Polynomial–Time Computation of the Dimension of 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

May, 1993

Introduction

In the paper an algorithm is described for the computation of the dimension of an 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 $n+1$ variables. The working time of the algorithm is polynomial in the size of input and d^n. The problem of the computation of the dimension has attracted the attention of specialists for approximately ten years. In [3] 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 [6] 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 [6] 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.

In this paper we consider only the case of projective varieties but some modification of the method is also valid for the computation of the dimensiosn of affine varieties. These results afford to compute all the components of a given dimension

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

c of the variety in time polynomial in $d^{(c+1)(n-c)}$ and the size of input which proves the hypothesis from [3]. We are going to present these algorithms in next papers.

By constructing the algorithm in this work the technics of the real algebraic geometry is essentially used. Here the result from [10] is crucial which in its turn is based on the result of [9], see below section 2. We consider algebraically closed fields but for them the existance of the automorphism of the complex conjugation is essential or more generally of the conjugation over a really closed subfield, see section 1.

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 find 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 $k = \mathbb{Q}(\approx_{\nVdash}, \ldots, \approx_{\leqslant}, \theta)$ be the field where $t_1, \ldots, t_l$ are algebraaically independant over the field $\mathbb{Q}$ and θ is algebraic over $\mathbb{Q}(\approx_{\nVdash}, \ldots, \approx_{\leqslant})$ with the minimal polynomial $F \in \mathbb{Q}[\approx_{\nVdash}, \ldots, \approx_{\leqslant}, \mathbb{Z}]$ and leading coefficient $lc_Z F$ of F is equal to 1. Let homogeneous polynomials $f_0, \ldots, f_m \in k[X_0, \ldots, X_n]$ be given. Consider the closed algebraic set or which is the same in this paper the algebraic variety

$$V = \{(x_0, \ldots, x_n) : f_i(x_0, \ldots, x_n) = 0 \ \forall 0 \leq i \leq m\} \subset \mathbb{P}^{\aleph}(\bar{\nexists}) .$$

This is a set of all common zeros of polynomials $f_0, \ldots, f_m$ in $\mathbb{P}^{\aleph}(\bar{\nexists})$, 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 present each polynomial $f = f_i$ in the form

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

where $a_0, a_{i_1, \ldots, i_n, j} \in \mathbb{Z}[\approx_{\nVdash}, \ldots, \approx_{\leqslant}]$, $\gcd_{\beth_{\nVdash}, \ldots, \beth_{\aleph}, \daleth}(\eth_{\nVdash}, \eth_{\beth_{\nVdash}, \ldots, \beth_{\aleph}, \daleth}) = \nVdash$. We define the length $l(a)$ of an integer a by the formula $l(a) = \min\{s \in \mathbb{Z} : |\eth| < \nVdash^{\sim - \nVdash}\}$. 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 $a_0, a_{i_1, \ldots, i_n, j}$. By definition

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

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

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

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

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

REMARK. 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 [3].

1 Constructing a real structure on the constant field

In this section l is not fixed. Let $k_1 = \mathbb{Q}(\approx_\nVdash, \ldots, \approx_\lessdot)[\eta]$ be some algebraic extension of k, where the element η has minimal polynomial $\varphi \in \mathbb{Q}[\approx_\nVdash, \ldots, \approx_\lessdot, \mathbb{Z}]$, $lc_Z \varphi = 1$, $l(\varphi) < M_2$ and $\deg_{t_\alpha} \varphi$, $\deg_Z \varphi < D_1$ for all α. Our aim is to construct a real structure on k_1. By the real structure we mean an embedding $k_1 \subset k_2(\sqrt{-1})$, where k_2 is a real ordered field, see [1].

Compute the discriminant

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

Find consequently $z_1, \ldots, z_l \in \mathbb{Q}$ such that $\Delta(z_1, \ldots, z_i, t_{i+1}, \ldots, t_n) \neq 0$. One can find $0 \leq z_i \leq 2D_1^2$, $z_i \in \mathbb{Z}$. The polynomial $\overline{\varphi} = \varphi(z_1, \ldots, z_l, Z) \in \mathbb{Q}[\mathbb{Z}]$ is separable, since $\Delta(z_1, \ldots, z_l) \neq 0$. Suppose that $\overline{\varphi}$ has not only real roots. In this case we shall find

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

(ii) polynomials $R_1, I_1 \in \mathbb{Q}[\mathbb{Z}]$ with $\deg_Z R_1, \deg_Z I_1 < \deg_Z \overline{\Psi}$, such that for a chosen not real root $\overline{\eta}$ of $\overline{\varphi}$ we have $\overline{\eta} = R_1(\overline{\xi}) + \sqrt{-1}\, I_1(\overline{\xi})$ in the field $\mathbb{Q}[\overline{\xi}, \sqrt{-\nVdash}]$.

Let $\overline{\varphi}_1 = \overline{\varphi}/(Z - \overline{\eta}) \in \mathbb{Q}[\overline{\eta}][\mathbb{Z}]$ and $\overline{A} = \mathbb{Q}[\overline{\eta}, \overline{\eta}_\nVdash \sqrt{-\nVdash}] = \mathbb{Q}[\overline{\eta}][\mathbb{Z}, \mathbb{Z}_\nVdash]/(\overline{\varphi}_\nVdash, \mathbb{Z}_\nVdash^\nVdash + \nVdash)$ 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 $\mathbb{Q}[\overline{\approx}_{\not\Vdash}, \overline{\approx}_{\not\Vdash}]$ over $\mathbb{Q}$. One can find $1 \le c \le 2D_1^2$, $c \in \mathbb{Z}$. Find the minimal polynomial $\overline{\Phi} \in \mathbb{Q}[\mathbb{Z}]$, $lc_Z\overline{\Phi} = 1$, of the element $\overline{v}$ over $\mathbb{Q}$ and polynomials $R_2, I_2 \in \mathbb{Q}[\mathbb{Z}]$; $\deg R_2, \deg I_2 < \deg\overline{\Phi}$, 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 $\overline{\Phi}_j \in \mathbb{Q}[\mathbb{Z}], lc_Z\overline{\Phi}_j = 1$. Set $\mathbb{Q}[\xi_{\mathtt{J}}, \sqrt{-\Vdash}] = \mathbb{Q}[\mathbb{Z}, \mathbb{Z}_{\not\Vdash}]/(\overline{\lesssim}_{\mathtt{J}}, \mathbb{Z}_{\not\Vdash}^{\not\Vdash}+\Vdash)$, 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 existance of γ follows immediately from the construction and the fact that $\overline{\eta}$ is not a real root of $\overline{\varphi}$. Finitely, we 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 $\overline{\varphi}$ has a real root $\overline{\eta}$ we can also take $\overline{\xi} = \overline{\nu}$, $\overline{\Psi} = \overline{\varphi}$, $R_1 = Z$, $I_1 = 0$. 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

$$\eta = \eta_0 + \sum_{(i_1,\dots,i_l)>(0,\dots,0)} \eta_{i_1,\dots,i_l} u_1^{i_1}\cdots u_l^{i_l} \in \mathbb{Q}[\overline{\eta}][[\approx_{\not\Vdash}, \dots, \approx_{\lessdot}]],$$

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

Define elements

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

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 $\varphi_1 = \varphi/(Z-\eta) \in \mathbb{Q}[\eta][\mathbb{Z}] \subset \mathbb{Q}[\overline{\xi}, \sqrt{-\Vdash}][[\approx_{\not\Vdash}, \dots, \approx_{\lessdot}]][\mathbb{Z}]$, since $\varphi \in \mathbb{Q}[\approx_{\not\Vdash}, \dots, \approx_{\lessdot}, \mathbb{Z}]$.

Set $\xi = \eta^{(1)} + c\eta^{(2)}$ where c is the same as for $v = v_1 + cv_2$, see above. Our aim now is to construct the minimal polynomial $\Psi \in \mathbb{Q}[\approx_{\not\Vdash}, \dots, \approx_{\lessdot}, \mathbb{Z}]$ of the element ξ and find $R, I \in \mathbb{Q}(\approx_{\not\Vdash}, \dots, \approx_{\lessdot})[\mathbb{Z}]$, $\deg_Z R, \deg_Z I < \deg_Z \Psi$, such that $\eta^{(1)} = R(\xi)$, $\eta^{(2)} = I(\xi)$ (we shall prove that such polynomials exist). So $\eta = R(\xi) + \sqrt{-1}\, I(\xi)$.

Let $m = (t_1 - z_1, \dots, t_l - z_l)$ be the maximal ideal of $\mathbb{Q}[\approx_{\not\Vdash}, \dots, \approx_{\lessdot}]$ generated by $t_1 - z_1, \dots, t_l - z_l$, $S = \mathbb{Q}[\approx_{\not\Vdash}, \dots, \approx_{\lessdot}]\backslash\gg$ and $B = S^{-1}\mathbb{Q}[\approx_{\not\Vdash}, \dots, \approx_{\lessdot}]$ the local ring. Let

$$A = B[\eta, \eta_1, \sqrt{-1}\,] = B[\eta][Z, Z_1]/(\varphi_1, Z_1^2+1),$$

where $\eta_1 = Z \bmod (\varphi_1, Z_1^2+1)$, $\sqrt{-1} = Z_1 \bmod (\varphi_1, Z_1^2+1)$. Therefore, we have $\overline{A} = A/mA$, $\overline{\eta} = \eta \bmod mA$, $\overline{\eta}_1 \bmod mA$.

Let $v_1 = \frac{1}{2}(\eta + \eta_1)$, $v_2 = \frac{1}{2\sqrt{-1}}(\eta - \eta_1)$, $v = v_1 + cv_2$, $v_1, v_2, v \in A$. Find the minimal polynomial $\Phi \in \mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})[\mathbb{Z}]$, $lc_Z \Phi = 1$, of the element v over $\mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})$.

Note that $\Phi \in \mathbb{Q}[\approx_{\not k}, \ldots, \approx_{\leqslant}, \mathbb{Z}]$ since v is integral over $\mathbb{Q}[\approx_{\not k}, \ldots, \approx_{\leqslant}]$ and this ring is integrally closed, see 2. Therefore, $\Phi(z_1, \ldots, z_l, \overline{v}) = 0$, since $\overline{A} = A/mA$ and $\overline{v} = v \bmod mA$. So $\deg_Z \Phi \geq \deg_Z \overline{\Phi}$.

On the other hand $\deg_Z \Phi$ coincides with the number of different elements

$$\frac{1}{2}(\eta' + \eta_1') + \frac{c}{\pm 2\sqrt{-1}}(\eta' - \eta_1'),$$

where η', η_1' are different roots of φ in $\overline{\mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})}$. The degree δ of $B[v_1, v_2] \otimes_B \mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})$ over $\mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})$ is equal to the number of different pairs

$$\left(\frac{1}{2}(\eta' + \eta_1'), \frac{1}{\pm 2\sqrt{-1}}(\eta' - \eta_1')\right).$$

So $\delta = \deg_Z \varphi(\deg_Z \varphi - 1)$ and $\deg_Z \Phi \leq \delta$. Similarly the degree $\overline{\delta} = [\mathbb{Q}[\overline{\approx}_{\not k}, \overline{\approx}_{\not k}] : \mathbb{Q}] = \deg_{\mathbb{Z}} \overline{\varphi}(\deg_{\mathbb{Z}} \overline{\varphi} - \not k)$ and $\deg \overline{\Phi} = \overline{\delta}$, since $\overline{v}$ is a primitive element of $\mathbb{Q}[\overline{\approx}_{\not k}, \overline{\approx}_{\not k}]$ over $\mathbb{Q}$. We have $\deg_Z \varphi = \deg_Z \overline{\varphi}$. Thus, $\overline{\delta} = \delta \geq \deg_Z \Phi \geq \deg_Z \overline{\Phi} = \overline{\delta}$. Therefore $\deg_Z \Phi = \deg_Z \overline{\Phi}$ and $\Phi(z_1, \ldots, z_l, Z) = \overline{\Phi}$. Besides that, v is a primitive element of $B[v_1, v_2] \otimes_B \mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})$ over $\mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})$. Therefore, there exist polynomials $R_3, I_3 \in \mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})[\mathbb{Z}]$, $\deg_Z R_3, \deg_Z I_3 < \deg_Z \Phi$ such that $R_3(v) = v_1$, $I_3(v) = v_2$. We find these polynomials R_3, I_3.

Let $\Delta_1 = \mathrm{Res}_Z(\Phi, \Phi_Z') \in \mathbb{Q}[\approx_{\not k}, \ldots, \approx_{\leqslant}]$ be the discriminant of Φ. Then $\Delta_1 R_3$ and
$\Delta_1 I_3 \in \mathbb{Q}[\approx_{\not k}, \ldots, \approx_{\leqslant}, \mathbb{Z}]$, since v_1 and v_2 are integral over $\mathbb{Q}[\approx_{\not k}, \ldots, \approx_{\leqslant}]$, see 2. Note that $\Delta_1(z_1, \ldots, z_l) = \mathrm{Res}_Z(\overline{\Phi}, \overline{\Phi}_2') \neq 0$. So $R_3 \mid_{t_1 = z_1, \ldots, t_l = z_l}, I_3 \mid_{t_1 = z_1, \ldots, t_l = z_l}$ are defined and coincide with R_1, I_1 since $\overline{v} = v \bmod mA$, $\overline{v}_1 = v_1 \bmod mA$, $\overline{v}_2 = v_2 \bmod mA$.

Factor $\Phi = \prod_i \Phi_i$, see 3, into the product of irreducible over $\mathbb{Q}(\approx_{\not k}, \ldots, \approx_{\leqslant})$ polynomials $\Phi_i \in \mathbb{Q}[\approx_{\not k}, \ldots, \approx_{\leqslant}, \mathbb{Z}]$, $lc_Z \Phi_i = 1$. Find i_0 such that $\overline{\Psi}$ divides $\Phi_{i_0}(z_1, \ldots, z_l,$
$Z)$. We set $\Psi = \Phi_{i_0}$ and R, I to be the residues of the division of R_3, I_3 by Φ_{i_0}.

Show that $\Psi(\xi) = 0$. Indeed, $\Phi(\xi) = 0$, since η and $\tilde{\eta}$ are different roots of φ, see above, and $\xi = \frac{1}{2}(\eta + \tilde{\eta}) + \frac{c}{2\sqrt{-1}}(\eta - \tilde{\eta})$. So there exists a unique index i_1 such that $\Phi_{i_1}(\xi) = 0$. This equality can be considered as an equality in the ring $\mathbb{Q}[\overline{\xi}, \sqrt{-\not k}][[\approx_{\not k}, \ldots, \approx_{\leqslant}]]$. Therefore, $\Phi_{i_1}(z_1, \ldots, z_l, \overline{\xi}) = 0$ and $i_0 = i_1$, $\Psi = \Phi_{i_1}$, since $\overline{\Phi}$ is separable.

We have

$$\begin{aligned} \eta &= R_3(\xi) + \sqrt{-1}\, I_3(\xi) \\ \tilde{\eta} &= R_3(\xi) - \sqrt{-1}\, I_3(\xi), \end{aligned}$$

since there exists an epimorphism $A \to B[\eta, \tilde{\eta}, \sqrt{-1}]$, such that $\eta \mapsto \eta$, $\eta_1 \mapsto \tilde{\eta}$, and, therefore, $v \mapsto \xi$, $v_1 \mapsto \frac{1}{2}(\eta + \tilde{\eta})$, $v_2 \mapsto \frac{1}{2\sqrt{-1}}(\eta - \tilde{\eta})$. Hence,

$$\begin{aligned} \eta &= R(\xi) + \sqrt{-1}\, I(\xi) \\ \tilde{\eta} &= R(\xi) - \sqrt{-1}\, I(\xi). \end{aligned}$$

The polynomial $\Psi(z_1, \ldots, z_l, Z)$ is separable since it divides $\overline{\Phi}$. So by Hensel's lemma the element ξ can be represented as a series

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

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

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

Thus we have constructed the required polynomial Ψ, R, I in the case when $\overline{\eta}$ is not real. If $\overline{\eta}$ is real we 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 $k_2 = \mathbb{Q}(\approx_{\not\perp}, \ldots, \curvearrowright_{\not<})[\xi]$. Consider the embedding $k_2 \subset \mathbb{Q}[\overline{\xi}]((\cong_{\not\perp}, \ldots, \cong_{\not<})) = \urcorner_{\not\perp}$ which is determined by (1). The order on k_2 will be induced by the order on the field of formal power series $\mathbb{Q}[\overline{\xi}]((\cong_{\not\perp}, \ldots \cong_{\not<}))$ or equivalently on the ring of formal power series $\mathbb{Q}[\overline{\xi}][[\approx_{\not\perp}, \ldots, \approx_{\not<}]]$. The monomials $t^{i_1} \cdots t_l^{i_l}$ 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 x such that $i_1 = j_1, \ldots, i_{x-1} = j_{x-1}$ and $i_x < j_x$. An element $\alpha \in \mathbb{Q}[\overline{\xi}][[\approx_{\not\perp}, \ldots, \approx_{\not<}]]$ 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 resume the results obtained in the following

LEMMA 1. For the field k_1 an embedding of fields over $\mathbb{Q}(\approx_{\not\perp}, \ldots, \approx_{\not<})$ can be constructed

$$k_1 = \mathbb{Q}(\approx_{\not\perp}, \ldots, \approx_{\not<})[\eta] \subset \mathbb{Q}(\approx_{\not\perp}, \ldots, \approx_{\not<})[\xi, \sqrt{-\not\perp}],$$

where ξ is an algebraic element over $\mathbb{Q}(\approx_{\not\perp}, \ldots, \approx_{\not<})$ with minimal polynomial $\Psi \in \mathbb{Q}[\approx_{\not\perp}, \ldots, \approx_{\not<}, \mathbb{Z}]$, $lc_Z \Psi = 1$ and

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

with $R(Z), I(Z) \in \frac{1}{\Delta_2}\mathbb{Q}[\approx_{\not\perp}, \ldots, \approx_{\not<}][\mathbb{Z}]$, $\Delta_2 = \mathrm{Res}_Z(\Psi, \Psi'_Z)$ 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 $\mathbb{Q}(\approx_{\not<}, \ldots, \approx_{<})[\xi]$ the order of a real ordered field is constructed. The working time of constructing Ψ, R, I and the order on $\mathbb{Q}(\approx_{\not<}, \ldots, \approx_{<})[\xi]$ is polynomial in D_1^l and M_2.

PROOF. The fact that $R, I \in \frac{1}{\Delta_2}\mathbb{Q}[\approx_{\not<}, \ldots, \approx_{<}, \mathbb{Z}]$ is proved similarly to that $R_3, I_3 \in \frac{1}{\Delta_1}\mathbb{Q}[\approx_{\not<}, \ldots, \approx_{<}, \mathbb{Z}]$, see above. The bounds for degrees, length and the working time follow immediately from the description of the algorithm. All the other statements were proved above.

LEMMA 2. Let $\omega \in \mathbb{Q}(\approx_{\not<}, \ldots, \approx_{<})[\xi]$, $\omega = \frac{1}{c}\sum_{0\le j\le \deg\Psi} c_j\xi^j$, where $c, c_j \in \mathbb{Z}[\approx_{\not<}, \ldots, \approx_{<}]$, $\deg_{t_\alpha} c, \deg_{t_\alpha} c_j < D$, $l(c), l(c_j) < M_3$ for all α, j. Then one can ascertain whether $\omega > 0$ within time polynomial in D_1^l, D^l, M_2, M_3.

PROOF. Changing ω for ωc^2 we can suppose that $c = 1$. The minimal polynomial $H(Z)$ of the element ω over $\mathbb{Q}(\approx_{\not<}, \ldots, \approx_{<})$ belongs to $\mathbb{Q}[\approx_{\not<}, \ldots, \approx_{<}, \mathbb{Z}]$ and $\deg_{t_\alpha} H = \delta_\alpha < \mathcal{P}(D, D_1)$ and $l(H) < (M_1 + M_2 + l)\mathcal{P}(D, D_1)$ for some polynomial $\mathcal{P}$, $\deg_Z H \le 2D_1^2$ for all α.

Let $\omega_{j_1,\ldots,j_l} u_1^{j_1}\cdots u_l^{j_l}$ be the maximal monomial of ω considered as an element of k_3. Show that $j_1 \le \delta_1, \ldots, j_l \le \delta_l$ and $\omega_{j_1,\ldots,j_l} \in \mathbb{Q}[\overline{\xi}]$ is one of the roots of the polynomial

$$((\cdots(H(Zu_1^{j_1}\cdots u_l^{j_l})/u_1^{\beta_1})\,|_{t_1=z_1}\cdots)/u_l^{\beta_l})\,|_{t_l=z_l},$$

where $\beta_1, \ldots, \beta_l$ are choosen maximal, such that after the cancellation to $u_i^{\beta_i}$ one obtains a polynomial from $\mathbb{Z}[\approx_{\not<}, \ldots, \approx_{<}][\mathbb{Z}]$.

Indeed, let $H = H_1(u_1, \ldots, u_l, Z)$ for some polynomial $H_1 \in \mathbb{Q}[\approx_{\not<}, \ldots, \approx_{<}, \mathbb{Z}]$. Considering Newton's polygon of H_1 relatively (Z, u_1) we get $j_1 \le \delta_1$, see e.g. [4]. Denote $H_2 = (H_1(Zu_1^{j_1})/u_1^{\beta_1})\,|_{t_1=z_1}$. We have $\deg_{t_\alpha} H_2 \le \deg_{t_\alpha} H_1$, $\alpha > 1$, $\deg_Z H_2 \le \deg_Z H_1$, $l(H_2) \le l(H_1)$ and $\omega_{j_1,\ldots,j_l} u_2^{j_2}\cdots u_l^{j_l}$ is a maximal monomial of H_2. Therefore, by induction we ascertain the required statements.

Thus, we can construct $\omega_{j_1,\ldots,j_l}$ in the required time and check whether $\omega_{j_1,\ldots,j_l} > 0$ within the same time; Lemma is proved.

Below we shall need the following

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 $\xi^* = \xi, R^* = R, I^* = I, \Psi^* = \Psi$.

PROOF. Suppose that the following requirements are satisfied:

(a) $\Delta(z_1^*, \ldots, z_l^*) \ne 0$,

(b) $\Delta_1(z_1^*, \ldots, z_l^*) \ne 0$,

(c) there exists a real root $\tilde{\xi}$ of the polynomial $\Psi(z_1^*, \ldots, z_l^*, Z)$.

Then we set $\overline{\eta}^* = (R\mid_{t_1=z_1^*,\ldots,t_l=z_l^*})(\tilde{\xi}) + \sqrt{-1}(I\mid_{t_1=z_1^*,\ldots,t_l=z_l^*}(\tilde{\xi})$ (it can be computed due to (b)). We have $\varphi(R(\xi) \pm \sqrt{-1}\, I(\xi)) = 0, \xi = R(\xi) + cI)\xi)$. So $\varphi(z_1^*, \ldots, z_l^*, \overline{\eta}^*) = 0$. Let $\overline{\xi}^*$ correspond to $\overline{\xi}$ in our construction when $\overline{\eta}^*$ corresponds to $\overline{\eta}$. Then we have $\overline{\xi}^* = \tilde{\xi}$ and by the uniqueness in Hensel's lemma $\xi^* = \xi, \Psi^* = \Psi, R^* = R$.

Note that in the assumptions of the Lemma (a), (b), and (c) are satisfied for some polynomial $\mathcal{P}$. Lemma is proved.

Remind that the field $\mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})$ has the order induced by the linear order on monomials $u_1^{j_1} \ldots u_l^{j_l}$ described above. Denote by $\mathbb{Q}(\approx_{\not\kappa}, \ldots^{\hbar}, \approx_{\leqslant})$ the real closure of the field $\mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})$ with this fixed order.

LEMMA 4. The construction of this section gives all the possible real structures of the field $\mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})[\eta]$ when $\mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})$ is a real ordered field with the fixed order decribed above. More exactly, for every embedding $\beta : \mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})[\eta] \to \mathbb{Q}(\approx_{\not\kappa}, \ldots^{\hbar}, \approx_{\leqslant})[\sqrt{-\not\kappa}]$ there exists an embedding

$$\beta_1 : \mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})[\eta] \to \mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})[\xi, \sqrt{-\not\kappa}]$$

from Lemma 1 and an embedding

$$\beta_2 : \mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})[\xi] \to \mathbb{Q}(\approx_{\not\kappa}, \ldots^{\hbar}, \approx_{\leqslant})$$

of real ordered fields which induces the embedding

$$\beta_2' : \mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})[\xi] \to \mathbb{Q}(\approx_{\not\kappa}, \ldots^{\hbar}, \approx_{\leqslant})[\sqrt{-\not\kappa}]$$

such that $\beta = \beta_2' \circ \beta_1$ (all embeddings over $\mathbb{Q}(\approx_{\not\kappa}, \ldots, \approx_{\leqslant})$).

The arbitrariness of the construction of this section consists in the choice of the root $\overline{\eta}$ of the polynomial $\overline{\varphi}$.

PROOF. Follows directly from the description of $\mathbb{Q}(\approx_{\not\kappa}, \ldots^{\hbar}, \approx_{\leqslant})$ as a field of multiple fraction–power series over real closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$, see e.g. [1].

2 Solving an auxiliary system over the field of real numbers

In this section by the proof of Lemma 5 we follow [10]. The proof of the analogue of Lemma 5 in [10] is based in its turn on the idea from [9]. We give proofs of Lemmas 5 and 6 for the completeness, their statements are slightly different from [10].

Let $f_1, \ldots, f_m \in \mathbb{R}[\mathbb{X}_{\not\kappa}, \ldots, \mathbb{X}_{\aleph}]$, $0 < \delta < \mathbb{R}$, $\deg f_i < d$, $1 \leq i \leq m$, $d \in \mathbb{Z}$. Consider the system with an inequality

$$f_1 = \ldots = f_m = 0,\ \delta - \sum_{1 \leq i \leq n} X_j^2 \geq 0 \tag{2}$$

Let $0 < \varepsilon \in \mathbb{R}$, $\varepsilon\delta^{d+1} < 1$. Consider also the following inequalities

$$g = (\delta - \sum_{1\le j\le n} X_j^2 + \varepsilon)(\varepsilon - \sum_{1\le i\le m} f_i^2) - \varepsilon^3 \sum_{1\le j\le n} X_j^{2d+2} > 0 \tag{3}$$

$$\delta - \sum_{1\le j\le n} X_j^2 \ge -\varepsilon, \quad \sum_{1\le i\le m} f_i^2 \le \varepsilon \tag{4}$$

LEMMA 5. (cf. [10]) Let system (2) have a solution. Then there exists a sequence $\{\varepsilon_i\}_{i=0}^{\infty}$, $0 < \varepsilon_i \in \mathbb{R}$, which tends to zero, such that for every i the system of equations in $X_1, \ldots, X_n$

$$\left.\frac{\partial g}{\partial X_1}\right|_{\varepsilon=\varepsilon_1} = \ldots = \left.\frac{\partial g}{\partial X_n}\right|_{\varepsilon=\varepsilon_i} = 0 \tag{5}$$

has a solution $x^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)}) \in \mathbb{R}^{\aleph}$ and the sequence $\{x^{(i)}\}_{i=0}^{\infty}$ tends to some solution $x = (x_1, \ldots, x_n) \in \mathbb{R}^{\aleph}$ of system (2).

PROOF. It follows from (2) that $\sum_j X_j^{2d+2} \le \delta^{d+1}$. (2) implies (3), since $\varepsilon^2 > \varepsilon^3\delta^{d+1}$. (2) implies (4).

Show that for each connected component W of solutions of (3) which contains some solution ξ of (2), also (4) is satisfied, i.e. every $\xi_1 \in W$ is a solution of (4).

Indeed, since W is a component of solutions of (3), functions $\delta - \sum_j X_j^2 + \varepsilon$ and $\sum_i f_i^2 - \varepsilon$ can not have zeros on W. So they have the same sign for all $\xi_1 \in W$, since W is connected. We have $\delta - \sum_j X_j^2 + \varepsilon > 0$, $\sum_i f_i^2 - \varepsilon < 0$ in the point ξ. Therefore, these inequalities are satisfied for all $\xi_1 \in W$, i.e. (4) is satisfied for all $\xi_1 \in W$.

Each connected component of solutions of (4) is bounded. Therefore, each connected component W of solutions of (3), which contains some solution of (2), is also bounded. Therefore, there exists a local maximum ξ_2 of g in the domain W. In the point ξ_2 the equality grad $g = 0$ is satisfied.

Connected components of solutions of (4) tend to connected components of solutions of (2) in the sense that for every $\tau > 0$ there exists $\sigma > 0$ such that for every $0 < \varepsilon < \sigma$ the τ–neighbourhood of the connected component W_1 of solutions (2) contains the connected component W_2 of solutions of (4) such that $W_2 \subset W_1$. From here the assertion of the Lemma follows immediately.

Now let ε be transcentental over $\mathbb{R}$. Consider the following system

$$\frac{\partial g}{\partial X_1} = \ldots = \frac{\partial g}{\partial X_n} = 0 \tag{6}$$

in the variables $\varepsilon, X_1, \ldots, X_n$. Let the set of zeros of 6 be $V \subset (\mathbb{A}^{\aleph} \times \mathbb{A}^{\aleph})(\mathbb{C})$ over the field $\mathbb{C}$. Denote by $\pi : \mathbb{A}^{\aleph} \times \mathbb{A}^{\aleph} \to \mathbb{A}^{\aleph}$ the projection to the second factor.

Let $U = V \backslash \{\varepsilon = 0\}$ be an open subset of V and $U(\mathbb{R})$ subset of U consisting of points with real coordinates, $\overline{U}$ and $\overline{U(\mathbb{R})}$ be closures of U and $U(\mathbb{R})$ respectively in the Zariski topology.

LEMMA 6. (c.f.[10])

(a) The set $\overline{U} \cap \{\varepsilon = 0\}$ is finite.

(b) If system (2) has some solution over $\mathbb{R}$ then there exists $\xi \in \pi(\overline{U(\mathbb{R})} \cap \{\varepsilon = 0\})$ which satisfies (2). This assertion is also true in the classic topology.

PROOF. Set $\varepsilon = \varepsilon_1/\varepsilon_0$, $X_i = Z_i/Z_0$, $1 \le i \le n$, and consider the homogeneous relatively $(\varepsilon_1, \varepsilon_0), (Z_0, \ldots, Z_n)$ system corresponding to (6), which is obtained from (6) by the given above substitution and multiplication to the least common denominator. Let we get the following system

$$g_1 = \ldots = g_n = 0 \tag{7}$$

It defines the set of solutions $W \subset (\mathbb{P}^{\not\kappa} \times \mathbb{P}^{\kappa})(\mathbb{C})$. Let $W = \bigcup_i W_i$ be the decomposition of W into irreducible components over $\mathbb{C}$. Denote by $\pi_1 : \mathbb{P}^{\not\kappa} \times \mathbb{P}^{\kappa} \to \mathbb{P}^{\not\kappa}$ the projection to the first factor. Then $\pi_1(W_i) = \mathbb{P}^{\not\kappa}$ or some point in $\mathbb{P}$ for every i. Show that if $\pi_1(W_i) = \mathbb{P}^{\not\kappa}$ then $\dim W_i = 1$. Indeed, $\emptyset \neq W_i \cap \{\varepsilon_0 = 0\} \subset \{(2d+2)Z_i^{2d+1} = 0, i = 1, \ldots, n\} \cap \{\varepsilon_0 = 0\} = \{p_0\}$, where p_0 is a point. So, $\dim W_i \le 1$ and, therefore, $\dim W_i = 1$.

We have $V \subset W$. Denote by $\overline{V}$ the closure of V in $\mathbb{P}^{\not\kappa} \times \mathbb{P}^{\kappa}$. Let $\overline{V} = \bigcup_j \overline{V}_j$ be the decomposition of $\overline{V}$ into irreducible components. Each component of $\overline{V}$ is also the component of W, and each component of W which is not contained in some hyperplane $\{\varepsilon_1 = c\,\varepsilon_0\}$, $c \in \mathbb{C}$, is the component of $\overline{V}$. This follows from the fact that $p_0 \in \mathbb{P}^{\not\kappa} \times \mathbb{A}^{\kappa}$.

Thus, we have proved that $\overline{W \backslash \{\varepsilon_1 = 0\}} \cap \{\varepsilon_1 = 0\}$ is finite. Therefore, $\overline{U} \cap \{\varepsilon = 0\}$ is finite, since $\overline{U} \subset \overline{W \backslash \{\varepsilon_1 = 0\}}$. The second assertion of the lemma follows from the Lemma 5.

COROLLARY

(a) Let W' (respectively $V', \overline{V}', U'$) denotes the union of all the components of W (respectively $V, \overline{V}, U$) which are not contained in some hyperplane $\{\varepsilon_1 = c\,\varepsilon_0\}$, $c \in \mathbb{C}$. Then $W' = \overline{V}' = \overline{V'}$, $V' = W' \cap \mathbb{A}^{\not\kappa} \times \mathbb{A}^{\kappa}$, $U' = V' \cap \{\varepsilon \neq 0\}$, $V' \subset \overline{U}$.

(b) We can consider (7) as a system over the field $\mathbb{C}(\varepsilon)$ in the variables $X_1, \ldots, X_n$ with the variety of solutions $\mathcal{W}$. Then irreducible over $\mathbb{C}(\varepsilon)$ components of $\mathcal{W}$ correspond bijectively to the irreducible over $\mathbb{C}$ components of W'.

PROOF. We need only to prove (b). But this general fact can be obtained by the localization of the rings of regular functions $\mathbb{C}[\mathbb{W} \cap \{\mathbb{Z}_\alpha \neq \curlyvee, \varepsilon\curlyvee \neq \curlyvee\}] = \mathbb{A}_\alpha$, $0 \leq \alpha \leq n$, relatively to the multiplicatively closed set $S = \mathbb{C}[\varepsilon]\backslash\{\curlyvee\}$, c.f. [3]. Irreducible components of $W' \cap \{Z_\alpha \neq 0, \varepsilon_0 \neq 0\}$ correspond bijectively to the minimal prime ideals of A_α which do not intersect S, i.e. to the minimal prime ideals of $S^{-1}A_\alpha = \mathbb{C}(\varepsilon)[\mathcal{W} \cap \{\mathbb{Z}_\alpha \neq \curlyvee, \varepsilon\curlyvee \neq \curlyvee\}]$ and, therefore, to the irreducible components defined over $\mathbb{C}(\varepsilon)$ of the variety $\mathcal{W} \cap \{Z_\alpha \neq 0, \varepsilon \neq 0\}$. This gives the required independnt of α bijection. The corollary is proved.

LEMMA 7. The assertion (b) of Lemma 6 when one consider classic topology can be expressed in the language $\mathcal{L}(\tilde{\mathbb{Q}})$ of the first order of the real closed field $\tilde{\mathbb{Q}}$, see [1].

PROOF. Let the bound for the degree d be fixed and $f_i = \sum_{j_1, \dots, j_n} f_{i,j_1,\dots,j_n} X_1^{j_1} \dots X_n^{j_n}$ where $f_{i,j_1,\dots,j_n} \in \mathbb{R}$ for all $i, j_1, \dots, j_n$. We shall consider all $f_{i,j_1,\dots,j_n}$, $X_1, \dots, X_n, \varepsilon, \delta$ as variables over the field $\tilde{\mathbb{Q}}$. Then the assertion (b) of the Lemma 6 can be written in the form

$$\begin{aligned}
&\forall f_{i,j_1,\dots,j_n} \forall\varepsilon\forall\delta\{\varepsilon > 0 \ \&\ \varepsilon\delta^{d+1} < 1 \ \&\ \delta > 0 \\
&\quad \Rightarrow [\exists X_1 \dots \exists X_n((X_1, \dots, X_n) \text{ satisfies (2)}) \\
&\qquad \Rightarrow \exists X_1' \dots \exists X_n'((X_1', \dots, X_n') \text{ satisfies (2) } \&\ (0, X_1', \dots, X_n') \in \overline{U(\mathbb{R})})]\}.
\end{aligned}$$

The conditions "$(X_1, \dots, X_n)$ satisfies (2)" and "$(X_1', \dots, X_n')$ satisfies (2)" can be expressed in $\mathcal{L}(\tilde{\mathbb{Q}})$. The condition "$(\varepsilon'', X_1'', \dots, X_n'') \in U(\mathbb{R})$" can be expressed in $\mathcal{L}(\tilde{\mathbb{Q}})$, since $U(\mathbb{R}) = \mathbb{V}(\mathbb{R})\backslash\{\varepsilon = \curlyvee\}$ where $V(\mathbb{R})$ is the set of solutions of (6) with real coordinates. So $(0, X_1', \dots, X_n') \in \overline{U(\mathbb{R})}$ can be expressed in the form $\forall\tau > 0 \exists\varepsilon''\exists X_1'' \dots \exists X_n''((\varepsilon'')^2 + \sum_i (X_i' - X_i'')^2 < \tau \ \&\ (\varepsilon'', X_1'', \dots, X_n'') \in U(\mathbb{R}))$, which gives the required expression in $\mathcal{L}(\tilde{\mathbb{Q}})$ for the assertion (b) of Lemma 6. Lemma is proved.

LEMMA 8. Let R be an arbitrary really closed field, $f_1, \dots, f_m \in R[X_1, \dots, X_n]$, $0 < \delta \in R$, $0 < \varepsilon \in R$, $\varepsilon\delta^{d+1} < 1$, $\deg f_i < d$, $d \in \mathbb{Z}$. Then the assertion (b) of Lemma 6 with changing $\mathbb{R}$ for R is satisfied, herewith the closure $\overline{U(R)}$ is considered as the closure in the Zariski topology. Besides that, $\overline{U(R)} \subset \overline{U}$ in the Zariski topology.

Therefore, if system (2) has some solution over R then there exists $\xi \in \pi(\overline{U} \cap \{\varepsilon = 0\})$, which satisfies (2), where $\overline{U}$ is the closure of $U \subset (\mathbb{A}^{\curlywedge} \times \mathbb{A}^{\kappa})(\mathbb{R}(\sqrt{-\curlywedge}))$ in the Zariski topology.

PROOF. Consider at first the topology of a really closed field. Then by Lemma 7, by the assertion (b) of Lemma 6 and the transfer principle, see [1], the first statement of the Lemma is satisfied but when the closure $\overline{U(R)}$ is considered in the topology of the really closed field R.

The Zariski topology in $(\mathbb{A}^{\nVdash} \times \mathbb{A}^{\nvDash})(\mathbb{R})$ is weaker than the topology of the really closed field. Therefore, the first statement of the lemma is satisfied also in the Zariski topology.

Note that the Zariski topology in $\mathbb{A}^{\nvDash+\nVdash}(\mathbb{R})$ when polynomials with coefficients from R are considered is induced by the Zariski topology in $\mathbb{A}^{\nvDash+\nVdash}(\mathbb{R}(\sqrt{-\nVdash}))$ when polynomials with coefficients from $R(\sqrt{-1})$ are considered. So $\overline{U(R)} \subset \overline{U}$ in the Zariski topologies. This implies the last statement of the Lemma. Lemma is proved.

3 Description of the algorithm for the computation of the dimension

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

$$L_j^{(s)} \in \mathbb{Z}[\mathbb{X}_{\aleph}, \ldots, \mathbb{X}_{\nvDash}],\ \sim + \nVdash \le \beth \le \nvDash,$$

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

for all i, j and the subset of $\mathbb{P}(\overline{\neg})$

$$V_s = \{h_1 = \ldots = h_s = L_{s+1}^{(s)} = \ldots = L_n^{(s)} = 0\}$$

of all common zeros of polynomials $h_1, \ldots, h_s, L_{s+1}^{(s)}, \ldots, L_n^{(s)}$ is finite, i.e. $\#V_s < +\infty$. The required dimension $\dim V = \dim\{f_0 = \ldots = f_m = 0\}$ is equal to $n - s_0$ where s_0 is the maximal s for which this construction can be done.

(2) The construction for the base $s = 1$ is easy. If $f_0(X_0, X_1, 0, \ldots, 0) \ne 0$ then one can take $h_1 = f_0$ and $L_i^{(1)} = X_i$, $i \ge 2$. In the general case it is not difficult to find an appropriate linear substitution such that after applying it the condition $f_0(X_0, X_1, 0, \ldots, 0) \ne 0$ will be satisfied.

(3) Now let $n > s \ge 1$ and suppose that $h_1, \ldots, h_s, L_{s+1}^{(s)}, \ldots, L_n^{(s)}$ are constructed. Denote for brevity $L_j^{(s)} = L_j$, $s+1 \le j \le n$. Using the algorithm from [3], see also [8], find all the points $\{x_j\}_{1\le j\le N}$ of the set V_s. Find a linear form L_0 with integer coefficients, such that $L_0(x_j) \ne 0$ for all $1 \le j \le N$.

(4) Let $x_j = (x_{j,0} : \ldots : x_{j,n}) \in \mathbb{P}^{\nvDash}$. Remind that in output of the algorithm from [3] for every j we have an isomorphism of fields over k

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

where $\varphi_j(\tau_j) = 0$, $\varphi_j \in k[Z]$ is an irreducible polynomial, $x_{j,\alpha} \ne 0$. Construct for every j a primitive element $\eta_j = \Theta + c\tau_j$ of the field $k(\tau_j)$ over

$\mathbb{Q}(\approx_{\nvDash}, \dots, \approx_{\lessdot})$, $c \in \mathbb{Z}$, with minimal polynomial $F_j \in \mathbb{Q}[\approx_{\nvDash}, \dots, \approx_{\lessdot}, \mathbb{Z}]$ over $\mathbb{Q}(\approx_{\nvDash}, \dots, \approx_{\lessdot})$. We can suppose that $lc_Z \Phi_j = 1$ changing if it is not so, η_j for $(lc_Z \Phi_j)\eta_j$.

(5) Consider the set of polynomials $\{\sum_{0 \le i \le m} c^i f_i \, : \, 1 \le c \le md^2+1, c \in \mathbb{Z}\} = \mathbb{H}$. 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 $1 \le j \le N'$, and $h(x_j) \ne 0$ when $N' < j \le N$. If $N' = 0$ then we set $h_{s+1} = h$, $L^{(s+1)}_{s+1+i} = L_{s+1+i}$ for every $i \ge 1$ and go to the step $s+1$. If $N' > 0$ we enumerate all the points x_j, $1 \le j \le N'$.

(7) For the considered $1 \le j \le N'$ construct for the field $\mathbb{Q}(\approx_{\nvDash}, \dots, \approx_{\lessdot})[\eta]$ a real structure by section 1, i.e. construct ξ_i, 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 $K = \mathbb{Q}(\approx_{\nvDash}, \dots, \approx_{\lessdot})[\xi_\jmath]$, $0 < \varepsilon_2 < \varepsilon_1$, and ε_2 has the greater order of smallness than ε_1. The field $K_1 = K(\varepsilon_1, \varepsilon_2)$ is a real ordered field.

Consider the system of equations with coefficients from the field $K_1(\sqrt{-1})$

$$h_1 = \ldots = h_s = h - \epsilon_2 L_0^d = 0. \tag{8}$$

Set $X_i = Y_i + \sqrt{-1}\, Z_i$, $0 \le i \le n$, where Y_i and Z_i are new variables. Then $h_i = h_{i,1} + \sqrt{-1}\, h_{i,2}$, $1 \le i \le s$, $h - \varepsilon_2 L_0^d = h^{(1)} + \sqrt{-1}\, h^{(2)}$, where $h_{i,1}, h_{i,2}, h^{(1)}, h^{(2)} \in K(\varepsilon_2)[Y_0, \dots, Y_n, Z_0, \dots, Z_n]$. Consider the system with coefficient from the field K_1

$$h_{1,1} = h_{1,2} = \ldots = h_{s,1} = h_{s,2} = h^{(1)} = h^{(2)} = 0 \tag{9}$$

The solutions of system (8) over the algebraic closure $\overline{K}_1$ of the field K_1 correspond bijectively to the solutions of system (9) over the real closure $\tilde{K}_1$ of the field K_1.

Let $x_j = (x_{j,0} : x_{j,1} : \ldots : x_{j,n})$, some $x_{j,\alpha} = 1$, $x_{j,u} = y_{j,u} + \sqrt{-1}\, z_{j,u}$, $y_{j,u}, z_{j,u} \in K$, $0 \le u \le n$. Denote $h^{(3)} = \sum_{0 \le i \le n}((Y_i - y_{j,i})^2 + (Z_i - z_{j,i})^2)$ and consider the system with an inequality

$$h_{1,1} = h_{1,2} = \ldots = h_{s,1} = h_{s,2} = h^{(1)} = h^{(2)} = 0, \; h^{(3)} \le \varepsilon_1 \tag{10}$$

with coefficients from the field K_1. Each solution of (10) over $\tilde{K}_1$ is the solution of (9) and gives the solution of (8) over $\overline{K}_1$.

(9) System (10) over $\tilde{K}_1$ is analogous to system (2) over $\mathbb{R}$. The variables $Y'_i = Y_i - y_{i,j}$, $Z'_i = Z_i - z_{i,j}$, $0 \le i \le n$ in (10) play the role of $X_1, \dots, X_n$ in (2) (but we shall not use Y'_i, Z'_i explicitely below). Construct the function

$$G = (\delta - h^{(3)} + \varepsilon)(\varepsilon - \sum_{1 \le i \le s} (h_{i,1}^2 + h_{i,2}^2) - (h^{(1)})^2 - (h^{(2)})^2)$$

$$- \varepsilon^3 \sum_{0 \le i \le n} ((Y_i - y_{i,j})^{2d+2} + (Z_i - z_{i,j})^{2d+2})$$

analogous to g from section 2. Here ε is transcendental over the field K_1.

Consider the system of equations with the coefficients from the field K_1 analogous to (6)

$$\frac{\partial G}{\partial Y_0} = \ldots = \frac{\partial G}{\partial Y_n} = \frac{\partial G}{\partial Z_0} = \ldots = \frac{\partial G}{\partial Z_n} = 0 \qquad (11)$$

Here ε is considered as a variable.

(10) Similarly to section 2 define the set U_1 for (11) corresponding to the set U for (6). We have $U_1 \subset (\mathbb{A}^{\not\vdash} \times \mathbb{A}^{\not\vdash \ltimes + \not\vdash})(\overline{\mathbb{K}_{\not\vdash}})$. Analogous to the proof of Lemma 6 we prove that $\overline{U}_1 \cap \{\varepsilon = 0\}$ is a finite set where $\overline{U}_1$ is the closure of U_1 in the Zariski topology. Therefore, each irreducible component V_α of $\overline{U}_1$ which has a non–empty intersection with $\{\varepsilon = 0\}$ has the dimension $\dim V_\alpha = 1$. Further, Lemma 8 implies that if (10) has a solution over the field $\tilde{K}_1$ then there exists $\xi \in \pi(\overline{U}_1 \cap \{\varepsilon = 0\})$ which satisfies (10). In the next paragraphs (11), (12), (13) we shall construct all the points from $\overline{U}_1 \cap \{\varepsilon = 0\}$.

(11) Consider the system

$$G_1 = \ldots = G_{2n+2} = 0 \qquad (12)$$

for the system (11) which is analogous to (7) for system (6) and the sets $W_1, V_1, \mathcal{W}_1, \overline{V}_1, W_1', V_1', \overline{V}_1'$ analogous to $W, V, \mathcal{W}, \overline{V}, W', V', \overline{V}'$. In the definitions one should change $\mathbb{C}, \mathbb{R}$ for $\overline{K}_1, \tilde{K}_1$. For $W_1', V_1', \overline{V}_1', U_1'$ the assertion (a) of the corollary of Lemma 6 is satisfied. The proof is without changes. The assertion (b) is satisfied if one changes $\mathbb{C}$ for $\overline{K}_1$ or K_1. The proof also is the same.

System (12) has a finite number of solutions in $\mathbb{P}^{\not\vdash \ltimes + \not\vdash}(\overline{\mathbb{K}_{\not\vdash}(\varepsilon)})$. We solve system (12) using the algorithm from [3] and find all the irreducible and defined over $K_1(\varepsilon)$ components v_α of $\mathcal{W}_1$. By the corollary of Lemma 6 each v_α correspond to the irreducible and defined over K_1 component V_α of V_1' and conversely each V_α correspond to some v_α. Note that $V_1' \subset \overline{U}_1$ and $V_1' \cap \{\varepsilon = 0\} = \overline{U}_1 \cap \{\varepsilon = 0\}$.

The component v_α is given in output of the algorithm from [3] by the isomorphism of fields over $K_1(\varepsilon)$

$$K_1(\varepsilon)[v_\alpha] = K_1(\varepsilon)[y_{\alpha,0}, \ldots, y_{\alpha,n}, z_{\alpha,0}, \ldots, z_{\alpha,n}] \simeq K_1(\varepsilon)[\eta_\alpha]. \qquad (13)$$

Here $K_1(\varepsilon)[v_\alpha]$ is the field of rational functions on v_α defined over $K_1(\varepsilon)$, $y_{\alpha,0}, \ldots, y_{\alpha,n}, z_{\alpha,0}, \ldots, z_{\alpha,n}$ are coordinate functions on v_α in $\mathbb{A}^{\not\vdash \ltimes + \not\vdash}(\overline{\mathbb{K}_{\not\vdash}(\varepsilon)})$, the element η_α is algebraic over $K_1(\varepsilon)$ and has minimal polynomial $\Phi_\alpha \in K_1(\varepsilon)[Z]$. By [3] the degrees $\deg_{t_j}, \deg_{\varepsilon_1}, \deg_{\varepsilon_2}, \deg_\varepsilon$, $1 \le j \le l$ of all $y_{\alpha,i}, z_{\alpha,i}$, Φ_α are less than $\mathcal{P}(d^n, d_1, d_2)$ and the lengths of coefficients from $\mathbb{Z}$ of these elements are less than $\mathcal{P}(d^n, d_1, d_2)(M_1 + M)$ for some polynomial $\mathcal{P}$.

(12) Our aim is to find all the points from $V_\alpha \cap \{\varepsilon = 0\}$. Use the algorithm from [4] (see also [5]) and construct roots of the polynomial Φ_α in the field of fraction–power series $\bigcup_{\nu\in\mathbb{N}} \overline{K_1}((\varepsilon^{1/\nu}))$ in the following way. The roots are divided into classes with indices β. For each class the field of constant $K_1[\eta'_{\alpha,\beta}]$ is constructed, where $\eta'_{\alpha,\beta}$ is an algebraic over K_1 element with minimal polynomial $\Phi_{\alpha,\beta} \in K_1[Z]$. There exists a root $\tilde{\eta}_{\alpha,\beta}$ of Φ_α such that

$$\tilde{\eta}_{\alpha,\beta} = \sum_{i_o \le i < \infty} v_{\alpha,\beta,i}\, \varepsilon^{1/\nu(\alpha,\beta)},$$

where $v_{\alpha,\beta,i} \in K_1[\eta'_{alpha,\beta}]$ for all i, $v_{\alpha,\beta,i_0} \neq 0$, $0 < \nu(\alpha,\beta) \in \mathbb{Z}$. Each root of Φ_α from the class β has coefficients conjugated over K_1 to the coefficients of $\tilde{\eta}_{\alpha,\beta}$, i.e. has the form $\sum_{i_0\le i<\infty}(\sigma v_{\alpha,\beta,i})\varepsilon^{1/\nu(\alpha,\beta)}$, where $\sigma : K_1[\eta'_{\alpha,\beta}] \to \overline{K}_1$ is an embedding over K_1.

By [4] for $\deg_{\varepsilon_1}, \deg_{\varepsilon_2}, \deg_{t_j}$ and the lengths of coefficients from $\mathbb{Z}$ of $\Phi_{\alpha,\beta}$ we have the same bounds as for Φ_α and for $v_{\alpha,\beta,i}$ the degrees less than $\mathcal{P}(d^n, d_1, d_2)(|i|+1)$ and $l(v_{\alpha,\beta,i)} < (M_1+M_2)\mathcal{P}(d^n,d_1,d_2)(|i|+1)\log(|i|+2)$. Besides that, for the order we have $|\mathrm{ord}_\varepsilon(\tilde{\eta}_{\alpha,\beta})| = |i_0/\nu(\alpha,\beta)| < \mathcal{P}(d^n,d_1,d_2)$. One can construct all $\Phi_{\alpha,\beta}$ in time polynomial in d^n, d_1, d_2, M_1, M and $v_{\alpha,\beta,i}$ in time polynomial in d^n, d_1, d_2, M_1, M, i for every i for some polynomial $\mathcal{P}$.

(13) Let $y_{\alpha,i} = y_{\alpha,i}(\varepsilon, \eta_\alpha)$, $z_{\alpha,i} = z_{\alpha,i}(\varepsilon,\eta_\alpha)$ in (13). Compute the first terms of expansions in $K_1[\eta'_{\alpha,\beta}]((\varepsilon^{1/\nu(\alpha,\beta)}))$ of the elements $y_{\alpha,i}(\varepsilon,\tilde{\eta}_{\alpha,\beta})$, $z_{\alpha,i}(\varepsilon,\tilde{\eta}_{\alpha,\beta})$. It can be done by bounds which were given above in time polynomial in d^n, d_1, d_2, M_1, M. Then substitute $\varepsilon = 0$ i.e. compute $y_{\alpha,i}(\varepsilon,\tilde{\eta}_{\alpha,\beta})|_\varepsilon = 0$, $z_{\alpha,i}(\varepsilon,\tilde{\eta}_{\alpha,\beta})|_\varepsilon = 0$.

We get elements $y_{\alpha,\beta,i}$, $z_{\alpha,\beta,i} \in K_1[\eta'_{\alpha,\beta}] \cup \{\infty\}$ (if the exponent in ε is negative we get ∞). We shall consider only β for which $y_{\alpha,\beta,i}$, $z_{\alpha,\beta,i} \in K_1[\eta'_{\alpha,\beta}]$ for all i. Construct a primitive element $\eta_{\alpha,\beta}$ of the field $K_1[y_{\alpha,\beta,0}, \ldots, y_{\alpha,\beta,n}, z_{\alpha,\beta,0}, \ldots, z_{\alpha,\beta,n}]$ over K_1. Denote by $P_{\alpha,\beta} \in K_1[Z]$ the constructed minimal polynomial of $\eta_{\alpha,\beta}$.

Thus (cf. [5]), all the possible isomorphisms over the field K_1 for all α, β

$$\overline{K_1} \supset K_1[y_0, \ldots, y_n, z_0, \ldots, z_n]$$

$$\simeq K_1[y_{0,\alpha,\beta}, \ldots, y_{n,\alpha,\beta}, z_{0,\alpha,\beta}, \ldots, z_{n,\alpha,\beta}] = K_1[\eta_{\alpha,\beta}] \qquad (14)$$

give all the points $(y_0, \ldots, y_n, z_0, \ldots, z_n) \in \pi(\overline{U_1} \cap \{\varepsilon = 0\})$.

Let σ be an embedding of the field $K_1[\eta_{\alpha,\beta}]$ in $\overline{K_1}$ over K_1. The the elements of $\overline{U_1} \cap \{\varepsilon = 0\}$ correspond to the elements $\sigma\,\eta_{\alpha,\beta}$ where α, β, σ are arbitrary in accordance with (14).

By [4] the degrees $deg_{t_j}, deg_{\varepsilon_1}, deg_{\varepsilon_2}$, $1 \le j \le l$ of all $y_{\alpha,\beta,i}$ $z_{\alpha,\beta,i}$ $P_{\alpha,\beta}$ are less than $\mathcal{P}(d^n, d_1, d_2)$ and the lengths of coefficients from $\mathbb{Z}$ of these elements are less than $(M_1 + M_2)\,\mathcal{P}(d^n, d_1, d_2)$ for some polynomial $\mathcal{P}$.

(14) Let $\Omega_2 = \bigcup_{\nu_1 \in \mathbb{N}} \overline{K(\varepsilon_1)}((\varepsilon_2^{1/\nu_2}))$ be the field of fraction–power series in ε_2 with coefficients from the algebraic closure $\overline{K(\varepsilon_1)}$ of $K(\varepsilon_1)$ and

$$\Omega = \cup_{\nu_1,\nu_2 \in \mathbb{N}} \overline{K}((\varepsilon_1^{1/\nu_1}))((\varepsilon_2^{1/\nu_2}))$$

the field of fraction–power series in ε_2 with coefficients from the field of fraction–power series $\Omega_1 = \cup_{\nu_1 \in \mathbb{N}} \overline{K}((\varepsilon_1^{1/\nu_1}))$ in ε_1 over $\overline{K}$. The fields Ω, Ω_1, Ω_2 are algebraically closed, $\overline{K(\varepsilon_1,\varepsilon_2)} \subset \Omega_2 \subset \Omega$, and for the real closure $K(\tilde{\varepsilon_1},\varepsilon_2)$ of $K(\varepsilon_1,\varepsilon_2)$ we have the embedding of real ordered fields

$$K(\tilde{\varepsilon_1},\varepsilon_2) \subset \bigcup_{\nu_1,\nu_2 \in \mathbb{N}} \tilde{K}((\varepsilon_1^{1/\nu_1}))((\varepsilon_2^{1/\nu_2}))\,,$$

herewith the last field is really closed, see [1].

(15) Now our aim is to find the points form $\pi(\overline{U_1} \cap \{\varepsilon = 0\})$ which are solutions of (10). By paragraphs (10), (13) and (14) it is sufficient for this to construct expansions in the field Ω of all the elements $\sigma\,\eta_{\alpha,\beta}$, i.e. to construct expansions of all the roots of polynomials $P_{\alpha,\beta}$ in Ω for all α, β.

(16) Apply the algorithm from [4], see also [5], and find the partial sums of the expansions of roots of $P_{\alpha,\beta}$ in Ω_2. We take the partial sums till the separation of roots in Newton's polygon method,see [4]. Herewith the irreducible polynomials $P_{\alpha,\beta,\gamma} \in K(\varepsilon_1)[Z]$ with the roots $\eta_{\alpha,\beta,\gamma}$ are constructed which satisfy the following properties. Let σ_1 be an arbitrary embedding of the field $K(\varepsilon_1)[\eta_{\alpha,\beta,\gamma}]$ in $\overline{K(\varepsilon_1)}$ over $K(\varepsilon_1)$. Then the set of fields $K(\varepsilon_1)[\sigma_1\,\eta_{\alpha,\beta,\gamma}]$ for all $\alpha, \beta, \gamma, \sigma_1$ coincides with the set of fields $K_{\alpha,\beta,\sigma}$, where the field $K_{\alpha,\beta,\sigma}$ is generated over $K(\varepsilon_1)$ by the coefficients from $\overline{K(\varepsilon_1)}$ of the expansion in Ω_2 of the element $\sigma\,\eta_{\alpha,\beta}$, for all α, β.

Besides that we have $deg_z(P_{\alpha,\beta,\gamma})$, deg_{ε_1}, $deg_{t_j}(P_{\alpha,\beta,\gamma}), < \mathcal{P}(d^n, d_1, d_2)$ for all j and $l(P_{\alpha,\beta,\gamma}) < (M_1 + M)\,\mathcal{P}(d^n, d_1, d_2))$ for all α, β, γ for some polynomial $\mathcal{P}$, see [4].

We can suppose also without loss of generality that $P_{\alpha,\beta,\gamma} \in K[\varepsilon_1, Z]$, $lc_z\,P_{\alpha,\beta,\gamma} = 1$.

(17) Apply again the algorithm from [4] and find partial sums of the expansions of roots of $P_{\alpha,\beta,\gamma}$ in Ω_1. We take the partial sums till the separation of roots of $P_{\alpha,\beta,\gamma}$ in Newton's polygon method, see [4]. Herewith the irreducible polynomials $P_{\alpha,\beta,\gamma,\delta} \in K[Z]$ with roots $\eta_{\alpha,\beta,\gamma,\delta}$ are constructed which satisfy the following properties. Let σ_2 be an arbitrary embedding of the field $K[\alpha, \beta, \gamma, \delta]$ in $\overline{K}$ over K. Then the set of fields $K[\sigma_2\,\eta_{\alpha,\beta,\gamma,\delta}]$ for all $\sigma_2, \alpha, \beta, \gamma, \delta$ coincides with the set of fields $K_{\alpha,\beta,\gamma,\sigma_1}$ for all $\alpha, \beta, \gamma, \sigma_1$, where the field $K_{\alpha,\beta,\gamma,\sigma_1}$ is generated over K by the coefficients from $\overline{K}$ of the expansion in Ω_1 of the element $\sigma_1\,\eta_{\alpha,\beta,\gamma}$.

Besides that, we have, see [4], $deg_z(P_{\alpha,\beta,\gamma,\delta})$, $deg_{t_j}(P_{\alpha,\beta,\gamma,\delta}) < \mathcal{P}(d^n, d_1, d_2)$ for all j and $l(P_{\alpha,\beta,\gamma,\delta}) < (M_1 + M)\,\mathcal{P}(d^n, d_1, d_2)$ for all $\alpha, \beta, \gamma, \delta$ and some polynomial $\mathcal{P}$.

We can suppose also without loss of generality that $P_{\alpha,\beta,\gamma,\delta} \in \mathbb{Q}[\approx_{\jmath}, \ldots, \approx_{\jmath}, \xi_{\jmath}, Z]$, $lc_z(P_{\alpha,\beta,\gamma,\delta}) = 1$ for all $\alpha, \beta, \gamma, \delta$.

(18) Now we shall choose new real structures for the fields $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_{\jmath}]$ and $K[\eta_{\alpha,\beta,\ \gamma,\delta}]$ for the considered index j and all $\alpha, \beta, \gamma, \delta$. Change for brevity $\alpha, \beta, \gamma, \delta$ for one index μ. Compute a primitive element $\xi_j + c\eta_\mu$, $c \in \mathbb{Z}$, of the field $K[\eta_\mu]$ over $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})$ with minimal polynomial $\phi_\mu \in \mathbb{Q}[\approx_{\jmath}, \ldots, \approx_{\jmath}, \mathbb{Z}]$, $lc_z(\phi_\mu) = 1$. Find the product of the resultants $\Delta_3 = \prod_\mu Res_z(\phi_\mu, \phi'_\mu)$. Let in the algorithm of section 1 by the construction of ξ_j the elements $z_1, \ldots, z_l \in \mathbb{Q}$ be chosen. Using lemma 3 for the element η_j instead of η find $z_1^*, \ldots, z_l^* \in BbbQ$ for which the conclusion of lemma 3 is satisfied and $\Delta_3(z_1^*, \ldots, z_l^*) \neq 0$. Thus, by lemma 3 we construct a new real structure of $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_{\jmath}]$ for which $\xi_j^* = \xi_j$, $R_j^* = R_j$, $I_j^* = I_j$.

By lemma 4 construct using the algorithm from section 1 all the real structures for the field $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_{\jmath} \approx]$ which induce this new real structure of the field $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_{\jmath}]$. These real structures of $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_\mu]$ exist by lemma 4, since $\tilde{K}(\sqrt{-1}) = \overline{K} \supset \mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_\mu]$. The number of these real structures of $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_\mu]$ is no more than $deg_z P_\mu$ by the construction of section 1. Considering one of these real structures we shall denote by ξ_μ, R_μ, I_μ, Ψ_μ the elements corresponding to ξ, R, I, Ψ of section 1.

(19) Note that systems (9), ..., (12) have the same form for the new real structure of $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_{\jmath}]$ as for the old one, since $\xi_j^* = \xi_j$. Further we shall consider only the new real structures for the fields $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_{\jmath}]\ \mathbb{K}[\eta_\mu]$ for all μ.

(20) Now we can find the elements of $\pi(\overline{U_1} \cap \{\varepsilon = 0\})$ which are solutions of (10). By paragraphs (15), (16), (17) if such a solution exists then there exists μ for which the field $\mathbb{Q}(\approx_{\jmath}, \ldots, \approx_{\jmath})[\eta_\mu]$ is a real ordered field in one of real structures constructed in paragraph (18), i.e. in one of real structures with $\eta_\mu = \xi_\mu$. This condiction means that the corresponding element of $\pi(\overline{U_1} \cap \{\varepsilon = 0\})$ belongs to $\mathbb{A}^{\jmath \ltimes + \jmath}(\mathbb{K}_{\jmath}^{\dagger})$.

The elements of $\pi(\overline{U_1} \cap \{\varepsilon = 0\})$ are given by (14). Now we substitute those of them, for which there exists $\mu = (\alpha, \beta, \gamma, \delta)$ and the real structure from paragraph (18) with $\xi_\mu = \eta_\mu$, in system (10) and check whether (10) is satisfied. By lemma 2 we can check the inequality from (10) in time polynomial in d^n, d_1, d_2, M, M_1. Thus, we can find all the elements of $\pi(\overline{U_1} \cap \{\varepsilon = 0\})$ which are solutions of (10). Therefore, by paragraph (10) we can find one of solutions of (10) over $(\tilde{K}_1)$ if (10) has any solutions over $(\tilde{K}_1)$.

The working time of the aglorithm described is polynomial in d^n, d_1, d_2, M, M_1.

4 Conclusion of the description of the algorithm

(21) LEMMA 9. The polynomial h is equal identically to zero on each irreducible component W_1 of the variety $W = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^{\aleph}(\overline{\mathbb{K}})$, such that $x_j \in W_1$ if and only if there exists no solutions of system (9) over the real closure $\overline{K_1}$ of K_1.

PROOF. Let h be equal identically to zero on each such W_1. Denote $V = \{h1 = \ldots = h_s = 0\} \subset \mathbb{A}^{\aleph+\not\aleph}(\overline{\mathbb{K}_{\not\aleph}})$. So, V is the set of all the zeros of $h_1, \ldots, h_s$ in $\mathbb{A}^{\aleph+\not\aleph}(\overline{\mathbb{K}_{\not\aleph}})$. Then there exists a homogeneous polynomial P with coefficients from $\overline{K}$ such that $(h\,/\,L_0^d)(V \cap \{PL_0 \neq 0\}) = \{0\}$ and $P(x_j) \neq 0$. Let $\overline{x_j} = (x_{j,0}, \ldots, x_{j,n}) \in \mathbb{A}^{\aleph+\not\aleph}$, where $x_j = (x_{j,0} : \ldots : x_{j,n}) \in \mathbb{P}^{\aleph+\not\aleph}$, see paragraph (10) of section 3. Denote by $\{|x-\overline{x_j}|^2 < \varepsilon_1\} \subset \mathbb{A}^{\aleph+\not\aleph}(\overline{\mathbb{K}_{\not\aleph}})$ the set corresponding to the set $\{h^{(3)} < \varepsilon_1\} \subset \mathbb{A}^{\not\aleph\aleph+\not\aleph}(\tilde{\mathbb{K}}_{\not\aleph})$, see paragraph (10) of section 3. Show that $\{|x-\overline{x_j}|^2 < \varepsilon_1\} \cap V \subset \{L_0P \neq 0\} \cap V$.

Indeed, otherwise there exists $x' \in \mathbb{A}^{\aleph+\not\aleph}(\overline{\mathbb{K}_{\not\aleph}})$ such that $(L_0P)(x') = 0$ and $|x' - \overline{x_j}|^2 < \varepsilon_1$, i.e. $(L_0P)(\overline{x_j} + (x' + \overline{x_j})) = 0$ where $x' + \overline{x_j} = u_1 + \sqrt{-1}u_2$, $(u_1, u_2) \in \mathbb{A}^{\not\aleph\aleph+\not\aleph}(\tilde{\mathbb{K}}_{\not\aleph})$ and (u_1, u_2) has infinitely small coordinates relatively to the field $\tilde{K}$. This leads to the contradiction, since $\overline{x_j} \in \mathbb{A}^{\aleph+\not\aleph}(\overline{\mathbb{K}})$ and $(L_0P)(\overline{x_j}) \neq 0$.

Thus, we have $(h\,/\,L_0^d)(\{|x-\overline{x_j}|^2 < \varepsilon_1\} \cap V) = \{0\}$, i.e. there are no solutions of (9) over $\tilde{K_1}$.

Conversely, suppose that h is not equal identically to zero on some component W_1 of W, such that $x_j \in W_1$. Let $V_1 \subset \mathbb{A}^{\aleph+\not\aleph}(\overline{\mathbb{K}})$ 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 $\overline{K}$ such that $V_2 \subset V_1, \overline{x_j} \in V_2$ and $h(V_2) \neq \{0\}$. Let t be a uniformizing element of some branch of V_2 containing the point $\overline{x_j}$. The coordinate functions x_r, $0 \leq r \leq n$, on V_2 in the neighbourhood of the points $\overline{x_j} = (x_{j,0}, \ldots, x_{j,n})$ can be represented as series

$$x_r = x_{r,j} + \sum_{i \geq 1} t^i \alpha_{r,i}, \ \alpha_{r,i} \in \overline{K}$$

$$(\frac{h}{L_0^d}) = h_0 t^{\nu} + \sum_{i \geq 1} t^{i+\nu} h_i, \ h_i \in \overline{K}, \ 0 < \nu \in \mathbb{Z}$$

It follows form here that one can solve the equation $h\,/\,L_0^d = \varepsilon_2$ relatively to t and represent

$$t = t_0 \varepsilon_2^{\frac{1}{\nu}} + \sum_{i \geq 1} t_i \varepsilon_2^{\frac{i}{\nu}}, \ t_i \in \overline{K}, \ t_0 \neq 0$$

$$x_r = x_{j,r} + \sum_{i \geq 1} \beta_{r,i}\, \varepsilon_2^{\frac{i}{\nu}} \in \Omega, \ \beta_{r,i} \in \overline{K}$$

$$y_r = y_{j,r} + \sum_{i \geq 1} \gamma_{r,i}\, \varepsilon_2^{\frac{i}{\nu}} \in \Omega, \ \gamma_{r,i} \in \tilde{K}$$

$$z_r = z_{j,r} + \sum_{i \geq 1} \delta_{r,i}\, \varepsilon_2^{\frac{i}{\nu}} \in \Omega, \ \delta_{r,i} \in \tilde{K}$$

where $x_r = y_r + \sqrt{-1}\, z_r$, see paragraph (10) of section 3, and field Ω is defined in paragraph (14) of section 3. Besides that, these expressions for X_r in Ω are algebraic over K_1 since $\overline{K}(W_3) \supset \overline{K}(h \,/\, L_0^d)$ is a finite extension of fields. Therefore, the expression for y_r and z_r are also algebraic over K_1, since they are linear combinations of roots of minimal polynomial for x_r over $K(\varepsilon_2)$, cf. section 1. Therefore, by paragraph (14) and the fact, that ε_2 is the infinitely small value of greater order of smalness than ε_1, we conclude that these expressions for y_r , z_r , $0 \le r \le n$, give the solution of system (10) over the field $\tilde{K}$. Lemma is proved.

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

(23) If $\delta = \delta_1 + \sqrt{-1}\delta_2 \in \overline{K_1}\,; \delta_1, \delta_2 \in \tilde{K_1}$ define $|\delta|^2 = \delta_1^2 + \delta_2^2 \in \tilde{K_1}$.

Let for the considered index j system (10) have a solution which is found in paragraph (20) of section 3. By paragraph (8) we get a solution $x_j^* = (x_{j,0}^* : \ldots : x_{j,n}^* \in \mathbb{P}^{\aleph}(\overline{\mathbb{K}_{\not\aleph}})$ of system (8) with $x_{j,i} \in K_1[\eta_{\alpha,\beta}, \sqrt{-1}] = K_2$ for some α, β, see paragraph (13) and (8). The condiction $h^{(3)} \le \varepsilon_1$ from (10) for x_j^* can be written in the form $\sum_{0 \le i \le n} |x_{j,i} - x_{j,i}^*|^2 \le \varepsilon_1$ where $\overline{x_j} = (x_{j,0}\,, \ldots, x_{j,n})$, see paragraph (21).

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

$$h_1 = \ldots = h_s = L'_{s+1} = \ldots = L'_n = 0 \tag{15}$$

with coefficient form the field K_2 .

(24) We define the element $\delta \in \overline{K_1}$ to be infinitely small relatively to the field $\tilde{K}$ if $|\delta|^2 \in \tilde{K_1}$ is infinitely small relatively to the field $\tilde{K}$.

LEMMA 10. Let W_1 be a component of the variety $W = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^{\aleph} \rtimes \gtrsim \prec \lessdot \beth \ltimes \mathbb{K}_{\not\aleph}$ 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 $x' = (x'_0 : \ldots : x'_n) \in W_1$ such that $(L_i - \delta_i L_0)(x') = 0$ and $x'_0 - x_{j,0}\,, \ldots, x'_n - x'_{j,n}$ are infinitely small relatively to the field $\tilde{K}$.

PROOF. We have $dim\, W_1 = n - s$ and $W_1 \cap \{L_0 = L_{s+1} = \ldots = L_n = 0\} = \varnothing$. It follows from here, see [7], that the projection $p : W_1 \longrightarrow \mathbb{P}^{\aleph - \sim}$, $(\mathbb{X}_{\not\aleph} : \ldots : \mathbb{X}_{\aleph}) \longmapsto (\mathbb{L}_{\not\aleph} : \mathbb{L}_{\sim + \not\aleph} : \mathbb{L}_{\sim + \not\aleph} : \ldots : \mathbb{L}_{\aleph})$ is defined everywhere and, therefore finite. Let $x^{(\alpha)} \in \mathbb{P}^{\aleph}(\overline{\mathbb{K}_{\not\aleph}})$, $\alpha \in \mathbb{A}$, ba all the different elements of the inverse image $p^{-1}((1 : \delta_{s+1} : \ldots : \delta_n))$.

We can assume without loss of generality that $L_0 = X_0$ and, therefore, $x_0^{(\alpha)} = 1$ where $x^{(\alpha)} = x_0^{(\alpha)} : \ldots : x_n^{(\alpha)})$ for all $\alpha \in A$, and $x_{j,0} = 1$ (otherwise one can find an appropriate linear changing of coordinates in $\mathbb{P}^{\aleph}$, over the field K such that one of new coordinates will be L_0).

Suppose that for every $\alpha \in A$ not all $x_i^{(\alpha)} - x_{ji}$, $1 \le i \le n$, are infinitely small relatively to the field $\tilde{K}$. Then there exists a linear form $L = \sum_{1 \le i \le n} l_i (X_i - X_0 x_{ji})$, $l_i \in \overline{K}$, such that the element $l^{(\alpha)} = \sum_{l \le i \le n} l_i (x_i^{(\alpha)} - x_{ji})$ is not infinite small realtively to $\tilde{K}$ for every $\alpha \in A$.

Now we consider the projection $p_1 : W_1 \longrightarrow \mathbb{P}^{\aleph - \sim + \not\aleph}$, $(\mathbb{X}_{\not\aleph} : \ldots : \mathbb{X}_{\aleph}) \longmapsto (\mathbb{L}_{\not\aleph} : \mathbb{L}_{\sim + \not\aleph} : \mathbb{L}_{\sim + \not\in} : \ldots : \mathbb{L}_{\aleph} : \mathbb{L})$. The set $p_1 (W_1)$ is a closed irreducible variety in $\mathbb{P}^{\aleph - \sim + \not\aleph} (\overline{\mathbb{K}_{\not\aleph}})$ of the codimension equal to 1, see [7]. So, $p_1 (W_1) = \{Q = 0\} \subset \mathbb{P}^{\aleph - \sim + \not\aleph}$, where $Q \in \overline{K} [L_0 , L_{s+1} , dots , L_n , L]$ is irreducible homogeneous polynomial with $lc_L Q = 1$, since p is finite. The polynomial $q(Z) = Q(1 , \delta_{s+1} , \ldots , \delta_n , Z) \in \overline{K_1} [Z]$ has the set of roots coinciding with $\{l^{(\alpha)} : \alpha \in A\}$, since $p_1 (W_1) = \{Q = 0\}$. The polynomial $Q (1 , 0 , \ldots 0 , Z)$ has the root $\sum_{l \le ! \le n} l_i (x_{j,i} - 1 x_{j,i} = 0$. So $q (0) = Q (1 , \delta_{s+1} , \ldots , \delta_n , 0)$ is infinitely small realtively to $\tilde{K}$. This leads to the contradiction, since each root $l^{(\alpha)}$, $\alpha \in A$, of $q (Z)$ is not infinitely small relatively $\tilde{K}$ and $lc_Z q = 1$. Lemma is proved.

(25) LEMMA 11. Suppose that the polynomial h is equal identically to zero on some component W_1 of the variety $W = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^{\aleph} (\overline{\mathbb{K}})$, such that $x_j \in W_1$ and there exists x_j^*, see paragraph (22). Then there exist two different solutions $x' = (x'_0 : \ldots : x'_n)$ and $x'' = (x''_0 : \ldots : x''_n)$ of system (15) such that $x_{ji} - x'_i$ and $x_{ji} - x''_i$ are infinitely small relatively to the field $\tilde{K}$ for all $0 \le i \le n$.

PROOF. By lemma 10 there exists the required $x' \in W_1$. We set $x'' = x_j^*$. By paragraph (23) the coordinates $x_{j,i} - x''_{j,i} = x_{j,i} - x^*_{j,i}$ are infinitely small relatively to the field $\tilde{K}$. So $L_0 (x'') \neq 0$ and $(h \,/\, L_0^d)(x'') = \varepsilon_2 \neq 0$. Therefore, $x'' \notin W_1$ and $x'' \neq x'$. Lemma is proved.

(26) Suppose that system (12) has $N_1 > N$ solutions. Find new linear forms $M_{s+1} , \ldots , M_n$ with coefficients from $\mathbb{Z}$ and $l (M_i) = O (n \, log \, d)$, $s+1 \le i \le n$, such that the system

$$h_1 = \ldots = h_s = M_{s+1} = \ldots = M_n) 0$$

has a finite number of solutions and at least N_1 solutions (all solutions in $\mathbb{P}^{\aleph} (\overline{\mathbb{K}})$).

Show that we can change an arbitrary coefficient in forms $L'_{s+1} , \ldots , L'_n$ for an integer coefficient with the required length such that the new obtained system analogous to (15) will have no less than N_1 solutions but a finite number of solutions.

Let $L'_{s+1} = \sum_{0 \le i \le n} l_{s+1,i} X_i$, $l_{s+l,i} \in \overline{K_1}$ and we wish to change, say, $l_{s+1,0}$ for a coefficient from $\mathbb{Z}$. At first change $l_{s+1,0}$ for a transcendental element t and denote by $L''_{s+1} = t X_0 + \sum_{0 \le i \le n} l_{s+1,i} X_i$ the form obtained. Consider the system

$$h_1 = \ldots = h_s = L''_{s+1} = L'_{s+2} = \ldots = L'_n = 0. \qquad (16)$$

Let $\Delta\,(U_0\,,\,\ldots\,,\,U_n,\ \,,\,t)\ \in\ \overline{K_1}\,[U_0\,,\,\ldots\,,\,U_n,\ \,,\,t]$ be the U-resultant of system (16), see [8]. Note that $\Delta\,(U_0\,,\,\ldots\,,\,U_n,\ \,,\,l_{s+1,0}) \neq 0$ is the U-resultant os system (15). So $\Delta \neq 0$ and the system (16) has a finite number of solutions. Further, we have $deg_{U_0\,,\,\ldots\,,\,U_n}(\Delta) \leq d^n\,,\ deg_t\,(\Delta) \leq \mathcal{P}\,(d^n)$ for some polynomial $\mathcal{P}$.

Let $\Delta = \prod_i \Delta_i^{e_i}$ be the decomposition of Δ into irreducible factors, where Δ_i are irreducible over $\overline{K_1}$ and $\Delta_i\ \in\ \overline{K_1}\,[U_0\,,\,\ldots\,,\,U_n,\ \,,\,t]$. Then $\sum_i deg_{U_0\,,\,\ldots\,,\,U_n}$ $(\Delta_i) = N_2$ is the number of solutions of system (16) over the field $\overline{K_1\,(t)}$.

We can find a linear changing of coordinates $(U_0\,,\,\ldots\,,\,U_n) \longmapsto (U_0'\,,\,\ldots\,,\,U_n')$ with coefficients from $\mathbb{Z}$ if it is necessary and suppose without loss of generality that $deg_{U_0\,,\,\ldots\,,\,U_n}\,(\Delta_i) = deg_{U_0}\,(\Delta_i)$\,, i.e. $lc_{U_0}\,(\Delta_i)\ \in\ \overline{K_1}[t]$. Let $R_i = Res_{U_0}\,(\Delta_i\,(\Delta_i)_{U_0})$ be the discriminant of the polynomial R_i and $R = \prod_i R_i$\,. Then $deg_t\,(R) \leq \mathcal{P}\,(d^n)$ for some polynomial $\mathcal{P}$.

If $R\,|_{t=t_0} \neq 0\,,\ t_0\ \in\ \overline{K_1}$ then each polynomial $\Delta_i\,|_{t=t_0}$ is separable. Therefore, the number of solutions N_3 of the system

$$h_1 = \ldots = h_s = L''_{s+1}\,|_{t=t_0} = L'_{s+2} = \ldots = L'_n = 0. \tag{17}$$

over the field $\overline{K_1}$ coincides with the number of solutions N_2 of system (16) over $K\,(t)$, i.e. $N_2 = N_3$\,. In the general case $N_3 \leq N_2$, if $N_3 < \infty$, i.e. if $\Delta_i\,|_{t=t_0}$ is not equal identically to zero for every i. Therefore, $N_1 \leq N_2$.

Thus, enumerating $\leq \mathcal{P}\,(d^n)$ integer values of t and solving each time system (17), we find $t = t_0$ such that system (17) has $N_2 \geq N_1$ solutions and $N_2 < +\infty$. We change $l_{s+1,0}$ for t_0 and get new forms $L'_{s+1}\,,\,\ldots\,,\,L'_n$\,.

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

(27) Return to paragraph (23). Solve system (15). It has a finite number of solutions. Indeed, the U-resultant Δ_1 of system (15) has coefficients which coindice with the coefficients of the U-resultant Δ_2 of the system $h_1 = \ldots = h_s = L_{s+1}^{(s)} = \ldots = L_n^{(s)} = 0$ up to infinitely small values relatively to $\tilde{K}$, i.e. $\Delta_1 - \Delta_2$ has infinitely small relatively to $\tilde{K}$ coefficients. We have $\Delta_2 \neq 0$, since $\sharp\, V_s < \infty$, see paragraph (1). Therefore, $\Delta_1 \neq 0$. This implies that system (15) has a finite number of solutions. If system (15) has $N_1 > N$ solutions we construct $M_{s+1}\,,\,\ldots\,,\,M_n$ by paragraph (26) and change $L_{s+1}\,,\,\ldots\,,\,L_n$ for $M_{s+1}\,,\,\ldots\,,\,M_n$. Then we return to the beginning of the algorithm for the considered s. The number of points of V_s, see paragraph (1) of section 3, now is greater than it was.

(28) 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 of system (15) $N_1 = N_1(j) = N$ for every $1 \leq h \leq N'$, 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 $W = \{h_1 = \ldots = h_s = 0\}$. Note that $W_1 \cap \{L_{s+1} = \ldots = L_n = 0\} \neq \emptyset$ since W_1 is projective 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 (1), and the assertion is proved for W_1. If $1 \leq j \leq N'$ then by lemma 9 the polynomial h is not equal identically to zero 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 11 there exist two different points x' and x'' which are solutions of (15) and $x_{ji} - x'_i$,$x_{ji} - x''_i$ are infinitely small relatively to the field $\tilde{K}$ for all $0 \leq i \leq n$. On the other side by lemma 10 for every $1 \leq j \leq N$ there exists a solution x''' of system (15) such that $x''' \in W_1$ and $x''' - x_{j,i}$ are infinitely small relative to $\tilde{K}$ for all $0 \leq i \leq n$. Therefore, system (15) has $\geq N + 1$ solutions, since points $x_j \in \mathbb{P}^{\aleph}(\mathbb{k})$. 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 $h_{s+1} = h$.

(29) Show that if for every $h \in H$ there exists x_j, $1 \leq j \leq \mathcal{N}' = N'(h)$ 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 $dim\,\{f_0 = \ldots = f_m = 0\} \leq n - s$. Let W_1 be the same as above. For each W_1 there exist at almost 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 no more than d^s. So, there exists $h \notin H$ such that h is not equal identically to zero on each component W_1. Then by lemma 9 for every x_j, $1 \leq j \leq N'$, there exists x_j^*. This is a contradiction. The assertion is proved.

(30) Let $s = n$. We shall enumerate $h \in H$. If there exists h such that $0 \in h(V_n)$ then $\{f_0 = \ldots = f_m = 0\} = \emptyset$ and $dim\,\{f_0 = \ldots = f_m = 0\} = -1$ and we set $h_{n+1} = h$. Otherwise $dim\,\{f_0 = \ldots = f_m\} = 0$.

(31) Return to paragraph (27). Find new linear forms $L_{s+2}^{(s+1)}, \ldots, L_n^{(s+2)}$ such that the system

$$h_1 = \ldots = h_{s+1} = L_{s+2}^{(s+1)} = \ldots = L_n^{(s+2)} = 0$$

has a finite number of solutions in $\mathbb{P}^{\aleph}(\mathbb{k})$. Define the set

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

We shall enumerate the elements $L \in \mathcal{L}$. Apply the algorithms from paragraph (1), ..., (30), changing s for $s + 1$ polinomials $h, \ldots, h_s$ for $h_1, \ldots, h_s, L^d$, forms $L_{s+1}, \ldots, L_n$ for $L_{s+2}, \ldots, L_n$ with $h = h_{s+1}$. If we get

$$dim\,\{h_1 = \ldots = h_s = L = h_{s+1} = 0\} = n - s - 1,$$

then we go to the next element $L \in \mathcal{L}$. Otherwise we set $L_{s+2}^{(s+1)} = L$ and we have

$$dim\,\{h_1 = \ldots = h_s = L_{s+2}^{(s+1)} = h_{s+1} = 0\} = n - s - 1.$$

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

Similarly sequentially for every $2 < i \leq n - s - 1$ we find $L_{s+i}^{(s+1)} \in \mathcal{L}$ such that

$$dim\,\{h_1 = \ldots = h_s = L_{s+2}^{(s+1)} = L_{s+i}^{(s+1)} = h_{s+1} = 0\} = n - s - i - 1.$$

Thus, we find all $L_{s+2}^{(s+1)}, \ldots, L_n^{(s+1)}$ and go to step $s + 1$, see paragraphs (3) and (30).

(32) We have concluded the description of the algorithm for the computation of the dimension. Note that in paragraph (27) by Bézouts inequality we have no more than d^s returns to the beginning of the step s. Therefore, by the construction described the general working time of the algorithm is polynomial in d^n, d_1, d_2, M_1, M_2.

The theorem from the introduction is completely 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 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)].

[4] **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.

[5] **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).

[6] **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.

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

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

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

[10] **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.