Monodromy and irreducibility criteria with algorithmic applications in zero–characteristic

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 V which is the set of all common zeroes of homogeneous polynomials of degrees less than d in $n+1$ variables in zero–characteristic. We suggest an algorithm to decide whether two (or more) given points of V belong to the same irreducible component of V. Besides that we show how to construct for each $s < n$ an $(s+1)$–dimensional plane in the projective space such that the intersection of every irreducible component of dimension $n-s$ of V with the constructed plane is transversal and is an irreducible curve. These algorithms are deterministic and polynomial in d^n and the size of input.

Introduction

Let k be a field of zero–characteristic with algebraic closure $\overline{k}$. Denote by $\mathbb{P}^n(\overline{k})$, $n \geq 0$, 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 $g_1, \ldots, g_m \in \overline{k}[X_0, \ldots, X_n]$ we shall 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).

In the algorithmic part of the paper we shall suppose that the field k is finitely generated over the field of rational numbers $\mathbb{Q}$. Let V be a projective algebraic variety which is a set of all common zeroes of homogeneous polynomials in $n+1$ variables of degrees less than d with coefficients from k. Now let $z_1, \ldots, z_u \in V$ be arbitrary points. We construct an algorithm to decide whether $z_1, \ldots, z_u$ belong to the same defined and irreducible over k (respectively $\overline{k}$) component of V with the working time polynomial in d^n and the size of input (respectively the same working time for fixed u), see Theorem 2. Besides that we construct linear forms $L_1, \ldots, L_{n-1}$ in $X_0, \ldots, X_n$ with integer coefficients of length $O(n \log d)$ such that for every $0 \leq s \leq n$ for every irreducible over $\overline{k}$ component W of V with $\dim W = n - s$ the intersection $W \cap \mathcal{Z}(L_{s+1}, \ldots, L_{n-1})$ is transversal and is an irreducible over $\overline{k}$ projective curve, see Theorem 1.

Note here that even the existence of the required linear forms $L_1, \ldots, L_{n-1}$ with length of integer coefficients $O(n \log d)$ is not trivial. In the algorithms of this paper we use essentially the results of [4]. We apply also the first Bertini theorem, see [1]. On the other hand, we need to attract the transcendental methods of theory of analytical functions similarly to [5], namely, the group of monodromy of an algebraic function to substantiate the algorithm (in [5] we used these methods not only for the proof of correctness but in the algorithm itself), see Theorem 3, Section 1. As an immediate consequence of Corollary 2 from this theorem we obtain the following nice result (the main case here is $n \geq 3$).

CRITERION FOR IRREDUCIBILITY *Let $\Phi \in k[X_0, \ldots, X_n]$, $n \geq 1$, be a separable homogeneous polynomial over a field of zero–characteristic. Let $\deg \Phi = \deg_{X_0} \Phi \geq 1$. Let R be the discriminant of Φ with respect to X_0 and R_0 be square free part of R (i.e., R_0 is a separable polynomial of the most degree dividing R). Let L be a nonzero linear form in $X_1, \ldots, X_n$ with coefficients from k, and $A = k[X_0, \ldots, X_n]/(L)$ (hence A is isomorphic to the ring of polynomial in n variables). Suppose that the polynomial $R_0 \bmod L \in A$ is separable. Then the irreducible over k factors of the polynomials Φ and $\Phi \bmod L \in A$ are in the one–to–one correspondence by the rule $\Psi \mapsto \Psi \bmod L$. In particular, if Φ is irreducible over k then $\Phi \bmod L$ is irreducible over k. Besides that for every linear subspace $\mathcal{L}$ of linear forms in $X_1, \ldots, X_n$ with $\dim \mathcal{L} \geq 3$ there is $L \in \mathcal{L}$ satisfying the formulated conditions.*

This criterion and Corollary 2 clarify the first Bertini theorem in the important cases. In one of the next the next papers we shall return to the first Bertini theorem in the general case from algorithmic point of view. The results of the present paper, namely Theorem 1, will be used there essentially. We shall need to prove in the next paper a more general version of Theorem 3 again. Although this version can be given already in this paper we decided to make the presentation more clear and omit the details related to the case of not finite morphisms.

We leave to the reader to deduce consequences of the given criterion for nonhomogeneous polynomials. It is interesting to prove analogs of this criterion for nonzero characteristic for arbitrary n and for nonhomogeneous polynomials with integer coefficients with small n.

In [6] we suggested a new method for representation of algebraic varieties which is based on the representative systems of points. The present paper is an important step to construct the algorithms for this method in zero–characteristic.

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

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

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 $V = \mathcal{Z}(f_1, \ldots, f_m)$.

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 $f = f_i$ in the form

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

where $a_0, a_{i_0,\ldots,i_n,j} \in \mathbb{Z}[t_1, \ldots, t_l]$, $\mathrm{GCD}_{\,i_0,\ldots,i_n,j}(a_0, a_{i_0,\ldots,i_n,j}) = 1$. Define the length $l(a)$ of an integer a by the formula $l(a) = \min\{s \in \mathbb{Z} : \ |a| < 2^{s-1}\}$. The length of coefficients $l(f)$ 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 $1 \leq \gamma \leq l$. In the similar way we shall define degrees and lengths of integer coefficients of other polynomials, in particular $\deg_{t_\gamma} F$ and $l(F)$ are defined. We shall suppose that we have the following bounds

$$\begin{gathered} \deg_{X_0,\ldots,X_n}(f_i) < d, \ \deg_{t_\gamma}(f_i) < d_2, \ l(f_i) < M, \\ \deg_Z(F) < d_1, \ \deg_{t_\gamma}(F) < d_1, \ l(F) < M_1 \, . \end{gathered}$$

for all $1 \leq i \leq m$. The size $L(f)$ of the polynomial f is defined to be the product of $l(f)$ to the number of all the coefficients from $\mathbb{Z}$ of f in the dense representation. We have

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

Similarly $L(F) < d_1^{l+1} M_1$. Unless we state otherwise, in what follows we suppose l to be fixed.

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 $X_{i_0}(z) \ne 0$ and an isomorphism of fields

$$k(z) = k((X_1/X_{i_0})(z), \dots, (X_n/X_{i_0})(z)) \simeq k[\eta] = k[Z]/(F_z) \qquad (1)$$

is given where $\sum_{0\le i\le n} c_i(X_i/X_{i_0})(z) \mapsto \eta$ under (1), the coefficients $c_i \in \mathbb{Z}$ are given and $F_z \in k[Z]$ is minimal polynomial of η over k with leading coefficient $\mathrm{lc}_Z F_z = 1$. So the point z is defined up to a conjugation over k and, more precisely, representation (1) gives defined over k and irreducible over k algebraic variety of dimension 0.

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

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

Let us define the size $L(z)$ of the point z to be $L(F_z)+\sum_{0\le i\le n} L(X_i/X_{i_0})$. Using the algorithm from [3] one can construct a system of homogeneous polynomial equations with coefficients from k giving the least defined over k and irreducible over k algebraic variety of dimension 0 containing z within the time polynomial in $L(z)$.

Let $W_1, W_2 \subset \mathbb{P}^n(\overline{k})$ (respectively $W_1, W_2 \subset \mathbb{A}^n(\overline{k})$) be two projective (respectively affine) algebraic varieties. Suppose that all the irreducible components of W_i have the same dimension $n - s_i$, $i = 1, 2$. Let W_3 be an irreducible 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 $\dim W_3 = n - s_1 - s_2$ and 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., $\dim(T_{x,W_1} \cap T_{x,W_2}) = n - s_1 - s_2$. We shall say that the intersection $W_1 \cap W_2$ is transversal if and only if it is transversal at every its component. In the similar way one defines transversality for intersection of a finite number of algebraic varieties.

THEOREM 1 *Let the field k, the algebraic variety V and polynomials F, $f_1, \dots, f_m$ be given as above. Then one can construct linear forms $L_0, L_1, \dots, L_{n+1}$ in $X_0, \dots, X_n$ with integer coefficients of length $O(n \log d)$ and the finite defined over k sets A_s, $V_{s,0}$, $0 \le s \le n$, of points of V satisfying the following properties. For every $0 \le s \le n$ denote by V_s the union of all irreducible components of V of dimension $n - s$.*

- *(a) Then for every $0 \le s \le n$ the set $A_s = V_s \cap \mathcal{Z}(L_{s+1}, \dots, L_n)$ is finite (or empty if $V_s = \emptyset$), consists of smooth points of V and the intersections of tangent spaces of V_s and $\mathcal{Z}(L_{s+1}, \dots, L_n)$ at all these points are transversal. The linear form L_0 does not vanish in any point of A_s, i.e., $0 \notin L_0(A_s)$, and the number of elements $\#L_{n+1}(A_s) = \#A_s = \deg V_s$.*

- *(b) For every $0 \le s \le n-1$ (the case $s = n-1$ is trivial) irreducible over $\overline{k}$ (respectively k) components of the algebraic varieties V_s and $V_s \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$ are in the one–to–one correspondence by the rule $W \mapsto W \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$. The last intersection is an irreducible over $\overline{k}$*

(respectively irreducible over k) curve. Besides that, if W is irreducible over $\overline{k}$ then the minimal fields of definition containing k of W and $W \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$ coincide.

(c) *For every $1 \le s \le n-1$ denote by $\Phi_s \in k[L_0, L_{s+1}, L_{s+2}, \dots, L_{n+1}] = B_s$ (here all L_j are considered as variables) the nonzero separable polynomial of minimal degree such that Φ_s is vanishing on V_s. Denote by R_s the discriminant of Φ_s with respect to of L_{n+1} and by $R_{s,0}$ square free part of R_s (i.e., $R_{s,0}$ is a separable polynomial of the most degree dividing R_s). Then $\deg_{L_{n+1}} \Phi_s = \deg \Phi_s = \deg V_s$ and the polynomial*

$$R_{s,0} \bmod (L_{s+1}, \dots, L_{n-1}) \in B_s/(L_{s+1}, \dots, L_{n-1})$$

is nonzero separable. We choose and fix Φ_s such that the leading coefficient of Φ_s with respect to L_{n+1} is equal to is equal to 1.

(d) *For every $0 \le s \le n$ irreducible over k components of the algebraic varieties V_s and $V_{s,0}$ are in the one–to–one correspondence by the rule $W \mapsto W \cap V_{s,0}$. Besides that, $V_{s,0} \subset A_s$ and $V_{n,0} = A_n = V_n$.*

(e) *For every $0 \le s \le n-1$ for every $z \in V_{s,0}$ representation (1) is constructed. Denote by W_z the uniquely defined irreducible over $\overline{k}$ component of V such that $z \in W_z$, denote by $k_z \supset k$ the minimal field of definition of the component W_z. Then $k(z) \supset k_z$ and the field k_z is constructed by the algorithm. It is given by its basis and multiplication table. Two points from $V_{s,0}$ belong to W_z if and only if they are conjugated to z over k_z. Hence one can easily define a representative system (we do not construct it) $V'_{s,0} \subset V_{s,0}$ of points of irreducible over $\overline{k}$ components of V_s. If $a \subset V_{s,0}$ is an arbitrary defined and irreducible over k component and $z \in a$ then $V'_{s,0} \cap a$ consists of $[k_z : k]$ points.*

The algorithm for constructing linear forms $L_0, L_1, \dots, L_{n+1}$, finite sets A_s, $V_{s,0}$, $0 \le s \le n$ and all fields $k_z \subset k(z)$, $z \in V_{s,0}$, is polynomial in d^n, d_1, d_2, M, M_1 and m. Note that for every point $z \in A_s$ in representation (1) obtained by the algorithm the degree $\deg_Z F_z \le \deg V_n \le d^n$ by the Bézout theorem.

In the next theorem u points $z_1, \dots, z_u \in V$ are given. Namely, we replace in (1) z, η, F_z by z_i, η_i, F_{z_i} and get the representations for z_i, $1 \le i \le u$. Besides that in the assertion (b) of this theorem, we shall suppose that the composite of fields $k[\eta_1, \dots, \eta_u]$ is given explicitly (by its basis and multiplication table over k). One need to fix u points here and hence it is essential to give not only the points $z_1, \dots, z_u$ but also the u–tuple of points $(z_1, \dots, z_u)$ uniquely up to a conjugation over k. Note that one can construct any composite of the fields $k[\eta_i]$, $1 \le i \le u$, over k within the time polynomial in $L(z_1), \dots, L(z_2)$ and $\prod_{1 \le i \le u} \deg F_{z_i}$, see [3]. In addition the size of the basis and the multiplication table of each constructed composite is polynomial in the sum of sizes of basises and multiplication tables of all fields $k[\eta_i]$, $1 \le i \le u$, and the degree of this composite over k. In what follows we shall suppose that this estimate is always holds for the given representation of the composite $k[\eta_1, \dots, \eta_u]$.

THEOREM 2 *Let the field k, the algebraic variety V and polynomials F, $f_1, \dots, f_m$ be given as above. Let $u \ge 2$ points $z_1, \dots, z_u \in V$ be given.*

(a) *Then for every $0 \le s \le n-1$ one can compute the number of irreducible over k components W of V with $\dim W = n-s$ such that $z_i \in W$ for all $1 \le i \le u$. The working time of this algorithm is polynomial in d^n, d_1, d_2, M, M_1, m and the sum of the sizes of $\sum_{1\le i\le u} L(z_i)$, of the points z_i, $1 \le i \le u$.*

(b) *Suppose that the composite of fields $k[\eta_1,\ldots,\eta_u]$ is given. Then for every $0 \le s \le n-1$ one can compute the number of irreducible over $\overline{k}$ components W of V with $\dim W = n-s$ such that $z_i \in W$ for all $1 \le i \le u$. The working time of this algorithm is polynomial in d^n, d_1, d_2, M, M_1, m, the sum of the sizes of $\sum_{1\le i\le u} L(z_i)$, of the points z_i, $1 \le i \le u$ and the degree $[k[\eta_1,\ldots,\eta_u] : k]$ of the extension of fields.*

REMARK 1 Theorem 1 and Theorem 2 are trivial for $s = 0$. One can take $L_i = X_i$, $0 \le i \le n$ and $L_{n+1} = X_n$ for $s = 0$. So in what follows we shall assume without loss of generality that the polynomials $f_1,\ldots,f_m$ are linearly independent over k. Hence $\dim V \le n-1$ and we shall suppose without loss of generality that $1 \le s$ in the statements of Theorem 1 and Theorem 2.

1 Monodromy and irreducibility

Let $n \ge 1$ and $1 \le s \le n$ be integers. Let k be an arbitrary field of zero–characteristic, V_s be a defined over k projective algebraic variety in $\mathbb{P}^n(\overline{k})$, and all the irreducible components of V_s have the same dimension $n-s$. Suppose that the degree $\deg V_s = D \ge 1$ (here and below D depends on s). Let $T_0, T_{s+1}, T_{s+2},\ldots,T_{n+1}$ be linear forms in $X_0,\ldots,X_n$ with coefficients from k. Let

$$A^{(s)} = V_s \cap \mathcal{Z}(T_{s+1},\ldots,T_n),\ \&\ 0 \notin T_0(A^{(s)}),\ \&\ \#(T_{n+1}/T_0)(A^{(s)}) = \deg V_s, \tag{2}$$

where the intersection is considered in $\mathbb{P}^n(\overline{k})$, and $\#$ denotes the number of the elements of a set. In particular, $\#A^{(s)} = D$ and the intersection $V_s \cap \mathcal{Z}(T_{s+1},\ldots,T_n)$ is transversal at each point by the Bézout theorem.

Consider the morphisms

$$p : V_s \to \mathbb{P}^{n-s}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (T_0 : T_{s+1}, T_{s+2} : \ldots : T_n), \tag{3}$$

$$V_s \to \mathbb{P}^{n-s+1}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (T_0 : T_{s+1}, T_{s+2} : \ldots : T_{n+1}). \tag{4}$$

We shall suppose that $T_0, T_{s+1}, T_{s+2},\ldots,T_n$, (respectively $T_0, T_{s+1}, T_{s+2},\ldots,$ T_{n+1} are coordinate functions on $\mathbb{P}^{n-s}(\overline{k})$, (respectively $\mathbb{P}^{n-s+1}(\overline{k})$). Then, cf., e.g., [4], the morphism p is finite dominant, the image of the morphism (4) is $\mathcal{Z}(\Phi)$ where $\Phi \in k[T_0, T_{s+1}, T_{s+2},\ldots,T_{n+1}]$ is a homogeneous separable polynomial, the degree $\deg_{T_{n+1}} \Phi = D$ and leading coefficient $\mathrm{lc}_{T_{n+1}}\Phi$ of Φ with respect to T_{n+1} is equal to 1. Denote by $q : V_s \to \mathcal{Z}(\Phi)$ the morphism induced by (4). Hence $q(V_s) = \mathcal{Z}(\Phi)$ and $\deg q(V_s) = D$. Denote by $k(V_s)$ and $k(q(V_s))$ the algebras of defined over k rational functions on V_s and $q(V_s)$ respectively (by definition these algebras are isomorphic to the direct products of fields of rational functions of all defined over k components of V_s and $q(V_s)$ respectively). The morphism q is finite dominant and defined over k. Besides that, q is birational in the sense that it induces the isomorphism $k(q(V_s)) \simeq k(V_s)$. Let $r : q(V_s) \to \mathbb{P}^{n-s}$ be the morphism of the linear projection to the coordinates $T_0, T_{s+1}, T_{s+2}, \ldots, T_n$. Hence $p = r \circ q$. The morphism r is defined over k and finite dominant since $\mathrm{lc}_{T_{n+1}} \Phi = 1$.

Denote by $R = \mathrm{Res}_{T_{n+1}}(\Phi, \partial\Phi/\partial T_{n+1}) \in k[T_0, T_{s+1}, T_{s+2}, \ldots, T_n]$ the discriminant with respect to T_{n+1} of the polynomial Φ. Hence $0 \neq R$ is a homogeneous with respect to $T_0, T_{s+1}, T_{s+2}, \ldots, T_n$ polynomial of degree $D(D-1)$. Let R_0 be square free part of R, i.e., R_0 is separable and $\mathcal{Z}(R) = \mathcal{Z}(R_0)$. The polynomial R_0 is uniquely defined up to a nonzero factor from k. We choose and fix R_0.

Let us identify $\mathcal{Z}(T_{s+1}, \ldots, T_n) \subset \mathbb{P}^n(\overline{k})$ (respectively in $\mathbb{P}^{n-s+1}(\overline{k})$, $\mathbb{P}^{n-s}(\overline{k})$) with $\mathbb{P}^{s+1}(\overline{k})$ (respectively $\mathbb{P}^2(\overline{k})$, $\mathbb{P}^1(\overline{k})$). Consider the projective algebraic curve $V_{s,*} = V_s \cap \mathcal{Z}(T_{s+1}, \ldots, T_{n-1}) \subset \mathbb{P}^{s+1}(\overline{k})$. Let us repeat the described construction to $V_{s,*} \subset \mathbb{P}^{s+1}(\overline{k})$ in place of $V_s \subset \mathbb{P}^n(\overline{k})$. Now n and s are replaced by $s+1$ and s respectively. The linear forms $T_0, T_{s+1}, T_{s+2}, \ldots, T_{n+1}$ are replaced by T_0, T_n, T_{n+1}. The new set $A^{(s)}$ is the same as it was initially. We get the objects p_*, q_*, r_*, Φ_*, R_*, $R_{0,*}$ which are similar to p, q, r, Φ, R, R_0 and satisfy the analogous properties by the similar reasons. Note that $\Phi_* = \Phi(T_0, 0, \ldots, 0, T_n, T_{n+1})$, $R_* = R(T_0, 0, \ldots, 0, T_n)$.

The following lemma is known.

LEMMA 1 *Let Z be a new variable. Let $g = Z^\nu + g_{\nu-1}Z^{\nu-1} + \ldots + g_0 \in \mathbb{C}[Z]$ be a polynomial of degree $\nu \geq 1$ with complex coefficients $g_i \in \mathbb{C}$, $0 \leq i \leq \nu - 1$. Let $z_1, \ldots, z_\nu \in \mathbb{C}$ be the roots of the polynomial g counting with the multiplicities. Then for every $0 < \varepsilon \in \mathbb{R}$ there is $0 < \delta \in \mathbb{R}$ satisfying the following property. Let $\widetilde{g}_0, \ldots, \widetilde{g}_{\nu-1} \in \mathbb{C}$. Suppose that $|\widetilde{g}_i - g_i| < \delta$ for every $0 \leq i \leq \nu - 1$. Let $\widetilde{z}_1, \ldots, \widetilde{z}_\nu \in \mathbb{C}$ be the roots of the polynomial $\widetilde{g} = Z^\nu + \widetilde{g}_{\nu-1}Z^{\nu-1} + \ldots + \widetilde{g}_0 \in \mathbb{C}[Z]$ counting with the multiplicities. Then there is a permutation σ of $1, \ldots, \nu$ such that $|\widetilde{z}_{\sigma(i)} - z_i| < \varepsilon$.*

In what follows applying this lemma in the present paper we shall suppose without loss of generality that $\sigma = 1$ is the identity permutation. Now we can formulate our irreducibility criterion.

THEOREM 3 *Let $n \geq 3$ and $1 \leq s \leq n-2$ be integers. Let V_s be an equidimensional projective algebraic variety in $\mathbb{P}^n(\overline{k})$ with $\dim V_s = n - s$. Let $T_0, T_{s+1}, T_{s+2}, \ldots, T_{n+1}$ be linear forms from $k[X_0, \ldots, X_n]$ satisfying (2). Let the polynomial Φ and its discriminant R be as above. Suppose that the intersection $\mathcal{Z}(R) \cap \mathcal{Z}(T_{s+1}, \ldots, T_{n-1})$ is transversal (it is considered in $\mathbb{P}^{n-s}(\overline{k})$), , i.e., that the polynomial $R_0(T_0, 0, \ldots, 0, T_n)$ is separable. Then the irreducible over $\overline{k}$ (respectively k) components of algebraic varieties V_s and $V_{s,*}$ are in the one–to–one correspondence by the rule $W \mapsto W \cap \mathcal{Z}(T_{s+1}, \ldots, T_{n-1})$.*

PROOF Since V_s and $V_{s,*}$ are defined over k it is sufficient to prove only the assertion related to the irreducible over $\overline{k}$ components. Denote by N (respectively N_*) the number of all irreducible over $\overline{k}$ components of V_s (respectively $V_{s,*}$). Condition (2) implies that the intersection $V_s \cap \mathcal{Z}(T_{s+1}, \ldots, T_{n-1})$ is transversal at each its irreducible component. Hence by the Bézout theorem the inequality $N_* \geq N$ holds, and if $N_* = N$ then the required one–to–one correspondence takes place. So it is sufficient to prove that $N = N_*$. Note that N (respectively N_*) is the number of irreducible over $\overline{k}$ components of $\mathcal{Z}(\Phi)$ (respectively $\mathcal{Z}(\Phi_*)$) since q (respectively q_*) is a finite birational isomorphism.

We shall assume without loss of generality that k is a subfield of the field of complex numbers $\mathbb{C}$. Recall that $R_* \in k[T_0, T_n]$ is a nonzero homogeneous polynomial. We shall suppose without loss of generality that T_0 does not divide R_* replacing if it is necessary T_0 by $T_0 + \lambda T_n$ with an appropriate integer λ. Let $y_1, \dots, y_u$ be all the pairwise different roots of the polynomial $R_*(1, T_n)$. Hence $u = \deg R_{0,*} = \deg R_0$ by the condition of the lemma. Let us choose a point $y \in \mathbb{C}$ such that $R_*(y) \neq 0$ and for every $1 \le i_1 \neq i_2 \le u$ the points y, y_{i_1}, y_{i_2} do not belong to the same line in $\mathbb{C}$ (considered as $\mathbb{R}^2$). Let $0 < m_1 \in \mathbb{R}$. Denote by b_i the closed disc with the radius m_1 around y_i, $1 \le i \le u$. Let us choose m_1 so small that any line in $\mathbb{C}$ trough y intersects at most one disc b_i, $1 \le i \le u$, and $|y_i - y_j| > 3m_1$, $|y - y_i| > m_1$ for all $1 \le i \neq j \le u$. Denote by c_i, $1 \le i \le u$, the circumference with the radius m_1 around y_i. Denote by z_i the intersection of the interval $[y, y_i]$ with c_i. Denote by e_i the union of the interval $[y, z_i]$ and c_i. Denote by γ_i, $1 \le i \le u$ the path from y to z_i along $[y, z_i]$, then by c_i around y_i counterclockwise, and back from z_i to y along the interval $[z_i, y]$. Set $e = \cup_{1 \le i \le u} e_i$ and $E_z = (T_{n+1}/T_0)(r_*^{-1}(1 : z))$ for every $z \in \mathbb{C}$. Note that for every $z \in \mathbb{C} \setminus \mathcal{Z}(R)$ the number of elements $\# E_z = D$.

Set $E = E_y$. Hence $\# E = D$. Let $a \in E$. Denote by ξ_a the analitical function in Z defined in a neighborhood of y such that $\Phi_*(1, Z, \xi_a) = 0$ and $\xi_a(y) = a$. The result of the analitic continuation of ξ_a along γ_i is $\xi_{\sigma_i(a)}$ where σ_i is the uniquely defined permutation of E. Denote by S_D the group of permutations of E and by G the subgroup of S_D generated by all σ_i, $1 \le i \le u$. Then it is known, see, e.g., [2], [10], that the number N_* of irreducible over $\overline{k}$ components of $V_{s,*}$ coincides with the number of classes of transitivity of G on E.

Let $\mu_i, \nu_i \in k$, $s+1 \le i \le n-1$ and $0 < \delta \in \mathbb{R}$. Denote by $\mathcal{A}_\delta$ the condition $\sum_{s+1 \le i \le n-1} (|\mu_i|^2 + |\nu_i|^2) < \delta$. Set $\widetilde{T}_i = T_i$, $i = 0, n, n+1$ and $\widetilde{T}_i = T_i - \mu_i T_0 - \nu_i T_n$ for all $s+1 \le i \le n-1$. There is $0 < \delta_0 \in \mathbb{R}$ such that under the condition $\mathcal{A}_{\delta_0}$ the linear forms $\widetilde{T}_i$ satisfy the same properties (considered above) as T_i, $i \in \{0, s+1, s+2, \dots, n+1\}$ do. In what follows we shall suppose that $\mathcal{A}_{\delta_0}$ holds. Then for $\widetilde{T}_i$ the objects $\widetilde{A}^{(s)}$, $\widetilde{\Phi}$, $\widetilde{R}$ and so on are defined. They correspond to $A^{(s)}$, Φ, R and so on. Note that $\Phi = \widetilde{\Phi}$, $R = \widetilde{R}$ (as polynomials in $X_0, \dots, X_n$), $N = \widetilde{N}$, $u = \widetilde{u} = \deg R_0$ and

$$\widetilde{\Phi}_* = \Phi(T_0, \mu_{s+1} T_0 + \nu_{s+1} T_n, \dots, \mu_{n-1} T_0 + \nu_{n-1} T_n, T_n, T_{n+1}), \quad (5)$$

$$\widetilde{R}_* = R(T_0, \mu_{s+1} T_0 + \nu_{s+1} T_n, \dots, \mu_{n-1} T_0 + \nu_{n-1} T_n, T_n). \quad (6)$$

Hence by Lemma 1 applied to the polynomial $R_*(1, Z)/\mathrm{lc}_Z(R_*(1, Z))$ there is $0 < \delta_1 < \delta_0$ such that $\mathcal{A}_{\delta_1}$ entails $|\widetilde{y}_i - y_i| < m_1/2$ for every $1 \le i \le u$. We shall suppose in what follows that $\mathcal{A}_{\delta_1}$ holds. Now we choose $\widetilde{y} = y$ and $\widetilde{m}_1 = m_1/2$.

Let $m_2 = \inf\{|a_1 - a_2| : a_1, a_2 \in E_z \,\&\, a_1 \neq a_2 \,\&\, z \in e\}$. Then $m_2 > 0$ due to the compactness of e. By Lemma 1 applied to the polynomials $\Phi_*(1, z, Z)$,$z \in e$, by (5) and due to the compactness of e there is $0 < \delta_2 \le \delta_1$ such that $\mathcal{A}_{\delta_2}$ entails that for every $z \in e$ for every $a \in E_z$ there is the unique $\widetilde{a} \in \widetilde{E}_z$ such that $|a - \widetilde{a}| < m_2/3$. We shall suppose in what follows that $\mathcal{A}_{\delta_2}$ holds.

Now there is the bijection $\tau : E \to \widetilde{E}$, $a \mapsto \widetilde{a}$, $|a - \widetilde{a}| < m_2/3$. Hence τ induces the isomorphism $S_D \to \widetilde{S}_D$. By our construction the path γ_i is homotopic to $\widetilde{\gamma}_i$ in $\mathbb{C} \setminus \mathcal{Z}(\widetilde{R}_*)$, for every $1 \le i \le u$. Therefore, $\widetilde{\sigma}_i = \tau \circ \sigma_i \circ \tau^{-1}$, for every $1 \le i \le u$. Hence the groups $G \simeq \widetilde{G}$ and $N_* = \widetilde{N}_*$.

Denote by $\mathcal{L}_{n-s+1}$, (respectively $\mathcal{L}_{n-s-1}$) the vector space of linear forms with coefficients from $\overline{k}$ with the basis $T_0, T_{s+1}, \ldots, T_n$ (respectively $T_{s+1}, \ldots, T_{n-1}$). According to the first Bertini, see [1], theorem applied subsequently $n-s-1$ times in any neighborhood in the classic topology of the vector subspace $\mathcal{L}_{n-s-1} \subset \mathcal{L}_{n-s+1}$ (the neighborhood of $\mathcal{L}_{n-s-1}$ is considered here in the corresponding Grassmann variety) there is an $(n-s-1)$–dimensional vector subspace $\mathcal{L} \subset \mathcal{L}_{n-s+1}$ such that $\dim q(V_s) \cap \mathcal{Z}(\mathcal{L}) = 1$, $\deg q(V_s) \cap \mathcal{Z}(\mathcal{L}) = D$, and for every irreducible over $\overline{k}$ component W of $q(V_s)$ the algebraic variety $W \cap \mathcal{Z}(\mathcal{L})$ is irreducible over $\overline{k}$. Hence one can choose $\mathcal{L}$ to be a linear subspace generated by $\widetilde{T}_{s+1}, \ldots, \widetilde{T}_{n-1}$ for some μ_i, ν_i, $s+1 \le i \le n-1$, satisfying $\mathcal{A}_{\delta_2}$. In this case $\widetilde{N}_* = \widetilde{N}$. Thus, $N = \widetilde{N} = \widetilde{N}_* = N_*$. The theorem is proved.

COROLLARY 1 *Let $1 \le s \le n-1$. Let us identify the set of all $(n-s+1)$–tuples $(L_0, L_{s+1}, \ldots, L_n)$ of linear forms $L_j \in \overline{k}[X_0, \ldots, X_n]$ with the affine space $\mathbb{A}^{(n-s)(n+1)}(\overline{k})$. Then the set of all $(L_0, L_{s+1}, \ldots, L_n)$ such that assertions (a) and (b) of Theorem 1 related to the ground field $\overline{k}$ hold for the considered fixed s is a nonempty defined over k open in the Zariski topology subset of $\mathbb{A}^{(n-s)(n+1)}(\overline{k})$.*

PROOF The case $s = n-1$ is easy. So we shall suppose that $s \le n-2$. Consider the affine space of the homogeneous polynomials in $n-s+2 \ge 3$ variables with coefficients from $\overline{k}$ of the given degree. It is known, see, e.g., [1], that the set of all irreducible over $\overline{k}$ homogeneous polynomials from this affine space is a nonempty open in the Zariski topology subset of the considered affine space. Now the corollary follows from the first paragraph of the proof (we leave the details to the reader). The corollary is proved.

COROLLARY 2 *Let $n \ge 2$ and $1 \le s \le n-1$ be integers. Let V_s be an equidimensional projective algebraic variety in $\mathbb{P}^n(\overline{k})$ with $\dim V_s = n-s$. Let $T_0, T_{s+1}, T_{s+2}, \ldots, T_{n+1}$ be linear forms from $k[X_0, \ldots, X_n]$ satisfying (2). Let the polynomial Φ and its discriminant R be as above. Let $L \in k[T_0, T_{s+1}, T_{s+2}, \ldots, T_n]$ be a nonzero linear form. Suppose that the intersection $\mathcal{Z}(R) \cap \mathcal{Z}(L)$ is transversal in $\mathbb{P}^{n-s}(\overline{k})$ (or which is equivalent $\deg \mathcal{Z}(R) = \deg(\mathcal{Z}(R) \cap \mathcal{Z}(L))$ in $\mathbb{P}^{n-s}(\overline{k})$). Then the intersection $V_s \cap \mathcal{Z}(L)$ is transversal, $\deg V_s = \deg V_s \cap \mathcal{Z}(L)$ in $\mathbb{P}^n(\overline{k})$ and the irreducible over $\overline{k}$ (respectively irreducible over k) components of V_s and $V_s \cap \mathcal{Z}(L)$ are in the one–to–one correspondence by the rule $W \mapsto W \cap \mathcal{Z}(L)$*

PROOF Let $\mathbb{P}^{n+1}(\overline{k})$ has homogeneous coordinates $X_0, \ldots, X_{n+1}$. Let us identify $\mathbb{P}^n(\overline{k}) = \mathcal{Z}(X_{n+1}) \subset \mathbb{P}^{n+1}(\overline{k})$. Hence $V_s \subset \mathbb{P}^{n+1}(\overline{k})$. Replacing if necessary n by $n+1$ and $T_0, T_{s+1}, \ldots, T_n$ by $T_0, T_{s+1}, \ldots, T_n$, X_{n+1} we shall suppose without loss of generality that $n \ge 3$ and $1 \le s \le n-2$. Set $\widetilde{T}_{s+1} = L$ (one should not confuse the tilde here and below with the one from the proof of the theorem). We have $R \bmod L \ne 0$. Therefore, there are linear forms $\widetilde{T}_0, \widetilde{T}_{s+2}, \ldots, \widetilde{T}_n$ in $T_0, T_{s+1}, T_{s+2}, \ldots, T_n$ with coefficients from k such that $\widetilde{T}_0, \widetilde{T}_{s+1}, \ldots, \widetilde{T}_n$ are linearly independent, the number of elements $\# r^{-1}(\mathcal{Z}(\widetilde{T}_{s+1}, \ldots, \widetilde{T}_n)) = \deg \Phi$, $0 \notin \widetilde{T}_0(\# r^{-1}(\mathcal{Z}(\widetilde{T}_{s+1}, \ldots, \widetilde{T}_n)))$ and the intersection $\mathcal{Z}(R) \cap \mathcal{Z}(\widetilde{T}_{s+1}, \ldots, \widetilde{T}_{n-1})$ is transversal. Let us replace in (2) T_0, $T_{s+1}, \ldots, T_n$ and T_{n+1} by $\widetilde{T}_0$, $\widetilde{T}_{s+1}, \ldots, \widetilde{T}_n$, and T_{n+1} respectively. Then the obtained condition holds. We get the polynomials $\widetilde{\Phi}$, $\widetilde{R}$ corresponding to the new linear forms according to the construction described before the Theorem 3. Now applying

Theorem 3 in the considered situation we get all the assertions of the corollary. The corollary is proved.

2 Proof of Theorem 1

At first our aim is to construct for every $1 \le s \le n$ some linear forms $Y_{s,0}, \dots, Y_{s,n+1}$ in $X_0, \dots, X_n$. Let $1 \le s \le n$ be arbitrary but fixed for some time. According to [4], Section 2 one can construct linear forms $L_{s,0}, L_{s,s+1}, L_{s,s+2}, \dots, L_{s,n}$ with integer coefficients of length $O(n \log d)$ and a finite set A'''_s such that $A'''_s = V_s \cap \mathcal{Z}(L_{s,s+1}, \dots, L_{s,n})$, the last intersection is transversal, consists of $D = \deg V_s$ smooth points of the algebraic variety V and $0 \notin L_{s,0}(A'''_s)$. Let us construct a linear form $L_{s,n+1}$ with integer coefficients of length $O(n \log d)$ such that $\#(L_{s,n+1}/L_{s,0})(A'''_s) = D$. Let us construct linear forms $L_{s,i}$, $1 \le i \le s$ with integer coefficients of length $O(n\,\log d)$ such that $L_{s,0}, \dots, L_{s,n}$ are linearly independent. Denote for brevity $Z_j = L_{s,j}$ for all j. Set $T_j = Z_j$ for all $0 \le j \le n+1$.

Denote for brevity $T = (T_0, \dots, T_{n+1})$. Let $\mathcal{B}'_s(T)$ means that (2) holds for T and all the points of $A^{(s)}$ are smooth points of V, herewith $\mathcal{B}'_s$ is considered as a function of T and all T_j may have coefficients from an extension of $\overline{k}$.

Suppose that $s \le n-2$ and $V_s \ne \emptyset$ for some time. In this case the linear forms T_j will be changed recursively in the algorithm. Our aim is to construct finally linear forms T_j with integer coefficients of length $O(n \log d)$ such that $T_0, T_{s+1}, \dots, T_{n+1}$ satisfy conditions of Theorem 3. At all steps of the described recursion $T_0, T_{s+1}, \dots, T_n$ are linear forms with integer coefficients in $Z_0, Z_{s+1}, \dots, Z_n$, and $T_j = Z_j$ for $1 \le j \le s$, $j = n, n+1$.

Let Φ, R, q, r be as in Section 1. Using the algorithm from [3] let us construct the curve $V_{s,*}$ and the polynomials Φ_*, R_*, see Section 1. Denote by $R_{*,0}$ the square free part of R_*. Set

$$v_s(T) = \deg R_0, \quad u_s(T) = \deg R_{*,0}.$$

Hence $v_s(T) \ge u_s(T)$. Similarly to the proof of Theorem 3 we can suppose without loss of generality that T_0 does not divide R_* replacing if necessary T_0 by $T_0 + \lambda T_n$ where λ is an integer of length $O(n\,\log d)$. Now leading coefficient $\mathrm{lc}_{T_n} R_* \in k$, $\deg R_* = \deg R$ and R is homogeneous. Hence $\mathrm{lc}_{T_n} R \in k$. Let us compute all the pairwise distinct roots $y_1, \dots, y_u$ of the polynomial $R_*(1, Z)$ (i.e., all the fields $k[y_i]$; here one need to factor $R_*(1, Z)$ over k using [3]). Hence $u_s(T) = u$. Now $\mathcal{Z}(R_*, T_0) = \emptyset$ in $\mathbb{P}^1(\overline{k})$. Further, the leading coefficient $\mathrm{lc}_{T_n} R_* \in k$, $\deg R_* = \deg R$ and R is homogeneous. Hence $\mathrm{lc}_{T_n} R \in k$. Therefore, the morphism $r_0 : \mathcal{Z}(R) \to \mathbb{P}^{n-s-1}(\overline{k})$ of the linear projection to the coordinates $T_0, T_{s+1}, \dots, T_{n-1}$ is finite dominant. Hence $\deg r_0 = \deg R_0$.

Let $\varepsilon_i > 0$ be an infinitesimal with respect to the field $k_{i-1} = k(\varepsilon_1, \dots, \varepsilon_{i-1})$, $1 \le i \le 5$. We shall suppose that the algebraic closure of the field $k_4 = k(\varepsilon_1, \dots, \varepsilon_4)$ is supplied with a real structure, see [9]. Hence one can consider systems of polynomial equations and inequalities with squares of absolute values over k_4. Let $X_{i,0}, \dots, X_{i,n}$, $1 \le i \le 4$, be new variables. Denote for brevity $X^{(i)} = (X_{i,0}, \dots, X_{i,n})$ for $1 \le i \le 4$ and $b(X^{(i)}) = b(X_{i,0}, \dots, X_{i,n})$ for an arbitrary polynomial b in $n+1$ variables. Consider the system of equations and inequalities

$$\left\{\begin{array}{ll}\sum_{s+1\le i\le n-1}|T_i(X^{(1)})|^2<\varepsilon_1, & \\ \varepsilon_3<|T_n(X^{(1)})-T_n(X^{(3)})|^2<\varepsilon_2, & \\ |T_{n+1}(X^{(i)})-T_{n+1}(X^{(i+1)})|^2=\varepsilon_4, & i=1,3, \\ T_j(X^{(i_1)})-T_j(X^{(i_2)})=0, & 1\le i_1<i_2\le 4, \quad s+1\le j\le n-1, \\ T_n(X^{(i)})-T_n(X^{(i+1)})=0, & i=1,3, \\ T_0(X^{(i)})-1=0, & 1\le i\le 4, \\ f_j(X^{(i)})=0, & 1\le j\le m, \quad 1\le i\le 4.\end{array}\right. \tag{7}$$

For an arbitrary projective algebraic variety $E\subset\mathbb{P}^n(\overline{k})$ we shall denote by $\mathrm{con}(E)$ 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 E.

LEMMA 2 [1] *System (7) has a solution in* $\mathrm{con}(V_s(\overline{k}_4))^4\subset\mathbb{A}^{4n+4}(\overline{k}_4)$ *if and only if* $u_s(T)<\deg r_0$.

PROOF Let $u_s(T)<\deg r_0$. Then by Lemma 1 and transfer principle, see [8], applied to the polynomial $R_*(1,Z)/\mathrm{lc}_Z R_*(1,Z)$ there are $z_{s+1},\dots,z_{n-1},z_{1,n},z_{3,n}\in\overline{k_3}$ such that $\sum_{s+1\le i\le n-1}|z_i|^2<\varepsilon_1$, $\varepsilon_3<|z_{1,n}-z_{3,n}|^2<\varepsilon_2$ and $R(1,z_{s+1},\dots,z_{n-1},z_{n,\alpha})=0$, $\alpha=1,3$. We have $R(1,z_{s+1},\dots,z_{n-1},T_n)\neq 0$ since leading coefficient $\mathrm{lc}_{T_n}R\in k$. Recall that leading coefficient $\mathrm{lc}_{T_{n+1}}\Phi=1$. Hence by Lemma 1 and transfer principle, see [8], applied to two polynomials $\Phi(1,z_{s+1},\dots,z_{n-1},z_{n,\alpha},Z)$, $\alpha=1,3$, there are $\widetilde{z}_{\alpha,n},\widetilde{z}_{\beta,n+1}\in\overline{k_4}$, $\alpha=1,3$, $\beta=1,2,3,4$ such that $\widetilde{z}_{\alpha,n}-z_{\alpha,n}$, $\alpha=1,3$, are infinitesimal with respect to k_3, $|\widetilde{z}_{\beta,n+1}-\widetilde{z}_{\beta+1,n+1}|^2=\varepsilon_4$, $\beta=1,3$ and $\Phi(1,z_{s+1},\dots,z_{n-1},\widetilde{z}_{\alpha,n},\widetilde{z}_{\beta,n+1})=0$ for $\alpha=1,3$, $\beta=\alpha,\alpha+1$. Set $\widetilde{z}_{\beta,n}=\widetilde{z}_{\alpha,n}$ for $\alpha=1,3$, $\beta=\alpha,\alpha+1$. The morphisms q is finite dominant. Therefore, there is a solution of system (7) with additional equations $T_j(X^{(\beta)})=z_j$, $s+1\le j\le n-1$, $T_j(X^{(\beta)})=\widetilde{z}_{\beta,j}$, $j=n,n+1$, $\beta=1,2,3,4$.

Conversely, if system (7) has a solution then as it is seen from the description of the algorithm, see below, $u_s(T)<\deg r_0$. The lemma is proved.

Let $\varphi_j=0$, $j\in J$ be the family of all the equalities (not inequalities) of system (7) apart of the equations $f_j(X^{(i)})=0$. Let us replace all the considered equations $\varphi_j=0$, $j\in J$ in (7) by one inequality $\sum_{j\in J}|\varphi_j|^2<\varepsilon_5$. This new system has a solution from $\mathrm{con}(V_s(\overline{k}_5))^4$ if and only if system (7) has a solution from $\mathrm{con}(V_s(\overline{k}_4))^4$. Now using the algorithms from [7], [4] applied to $\mathrm{con}(V(\overline{k}_5))^4\subset\mathbb{A}^{4n+4}(\overline{k}_5)$ we can construct a solution from $\mathrm{con}(V_s(\overline{k}_5))^4$ of this new system if it exists. For every $a\in\overline{k}_j$ that is not infinitely large with respect to k_{j-1} denote, see [9] Section 1, by $\mathrm{st}_{\varepsilon_j}a\in\overline{k}_{j-1}$ the element such that $a-\mathrm{st}_{\varepsilon_j}a$ is an infinitesimal with respect to k_{j-1}. Computing the standard part $\mathrm{st}_{\varepsilon_5}$, see [9] Section 1, of this solution we construct a solution $X_{i,j}=x_{i,j}\in\overline{k}_4$, $1\le i\le 4$, $0\le j\le n$ of system (7) from $\mathrm{con}(V_s(\overline{k}_4))^4$ if it exists.

Suppose that (7) does not have a solution. Then $u_s(T)=\deg r_0=\deg R_0$ by Lemma 2 and the linear forms T_i satisfying the conditions of Theorem 3 are constructed. Suppose that (7) has a solution. Let us compute $x_j=\mathrm{st}_{\varepsilon_4}x_{1,j}$, $0\le j\le n$. Set $T'_j=T_j-T_j(x_0,\dots,x_n)T_0$, $s+1\le j\le n-1$, and $T'_j=T_j$, $j=0,\dots,s,\,n,n+1$. Let the notation T' for T'_j be similar to T defined for T_j.

[1] The corresponding lemma from the Russian journal version is slightly corrected here. This required additional reference to [7] in the algorithm.

Then the property $\mathcal{B}'_s(T')$ is true. Let the number $u(T')$ for T' be similar to $u(T)$ defined for T. From (7) we get $u' = u_s(T') > u_s(T) = u$.

Let $T''_0, T''_{s+1}, \ldots, T''_{n+1}$ be linear forms in $Z_0, Z_{s+1}, \ldots, Z_{n+1}$. Denote $v_s = v_s(T)$. Let $0 \le a$ be an integer. The property $\mathcal{B}'_s(T'')\&(u_s(T'') \ge a)$ is a good property of the argument T'' in a sense similar to [9], see also, [4]. Denote for brevity the considered property by $\mathcal{B}_s(T'', a)$ and set $\mathcal{B}_s(T'') = \mathcal{B}_s(T'', v_s)$. Hence (the reader can see it also directly) one can replace subsequently the nonzero coefficients in Z_j of linear forms $T'_{s+1}, \ldots, T'_{n-1}$ by integers of length $O(n \log d)$ and obtain new linear forms T'' such that $\mathcal{B}_s(T'', u')$ holds and $T''_j = T_j$ for $j = 0, \ldots, s, n, n+1$. Now we replace T by T'' and proceed to the next step of the recursion. The number of such steps with the replacement T by T'' at the end is bounded from above by d^{n-s} by the Bézout theorem.

The new morphism r_0 is distinct from the old one only by the automorphism of $\mathbb{P}^{n-s-1}(\overline{k})$. The morphism r_0 is finite dominant. Hence T_0 may divide R_* only in the first step of the recursion. So after the first step T_j, $j = 0, \ldots, s$, $n, n+1$ are not replaced.

Thus, finally we obtain the linear forms T such that $T_0, T_{s+1}, \ldots, T_{n+1}$ satisfy conditions of Theorem 3. In what follows we shall not suppose that $s \le n-2$ and $V_s \ne \emptyset$. Define the property $\mathcal{B}_{n-1} = \mathcal{B}'_{n-1}$. Set $Y_{s,j} = T_j$ for all $0 \le j \le n+1$. In what follows we shall not suppose that s is fixed. Denote $Y_s = (Y_{s,0}, \ldots, Y_{s,n+1})$, $1 \le s \le n$. Then $\mathcal{B}_s(Y_s)$ is true for every $1 \le s \le n-1$. Let $0 \le j \le n-1$. Consider the property $\mathcal{C}_j = \mathcal{B}_1 \& \ldots \& \mathcal{B}_j$ of linear forms in $X_0, \ldots, X_n$ (hence $\mathcal{C}_0$ is identically true). Let $L' = (L'_0, \ldots, L'_{n+1})$ where all L'_i are linear forms in $X_0, \ldots, X_n$. By definition $\mathcal{C}_n(L')$ is true if and only if $\mathcal{C}_{n-1}(L')$ is true and the assertion (a) of Theorem 1 holds for $L'_0, \ldots, L'_{n+1}$ in place of $L_0, \ldots, L_{n+1}$. Note that $\mathcal{C}_j$ is a good property, see [9], [4], for every $0 \le j \le n$.

Set $Y_i^{(0)} = X_i$, $0 \le i \le n$, and $Y_{n+1}^{(0)} = X_n$. Let $0 \le j \le n-1$ be an integer. Suppose that we have constructed recursively $Y^{(j)} = (Y_0^{(j)}, \ldots, Y_{n+1}^{(j)})$ where all $Y_i^{(j)}$ are linear forms in $X_0, \ldots, X_n$ with integer coefficients of length $O(n \log d)$ such that $\mathcal{C}_j(Y^{(j)})$ is true. Let ε be a transcendental element over the field k. Set $Y^{(j)} + \varepsilon Y_{j+1} = (Y_0^{(j)} + \varepsilon Y_{j+1,0}, \ldots, Y_{n+1}^{(j)} + \varepsilon Y_{j+1,n+1})$ (we extend here k till $k(\varepsilon)$). Then $\mathcal{C}_{j+1}(Y^{(j)} + \varepsilon Y_{j+1})$ is true. Since $\mathcal{C}_{j+1}$ is a good property one can replace subsequently the nonzero coefficients in X_i, $0 \le i \le n$, of linear forms from $Y^{(j)} + \varepsilon Y_{j+1}$ by integers of length $O(n \log d)$ and obtain new linear forms $Y^{(j+1)}$ such that $\mathcal{C}_{j+1}(Y^{(j+1)})$ is true.

At the end we check whether $v_s(Y^{(n)}) = v_s$ for every $1 \le s \le n-2$ such that $V_s \ne \emptyset$. If it is not true then $v_s(Y^{(n)}) > v_s$ for some s. In this case we replace $L_{s,i} = Y_i^{(n)}$ for all $1 \le s \le n$, $0 \le i \le n+1$ and return to the beginning of the described construction.

Since $v_s \le d^s(d^s - 1)$ for all s finally we shall come to the case when $v_s(Y^{(n)}) = v_s$ for all $1 \le s \le n-2$ such that $V_s \ne \emptyset$. Since $u_s(Y^{(n)}) \ge v_s$ by the described construction we have $u_s(Y^{(n)}) = v_s(Y^{(n)})$ for all considered s and one can apply Theorem 3 with $Y^{(n)}$ in place of T. Finally we set $L = Y^{(n)}$. Now assertions (a), (b) and (c) of Theorem 1 hold.

Let us prove (d) and (e). Let $s = n$. Then we define $V_{n,0} = A_n$. For every $1 \le s < n-1$ using the algorithm of [3] we construct all the defined over k and irreducible over k components of dimension 1 of the intersection $V \cap \mathcal{Z}(L_{s+1}, \ldots, L_{n-1})$. Denote by W_j, $j \in J_s$, the obtained curves. Again using the algorithm from [3] we choose for every $j \in J_s$ a defined over k and irreducible over k component $a_j \subset A_s \cap W_j$. Set $V_{s,0} = \cup_{j \in J_s} a_j$. Now the assertion (d) hold.

Let $z \in A_s$ and σ be a k–automorphism of $\overline{k}$. Then $\sigma(z) = z$ implies $\sigma(W_z) = W_z$ by our construction. Hence $k_z \subset k(z)$. Besides that, $\sigma(W_z) = W_z$ if and only if $\sigma(W_z \cap \mathcal{Z}(L_1, \dots, L_{n-1})) = W_z \cap \mathcal{Z}(L_1, \dots, L_{n-1})$ due to (b). Hence the minimal fields of definitions containing k of W_z and $W_z \cap \mathcal{Z}(L_1, \dots, L_{n-1})$ coincide.

Using the algorithm from [3] we construct all the defined over $\overline{k}$ and irreducible over $\overline{k}$ components of the algebraic varieties W_j, $j \in J_s$ and their minimal fields of definition. More precisely, these minimal fields of definitions are conjugated over k to the field k_j which is constructed by the algorithm. The algorithm also constructs a finite family of polynomials $\psi_{j,i} \in k_j[X_0, \dots, X_n]$, $i \in I_j$, such that $\mathcal{Z}(\psi_{j,i}, i \in I_j)$ is conjugated over k to each irreducible over $\overline{k}$ component of W_j. Let $z \in a_j \subset W_j$. For every $j \in J_s$ again using the algorithm from [3] we construct all the embeddings $\tau : k_j \to k(z)$ over k (there are at most $[k_j : k]$ such embeddings). Let us extend τ to the ring of polynomials in $X_0, \dots, X_n$ trivially, i.e., by the rule $\tau(X_i) = X_i$ for every i. Then there is only one τ such that $\tau(\psi_{j,i})(z) = 0$ for every $i \in I_j$. We compute this τ and set $k_z = \tau(k_j)$. Now the assertion of (e) hold. The required estimation for the working time of the described algorithm follows immediately from ones of the applied algorithms. Theorem 1 is proved.

REMARK 2 Let L be as in the proof of Theorem 1 and ε be a transcendental element over k. Let $L'_0, \dots, L'_n \in k[X_0, \dots, X_n]$ be arbitrary linear forms. Set $\widetilde{L}_j = L_j + \varepsilon L'_j$ for $0 \le j \le n$ and $\widetilde{L}_{n+1} = L_{n+1}$, $\widetilde{L} = (\widetilde{L}_0, \dots, \widetilde{L}_{n+1})$. Let us replace the field k by $k(\varepsilon)$ and L by $\widetilde{L}$. Then, see the statement of Theorem 1, the polynomials $\widetilde{\Phi}_s$, $\widetilde{R}_s$, $\widetilde{R}_{s,0}$ corresponding to $\widetilde{L}$ are defined. They are similar to Φ_s, R_s, $R_{s,0}$. Let us consider $\widetilde{\Phi}_s$, $\widetilde{R}_s$, $\widetilde{R}_{s,0}$ as polynomials in $X_0, \dots, X_n$ with coefficients from $k(\varepsilon)$. Then the least common denominator from $k[\varepsilon]$ of the coefficients of $\widetilde{\Phi}_s$ is not zero at $\varepsilon = 0$. Substituting $\varepsilon = 0$ we get $\widetilde{\Phi}_s|_{\varepsilon=0} = \Phi_s$ and $\widetilde{R}_s|_{\varepsilon=0} = R_s$. Further,

$$v_s(\widetilde{L}) \ge v_s(L) \tag{8}$$

for every $1 \le s \le n-2$ such that $V_s \ne \emptyset$. If at least one of inequalities (8) is strict then extending the field k till $k(\varepsilon)$ and applying the construction from the proof of the theorem to $L_{s,i} = \widetilde{L}_i$, $1 \le s \le n$, $0 \le i \le n+1$, we get new linear forms $\overline{L}$ similar to L such that $v_s(\overline{L}) \ge v_s(L)$ for all considered s and at least one of the last inequalities is strict. Hence replacing L by $\overline{L}$ one can iterate in the same way until all the inequalities from (8) become the equalities.

Suppose that (8) are equalities. Then by our definitions $\widetilde{R}_{s,0}|_{\varepsilon=0} = R_{s,0}$. Hence the linear forms $\widetilde{L}_j$ in place of T_j (respectively L_j), $0 \le j \le n+1$, satisfy conditions of Theorem 3 (respectively Theorem 1) with $k(\varepsilon)$ in place of k.

REMARK 3 *We do not construct linear forms L in general position with maximal possible $v_s(L)$. So we need to formulate and use the previous remark as some weak reduction to general position. Actually one can use also below Corollary 1 in place of Remark 2.*

3 Proof of Theorem 2

Let us prove assertion (b) of Theorem 2. Extending the field k till $k[\eta_1, \dots, \eta_u]$ we shall suppose in what follows that $k = k[\eta_1, \dots, \eta_u]$. Note that if $z_1, \dots, z_u$ belong to an irreducible over $\overline{k}$ component W of V then they belong to each conjugated over k to W component. Let ε be an infinitesimal with respect to the field k. Hence, see [9], Section 1, the mapping $\mathrm{st}_\varepsilon : \mathbb{P}^n(\overline{k(\varepsilon)}) \to \mathbb{P}^n(\overline{k})$ is defined such that $\mathrm{st}_\varepsilon(z)$ is an infinitely close to z element.

Let us construct linear forms $L_0, \dots, L_{n+1}$ from Theorem 1. Let $1 \le s \le n-1$. Let us construct for every $2 \le i \le u$ linearly independent linear forms $L_{i,0}, \dots, L_{i,n}$ in $L_0, \dots, L_n$ with coefficients from k of length polynomial in n, $L(z_1)$, $L(z_i)$ such that $L_{i,j}(z_\alpha) = 0$ for $1 \le j \le n-1$, $\alpha = 1, i$ and $L_{i,0}(z_\alpha) \ne 0$ for $\alpha = 1, i$. For $\alpha = 1, i$ put $\lambda_{i,\alpha} = (L_{i,n}/L_{i,0})(z_\alpha) \in k$. Set $L'_{i,j} = L_{i,j} + \varepsilon L_j$, $0 \le j \le n$. By Remark 2 applied to ε^{-1} in place of ε we shall suppose without loss of generality that $v_s(L) = v_s(L'_{i,0}, \dots, L'_{i,n}, L_{n+1})$ for all $2 \le i \le u$ and $1 \le s \le n-2$ such that $V_s \ne \emptyset$. Then by Theorem 3 and Theorem 1 for every $1 \le s \le n-1$ the irreducible over k (respectively $\overline{k}$) components of V_s and irreducible over $k(\varepsilon)$ (respectively $\overline{k}(\varepsilon)$) components of dimension 1 of $V \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})$ are in the one–to–one correspondence by the rule

$$W \mapsto W \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1}) = W_{s,i}, \tag{9}$$

and besides that, $\deg W = \deg W_{s,i}$ in (9) for every irreducible over $\overline{k}$ component W of V_s. Besides that, by Theorem 1 for every $1 \le s_1 \le n$ the intersection $V_{s_1} \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$ is nonempty if and only if $s_1 \le s+1$ and $V_{s_1} \ne \emptyset$. In the last case $\dim(V_{s_1} \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})) = s - s_1 + 1$. Therefore, cf., e.g., [3],

(*) for every $1 \le s_1 \le n$ the intersection $V_{s_1} \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1}) \ne \emptyset$ if and only if $s_1 \le s+1$ and $V_{s_1} \ne \emptyset$. In the last case $\dim(V_{s_1} \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})) = s - s_1 + 1$.

Suppose that $z_\alpha \in W$. Then, see, e.g., [9], Proposition 6, the set $W_{s,i} \cap \mathcal{Z}(L_{i,n} - \lambda_{i,\alpha} L_{i,0})$ is finite and $z_\alpha \in \mathrm{st}_\varepsilon(W_{s,i} \cap \mathcal{Z}(L_{i,n} - \lambda_{i,\alpha} L_{i,0}))$. Conversely, if $z_\alpha \in \mathrm{st}_\varepsilon(W_{s,i})$ then $z_\alpha \in W$.

Now we are going to compute all $W_{s,i}$ and choose among them such that $z_\alpha \in \mathrm{st}_\varepsilon(W_{s,i})$ for $\alpha = 1, i$. Consider ε as an variable. Let $\mathbb{A}^{n+2}(\overline{k})$ be defined over k and have the coordinates $X_0, \dots, X_{n+1}$, ε. Using the algorithm of [3] we construct all the defined over k and irreducible over k components W'' of dimension 3 of the intersection $\mathcal{Z}(f_1, \dots, f_m) \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})$ in $\mathbb{A}^{n+2}(\overline{k})$. For every W'' we construct a point from it and then $\lambda_0 \in \overline{k}$ (it depends on W'') such that $W'' \cap \mathcal{Z}(\varepsilon - \lambda_0) \ne \emptyset$. Further, using [3] we construct $W'' \cap \mathcal{Z}(\varepsilon - \lambda_0)$ and decide whether $\dim W'' \cap \mathcal{Z}(\varepsilon - \lambda_0) = \dim W''$. Thus, we (can) choose among components W'' all that are not contained in any finite union of hyperplanes $\mathcal{Z}(\varepsilon - \lambda)$, $\lambda \in \overline{k}$. Denote by $\widetilde{W}_j$, $j \in J_{s,i}$, the family of obtained algebraic varieties. More precisely, for every $j \in J_{s,i}$ the algorithm construct a finite family of polynomials $\varphi_{j,v} \in k[X_0, \dots, X_n, \varepsilon]$, $v \in I_j$, such that $\widetilde{W}_j = \mathcal{Z}(\varphi_{j,v},\, v \in I_j)$ in $\mathbb{A}^{n+2}(\overline{k})$. The algorithm construct also the number μ_j of all irreducible over $\overline{k}$ components of $\widetilde{W}_j$ for every $j \in J_{s,i}$.

Set $W_j = \mathcal{Z}(\varphi_{j,v},\, v \in I_j)$ in $\mathbb{P}^n(\overline{k(\varepsilon)})$. Then, cf., e.g., [3], W_j, $j \in J_{s,i}$, is the family of defined over $k(\varepsilon)$ and irreducible over $k(\varepsilon)$ components of dimension 1 of $V_s \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})$. Further, μ_j is the number of defined over $\overline{k}(\varepsilon)$ and irreducible over $\overline{k}(\varepsilon)$ components of W_j, $j \in J_{s,i}$. Notice also that if $W_{s,i} = W_j$ in (9) then μ_j is the number of irreducible over $\overline{k}$ component of W. One sees that $\mathrm{st}_\varepsilon(W_j) = \mathcal{Z}(\varphi_{j,v}|_{\varepsilon=0},\ v \in I_j)$, $j \in J_{s,i}$. Let us construct for every $2 \le i \le u$ the subset $J''_{s,i} \subset J_{s,i}$ of all j such that $(\varphi_{j,v}|_{\varepsilon=0})(z_\alpha) = 0$ for all $v \in I_j$, $\alpha = 1, i$.

Denote by W_j, $j \in J_s$ the family of defined over k components of dimension $n-s$ of V. Let $W = W_j$ in (9). Then $W_{s,i} = W_{j_1}$ for the uniquely defined $j_1 \in J_{s,i}$. Denote $j_1 = \gamma_{s,i}(j)$. Hence $\gamma_{s,i} : J_s \to J_{s,i}$ are bijections for all $2 \le i \le u$. Let us identify $J_s = J_{s,2}$, i.e., we suppose that $\gamma_{s,2}$ is the identity mapping. Now we are going to construct all $\gamma_{s,i}$, $2 \le i \le u$. If $s = n-1$ then $J_s = J_{s,i}$ and $\gamma_{s,i}$ is an identity mapping for every $2 \le i \le u$.

Let $s \le n-2$. Set $i_2 = 2$. For all $3 \le i_1 \le u$ and $\nu = 1, 2$ we construct linearly independent linear forms $L''_{i_1,i}$, $s+1 \le i \le n-2$, and a linear form $L'''_{i_1,\nu}$ with coefficients from $k(\varepsilon)$ of lengths polynomial in n and $L(z_1)$, $L(z_2)$, $L(z_{i_1})$ such that

$$\begin{array}{l} \mathcal{Z}(L''_{i_1,i},\ s+1 \le i \le n-2) \supset \mathcal{Z}(L'_{i_\nu,i},\ s+1 \le i \le n-1),\ \nu = 1,2 \\ \mathcal{Z}(L''_{i_1,i},\ s+1 \le i \le n-2) \cap \mathcal{Z}(L'''_{i_1,\nu}) = \mathcal{Z}(L'_{i_\nu,i},\ s+1 \le i \le n-1),\ \nu = 1,2. \end{array} \tag{10}$$

Denote by V'_{s,i_1} the union of all irreducible over $k(\varepsilon)$ components W' of dimension 2 of $V \cap \mathcal{Z}(L''_{i_1,i},\ s+1 \le i \le n-2)$. By (*) and (10) the algebraic variety V'_{s,i_1} is the union of all irreducible over $k(\varepsilon)$ components W' of dimension 2 of $V_s \cap \mathcal{Z}(L''_{i_1,i},\ s+1 \le i \le n-2)$. The intersection $V \cap \mathcal{Z}(L'_{2,s+1}, \dots, L'_{2,n-1})$ is transversal at each curve and (9) is a bijection for $i = 2$. Hence the inclusion of (10) with $\nu = 2$ implies that the irreducible over k components of V_s and irreducible over $k(\varepsilon)$ components of V'_{s,i_1} are in the one–to–one correspondence by the rule

$$W \mapsto W \cap \mathcal{Z}(L''_{i_1,i},\ s+1 \le i \le n-2) = W'_{s,i_1}, \tag{11}$$

and $W'_{s,i_1} \cap \mathcal{Z}(L'''_{i_1,\nu}) = W_{s,i_\nu}$, $\nu = 1,2$. Using the algorithm of [3] we construct all the defined over $k(\varepsilon)$ and irreducible over $k(\varepsilon)$ components of V'_{s,i_1}. Denote by W'_j, $j \in J'_{s,i_1}$ the family of obtained components. More precisely, for every $j \in J'_{s,i_1}$ the algorithm construct a family of polynomials $\varphi_{j,v} \in k(\varepsilon)[X_0, \dots, X_n]$, $v \in I_j$ such that $W'_j = \mathcal{Z}(\varphi_{j,v},\ v \in I_j)$. For every $j \in J'_{s,i_1}$ the intersection $\mathcal{Z}(\varphi_{j,v},\ v \in I_j) \cap \mathcal{Z}(L'''_{i_1,\nu}) = \mathcal{Z}(\varphi_{j_\nu,i},\ i \in I_{j_\nu})$ for the uniquely defined $j_\nu \in J_{s,i_\nu}$ for $\nu = 1,2$. Using the algorithm from [3] we construct these j_1, j_2. Now one sees that $(\gamma_{s,i_1} \circ \gamma_{s,2}^{-1})(j_2) = j_1$. Thus, we can construct all $\gamma_{s,i}$, $2 \le i \le u$.

Finally, for every $1 \le s \le n-1$ we compute the intersection $\bigcap_{2 \le i \le u} \gamma_{s,i}^{-1}(J''_{s,i}) = J''_s$. According to our construction the number of irreducible over $\overline{k}$ components of V of dimension $n-s$ containing $z_1, \dots, z_u$ is $\sum_{j \in J''_s} \mu_j$ (recall $J''_s \subset J_s = J_{2,s}$) for every $1 \le s \le n-1$. The algorithm for the assertion (b) is described. The required estimation for the working time of this algorithm follows immediately from ones of the applied algorithms. The assertion (b) of Theorem 2 is proved.

To prove (a) we construct the finite sets $V_{s,0}$ from Theorem 1 and all its defined over k and irreducible over k components a_j, $j \in J_s$. Hence defined over k and irreducible over k components of V_s and $V_{s,0}$ are in the one–to–one by the rule $W \mapsto W \cap V_{s,0}$. Let $z^{(j)} \in a_j$ and $W \cap V_{s,0} = a_j$. Denote $W_j = W$. We introduce the representation for $z^{(j)}$, $j \in J_s$ replacing in (1) z, η, F_z by $z^{(j)}, \eta^{(j)}, F_{z^{(j)}}$. The field $k(z^{(j)}) \simeq k[\eta^{(j)}]$. Using the algorithm from [3] we construct for every $1 \leq i \leq u$, $j \in J_s$ all pairwise non–isomorphic composites $k_{j,w}$, $w \in I_{j,i}$, of the fields $k[\eta_i]$ and $k[\eta^{(j)}]$ over k. Now $z_i \in W_j$ if and only if there is $w \in I_{j,i}$ such that the points z_i and $z^{(j)}$ with the field $k[\eta_i, \eta^{(j)}] \simeq k_{j,w}$ belong to the same irreducible over $\overline{k}$ component of V_s (which is contained in W_j). Using the described algorithm for the assertion (b) one can decide whether there is $w \in I_{j,i}$ satisfying the formulated condition and, therefore, construct the algorithm for (a). The required estimation for the working time of this algorithm follows immediately from ones of the applied algorithms. The theorem is proved.

References

[1] **Baldassarry M.:** *"Algebraic varieties"*, Springer–Verlag, Berlin–Göttingen–Heidelberg, 1956.

[2] **Chebotarev N. G.:** *"Theorie of algebraic functions"*, OGIZ, Moscow, Leningrad 1948 (in Russian).

[3] **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, (4), (1986) p. 1838–1882].

[4] **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)[2].

[5] **Chistov A. L.:** *"Polynomial–time computation of the Galois group over a zero–characteristic functional field with algebraically closed constant field"*, In "Mathematical methods of constructing and analysis of algorithms", Leningrad, "Nauka", 1990, p. 200–232 (in Russian).

[6] **Chistov A. L.:** *"Efficient Smooth Stratification of an Algebraic Variety in Zero–Characteristic and its Applications"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 266 (2000) p.254–311 (in Russian).

[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).

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

[9] **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.

[10] **Jordan C.:** *"Traité des substitutions et des équations algébriques"*, Paris 1870.

[2]Preliminary versions of [4], [7] and [6] in English can be found as Preprints (1999) of St.Petersburg Mathematical Society, http://www.MathSoc.spb.ru