Polynomial–Time Computation of the Dimension of Affine Algebraic Varieties in Zero–Characteristic

Alexander L. Chistov*

St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia

and

Department of Computer Science
University of Bonn

March, 1994

Introduction

In the paper an algorithm is described for the computation of the dimension of an affine algebraic variety over a zero characteristic ground field. The variety is given as a set of zeros of a family of polynomials of the degree less than d in n variables. The working time of the algorithm is polynomial in the size of input and d^n. This paper continues [3] where the case of projective varieties was considered by the autor. The problem of the computation of the dimension has attracted the attention of specialists for approximately ten years. In [4] an algorithm is suggested for decomposing an algebraic variety into the irreducible components with the complexity polynomial in d^{n^2}. This algorithm has the best known bound for the complexity of the computation of the dimension in the case of arbitrary characteristic. In [7] a well parallelizable arithmetical network is constructed for the computation of the dimension in non–uniform polynomial sequential time in the size of input and d^n. In [7] the problem also is stated to find an algorithm with a bitwise complexity $d^{\mathcal{O}(n)}$. The result of the present paper solves this problem for varieties over fields of zero characteristic. In the case of non–zero characteristic the problem is still open.

The case of projective varieties can be easily reduced to the affine one. So the result of the present paper is also the generalisation of [3]. Although the affine case

*Research partially supported by the Volkswagen–Stiftung, Program on Computational Complexity, University of Bonn

is more difficult the technics required is developed in [3]. Namely, the results of real algebraic geometry are essentually used. We consider an algebraically closed field of zero characteristic as the extension of degree 2 of a real ordered field. The required property can be formulated over this real ordered field. After that we can apply the "tranfer principle", see [1], and reduce everything to the case of the field of real numbers. For this field we have the developed theory. The result from [11] is crucial which in its turn is based on the result of [10], see below section 2.

Note that the probabilistic algorithm for the computation of the dimension is simple in every characteristic. For every s one takes in random an hyperplane H_s of the dimension s, adds to the initial family of polynomials linear ones which determine H_s and finds whether the set of zeros of this new family is finite. This can be done in time polynomial in d^n. The dimension will be equal to $n - s_1$ where s_1 is the maximal s for which this set of zeros is finite.

Now we give the precise statements. Let $k = \mathbb{Q}(t_1, \ldots, t_l, \theta)$ be the field 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. Let polynomials $f_0, \ldots, f_m \in k[X_1, \ldots, X_n]$ be given. Consider the closed algebraic set or which is the same in this paper the algebraic variety

$$V = \{(x_1, \ldots, x_n) : \ f_i(x_1, \ldots, x_n) = 0 \ \forall 0 \leq i \leq m\} \subset \mathbb{A}^n(\bar{k}) .$$

This is a set of all common zeros of polynomials $f_0, \ldots, f_m$ in $\mathbb{A}^n(\bar{k})$, where $\bar{k}$ is an algebraic closure of k. The dimension $\dim V$ of V is defined to be the maximum of dimensions of all irreducible components of V.

We shall represent each polynomial $f = f_i$ in the form

$$f = \frac{1}{a_0} \sum_{i_0, \ldots, i_n} \sum_{0 \leq j < deg F} a_{i_1, \ldots, i_n, j} \theta^j X_0^{i_0} \cdots X_n^{i_n} ,$$

where $a_0, a_{i_1,\ldots,i_n,j} \in \mathbb{Z}[t_1, \ldots, t_l]$, $\gcd_{i_1,\ldots,i_n,j}(a_0, a_{i_1,\ldots,i_n,j}) = 1$. 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 length of coefficients from $\mathbb{Z}$ of polynomials $a_0, a_{i_1,\ldots,i_n,j}$ and the degree

$$\deg_{t_\alpha}(f) = \max_{i_1,\ldots,i_n,j} \{\deg_{t_\alpha}(a_0), \deg_{t_\alpha}(a_{i_1,\ldots,i_n,j})\} ,$$

where $1 \leq \alpha \leq l$. In the similar way $\deg_{t_\alpha} F$ and $l(F)$ are defined.

We shall suppose that we have the following bounds

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

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 $L(F) < d_1^{l+1} M_1$. Below if there is no special mention about it we set l to be fix.

THEOREM 1. The dimension $dimV$ of the variety V of common zeros of polynomials $f_0, \ldots, f_m$ in the projective space $\mathbb{A}^n(\bar{k})$ over $\bar{k}$ can be computed within the time polynomial in d^n, d_1, d_2, M, M_1.

REMARK 1. The working time of the algorithm from the theorem is essentialy the same as by solving system of polynomial equations with a finite set of solutions in projective space. So it can be formulated also in the case when l is not fixed, see [4].

1 Preliminary results

In [3] we developed the tecnics for constructing a real structure on the constant field. Namely, let l is not fixed now. Let $k_1 = \mathbb{Q}(t_1, \ldots, t_l)[\eta]$ be some algebraic extension of k, where the element η has minimal polynomial $\varphi \in \mathbb{Q}[t_1, \ldots, t_l, Z]$, $\mathrm{lc}_Z \varphi = 1$, $l(\varphi) < M_2$ and $\deg_{t_\alpha} \varphi$, $\deg_Z \varphi < D_1$ for all α. Our aim is to construct a real structure on k_1.

The real structure of k_1 is defined to be an embedding $k_1 \subset k_2(\sqrt{-1})$, where k_2 is a real ordered field, see [1].

Compute the discriminant

$$0 \neq \Delta = \mathrm{Res}_Z(\varphi, \varphi'_Z) \in \mathbb{Q}[t_1, \ldots, t_l].$$

Choose $z_1, \ldots, z_l \in \mathbb{Q}$ such that $\Delta(t_1, \ldots, t_l) \neq 0$. The polynomial

$\overline{\varphi} = \varphi(z_1, \ldots, z_l, Z) \in \mathbb{Q}[Z]$ is separable, since $\Delta(z_1, \ldots, z_l) \neq 0$.

Let $\overline{\varphi} \in \mathbb{Q}[Z]$ and $\overline{\eta}$ be an arbitrary root of $\overline{\varphi}$. We constructed in [3]

(i) an irreducible polynomial $\overline{\Psi} \in \mathbb{Q}[Z], \mathrm{lc}_Z \overline{\Psi} = 1$, which has a real root $\overline{\xi}$,

(ii) polynomials $R_1, I_1 \in \mathbb{Q}[Z]$ with $\deg_Z R_1, \deg_Z I_1 < \deg_Z \overline{\Psi}$, such that for a chosen root $\overline{\eta}$ of $\overline{\varphi}$ we have $\overline{\eta} = R_1(\overline{\xi}) + \sqrt{-1}\, I_1(\overline{\xi})$ in the field $\mathbb{Q}[\overline{\xi}, \sqrt{-1}]$.

Besides that, $\overline{\xi} = \overline{\eta}$ if $\overline{\eta}$ is real and $\mathbb{Q}[\overline{\xi}, \sqrt{-1}] = \mathbb{Q}[\overline{\eta}, \overline{\eta}_1]$ where $\overline{\eta}_1$ is conjugated to $\overline{\eta}$ if $\overline{\eta}$ is not real.

More precisely, let $\overline{\varphi}_1 = \overline{\varphi}/(Z - \overline{\eta}) \in \mathbb{Q}[\overline{\eta}][Z]$ and

$$\overline{A} = \mathbb{Q}[\overline{\eta}, \overline{\eta}_1 \sqrt{-1}] = \mathbb{Q}[\overline{\eta}][Z, Z_1]/(\overline{\varphi}_1, Z_1^2 + 1)$$

be a separable $\mathbb{Q}$–algebra, where

$$\overline{\eta}_1 = Z \bmod (\overline{\varphi}_1, Z_1^2 + 1), \ \sqrt{-1} = Z_1 \bmod (\overline{\varphi}_1, Z_1^2 + 1).$$

Let $\overline{v}_1 = \frac{1}{2}(\overline{\eta} + \overline{\eta}_1)$, $\overline{v}_2 = \frac{1}{2\sqrt{-1}}(\overline{\eta} - \overline{\eta}_1)$; $\overline{v}_1, \overline{v}_2 \in \overline{A}$. Construct an element $\overline{v} = \overline{v}_1 + c\overline{v}_2$ which is a primitive element of the separable algebra $\mathbb{Q}[\overline{v}_1, \overline{v}_2]$ over $\mathbb{Q}$. One can find the minimal integer c such that $1 \le c \le 2D_1^2$. Find the minimal polynomial $\overline{\Phi} \in \mathbb{Q}[Z]$, $\mathrm{lc}_Z \overline{\Phi} = 1$, of the element $\overline{v}$ over $\mathbb{Q}$ and polynomials $R_2, I_2 \in \mathbb{Q}[Z]$; $\deg R_2, \deg I_2 < \deg \overline{\Phi}$, such that $R_2(\overline{v}) = \overline{v}_1$, $I_2(\overline{v}) = \overline{v}_2$.

Factor $\overline{\Phi} = \prod_j \overline{\Phi}_j$ into the product of ireducible polynomials $\overline{\Phi}_j \in \mathbb{Q}[Z], \mathrm{lc}_Z \overline{\Phi}_j = 1$. Set $\mathbb{Q}[\overline{\xi}_j, \sqrt{-1}] = \mathbb{Q}[Z, Z_1]/(\overline{\Phi}_j, Z_1^2 + 1)$, where $\overline{\xi}_j = Z \bmod (\overline{\Phi}_j, Z_1^2 + 1)$, $\sqrt{-1} = Z_1 \bmod (\overline{\Phi}_j, Z_1^2 + 1)$. Find γ such that $\overline{\Phi}_\gamma$ has a real root $\overline{\xi}_\gamma$ for which $R_2(\overline{\xi}_\gamma) + \sqrt{-1}\, I_2(\overline{\xi}_\gamma) = \overline{\eta}$. The existence of γ follows immediately from the construction and the fact that $\overline{\eta}$ is not a real root of $\overline{\varphi}$. Finilly, set $\overline{\Psi} = \overline{\Phi}_\gamma$, $\overline{\xi} = \overline{\xi}_\gamma$ and R_1, I_1 to be the residues from the division of R_2 and I_2 by $\overline{\Phi}_\gamma$.

In the case when $\overline{\eta}$ is real take $\overline{\xi} = \overline{\eta}$, $\overline{\Psi} = \overline{\varphi}$, $R_1 = Z$, $I_1 = 0$. So in any case we can construct $\overline{\xi}$, $\overline{\Psi}$, R_1, I_1 for which (i) and (ii) hold.

Denote $u_i = t_i - z_i$, $1 \le i \le l$. By Hensel's lemma the element η can be represented as a series

$$\eta = \eta_0 + \sum_{(i_1, \dots, i_l) > (0, \dots, 0)} \eta_{i_1, \dots, i_l} u_1^{i_1} \cdots u_l^{i_l} \in \mathbb{Q}[\overline{\eta}][[u_1, \dots, u_l]],$$

where $\eta_0 = \overline{\eta}$, $\eta_{i_1, \dots, i_l} \in \mathbb{Q}[\overline{\eta}] \subset \mathbb{Q}[\overline{\xi}, \sqrt{-1}]$. Therefore, $\eta_0 = \eta_0^{(1)} + \sqrt{-1}\, \eta_0^{(2)}$, $\eta_{i_1, \dots, i_l} = \eta^{(1)}_{i_1, \dots, i_l} + \sqrt{-1}\, \eta^{(2)}_{i_1, \dots, i_l}$, where $\eta_0^{(1)}, \eta_0^{(2)}, \eta^{(1)}_{i_1, \dots, i_l}, \eta^{(2)}_{i_1, \dots, i_l} \in \mathbb{Q}[\overline{\xi}]$.

Define elements

$$\begin{aligned} \eta^{(1)} &= \eta_0^{(1)} + \sum_{(i_1, \dots, i_l) > (0, \dots, 0)} \eta^{(1)}_{i_1, \dots, i_l} u_1^{i_1} \cdots u_l^{i_l}, \\ \eta^{(2)} &= \eta_0^{(2)} + \sum_{(i_1, \dots, i_l) > (0, \dots, 0)} \eta^{(2)}_{i_1, \dots, i_l} u_1^{i_1} \cdots u_l^{i_l}. \end{aligned}$$

Suppose that $\overline{\eta}$ is not real. Then we have $\eta = \eta^{(1)} + \sqrt{-1}\, \eta^{(2)}$. The element $\tilde{\eta} = \eta^{(1)} - \sqrt{-1}\, \eta^{(2)}$ is a root of the polynomial $\varphi_1 = \varphi/(Z - \eta) \in \mathbb{Q}[\eta][Z] \subset \mathbb{Q}[\overline{\xi}, \sqrt{-1}][[u_1, \dots, u_l]][Z]$, since $\varphi \in \mathbb{Q}[t_1, \dots, t_l, Z]$.

Set $\xi = \eta^{(1)} + c\eta^{(2)}$ where c is the same as for $v = v_1 + cv_2$, see above. We constructed in [3] the minimal polynomial $\Psi \in \mathbb{Q}[t_1, \dots, t_l, Z]$ of the element ξ and found $R, I \in \mathbb{Q}(t_1, \dots, t_l)[Z]$, $\deg_Z R, \deg_Z I < \deg_Z \Psi$, such that $\eta^{(1)} = R(\xi)$, $\eta^{(2)} = I(\xi)$. So $\eta = R(\xi) + \sqrt{-1}\, I(\xi)$. Besides that, the polynomial $\Psi(z_1, \dots, z_l, Z)$ is separable and divides $\overline{\Phi}$. So by Hensel's lemma the element ξ can be represented as a series

$$\xi = \xi_0 + \sum_{(i_1, \dots, i_l) > (0, \dots, 0)} \xi_{i_1, \dots, i_l} u_1^{i_1} \cdots u_l^{i_l}, \tag{1}$$

where $\xi_0 = \overline{\xi}$, $\xi_{i_1, \dots, i_l} \in \mathbb{Q}[\overline{\xi}]$. From (1) and the equalities $\eta = \eta^{(1)} + \sqrt{-1}\, \eta^{(2)} = R(\xi) + \sqrt{-1}\, I(\xi)$ we infer that

$$\eta^{(1)} = R(\xi), \eta^{(2)} = I(\xi).$$

If $\overline{\eta}$ is real set $\Psi = \varphi$, $\xi = \eta = \eta^{(1)}$, $\eta^{(2)} = 0$, $R = Z$, $I = 0$ and all the formulated above statements are satisfied.

Now define an order of a real field on the field $k_2 = \mathbb{Q}(t_1, \dots, t_l)[\xi]$. Consider the embedding $k_2 \subset \mathbb{Q}[\overline{\xi}]((u_1, \dots, u_l)) = k_3$ which is determined by (1). The order on k_2 will be induced by the order on the field of formal power series $\mathbb{Q}[\overline{\xi}]((u_1, \dots u_l))$ or equivalently on the ring of formal power series $\mathbb{Q}[\overline{\xi}][[u_1, \dots, u_l]]$. The monomials $u^{i_1} \cdots u_l^{i_l}$ in the field k_3 are linearly ordered in the following way: $u_1^{i_1} \cdots u_l^{i_l} > u_1^{j_1} \cdots u_l^{j_l}$ iff there exists w such that $i_1 = j_1, \dots, i_{w-1} = j_{w-1}$ and $i_w < j_w$. An element $\alpha \in \mathbb{Q}[\overline{\xi}][[u_1, \dots, u_l]]$ is positive iff the coefficient from $\mathbb{Q}[\overline{\xi}]$ in the maximal monomial of α with a non–zero coefficient is positive. The order on $\mathbb{Q}[\overline{\xi}] \subset \mathbb{R}$ is induced by the order in $\mathbb{R}$. This order on k_3 is an order of a real field, see [2].

We have [3] the following lemmas.

LEMMA 1. For the field k_1 an embedding of fields over $\mathbb{Q}(t_1, \dots, t_l)$ can be constructed

$$k_1 = \mathbb{Q}(t_1, \dots, t_l)[\eta] \subset \mathbb{Q}(t_1, \dots, t_l)[\xi, \sqrt{-1}\,],$$

where ξ is an algebraic element over $\mathbb{Q}(t_1, \dots, t_l)$ with minimal polynomial $\Psi \in \mathbb{Q}[t_1, \dots, t_l, Z]$, $\mathrm{lc}_Z \Psi = 1$ and

$$\eta = R(\xi) + \sqrt{-1}\, I(\xi)$$

with $R(Z), I(Z) \in \frac{1}{\Delta_2}\mathbb{Q}[t_1, \dots, t_l][Z]$, $\Delta_2 = \mathrm{Res}_Z(\Psi, \Psi'_Z)$ is the discriminant of Ψ; $\deg_Z R, \deg_Z I < \deg_Z \Psi \le D_1^2$; $\deg_{t_\alpha} \Psi, \deg_{t_\alpha} R, \deg_{t_\alpha} I \le \mathcal{P}(D_1)$; $l(\Psi), l(R), l(I) < (M_2 + l)\mathcal{P}(D_1)$ for some polynomial $\mathcal{P}$ and all α. For $\mathbb{Q}(t_1, \dots, t_l)[\xi]$ the order of a real ordered field is constructed. The working time of constructing Ψ, R, I and the order on $\mathbb{Q}(t_1, \dots, t_l)[\xi]$ is polynomial in D_1^l and M_2.

LEMMA 2. Let $\omega \in \mathbb{Q}(t_1, \dots, t_l)[\xi]$, $\omega = \frac{1}{c}\sum_{0 \le j \le \deg \Psi} c_j \xi^j$, where $c, c_j \in \mathbb{Z}[t_1, \dots, t_l]$, $\deg_{t_\alpha} c, \deg_{t_\alpha} c_j < D$, $l(c), l(c_j) < M_3$ for all α, j. Then one can ascertain whether $\omega > 0$ within time polynomial in D_1^l, D^l, M_2, M_3.

LEMMA 3. There exists a polynomial $\mathcal{P}$ such that changing in the construction described elements z_i for arbitrary elements $z_i^* \in \mathbb{Q}$ with $|z_i - z_i^*| < 2^{-\mathcal{P}(D_1)(M_2+l)}$, $1 \le i \le l$, we can choose $\overline{\eta}^*$ instead of $\overline{\eta}$ so that we get ξ^* instead of ξ such that $R^* = R, I^* = I, \Psi^* = \Psi$.

Remind that the field $\mathbb{Q}(t_1, \dots, t_l)$ has the order induced by the linear order on monomials $u_1^{j_1} \dots u_l^{j_l}$ described above. Denote by $\mathbb{Q}(\widetilde{t_1, \dots}, t_l)$ the real closure of the field $\mathbb{Q}(t_1, \dots, t_l)$ with this fixed order.

LEMMA 4. The construction of this section gives all the possible real structures of the field $\mathbb{Q}(t_1, \dots, t_l)[\eta]$ when $\mathbb{Q}(t_1, \dots, t_l)$ is the real ordered field with the fixed order decribed above. More exactly, for every embedding β : $\mathbb{Q}(t_1, \dots, t_l)[\eta] \to \mathbb{Q}(\widetilde{t_1, \dots}, t_l)[\sqrt{-1}\,]$ there exist an embedding

$$\beta_1 : \mathbb{Q}(t_1, \dots, t_l)[\eta] \to \mathbb{Q}(t_1, \dots, t_l)[\xi, \sqrt{-1}\,]$$

from Lemma 1 and an embedding

$$\beta_2 : \mathbb{Q}(t_1, \dots, t_l)[\xi] \to \mathbb{Q}(\widetilde{t_1, \dots}, t_l)$$

of real ordered fields which induces the embedding

$$\beta_2' : \mathbb{Q}(t_1, \dots, t_l)[\xi, \sqrt{-1}\,] \to \mathbb{Q}(\widetilde{t_1, \dots}, t_l)[\sqrt{-1}\,]$$

such that $\beta = \beta_2' \circ \beta_1$ (all embeddings over $\mathbb{Q}(t_1, \dots, t_l)$).

Now let $K = \mathbb{Q}(t_1, \dots, t_l)[\xi]$ be real ordered field and $\varepsilon_1 > \varepsilon_2 > \varepsilon_3 > \varepsilon_4 > 0$ be infinitely small values ralatively to the field K such that ε_2 is an infinitely small value ralatively to the field $K(\varepsilon_1)$, ε_3 is an infinitely small value ralatively to the field $K(\varepsilon_1, \varepsilon_2)$ and ε_4 is an infinitely small value ralatively to the field $K(\varepsilon_1, \varepsilon_2, \varepsilon_3)$. Set $K_1 = K(\varepsilon_1, \varepsilon_2, \varepsilon_4)$. Denote by $\tilde{K}_1$ the real closure of the field K_1, see [1]. So $\overline{K}_1 = \tilde{K}_1(\sqrt{-1}\,)$ for the algebraic closure $\overline{K}_1$ of the field K_1.

If $\delta = \delta_1 + \sqrt{-1}\delta_2 \in \overline{K_1}\,; \delta_1, \delta_2 \in \tilde{K}_1$ define $|\delta| = \sqrt{\delta_1^2 + \delta_2^2} \in \tilde{K}_1$. We define the element $\delta \in \overline{K_1}$ to be infinitely small (respectively infinitely great) relatively to the field $\tilde{K}$ if $|\delta|^2 \in \tilde{K}_1$ is infinitely small (respectively infinitely great) relatively to the real closure $\tilde{K}$ of the field K.

Let $g_1, \dots, g_s \in K_1(\sqrt{-1}\,)[X_0, \dots, X_n\,]$ and $x_i = y_i + \sqrt{-1}z_i \in K_1(\sqrt{-1}\,)$, $y_i, z_i \in K_1$, $i = 1, \dots, n$. Consider the system of equations and an inequality

$$g_1 = g_2 = \ldots = g_s = 0, \sum_{0 \le i \le n} |X_i - x_i|^2 \le \varepsilon_3 \tag{2}$$

with coefficients from the field $K_1(\sqrt{-1}\,)$.

We have the following result similar to that which was proved in sections 2 and 3 of [3].

THEOREM 2. One can construct a new order of the real field on K which induces the new real structure on $K_1(\sqrt{-1}\,)$ and $\overline{K_1}$ and find a solution $x^* = (x_0^*, \dots, x_n^*) \in \mathbb{A}^{n+1}(\overline{K_1})$ of system (2) relatively to this real structure of $K_1(\sqrt{-1}\,)$ or ascertain that system (2) has no solutions in $\mathbb{A}^{n+1}(\overline{K_1})$. More precisely, one can construct an irreducible over K_1 polynomial $P_{\alpha,\beta} \in K_1[\,Z\,]$ (in the denotations of [3] section 3) which has the root $\eta_{\alpha,\beta}$ and elements $x_{0,\alpha,\beta}^* \dots, x_{n,\alpha,\beta}^* \in K_1[\eta_{\alpha,\beta}, \sqrt{-1}\,]$ such that the solution x^* is given by the isomorphism over the field K_1

$$\overline{K_1} \supset K_1\,[x_0^*, \dots, x_n^*\,]$$

$$\simeq K_1\,[x_{0,\alpha,\beta}, \dots, x_{n,\alpha,\beta}\,] = K_1\,[\eta_{\alpha,\beta}, \sqrt{-1}] \tag{3}$$

under which $x_i^* \longmapsto x_{i,\alpha,\beta}$ for all i. The working time of this algorithm is polynomial in the time which is required for solving systems of polynomial equations with finite number of solutions in $\mathbb{P}^n$ with the same size of input as system (2) has. Similarly the estimations for degrees and sizes of coefficients of $x_{0,\alpha,\beta}$, $P_{\alpha,\beta}$ are analogous to ones for output of the algorithm for solving systems of polynomial equations with finite number of solutions in $\mathbb{P}^n$ with the same size of input as system (2) has.

In [3] in section 3 the similar result was proved for the system

$$h_1 = \ldots = h_s = h - \varepsilon_2 L_0^{d-1} = 0, \sum_{1 \le i \le n} |X_i - x_{j,i}|^2 \le \varepsilon_1 \qquad (4)$$

Here there are only two infinitely small values ε_1 and ε_2 and system has the special form in $\mathbb{P}^n$. But the proof of Theorem 1 remains just the same as it was in [3] in section 3. It is based on the result from [11] which reduces the initial system to the case of systems of polynomial equations with finite number of solutions in $\mathbb{P}^n$ when systems are considered over $\mathbb{R}$. In the general case we apply the "transfer principle" and the Newton polygons method, see sections 2 and 3 of [3]. The required estimations of coefficients in the Newton polygons method when one consider in the proof fraction–power series in ε_i are obtained in [5], see also [6]. The algorithm for solving systems of polynomial equations with finite number of solutions in $\mathbb{P}^n$ is described in [4], see also [9].

REMARK 2. We change the real structure in section 3 of [3] to avoid considering arbitrary multiple–fractional series in $t_1, \ldots, t_l$. We use only simple Hensel's lemma for constructing real structures in section 1 of [3]. If one get appropriate estimations for coefficients of arbitrary multiple–fractional series similar to the estimations which were obtained in [5] for the Newton polygons method then one will not need to change the real structure. The required estimations for coefficients of arbitrary multiple–fractional series can be obtained but it is a quite different subject.

REMARK 3. Note that if $g_1, \ldots, g_s \in K(\varepsilon_4)(\sqrt{-1})[X_0, \ldots, X_n]$ and $x_i \in K(\varepsilon_4)(\sqrt{-1})$, $i = 1, \ldots, n$, then $K_3 \subset \overline{K(\varepsilon_3, \varepsilon_4)}$ and $P_{\alpha,\beta} \in K(\varepsilon_3, \varepsilon_4)[Z]$.

2 Description of the algorithm for the computation of the dimension in the affine space

(1) Denote by $g_i \in K[X_0, \ldots, X_n]$ the homogenization of f_i, i.e.

$$g_i = X_0^{\deg f_i} f_i(X_1/X_0, \ldots, X_n/X_0)$$

for $0 \le i \le m$. We shall suppose without loss of generality that $\deg(g_i) = \deg_{X_0, \ldots, X_n}(g_i) = d - 1$. If it is not so, we can change each g_i for the family $\{f_i X_j^{-\deg(g_i)+d-1}\}_{0 \le j \le n}$.

Using induction by $s \ge 1$ we shall construct polynomials $h_1, \ldots, h_s$ and linear forms $L_{s+1}^{(s)}, \ldots, L_n^{(s)}$ in $X_0, \ldots, X_n$ with integer coefficients of the size $O(n\log d)$ such that

$$h_i = \sum_{0 \le j \le m} \lambda_{i,j} g_j, \ \lambda_{i,j} \in \mathbb{Z}$$

for all i, j. Besides that, the following property will be fulfilled. Let

$$W = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^n(\overline{k})$$

be the variety of all common zeros of polynomials $h_1, \dots, h_s$ in $\mathbb{P}^n(\overline{k})$ and W' be the union of all the components W_1 of W such that $W_1 \cap \mathbb{A}^n(\overline{k}) \neq \emptyset$. Then

$$W' \cap \{L_{s+1}^{(s)} = \dots = L_n^{(s)} = 0\} \cap \{X_0 = 0\} = \emptyset,$$

In particular each component W_1 of W has the dimension equal to $n-s$ in this case.

(2) The construction for the base $s=0$ is easy. One can take $L_i^{(0)} = X_i$, $i \geq 1$.

(3) Now let $n > s \geq 0$ and suppose that $h_1, \dots, h_s, L_{s+1}^{(s)}, \dots, L_n^{(s)}$ are constructed. Denote for brevity $L_j^{(s)} = L_j$, $s+1 \leq j \leq n$. Using the algorithm from [4], see also [9], we shall find all the points $\{x_j\}_{1 \leq j \leq N}$ of the set

$$V_s = W \cap \mathbb{A}^n(\overline{k}) \cap \{L_{s+1} = \dots = L_n = 0\} = W' \cap \{L_{s+1} = \dots = L_n = 0\}$$

. Find a linear form L_0 with integer coefficients, such that $L_0(x_j) \neq 0$ for all $1 \leq j \leq N$.

(4) Consider $x_j = (x_{j,0} : \dots : x_{j,n}) \in \mathbb{P}^n(\overline{k})$. Remind that in output of the algorithm from [4] for every j we have an isomorphism of fields over k

$$k\left(\frac{x_{j,0}}{x_{j,\alpha}}, \dots, \frac{x_{j,n}}{x_{j,\alpha}}\right) \simeq k[\tau_j],$$

where $\varphi_j(\tau_j) = 0$, $\varphi_j \in k[Z]$ is an irreducible polynomial, $x_{j,\alpha} \neq 0$. Construct for every j a primitive element $\eta_j = \theta + c\tau_j$ of the field $k(\tau_j)$ over $\mathbb{Q}(t_1, \dots, t_l)$, $c \in \mathbb{Z}$, with minimal polynomial $\Phi_j \in \mathbb{Q}[t_1, \dots, t_l, Z]$ over $\mathbb{Q}(t_1, \dots, t_l)$. We can suppose that $lc_Z \Phi_j = 1$ changing if it is not so, η_j for $(lc_Z \Phi_j)\eta_j$. Since $x_j \in \mathbb{A}^n(\overline{k}) \subset \mathbb{P}^n(\overline{k})$ we can set $\alpha = 0$ and $x_{j,0} = 1$. Denote $\overline{x_j} = (x_{j,0}, \dots, x_{j,n}) \in \mathbb{A}^{n+1}(\overline{k})$.

(5) Consider the set of polynomials $\{\sum_{0 \leq i \leq m} c^i g_i : 1 \leq c \leq m(d-1)^s + 1, c \in \mathbb{Z}\} = H$. We shall enumerate the elements of H. Let $h \in H$.

(6) Find all j for which $h(x_j) = 0$. Let, say, $h(x_j) = 0$ when $1 \leq j \leq N'$, and $h(x_j) \neq 0$ when $N' < j \leq N$. If $N' = 0$ then we set $h_{s+1} = h$, $L_{s+1+i}^{(s+1)} = L_{s+1+i}$ for every $i \geq 1$ and go to the step $s+1$. If $N' > 0$ we shall enumerate all the points x_j, $1 \leq j \leq N'$.

(7) For the considered $1 \leq j \leq N'$ construct for the field $\mathbb{Q}(t_1, \dots, t_l)[\eta_j]$ a real structure by section 1, i.e. construct ξ_j, Ψ_j, R_j, I_j for η_j analogous to ξ, Ψ, R, I for η.

(8) Let ε_1 and ε_2 be algebraically independent infinitely small values for the field $K = \mathbb{Q}(t_1, \dots, t_l)[\xi_j]$, $0 < \varepsilon_2 < \varepsilon_1$, and ε_2 is infinitely small value relatively to the field $K(\varepsilon_1)$. The field $K_1 = K(\varepsilon_1, \varepsilon_2)$ is a real ordered field.

Let $\overline{x}_j = (x_{j,0}, \dots, x_{j,n}) \in \mathbb{A}^{n+1}(\overline{k})$ with $x_{j,0} = 1$ in accordance with paragraph (4). Consider the system of equations with coefficients from the field $K_1(\sqrt{-1})$

$$h_1 = \dots = h_s = h - \varepsilon_2 L_0^d = 0, \quad \sum_{0 \leq i \leq n} |X_i - x_{j,i}|^2 \leq \varepsilon_1 \qquad (5)$$

(9) Apply Theorem 2 to system (5) (here there are only two infinitely small values ε_1, and ε_2). We construct a new order of the real field on K which induces new real structures on $K_1(\sqrt{-1})$ and $\overline{K_1}$. If system (5) has any solution relatively to this new real structures we get a solution $x_j^* = (x_{j,0}^*, \ldots, x_{j,n}^*) \in \mathbb{A}^{n+1}(\overline{K_1})$. This solution is given in the form (3). If system (5) has no solutions we ascertain this fact.

(10) Suppose that we found $1 \le j \le N'$, for which system (5) has no solutions. Then we go to the consideration of the next element $h \in H$.

(11) Let for the considered index j system (5) have a solution which $x_j^* = (x_{j,0}^*, \ldots, x_{j,n}^*) \in \mathbb{A}^{n+1}(\overline{K_1})$ which is found in paragraph (9). By paragraph (9) we have $x_{j,i}^* \in K_1[\eta_{\alpha,\beta}, \sqrt{-1}] = K_2$.

By (5) we have $\sum_{0\le i\le n} |x_{j,i}-x_{j,i}^*|^2 \le \varepsilon_1$. Remind that $\overline{x_j} = (x_{j,0}, \ldots, x_{j,n}) \in \mathbb{A}^{n+1}(\overline{k})$, see paragraph (4).

Find $\lambda_i \in K_2$ such that $(L_i - \lambda_i L_0)(x_j^*) = 0,\ s{+}1 \le i \le n$. Set $L_i' = L_i - \lambda_i L_0$. Consider the system

$$h_1 = \ldots = h_s = L_{s+1}' = \ldots = L_n' = 0 \qquad (6)$$

with coefficient from the field K_2.

(12) We need the following four lemmas.

LEMMA 5. The polynomial h is equal identically to zero on each irreducible component W_1 of the variety $W = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^n(\overline{k})$, such that $x_j \in W_1$ if and only if there exist no solutions of system (5) over the algebraic closure $\overline{K_1}$ of K_1.

PROOF. It coincides with the proof of Lemma 9 in [3].

LEMMA 6. Let W_1 be a component of the variety $W = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^n(\overline{K_1})$ such that $x_j = (x_{j,0} : \ldots : x_{j,n}) \in W_1$ for some $1 \le j \le N$ and let $\delta_i \in \overline{K_1}$, $s+1 \le i \le n$, be infinitely small values relatively to the field $\tilde{K}$.

Then there exists $x_0', \ldots, x_n' \in \overline{K_1}$ such that $x' = (x_0' : \ldots : x_n') \in W_1$, $(L_i - \delta_i L_0)(x') = 0$ and $x_0' - x_{j,0}, \ldots, x_n' - x_{j,n}$ are infinitely small relatively to the field $\overline{K}$.

PROOF. It coincides with the proof of Lemma 10 in [3].

LEMMA 7. Suppose that the polynomial h is equal identically to zero on some component W_1 of the variety $W = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^n(\overline{K})$, such that $x_j \in W_1$ and there exists x_j^*, see paragraph (9). Then there exist two different solutions $x' = (x_0', \ldots, x_n')$ and $x'' = (x_0'', \ldots, x_n'')$ of system (5) such that $x_{j,i} - x_i'$ and $x_{j,i} - x_i''$ are infinitely small relatively to the field $\overline{K}$ for all $0 \le i \le n$.

PROOF. It coincides with the proof of Lemma 11 in [3].

The next lemma is a generalization of Lemma 6. Remind that in paragraph (1) the variety W' was defined. Let K' be an arbitrary extension of K with a real structure and K'' an extension of K' by finite number of infinitely small values.

LEMMA 8. Let $D_i \in K'[X_0, \ldots, X_n]$, $s+1 \leq i \leq n$, be linear forms in $X_0, \ldots, X_n$ and $\widetilde{D}_i \in K''[X_0, \ldots, X_n]$, $s+1 \leq i \leq n$, linear forms in $X_0, \ldots, X_n$ all the coefficints of which are infinitely small values relatively to the field K'.

(a) Let $x''_0, x''_1, \ldots, x''_n \in \overline{K''}$ be such that $x'' = (x''_0 : x''_1 : \ldots : x''_n) \in W'$, $(D_i - \widetilde{D}_i)(x'') = 0$, $s+1 \leq i \leq n$, x''_i is not infinitely great relatively to the field $\overline{K'}$ for every $0 \leq i \leq n$ and $x''_{i_0} \neq 0$ is not infinitely small relatively to the field $\overline{K'}$ for some $0 \leq i_0 \leq n$. Then there exist $x'_0, x'_1, \ldots, x'_n \in \overline{K'}$ such that $x' = (x'_0 : x'_1 : \ldots : x'_n) \in W'$, $D_i(x') = 0$ and $x''_i - x'_i$, , $s + 1 \leq i \leq n$ are infinitely small values relatively to the field $\overline{K'}$.

(b) Let $W' \cap \{D_{s+1} = \ldots = D_n = 0\} \cap \{X_0 = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{K'})$. Then $W' \cap \{D_{s+1} - \widetilde{D}_{s+1} = \ldots = D_n - \widetilde{D}_n = 0\} \cap \{X_0 = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{K''})$.

(c) Let $W' \cap \{D_{s+1} = \ldots = D_n = 0\}$ be a finite set in $\mathbb{P}^n(\overline{K'})$. Then there exist only a finite number of $x'' = (x''_0 : x''_1 : \ldots : x''_n) \in W'$ in $\mathbb{P}^n(\overline{K''})$ such that $(D_i - \widetilde{D}_i)(x'') = 0$.

(d) Let $W' \cap \{D_{s+1} = \ldots = D_n = 0\}$ be a finite set in $\mathbb{P}^n(\overline{K'})$ and $x'_0, x'_1, \ldots, x'_n \in \overline{K'}$ be such that $x' = (x'_0 : x'_1 : \ldots : x'_n) \in W' \cap \{D_{s+1} = \ldots = D_n = 0\}$. Then there exist $x''_0, x''_1, \ldots, x''_n \in \overline{K''}$ such that $x'' = (x''_0 : x''_1 : \ldots : x''_n) \in W'$ in $\mathbb{P}^n(\overline{K''})$, $(D_i - \widetilde{D}_i)(x'') = 0$ and $x''_i - x'_i$, , $s+1 \leq i \leq n$ are infinitely small values relatively to the field $\overline{K'}$.

PROOF.

(a) Let $z \in \overline{K''}$ be an element which is not infinitely great relatively to the field $\overline{K'}$. Then,see e.g. [1], the standart part $\mathrm{st}(z) \in \overline{K'}$ is defined. It coincides with the free term in the expansion of z in multiple fraction-power series in algebraically independent infinitely small values over $\overline{K'}$, see e.g. [1]. So $z - \mathrm{st}(z)$ is infinitely small value relatively to the field $\overline{K'}$. Therefore, the point $\mathrm{st}(x'') = (\mathrm{st}(x''_0) : \mathrm{st}(x''_1) : \ldots : \mathrm{st}(x''_n)) \in W \cap \{D_{s+1} = \ldots = D_n = 0\}$ is the required element $x' \in \mathbb{P}^n(\overline{K'})$.

(b) Suppose contrary that there exist $x''_0, x''_1, \ldots, x''_n \in \overline{K''}$ such that $x'' = (x''_0 : x''_1 : \ldots : x''_n) \in W' \cap \{X_0 = 0\}$ and $(D_i - \widetilde{D}_i)(x'') = 0$, $s+1 \leq i \leq n$. Show that we can assume without loss of generality that every x''_i is not infinitely great relatively to the field $\overline{K'}$ for $0 \leq i \leq n$ and $x''_{i_0} \neq 0$ is not infinitely small relatively to the field $\overline{K'}$ for some $0 \leq i_0 \leq n$. Indeed, let $|x''_\alpha|$ be maximal of all $|x''_i|$, $s+1 \leq i \leq n$. Then changing x'' for $x''/|x''_\alpha|$ we get new x'' with the required property. Now the assertion of (b) follows from (c).

(c) Choose a linear form $D_0 \in K'[X_0, \ldots, X_n]$ such that for every $x' \in W' \cap \{D_{s+1} = \ldots = D_n = 0\}$ in $\mathbb{P}^n(\overline{K'})$ we have $D_0(x') \neq 0$. The projection $p : W' \longrightarrow \mathbb{P}^{n-s}$, $(X_0 : \ldots : X_n) \longmapsto (D_0 : D_{s+1} : D_{s+2} : \ldots : D_n)$, is defined everywhere and, therefore finite, see [9]. Show that the projectin $\tilde{p} : W' \longrightarrow \mathbb{P}^{n-s}$, $(X_0 : \ldots : X_n) \longmapsto (D_0 : D_{s+1} - \widetilde{D}_{s+1} : D_{s+2} - \widetilde{D}_{s+2} : \ldots : D_n - \widetilde{D}_n)$ is also defined everywhere. Let $z = (z_0 : \ldots : z_n) \in \mathbb{P}^n(\overline{K''})$. We can assume without loss of generality, see (b), that every z_i is not infinitely great relatively to the field $\overline{K'}$ for $0 \leq i \leq n$ and $x''_{i_0} \neq 0$ is not infinitely small relatively to the field $\overline{K'}$ for some $0 \leq i_0 \leq n$. Therefore, $\mathrm{st}(z) \in \mathbb{P}^n(\overline{K'})$ is defined, see (a). There exists $s+1 \leq i \leq n$ or $i = 0$ for which $D_i(\mathrm{st}(z)) \neq 0$ since p is defined everywhere. Then $(D_i - \widetilde{D}_i)(z) \neq 0$. Thus, $\tilde{p}$ is also defined everywhere and finite. So, there exist only a finite number of $x'' = (x''_0 : x''_1 : \ldots : x''_n) \in W$ in $\mathbb{P}^n(\overline{K''})$ such that $(D_i - \widetilde{D}_i)(x'') = 0$, $s+1 \leq i \leq n$ since each such x' is an element of the finite set $\tilde{p}^{-1}((1 : 0 : \ldots : 0))$. Here $\tilde{p}^{-1}$ denotes the inverse image of $\tilde{p}$.

(d) There exists a linear form $D \in K'[X_0, \ldots, X_n]$ such that $(D/D_0)(x'_1) \neq (D/D_0)(x'_2)$ for every different $x'_1, x'_2 \in W' \cap \{D_{s+1} = \ldots = D_n = 0\}$ in $\mathbb{P}^n(\overline{K'})$. Consider the projections $p_1 : W' \longrightarrow \mathbb{P}^{n-s+1}$, $(X_0 : \ldots : X_n) \longmapsto (D_0 : D_{s+1} : D_{s+2} : \ldots : D_n : D)$ and $\tilde{p_1} : W' \longrightarrow \mathbb{P}^{n-s+1}$, $(X_0 : \ldots : X_n) \longmapsto (D_0 : D_{s+1} - \widetilde{D}_{s+1} : D_{s+2} - \widetilde{D}_{s+2} : \ldots : D_n - \widetilde{D}_n : D)$. Since $\tilde{p}$ is finite (see the proof of (c)) there exists a polynomial $\widetilde{G} \in \overline{K''}[Z_0, Z_{s+1}, Z_{s+2}, \ldots, Z_n, Z]$ such that $\tilde{p_1}(W') = \{\widetilde{G} = 0\}$ in $\mathbb{P}^{n-s+1}(\overline{K''})$ and $\mathrm{lc}_Z \widetilde{G} = 1$.

Show that each coefficient of $\widetilde{G}$ is not infinitely great relatively to the field $\overline{K'}$. Suppose contrary. Then there exists $x'_0, x'_{s+1}, \ldots, x'_n \in \overline{K'}$ such that there exists a coefficient of the polynomial $g_1 = \widetilde{G}(x'_0, x'_{s+1}, \ldots, x'_n, Z) \in \overline{K''}[Z]$ which is infinitely great relatively to the field $\overline{K'}$. So, $x' = (x'_0 : x'_{s+1} : \ldots : x'_n) \in \mathbb{P}^{n-s}(\overline{K'})$. The set of roots of g_1 coincides with $(D/D_0)(\tilde{p_1}^{-1}(x'))$ since $\tilde{p_1}(W') = \{\widetilde{G} = 0\}$. For every $x'' = (x''_0 : x''_1 : \ldots : x''_n) \in \tilde{p_1}^{-1}(x')$ choose $x''_0, x''_{s+1}, \ldots, x''_n \in \overline{K''}$ such that $x'' = (x''_0 : x''_1 : \ldots : x''_n)$ and every x''_i is not infinitely great relatively to the field $\overline{K'}$ for $0 \leq i \leq n$ for and $x''_{i_0} \neq 0$ is not infinitely small relatively to the field $\overline{K'}$ for some $0 \leq i_0 \leq n$, see the proof of (b). So $\mathrm{st}(x'')$ is defined and $(D/D_0)(x'') = (D/D_0)(\mathrm{st}(x''))$ is not infinitely great for every x''. This leads to the contradiction since now we get that each root of g_1 is not infinitely great relatively to the field $\overline{K'}$ and $\mathrm{lc}_Z g_1 = 1$. The assertion is proved.

Thus, the polynomial $\mathrm{st}(\widetilde{G}) = G \in \overline{K'}[Z_0, Z_{s+1}, Z_{s+2}, \ldots, Z_n, Z]$ is defined (the coefficints of G are the standart parts of coefficints of $\widetilde{G}$). We have $p_1(W') \subset \{G = 0\}$ in $\mathbb{P}^{n-s+1}(\overline{K'})$. Denote $g = G(1, 0, 0, \ldots, 0, Z)$ and $\tilde{g} = \widetilde{G}(1, 0, 0, \ldots, 0, Z)$. So $g((D/D_0)(x')) = 0$ for every $x' \in W' \cap \{D_{s+1} = \ldots = D_n = 0\}$ in $\mathbb{P}^n(\overline{K'})$ and $\tilde{g}((D/D_0)(x'))$ is infinitely small value relatively to the field $\overline{K'}$. Since $\mathrm{lc}_Z \tilde{g} = 1$ there exists a root

χ of $\tilde{g}$ such that $\chi - (D/D_0)(x')$ is infinitely small value relatively to the field $\overline{K'}$. But $\chi = (D/D_0)(x'')$ for some $x'' \in W'$ in $\mathbb{P}^n(\overline{K''})$ such that $(D_i - \widetilde{D}_i)(x'') = 0$ for $s+1 \le i \le n$. We can choose, see the proof of (b), $x''_0, x''_{s+1}, \ldots, x''_n \in \overline{K''}$ such that $x'' = (x''_0 : x''_1 : \ldots : x''_n)$, each x''_i, $0 \le i \le n$ is not infinitely great relatively to the field $\overline{K'}$ and $x''_{i_0} \neq 0$ is not infinitely small relatively to the field $\overline{K'}$ for some $0 \le i_0 \le n$. So by (a), $\mathrm{st}(x'') \in W' \cap \{D_{s+1} = \ldots = D_n = 0\}$ in $\mathbb{P}^n(\overline{K'})$. Finally, $(D/D_0)(x') = (D/D_0)(\mathrm{st}(x''))$ and therefore, $x' = \mathrm{st}(x'')$. Lemma is proved.

(13) System (6) defines a closed set in $\mathbb{P}^n(\overline{K_2})$. By Lemma 8 (d) system (6) has only a finite number of solutions in $\mathbb{A}^n(\overline{K_2}) = \mathbb{P}^n(\overline{K_2}) \cap \{X_0 \neq 0\}$ and $W' \cap \{L'_{s+1} = \ldots = L'_n\} \cap \{X_0 = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{K_2})$.

Apply the algorithm from [4] and find all the solutions x_γ, $\gamma \in \Gamma$ of system (6) in $\mathbb{A}^n(\overline{K_2})$. Denote by $N_1 = \#\Gamma$ the number of elements of Γ.

(14) We need an auxiliary algorithm. In input of this algorithm linear forms $D_i \in K_2[X_0, \ldots, X_n]$, $s+1 \le i \le n$ in $X_0, \ldots, X_n$ are given with $\deg_{\varepsilon_j} D_i$, $\deg_{t_j} D_i \le \mathcal{P}(d^n, d_1, d_2)$, $l(D_i) \le (M_1 + M_2)\mathcal{P}(d^n, d_1, d_2)$ for all i, j. Besides that, these forms satisfy to one of the following conditions

(a) $N_2 = \#W' \cap \{D_{s+1} = \ldots = D_n = 0\} < +\infty$, $W' \cap \{D_{s+1} = \ldots = D_n = 0\} \cap \{X_0 = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{K_2})$;

(b) $\#W' \cap \{D_{s+1} = \ldots = D_n = 0\} < +\infty$, $N_2 = \#W' \cap \{D_{s+1} = \ldots = D_n = 0\} \cap \mathbb{A}^n(\overline{K_2})$.

In output of the auxiliary algorithm we have linear forms $M_{s+1}, \ldots, M_n$ with coefficients from $\mathbb{Z}$ and of the size $l(M_i) = O(n \log d)$, $s+1 \le i \le n$ such that

if condition (a) is satisfied then $N_2 \le \#W' \cap \{M_{s+1} = \ldots = M_n = 0\} < +\infty$, $W' \cap \{M_{s+1} = \ldots = M_n = 0\} \cap \{X_0 = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{K_2})$;

if condition (b) is satisfied then $\#W' \cap \{M_{s+1} = \ldots = M_n = 0\} < +\infty$, $N_2 \le \#W' \cap \{M_{s+1} = \ldots = M_n = 0\} \cap \mathbb{A}^n(\overline{K_2})$.

In the description of the auxiliary algorithm below we don't suppose that we are given the forms $L_{s+1}, \ldots, L_n$ but use only the definition of W' i.e. suppose only that $h_1 \ldots, h_s$ are given.

At first, show that we can change an arbitrary coefficient in forms $D_{s+1}, \ldots, D_n$ for an integer coefficient with the required length such that the condition (a) (respectively (b)) will be satisfied for new forms if the condition (a) (respectively (b)) is satisfied.

Let $D_{s+1} = \sum_{0 \le i \le n} l_{s+1,i} X_i$, $l_{s+l,i} \in \overline{K_1}$ and we wish to change, say $l_{s+1,0}$, for a coefficient from $\mathbb{Z}$. At first change $l_{s+1,0}$ for an element $l_{s+l,0} - \varepsilon_3$ where ε_3 is an infinitely small value relatively to the field K_2. Denote by $D'_{s+1} = (l_{s+l,0} - \varepsilon_3) X_0 + \sum_{0 \le i \le n} l_{s+1,i} X_i$ the form obtained. Consider the system

$$h_1 = \ldots = h_s = D'_{s+1} = D_{s+2} = \ldots = D_n = 0. \tag{7}$$

Denote by Ξ the set of solutions of this system in $\mathbb{A}^n(\overline{K_2})$. By Lemma 8 we have $\#\Xi = N_3 \geq N_2$ but $\#\Xi < +\infty$ if (a) or (b) are satisfied and $W' \cap \{D'_{s+1} = D_{s+2} = \ldots = D_n = 0\} \cap \{X_0 = 0\} = \emptyset$ (respectively $\#W' \cap \{D'_{s+1} = D_{s+2} = \ldots = D_n = 0\} < +\infty$) in $\mathbb{P}^n(\overline{K_2})$ if (a) (respectively (b)) is satisfied.

Denote $U' = W' \cap \{D_{s+2} = \ldots = D_n = 0\}$. For every irreducible component W'' (it is a curve) of U' there exists at most one value ε^* of ε_3 such that $D'_{s+1}|_{\varepsilon_3 = \varepsilon^*}$ is vanishing on W''. Further, for every irreducible component W''' of $U' \cap \{X_0 = 0\}$ there exists at most one value ε^* of ε_3 such that $D'_{s+1}|_{\varepsilon_3=\varepsilon^*}$ is vanishing on W''' if (a) is satisfied. So, by the Bésout inequality, there exists at most $2(d-1)^s$ different values $\varepsilon^* \in \overline{K_2}$ of ε_3 such that the system

$$h_1 = \ldots = h_s = D'_{s+1}|_{\varepsilon_3=\varepsilon^*} = D_{s+2} = \ldots = D_n = 0. \tag{8}$$

has infinitely many solutions in $\mathbb{A}^n(\overline{K_2})$ or $W' \cap \{D'_{s+1}|_{t=t_0} = D_{s+2} = \ldots = D_n = 0\} \cap \{X_0 = 0\} \neq \emptyset$ in $\mathbb{P}^n(\overline{K_2})$ if (a) is satisfied. Similarly there exists at most $(d-1)^s$ different values $\varepsilon^* \in \overline{K_2}$ of ε_3 such that $W' \cap \{D'_{s+1}|_{t=t_0} = D_{s+2} = \ldots = D_n = 0\}$ is infinite in $\mathbb{P}^n(\overline{K_2})$ if (b) is satisfied.

(15) LEMMA 9. There exist at most $2(d-1)^{2s}$ different values $\varepsilon^* \in \overline{K_2}$ of ε_3 such that the number of solutions of system (8) in $\mathbb{A}^n(\overline{K_2})$ is less than N_3.

PROOF. There exists a linear form $L = c_0X_0 + \ldots + c_nX_n$ with integer coefficients c_i such that the function L/X_0 has N_3 different values on the set of solutions of system (7) in $\mathbb{A}^n(\overline{K_2})$, i.e. $\#(L/X_0)(\Xi) = N_3$ and L is not vanishing in each point of the finite set $W' \cap \{D_{s+1} = \ldots = D_n\} \cap \{X_0 = 0\}$. The projection $p' : U' \longrightarrow \mathbb{P}^2$, $(X_0 : \ldots : X_n) \longmapsto (X_0 : D_{s+1} : L)$, is defined everywhere since L is not vanishing in each point of the finite set $W' \cap \{D_{s+1} = \ldots = D_n\} \cap \{X_0 = 0\}$. Therefore, $p'(U') \subset \mathbb{P}^2$ is a closed set in the Zariski topology of dimension 1 and the projection $p' : U' \longrightarrow p'(U')$ is finite. So $p'(U') = \{G(X_0, D_{s+1}, L) = 0\}$ where $G \in \overline{K}[Z_0, Z_1, Z_2]$ is a separable polynomial of degree $\deg_{Z_0,Z_1,Z_2} G \leq \deg U' \leq (d-1)^s$. We have $G(1, \varepsilon_3, (L/X_0)(\chi)) = 0$ for every solution of system (7) in $\mathbb{A}^n(\overline{K_2})$. Therefore, $\deg_{Z_2} G \geq N_3$. Denote by Ξ^* the set of solutions of system (8) in $\mathbb{A}^n(\overline{K_2})$. Now we have $(L/X_0)(\Xi^*) = \{\chi^* : G(1, \varepsilon^*, (L/X_0)(\chi^*)) = 0\}$. Denote $R(Z_1, Z_2) = \mathrm{Res}_{Z_2}(G, G'_{Z_2})$ the discriminant of the polynomial G relatively to Z_2. So if $R(1, \varepsilon^*) \neq 0$ then $\Xi^* \geq (L/X_0)(\Xi^*) \geq \deg_{Z_2} G \geq N_3$. We have $R \neq 0$ since R is seprable. The degree $\deg_{Z_3} R \leq 2(d-1)^{2s}$. Further, $R(1, Z) \neq 0$ since R is homogeneous as the discriminant of the homogeneous polynomial G. The degree $\deg_Z R(1, Z) \leq deg_{Z_3} R \leq 2(d-1)^{2s}$. From here the assertion of the lemma follows immediately.

(16) In the proof of the following lemma we don't suppose that we are given the forms $L_{s+1}, \ldots, L_n$ but use only the definition of W' i.e. suppose only that $h_1 \ldots, h_s$ are given.

LEMMA 10. Let $D_i \in K_2[X_0, \ldots, X_n]$, $s+1 \le i \le n$, be linear forms in $X_0, \ldots, X_n$ with $\deg_{\varepsilon_j} D_i$, $\deg_{t_j} D_i \le \mathcal{P}(d^n, d_1, d_2)$, $l(D_i) \le (M_1 + M_2)\mathcal{P}(d^n, d_1, d_2)$ for all i, j. Denote $U = W' \cap \{D_{s+1} = \ldots = D_n = 0\}$ when $n \ge s$ and $U' = W' \cap \{D_{s+2} = \ldots = D_n = 0\}$ when $n \ge s+1$ in $\mathbb{P}^n(\overline{K_2})$.

(a) Suppose that $\dim U = 0$. Then one can construct all the irreducible over $\overline{K_2}$ components (they are points) of the variety U in time polynomial in M_1, M_2, d^n, d_1, d_2.

(b) Suppose that $\dim U' = 1$. Then one can construct all the irreducible over $\overline{K_2}$ components (they are curves) of the variety U' in time polynomial in M_1, M_2, d^n, d_1, d_2.

(c) Suppose that $\dim U = 0$. Then one can construct all the irreducible over $\overline{K_2}$ components (they are points) of the variety $U \cap \{X_0 = 0\}$ in time polynomial in M_1, M_2, d^n, d_1, d_2.

(d) Suppose that $\dim U' = 1$. Then one can construct all the irreducible over $\overline{K_2}$ components (they are points or curves) of the variety $U' \cap \{X_0 = 0\}$ in time polynomial in M_1, M_2, d^n, d_1, d_2.

PROOF. Let Y be an algebraically independent element over the field K_2. Consider the following systems of equations

$$\begin{cases} h_i - YX_i^{d-1} = 0, & 1 \le i \le s \\ D_j - YX_j = 0, & s+1 \le j \le n \end{cases} \tag{9}$$

and

$$\begin{cases} h_i - YX_i^{d-1} = 0, & 1 \le i \le s \\ D_j - YX_j = 0, & s+2 \le j \le n \end{cases} \tag{10}$$

These systems can be considered as systems with coefficints in $K_2(Y)$ with the set of solutions in $\mathbb{P}^n(\overline{K_2(Y)})$ or as systems with coefficints in K_2 with the set of solutions in $(\mathbb{P}^n \times \mathbb{A}^1)(\overline{K_2})$ when Y is considered as a coordinate in $\mathbb{A}^1$.

Denote by $\{w_\lambda\}_{\lambda \in \Lambda}$ (respectively $\{v_\lambda\}_{\lambda \in \Lambda_1}$) the family of all defined and irreducible over the field $K_2(Y)$ components of the variety of solutions of system (9) (respectively (10)). Apply the algorithm from [4] and find $\{w_\lambda\}_{\lambda \in \Lambda}$ and $\{v_\lambda\}_{\lambda \in \Lambda_1}$.

We have $\dim(w_\lambda) = 0$ and $\dim(v_\lambda) = 1$, see e.g. [4] (so system (9) is just a system with a finite number of solutions in $\mathbb{P}^n(\overline{K_2(Y)})$

Now consider Y as a variable. Denote by U_Y (respectively U'_Y) the union of all the irreducible components W'' of the variety of solutions of system (9) (respectively (10)) in $(\mathbb{P}^n \times \mathbb{A}^1)(\overline{K_2})$ such that W'' is not contained in the union of a finite number of hyperplanes $\{Y = c\}$, $c \in \overline{K_2}$. Then, see [4] and c.f. also [3] section 2, the corollary of lemma 6, every w_λ (respectively v_λ) corresponds bijectively to the irreducible and defined over K_2 component W_λ (respectively V_λ) of the variety U_Y (respectively U'_Y). The algorithm from [4] construct simultaneously with $\{w_\lambda\}_{\lambda \in \Lambda}$ and $\{v_\lambda\}_{\lambda \in \Lambda_1}$ also $\{W_\lambda\}_{\lambda \in \Lambda}$ and

$\{V_\lambda\}_{\lambda\in\Lambda_1}$. Remind that the polynomial equtions over K_2 which give W_λ as a set of solutions give also w_λ under this correspondence if one consider Y as an element of the coefficient field. In output of the algorithm from [4] w_λ and W_λ are given by their "general points" and special systems of equations of the required size. The similar is true for v_λ and V_λ.

Using the algorithm from [4] find all the components $\{W_{\lambda,\mu}\}_{\mu\in M_\lambda}$ defined and irreducible over $\overline{K_2}$ of the variety $W_\lambda\cap\{Y=0\}$, $\lambda\in\Lambda$ and all the components $\{V_{\lambda,\mu}\}_{\mu\in M_\lambda}$ defined and irreducible over $\overline{K_2}$ of the variety $V_\lambda\cap\{Y=0\}$, $\lambda\in\Lambda_1$. It can be done also using Newton's polygon method by constructing expansions of coordinates of the "general point" of W_λ (respectively V_λ) in the field of fraction-power series $\Omega=\bigcup_{\nu\in\mathbb{N}}\overline{K_2(\varepsilon_3)}((Y^{1/\nu}))$ and taking the free term, c.f. [3] section 3, paragraphs (11), (12), (13).

We claim that each component $W_{\lambda,\mu}$ (respectively $V_{\lambda,\mu}$) which is not contained in $\{X_0=0\}$ is a component of the variety U (respectively U') and each component of U (respectively U') which (may be contained in $\{X_0=0\}$) is equal to $W_{\lambda,\mu}$ (respectively $V_{\lambda,\mu}$) for some $\lambda\in\Lambda$, $\mu\in M_\lambda$ (respectively $\lambda\in\Lambda_1$, $\mu\in M_\lambda$).

Indeed, we have $U\cap\mathbb{A}^n(\overline{K_2})$ (respectively $U'\cap\mathbb{A}^n(\overline{K_2})$) is a subset of solutions of system (9) (respectively (10)) with the coordinate $Y=0$ in $\mathbb{A}^n(\overline{K_2})$. Let S_0 be acomponent of U (respectively U'). Then S_0 is not contained in a component of solutions of (9) (respectively (10)) which is contained in $\{Y=0\}$ since, otherwise, S_0 would be a component of (9) (respectively (10)) and the codimension of S_0 would be less than the number of equations in (9) (respectively (10)). So we get the contradiction.

Thus, the set of components $W_{\lambda,\mu}$ (respectively $V_{\lambda,\mu}$) which are not contained in $\{X_0=0\}$ coincides with the set of components of U (respectively U') which have a non-empty intersection with $\mathbb{A}^n(\overline{K_2})$. This proves the first statement and the second statement when $n=s$ (respectively $n=s+1$) since in this case $U=W'$ (respectively $U'=W'$) and all the components of U (respectively U') have a non-empty intersection with $\mathbb{A}^n(\overline{K_2})$.

Now we can suppose that $n>s$ (respectively $n>s+1$). In the proof of the second statement one should take into account that some components of U and U' may be contained in components of greater dimension lying in $\{X_0=0\}$ of the vatiety of solutions of systems (9) and (10) respectively. So this proof is slightly more complicated.

There exist linear forms $D'_i=\delta_{i,i-1}D_{i-1}+\ldots+\delta_{i,n}D_n$, $\delta_{i,j}\in\mathbb{Z}$, $i-1\leq j\leq n$, $\delta_{i,i-1}\neq 0$, $s+2\leq i\leq n$ (respectively $s+3\leq i\leq n$) such that $\dim W'\cap\{D'_{s+2}=\ldots=D'_r=0\}=n-r+1$, $\dim W'\cap\{D'_{s+2}=\ldots=D'_r=0\}\cap\{X_0=0\}=n-r$, for all $s+2\leq r\leq n$ (respectively $\dim W'\cap\{D'_{s+3}=\ldots=D'_r=0\}=n-r+2$, $\dim W'\cap\{D'_{s+3}=\ldots=D'_r=0\}\cap\{X_0=0\}=n-r+1$ for all $s+3\leq r\leq n$).

These forms can be choosen by induction since each time when $r<n$ there are no components of $W'\cap\{D'_{s+2}=\ldots=D'_r=0\}\cap\{X_0=0\}$ (respectively

$W' \cap \{D'_{s+3} = \ldots = D'_r = 0\} \cap \{X_0 = 0\}$) on which all the forms $D_r, \ldots, D_n$ are vanishing. So there exists a linear combination of them which is not vanishing on every component of $W' \cap \{D'_{s+2} = \ldots = D'_r = 0\} \cap \{X_0 = 0\}$ (respectively $W' \cap \{D'_{s+3} = \ldots = D'_r = 0\} \cap \{X_0 = 0\}$).

Denote $U_1 = W' \cap \{D'_{s+1} = \ldots = D'_n = 0\}$ and $U_2 = W' \cap \{D'_{s+2} = \ldots = D'_n = 0\}$ in $\mathbb{P}^n(\overline{K_2})$. Note that U_1 and U_2 do not have components which are contained in $\{X_0 = 0\}$ by the construction described of the forms D_i. Besides that, all the components of U_1 (respectively U_2) are of dimension one (respectively two) and $U_1 \cap \{D_n = 0\} = U$ (respectively $U_2 \cap \{D_n = 0\} = U'$). We shall need also the systems of equations

$$\left\{ \begin{array}{ll} h_i - YX_i^{d-1} = 0, & 1 \le i \le s \\ D'_j - Y(\delta_{j,j-1}X_{j-1} + \ldots + \delta_{j,n}X_n) = 0, & s+2 \le j \le n \end{array} \right. \tag{11}$$

and

$$\left\{ \begin{array}{ll} h_i - YX_i^{d-1} = 0, & 1 \le i \le s \\ D'_j - Y(\delta_{j,j-1}X_{j-1} + \ldots + \delta_{j,n}X_n) = 0, & s+3 \le j \le n \end{array} \right. \tag{12}$$

Denote by $U_{1,Y}$ (respectively $U_{2,Y}$) the union of all the irreducible components W'' of the variety of solutions of system (11) (respectively (12)) in $(\mathbb{P}^n \times \mathbb{A}^1)(\overline{K_2})$ such that W'' is not contained in the union of a finite number of hyperplanes $\{Y = c\}$, $c \in \overline{K_2}$. We have $\dim U_{1,Y} = 1, \dim U_{2,Y} = 2$, see e.g. [4] and c.f. also [3] section 2, the corollary of lemma 6

Now let S_1 be a component of U (respectively U'). There exists an irreducible component S_2 of U_1 (respectively U_2) such that $S_1 \subset S_2$. Then S_1 is a component of $S_2 \cap \{D_n = 0\}$ since dim $S_2 \cap \{D_n = 0\}$ = dim S_1.

Show that S_2 is not contained in a component S_3 of the variety of solutions of system (11) (respectively (12)) in $(\mathbb{P}^n \times \mathbb{A}^1)(\overline{K_2})$ such that $S_3 \subset \{Y = 0\}$. Indeed, otherwise $S_2 \subset S_3$, $S_3 \subset \{h_1 = \ldots = h_s = D'_{s+2} = \ldots = D'_n = 0\}$ (respectively $S_3 \subset \{h_1 = \ldots = h_s = D'_{s+3} = \ldots = D'_n = 0\}$) and $S_3 \cap \mathbb{A}^n(\overline{K_2}) \neq \emptyset$. So $S_3 = S_2$ is a component of U_1 (respectively U_2). But $\dim S_2 = 1$ (respectively $= 2$), dim $S_3 \geq 2$ (respectively ≥ 3) and we get the contradiction.

Thus, there exists a component S_4 of the variety $U_{1,Y}$ (respectively $U_{2,Y}$) such that $S_4 \cap \{Y = 0\} \supset S_2$. Then S_2 is a component of $S_4 \cap \{Y = 0\}$ since $\dim S_2 = \dim S_4 \cap \{Y = 0\}$.

Since $\dim S_1 = \dim S_4 - 2$ there exists an irreducible component S_5 of the variety $S_4 \cap \{D_n - YX_n = 0\}$ such that S_1 is a component of $S_5 \cap \{Y = 0\}$.

Show that S_5 is not contained in the union of a finite number of hyperplanes $\{Y = c\}$, $c \in \overline{K_2}$. Indeed, otherwise $S_5 \subset \{Y = 0\}$ since $S_5 \cap \{Y = 0\} \supset S_1 \neq \emptyset$. So $S_5 = S_1$ and we get the contradiction: $\dim S_4 - 1 \leq \dim S_5 = \dim S_1 = \dim S_4 - 2$.

Thus, S_5 is contained in a component of U_Y (respectively U'_Y) since system (11) (respectively (12)) with the additional equation $D_n - YX_n = 0$ is equivalent to (9) (respectively (10)). Further, $\dim S_5 \geq \dim S_4 - 1 = \dim U_Y$

(respectively $= \dim U'_Y$). Therefore, S_5 coincides with a component W_λ (respectively V_λ) for some λ and S_1 coincides with a component $W_{\lambda,\mu}$ (respectively $V_{\lambda,\mu}$) for some λ, μ. The second statement is proved.

Now to prove (a) and (b) we need only a criteria to determine whether the component $W_{\lambda,\mu} \subset U$ (respectively $V_{\lambda,\mu} \subset U'$) for a component $W_{\lambda,\mu}$ (respectively $V_{\lambda,\mu}$) such that $W_{\lambda,\mu} \subset \{X_0 = 0\}$ (respectively $V_{\lambda,\mu} \subset \{X_0 = 0\}$).

We can verify whether the linear forms D_i are vanishing on $W_{\lambda,\mu}$ (respectively $V_{\lambda,\mu}$) substituting the "general point" of $W_{\lambda,\mu}$ (respectively $V_{\lambda,\mu}$) in D_i for $s+1 \leq i \leq n$ (respectively for $s+2 \leq i \leq n$). So it is enough to check whether $W_{\lambda,\mu} \subset W'$ (respectively $V_{\lambda,\mu} \subset W'$).

In the following Lemma 11 a criteria is given which affords to determine whether a point from $\{X_0 = 0\}$ belongs to W'. Using Lemma 11 we can verify whether $W_{\lambda,\mu} \subset W'$.

Consider $V_{\lambda,\mu}$. Construct arbitrary $(d-1)^{2s}+1$ points of $V_{\lambda,\mu}$ in $\mathbb{P}^n(\overline{K_2})$ (one can take e.g. appropriate specializations of the "general point" of $V_{\lambda,\mu}$) and verify using Lemma 11 whether they belong to W'. We claim that if $W_{\lambda,\mu} \not\subset W'$ then at least one of the constructed points does not belong to W'. Indeed, deg $W' \leq (d-1)^s$ and deg $W_{\lambda,\mu} \leq (d-1)^s$. So their intersection has at most $(d-1)^{2s}$ points by the Bézout inequality. Thus, we constructed everything which is required in (a) and (b).

The statement (c) for $U \cap \{X_0 = 0\}$ follows from (a) immediately. The components of dimension one of $U' \cap \{X_0 = 0\}$ are the components of U' lying in $\{X_0 = 0\}$. Other components of $U' \cap \{X_0 = 0\}$ are some components of $V_{\lambda,\mu} \cap \{X_0 = 0\}$ where $V_{\lambda,\mu} \not\subset \{X_0 = 0\}$ for some $\lambda \in \Lambda_1$, $\mu \in M$. We can construct all the points from $V_{\lambda,\mu} \cap \{X_0 = 0\}$ using e.g. the Newton polygons method by constructing expansions of coordinates of the "general point" of V_λ in the field of fraction-power series and taking the free term, c.f. [3] section 3, paragraphs (11), (12), (13). Thus, we constructed everything which is required in (c) and (d).

The required estimation for the working time of the algorithm described in the proof of this Lemma follows directly from the estimations for the working time of the algorithms applied. Lemma is proved.

(17) Let $0 \leq \varepsilon_4 \leq \varepsilon_3$ be infinitely small values for the field $\overline{K_2}$ and ε_4 is infinitely small value for the field $\overline{K_2(\varepsilon_3)}$. Let K has an order of the real field such as it is described in section 1. It induces the real structure on $\overline{K_2(\varepsilon_3, \varepsilon_4)} = \overline{K(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)}$

LEMMA 11. Let $(x'_1, \ldots, x'_n) \in \mathbb{A}^n(\overline{K_2})$, $x'_r \neq 0$ and $\deg_{\varepsilon_1} x'_i$, $\deg_{\varepsilon_2} x'_i$ $\deg_{t_j} x'_i \leq \mathcal{P}(d^n, d_1, d_2)$, $l(x'_i) \leq (M_1 + M_2)\mathcal{P}(d^n, d_1, d_2)$ for all i, j. Then one can ascertain whether the point $x' = (0 : x'_1 : \ldots : x'_n) \in W'$ in time polynomial in d^n, d_1, d_2, M_1, M_2.

More precisely $x' \in W'$ if and only if the system of equations and an inequality

$$h_1 = \ldots = h_s = X_0 - \varepsilon_4 X_r = 0,\ |X_0|^2 + \sum_{1 \leq j \leq n} |X_j - x'_j|^2 \leq \varepsilon_3 \qquad (9)$$

has a solution $x^* \in \mathbb{A}^{n+1}(\overline{K_2(\varepsilon_3, \varepsilon_4)})$

Thus, applying Theorem 2 we can ascertain whether $x' \in W'$ and if it is so, construct a new order of the real field on K which induces the new real structure on the field $\overline{K_2(\varepsilon_3, \varepsilon_4)}$ and find a solution $x^* = (x_0^*, \dots, x_n^*) \in \mathbb{A}^{n+1}(K_3)$ of system (9) relatively to this real structure of $\overline{K_2(\varepsilon_3, \varepsilon_4)}$. Here the field $K_3 \subset \overline{K_2(\varepsilon_3, \varepsilon_4)}$, $K_3 = K_2(\varepsilon_3, \varepsilon_4)[\eta^{(1)}, \sqrt{-1}]$ and $\eta^{(1)}$ is an algebraic element over $K_2(\varepsilon_3, \varepsilon_4)$ with minimal polynomial $\psi^{(1)} \in K_2(\varepsilon_3, \varepsilon_4)[Z]$ such that $\deg_{\varepsilon_i} \psi^{(1)}$, $\deg_{t_j} \psi^{(1)} \le \mathcal{P}(d^n, d_1, d_2)$, $l(\psi^{(1)}) \le (M_1 + M_2)\mathcal{P}(d^n, d_1, d_2)$ for all i, j.

PROOF. It coincides essentially with the proof of Lemma 5 or Lemma 9 in [3]. We can assume that $x' \in \{h_1 = \dots = h_s = 0\} = W$. Now the statement of the Lemma is equivalent to the following one: system (9) has no solutions iff the hyperplane $\{X_0 = 0\}$ contains all the components W_1 of the variety $W = \{h_1 = \dots = h_s = 0\} \subset \mathbb{P}^n(\overline{K})$ such that $x' \in W_1$.

Let X_0 be equal identically to zero on each such W_1. Denote $V = \{h_1 = \dots = h_s = 0\} \subset \mathbb{A}^{n+1}(\overline{K_2(\varepsilon_3, \varepsilon_4)})$. Then there exists a homogeneous polynomial P with coefficients from $\overline{K_2}$ such that $(X_0 / X_r)(V \cap \{P X_r \neq 0\}) = \{0\}$ and $P(x_j) \neq 0$. Let $\overline{x} = (0, x_1', \dots, x_n') \in \mathbb{A}^{n+1}$. Denote $\{|X - \overline{x}|^2 < \varepsilon_3\} \subset \{|X_0|^2 + \sum_{1 \le j \le n} |X_j - x_j'|^2 \le \varepsilon_3\} \subset \mathbb{A}^{n+1}(\overline{K_2(\varepsilon_3, \varepsilon_4)})$. Show that $\{|X - \overline{x}|^2 < \varepsilon_3\} \cap V \subset \{X_r P \neq 0\} \cap V$.

Indeed, otherwise there exists $x' \in \mathbb{A}^{n+1}(\overline{K_2(\varepsilon_3, \varepsilon_4)})$ such that $(X_r P)(x') = 0$ and $|x' - \overline{x}|^2 < \varepsilon_3$, i.e. $(X_r P)(\overline{x} + (x' - \overline{x})) = 0$ where $x' - \overline{x}$ has infinitely small coordinates relatively to the field $\overline{K_2}$. This leads to the contradiction, since $\overline{x} \in \mathbb{A}^{n+1}(\overline{K_2})$ and $(X_r P)(\overline{x}) \neq 0$.

Thus, we have $(X_0 / X_r)(\{|X - \overline{x}|^2 < \varepsilon_3\} \cap V) = \{0\}$, i.e. there are no solutions of (13) over $\overline{K_2(\varepsilon_3, \varepsilon_4)}$.

Conversely, suppose that X_0 is not equal identically to zero on some component W_1 of W, such that $x' \in W_1$. Let $V_1 \subset \mathbb{A}^{n+1}(\overline{K_2})$ be component of V corresponding to W_1, i.e. V_1 is given by the same equations as W_1.

There exists a closed algebraic curve V_2 defined and irreducible over $\overline{K_2}$ such that $V_2 \subset V_1$, $\overline{x} \in V_2$ and $X_0(V_2) \neq \{0\}$. Let t be a uniformizing element of some branch of V_2 containing the point $\overline{x}$. The coordinate functions $x^{(\rho)}$, $0 \le \rho \le n$, on V_2 in the neighbourhood of the points $\overline{x} = (0, x_1', \dots, x_n')$ can be represented as series

$$x^{(\rho)} = x_\rho' + \sum_{i \ge 1} t^i \alpha_{\rho,i}, \ \alpha_{\rho,i} \in \overline{K}, \ x_0' = 0,$$

$$\frac{x^{(0)}}{x^{(r)}} = \alpha_0 t^\nu + \sum_{i \ge 1} t^{i+\nu} \alpha_i, \ \alpha_i \in \overline{K_2}, \ 0 < \nu \in \mathbb{Z}, \alpha_0 \neq 0.$$

It follows form here that one can solve the equation $X_0 / X_r = \varepsilon_4$ relatively to t and represent

$$t = t_0 \varepsilon_4^{\frac{1}{\nu}} + \sum_{i \ge 1} t_i \varepsilon_4^{\frac{i}{\nu}} \in \Omega, \ t_i \in \overline{K_2}, \ t_0 \neq 0$$

$$x^{(\rho)} = x'_\rho + \sum_{i\geq 1} \beta_{\rho,i}\, \varepsilon_4^{\frac{i}{\nu}} \in \Omega\,,\ \beta_{\rho,i} \in \overline{K_2}$$

where the field Ω is the field of fration power series in ε_4 with coefficients in $\overline{K_2}$ Besides that, these expressions for $x^{(\rho)}$ in Ω are algebraic over K_2 since $\overline{K_2}(V_2) \supset \overline{K_2}(x^{(0)}\,/\,x^{(r)})$ is a finite extension of fields due to the fact that $X_0(V_2) \neq \{0\}$. Therefore, c.f. [3] paragraph (14), since ε_4 is the infinitely small value relatively to the field $K_2(\varepsilon_3)$ we conclude that these expressions for $x^{(\rho)}$, $0 \leq \rho \leq n$, give the solution of system (9) over the field $\overline{K_2(\varepsilon_3, \varepsilon_4)}$. Lemma is proved.

REMARK 4. Note that if $x' \in \overline{K}$ then $K_3 \subset \overline{K(\varepsilon_3, \varepsilon_4)}$, $\psi^{(1)} \in K(\varepsilon_3, \varepsilon_4)[Z]$. It follows from Remark 3.

(18) Return to the description of the auxiliary algorithm. Namely to the construction of $M_{s+1}, \ldots, M_n$,see paragraph (14). Enumerate $2(d-1)^{2s}+2(d-1)^s+1$ different values ε^* of ε_3 such that $l_{s+1,0} - \varepsilon^*$ are integers of the required size.

Apply Lemma 10 and construct all the irreducible components of U' and $U' \cap \{X_0 = 0\}$. Substitute "general points" of components of U' in the form $D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*}$ and check whether $D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*}$ is vanishing on any of these components , i.e. which is the same whether system (8) has a finite number of solutions in $\mathbb{P}^n(\overline{K_2})$. Substitute "general points" of components of $U' \cap \{X_0 = 0\}$ in the form $D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*}$ and check whether $D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*}$ is vanishing on any of these components. If $D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*}$ is not vanishing on any of these components then $W' \cap \{D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*} = D_{s+2} = \ldots = D_n = 0\} \cap \{X_0 = 0\} = \emptyset$ (respectively $\# W' \cap \{D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*} = D_{s+2} = \ldots = D_n = 0\} \cap \{X_0 = 0\} < +\infty$) in $\mathbb{P}^n(\overline{K_2})$ if (a) (respectively (b)) is satisfied.

By paragraph (14) there exists $\geq 2(d-1)^{2s}+1$ different values ε^* among enumerated such that system (8) has a finite number of solutions in $\mathbb{P}^n(\overline{K_2})$ and $W' \cap \{D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*} = D_{s+2} = \ldots = D_n = 0\} \cap \{X_0 = 0\} = \emptyset$ (respectively $\# W' \cap \{D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*} = D_{s+2} = \ldots = D_n = 0\} \cap \{X_0 = 0\} < +\infty$) in $\mathbb{P}^n(\overline{K_2})$ if (a) (respectively (b)) is satisfied.

For these values ε^* apply again Lemma 10, construct all the irreducible components of U and check whether $\# U \cap \mathbb{A}^n(\overline{K_2}) \geq N_3$. By Lemma 9 there exists a value ε_0^* among enumerated such that $N_2 \leq N_3 \leq \# U \cap \mathbb{A}^n(\overline{K_2}) < +\infty$ and and $W' \cap \{D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*} = D_{s+2} \ldots = D_n = 0\} \cap \{X_0 = 0\} = \emptyset$ (respectively $\# W' \cap \{D'_{s+1}\,|_{\varepsilon_3=\varepsilon^*} = D_{s+2} \ldots = D_n = 0\} \cap \{X_0 = 0\} < +\infty$) in $\mathbb{P}^n(\overline{K_2})$ if (a) (respectively (b)) is satisfied. We change $l_{s+1,0}$ for $l_{s+1,0} - \varepsilon_0^*$ and get new forms $D_{s+1}\,, \ldots, D_n$.

Applying the procedure described further to the second, third, ... coefficients of the forms $D_{s+1}\,, \ldots, D_n$, we get the required $M_{s+1}\,, \ldots, M_n$.

(19) Return to the description of the algorithm, see paragraph (13). Consider the case when $N_1 > N$, see paragraph (13). In this case using the auxiliary algorithm with condition (a) we change the forms $L_{s+1}\,, \ldots, L_n$ for $M_{s+1}\,, \ldots, M_n$ and return to the beginning of the algorithm for the considered s. We get $\#V_s \geq N_1 > N$ for new linear forms, i.e. the number of points of V_s, see paragraph (1), now is greater than it was.

(**20**) Show that if for the considered h for every x_j, $1 \leq j \leq N'$, there exists x_j^* and the number of solutions in $\mathbb{A}^n(\overline{K})$ of system (6) $N_1 = N_1(j) = N$ for every $1 \leq j \leq N'$, then

$$\dim\{h_1 = \ldots = h_s = h = 0\} = \dim\{h_1 = \ldots = h_s = 0\} - 1.$$

Indeed, it is sufficient to prove that h is not equal identically to zero on each component W_1 of the variety W'. Note that $W_1 \cap \{L_{s+1} = \ldots = L_n = 0\} \cap \mathbb{A}^n(\overline{K}) \neq \emptyset$ since W_1 is projective, $W' \cap \{L_{s+1} = \ldots = L_n = 0\} \cap \{X_0 = 0\} = \emptyset$ and $\dim W_1 = n - s$. So there exists $1 \leq j \leq N$ such that $x_j \in W_1$.

If $N' < j \leq N$ we have $h(x_j) \neq 0$, see paragraph (6), and the assertion is proved for W_1. If $1 \leq j \leq N'$ then by lemma 5 the polynomial h is not vanishing on some component W_2 of W such that $x_j \in W_2$. Suppose that h is equal identically to zero on W_1. Then by lemma 7 there exist two different points x' and x'' which are solutions of (6) and $x_{j,i} - x'_i, x_{j,i} - x''_i$ are infinitely small relatively to the field $\overline{K}$ for all $0 \leq i \leq n$. On the other side by lemma 6 for every $1 \leq j_1 \leq N$ there exists a solution x''' of system (6) such that $x''' \in W_1$ and $x'''_i - x_{j_1,i}$ are infinitely small relative to $\overline{K}$ for all $0 \leq i \leq n$. Therefore, system (6) has $\geq N+1$ solutions in $\mathbb{A}^n(\overline{K})$, since points $x_{j_1} \in \mathbb{P}^n(\overline{K})$. This leads to the contradiction. Thus, h is not equal identically to zero on W_1. The assertion is proved. We set in this case $h_{s+1} = h$.

(**21**) Show that if for every $h \in H$ there exists x_j, $1 \leq j \leq N' = N'(h)$ for which does not exist x_j^*, then

$$\dim\{f_0 = \ldots = f_m = 0\} = \dim\{h_1 = \ldots = h_s = 0\} = n - s.$$

Indeed, suppose that $\dim\{f_0 = \ldots = f_m = 0\} < n - s$. Let W_1 be the same as above. For each W_1 there exist at most m different $h \in H$ such that h is equal identically to zero on W_1. By Bézout's inequality the number of components W_1 is $\leq (d-1)^s$. So, there exists $h \in H$ such that h is not equal identically to zero on each component W_1. Then by lemma 5 for every x_j, $1 \leq j \leq N'$, there exists x_j^*. We get the contradiction. The assertion is proved.

(**22**) Let $s = n$. We shall enumerate $h \in H$. If there exists h such that $0 \notin h(V_n)$ then $\{f_0 = \ldots = f_m = 0\} \cap \mathbb{A}^n(\overline{k}) = \emptyset$ and $\dim\{f_0 = \ldots = f_m = 0\} \cap \mathbb{A}^n(\overline{k}) = -1$ and we set $h_{n+1} = h$. Otherwise $\dim\{f_0 = \ldots = f_m\} \cap \mathbb{A}^n(\overline{k}) = 0$.

(**23**) Return to paragraph (20). Let $h = h_0$ and W' be as above. We shall construct linear forms $L''_{s+2}, \ldots, L''_n$ in $X_0, \ldots, X_n$ with coefficients from $\mathbb{Z}$ of the size $O(n \log d)$ such that

$$W' \cap \{h = 0\} \cap \{L''_{s+1} = \ldots = L''_n = 0\}$$

is a finite set in $\mathbb{P}^n(\overline{k})$. Define the set

$$\mathcal{L} = \{ \sum_{1 \le i \le n-s} c^i L_{s+i} \,:\, c \in \mathbb{Z}, 1 \le c \le (d-1)^{s+1}(n-s)+1 \}.$$

We shall enumerate the elements $L \in \mathcal{L}$. Let

$$\tilde{W} = \{h_1 = \ldots = h_s = L = 0\} \subset \mathbb{P}^n(\overline{k})$$

be the variety of all common zeros of polynomials $h_1, \ldots, h_s, L$ in $\mathbb{P}^n(\overline{k})$ and $\tilde{W}'$ be the union of all the components W_1 of $\tilde{W}$ such that $W_1 \cap \mathbb{A}^n(\overline{k}) \neq \emptyset$. Show that $\tilde{W}' = W' \cap \{L = 0\}$. Indeed, one should only to check that $\dim W' \cap \{L = 0\} \cap \{X_0 = 0\} = \dim W' - 2$. But this fact follows from the equality $W' \cap \{L = 0\} \cap \{L_{s+2} = \ldots = L_n = 0\} \cap \{X_0 = 0\} = \emptyset$. The statement is proved.

Thus,

$$\tilde{W}' \cap \{L_{s+2} = \ldots = L_n = 0\} \cap \{X_0 = 0\} = \emptyset\,.$$

In particular each component W_1 of W has the dimension equal to $n-s-1$ in this case.

Apply the algorithm from paragraph (6), ..., (22), changing s for $s+1$ the polynomials $h_1, \ldots, h_s$ for $h_1, \ldots, h_s, L^{d-1}$, the forms $L_{s+1}, \ldots, L_n$ for $L_{s+2}, \ldots, L_n$ with $h = h_{s+1}$ (we just checked that it can be done). If we get

$$\dim \{h_1 = \ldots = h_s = L = h_{s+1} = 0\} \cap \mathbb{A}^n(\overline{k}) = n-s-1,$$

then go to the consideration of the next element $L \in \mathcal{L}$. Otherwise, set $L''_{s+2} = L$ and we have

$$\dim \{h_1 = \ldots = h_s = L''_{s+2} = h_{s+1} = 0\} \cap \mathbb{A}^n(\overline{k}) = n-s-2.$$

Note that such $L \in \mathcal{L}$ exists, since by Bézout's inequality there exists $\le (d-1)^{s+1}$ components W'' of the variety $\{h_1 = \ldots = h_{s+1} = 0\} \cap \mathbb{A}^n(\overline{k})$ and for each W'' there exists $\le n-s$ linear forms $L \in \mathcal{L}$ vanishing on W''.

Similarly sequentially for every $2 < i \le n-s-1$ construct $L''_{s+i} \in \mathcal{L}$ such that

$$\dim \{h_1 = \ldots = h_s = L''_{s+2} = \ldots = L''_{s+i} = h_{s+1} = 0\} \cap \mathbb{A}^n(\overline{k}) = n-s-i-1.$$

Thus, we get all the forms $L''_{s+2}, \ldots, L''_n$. It is fulfilled $W' \cap \{ L''_{s+2} = \ldots = L''_n = 0 \} \cap \{ L_{s+1} = 0 \} \cap \{ X_0 = 0 \} = \emptyset$. So the variety of dimension one $W' \cap \{ L''_{s+2} = \ldots = L''_n = 0 \}$ does not have irreducible components lying in $\{ X_0 = 0 \}$ and, therefore, $W' \cap \{ h_{s+1} = 0 \} \cap \{ L''_{s+2} = \ldots = L''_n = 0 \}$ is a finite set in $\mathbb{P}^n(\overline{k})$. The required property is satisfied.

(24) Let $n > s+1$. Now our aim is to construct linear forms $L^{(s+1)}_{s+2}, \ldots, L^{(s+1)}_n$, see paragraph (1)

Apply Lemma 10 when s is changed for $s+1$, polynomials $h_1, \ldots, h_s$ for $h_1, \ldots, h_s, h_{s+1}$ and $D_i = L''_i$, $s+2 \le i \le n$. Denote $\bar{W} = \{h_1 = \ldots =$

$h_s = h_{s+1} = 0\} \subset \mathbb{P}^n(\overline{k})$ and $\bar{W}'$ be the union of all the components W_1 of $\bar{W}$ such that $W_1 \cap \mathbb{A}^n(\overline{k}) \neq \emptyset$. Using Lemma 10 construct all the irreducible components S_1 of $U = \bar{W}' \cap \{L''_{s+2} = \ldots = L''_n = 0\}$ in $\mathbb{P}^n(\overline{k})$ and all the irreducible components S_2 of $U' = \bar{W}' \cap \{L''_{s+3} = \ldots = L''_n = 0\}$ in $\mathbb{P}^n(\overline{k})$ and S_3 of $U' \cap \{X_0 = 0\}$. Choose a linear form $L''_0 \in \mathcal{L}_1 = \{X_0 + cX_1 + \ldots + c^n X_n : 1 \leq c \leq n(d-1)^{s+1}+1,\ c \in \mathbb{Z}\}$ such that $L''_0(S_1) \neq 0$ for each component S_1 of U. Denote $N_4 = \#U \cap \mathbb{A}^n(\overline{k})$.

(25) Consider the case when $\dim U' \cap \{X_0 = 0\} = 0$. Choose a linear form $L \in \mathcal{L}_1 = \{X_0 + cX_1 + \ldots + c^n X_n : 1 \leq c \leq n(d-1)^{s+1}+1,\ c \in \mathbb{Z}\}$ such that $L(S_3) \neq 0$ for each component S_3 of $U' \cap \{X_0 = 0\}$.

Thus, we get $\bar{W}' \cap \{L = L''_{s+3} = \ldots = L''_n = 0\} \cap \{X_0 = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{k})$. The forms $L, L''_{s+3}, \ldots, L''_n$ satisfy to all the conditions which are required for $L^{(s+1)}_{s+2}, \ldots, L^{(s+1)}_n$ apart of the bound, may be, for the size of coefficients from $\mathbb{Z}$. So, if it nescessary, apply the auxiliary algorithm with condition (a), see paragraphs (14) and (18), changing s for $s+1$ the variety W' for $\bar{W}'$ and $D_{s+1}, \ldots, D_n$ for $L, L''_{s+3}, \ldots, L''_n$. We get the forms $M_{s+2}, \ldots, M_n$ with the required size of coefficients from $\mathbb{Z}$ such that $\bar{W}' \cap \{M_{s+2} = \ldots = M_n = 0\} \cap \{X_0 = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{k})$. Set $L^{(s+1)}_i = M_i$, $s+2 \leq i \leq n$ in this case when $\dim U' \cap \{X_0 = 0\} = 0$.

(26) Consider the case when $\dim U' \cap \{X_0 = 0\} = 1$ in this and next paragraphs. Choose and fix a component S_3 of $U' \cap \{X_0 = 0\}$ such that $\dim S_3 = 1$. Construct a point $x' \in S_3$, c.f. the proof of Lemma 10. Apply Lemma 11 changing s for $s+1$, the variety W' for $\bar{W}'$, polynomials $h_1, \ldots, h_s$ for $h_1, \ldots, h_s, h_{s+1}$ and find a point $x^* \in \bar{W}'$ in $\mathbb{P}^n(\overline{K_3})$ such that $\mathrm{st}\, x^* = x'$ relatively to some real structure. We shall consider below in paragraph (27) this real structure. By Remark 4 we have $K_3 \subset \overline{K(\varepsilon_3, \varepsilon_4)}$. Change the denotations $\varepsilon_3, \varepsilon_4$ for $\varepsilon_1, \varepsilon_2$. Then $K_3 \subset \overline{K(\varepsilon_1, \varepsilon_2)}$ and K_3 may play the role of K_2 in the conditions of the other lemmas.

(27) Find $\gamma_i \in K_3$ such that

$$(L''_i - \gamma_i L''_0)(x^*) = 0,\ s+2 \leq i \leq n.$$

Denote $M'_i = L''_i - \gamma_i L''_0$ for $s+2 \leq i \leq n$. Note that γ_i are infinitely small values relatively to the field K since in the considered real structure , see paragraph (27) , we have $\mathrm{st}\, x^* = x' \in \mathbb{P}^n(\overline{k})$.

Apply Lemma 8 (d) and (c) changing s for $s+1$, the variety W' for $\bar{W}'$, polynomials $h_1, \ldots, h_s$ for $h_1, \ldots, h_s, h_{s+1}$ when the forms $D_i = L''_i$, $\widetilde{D}_i = \gamma_i L''_0$, $s+2 \leq i \leq n$. We get that $N_4 = \#\bar{W}' \cap \{L''_{s+2} = \ldots = L''_n = 0\} \cap \mathbb{A}^n(\overline{k}) < \#\bar{W}' \cap \{M'_{s+2} = \ldots = M'_n = 0\} \cap \mathbb{A}^n(\overline{k}) = N_5 < +\infty$ since $x^* \in \bar{W}' \cap \{M'_{s+2} = \ldots = M'_n = 0\} \cap \mathbb{A}^n(\overline{k})$ but $\mathrm{st}\, x^* = x' \notin \bar{W}' \cap \{L''_{s+2} = \ldots = L''_n = 0\} \cap \mathbb{A}^n(\overline{k})$.

Apply Lemma 10 changing s for $s+1$, the variety W' for $\bar{W}'$, polynomials $h_1, \ldots, h_s$ for $h_1, \ldots, h_s, h_{s+1}$ the field K_2 for K_3 when the forms $D_i = M'_i$,

$s+2 \le i \le n$. Thus, construct all the irreducible components of $\bar{W}' \cap \{M'_{s+2} = \ldots = M'_n = 0\}$ in $\mathbb{P}^n(\overline{K_3})$.

Apply the auxiliary algorithm from paragraphs (14) and (18) with the condition (b) changing s for $s+1$, the variety W' for $\bar{W}'$, polynomials $h_1, \ldots, h_s$ for $h_1, \ldots, h_s$, h_{s+1} the field K_2 for K_3 when the forms $D_i = M'_i$ $s+2 \le i \le n$. The condition (b) is satisfied here by lemma 8 (c). Thus, construct forms $M_{s+2}, \ldots, M_n$ with the required size of coefficients from $\mathbb{Z}$ such that $\#\bar{W}' \cap \{M_{s+2} = \ldots = M_n = 0\} \cap \mathbb{A}^n(\overline{k}) \ge N_5$.

Change the forms $L''_{s+2}, \ldots, L''_n$ for $M_{s+2}, \ldots, M_n$ and return to the beginning of paragraph (24).

(28) We have $\#U \cap \mathbb{A}^n(\overline{k}) \le (d-1)^{s+1}$ for arbitrary forms $L''_{s+2}, \ldots, L''_n$ such that $\#U < +\infty$ by Bésout's inequality. So, there are at most $(d-1)^{s+1}$ returns from paragraph (27) to paragraph (24). Therefore, we shall construct linear forms $L^{(s+1)}_{s+2}, \ldots, L^{(s+1)}_n$ in the required time in paragraph (25).

Similarly there are at most $(d-1)^s$ returns from paragraph (19) to paragraph (1).

The required estimation for the working time of the all algorithm described follows directly from the estimations for the working time of the algorithms applied. Theorem 1 is proved.

References

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

[2] **Bourbaki N.:** *"Algèbre commutative"*, Chap. 1–7, Actualités Sci. Indust., nos. 1290, 1293, 1308, 1314, Paris 1961, 1964, 1965.

[3] **Chistov A. L.:** *"Polynomial–Time Computation of the Dimension of Algebraic Varieties in Zero–Characteristic"*, Research Report No. 8597-CS, Institut fuer Informatik der Universitaet Bonn, May 1993, 23 p.

[4] **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), pp. 124–188 (Russian) [English transl.: J. Sov. Math. 34 (4) (1986)].

[5] **Chistov A. L.:** *"Polynomial complexity of the Newton–Puiseux algorithm"*, (Lecture Notes in Computer Science, Vol. 233), Springer, New York, Berlin, Heidelberg, 1986, pp. 247–255.

[6] **Chistov A. L.:** *"Polynomial complexity algorithms for computational problems in the theory of algebraic curves"*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 176 (1989) pp. 127–150 (Russian).

[7] **Giusti M., Heintz J.:** *"La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial"* Preprint, Ecole Polytechnique, France et Univesidad de Buenos Aires, Argentina, Octobre 1991.

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

[9] **Lazard D.:** *"Résolution des systèmes d'équations algébrique"*, Theoretical Computer Science 15 (1981), pp. 77–110.

[10] **Milnor J.:** *"On Betti numbers of real varieties"*, Proceedings of the American Math. Soc. 15 (2) (1964), pp. 275–280.

[11] **Renegar J.:** *"A faster PSPACE algorithm for deciding the existential theory of reals"*, Proc. 29th Annual Symp. on Foundations of Computer Sci., October 24–26, 1988, pp. 291–295.