2n-s+3}(\overline{k})$ has the coordinate functions $X_0, \ldots, X_n$, $Z_s, \ldots, Z_{v+1}$, $T_{v+1}, \ldots, T_n$. Consider the affine algebraic variety $V_1 \subset \mathbb{A}^{2n-s+3}(\overline{k})$ which is the set of all common zeroes of the polynomials $f_1, \ldots, f_m$; $Z_s e_0 - 1$; $Z_j e_0 - e_{j-s}$, $s+1 \le j \le v+1$; $T_j L_0 - L_{\iota_j}$, $v+1 \le j \le n$ (here $\iota_j = i_{v,j}$); $L_0 - 1$. Denote for brevity the last family of polynomials by $g_i \in k[X_0, \ldots, X_n, Z_s, \ldots, Z_{v+1}, T_{v+1}, \ldots, T_n]$, $1 \le i \le m_1 = m + n - s + 3$. We shall identify $V_1 = V \setminus \mathcal{Z}(e_0 L_0) \subset V$. So $X_i(x'')$, $0 \le i \le n$; $Z_i(x'')$, $s \le j \le v+1$; $T_i(x'')$, $v+1 \le j \le n$, are defined for every $x'' \in V_1$.

In what follows we shall identify for convenience of notations the tangent space $\mathcal{Z}(\sum_{1 \le i \le n} a_{\gamma,i} dX_i,\ \gamma \in \Gamma)$ (where $a_{\gamma,i}$ belongs to the coefficients field) in a point of an affine algebraic variety with the subspace
$\mathcal{Z}(\sum_{1 \le i \le n} a_{\gamma,i} X_i,\ \gamma \in \Gamma) \subset \mathbb{A}^n$, herewith $\mathbb{A}^n$ has the coordinates functions $X_1, \ldots, X_n$. We shall use the similar identification also for other affine spaces, in particular, for A^{2n-s+3} with the coordinates $X_0, \ldots, X_n$, $Z_{s+1}, \ldots, Z_{v+1}$, $T_{v+1}, \ldots, T_n$.

LEMMA 1 *Let $\xi \in V_1$ be a smooth point (it may have the coordinates in an arbitrary extension of $\overline{k}$) and $\xi \in W$. Let T_{ξ,V_1} be the tangent spaces of V at the point ξ. Then the intersection $T_{\xi,V_1} \cap \mathcal{Z}(Z_{s+1},\dots,Z_v,T_{v+1},\dots,T_n) = \{0\}$ if and only if the differential $d_\xi \pi_v$ is an isomorphism.*

PROOF Performing a non–degenerated linear transformation of $X_0,\dots,X_n$ we shall suppose without loss of generality for convenience of notation that $L_0 = X_0$. Let $H_1,\dots,H_s \in k[X_0,\dots,X_n]$ be homogeneous polynomials such that $H_i/X_0^{\deg H_i}$, $1 \le i \le s$, is a system of local parameters in the point ξ of the projective algebraic variety V. One can choose H_i using linear projections $\mathbb{P}^n(\overline{k}) \to \mathbb{P}^{n-s+1}(\overline{k})$ in general position such that $\deg H_i \le \deg W \le d^s$ for all $1 \le i \le s$ (we do not use the last fact now in the proof of the lemma but shall use it later).

Then $H_i(1,X_1,\dots,X_n)$, $1 \le i \le s$; $Z_s e_0 - 1$; $(Z_j e_0 - e_{j-s})(1,X_1,\dots,X_n)$, $s+1 \le j \le v+1$; $(T_j L_0 - L_{\iota_j})(1,X_1,\dots,X_n)$, $v+1 \le j \le n$; $X_0 - 1$, is a system of local parameters of V_1 in the point ξ. Denote the last system of local parameters by $h_1,\dots,h_{n+3}$. Then $T_{\xi,V_1} \cap \mathcal{Z}(Z_{s+1},\dots,Z_v,T_{v+1},\dots,T_n) = \{0\}$ if and only if the differentials of the polynomials $d_\xi h_1,\dots,d_\xi h_{n+3}$, $d_\xi Z_{s+1},\dots,d_\xi Z_v$, $d_\xi T_{v+1},\dots,d_\xi T_n$ at the point ξ are linearly independent. The differential $d_\xi \pi_v$ is an isomorphism if and only if the differentials of the rational functions $d_\xi h_1,\dots,$ $d_\xi h_s$, $d_\xi(e_1/e_0)$, $\dots,d_\xi(e_{v-s}/e_0)$, $d_\xi(L_{\iota_{v+1}}/L_0),\dots,d_\xi(L_{\iota_n}/L_0)$ are linearly independent. Now the lemma is obtained by the direct comparison of the corresponding Jacobi matrices taking into account that $(e_0 L_0)(\xi) \ne 0$. The lemma is proved.

Let $X_0',\dots,X_n'$, $Z_s',\dots,Z_{v+1}'$, $T_{v+1}',\dots,T_n'$, be new variables. Consider the system of equalities and inequalities in $X_0,\dots,X_n$, $Z_s,\dots,Z_{v+1}$, $T_{v+1},\dots,T_n$ $X_0',\dots,X_n'$, $Z_s',\dots,Z_{v+1}'$, $T_{v+1}',\dots,T_n'$ with coefficients from $\overline{k_5'}$:

$$\begin{cases} g_i = 0, & 1 \le i \le m_1, \\ g_i(X_0',\dots,X_n',Z_s',\dots,Z_{v+1}',T_{v+1}',\dots,T_n') = 0, & 1 \le i \le m_1, \\ \sum_{0\le i\le n} |X_i - X_i(x^{(v)})|^2 + \sum_{s+1\le i\le v+1} |Z_i - Z_i(x^{(v)})|^2 + \\ \sum_{v+1\le i\le n} |T_i - T_i(x^{(v)})|^2 = \varepsilon_3, \\ \sum_{0\le i\le n} |X_i - X_i'|^2 + \sum_{s+1\le i\le v+1} |Z_i - Z_i'|^2 + \\ \sum_{v+1\le i\le n} |T_i - T_i'|^2 = \varepsilon_5^2, \\ Z_i - Z_i' = 0, & s+1 \le i \le v, \\ |Z_{v+1} - Z_{v+1}'|^2 > \varepsilon_5^2 \varepsilon_4. \end{cases} \tag{17}$$

By (d), Lemma 1 and Lemma 6 [6] system (17) has a solution $\xi_1 \in \mathbb{A}^{2n-s+2}(\overline{k_5})$. Let us construct such a solution ξ_1. Put $\widetilde{x}_{v+1,i} = X_i(\xi_1)$, $0 \le i \le n$, and $\widetilde{x}_{v+1} = (\widetilde{x}_{v+1,0} : \dots : \widetilde{x}_{v+1,n})$. Then $\widetilde{x}_{v+1} \in W$ is a smooth point of V satisfying (a) and (b). Let us construct using Theorem 4 [6] the tangent space $T_{\widetilde{x}_{v+1},W}$. By Corollary 2 [6] there is $v+1 \le \gamma \le n$ ($\gamma = i_0$ in the notation of [6] Section 3) such that the intersection

$$T_{\widetilde{x}_{v+1},W} \cap \mathcal{Z}(Z_{s+1},\dots,Z_v,Z_{v+1},T_{v+1},\dots,T_{\gamma-1},T_{\gamma+1},\dots,T_n) = \{0\}.$$

Let us compute such an integer γ constructing the corresponding intersections. Now set $i_{v+1,j} = i_{v,j-1}$ for $v+2 \le j \le \gamma$, and $i_{v+1,j} = i_{v,j}$ for $\gamma+1 \le j \le n$. Then by Lemma 1 with $v+1$ in place of v the differential $d_{\widetilde{x}_{v+1}} \pi_{v+1}$ is an isomorphism. Hence the point $\widetilde{x}_{v+1}$ satisfies condition (a), (b), (d). Therefore,

by previous remarks one can construct a point $x^{(v+1)}$ satisfying (a)–(d). Thus, finally we shall construct $x^{(n)}$. The first auxiliary algorithm is described.

3 Several Lemmas

LEMMA 2 *Let k be a arbitrary field of zero–characteristic. Let W_1 and W_2 be defined over k algebraic varieties and W_2 be irreducible over k. Let $\pi : W_1 \to W_2$ be a dominant (this means that the restriction of π to any irreducible over k component of W_1 is dominant) regular defined over k morphism. Let $\dim W_1 = \dim W_2$. Denote by $k(W_1)$ the direct product of the fields of defined over k rational functions of all irreducible over k components of W_1. Hence the degree $[k(W_1) : k(W_2)]$ is defined.*

(i) Let $z \in W_2$ be a normal point. Denote by $\nu(z)$ the number of connected components of $\pi^{-1}(z)$. Then $\nu(z) \leq [k(W_1) : k(W_2)] = \deg \pi$. In particular, if the number of elements $\#\pi^{-1}(z) < +\infty$ then $\#\pi^{-1}(z) \leq [k(W_1) : k(W_2)] = \deg \pi$.

(ii) There is a smooth point $z \in W_2$ such that $\#\pi^{-1}(z) = \deg \pi$.

(iii) Let $z \in W_2$ be a normal point and $\#\pi^{-1}(z) = \deg \pi$. Then there is an open in the Zariski topology subset $U' \subset W_2$ such that $z \in U'$ and the morphism $\pi^{-1}(U') \to U'$ induced by π is finite.

(iv) Let $z \in W_2$ be a normal (respectively smooth) point and $\#\pi^{-1}(z) = \deg \pi$. Then every $x \in \pi^{-1}(z)$ is a normal (respectively smooth) point of W_1 and the differential $d_x\pi : T_{x,W_1} \to T_{z,W_2}$ is an isomorphism of the Zariski tangent spaces of W_1 and W_2 at the points x and z respectively. One can choose U' such that all the points of U' are normal (respectively smooth) and the number of elements $\#\pi^{-1}(z_1) = \deg \pi$ for every $z_1 \in U'$.

PROOF We can suppose without loss of generality that W_2 is an affine variety, W_1 is irreducible over k, and $k = \overline{k}$. Denote $[k(W_1) : k(W_2)] = \alpha$. Let $z \in W_2$ be an normal point. Denote by $\widetilde{W}_i$, $i = 1, 2$, the normalization of the algebraic variety W_i in the field $k(W_1)$. So we have the commutative diagram of morphisms of algebraic varieties

$$\begin{array}{ccc} \widetilde{W}_1 & \xrightarrow{\widetilde{\pi}} & \widetilde{W}_2 \\ {\scriptstyle \pi_1}\downarrow & & {\scriptstyle \pi_2}\downarrow \\ W_1 & \xrightarrow{\pi} & W_2, \end{array}$$

where π_1 and π_2 are finite morphisms and $\widetilde{\pi}$ is a birational isomorphism induced by π. The morphism π_2 is finite and z is a normal point. Therefore, the coefficients of the minimal polynomial of each element of $\overline{k}[\widetilde{W}_2]$ over $\overline{k}(W_2)$ belong to the the local ring $\mathcal{O}_{z,W_2}$ of the algebraic variety W_2 in the point z provided that leading coefficient of this minimal polynomial is 1. Hence $\#\pi_2^{-1}(z) \leq \alpha$. By the Zariski main theorem, see, e.g., [9], for every $z' \in \pi_2^{-1}(z)$ if $\widetilde{\pi}^{-1}(z') \neq \emptyset$ then $\widetilde{\pi}^{-1}(z')$ is connected. For an arbitrary algebraic variety

W denote for brevity by $\nu(W)$ the number of all connected components of W. Hence, $\#\pi_2^{-1}(z) \geq \nu(\pi_1^{-1}(\pi^{-1}(z)))$. Hence $\nu(\pi^{-1}(z)) \leq \alpha$ and (i) is proved.

Assertion (ii) is known. Under conditions of (iii) the number of elements $\#\pi_2^{-1}(z) = \#\pi_1^{-1}(\pi^{-1}(z))$ and $\widetilde{\pi}$ is invertible in some neighborhood in the Zariski topology U'' of the finite set $\pi_2^{-1}(z)$. So we have the isomorphism of algebraic varieties $\widetilde{\pi}^{-1}(U'') \simeq U''$ induced by $\widetilde{\pi}$. Set $U' = W_2 \setminus \pi_2(\widetilde{W_2} \setminus U'')$. Then $z \in U'$ and the morphism

$$\pi_1^{-1}(\pi^{-1}(U')) = \widetilde{\pi}^{-1}(\pi_2^{-1}(U')) \to U'$$

is finite. Hence, the morphism $\pi^{-1}(U') \to U'$ is also finite.

To prove (iv) we shall suppose without loss of generality that all the points of U' are normal (respectively smooth) points of W_2 and U' is affine. Let us choose a function $y \in k[W_1]$ such that the number of elements $\#y(\pi^{-1}(z)) = \#\pi^{-1}(z)$ and y is a primitive element of $k(W_1)$ over $k(W_2)$. Let $\phi \in k(W_2)[Z]$ be the minimal polynomial of the element y over $k(W_2)$, and leading coefficient $\mathrm{lc}_Z(\phi) = 1$. Since $k[U']$ is integrally closed $\phi \in k[U'][Z]$. Set the algebraic variety $U''' = \{(\pi(x), y(x)) : x \in \pi^{-1}(U')\}$. Hence one can identify $U''' = \mathcal{Z}(\phi) \subset U' \times \mathbb{A}^1(\overline{k})$. We have the morphisms $\pi' : \pi^{-1}(U') \to U'''$, $\pi'(x) = (\pi(x), y(x))$, and $\pi'' : U''' \to U'$, $\pi''((x_1, x_2)) = x_1$. The morphisms π', π'' are finite dominant and π' is a birational isomorphism.

Now $\deg_Z \phi = \deg \pi$. Let $\phi = \sum_i \phi_i Z^i$, $\phi_i \in k[U']$. Set $\phi|_z = \sum_i \phi_i(z) Z^i \in k[Z]$. The polynomial $\phi|_z$ has $\deg \pi$ pairwise distinct roots $Z = y(x)$, $x \in \pi^{-1}(z)$. Therefore, the derivative $(d(\phi|_z)/dZ)(y(x)) \neq 0$ for every point $x \in \pi^{-1}(z)$. Hence the differential $d_{\pi'(x)}\pi''$ is an isomorphism for every $x \in \pi^{-1}(z)$. Denote by $R = \mathrm{Res}_Z(\phi, \partial\phi/\partial Z) \in k[U']$ the discriminant of ϕ with respect to Z. Obviously $R(z) \neq 0$. We choose U' such that the $R(z_1) \neq 0$ for every $z_1 \in U'$. Then $\#\pi^{-1}(z_1) = \deg \pi$ for every $z_1 \in U'$. It is known that the integral closure of the ring $k[U''']$ is contained in the module $R^{-1}k[U''']$. Hence $k[U''']$ is integrally closed since $R^{-1} \in k[U''']$. Thus, the algebraic variety U''' is normal (respectively obviously U''' is smooth). In particular every $\pi'(x)$ is a normal (respectively smooth) point of U'''. By the Zariski main theorem applied to the morphism π' the point x is a normal (respectively smooth) point of $\pi^{-1}(U')$ and the differential $d_x\pi'$ is an isomorphism for every $x \in \pi^{-1}(z)$. Since $\pi = \pi'' \circ \pi'$ on $\pi^{-1}(U')$, this implies (iv). The lemma is proved.

LEMMA 3 *Let $W \subset \mathbb{P}^n(\overline{k})$ be a defined over k and irreducible over k projective algebraic variety and $\dim W = n - s$, $0 \leq s \leq n$. Let $g_0, g_{s+1}, \ldots, g_n \in k[X_0, \ldots, X_n]$ be homogeneous polynomials of the same degree and the morphism*

$$\rho : W \setminus \mathcal{Z}(g_0, g_{s+1}, \ldots, g_n) \to \mathbb{P}^{n-s}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (g_0 : g_{s+1} : \ldots : g_n)$$

is dominant. Let $\mathfrak{l} \subset \mathbb{P}^{n-s}(\overline{k})$ be a line. Then the dimension of every irreducible component of $\rho^{-1}(\mathfrak{l})$ is at least 1.

PROOF Indeed, after a nondegenerate linear transformation of $g_0, g_{s+1}, \ldots, g_n$ over k we can suppose without loss of generality that $\rho^{-1}(\mathfrak{l}) = W \cap \mathcal{Z}(g_{s+1}, \ldots, g_{n-1}) \setminus \mathcal{Z}(g_0, g_{s+1}, \ldots, g_n)$. This implies the required assertion. The lemma is proved.

LEMMA 4 *Under conditions of Lemma 3 let $x \in \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(g_0)$ be a point. Let x be an isolated point of $\rho^{-1}\rho(x)$. Let $\mathfrak{l} \subset \mathbb{P}^{n-s}(\overline{k})$ be a line containing*

the point $\rho(x)$. Suppose that there is $\widetilde{z} \in \mathfrak{l}$ such that the number of elements $\#\rho^{-1}(\widetilde{z}) = \deg \rho$. Let C be the projective curve such that $C \setminus \mathcal{Z}(g_0, g_{s+1}, \dots, g_n)$ is the union of all irreducible components of $\rho^{-1}(\mathfrak{l})$ containing x (such a curve C exists by Lemma 3). Denote by $\rho|_C : C \setminus \mathcal{Z}(g_0, g_{s+1}, \dots, g_n) \to \mathfrak{l}$ the restriction of ρ to C and $\mathfrak{l}$. Then the differential $d_x\rho$ is an isomorphism if and only if the differential $d_x(\rho|_C)$ is an isomorphism.

PROOF Similarly to the proof of Lemma 3 we shall suppose without loss of generality that $\rho^{-1}(\mathfrak{l}) = W \cap \mathcal{Z}(g_{s+1}, \dots, g_{n-1}) \setminus \mathcal{Z}(g_0, g_{s+1}, \dots, g_n)$ and $g_n(x) = 0$. Denote by C_γ, $\gamma \in \Gamma$, the family of all irreducible over $\overline{k}$ components of C. For arbitrary algebraic varieties E_1, E_2, E_3 denote by $i(E_1, E_2; E_3)$ the index of intersection, see [9], of E_1 and E_2 at the variety E_3 when this index is defined. Then it is known that, see [9],

$$i(W, \mathcal{Z}(g_{s+1}, \dots, g_n); x) = \sum_{\gamma \in \Gamma} i(W, \mathcal{Z}(g_{s+1}, \dots, g_{n-1}); C_\gamma) i(C_\gamma, \mathcal{Z}(g_n); x).$$

Further, if C is irreducible over $\overline{k}$ then $i(W, \mathcal{Z}(g_{s+1}, \dots, g_{n-1}); C) = 1$ since the corresponding intersection is transversal by Lemma 2 and due to the existence of $\widetilde{z}$. Now $i(W, \mathcal{Z}(g_{s+1}, \dots, g_n); x) = 1$ (respectively $i(C, \mathcal{Z}(g_n); x) = 1$) if and only if the differential $d_x\rho$ (respectively $d_x(\rho|_C)$) is an isomorphism. Hence if $d_x\rho$ is an isomorphism then $d_x(\rho|_C)$ is an isomorphism. Conversely, if $d_x(\rho|_C)$ is an isomorphism then $i(C, \mathcal{Z}(g_n); x) = 1$. Hence the curve C is irreducible over $\overline{k}$ and $i(W, \mathcal{Z}(g_{s+1}, \dots, g_{n-1}); C) = 1$. This implies that $d_x\rho$ is an isomorphism The lemma is proved.

Let the infinitesimals $\varepsilon_i > 0$, $1 \le i \in \mathbb{Z}$, and the fields k_i, $\overline{k_i}$, $i \ge 0$, supplied with a real structure be the same as in Section 2.

LEMMA 5 *Under conditions of Lemma 3 let W be a component of $V = \mathcal{Z}(f_1, \dots, f_m)$. Suppose that $x = (x_0 : \dots : x_n) \in W$, all $x_i \in \overline{k}$, $g_0(x) \ne 0$ and x is an isolated point of $\rho^{-1}\rho(x)$. Set $\widetilde{x} = (x_0, \dots, x_n) \in \mathrm{con}(W)$. Consider the system of polynomial equations and inequalities with respect to the indeterminates $X_0, \dots, X_n$, $Y_0, \dots, Y_n$ with coefficients from $\overline{k_3}$:*

$$\begin{cases} \sum_{s+1 \le i \le n} |g_i - g_i(\widetilde{x})|^2 = \varepsilon_2, \\ g_i - g_i(Y_0, \dots, Y_n) = 0, \qquad\qquad s+1 \le i \le n, \\ \sum_{0 \le i \le n} |X_i - X_i(\widetilde{x})|^2 \le \varepsilon_1, \\ \sum_{0 \le i \le n} |Y_i - X_i(\widetilde{x})|^2 \le \varepsilon_1, \\ \sum_{0 \le i \le n} |X_i - Y_i|^2 \ge \varepsilon_3, \\ g_0 = g_0(x_0, \dots, x_n), \\ g_0(Y_0, \dots, Y_n) = g_0(x_0, \dots, x_n). \end{cases} \tag{18}$$

Then system (18) has a solution

$$(x_0^*, \dots, x_n^*, y_0^*, \dots, y_n^*) \in \mathrm{con}(W) \times \mathrm{con}(W) \subset \mathbb{A}^{2n+2}(\overline{k}) \tag{19}$$

if and only if the differential $d_x\rho$, see Lemma 3, is not an isomorphism.

PROOF System (18) has solution (19) if and only if

(i) there are a point $z^* \in \mathbb{P}^{n-s}(\overline{k})$ and two distinct points $x^*, y^* \in \rho^{-1}(z^*)$ such that z^* is infinitely close to $\rho(x)$ and x^*, y^* are infinitely close to x.

Hence by the implicit function theorem it is sufficient to prove that

(ii) if the differential $d_x\rho$ is not an isomorphism then assertion (i) holds.

By Lemma 2 there is a point $z' \in \mathbb{P}^{n-s}(\overline{k})$ such that the number of elements $\#\rho^{-1}(z') = \deg\rho$. There exists a line $\mathfrak{l} \subset \mathbb{P}^{n-s}(\overline{k})$ such that $\rho(x) \in \mathfrak{l}$, $z' \in \mathfrak{l}$. Let C and $\rho|_C$ be the same as in Lemma 4. By Lemma 4 one can replace in (ii) the differential $d_x\rho$ by $d_x(\rho|_C)$. Further, in (i) one can replace ρ by $\rho|_C$ and $\mathbb{P}^{n-s}(\overline{k})$ by $\mathfrak{l}$. Using the Veronese isomorphism of degree $\deg g_0$, see [9], one can assume without loss of generality that ρ is a linear projection. For the linear projection of a curve assertion (ii) is straightforward, cf. [6]. The lemma is proved.

LEMMA 6 *Under conditions of Lemma 3 let* $z = (1 : z_{s+1} : \ldots : z_n) \in \mathbb{P}^{n-s}(\overline{k})$, *the numbers of elements* $\#\rho^{-1}(z) < \deg\rho$ *and for every* $x \in \rho^{-1}(z)$ *the differential* $d_x\rho$ *is an isomorphism. Consider the system of polynomial equations and inequalities with respect to the indeterminates* $X_0, \ldots, X_n$ *with coefficients from* $\overline{k_2}$*:*

$$\left\{\begin{array}{l} \sum_{s+1\le i\le n} |g_i - z_i|^2 = \varepsilon_2, \\ \sum_{0\le i\le n} |X_i|^2 \ge \varepsilon_1^{-1}, \\ g_0 = 1. \end{array}\right. \tag{20}$$

Then system (20) has a solution

$$(x_0^*, \ldots, x_n^*) \in \mathrm{con}(W) \subset \mathbb{A}^{n+1}(\overline{k_2}). \tag{21}$$

PROOF By Lemma 2 there is a point $\widetilde{z} = (1 : \widetilde{z}_{s+1} : \ldots : \widetilde{z}_n) \in \mathbb{P}^{n-s}(\overline{k})$ such that the numbers of elements $\#\rho^{-1}(\widetilde{z}) = \deg\rho$. Let $\mathfrak{l} \subset \mathbb{P}^{n-s}(\overline{k})$ be the line containing the points $z, \widetilde{z}$. Then by Lemma 2 and Lemma 5 there is a projective irreducible over $\overline{k}$ curve $C_1 \subset \mathbb{P}^n(\overline{k})$ such that $C_1 \setminus \mathcal{Z}(g_0, g_{s+1}, \ldots, g_n)$ is an irreducible component of $\rho^{-1}(\mathfrak{l})$ and the intersections $C_1 \cap \rho^{-1}(\widetilde{z}) \ne \emptyset$, $C_1 \cap \mathcal{Z}(g_0, g_{s+1}, \ldots, g_n) \ne \emptyset$ in $\mathbb{P}^n(\overline{k})$. Considering a branch of the curve C_1 at a point $\xi \in C_1 \cap \mathcal{Z}(g_0, g_{s+1}, \ldots, g_n)$ we get the required solution of system (20). The lemma is proved.

LEMMA 7 *Let* $Q \subset \mathbb{P}^n(\overline{k})$ *be a projective algebraic variety. Let* $g_0, \ldots, g_r \in \overline{k}[X_0, \ldots, X_n]$ *be homogeneous polynomials with* $\deg g_i = d'$ *if* $g_i \ne 0$. *Let* $\rho_1 : Q \setminus \mathcal{Z}(g_0, \ldots, g_r) \to \mathbb{P}^r(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (g_0 : \ldots : g_r)$, *be the regular morphism. Denote by* Q' *the closure in the Zariski topology of* $\rho_1(Q \setminus \mathcal{Z}(g_0, \ldots, g_r))$. *Suppose that* $\dim Q' \le \nu$. *Then* $\deg Q' \le (d')^\nu \deg Q$ *where by definition* $\deg Q$ *(respectively* $\deg Q'$*) is the sum of the degrees of all the irreducible components of all dimensions of* Q *(respectively* Q'*). Suppose additionally that all the irreducible components of* Q *are of dimensions at least* $n - s$ *and* Q *is a union of some irreducible components of the set of all zeroes of homogeneous polynomials of degrees less than* d. *Then by the Bézout theorem* $\deg Q' \le d^s(d')^\nu$.

PROOF We can suppose without loss of generality that Q is irreducible over $\overline{k}$ and $\dim Q' = \nu$. Let $\mathcal{L}$ be a linear subspace of $\mathbb{P}^r(\overline{k})$ of codimension ν in general position. The degree of the closure $\deg\overline{\rho_1^{-1}(Q' \cap \mathcal{L})} \le (d')^\nu \deg Q$ by the Bézout theorem. On the other hand, $\deg Q'$ is bounded from above by the number of connected components of $\rho_1^{-1}(Q' \cap \mathcal{L})$ and hence by the degree $\deg\overline{\rho_1^{-1}(Q' \cap \mathcal{L})}$. Therefore, $\deg Q' \le (d')^\nu \deg Q$. The lemma is proved.

LEMMA 8 *Let $C \subset \mathbb{P}^n(\overline{k})$ be a projective curve of degree D defined over k and and $g_0, g_1 \in k[X_0, \ldots, X_n]$ be homogeneous polynomials of the same degree D_1 such that for every irreducible over k component C_1 of C the polynomial g_0 is not vanishing on C_1 and $g_1/g_0 \in k(C_1)$ is transcendental over k. Consider the morphism $\tau : C \setminus \mathcal{Z}(g_0, g_1) \to \mathbb{P}^1(\overline{k})$, $\tau(x) = (g_0(x) : g_1(x))$. Then the number of points $z \in \mathbb{P}^1(\overline{k})$ such that $\#\tau^{-1}(z) < \deg \tau$ is bounded from above by $DD_1(DD_1 - 1)$.*

PROOF Let $k(C)$ be the total quotient ring of the ring of regular functions $k[C \setminus \mathcal{Z}(g_0)]$. Let $C \to v(C)$, see [9], be the Veronese isomorphism of degree $\deg g_0$. Then $\deg v(C) \le DD_1$ by the Bézout theorem. Replacing C by $v(C)$ we shall suppose without loss of generality that g_0 and g_1 are linear forms. By the theorem about primitive element there is a linear form $g_2 \in k[X_0, \ldots, X_n]$ such that the embedding $k[g_1/g_0, g_2/g_0] \to k[C \setminus \mathcal{Z}(g_0)]$ induces the isomorphism of $k(g_1/g_0)[(g_2/g_0)|_C] \simeq k(C)$ and additionally $C \cap \mathcal{Z}(e_0, e_1, e_2) = \emptyset$. Consider the regular morphism $\tau_1 : C \to \mathbb{P}^2(\overline{k})$, $\tau_1(x) = (g_0(x) : g_1(x) : g_2(x))$. Then $\tau_1(C) = C_2 \subset \mathbb{P}^2(\overline{k})$ is a projective curve of degree at most DD_1. Hence $C_2 = \mathcal{Z}(\Phi)$ where $\Phi \in k[X_0, X_1, X_2]$ is a separable polynomial of degree at most DD_1. The morphism $\tau_2 : C \to C_2$ induced by τ_1 is finite birational isomorphism. Denote by $R = \mathrm{Res}_{X_2}(\Phi, \partial\Phi/\partial X_2)$ the discriminant of Φ with respect to X_2 (here and below by definition the discriminant is the resultant of the polynomial and its derivative; this definition is different from the generally accepted by a factor $\mathrm{lc}_{X_2}\Phi$, but it is more convenient for us). Denote by $\tau_3 : C_2 \setminus \mathcal{Z}(g_0, g_1) \to \mathbb{P}^1(\overline{k})$ the morphism induced by τ. Then the restriction of τ_2 is the isomorphism $C \setminus \tau^{-1}(\mathcal{Z}(R)) \to C_2 \setminus \tau_3^{-1}(\mathcal{Z}(R))$. Further consider the projection $\tau_4 : C_2 \setminus \tau_3^{-1}(\mathcal{Z}(R)) \to \mathbb{P}^1(\overline{k}) \setminus \mathcal{Z}(R)$ which is the restriction of τ_3. Then τ_4 is étale, see the definition in [9]. Note that $\tau_3 \circ \tau_2$ is the restriction of τ. The degree $\deg(R) \le DD_1(DD_1 - 1)$. This implies the assertion of the lemma. The lemma is proved.

4 Proof of assertions (a)–(d)

Now we proceed to the description of the algorithm for Theorem 1. Let us compute $\dim W$ by [6] or Theorem 2 of [8]. Let us decide using, e.g., Theorems 1 and 2 from [8] whether e_0 vanishes on W. Performing if necessary a permutation of indices $0, \ldots, r$ we shall suppose without loss of generality in what follows that e_0 does not vanish on W. Let $L_1, \ldots, L_{n+1}$ be linear forms introduced at the beginning of Section 2. We have $W \cap \mathcal{Z}(L_{s+1}, \ldots, L_n) \cap \mathcal{Z}(e_0) = \emptyset$. Hence using Theorems 1 and 2 of [8] we can construct a point $\widetilde{x}^{(0)} \in W$ that is a smooth point of V and $e_0(\widetilde{x}^{(0)}) \neq 0$. Replacing $x^{(0)}$ by $\widetilde{x}^{(0)}$ we shall suppose in what follows that that $e_0(x^{(0)}) \neq 0$ and that $x^{(0)}$ is a smooth point of V. Using Theorem 5 of [6] one can decide whether a given family of rational functions from $k(W)$ is a basis of transcendency of $k(W)$. As an easy consequently one can compute the transcendency degree over k of the given family of rational functions from $k(W)$ (one need only to add to the given family the known basis of transcendency $k(W)$ and then apply Theorem 5 of [6] to subfamilies of the new obtaned family of rational functions). So we compute the transcendency degree of the family of rational functions $e_1/e_0, \ldots, e_r/e_0 \in k(W)$ over k, i.e., $\dim W'$. We shall suppose in what follows without loss of generality in the proof that $\dim W = \dim W' = n - s$. We compute also applying Theorem 5 of [6]

indices $0 = i_0 < \ldots < i_{n-s} \le r$ such that the transcendency degree of the family of rational functions $e_{i_j}/e_{i_0} \in k(W)$, $1 \le j \le n-s$, is $n-s$. Performing if necessary a permutation of $0, \ldots, n$ we shall suppose in what follows that $i_j = j$ for all $0 \le j \le n-s$. In what follows applying Lemmas 3–6 we set W to be the considered irreducible component of V and $g_0 = e_0$, $g_i = e_{i-s}$, $s+1 \le i \le n$. Hence the morphism π_n from Section 2 is the restriction of ρ.

Now we are going to describe a recursion where $z' \in \mathbb{P}^{n-s}(\overline{k})$ is the current point. At the end of this recursion we get z' such that the number of elements $\#\rho^{-1}(z') = \deg \rho$, all the elements of $\rho^{-1}(z')$ are smooth points of V, and all the elements from $p(\rho^{-1}(z'))$ are smooth points of W'. As the base set $z' = \rho(x^{(0)})$. At each step $X_0(z') \ne 0$ (we suppose that $X_0, \ldots X_{n-s}$ are homogeneous coordinates on $\mathbb{P}^{n-s}(\overline{k})$) and $\rho^{-1}(z') \ne \emptyset$. For the point z' we shall define the integers $N_i(z') \ge 0$, $0 \le i \le 5$. At the end of each step that is not final we get a point z'' similar to z' such that $N_i(z'') \ge N_i(z')$ for $i = 1, 3, 4, 5$ and at least one of these four inequalities is strict. Further, we shall replace z' by z'' and proceed to the next step. The estimate for the number of steps will be obtained from the Bézout theorem.

Let us describe the general step of this recursion. Let us represent $z' = (1 : z'_1 : \ldots : z'_{n-s})$. Hence all $z'_i \in \overline{k}$, $1 \le i \le n-s$. Applying Theorem 2 to $\mathrm{con}(V)$ and

$$U'' = \left\{x \in \mathbb{A}^{n+1}(\overline{k}) \,:\, e_i(x) - z'_i = 0, \quad 0 \le i \le n-s\right\},$$

we construct a finite set S_0 of points of V such that the intersection of S_0 with every connected component of $\rho^{-1}(z')$ is nonempty. The number of elements $\#S_0$ is bounded from above by a polynomial in $(dd')^n$ by Theorem 2. Applying, Theorem 2 [8] we shall suppose without loss of generality that $S_0 = S_0(z') \subset W$. Hence $S_0(z') \ne \emptyset$ since $\rho^{-1}(z') \ne \emptyset$ by the assumption of the recursion. Let $x \in S_0$. Then $e_0(x) \ne 0$. Let $x = (x_0 : \ldots : x_n)$ where all $x_i \in \overline{k}$. Denote by U''_x the set of points from $\mathbb{A}^{n+1}(\overline{k_1})$ satisfying the following system of polynomial equations and inequalities with coefficients from $\overline{k_1}$:

$$\left\{\begin{array}{ll} \sum_{0 \le i \le n} |X_i - x_i|^2 = \varepsilon_1, & \\ e_i - z'_i e_0 = 0, & 1 \le i \le n-s, \\ e_0 = e_0(x). & \end{array}\right. \tag{22}$$

For every $x \in S_0$ using Theorem 2 [8] and applying Theorem 2 to $\mathrm{con}(V)$ and U''_x we decide whether there is a point $\widetilde{x} \in \rho^{-1}(z')$ that is infinitely close to x, i.e., whether x is not an isolated point of W. So deleting some points from S_0 we get the subset $S_1 = S_1(z')$ *of all isolated points of* $\rho^{-1}(z')$. Denote by $S_2 = S_2(z')$ *the set of all points of* $S_1(z')$ *which belong to the unique irreducible over* $\overline{k}$ *component of* V (i.e., only to one of the irreducible over $\overline{k}$ components of W). By Theorem 2 [8] using the given point $x^{(0)} \in W$ we construct the set $S_2(z')$. Put $S_5(z') = p(S_1(z'))$. The set $S_5(z')$ consists of classes of conjugated over k points of $\mathbb{P}^r(\overline{k})$. Hence one can easily construct these classes and compute the number of elements $\#S_5(z')$.

For every $x \in S_1$ using Theorem 2 [8] and applying Theorem 2 to $\mathrm{con}(V) \times \mathrm{con}(V)$ we decide whether system (18) has a solution (19) and construct this solution if it exists. Set $x^* = (x_0^* : \ldots : x_n^*) \in W(\overline{k_3})$ and $z^* = \rho(x^*) \in \mathbb{P}^{n-s}(\overline{k_3})$ for solution (19). Denote by $S_3 = S_3(z')$ *(respectively* $S_4 = S_4(z')$*) the set of all* $x \in S_1(z')$ *(respectively* $x \in S_2(z')$*) such that the differential* $d_x\rho$ *is an*

isomorphism. Hence by Lemma 5 and Theorem 2 one can construct the sets $S_3(z')$ and $S_4(z')$.

Let $z^{(2)} = (1 : z_1^{(2)} : \ldots : z_{n-s}^{(2)}) \in \mathbb{P}^{n-s}(\overline{k_\alpha})$ be an arbitrary point where $0 < \alpha \in \mathbb{Z}$ is arbitrary but fixed (for estimates of the complexity of algorithms). Let $X_0(z^{(2)}) \neq 0$ and $\rho^{-1}(z^{(2)}) \neq \emptyset$. Let us define the sets $S_i(z^{(2)})$, $1 \leq i \leq 5$, replacing in the definition of the sets S_i the point z' by $z^{(2)}$ and the field k by a finite extension of k_α containing the coordinates of the point $z^{(2)}$. We can construct the sets $S_i(z^{(2)})$, $0 \leq i \leq 5$, similarly to $S_i(z)$ replacing the ground field. Denote the number of elements $\#S_i(z^{(2)}) = N_i(z^{(2)})$, $0 \leq i \leq 5$.

Let $\mathfrak{l} \subset \mathbb{P}^{n-s}(\overline{k_\alpha})$ be a line through a point $z^{(2)}$. By the Bézout theorem there are at most a polynomial in $d^n(d')^{n-s}$ number of points $z \in \mathfrak{l}$ such that $\rho^{-1}(z) = \emptyset$. Denote by $\mathfrak{c}$ the union of all the irreducible components E of $\rho^{-1}(\mathfrak{l})$ such that $E \cap S_1(z^{(2)}) \neq \emptyset$. Suppose that $S_1(z^{(2)}) \neq \emptyset$. Then $\mathfrak{c}$ is a curve and $N_1(z) \leq d' \deg \mathfrak{c} \leq (d')^{n-s} d^s$ for every $z \in \mathfrak{l}$ by the definition of $\mathfrak{c}$ and the Bézout theorem. Denote by $\rho|_{\mathfrak{c}} : \mathfrak{c} \to \mathfrak{l}$ the restriction of ρ to $\mathfrak{c}$ and $\mathfrak{l}$. By Lemma 8 and the Bézout theorem there is at most a polynomial in $d^n(d')^{n-s}$ number of points $z \in \mathfrak{l}$ such that $\#\rho^{-1}(z) \cap \mathfrak{c} \neq \deg \rho|_{\mathfrak{c}}$ or $N_2(z) < N_2(z^{(2)})$. Let $x' \in S_3(z^{(2)})$. Considering the local parameters of W in the point x' with degrees bounded from above by d^s, cf. the proof of Lemma 1, one sees that there is a polynomial $\Delta_{x'} \in k[X_0, \ldots, X_n]$ (it is a minor of the corresponding Jacobi matrix) such that $\deg \Delta_{x'} < sd^s + (n-s)(d')^{n-s}$, $\Delta_{x'}(x') \neq 0$ and $d_x\rho$ is an isomorphism for every $x \in W \setminus \mathcal{Z}(\Delta_{x'})$. Hence there is at most a polynomial in $d^s(d')^{n-s}$ number of points $z \in \mathfrak{l}$ such that $N_3(z) < N_3(z^{(2)})$ or $N_4(z) < N_4(z^{(2)})$. Finally, let $\nu = \max\{\#p((\rho^{-1}(z) \cap \mathfrak{c})) : z \in \mathfrak{l}\}$. Hence $\nu \geq N_5(z^{(2)})$. Then there is a linear form $L_0' \in k[X_0, \ldots, X_r]$ such that $\nu = \max\{\#(L_0'/X_0)(p(\rho^{-1}(z) \cap \mathfrak{c})) : z \in \mathfrak{l} \setminus \mathcal{Z}(X_0)\}$. Considering the corresponding resultant (we leave the details to the reader) one sees that there are at most a polynomial in $d^s(d')^{n-s}$ number of point $z \in \mathfrak{l} \setminus \mathcal{Z}(X_0)$ such that $\#(L_0'/X_0)(p(\rho^{-1}(z) \cap \mathfrak{c})) \neq \nu$.

Thus, $\mathfrak{l}$ contains at most a polynomial in $d^n(d')^{n-s}$ number of points $z^{(3)}$ such that $N_i(z^{(3)}) < N_i(z^{(2)})$ for some $1 \leq i \leq 5$ or $\rho^{-1}(z^{(3)}) = \emptyset$. Hence using the algorithm of reduction to integer coefficients one can replace subsequently the coordinates $z_1^{(2)}, \ldots, z_{n-s}^{(2)}$ by integers $z_1^{(4)}, \ldots, z_{n-s}^{(4)}$ with lengths $O(n \log d + (n-s)\log(d'))$ and obtain a point $z^{(4)} = (1 : z_1^{(4)} : \ldots : z_{n-s}^{(4)}) \in \mathbb{P}^{n-s}(\overline{k})$ such that $N_i(z^{(4)}) \geq N_i(z^{(2)})$ for all $1 \leq i \leq 5$ and $\rho^{-1}(z^{(4)}) \neq \emptyset$. We shall refer to this construction with the input $z^{(2)}$ and the output $z^{(4)}$ as to *the second auxiliary algorithm.*

Let us return to the description of the algorithm. Suppose that $N_0(z') = N_1(z')$ and system (18) has a solution (19) for some $x \in S_1(z')$. Then $N_1(z^*) > N_1(z')$. Besides that, $N_i(z^*) \geq N_i(z')$ for $i = 3, 4, 5$ since z^* is infinitely close to z'. Using the second auxiliary algorithm with the input z^* we get a point z'' such that $N_1(z'') > N_1(z)$ and $N_i(z'') \geq N_i(z')$ for $i = 3, 4, 5$. Then we replace z' by z'' and proceed to the next step of the recursion.

Now suppose that $N_0(z') = N_1(z')$ but for every $x \in S_1(z')$ system (18) does not have a solution (19). Then $N_0(z') = N_1(z') = N_3(z')$. Suppose that in the considered case $N_4(z') < N_3(z')$. Then applying Theorem 2 [8] we construct a point $x' \in S_3(z')$ that belongs to more than one irreducible over $\overline{k}$ component of V. Similarly to the construction of the point $\widetilde{x}_s$ in the first auxiliary algorithm we compute a point $\widetilde{x} \in W$ that is a smooth point of V and is infinitely close to x'. Set $\widetilde{z} = \rho(\widetilde{x})$. Then $N_i(\widetilde{z}) \geq N_i(z')$ for $i = 1, 3, 5$ and $N_4(\widetilde{z}) > N_4(z')$. In

this case as above applying the second auxiliary algorithm we construct a point z'' such that $N_i(z'') \geq N_i(z')$ for $i = 1, 3, 5$ and $N_4(z'') \geq N_4(\widetilde{z}) > N_4(z')$, then replace z' by z'' and proceed to the next step of the recursion.

Now suppose that $N_0(z') = N_1(z') = N_3(z') = N_4(z')$. Then using Theorem 2 [8] and applying Theorem 2 to $\mathrm{con}(V)$ we decide whether system (20) has solution (21) and construct this solution if it exists. By Lemma 6 such a solution exists if and only if $N_4(z') < \deg \rho$. Set $x^* = (x_0^* : \ldots : x_n^*) \in W(\overline{k_2})$ and $z^* = \rho(x^*) \in \mathbb{P}^{n-s}(\overline{k_2})$ for solution (21).

Suppose that solution (21) exists. Then we decide whether $x^* \in S_1(z^*)$. Since $\sum_{0 \leq i \leq n} |x_i^*|^2$ is infinitely large and $e_0(x_0^*, \ldots, x_n^*) = 1$ the point x^* is not infinitely close to any point from $S_1(z')$. On the other hand, by the implicit function theorem there are $N_1(z')$ point of $S_1(z^*)$ which are infinitely close to the corresponding points from $S_1(z')$. Hence $N_1(z^*) \geq N_1(z')$ and $N_i(z^*) \geq N_i(z')$ for $i = 3, 4, 5$. Besides that, if $x^* \in S_1(z^*)$ then $N_1(z^*) > N_1(z')$. In the last case as above applying the second auxiliary algorithm we construct a point z'' such that $N_1(z'') > N_1(z')$ and $N_i(z'') \geq N_i(z')$ for $i = 3, 4, 5$. Then replace z' by z'' and proceed to the next step of the recursion.

Now we are going to consider simultaneously two cases:

1) $N_0(z') = N_1(z') = N_3(z') = N_4(z') < \deg \rho$ and $x^* \notin S_1(z^*)$ for the constructed x^*,

2) $N_0(z') \neq N_1(z')$.

In the case 2) we set $z^* = z'$ and choose an arbitrary point $x^* \in S_0(z') \setminus S_1(z')$ So now $x^* \in \rho^{-1}(z^*) \setminus S_1(z^*)$ and $z^* \in \mathbb{P}^{n-s}(\overline{k_2})$ for the both cases 1) and 2). The point x^* is not infinitely close to any point from $S_1(z^*)$. Let us replace, see (16), in the construction of the point $\widetilde{x}_s$ in the first auxiliary algorithm $\widetilde{x}_s$ by $\widetilde{x}$ and the ground field k by k_2 (so k_2 is replaced by k_4). Then similarly to the considered construction we compute a point $\widetilde{x} \in W(\overline{k_4})$ that is a smooth point of V and is infinitely close to x^* with respect to the field $\overline{k_2}$. Then $\widetilde{x} \notin \mathcal{Z}(e_0, \ldots, e_r)$. Set $\widetilde{z} = p(\widetilde{x})$. Then $\widetilde{z}$ is infinitely close to z^* with respect to the field k_2. Hence $N_i(\widetilde{z}) \geq N_i(z^*)$ for $i = 1, 3, 4, 5$. If $N_1(\widetilde{z}) > N_1(z^*)$ then we apply the second auxiliary algorithm to the point $\widetilde{z}$, obtain a point z'', replace z' by z'' and proceed to the next step of the recursion.

Suppose that $N_1(\widetilde{z}) = N_1(z^*)$. Hence the points of $S_1(z^*)$ and $S_1(\widetilde{z})$ are in the one–to–one correspondence by the implicit function theorem. Therefore, $\widetilde{x} \notin S_1(\widetilde{z})$. Then replacing the ground field k by k_4 and x^* by $\widetilde{x}$ we shall suppose without loss of generality that $x^* \in W(\overline{k_4})$ is a smooth point of V. Let us choose a linear form L_0 such that $L_0(x^*) \neq 0$, see the beginning of Section 2. So we have at present linear forms $L_0, L_{s+1}, \ldots, L_n$. Let us apply the first auxiliary algorithm to the point x^* (now one needs to replace in this algorithm $\varepsilon_1, \ldots, \varepsilon_5$ by $\varepsilon_5, \ldots, \varepsilon_9$ respectively) and get $x^{**} \in \mathbb{P}^{n-s}(\overline{k_6})$. Put $z^{**} = \rho(x^{**})$. Then $N_1(z^{**}) > N_1(z^*) \geq N_1(z')$. The point x^{**} is infinitely close to x^* with respect to the field k_4. Hence $N_i(z^{**}) \geq N_i(z^*)$, $i = 3, 4, 5$. As above applying the second auxiliary algorithm to the input z^* we construct a point z'' such that $N_1(z'') > N_1(z')$, $N_i(z'') \geq N_i(z)$, $i = 3, 4, 5$, replace z' by z'' and proceed to the next step of the recursion.

Thus, finally we shall come to the case when $N_0(z') = N_1(z') = N_3(z') = N_4(z')$ and system (20) does not have solution (21). Then by Lemma 6 the number of elements $\#\rho^{-1}(z') = \deg \rho = N_4(z')$.

Let $X_0, \ldots, X_r$ be the homogeneous coordinate functions of $\mathbb{P}^r(\overline{k})$. Denote by $\rho_2 : W' \setminus \mathcal{Z}(X_0, \ldots, X_{n-s}) \to \mathbb{P}^{n-s}(\overline{k})$, $(X_0, \ldots, X_r) \mapsto (X_0 : \ldots : X_{n-s})$ the linear projection. Then according to our definitions $\rho = \rho_2 \circ \rho_1$ where ρ_1 is the restriction of p' to $W \setminus \mathcal{Z}(e_0, \ldots, e_{n-s})$. Now $N_4(z') = \deg \rho = \deg \rho_2 \deg \rho_1$.

Let $x = (x_0, \ldots, x_n) \in S_1(z')$ and all $x_j \in \overline{k}$. Consider the system of polynomial equations and inequalities in $X_0, \ldots, X_n, Y_0, \ldots, Y_n$ with coefficients from $\overline{k_2}$:

$$\begin{cases} e_j = e_j(Y_0, \ldots, Y_n), & 1 \le j \le n-s, \\ \sum_{1 \le j \le n-s} |e_j - z'_j|^2 \le \varepsilon_1, \\ \sum_{0 \le j \le r} |e_j - e_j(Y_0, \ldots, Y_r)|^2 = \varepsilon_2, \\ e_0 = 1, \\ e_0(Y_0, \ldots, Y_r) = 1. \end{cases} \tag{23}$$

LEMMA 9 *Let $N_4(z') = \deg \rho$. Then the number of elements $\# S_5(z') = N_5(z') = \deg \rho_2$ if and only if system (23) does not have a solution*

$$(x_0^*, \ldots, x_n^*, y_0^*, \ldots, y_n^*) \in \mathrm{con}(W) \times \mathrm{con}(W) \subset \mathbb{A}^{2n+2}(\overline{k_2}). \tag{24}$$

Besides that, if $N_5(z') = \deg \rho_2$ then $p(\rho^{-1}(z')) = \rho_2^{-1}(z')$. Hence then the number of elements $\# \rho_2^{-1}(z') = \deg \rho_2$, by Lemma 2 every $x' \in \rho_2^{-1}(z')$ is a smooth point of W', and the differential $d_{x'} \rho_2$ is an isomorphism. Further, consider an arbitrary solution (24) of system (23). Set $z^* = \rho((x_0^* : \ldots : x_n^*))$. Then $N_5(z^*) > N_5(z')$.

PROOF By Lemma 2 there is an open in the Zariski topology neighborhood U of the point z' such that the morphism $\rho^{-1}(U) \to U$ induced by ρ is finite dominant, the number of elements $\# \rho^{-1}(z) = \deg \rho$ for every $z \in U$, and all the points from $\rho^{-1}(U)$ are smooth points of V. Hence the morphism $\rho_2^{-1}(U) \to U$ induced by ρ_2 is also finite dominant. Therefore, $p(\rho^{-1}(z')) = \rho_2^{-1}(z')$ for every $z \in U$ and $N_5(z) = \# \rho_2^{-1}(z) \le \deg \rho_2$ by Lemma 2.

If $N_5(z') = \deg \rho_2$ then by Lemma 2 the numbers of elements $\# \rho_1^{-1}(z''') = \deg \rho_1 = \deg p'$ for every $z''' \in \rho_2^{-1}(z')$. Hence by Lemma 2 and the implicit function theorem system (23) does not have solution (24). The inverse implication is also true by Lemma 2.

On the other hand, consider an arbitrary solution (24). Denote $y^* = (y_0^* : \ldots : y_n^*)$. The morphism ρ_2 is finite dominant and z^* is infinitely to close to z'. Hence for every $y \in \rho^{-1}(z')$ there is $y' \in \rho^{-1}(z^*)$ such that $\rho_1(y')$ is infinitely close to $\rho_1(y)$. Further, the points $\rho_1(x^*), \rho_1(y^*) \in \rho_2^{-1}(z^*)$ are infinitely close to $\rho_1(y) \in \rho_2^{-1}(z')$ for some $y \in \rho^{-1}(z')$. Any two points from $\rho_2^{-1}(z')$ are not infinitely close. Hence $N_5(z') < N_5(z^*) \le \deg \rho_2$ since $z^* \in U$. The lemma is proved.

Let us return to the description of the general step of the recursion. We consider the case when $N_i(z') = \deg \rho$ for $i = 1, 3, 4$. Let us decide using Theorem 2 whether system (23) has solution (24) and construct such a solution if it exists. Suppose that system (23) has a solution (24). We construct the point $z^* = \rho((x_0^* : \ldots : x_n^*))$. Then $N_i(z^*) = N_i(z')$ for $i = 1, 3, 4$ by Lemma 2 since z^* is infinitely close to z'. Further, $N_5(z^*) > N_5(z')$ by Lemma 9. We apply the second auxiliary algorithm to the point z^* and obtain z'' such that $N_i(z'') = N_i(z')$ for $i = 1, 3, 4$ and $N_5(z'') \ge N_5(z^*) > N_5(z')$. We replace z' by z'' and proceed to the next step of the recursion.

If system (23) does not have a solution then $N_5(z') = \deg \rho_2$ by Lemma 9 and the recursion is finished. The point z' satisfy assertion (b) of Theorem 1 by Lemma 2. Note that at every step of the described recursion $N_i(z') \le N_0(z')$, $1 \le i \le 5$, and $N_0(z')$ is bounded from above by a polynomial in $(dd')^n$, see above. Hence the total number of steps in the described recursion is bounded from above by a polynomial in $(dd')^n$. The algorithm for assertions (a) and (b) of Theorem 1 is described.

Let us describe the algorithm for (c). We use the recursion on r. The case $r = n - s$ is trivial. Let $z' = (1 : z'_1 : \ldots : z'_{n-s})$ be the point constructed in the algorithm from (b). By Lemma 7 the degree $\deg W' \le d^s(d')^{n-s}$. Hence one can construct a point $y = (1 : z'_1 : \ldots : z'_r)$ such that $y \notin p(\rho^{-1}(z'))$ and all z'_j, $n - s + 1 \le j \le r$ are integers with lengths $O(n \log d + (n - s) \log d')$. Then by Lemma 2 the point $y \notin W'$.

Denote by $p_y : \mathbb{P}^r(\overline{k}) \to \mathbb{P}^{r-1}(\overline{k})$ the linear projection with the center y. Then $p_y(W')$ is closed in $\mathbb{P}^{r-1}(\overline{k})$ and p_y induces the finite birational morphism $p'_y : W' \to p_y(W')$.

REMARK 5 *Notice that* $\deg W' = \deg p_y(W')$. *If* $r > n - s + 1$ *then one can choose* $z'_r = 0$.

Now we apply recursively the algorithm from (c) for the morphism $p_y \circ p : W \to \mathbb{P}^{r-1}(\overline{k})$. So the analog of (7) holds for $p_y(W')$; $r - 1$; and some constructed linear forms $\overline{L}_0, \overline{L}_{s+1}, \ldots, \overline{L}_n \in k[X_0, \ldots, X_{r-1}]$ in place of W'; r; $L'_0, L'_{s+1}, \ldots, L'_n \in k[X_0, \ldots, X_r]$ respectively. Set $L''_j = \overline{L}_j(X_1 - z'_1X_0, \ldots, X_r - z'_rX_0)$, $j \in \{0, s+1, \ldots, n\}$. Then $L''_0, L''_{s+1}, \ldots, L''_n$ are linear forms from $k[X_0, \ldots, X_r]$ with integer coefficients such that (7) is satisfied with $L''_0, L''_{s+1}, \ldots, L''_n$ in place of $L'_0, L'_{s+1}, \ldots, L'_n$.

Set $e''_i = L''_i(e_0, \ldots, e_r)$, $i \in \{0, s+1, \ldots, n\}$. Denote by

$$\rho'' : W \setminus \mathcal{Z}(e''_0, e''_{s+1}, \ldots, e''_n) \to \mathbb{P}^{n-s}(\overline{k}), \quad (X_0, \ldots, X_n) \mapsto (e''_0 : e''_{s+1} : \ldots : e''_n) \tag{25}$$

the dominant morphism. Now applying the algorithm from (b) for ρ'' in place of ρ one computes $\deg \rho''$. By Lemma 1 [6] this degree $\deg \rho'' = \deg p' \deg W'$. So $\deg W'$ is computed.

Let us identify $\mathbb{A}^{(r+1)(n-s+1)}(\overline{k})$ with the space of all $(n - s + 1)$–tuples of linear forms from $\overline{k}[X_0, \ldots, X_r]$, cf. assertion (d) of Theorem 1. Then for any line $\mathfrak{l} \subset \mathbb{A}^{(r+1)(n-s+1)}(\overline{k})$ such that $(L''_0, L''_{s+1}, \ldots, L''_n) \in \mathfrak{l}$ there are at most a polynomial in $\deg W'$ number of elements $(L'''_0, L'''_{s+1}, \ldots, L'''_n) \in \mathfrak{l}$ such that (7) does not hold for $L'''_0, L'''_{s+1}, \ldots, L'''_n$. One can decide whether (7) holds for any $(L'''_0, L'''_{s+1}, \ldots, L'''_n) \in \mathfrak{l}$ as follows. Set $e'''_i = L'''(e_0, \ldots, e_r)$, $i \in \{0, s+1, \ldots, n\}$ and define ρ''' replacing in the definition of ρ'' the linear forms $L''_0, L''_{s+1}, \ldots, L''_n$ by $L'''_0, L'''_{s+1}, \ldots, L'''_n$. Let us apply the algorithm from (b) for ρ''' in place of ρ. Now by Lemma 1 [6] and the Bézout theorem $\deg \rho''' \le \deg(p') \deg W'$ and this inequality is strict if and only if (7) does not hold for $L'''_0, L'''_{s+1}, \ldots, L'''_n$.

Hence using the algorithm of reduction to integer coefficients one can replace subsequently all nonzero coefficients of $L''_0, L''_{s+1}, \ldots, L''_n$ by integers of length $O(n \log d + (n - s) \log(d'))$ and obtain $L^*_0, L^*_{s+1}, \ldots, L^*_n$ such that (7) holds for $L^*_0, L^*_{s+1}, \ldots, L^*_n$ in place of $L'_0, L'_{s+1}, \ldots, L'_n$. Set $e^*_i = L^*(e_0, \ldots, e_r)$, $i \in \{0, s+1, \ldots, n\}$ and define ρ^* replacing in the definition of ρ'' the linear forms $L''_0, L''_{s+1}, \ldots, L''_n$ by $L^*_0, L^*_{s+1}, \ldots, L^*_n$. Further, applying the algorithm from (b) for the morphism ρ^* in place of ρ one obtains a point $z^* = (1 : z^*_{s+1} : \ldots : z^*_n)$

similar to z'. Hence all z_j^* are integers of length $O(n \log d + (n-s)\log(d'))$. Finally we set $L'_0 = L_0^*$ and $L'_j = L_j^* - z_j^* L_0^*$. Now (4) by Lemma 2, and (6), (3), (5) hold. The algorithm for assertion (c) is described. The required estimation for the working time of the algorithm from (a)–(c) follows immediately from the ones of the applied algorithms.

Let us prove (d). Set W'_1 to be the closure in the Zariski topology of $p(W \cap (\overline{V \setminus W}) \setminus \mathcal{Z}(e_0, \ldots, e_r))$. By Lemma 2 conditions (3)–(6) holds if and only if (3) and (6) are satisfied, $W' \cap \mathcal{Z}(L'_0, L'_{s+1}, \ldots, L'_n) = \emptyset$, and $W'_1 \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n) = \emptyset$. But, see, e.g., [10], from elimination theory it follows that the set of all $(L'_0, L'_{s+1}, \ldots, L'_n)$ such that $W' \cap \mathcal{Z}(L'_0, L'_{s+1}, \ldots, L'_n) = \emptyset$ (respectively $W'_1 \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n) = \emptyset$) is a nonempty open in the Zariski topology subset of $\mathbb{A}^{(r+1)(n-s+1)}(\overline{k})$. Hence also $\mathcal{U}'_0$ is nonempty and open in the Zariski topology by Lemma 2.

Let $(L'_0, L'_{s+1}, \ldots, L'_n) \in \mathfrak{l}' \cap \mathcal{U}'_0$ be an arbitrary element (not necessary constructed above). Set $e'_i = L'(e_0, \ldots, e_r)$, $i \in \{0, s+1, \ldots, n\}$ and define ρ' replacing in the definition of ρ'' the linear forms $L''_0, L''_{s+1}, \ldots, L''_n$ by $L'_0, L'_{s+1}, \ldots, L'_n$. Set

$$\mathfrak{l}'' = \bigcup_{(L''_0, L''_{s+1}, \ldots, L''_n) \in \mathfrak{l}'} \mathcal{Z}(L''_{s+1}, \ldots, L''_n) \subset \mathbb{P}^{n-s}(\overline{k}).$$

Then $\mathfrak{l}''$ is a line or consists of one point. If $\mathfrak{l}''$ is a point then assertion (d) is trivial. Suppose that $\mathfrak{l}''$ is a line. Recall that in the second auxiliary algorithm for (b) we get the estimations for the number of bad points of the line $\mathfrak{l}$, i.e., points z such that $N_i(z) < N_i(z^{(2)})$ for some $0 \le i \le 5$. Let us apply these estimations from the second auxiliary algorithm to ρ', $\mathfrak{l}''$ and the point from $\mathcal{Z}(L'_{s+1}, \ldots, L'_n)$ in place of ρ, $\mathfrak{l}$ and $z^{(2)}$ respectively. Then we obtain immediately assertion (d). Assertion (d) is proved.

5 Proof of assertions (e) and (f)

Now our aim is to prove (f). Let $L'_j \in \overline{k}[X_0, \ldots, X_r]$, $j \in \{0, s+1, s+2, \ldots, n\}$, and (3) holds. Recall that $e'_i = L'_j(e_0, \ldots, e_r)$, $j \in \{0, s+1, s+2, \ldots, n\}$. Set

$$\widetilde{W_i} = \overline{(W \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_i)}, \quad s \le i \le n. \tag{26}$$

Put W_i, $s \le i \le n$, to be the union of all the irreducible over $\overline{k}$ components E of $\widetilde{W_i}$ such that E contains a point from $A = W \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_n) \setminus \mathcal{Z}(e_0, \ldots, e_r)$. Then by (3), Lemma 2 and the implicit function theorem $\dim W_i = n - i$ and for every irreducible component E of W_i the dimension $\dim \overline{p(E \setminus \mathcal{Z}(e_0, \ldots, e_r))} = n - i$.

LEMMA 10 *Suppose that (3) holds for linear forms $L'_j \in \overline{k}[X_0, \ldots, X_r]$, $j \in \{0, s+1, s+2, \ldots, n\}$. Then the set $W' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n) = p(A)$ is finite. If additionally $A \cap \mathcal{Z}(e'_0) = \emptyset$ then $W' \cap \mathcal{Z}(L'_0, L'_{s+1}, \ldots, L'_n) = \emptyset$.*

PROOF We can assume without loss of generality that $A \cap \mathcal{Z}(e'_0) = \emptyset$. Let us define the morphism ρ' replacing in (25) all L''_j, e''_j by L'_j, e'_j. Then by the theorem about dimensions of fibers, see [11], the morphism ρ' is dominant. Hence the morphism $\rho'_2 : W' \setminus \mathcal{Z}(L'_0, L'_{s+1}, \ldots, L'_n) \to \mathbb{P}^{n-s}(\overline{k})$, $(X_0 : \ldots : X_r) \mapsto (L'_0, L'_{s+1} : \ldots : L'_n)$ is also dominant. By (3) and Lemma 2 there is a

neighborhood U with respect to the Zariski topology of the point $z = (1 : 0 : \ldots : 0)$ such that the morphism $(\rho')^{-1}(U) \to U$ induced by ρ' is finite dominant. Hence the morphisms $(\rho')^{-1}(U) \to (\rho'_2)^{-1}(U)$ and $(\rho'_2)^{-1}(U) \to U$ induced by p and ρ'_2 are also finite dominant. This implies the required assertions. The lemma is proved.

For $s \le i \le n$ denote by W'_i the intersection of $W' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_i)$ in $\mathbb{P}^r(\overline{k})$. So $p^{-1}(W'_i)$ is a subvariety of (26). Denote by $W''_i \subset W'_i$ the subset of all points $z \in W'_i$ such that the number of elements $\#p^{-1}(z) \ne \deg p'$ or z is a singular point of W'_i. By Lemma 10 the dimension $\dim W'_i = n - i$, and for every irreducible component E' of W'_i the intersection $E' \cap\ p(A) \ne \emptyset$.

Let $s + 1 \le i \le n$. By (3) and the implicit function theorem $\dim W_{i-1} \cap \mathcal{Z}(e'_i) = n - i$. Denote by $W_i^{(3)}$ the union of all the irreducible components E of $W_{i-1} \cap \mathcal{Z}(e'_i)$ such that $E \not\subset \mathcal{Z}(e_0, \ldots, e_r)$ and $\dim \overline{p(E \setminus \mathcal{Z}(e_0, \ldots, e_r))} < n - i - 1$. Hence $W_i^{(3)} \subset W^{(4)}$ (in particular $W_n^{(3)} = \emptyset$).

If an $(n - s + 1)$–tuple of linear forms $L' = (L'_0, L'_{s+1}, \ldots, L'_n)$ is given and (3) holds then we denote also $W_i = W_i(L')$, $\widetilde{W}_i = \widetilde{W}_i(L')$, $W'_i = W'_i(L')$, $W''_i = W''_i(L')$, $W_i^{(3)} = W_i^{(3)}(L')$.

Let $X_0, \ldots, X_r$ and $X_0, X_{s+1}, \ldots, X_n$ be homogeneous coordinate functions on $\mathbb{P}^r(\overline{k})$ and $\mathbb{P}^{n-s}(\overline{k})$ respectively. Let us identify $\mathbb{P}^{r-i}(\overline{k}) = \mathcal{Z}(L'_{s+1}, \ldots, L'_i) \subset \mathbb{P}^r(\overline{k})$ and $\mathbb{P}^{n-i}(\overline{k}) = \mathcal{Z}(X_{s+1}, \ldots, X_i) \subset \mathbb{P}^{n-s}(\overline{k})$. Let E be an irreducible over $\overline{k}$ component of the variety $\widetilde{W}_i$ for some $s \le i \le n$. Set $E' = \overline{p(E \setminus \mathcal{Z}(e_0, \ldots, e_r))} \subset \mathbb{P}^r(\overline{k})$. Recall that ρ' is defined in the proof of Lemma 10. Denote by $p|_E : E \setminus \mathcal{Z}(e_0, \ldots, e_r) \to \mathcal{Z}(L'_{s+1}, \ldots, L'_i)$ and $\rho'|_E : E \setminus \mathcal{Z}(e'_0, e'_{s+1}, \ldots, e'_n) \to \mathcal{Z}(X_{s+1}, \ldots, X_i)$ the restrictions of p and ρ'. Denote by $p'|_E : E \setminus \mathcal{Z}(e_0, \ldots, e_r) \to E'$ the restriction of p' to E and E'.

LEMMA 11 *Let linear forms $L'_{s+1}, \ldots, L'_n \in \overline{k}[X_0, \ldots, X_r]$ satisfy conditions (3), and let $s \le i \le n$ be an integer. Then the following assertions hold.*

1) *For an irreducible component E of $\widetilde{W}_i$ the dimension $\dim E = \dim E' = n - i$ if and only if E is an irreducible component of W_i. Hence*

$$W_{i-1}(L') \cap \mathcal{Z}(e'_i) \setminus \mathcal{Z}(e_0, \ldots, e_r) = W_i(L') \cup W_i^{(3)}(L') \setminus \mathcal{Z}(e_0, \ldots, e_r). \quad (27)$$

2) *The dimension $\dim W'_i = n - i$, $W'_i \cap \mathcal{Z}(L'_{i+1}, \ldots, L'_n) = p(A)$, the morphism $W_i \setminus \mathcal{Z}(e_0, \ldots, e_r) \to W'_i$ is dominant. In particular, for every irreducible component E' of W'_i there is an irreducible component E of W_i such that the morphism $E \setminus \mathcal{Z}(e_0, \ldots, e_r) \to E'$ is dominant. Finally for every irreducible component E of W_i the number of elements*

$$\#\big((E \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e'_{i+1}, \ldots, e'_n)\big) = \deg(p') \deg E', \quad (28)$$

and hence $E' \cap p(A) \ne \emptyset$.

3) *If (3) and (6) hold then for every irreducible component W' of W'_i the number of elements*

$$\#\big(E' \cap \mathcal{Z}(L'_{i+1}, \ldots, L'_n)\big) = \deg E'. \quad (29)$$

4) Let $s+1 \le j \le n-1$ be an integer. Then (8) holds for all $s+1 \le i \le j$ if and only if $\widetilde{W}_i = W_i$ for all $s+1 \le i \le j$, i.e., by (27) if and only if $W_i^{(3)} = \emptyset$ for all $s+1 \le i \le j$.

PROOF Assertion 4) follows from 1)–3) and (27). Assertion 3) follows from (3) and 1), 2) immediately. By Lemma 10 the dimension $\dim W_i' = n-i$, and every irreducible component of W_i' contains a point from $p(A)$. The morphism $(\rho')^{-1}(U) \to (\rho_2')^{-1}(U)$ from the proof of Lemma 10 is finite and $A \subset (\rho_2')^{-1}(U)$. This implies 2).

Suppose that 1) is not true. Then there is an irreducible over $\overline{k}$ component E of $\widetilde{W}_i$ such that $E \cap A = \emptyset$. Replacing L_0' by a new linear form we shall assume without loss of generality that $A \cap \mathcal{Z}(e_0') = \emptyset$. Then the morphism ρ_2' from the proof of Lemma 10 is finite dominant by the last assertion of Lemma 10. Therefore the morphism $E \to \mathbb{P}^{n-i}(\overline{k})$ induced by ρ_2' is also finite dominant. We claim that $E \subset W^{(4)}$. Indeed, otherwise, the restriction $\rho'|_E$ is a dominant morphism and hence there is a point $z^* \in \mathbb{P}^{n-i}(\overline{k})$ infinitely close to $z' = (1 : 0 : \ldots : 0)$ and such that $(\rho')^{-1}(z^*) \cap E \ne \emptyset$. Every point from $(\rho')^{-1}(z')$ is not infinitely close to any point from E. By the implicit function theorem and 2) there are $\deg(p') \deg E'$ pairwise distinct isolated points from $(\rho')^{-1}(z^*)$ that are infinitely close to the corresponding points from $(\rho')^{-1}(z')$. Hence the number of the connected components of the inverse image $\#(\rho')^{-1}(z^*)$ is more than $\deg(p') \deg E'$. This contradicts to Lemma 2 and proves the required assertion. The lemma is proved.

Now under conditions of (f) for every $s \le i \le n$ by assertions 3) and 4) of Lemma 11 (9) holds, and the dimension $\dim W_i'' \le n-i-1$. For every $s \le i \le n-1$ each irreducible component of $W_i' \cap \mathcal{Z}(L_{i+1}')$ contains a point from $W_i' \cap \mathcal{Z}(L_{i+1}', \ldots, L_n')$. All the points from the last intersection are smooth points of W_i' by (6) and Lemma 2. Hence each irreducible component of $W_i' \cap \mathcal{Z}(L_{i+1}')$ is not an irreducible component of W_i''. In particular, each irreducible component of $W' \cap \mathcal{Z}(L_{s+1}')$ is not an irreducible component of W''.

Further, Lemma 11 implies that each irreducible component of the algebraic variety $W^{(4)} \setminus \mathcal{Z}(e_0, \ldots, e_r)$ is not an irreducible component of $(W \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e_{i+1}')$. Obviously condition (8) for $i = n-1$ implies (12). Finally, if (5) holds then by Lemma 11 each irreducible component of $(W \setminus \mathcal{Z}(e_0, \ldots, e_r)) \cap \mathcal{Z}(e_{s+1}')$ is not an irreducible component $(\overline{V \setminus W}) \setminus \mathcal{Z}(e_0, \ldots, e_r)$. Now the remaining part of assertion (f) follows from the following lemma.

LEMMA 12 *Let linear forms $L_{s+1}', \ldots, L_n' \in \overline{k}[X_0, \ldots, X_r]$ satisfy condition (3) and (8). Then for every $s \le i \le n-1$ the algebraic variety $W_i'' \cap \mathcal{Z}(L_{i+1}') \subset W_{i+1}''$ and hence (10), (11) hold.*

PROOF By the definitions of W_{i+1}'' and W_i'' it is sufficient to prove that any singular point of W_i' is a singular point of $W_i' \cap \mathcal{Z}(L_{i+1}')$. Suppose contrary, that $x' \in W_i'$ is singular but $x' \in W_i' \cap \mathcal{Z}(L_{i+1}')$ is smooth. Hence there is only one irreducible over $\overline{k}$ component E of $W_i' \cap \mathcal{Z}(L_{i+1}')$ such that $x' \in E$. Then there are linearly independent linear forms $L_j'' \in \overline{k}[X_0, \ldots, X_r]$, $i+2 \le j \le n$, such that the intersection $E \cap \mathcal{Z}(L_{i+2}'', \ldots, L_n'')$ is transversal at the point x'. Set $L_{i+1}'' = L_{i+1}'$. Denote by $i(W_i', \mathcal{Z}(L_{i+1}'); E)$ (respectively $i(W_i', \mathcal{Z}(L_{i+1}'', \ldots, L_n''); x')$, $i(E, \mathcal{Z}(L_{i+2}'', \ldots, L_n''); x')$) the index of intersection of W_i' and $\mathcal{Z}(L_{i+1}')$ at E (respectively W_i' and $\mathcal{Z}(L_{i+1}'', \ldots, L_n'')$ at x',

E and $\mathcal{Z}(L''_{i+2},\dots,L''_n)$ at x'), see [9]. Then $i(E,\mathcal{Z}(L''_{i+2},\dots,L''_n);x')=1$ since the corresponding intersection is transversal. The intersection $W'_i\cap\mathcal{Z}(L'_{i+1})$ is transversal at E since the intersection $W'_i\cap\mathcal{Z}(L'_{i+1})\cap\mathcal{Z}(L'_{i+2},\dots,L'_n)$ is transversal by (6) and Lemma 2. Therefore, $i(W'_i,\mathcal{Z}(L'_{i+1});E)=1$. The index $i(W'_i,\mathcal{Z}(L''_{i+1},\dots,L''_n);\,x')>1$ since x' is a singular point of W'_i. On the other hand, by the property of indices of intersection corresponding to the associativity of intersection, see [9],

$$i(W'_i,\mathcal{Z}(L''_{i+1},\dots,L''_n);x')=i(W'_i,\mathcal{Z}(L'_{i+1});E)i(E,\mathcal{Z}(L''_{i+2},\dots,L''_n);x').$$

This contradiction proves the lemma.

Let us prove (e).

LEMMA 13 *Let us extend the ground field k till k', where k' is a finitely generated field over k. Let $L'=(L'_0,L'_{s+1},\dots,L'_n)$, where all $L'_j\in\overline{k'}[X_0,\dots,X_r]$ are linear forms. Suppose that L' satisfies conditions (3), (4), (5) and (6) (with k' in place of k). Let $\mathfrak{l}\subset\mathbb{A}^{(r+1)(n-s+1)}(\overline{k'})$ be a line such that $L'\in\mathfrak{l}$. Then for all $L''\in\mathfrak{l}$, except at most a polynomial in $d^n(d')^{n-s}$ number, conditions (3), (4), (5) and (6) hold for L'' (with L'' and k' in place of L' and k), and the inequality $\deg W_i(L'')\geq\deg W_i(L')$ is satisfied for every $s\leq i\leq n-1$.*

PROOF Recall that $e'_j=L'_j(e_0,\dots,e_r)$ for all $j\in\{0,s+1,\dots,n\}$. There are homogeneous polynomials $h_1,\dots,h_s$ of degrees bounded from above by a polynomial in d^s such that W is an irreducible component of the algebraic variety $\mathcal{Z}(h_1,\dots,h_s)$; all the points from $(W\setminus\mathcal{Z}(e_0,\dots,e_r))\cap\mathcal{Z}(e'_{s+1},\dots,e'_n)$ are smooth points of $\mathcal{Z}(h_1,\dots,h_s)$; the intersection of n hypersurfaces $\mathcal{Z}(h_1),\dots,\mathcal{Z}(h_s)$, $\mathcal{Z}(e'_{s+1}),\dots,\mathcal{Z}(e'_n)$ is transversal at every point from $(W\setminus\mathcal{Z}(e_0,\dots,e_r))\cap\mathcal{Z}(e'_{s+1},\dots,e'_n)$.

Further, there exists a linear subspace $\mathcal{L}_i\subset\mathbb{P}^n(\overline{k'})$ with $\dim\mathcal{L}_i=i$ such that the intersection $\widetilde{W}_i(L')\cap\mathcal{L}_i$ is transversal, hence the intersection $W_i(L')\cap\mathcal{L}_i=\mathcal{A}_i$ is transversal and finite, and all the elements of $\mathcal{A}_i$ are isolated points of $\widetilde{W}_i(L')\cap\mathcal{L}_i$; the element $\mathcal{A}_i\cap\mathcal{Z}(e'_0)=\emptyset$, and hence all the elements of $\mathcal{A}_i$ are isolated points of $W\cap\mathcal{Z}(e'_{s+1},\dots,e'_i)\cap\mathcal{L}_i$; for every point $z\in\mathcal{A}_i$ the intersection of n hypersurfaces $\mathcal{Z}(h_1),\dots,\mathcal{Z}(h_s)$, $\mathcal{Z}(e'_{s+1}),\dots,\mathcal{Z}(e'_i)$, $\mathcal{Z}(e'_{i+1}-(e'_{i+1}/e'_0)(z)e'_0),\dots,\mathcal{Z}(e'_n-(e'_n/e'_0)(z)e'_0)$ is transversal at z. All these are conditions of general position which can be easily satisfied.

Let a generic point $\widetilde{L}=(\widetilde{L}_0,\widetilde{L}_{s+1},\dots,\widetilde{L}_n)$ of $\mathfrak{l}$ has the form $\widetilde{L}_j=L'_j+\varepsilon L'''_j$ where ε is a transcendental element over k' and $L'''_j\in\overline{k'}[X_0,\dots,X_r]$ are linear forms for all $j\in\{0,s+1,\dots,n\}$. Set $\widetilde{e}_j=\widetilde{L}_j(e_0,\dots,e_r)$, $e'''_j=L'''_j(e_0,\dots,e_r)$, $e''_j=L''_j(e_0,\dots,e_r)$ for all j. Let ε be the coordinate function of $\mathbb{A}^1$, and ε be the coordinate of $\widetilde{L}$. We shall assume that the coordinate of L'' is $\varepsilon''\in\overline{k'}$. Consider the algebraic variety $\widetilde{W}_{\varepsilon,i}=(W\times\mathbb{A}^1(\overline{k'}))\cap\mathcal{Z}(\widetilde{e}_{s+1},\dots,\widetilde{e}_i)\subset\mathbb{P}^n(\overline{k'})\times\mathbb{A}^1(\overline{k'})$. Notice that every point from $\mathcal{A}_i\times\{0\}$ is an isolated point of $\widetilde{W}_{\varepsilon,i}\cap(\mathcal{L}_i\times\{0\})=(W\cap\mathcal{Z}(e'_{s+1},\dots,e'_i)\cap\mathcal{L}_i)\times\{0\}$. Denote by $W_{\varepsilon,i}$ the union of all the irreducible components E of $\widetilde{W}_{\varepsilon,i}$ such that $E\cap(\mathcal{L}_i\times\{0\})\cap(\mathcal{A}_i\times\{0\})\neq\emptyset$, and hence $\dim E=n-i+1$. Obviously every irreducible component of $W_i(L')\times\{0\}$ is an irreducible component of $W_{\varepsilon,i}\cap(\mathbb{P}^n(\overline{k'})\times\{0\})$.

Set $C_{\varepsilon,i}$ to be the union of all the irreducible components E_1 of $\widetilde{W}_{\varepsilon,i}\cap(\mathcal{L}_i\times\mathbb{A}^1(\overline{k'}))$ such that $E_1\cap(\mathcal{A}_i\times\{0\})\neq\emptyset$. Hence every irreducible component E_2 of

$C_{\varepsilon,i}$ is a curve, and E_2 is an irreducible component of $W_{\varepsilon,i} \cap (\mathcal{L}_i \times \mathbb{A}^1(\overline{k'}))$. Finally, note that for every irreducible component E of $W_{\varepsilon,i}$ there is an irreducible component E_2 of $C_{\varepsilon,i}$ such that $E_2 \subset E_1$.

Let $\varepsilon'' \in \overline{k'}$. Denote $W_{\varepsilon,i} \cap \mathcal{Z}(\varepsilon - \varepsilon'') = W_{\varepsilon'',i} \times \{\varepsilon''\}$ where $W_{\varepsilon'',i} \subset \mathbb{P}^n(\overline{k'})$, and $\dim W_{\varepsilon'',i} = n - i$. Hence $(W_{\varepsilon'',i} \cap \mathcal{L}_i) \times \{\varepsilon''\} \supset \mathcal{Z}(\varepsilon - \varepsilon'') \cap C_{\varepsilon,i}$. By the Bézout theorem and Theorem 1 (d) (with the field k' in place of k) for all $\varepsilon'' \in \overline{k'}$, except at most a polynomial in $d^n(d')^{n-s}$ number, the following assertions hold for all $s \le i \le n-1$: conditions (3), (4) (5) and (6) hold for L'' (with L'' and k' in place of L' and k); the intersection $W_{\varepsilon'',i}$ is a union of some irreducible components of dimension $n-i$ of $(W \cap \mathcal{Z}(e''_{s+1}, \ldots, e''_i)) \times \{\varepsilon''\}$; for every $z \in W_{\varepsilon'',i} \cap \mathcal{L}_i$ if $(z, \varepsilon'') \in C_{\varepsilon,i}$ then z is an isolated point of $W_{\varepsilon'',i} \cap \mathcal{L}_i$; the number of elements $+\infty > \#(\mathcal{Z}(\varepsilon - \varepsilon'') \cap C_{\varepsilon,i}) \ge \#(\mathcal{Z}(\varepsilon) \cap C_{\varepsilon,i}) = \#\mathcal{A}_i$; the intersection of n hypersurfaces $\mathcal{Z}(h_1), \ldots, \mathcal{Z}(h_s)$, $\mathcal{Z}(e''_{s+1}), \ldots, \mathcal{Z}(e''_i)$, $\mathcal{Z}(e''_{i+1} - (e''_{i+1}/e''_0)(z)e''_0), \ldots, \mathcal{Z}(e''_n - (e''_n/e''_0)(z)e''_0)$ is transversal at every point $z \in W_{\varepsilon'',i} \cap \mathcal{L}_i$ such that $(z, \varepsilon'') \in C_{\varepsilon,i}$. The last condition related to the intersection of hypersurfaces means that the restriction of the morphism ρ' to $W_{\varepsilon'',i}$ is dominant. Therefore, for the considered ε'' the algebraic variety $W_{\varepsilon'',i}$ is a union of some irreducible components of $W_i(L'')$ and $\deg W_{\varepsilon'',i} \ge \deg W_i(L')$. The lemma is proved.

Now suppose that $L' \in \mathcal{U}'_0$, see assertion (d), is constructed by (c). So all the linear forms L'_j have integer coefficients of length $O(n \log d + (n-s)\log(d'))$. We shall describe an algorithm recursive by L'. At the end of the recursion L' will satisfy assertion (e).

Let us describe the general step of the recursion. At the beginning of the step the current L' is given. The recursive assumption is that an integer $s \le i \le n-2$ is known such that $\widetilde{W}_j(L') = W_j(L')$ for all $s \le j \le i$ (at the first step $i = s$). Let us apply Theorem 1 [8] to the algebraic variety $\widetilde{V}_i = (V \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_i)) \cup \mathcal{Z}(e'_{i+1})$ and construct linear forms $L_0, \ldots, L_{n+1}$ from this theorem. For every $s \le j \le n-1$ applying Theorem 5 [6] (which allow to decide whether a morphism is dominant) and Theorem 2 [8] to $V \cap \mathcal{Z}(e'_{s+1}, \ldots, e'_j)$ we compute all the degrees $\deg W_j(L')$. In what follows we shall compute in the similar way the degrees $\deg W_j(L'')$, $s \le j \le n-1$, for L'' analogous to L'.

The morphism $W_i(L') \setminus \mathcal{Z}(e'_0, e'_{i+1}, \ldots, e'_n) \to \mathcal{Z}(L'_{s+1}, \ldots, L'_i)$, $(X_0 : \ldots : X_n) \mapsto (e'_0 : e'_{i+1} : \ldots : e'_n)$, is dominant. Therefore, the dimension $\dim W_i(L') \cap \mathcal{Z}(e'_{i+1}) = n-i-1$. Hence e'_{i+1} does not vanish on any irreducible component of $W_i(L')$. Hence $W \cap \mathcal{Z}(L_{i+1}, \ldots, L_n) \cap \mathcal{Z}(e'_{i+1}) = \emptyset$ according to the construction of $L_0, \ldots, L_{n+1}$.

Denote $L''_j = L_j$ for $i+2 \le j \le n$. We shall describe a recursive algorithm by $(L''_{i+2}, \ldots, L''_n)$ (the element for the base of this second embedded recursion is defined). The recursive assumption is that $L''_j = L_j - \mu_j L_{i+1}$ for some integers μ_j for all $i+2 \le j \le n$. At the end of this recursion we shall obtain an element $(L''_{i+2}, \ldots, L''_n)$ such that $(W_{i+1}(L') \cup W^{(3)}_{i+1}(L')) \cap \mathcal{Z}(L''_{i+2}, \ldots, L''_n) \cap \mathcal{Z}(e_0, \ldots, e_r) = \emptyset$.

Let us describe the general step of this embedded recursion. Let us construct using the algorithm from [2] all the irreducible components of dimension 1 of the intersection $\widetilde{V}_i \cap \mathcal{Z}(L''_{i+2}, \ldots, L''_n)$ and using Theorem 2 [8] choose among them all the irreducible curves C_γ, $\gamma \in \Gamma$ such that $C_\gamma \subset W_i(L')$. By Theorem 1 [8] each curve C_γ contains a point $y \in W_i(L') \cap \mathcal{Z}(L_{i+1}, \ldots, L_n)$, and every y is a smooth point of $\widetilde{V}_i$. Denote $C_i = \bigcup_{\gamma \in \Gamma} C_\gamma$. Now $C_i = W_i(L') \cap \mathcal{Z}(L''_{i+2}, \ldots, L''_n)$.

Let us construct by [2] the finite set $S_{i+1} = S(L''_{i+2}, \ldots, L''_n) = C_i \cap \mathcal{Z}(e'_{i+1})$. Every irreducible component of $W_i(L') \cap \mathcal{Z}(e'_{i+1})$ contains a point from S_{i+1}, and the number of elements $\#S_{i+1}$ is bounded from above by a polynomial in $d^n(d')^{n-s}$ by the Bézout theorem. Set $S'_{i+1} = S'(L''_{i+2}, \ldots, L''_n) = S_{i+1} \setminus \mathcal{Z}(e_0, \ldots, e_r)$ (we shall use also the similar notation for linear forms with coefficients from other fields). Notice that $S(L''_{i+2}, \ldots, L''_n) \cap \mathcal{Z}(L_{i+1}) = \emptyset$ for arbitrary μ_j.

Let us enumerate the points $z \in S_{i+1} \setminus S'_{i+1}$. Consider the following system of polynomial equations and inequalities with coefficients from $\overline{k_2}$.

$$\begin{cases} \sum_{0\le i\le r} |e_i|^2 = \varepsilon_2, \\ \sum_{0\le i\le n} |X_i - (X_i/L_{i+1})(z)|^2 \le \varepsilon_1, \\ e'_j = 0, & s+1 \le j \le i+1, \\ L_{i+1} = 1. \end{cases} \tag{30}$$

Let us apply Theorem 2 to this system and the variety $\mathrm{con}(V)$ and construct the set $S'' \subset \mathbb{A}^{n+1}(\overline{k_2})$ from the statement of this theorem. Denote by $S''' \subset \mathbb{P}^n(\overline{k_2})$ the set corresponding to S'' by the natural projection $\mathbb{A}^{n+1}\setminus\{0\} \to \mathbb{P}^n$. Further, using Theorem 2 [8] we decide whether there is a point $x^* \in S''' \cap W(\overline{k_2})$. Obviously such a point exists if and only if $z \in W_{i+1}(L') \cap W^{(3)}_{i+1}(L')$. Suppose that such a point exists. Then set $\mu^*_j = (L''_j/L_{i+1})(x^*)$ and $L^*_j = L''_j - \mu^*_j L_{i+1}$ for all $i+2 \le j \le n$.

Hence $x^* \in S'(L^*_{i+2}, \ldots, L^*_n)$ and for every $z_1 \in S'(L''_{i+2}, \ldots, L''_n)$ there is $z^*_1 \in S'(L^*_{i+2}, \ldots, L^*_n)$ which is infinitely close to z_1 by, e.g., Proposition 6 [5]. Hence the number of elements $\#S'(L^*_{i+2}, \ldots, L^*_n) > \#S'(L''_{i+2}, \ldots, L''_n)$. Using the algorithm of reduction to integer coefficients, see Proposition 2, one can replace subsequently elements μ^*_j by integers $\mu^{(1)}_j$ (we find them by the enumeration) of length $O(n\log d + (n-s)\log(d'))$ and obtain linear forms $L^{(1)}_j = L''_j - \mu^{(1)}_j L_{i+1}$, $i+2 \le j \le n$, such that $\#S'(L^{(1)}_{i+2}, \ldots, L^{(1)}_n) \ge \#S'(L^*_{i+2}, \ldots, L^*_n)$. This follows from the Bézout theorem, cf. the proof of Lemma 13. We leave the details to the reader here. Now we replace $(L''_{i+2}, \ldots, L''_n)$ by $(L^{(1)}_{i+2}, \ldots, L^{(1)}_n)$ and proceed to the next step of the recursion.

If $x^* \in S''' \cap W(\overline{k_2})$ does not exists and not all the points from $S_{i+1} \setminus S'_{i+1}$ are enumerated then we proceed to the next point $z \in S_{i+1} \setminus S'_{i+1}$. If all the points from $S_{i+1} \setminus S'_{i+1}$ are enumerated then we have obtained the required element $(L''_{i+2}, \ldots, L''_n)$. The second recursion is described.

Let us construct a linear form $L'''_{i+1} \in k[X_0, \ldots, X_r]$ with integer coefficients of length $O(n\log d + (n-s)\log(d'))$ such that $S'_{i+1}(L''_{i+2}, \ldots, L''_n) \cap \mathcal{Z}(L'''_{i+1}(e_0, \ldots, e_r)) = \emptyset$. Let ε_1 be a be an infinitesimal with respect to the field k. Set $k_1 = k(\varepsilon_1)$ and $\widetilde{L}_{i+1} = L'_{i+1} + \varepsilon_1 L'''_{i+1}$. Put $\widetilde{L}_\alpha = L'_\alpha$ for all $\alpha \in \{0, s+1, \ldots, n\} \setminus \{i+1\}$, and $\widetilde{L} = (\widetilde{L}_0, \widetilde{L}_{s+1}, \ldots, \widetilde{L}_n)$. Since $\mathcal{U}'_0$ is an open in the Zariski topology subset, the element $\widetilde{L}$ satisfies (3), (4), (5) and (6) with k_1 in place of k. We have $W^{(3)}_{i+1}(\widetilde{L}) \subset W_i(L') \cap W^{(4)}$. Hence $W^{(3)}_{i+1}(\widetilde{L})$ is a union of some irreducible components of dimension $n-i-1$ of the variety $W_i(L') \cap W^{(4)}$. In particular, $W^{(3)}_{i+1}(\widetilde{L})$ is defined over $\overline{k}$. Therefore, $W^{(3)}_{i+1}(L') \supset W^{(3)}_{i+1}(\widetilde{L})$. Since $\widetilde{e}_{i+1} = \widetilde{L}_{i+1}(e_0, \ldots, e_r)$ does not vanish on any irreducible component E of $W^{(3)}_{i+1}(L')$ the algebraic variety $W^{(3)}_{i+1}(\widetilde{L}) = \emptyset$. Hence

$W_{i+1}(\widetilde{L}) \setminus \mathcal{Z}(e_0,\dots,e_r) = W_i(L') \cap \mathcal{Z}(\widetilde{e}_{i+1}) \setminus \mathcal{Z}(e_0,\dots,e_r)$ over the field $\overline{k_1}$. Now in Lemma 13 put $k' = k$ and $\mathfrak{l}$ to be the line containing L' and L'''. There are infinitely many isomorphic generic points of this line. Hence extending k till k_1 and applying Lemma 13 we obtain that *the degrees* $\deg W_j(\widetilde{L}) \geq \deg W_j(L')$ *for all* $s \leq j \leq n-1$.

LEMMA 14 *Suppose* $\widetilde{W}_j(L') = W_j(L')$ *for all* $s \leq j \leq i$ *and there exists an irreducible component* E *of* $W^{(3)}_{i+1}(L')$. *Then the degree* $\deg W_{i+1}(\widetilde{L}) > \deg W_{i+1}(L')$.

PROOF In the proof of this lemma we shall assume without loss of generality that the linear forms $L_{i+2},\dots,L_n$ satisfy additionally the conditions: $\#(W_i(L') \cap \mathcal{Z}(e'_{i+1}) \cap \mathcal{Z}(L_{i+2},\dots,L_n)) = \deg(W_i \cap \mathcal{Z}(e'_{i+1}))$; for every irreducible component E_1 of $W_i(L') \cap \mathcal{Z}(e'_{i+1})$ such that $E_1 \not\subset \mathcal{Z}(e_0,\dots,e_r)$ the intersection $E_1 \cap \mathcal{Z}(L_{i+2},\dots,L_n) \cap \mathcal{Z}(e_0,\dots,e_r) = \emptyset$ (such linear forms $L_{i+2},\dots,L_n$ exist in general position, and we do not need to construct them at present).

Let $z^{(0)} \in E \cap \mathcal{Z}(L_{i+2},\dots,L_n)$. Then $z^{(0)} \notin W_{i+1}(L') \cap \mathcal{Z}(L_{i+2},\dots,L_n)$ and $z^{(0)} \notin \mathcal{Z}(e_0,\dots,e_r)$.

Since ε is an infinitesimal, for every point $z \in W_i(L') \cap \mathcal{Z}(e'_{i+1}) \cap \mathcal{Z}(L_{i+2},\dots,L_n)$ there is a point $z^* \in W_i(L') \cap \mathcal{Z}(\widetilde{e}_{i+1}) \cap \mathcal{Z}(L_{i+2},\dots,L_n)$ such that z^* is infinitely close to z (here we leave the details to the reader). In particular, there is a point of $W_i(L') \cap \mathcal{Z}(\widetilde{e}_{i+1}) \cap \mathcal{Z}(L_{i+2},\dots,L_n)$ which is infinitely close to $z^{(0)}$. This implies the assertion of the lemma. The lemma is proved.

Let us return to the description of the algorithm. Let us compute all $\deg W_j(\widetilde{L})$, $s \leq j \leq n-1$ (similarly to the computation of $\deg W_j(L')$ above; here one should extend the field k till k_1). Suppose that $\deg W_{j_1}(\widetilde{L}) > \deg W_{j_1}(L')$ for some $s+1 \leq j_1 \leq n-1$. Then by Lemma 13 one can apply the algorithm of reduction to integer coefficients, see Proposition 2. We replace subsequently all the coefficients of the linear forms $\widetilde{L}_j$ by integers of length $O(n\log d + (n-s)\log(d'))$ and obtain new linear forms L''_j, $j \in \{0, s+1,\dots,n\}$ such that $L'' = (L''_0, L''_{s+1},\dots,L''_n) \in \mathcal{U}'_0$, the degrees $\deg W_j(L'') \geq \deg W_j(\widetilde{L})$ for all $s \leq j \leq n-1$, and hence $\deg W_{j_1}(L'') > \deg W_{j_1}(L')$. In this case we replace L' by L'' and proceed to the next step of the recursion with the same i. By the Bézout theorem there might be at most $d^s(d')^{n-j_1}$ steps when $\deg W_{j_1}(\widetilde{L}) > \deg W_{j_1}(L')$.

Now suppose $\deg W_j(\widetilde{L}) = \deg W_j(L')$ for all $s+1 \leq j \leq n-1$. Then by Lemma 14 and Lemma 11 we have $W_{i+1}(L') \setminus \mathcal{Z}(e_0,\dots,e_r) = W_i(L') \cap \mathcal{Z}(e'_{i+1}) \setminus \mathcal{Z}(e_0,\dots,e_r)$. Hence $W_{i+1}(L') = \widetilde{W}_{i+1}(L')$. In this case if $i+1 \leq n-2$ we replace i by $i+1$ and proceed to the next step of the recursion with the same L'.

Finally we shall come to the case when $\deg W_{i+1}(\widetilde{L}) = \deg W_{i+1}(L')$ and $i = n-2$. Then condition (8) holds for all $s+1 \leq i \leq n-1$ by Lemma 14 and Lemma 11. This step is final. The required estimation for the working time of the described algorithm for assertion (e) follows immediately from the ones of the applied algorithms. Theorem 1 is proved completely.

REMARK 6 *Let* k' *be an arbitrary finitely generated extension of* k *(and* k' *is given similarly to* k, *see the Introduction). Let us extend the ground field* k *till* k'. *Suppose that* $L' \in \mathcal{U}'_0$ *is given, and all linear forms* $L'_j \in k'[X_0,\dots,X_r]$, $j \in \{0, s+1,\dots,n\}$. *Actually the algorithm for assertion (e) allows to decide*

whether (8) holds for all $s+1 \le i \le n-1$ *(with* k' *in place of* k*). Further, if (8) is not fulfilled then one can construct an element* $L'' \in \mathcal{U}_0'$ *such that all linear forms* L_j'' *have integer coefficients of length* $O(n \log d + (n-s) \log d')$*, condition (8) holds for* L'' *(in place of* L'*), the inequalities* $\deg W_j(L'') \ge \deg W_j(L')$ *hold for all* $s \le j \le n-1$*, and at least one of the last inequalities is strict. The working time of this modification of the algorithm from (e) is polynomial in* d^n*,* $(d')^n$*,* d_1*,* d_2*,* d_2'*,* M*,* M'*,* M_1*,* m*,* r*,* N*,* $\mathrm{L}(x^{(0)})$*, the size* $\mathrm{L}(L')$*, and the size of minimal polynomial of the primitive element of* k' *over a purely transcendental extension of* k*.*

References

[1] **Bochnak J., Coste M., Roy M.–F.:** *"Géométrie algébrique réelle"*, Springer–Verlag, Berlin, Heidelberg, New York, 1987.

[2] **Chistov A. L.:** *"Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time"*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 137 (1984), p. 124–188 (in Russian) [English transl.: J. Sov. Math. 34, No.4, (1986) p. 1838–1882].

[3] **Chistov A. L.:** *"Polynomial complexity of the Newton–Puiseux algorithm"*, in Lecture Notes in Computer Science, Vol. 233, Springer, 1986, p. 247–255.

[4] **Chistov A. L.:** *" Polynomial–Time Computation of the Dimension of Algebraic Varieties in Zero–Characteristic"*, Journal of Symbolic Computation, 22 # 1 (1996) 1–25.

[5] **Chistov A. L.:** *"Polynomial–time computation of the dimensions of components of algebraic varieties in zero–characteristic"*, Journal of Pure and Applied Algebra, 117 & 118 (1997) 145–175.

[6] **Chistov A. L.:** *"Polynomial–time computation of the degrees of algebraic varieties in zero–characteristic and its applications"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 258 (1999), p. 7–59 (in Russian)[1]

[7] **Chistov A. L.:** *"Strong version of the basic deciding algorithm for the existential theory of real fields"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 256 (1999) p. 168–211 (in Russian). [English transl.: J. of Mathematical Sciences v.107 No.5 p.4265–4295]

[8] **Chistov A. L.:** *"Monodromy and irreducibility criteria with algorithmic applications in zero–characteristic"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 292 (2002) p. 130–152 (in Russian) [in English, see Preprint of St.Petersburg Mathematical Society (2004)].

[9] **Hartshorne R.:** *"Algebraic geometry"*, Springer–Verlag, New York, Heidelberg, Berlin, 1977.

[10] **Hodge W. V. D., Pedoe D.:** *"Methods of algebraic geometry"*, v. 1, Cambridge, 1947.

[11] **Mumford D.:** *"Algebraic geometry I. Complex projective varieties"*, Springer–Verlag, Berlin, Heidelberg, New York, 1976.

[1] Preliminary versions of [6], [7], in English can be found as Preprints (1999) , http://www.MathSoc.spb.ru