J. Symbolic Computation (1988) **5**, 37–64

Solving Systems of Polynomial Inequalities in Subexponential Time

D. Yu. GRIGOR'EV AND N. N. VOROBJOV (Jr)

Leningrad Department of Mathematical Steklov Institute of the Academy of Sciences of the USSR, Fontanka embankment, 27, Leningrad, 191011, USSR and Leningrad State University, Universitetskaya embankment, 7/9, Leningrad, 199164, USSR

(*Received* 20 *March* 1985)

Let the polynomials $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$ have degrees $\deg(f_i) < d$ and absolute value of any coefficient of f_i less than or equal to 2^M for all $1 \leqslant i \leqslant k$. We describe an algorithm which recognises the existence of a real solution of the system of inequalities $f_1 \geqslant 0, \ldots, f_k \geqslant 0$. In the case of a positive answer the algorithm constructs a certain finite set of solutions (which is, in fact, a representative set for the family of components of connectivity of the set of all real solutions of the system). The algorithm runs in time polynomial in $M(kd)^{n^2}$. The previously known upper time bound for this problem was $(Mkd)^{2^{O(n)}}$.

Introduction

The problem of finding real solutions of systems of polynomial inequalities is of known significance for symbolic computation. For the first time the decidability of this problem was proven by Tarski (1951). However, the time-bound of the algorithm from Tarski (1951) is non-elementary (in particular, the time-bound cannot be estimated by any tower of exponents). Later, exponential-time algorithms were devised for this problem (Collins, 1975; Wüthrich, 1976). In fact, Tarski (1951), Collins (1975) and Wüthrich (1976) consider a more general problem, namely, quantifier elimination in the first order theory of real closed fields.

In the present paper we describe a subexponential-time algorithm for finding real solutions of systems of polynomial inequalities (see also Vorobjov & Grigor'ev, 1985). This algorithm essentially involves the subexponential-time algorithm for solving systems of polynomial equations over an algebraically closed field (Chistov & Grigor'ev, 1983*a*, *b*; Chistov, 1984; Grigor'ev, 1984; see also Chistov & Grigor'ev, 1984; Grigor'ev, 1987). Before the papers by Chistov & Grigor'ev (1983*a*, *b*) only exponential-time algorithms were known for the latter problem (see e.g. Collins, 1975; Wüthrich, 1976; Heintz, 1983). On the other hand, it is clear that the problem of solving systems of inequalities over real numbers is more general than the problem of solving systems of equations, for example, over the field of complex numbers.

Let $f_1, \ldots, f_k \in \mathbb{Z}[X_1, \ldots, X_n]$ be input polynomials. An algorithm described in the present paper finds a certain set of solutions in $\mathbb{R}^n$ (or indicates their absence) of a system of inequalities

$$f_1 > 0, \ldots, f_m > 0, f_{m+1} \geqslant 0, \ldots, f_k \geqslant 0. \tag{1}$$

0747–7171/88/010037+28 $03.00/0

A rational function $g \in \mathbb{Q}(Y_1, \ldots, Y_s)$ can be represented as $g = g_1/g_2$ where the polynomials $g_1, g_2 \in \mathbb{Z}[Y_1, \ldots, Y_s]$ are relatively prime. Denote by $l(g)$ the maximum bit lengths of the (integer) coefficients of the polynomials g_1, g_2. Throughout this paper we suppose that the following inequalities are valid:

$$\deg_{X_1, \ldots, X_n}(f_i) < d, \; l(f_i) \leqslant M, \quad 1 \leqslant i \leqslant k. \tag{2}$$

We estimate the size of system (1) by the value $\mathscr{L} = kMd^n$ (cf. Chistov & Grigor'ev, 1983*a*, *b*; Chistov, 1984; Grigor'ev, 1984; also Chistov & Grigor'ev, 1984).

The running time of the algorithms for solving systems of inequalities from Collins (1975) and Wüthrich (1976) is bounded by $(Mkd)^{2^{O(n)}}$.

The notation $h_1 \leqslant \mathscr{P}(h_2, \ldots, h_t)$ for functions $h_1, \ldots, h_t > 0$ means that for suitable natural numbers q, p an inequality $h_1 \leqslant p(h_2 \ldots h_t)^q$ is true.

A subset in $\mathbb{R}^n$ is called semi-algebraic if it consists of all points in $\mathbb{R}^n$ satisfying an appropriate quantifier-free formula Π with the atomic subformulas of the form $(g_j \geqslant 0)$ with $g_j \in \mathbb{R}[X_1, \ldots, X_n]$. We denote this subset by $\{\Pi\} \subset \mathbb{R}^n$.

Let

$$\mathscr{V} = \{(f_1 > 0) \& \ldots \& (f_m > 0) \& (f_{m+1} \geqslant 0) \& \ldots \& (f_k \geqslant 0)\} \subset \mathbb{R}^n$$

be a semi-algebraic set consisting of all solutions of system (1). The set $\mathscr{V}$ is decomposable (uniquely) in the disjoint union of its components of connectivity $\mathscr{V}_i$, i.e.

$$\mathscr{V} = \bigcup_i \mathscr{V}_i.$$

Moreover, every set $\mathscr{V}_i$ is also semi-algebraic (see e.g. Collins, 1975; Wüthrich, 1976). A finite set $\mathscr{T} \subset \mathscr{V}$ is called a representative set for $\mathscr{V}$ (or in other words, for the system (1)) iff for each index i the intersection $\mathscr{V}_i \cap \mathscr{T} \neq \phi$. Denote by $\tilde{\mathbb{Q}} \subset \mathbb{R}$ the field of all real algebraic numbers. The main result of the present paper is the following theorem (see also Vorobjov & Grigor'ev, 1985; Grigor'ev, 1987).

THEOREM. *There is an algorithm which, for any system of inequalities of the kind* (1), *satisfying* (2), *produces some representative set* $\mathscr{T} \subset \mathscr{V} \cap \tilde{\mathbb{Q}}^n$ *with a number of points not exceeding* $\mathscr{P}((kd)^{n^2})$. *The running time of the algorithm is less than* $\mathscr{P}(M, (kd)^{n^2}) \leqslant \mathscr{P}(\mathscr{L}^{\log^2 \mathscr{L}})$ (*i.e. the time-bound is subexponential in* $\mathscr{L}$). *For every point* $(\chi_1, \ldots, \chi_n) \in \mathscr{T}$ *the algorithm constructs a corresponding polynomial* $\Phi \in \mathbb{Q}[Z]$, *that is irreducible over* $\mathbb{Q}$, *and the expressions*

$$\chi_i = \chi_i(\omega) = \sum_j \beta_j^{(i)} \omega^j \in \mathbb{Q}[\omega],$$

where $\beta_j^{(i)} \in \mathbb{Q}$, $1 \leqslant i \leqslant n$, $0 \leqslant j < \deg(\Phi)$ *and* $\omega \in \tilde{\mathbb{Q}}$, $\Phi(\omega) = 0$. *Besides that, the algorithm produces a pair of rational numbers* $b_1, b_2 \in \mathbb{Q}$ *such that inside the interval* $(b_1, b_2) \subset \mathbb{R}$ *there is a unique real root* $\omega \in (b_1, b_2)$ *of the polynomial* Φ. *In addition, the equality*

$$\omega = \sum_{1 \leqslant j \leqslant n} \lambda_i \chi_i(\omega)$$

is fulfilled for certain natural numbers $1 \leqslant \lambda_i \leqslant \deg(\Phi)$, $1 \leqslant i \leqslant n$. *Finally, the polynomials and expressions constructed satisfy the following bounds:*

$$\deg(\Phi) \leqslant \mathscr{P}((kd)^n); \quad l(\Phi), l(\chi_i(\omega)), l(b_1), l(b_2) \leqslant M\mathscr{P}((kd)^n).$$

REMARK. Based on the description of the points constructed in the theorem and using, e.g. Heindel (1971), one can find, for any rational $0 < \delta \leqslant 1$, rational δ-approximations to the points from the set $\mathscr{T}$ within time $\mathscr{P}(\log(1/\delta), M, (kd)^{n^2})$.

For the proof of the theorem we need the algorithms from Chistov & Grigor'ev (1982, 1983*a*, *b*), Chistov (1984), Grigor'ev (1984), also Chistov & Grigor'ev (1984) on polynomial factoring and on solving systems of algebraic equations. Now we formulate exactly these results. Taking into account that only fields of characteristic zero are considered in the present paper, and in order to avoid complex formulas due to inseparable fields extensions, we restrict ourselves here to the zero characteristic case.

Thus, consider a ground field $F = \mathbb{Q}(T_1, \ldots, T_e)[\eta]$, where the elements $T_1, \ldots, T_e$ are algebraically independent over $\mathbb{Q}$, the element η is algebraic over the field $\mathbb{Q}(T_1, \ldots, T_e)$. Denote by

$$\varphi = \sum_{0 \leqslant i \leqslant \deg_z(\varphi)} (\varphi_i^{(1)}/\varphi^{(2)}) Z^i \in \mathbb{Q}(T_1, \ldots, T_e)[Z]$$

its minimal polynomial over $\mathbb{Q}(T_1, \ldots, T_e)$ with leading coefficient $lc_z(\varphi) = 1$, where $\varphi_i^{(1)}, \varphi^{(2)} \in \mathbb{Z}[T_1, \ldots, T_e]$ and the degree $\deg(\varphi^{(2)})$ is the least possible. Any polynomial $f \in F[X_1, \ldots, X_n]$ can be uniquely represented in a form

$$f = \sum_{0 \leqslant i < \deg_z(\varphi);\, i_1, \ldots, i_n} (a_{i, i_1, \ldots, i_n}/b) \eta^i X_1^{i_1} \ldots X_n^{i_n},$$

where $a_{i, i_1, \ldots, i_n}, b \in \mathbb{Z}[T_1, \ldots, T_e]$ and the degree $\deg(b)$ is the least possible. Define

$$\deg_{T_j}(f) = \max_{i_1, \ldots, i_n} \{\deg_{T_j}(a_{i, i_1, \ldots, i_n}), \deg_{T_j}(b)\}.$$

Let

$$\deg_{X_m}(f) < \tau, \quad \deg_{T_j}(f) < \tau_2, \quad \deg_{T_j}(\varphi) < \tau_1, \quad \deg_z(\varphi) < \tau_1,$$
$$l(f) \leqslant M_2, \quad l(\varphi) \leqslant M_1 \quad \text{for all} \quad 1 \leqslant m \leqslant n, \quad 1 \leqslant j \leqslant e.$$

As the size $L_1(f)$ of the polynomial f we consider in proposition 1 the value $\tau^{n+e}\tau_2^e\tau_1 M_2$ and analogously $L_1(\varphi) = \tau_1^{e+1} M_1$.

PROPOSITION 1 (Chistov & Grigor'ev, 1982, 1984; Chistov, 1984; Grigor'ev, 1984). *One can factor a polynomial f over F within time polynomial in the sizes $L_1(f)$, $L_1(\varphi)$. Furthermore, for any divisor $f_1 | f$ where a polynomial $f_1 \in F[X_1, \ldots, X_n]$ has a certain coefficient equal to* 1, *the following bounds are true:*

$$\deg_{T_j}(f_1) \leqslant \tau_2 \mathscr{P}(\tau, \tau_1), \quad l(f_1) \leqslant (M_1 + M_2 + e\tau_2 + n)\mathscr{P}(\tau, \tau_1).$$

For the cases when the field F is finite or F is a finite extension of $\mathbb{Q}$, other polynomial-time algorithms for factoring are described in Lenstra (1984).

Now we proceed to the problem of solving systems of algebraic equations. Let the input system $f_1 = \ldots = f_k = 0$ be given, where the polynomials $f_1, \ldots, f_k \in F[X_1, \ldots, X_n]$. Let

$$\deg_{X_1, \ldots, X_n}(f_i) < d, \quad \deg_{T_1, \ldots, T_e, Z}(\varphi) < d_1,$$
$$\deg_{T_1, \ldots, T_e}(f_i) < d_2, \quad l(f_i) \leqslant M_2 \quad \text{for all} \quad 1 \leqslant i \leqslant k.$$

As the size L of the system is proposition 2 we consider the value $kd^n d_1 d_2^e M_2 + d_1^{e+1} M_1$.

The variety $\mathscr{W} \subset \bar{F}^n$ of all roots (defined over the algebraic closure $\bar{F}$ of the field F) of the system $f_1 = \ldots = f_k = 0$ is decomposable as the union of its components

$$\mathscr{W} = \bigcup_\alpha W_\alpha$$

defined and irreducible over the field F. The algorithm from proposition 2 finds the components W_α and outputs every W_α in the two following manners: by its general point (see below) and, on the other hand, by a certain system of algebraic equations such that W_α coincides with the variety of all roots of this system.

Let $W \subset \bar{F}^n$ be a closed variety of dimension $\dim W = n-m$ defined and irreducible over F. Denote by $t_1, \ldots, t_{n-m}$ some algebraically independent elements over F. A general point of the variety W can be given by the following field isomorphism:

$$F(t_1, \ldots, t_{n-m})[\theta] \simeq F(X_1, \ldots, X_n) = F(W), \qquad (*)$$

where the element θ is algebraic over the field $F(t_1, \ldots, t_{n-m})$. Denote by $\Phi(Z) \in F(t_1, \ldots, t_{n-m})[Z]$ its minimal polynomial over $F(t_1, \ldots, t_{n-m})$ with leading coefficient $lc_z(\Phi) = 1$. The elements $X_1, \ldots, X_n$ are considered as the rational (coordinate) functions on the variety W. Under the isomorphism $(*)$ $t_i \to X_{j_i}$ for suitable $1 \leqslant j_1 < \ldots < j_{n-m} \leqslant n$, where $1 \leqslant i \leqslant n-m$. Besides, θ is the image under isomorphism $(*)$ of an appropriate linear function $\sum_{1 \leqslant i \leqslant n} c_i X_i$, where c_i are integers. The algorithm from proposition 2 represents the isomorphism $(*)$ by the integers $c_1, \ldots, c_n$ and apart from that by the images of the coordinate functions $X_1, \ldots, X_n$ in the field $F(t_1, \ldots, t_{n-m})[\theta]$. Sometimes in the formulation of proposition 2 we identify a rational function with its image under the isomorphism.

Proposition 2 (Chistov & Grigor'ev, 1983*a*, *b*, 1984; Chistov, 1984; Grigor'ev, 1984). *An algorithm can be designed which produces a general point of every component W_α and constructs a certain family of polynomials $\psi_\alpha^{(1)}, \ldots, \psi_\alpha^{(N)} \in F[X_1, \ldots, X_n]$ such that W_α coincides with the variety of all roots of the system $\psi_\alpha^{(1)} = \ldots = \psi_\alpha^{(N)} = 0$. Denote by $n-m = \dim W_\alpha$, $\theta_\alpha = \theta$, $\Phi_\alpha = \Phi$ (see $(*)$). Then $\deg_z(\Phi_\alpha) \leqslant \deg(W_\alpha) \leqslant d^m$, for all j, s, the degrees*

$$\deg_{T_1, \ldots, T_e, t_1, \ldots, t_{n-m}}(\Phi_\alpha),\ \deg_{T_1, \ldots, T_e, t_1, \ldots, t_{n-m}}(X_j),\ \deg_{T_1, \ldots, T_e}(\psi_\alpha^{(s)}) \leqslant d_2 \mathscr{P}(d^m, d_1),$$

and

$$\deg_{X_1, \ldots, X_n}(\psi_\alpha^{(s)}) \leqslant d^{2m}.$$

The number of equations $N \leqslant m^2 d^{4m}$. Furthermore,

$$l(\Phi_\alpha),\ l(X_j) \leqslant (M_1 + M_2 + (n+e)d_2)\mathscr{P}(d^m, d_1)$$

and

$$l(\psi_\alpha^{(s)}) \leqslant (M_1 + M_2 + e d_2)\mathscr{P}(d^n, d_1).$$

Finally, the total running time of the algorithm can be bounded by $\mathscr{P}(M_1, M_2, (d^n d_1 d_2)^{n+e}, k)$. Obviously, the latter value does not exceed $\mathscr{P}(L^{\log L})$, in other words, is subexponential in the size.

The contents of the paper are briefly as follows. In section 1 a device is introduced for justifying the calculations with infinitesimals which are involved below in sections 2, 3. Some properties of semi-algebraic sets over ordered extensions by infinitesimals of the field $\tilde{\mathbb{Q}}$ are ascertained.

In section 2 an algorithm is suggested that produces a representative set for the variety of all real roots of a given polynomial. For this purpose an infinitesimal "perturbation" of the initial polynomial is considered, so that the variety of all the real roots of the "perturbed" polynomial turns out to be a smooth hypersurface. The algorithm finds on this hypersurface points with some fixed directions of the gradient, solving an appropriate system of algebraic equations over an algebraically closed field with the help of proposition 2.

In section 3 we prove at first some bounds on real algebraic solutions of the system (1).

After that, for the given system (1), the algorithm yields a relevant polynomial and applies the construction from section 2 in order to produce a representative set for the variety of real roots of this polynomial. Then among the points produced the algorithm picks out all the points satisfying system (1). This completes the proof of the theorem.

In section 4 an outline of the whole algorithm is given, omitting some details covered in sections 2, 3.

1. Calculations with Infinitesimals

Let K, in the course of this section, denote an arbitrary real closed field (see e.g. Lang, 1965) and an element $\varepsilon > 0$ infinitesimal relatively to the elements of the field K, i.e. for any positive element $0 < \alpha \in K$ in the ordered field $K(\varepsilon)$ the inequalities $0 < \varepsilon < \alpha$ are valid. Obviously, the element ε is transcendental over K. For an ordered field K_1 we denote by $\tilde{K}_1 \supset K_1$ its unique (up to isomorphism) real closure, preserving the order on K_1 (see e.g. Lang, 1965).

Let us remind some well-known statements about real closed fields. A Puiseux series (or in other words power-fractional series) over the field K is a series of the kind

$$a = \sum_{i \geqslant 0} \alpha_i \varepsilon^{\nu_i/\mu},$$

where $0 \neq \alpha_i \in K$ for all $i \geqslant 0$, the integers $\nu_0 < \nu_1 < \ldots$ increase and the natural number $\mu \geqslant 1$. The field $K((\varepsilon^{1/\infty}))$ consisting of all Puiseux series (with added zero) is real closed, and hence $K((\varepsilon^{1/\infty})) \supset \widetilde{K(\varepsilon)} \supset K(\varepsilon)$. Besides, the field $K[\sqrt{-1}]((\varepsilon^{1/\infty})) = \bar{K}((\varepsilon^{1/\infty}))$ is algebraically closed (here and further a bar over a field denotes its algebraic closure).

If $\nu_0 < 0$, then the element $a \in K((\varepsilon^{1/\infty}))$ is infinitely large; if $\nu_0 > 0$, then a is infinitesimal (relatively to the elements of the field K). A vector $(a_1, \ldots, a_n) \in (K((\varepsilon^{1/\infty})))^n$ is called K-finite if each coordinate a_i $(1 \leqslant i \leqslant n)$ is not infinitely large relatively to the elements of K. For any K-finite element $a \in K((\varepsilon^{1/\infty}))$ its standard part $st(a) \in K$ is definable, namely $st(a) = \alpha_0$ in the case $\nu_0 = 0$ and $st(a) = 0$ if $\nu_0 > 0$. Analogously one can define the standard part of a Puiseux series from the field $\bar{K}((\varepsilon^{1/\infty}))$. For any K-finite vector $(a_1, \ldots, a_n) \in (K((\varepsilon^{1/\infty})))^n$ its standard part is defined by an equality

$$st(a_1, \ldots, a_n) = (st(a_1), \ldots, st(a_n)).$$

For a set $W \subset (K((\varepsilon^{1/\infty})))^n$ consisting of only K-finite vectors we define

$$st(W) = \{st(w) : w \in W\}.$$

It is well known (Tarski, 1951) that all real closed fields are elementary equivalent and that any extension between real closed fields is elementary. This means that if K_1, K_2 are real closed fields where $K_1 \subset K_2$ and Π is any closed formula (without free variables) of the first order theory of the field K_1, then the truth values of Π in the fields K_1 and K_2 coincide. We refer below to this statement as to the "transfer principle". Sometimes the first order theory of the real closed fields is called Tarski algebra.

Now we shall demonstrate, how the transfer principle can work and show (a known fact) that any semi-algebraic set over a real closed field K can be represented uniquely as a union of its components of connectivity, each in its turn being a semi-algebraic set. Consider a semi-algebraic set $W = \{\Pi\} \subset K^n$, determined by a quantifier-free formula Π of Tarski algebra with the atomic subformulas of the kind $(f \geqslant 0)$, where the polynomials $f \in K[X_1, \ldots, X_n]$. By the format of the formula Π we mean the sum of the number of its variables, the number of atomic subformulas and the degrees of the polynomials f.

In the case of the field $K = \mathbb{R}$ the set W is uniquely representable as the union of its components of connectivity

$$W = \bigcup_i W_i,$$

where every W_i is in its turn a semi-algebraic set (and connected in the euclidean topology). From the papers by Collins (1975) and Wüthrich (1976) one can deduce the existence of a function $\mathfrak{N}$ such that if the format of the formula Π is less than $\mathcal{N}$, then the number of the components W_i is less than $\mathfrak{N}(\mathcal{N})$ and, moreover, one can find quantifier-free formulas Π_i of Tarski algebra, each of format less than $\mathfrak{N}(\mathcal{N})$, such that $W_i = \{\Pi_i\}$. Indeed, the algorithms from Collins (1975) and Wüthrich (1976) allow to produce a cylindrical algebraic decomposition of a semi-algebraic set and as a corollary to produce the decomposition in the components of connectivity. For a given format $\mathcal{N}$ of an initial formula (with symbolic coefficients) each of the two algorithms can be represented as a rooted tree (directed outward the root) having vertices either with the out-degree one or out-degree three. To the root corresponds the initial formula, to any vertex of the tree with out-degree one corresponds an arithmetic operation, finally, to any vertex with out-degree three corresponds a polynomial. The computation for an arbitrary initial formula, with the specified coefficients substituted instead of the symbolic ones, proceeds along a suitable path of the tree starting from the root, performing the corresponding arithmetic operation in a vertex with out-degree one, and branching in a vertex with out-degree three according to the sign of the corresponding polynomial. This representation as a tree provides the desired function $\mathfrak{N}$.

Thus, for a given $\mathcal{N}$, one can obtain a formula $\Omega_{\mathcal{N}}$ of Tarski algebra (for the case of the field $K = \mathbb{R}$), expressing the existence of a decomposition of any semi-algebraic set $W = \{\Pi\}$ with the format of Π less than $\mathcal{N}$, into its components of connectivity

$$W = \bigcup_i \{\Pi_i\}$$

such that the format of every Π_i, and the number of them, are less than $\mathfrak{N}(\mathcal{N})$. Moreover, the formula $\Omega_{\mathcal{N}}$ states that for each pair of indices $i \neq j$ the components $\{\Pi_i\}$ and $\{\Pi_j\}$ are "separated", i.e. the following formula of Tarski algebra is valid:

$$\forall\, ((a_1, \ldots, a_n) \in \{\Pi_i\})\ \exists\, z > 0 (\forall\, (b_1, \ldots, b_n) \in \{\Pi_j\})\Big(\sum_{1 \leqslant l \leqslant n} (a_l - b_l)^2 \geqslant z\Big).$$

Besides, the formula $\Omega_{\mathcal{N}}$ claims the "connectedness" of every $\{\Pi_i\}$, this means that there do not exist two "separated" semi-algebraic subsets of $\{\Pi_i\}$, each determined by a quantifier-free formula of Tarski algebra with format less than $\mathfrak{N}(\mathfrak{N}(\mathcal{N}))$.

Apart from that, for given $\mathcal{N}, \mathcal{M}$ one can prove (for the case of the field $K = \mathbb{R}$) a formula $\Omega_{\mathcal{N},\mathcal{M}}$ of Tarski algebra expressing the following. If $\{\Pi\}$ (where the format of Π is less than $\mathcal{N}$) can be represented as a union of more than one and less than $\mathcal{M}$ pairwise "separated" semi-algebraic sets, each being determined by a quantifier-free formula of Tarski algebra of format less than $\mathcal{M}$, then $\{\Pi\}$ can be represented as a union of more than one and less than $\mathfrak{N}(\mathcal{N})$ pairwise "separated" semi-algebraic "connected" sets, each being determined by a quantifier-free formula of Tarski algebra of format less than $\mathfrak{N}(\mathcal{N})$.

Applying the transfer principle to all the formulas $\Omega_{\mathcal{N}}, \Omega_{\mathcal{N},\mathcal{M}}$, one concludes that any semi-algebraic set (over a real closed field K) can be uniquely represented as a union of its pairwise "separated" "components of connectivity", moreover, each component is semi-algebraic and is "connected", i.e. cannot be represented as a union of a finite number of pairwise "separated" semi-algebraic sets. Below we utilise the terms "connected semi-algebraic set" and "components of connectivity of a semi-algebraic set" without quotation marks since the notion of connectedness in any topology will not be considered.

Denote by

$$\mathscr{D}_w(R) = \{(X_1-w_1)^2+\ldots+(X_n-w_n)^2 \leqslant R^2\}$$

the closed ball of radius $R \geqslant 0$ with the centre in the point $w=(w_1, \ldots, w_n)$.

LEMMA 1.

(a) *Any semi-algebraic set $W \subset (\widetilde{K(\varepsilon)})^n$ consisting only of K-finite points lies in a ball $\mathscr{D}_0(R)$ for a certain radius $R \in K$.*

(b) *Let $V \subset K^n$, $W \subset (\widetilde{K(\varepsilon)})^n$ be semi-algebraic sets and let, apart from that, W consist only of K-finite points and $st(W) = V$. Let*

$$V = \bigcup_m V_m, \quad W = \bigcup_l W_l$$

be the decompositions of the sets V, W respectively, into their components of connectivity. Then, for every index m, there exist such indices $l_1, \ldots, l_s$ that $st(W_{l_1} \cup \ldots \cup W_{l_s}) = V_m$. Moreover, for each index l there is a unique index m such that $st(W_l) \subset V_m$.

PROOF. (a) Assume that, on the contrary, for some index $1 \leqslant i \leqslant n$ and any $\alpha \in K$, there is a point $w = (w_1, \ldots, w_n) \in W$ such that the absolute value $|w_i| > \alpha$. Consider the projection $\pi: (\widetilde{K(\varepsilon)})^n \to \widetilde{K(\varepsilon)}$ on the coordinate X_i. Then $\pi(W) \subset \widetilde{K(\varepsilon)}$ is a semi-algebraic set (Tarski, 1951). Therefore, $\pi(W)$ coincides with the union of a finite number of intervals (maybe endless in one or both sides). Consider the extreme right interval (analogously one can consider the extreme left interval). It cannot be of the form $\{X_i > a\}$ or $\{X_i \geqslant a\}$, otherwise the set W would contain points with infinitely large coordinate X_i. Thus, the extreme right interval has one of the four following forms: $\{a \leqslant X_i \leqslant b\}$, or $\{a < X_i \leqslant b\}$, or $\{a \leqslant X_i < b\}$, or $\{a < X_i < b\}$. If the element b is infinitely large (relatively to the field K), then there exists an infinitely large element $c \in \widetilde{K(\varepsilon)}$ such that $a < c < b$ in the case when $a < b$. Otherwise, put $c = a = b$, which again leads to a contradiction. Hence, the element b is K-finite. The extreme left interval satisfies the analogous property. So, we arrive at a contradiction with the assumption at the beginning of the proof.

(b) First of all we shall show that for any semi-algebraic set $V \subset K^n$ and its component of connectivity V_1, one can construct an open (in the topology with the base consisting of all open balls) semi-algebraic set $U \subset K^n$ such that $V_1 \subset U$ and, besides that, for every point $v \in V \backslash V_1$ there exists $\tau > 0$, for which the intersection $U \cap \mathscr{D}_v(\tau) = \phi$ (in other words, $V \cap \bar{U} = V_1$, where $\bar{U}$ denotes the topological closure of U). Namely, as U one can take the set of all points $u \in K^n$, satisfying the following requirement. There exist $0 \leqslant \tau^{(u)} \in K$, $0 < \tau_0^{(u)} \in K$ and a point $v_1 \in V_1$ such that the distance $\|v_1 - u\| \leqslant \tau^{(u)}$ and for each point $v \in V \backslash V_1$ the distance $\|v - u\| \geqslant \tau^{(u)} + \tau_0^{(u)}$.

The latter requirement can be expressed by a formula of Tarski algebra, therefore the set $U \subset K^n$ is semi-algebraic (Tarski, 1951). The set $V_1 \subset U$ since, for any point $v_1 \in V_1$, one can put $\tau^{(v_1)} = 0$ and take $\tau_0^{(v_1)}$ from the definition of "separation" (see above). Now let us show that U is open. Let a point $u \in U$, let us prove the inclusion $\mathscr{D}_u(\tau_0^{(u)}/3) \subset U$. For every point $u_1 \in \mathscr{D}_u(\tau_0^{(u)}/3)$ put $\tau^{(u_1)} = \tau^{(u)} + \tau_0^{(u)}/3$, $\tau_0^{(u_1)} = \tau_0^{(u)}/3$. Then these $\tau^{(u_1)}$, $\tau_0^{(u_1)}$ are the required ones. Indeed, there is such a point $v_1 \in V_1$ that $\|u - v_1\| \leqslant \tau^{(u)}$, henceforth,

$$\|u_1 - v_1\| \leqslant \|u_1 - u\| + \|u - v_1\| \leqslant \tau^{(u_1)}.$$

Apart from that, for each point $v \in V \setminus V_1$, the following inequalities are valid:

$$\|v-u_1\| \geqslant \|v-u\| - \|u-u_1\| \geqslant \tau^{(u)} + \tau_0^{(u)} - \tau_0^{(u)}/3 = \tau^{(u_1)} + \tau_0^{(u_1)}.$$

Finally, let a point $v \in V \setminus V_1$. According to the definition of the "separation", there exists $0 < \tau_1 \in K$ such that the intersection $\mathscr{D}_v(\tau_1) \cap V_1 = \phi$. Let us check that $\mathscr{D}_v(\tau_1/2) \cap U = \phi$. Suppose the contrary, let a certain point $u_2 \in \mathscr{D}_v(\tau_1/2) \cap U$. Then, by virtue of the requirement formulated above,

$$\tau^{(u_2)} + \tau_0^{(u_2)} \leqslant \|u_2 - v\| \leqslant \tau_1/2,$$

but on the other hand,

$$\mathscr{D}_{u_2}(\tau_1/2) \cap V_1 \subset \mathscr{D}_v(\tau_1) \cap V_1 = \phi,$$

therefore, $\tau^{(u_2)} > \tau_1/2$. The obtained contradiction completes the proof of the properties of the constructed set U.

In order to prove (b) it is sufficient to show that for any component of connectivity W_l there is a unique component V_m containing the set $st(W_l)$. Assume that, on the contrary, there exist for definiteness some points

$$v_1^{(0)} \in V_1 \cap st(W_l), \quad v_2^{(0)} \in V_2 \cap st(W_l).$$

Consider points $w_1^{(0)}, w_2^{(0)} \in W_l$ such that $st(w_1^{(0)}) = v_1^{(0)}$, $st(w_2^{(0)}) = v_2^{(0)}$. The semi-algebraic set constructed above U is $\{\Pi\} \subset K^n$ for a relevant quantifier-free formula Π of Tarski algebra. Introduce a semi-algebraic set $U^{(\varepsilon)} = \{\Pi\} \subset (\widetilde{K(\varepsilon)})^n$ determined by the same formula Π. Let a point $v_1 \in V_1$. There exists $0 < \tau_1 \in K$ such that $\mathscr{D}_{v_1}(\tau_1) \subset U$. In other words, the following statement is true:

$$\forall\, x\, (\|x - v_1\| \leqslant \tau_1 \Rightarrow \Pi(x)).$$

The latter statement can be expressed by a formula of Tarski algebra. Hence, this formula is true also over the field $\widetilde{K(\varepsilon)}$ by the transfer principle. This entails the inclusion $\mathscr{D}_{v_1}(\tau_1) \subset U^{(\varepsilon)}$. Let a point $v_2 \in V \setminus V_1$. Then for a suitable $0 < \tau_2 \in K$ the intersection $\mathscr{D}_{v_2}(\tau_2) \cap U = \phi$. Reasoning analogously as above, one can conclude that $\mathscr{D}_{v_2}(\tau_2) \cap U^{(\varepsilon)} = \phi$. Thus, if a point $w_1 \in W_l \cap U^{(\varepsilon)}$, then $st(w_1) \in (V \cap U) = V_1$, and if a point $w_2 \in W_l \setminus U^{(\varepsilon)}$, then $st(w_2) \in V \setminus U = V \setminus V_1$, taking into account that the standard parts $st(w_1), st(w_2)$ are definable and the distances $\|w_1 - st(w_1)\|$, $\|w_2 - st(w_2)\|$ are infinitesimals.

Let us check that the semi-algebraic set $W_l \cap U^{(\varepsilon)}$ is separated from its complement $W_l \setminus U^{(\varepsilon)}$ in the set W_l. According to what we proved above, the points $w_1^{(0)} \in W_l \cap U^{(\varepsilon)}$, $w_2^{(0)} \in W_l \setminus U^{(\varepsilon)}$. Therefore both sets $W_l \cap U^{(\varepsilon)}$ and $W_l \setminus U^{(\varepsilon)}$ are non-empty. Let a point $w_1 \in W_l \cap U^{(\varepsilon)}$. Then for a suitable $0 < \tau_3 \in K$ the inclusion $\mathscr{D}_{st(w_1)}(\tau_3) \subset U$ is true. This implies $\mathscr{D}_{w_1}(\tau_3/2) \cap (W_l \setminus U^{(\varepsilon)}) = \phi$. Similarly, one can consider a point $w_2 \in W_l \setminus U^{(\varepsilon)}$. This contradicts to the connectivity of W_l and concludes the proof of the lemma.

Apparently, the set $st(W) \subset K^n$ is semi-algebraic for any semi-algebraic set $W \subset (\widetilde{K(\varepsilon)})^n$ (consisting only of not infinitely large points relatively to the field K), but we shall not need this statement further and shall not dwell on its proof.

Define the boundary ∂W of a set $W \subset K^n$ as the set of points $w \in K^n$ such that for each $\tau > 0$ both sets $\mathscr{D}_w(\tau) \cap W \neq \phi$, $\mathscr{D}_w(\tau) \setminus W \neq \phi$. In the following lemma the polynomials $f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$ and the element $0 < R \in K$. Introduce the semi-algebraic sets

$$V = \{(f_1 \geqslant 0) \& \ldots \& (f_k \geqslant 0)\} \subset K^n,$$

$$V^{(\varepsilon)} = \{(f_1 + \varepsilon > 0) \& \ldots \& (f_k + \varepsilon > 0)\} \subset (\widetilde{K(\varepsilon)})^n$$

and the polynomial

$$g = (f_1 + \varepsilon) \ldots (f_k + \varepsilon) - \varepsilon^k \in K[\varepsilon][X_1, \ldots, X_n].$$

LEMMA 2.

(*a*) $V \cap \mathcal{D}_0(R) = st(V^{(\varepsilon)} \cap \mathcal{D}_0(R))$

$$= st(V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathcal{D}_0(R)) \subset (V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathcal{D}_0(R));$$

(*b*) *The boundary*

$$\partial(V^{(\varepsilon)} \cap \{g \geqslant 0\}) \subset (V^{(\varepsilon)} \cap \{g \geqslant 0\})$$

and, for every point $u \in \partial(V^{(\varepsilon)} \cap \{g \geqslant 0\})$, *the equality* $g(u) = 0$ *is fulfilled.*

(*c*) *On any component of connectivity* $U_1 \subset (\widetilde{K(\varepsilon)})^n$ *of the semi-algebraic set* $\{g \geqslant 0\}$ *each polynomial* $f_i + \varepsilon$, $1 \leqslant i \leqslant k$ *has a constant sign.*

(*d*) *Let a point* $x \in \partial V \subset V \subset K^n$. *Then there exists a point*

$$z \in (V^{(\varepsilon)} \cap \{g = 0\}) \subset (\widetilde{K(\varepsilon)})^n$$

such that the distance $\|z - x\|$ *is infinitesimal relatively to the field* K.

PROOF. (a) Let $w \in V^{(\varepsilon)} \cap \mathcal{D}_0(R)$. Then the elements $f_i(w) - f_i(st(w))$, $1 \leqslant i \leqslant k$ and $\|w - st(w)\|$ are infinitesimals, therefore, $st(w) \in V \cap \mathcal{D}_0(R)$. Now let $v \in V \cap \mathcal{D}_0(R)$. Then $f_i(v) + \varepsilon \geqslant \varepsilon > 0$ and $g(v) \geqslant 0$. This entails $v \in V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathcal{D}_0(R)$ and, taking into account the equality $v = st(v)$, one deduces that

$$v \in st(V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathcal{D}_0(R)).$$

(b) Let $w \in \partial(V^{(\varepsilon)} \cap \{g \geqslant 0\})$. Assume that either $f_i(w) + \varepsilon < \beta < 0$ for a certain $1 \leqslant i \leqslant k$ or, respectively, $g(w) < \beta < 0$, where $\beta \in \widetilde{K(\varepsilon)}$. There exists $0 < \tau \in \widetilde{K(\varepsilon)}$ such that for any point $w_1 \in \mathcal{D}_w(\tau)$ the inequalities $|f_i(w_1) - f_i(w)| \leqslant -\beta/2$, $1 \leqslant i \leqslant k$ and $|g(w_1) - g(w)| \leqslant -\beta/2$ are valid. On the other hand, according to the definition of the boundary, one can find a point $w_2 \in (V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathcal{D}_w(\tau))$. This leads to a contradiction to the assumption. Thus, we have obtained the inequalities $f_i(w) + \varepsilon \geqslant 0$, $1 \leqslant i \leqslant k$ and $g(w) \geqslant 0$. If $f_i(w) + \varepsilon = 0$ for a certain i, then $g(w) = -\varepsilon^k < 0$. Hence, $w \in (V^{(\varepsilon)} \cap \{g \geqslant 0\})$, i.e.

$$\partial(V^{(\varepsilon)} \cap \{g \geqslant 0\}) \subset (V^{(\varepsilon)} \cap \{g \geqslant 0\}).$$

Reasoning analogously one can also prove that in every point v on the boundary of an arbitrary semi-algebraic set

$$\{(g^{(1)} > 0) \& \ldots \& (g^{(s)} > 0) \& (g^{(s+1)} \geqslant 0) \& \ldots \& (g^{(m)} \geqslant 0)\}$$

the inequalities $g^{(i)}(v) \geqslant 0$ for all $1 \leqslant i \leqslant m$ are true and an equality $g^{(i_0)}(v) = 0$ is fulfilled for a certain $1 \leqslant i_0 \leqslant m$. This implies the equality $g(w) = 0$ for any point $w \in \partial(V^{(\varepsilon)} \cap \{g \geqslant 0\})$ by that proved above.

(c) Suppose that a polynomial $f_i + \varepsilon$ changes its sign on U_1 for some $1 \leqslant i \leqslant k$. Then there exists such a point $x \in U_1$ that $(f_i + \varepsilon)(x) = 0$ by virtue of the connectivity of U_1. This leads to a contradiction since $g(x) = -\varepsilon^k < 0$.

(d) For each fixed m, the following formula of Tarski algebra

$$\begin{aligned}&\forall\, x\ \forall\, h(((\deg(h) \leqslant m) \& (h(x) > 0))\\ &\qquad \Rightarrow ((\forall\ y(h(y) > 0)) \vee \exists\, \tau\ \exists\, z\ \forall\, z_1((\|x - z\| = \tau) \& (h(z) = 0) \& ((\|x - z_1\| < z)\\ &\qquad \Rightarrow (h(z_1) > 0)))))\end{aligned}$$

is true where $h \in K[X_1, \ldots, X_n]$ denotes a polynomial with degree $\deg h \leqslant m$. One can prove it, first, for the case $K = \mathbb{R}$ and then use the transfer principle. Apply the formula to the polynomial $h = g$ and the point $x \in \partial V$. Note that $f_i(x) \geqslant 0$ for all $1 \leqslant i \leqslant k$ (see the proof of item (b) of the present lemma). Therefore $g(x) \geqslant 0$. If $g(x) = 0$ we can take $z = x$ because of item (a) of the present lemma. So we assume that $g(x) > 0$.

If $\forall\, y(g(y)>0)$ is fulfilled, then $\forall\, y((f_i+\varepsilon)(y)>0)$ is valid for all $1\leqslant i\leqslant k$ by virtue of item (c) of the present lemma. But, on the other hand, there exists a point $y_0\in K^n$ and an index $1\leqslant i_0\leqslant k$ satisfying the inequality $0>f_{i_0}(y_0)\in K$, i.e. $y_0\notin V$ taking into account that $x\in\partial V$. Hence, $f_{i_0}(y_0)+\varepsilon<0$ and we obtain the contradiction.

Thus, one can find a point $z\in(\widetilde{K(\varepsilon)})^n$ such that $g(z)=0$ and for any point $z_1\in\mathscr{D}_x(\tau)$, where $\tau=\|z-x\|$, the inequality $g(z_1)\geqslant 0$ is true. Then item (c) of the present lemma implies the inclusion $\mathscr{D}_x(\tau)\subset V^{(\varepsilon)}\cap\{g\geqslant 0\}$. So, if τ is infinitesimal, then z is the desired point. Otherwise, let $0<\tau_1<\tau$ and $\tau_1\in K$. Then item (a) of the present lemma implies that for each point $y\in\mathscr{D}_x(\tau_1)\cap K^n$, the inclusion $y\in V$ is valid. In other words, $\mathscr{D}_x(\tau_1)\subset V$. This contradicts with the condition $x\in\partial V$ and completes the proof of the lemma.

Lemma 3. *Let $0\not\equiv f\in K[X_1,\ldots,X_n]$ and assume that, for any point $x\in(\widetilde{K(\varepsilon)})^n$, the inequality $f(x)\geqslant 0$ is fulfilled. Assume that $f(a)=0$ for some $a\in K^n$. Then one can find a point $\alpha\in(\widetilde{K(\varepsilon)})^n$ such that the distance $\|a-\alpha\|$ is infinitesimal, the equality $f(\alpha)=\varepsilon$ is correct, and apart from that, $\|\alpha\|<\|a\|$ provided that $a\neq 0$.*

Proof. One can find a point $b\in K^n$ satisfying the requirement $0<\beta=f(b)\in K$, and besides that, if $a\neq 0$, then $\|b\|<\|a\|$. We can reduce the whole proof to the case of one variable ($n=1$) introducing a polynomial

$$h(Z)=f(a+Z(b-a))\in K[Z].$$

Evidently $h(0)=0$, $h(1)=\beta$. There exists $z\in\widetilde{K(\varepsilon)}$ such that $0<z<1$ and $h(z)=\varepsilon$ (obviously, the number of elements z satisfying the latter conditions does not exceed $\deg(h)$). Denote by z_0 the least among these elements z. Then, for any $0<z_1<z_0$, where $z_1\in\widetilde{K(\varepsilon)}$, the inequalities $0\leqslant h(z_1)<\varepsilon$ are true. The element z_0 is infinitesimal, since otherwise there exists an element $z_1\in K$, for which the inequalities $0<z_1<z_0$ and $0<h(z_1)\in K$ are valid. This leads to the contradiction. One can put $\alpha=a+z_0(b-a)$, with $\|\alpha\|\leqslant(1-z_0)\|a\|+z_0\|b\|<\|a\|$, provided that $a\neq 0$. The lemma is proved.

Now we proceed to considering the critical values of a polynomial $f\in K[X_1,\ldots,X_n]$. An element $z\in K$ is called a critical value of the polynomial f if the system of equations

$$f-z=\frac{\partial f}{\partial X_1}=\ldots=\frac{\partial f}{\partial X_n}=0 \tag{3}$$

has a solution in the space K^n.

Let Π_1 be any quantifier-free formula of the first order theory of the field $\mathbb{R}$ and $W=\{\Pi_1\}\subset\mathbb{R}^n$ be the semi-algebraic set. If $\pi:\mathbb{R}^n\to\mathbb{R}^m$ is a linear projection, then Tarski's theorem (Tarski, 1951) states that $\pi(W)\subset\mathbb{R}^m$ is also a semi-algebraic set. Moreover, one can construct a quantifier-free formula Π_2, defined over the same field as the formula Π_1, such that $\pi(W)=\{\Pi_2\}$ and the format of Π_2 is bounded by a function depending only on the format of Π_1 (see e.g. Collins, 1975; Wüthrich, 1976). Therefore, the statement of Tarski theorem is also correct for an arbitrary real closed field K.

Observe that the set of all critical values of a polynomial f coincides with the projection of the semi-algebraic set consisting of all roots of system (3) in the space K^{n+1} with coordinates $Z, X_1,\ldots,X_n$ on the line K^1 defined by coordinate Z. Therefore, the set of all critical values is semi-algebraic over the field generated by the coefficients of the polynomial f according to Tarski's theorem. From this statement and Sard's theorem (asserting that in the case $K=\mathbb{R}$, the set of critical values has the measure null, see e.g. Milnor (1965), one infers that, in the case $K=\mathbb{R}$, there is a finite number of critical values z (see (3)).

The result of Milnor (1964) implies that the number of components of connectivity of the semialgebraic set consisting of all roots of system (3) in the space $\mathbb{R}^{n+1}$ is not greater than $\mathscr{P}((\deg(f))^n)$. Hence, the number of critical values also does not exceed $\mathscr{P}((\deg(f))^n)$. For polynomials f of a given degree $\deg(f)$ the latter statement can be expressed by a formula of Tarski algebra. Therefore, the same bound on the number of critical values is true also for an arbitrary real closed field K. In particular, all critical values of a polynomial are algebraic over the field generated by the coefficients of the polynomial.

LEMMA 4.

(*a*) *If* $f \in K[X_1, \ldots, X_n]$, *then an element* ε *infinitesimal relatively to the field* K *is not a critical value of polynomial* f *(over the field* $\widetilde{K(\varepsilon)}$*).*

(*b*) *Let* $f \in K[X_1, \ldots, X_n]$ *and* $z \in K$. *If* z *is not a critical value of polynomial* f *then, for any vector* $0 \neq u \in K^n$ *and every component of connectivity* W *of the variety* $\{f = z\} \subset K^n$ *such that* $W \subset \mathscr{D}_0(R)$ *for a certain* $R \in K$, *one can find a point* $w \in W$ *such that the gradient* $((\partial f/\partial X_1)(w), \ldots, (\partial f/\partial X_n)(w)) \neq 0$ *in this point is collinear to vector* u.

PROOF. (a) Item (a) follows from the fact that all the critical values are algebraic over the field K.

(b) In the case $K = \mathbb{R}$, the statement is proved, e.g. in Thorpe (1979). For an arbitrary real closed field K make use of the transfer principle.

2. Finding Real Roots of a Polynomial

Let a polynomial $g_1 \in \mathbb{Z}[\varepsilon_1][X_1, \ldots, X_{n-1}]$ be given where $\varepsilon_1 > 0$ is infinitesimal relatively to the field $\tilde{\mathbb{Q}}$. We assume the fulfilment of the following inequalities $\deg_{\varepsilon_1, X_1, \ldots, X_{n-1}}(g_1) < d$ and $l(g_1) \leq M$ (cf. (2) in the introduction). Define the field $F_1 = \widetilde{\mathbb{Q}(\varepsilon_1)}$. In the course of this section we fix a natural number R (it will be specified in the next section).

In the present section we look for roots of the equation $g_1 = 0$ in a ball $\mathscr{D}_0(R) \subset F_1^{n-1}$. The general case of finding the solutions of a system of inequalities will be reduced to this one in section 3. We introduce a new variable X_n and the polynomial $g = g_1^2 + (X_1^2 + \ldots + X_n^2 - R^2)^2$, which yields the semi-algebraic set $V_0 = \{g = 0\} \subset F_1^n$. Evidently, $\pi(V_0) = \{g_1 = 0\} \cap \mathscr{D}_0(R)$ where the projection π is defined by the formula $\pi(X_1, \ldots, X_n) = (X_1, \ldots, X_{n-1})$. The algorithm described in the present section, produces a certain representative set $\mathscr{S}' \subset V_0$ for the semi-algebraic set V_0 (or determines that $V_0 = \phi$) and, incidentally, a representative set $\mathscr{S} = \pi(\mathscr{S}')$ for the set $\pi(V_0)$.

Let an element $\varepsilon > 0$ be infinitesimal relatively to the field F_1. Define $F = \widetilde{F_1(\varepsilon)}$. Then ε is not the critical value of the polynomial g according to lemma 4(a). Introduce the semi-algebraic set $V_\varepsilon = \{g = \varepsilon\} \subset F^n$, observe that $V_\varepsilon \subset \mathscr{D}_0(R + \varepsilon^{1/4}) \subset \mathscr{D}_0(R+1)$. In the present section the term "standard part" *st* concerns the situation when the field $K = F_1$ (see section 1), i.e. for an element $a \in F$ its standard part $st(a) \in F_1$, provided that $st(a)$ is definable.

Denote by $N = (4d)^n$ and introduce the family $\Gamma \subset \mathbb{Z}^{n-1}$ consisting of N^{n-1} integer vectors $\Gamma = \{\gamma = (\gamma_2, \ldots, \gamma_n)\}$ where each γ_i runs independently over all values $1, \ldots, N$.

For every index $1 \leqslant i \leqslant n$ and a vector $\gamma = (\gamma_2, \ldots, \gamma_n) \in \Gamma$, consider the following system of equations where

$\Delta = \sum_{1 \leqslant j \leqslant n} (\partial g/\partial X_j)^2$:

$$g - \varepsilon = \left(\frac{\partial g}{\partial X_2}\right)^2 - \frac{\gamma_2}{Nn}\Delta = \ldots = \left(\frac{\partial g}{\partial X_i}\right)^2 - \frac{\gamma_i}{Nn}\Delta = 0. \tag{4i}$$

Below, in the course of the following lemma, we consider $g \in \mathbb{Q}[\varepsilon_1][X_1, \ldots, X_n]$ as an arbitrary polynomial, and let $\bar{W}_{\gamma_2, \ldots, \gamma_i} \subset \bar{F}^n$ denote the variety of all points defined over the algebraic closure $\bar{F} = F[\sqrt{-1}]$ satisfying the system (4i) for the chosen polynomial g.

LEMMA 5. *There exist integers $1 \leqslant \gamma_2, \ldots, \gamma_i \leqslant N$ such that for each $1 \leqslant i \leqslant n$ any absolutely irreducible component $\bar{U}_m^{(i)} \subset \bar{F}^n$ of the variety $\bar{W}_{\gamma_2, \ldots, \gamma_i}$, containing at least one point from the space F^n, has a dimension $\dim_{\bar{F}}(\bar{U}_m^{(i)}) = n - i$.*

The proof of the lemma and the construction of the $\gamma_2, \ldots, \gamma_i$ will be conducted by induction on i. The base of induction for $i = 1$ is clear. Let us prove the lemma for arbitrary $i > 1$ supposing that for smaller numbers the lemma is already proved and the corresponding $1 \leqslant \gamma_2, \ldots, \gamma_{i-1} \leqslant N$ are constructed. Let an absolutely irreducible component $\bar{U}_l^{(i-1)}$ of the variety $\bar{W}_{\gamma_2, \ldots, \gamma_{i-1}}$ contain at least one point from F^n. Then for at most one $1 \leqslant \varkappa \leqslant N$ the polynomial $(\partial g/\partial X_i)^2 - \varkappa\Delta/Nn$ vanishes identically on $\bar{U}_l^{(i-1)}$. Otherwise, Δ would vanish on $\bar{U}_l^{(i-1)}$ and also would vanish all the partial derivatives $(\partial g/\partial X_j)$, $1 \leqslant j \leqslant n$. In particular, the partial derivatives would vanish at every point of the non-empty set $\bar{U}_l^{(i-1)} \cap F^n \subset \{g = \varepsilon\}$. We get a contradiction since ε is not a critical point of the polynomial g by virtue of lemma 4(a).

According to Bezout's inequality (see Shafarevich, 1974; Heintz, 1983) the number of components of the kind $\bar{U}_l^{(i-1)}$ is less than N. Therefore, for a suitable $1 \leqslant \varkappa \leqslant N$, the polynomial $(\partial g/\partial X_i)^2 - \varkappa\Delta/Nn$ does not vanish identically on any component of the kind $\bar{U}_l^{(i-1)}$ such that $\bar{U}_l^{(i-1)} \cap F^n \neq \phi$. Put $\gamma_i = \varkappa$. Then the dimension of each absolutely irreducible component of the variety

$$\{(\partial g/\partial X_i)^2 - \gamma_i\Delta/Nn = 0\} \cap \bar{U}_l^{(i-1)} \subset \bar{F}^n$$

equals to $(n-i)$, provided that $\bar{U}_l^{(i-1)} \cap F^n \neq \phi$, according to the inductive hypothesis and to the theorem on the dimension of intersection (Shafarevich, 1974). The lemma is proved.

Lemmas 4(a), 4(b), (5) entail (taking into account that the set V_ε is situated in the ball $\mathscr{D}_0(R+1)$) the following

COROLLARY. *There exists a vector $\gamma^{(1)} = (\gamma_2, \ldots, \gamma_n) \in \Gamma$ such that every solution from F^n of the system (4n) is an isolated point in the variety $\bar{V}^{(\varepsilon)} = \bar{W}_{\gamma_2, \ldots, \gamma_n} \subset \bar{F}^n$ of all the points satisfying the system (4n). Moreover, any component of connectivity of the semi-algebraic set $V_\varepsilon = \{g = \varepsilon\} \subset F^n$ contains a certain solution of the system (4n) for each vector $\gamma^{(1)} \in \Gamma$.*

Now we proceed to producing a representative set for the semi-algebraic set V_ε and later on for the semi-algebraic set V_0.

The algorithm looks over all the vectors $\gamma \in \Gamma$. Let us fix a certain vector

$\gamma = (\gamma_2, \ldots, \gamma_n) \in \Gamma$. Applying the algorithm from proposition 2 (see also theorem 2 from Chistov & Grigor'ev, 1984), to the system (4n) one can decompose the variety

$$\bar{V}^{(\varepsilon)} = \bigcup_j \bar{V}_j^{(\varepsilon)}$$

on the components $\bar{V}_j^{(\varepsilon)}$ defined and irreducible over the field $\mathbb{Q}(\varepsilon_1, \varepsilon)$.

Select among them all the null-dimensional components. Thus, let $\dim \bar{V}_j^{(\varepsilon)} = 0$ for some j. The algorithm from proposition 2 represents the component $\bar{V}_j^{(\varepsilon)}$ in the following form. A polynomial $\Phi \in \mathbb{Q}[\varepsilon_1, \varepsilon][Z]$, irreducible over $\mathbb{Q}$, is constructed such that for every point $(\xi_1, \ldots, \xi_n) \in \bar{V}_j^{(\varepsilon)}$ the field

$$\mathbb{Q}(\varepsilon_1, \varepsilon)(\xi_1, \ldots, \xi_n) = \mathbb{Q}(\varepsilon_1, \varepsilon)[\theta] \simeq \mathbb{Q}(\varepsilon_1, \varepsilon)[Z]/(\Phi),$$

where $\Phi(\theta) = 0$ and the primitive element

$$\theta = \sum_{1 \leqslant j \leqslant n} \lambda_i \xi_i$$

for appropriate natural numbers $1 \leqslant \lambda_i \leqslant \deg_z(\Phi) \leqslant N$. Apart from that, the algorithm explicitly finds expressions

$$\xi_i = \xi_i(\theta) = \sum_{0 \leqslant e < \deg \Phi} \beta_i^{(e)} \theta^e$$

for the relevant $\beta_i^{(e)} \in \mathbb{Q}(\varepsilon_1, \varepsilon)$, $1 \leqslant i \leqslant n$, $0 \leqslant e < \deg_z(\Phi)$. All points of the component $\bar{V}_j^{(\varepsilon)}$ are conjugate over the field $\mathbb{Q}(\varepsilon_1, \varepsilon)$ and they correspond bijectively to roots (from the field $\bar{F}$) of the polynomial Φ. Finally, the algorithm yields irreducible (over $\mathbb{Q}$) polynomials $\Phi_1, \ldots, \Phi_n \in \mathbb{Q}[\varepsilon_1, \varepsilon][Z]$ such that $\Phi_i(\xi_i) = 0$, $1 \leqslant i \leqslant n$.

The following bounds are valid: the degrees

$$\deg_{\varepsilon_1, \varepsilon, Z}(\Phi), \deg_{\varepsilon_1, \varepsilon, Z}(\Phi_i), \deg_{\varepsilon_1, \varepsilon}(\xi_i(\theta)) \leqslant \mathscr{P}(d^n)$$

and the lengths of coefficients

$$l(\Phi), l(\Phi_i), l(\xi_i(\theta)) \leqslant (M + \log R)\mathscr{P}(d^n)$$

for the component $\bar{V}_j^{(\varepsilon)}$ and any index $1 \leqslant i \leqslant n$ by virtue of proposition 2.

Observe that a family of points of the kind $(\xi_1, \ldots, \xi_n) \in \bar{V}_j^{(\varepsilon)} \cap F^n$ for all possible vectors $\gamma \in \Gamma$ and null-dimensional components $\bar{V}_j^{(\varepsilon)}$ forms a representative set for the semi-algebraic set V_ε according to the corollary of lemma 5 (see above).

Now we shall turn to producing a representative set $\mathscr{S}'$ for the semi-algebraic set V_0.

If $(\xi_1, \ldots, \xi_n) \in \bar{V}_j^{(\varepsilon)} \cap F^n$, then taking into account the inequality $\xi_1^2 + \ldots + \xi_n^2 < R^2 + 1$ one concludes that the standard part $st(\xi_1, \ldots, \xi_n) \in F_1^n$ is defined. On the other hand, $0 = st(\phi_i(\xi_i)) = \psi_i(st(\xi_i))$, where we denote by $\psi_i = st(\phi_i) \in \mathbb{Q}[\varepsilon_1][Z]$ the polynomial obtained from Φ_i by coefficient-wise taking of a standard part. Notice that the polynomials ψ_i satisfy the same bounds as the polynomials Φ_i(see above).

In the sequel, we shall need the following auxiliary

LEMMA 6. *Let*

$$\theta' = \sum_{1 \leqslant j \leqslant n} \lambda_i' \xi_i \in \mathbb{Q}(\varepsilon_1, \varepsilon)(\xi_1, \ldots, \xi_n),$$

where the natural numbers $1 \leqslant \lambda_i' \leqslant \deg_z(\Phi)$. *Let* $\Phi^{(1)} \in \mathbb{Z}[\varepsilon_1, \varepsilon][Z]$ *be an irreducible (over* $\mathbb{Z}$*) polynomial such that* $\Phi^{(1)}(\theta') = 0$. *Then the following bounds are fulfilled:*

$$\deg_z(\Phi^{(1)}) \leqslant \deg_z(\Phi); \quad \deg_{\varepsilon_1, \varepsilon}(\Phi^{(1)}) \leqslant \mathscr{P}(d^n)$$

and

$$l(\Phi^{(1)}) \leqslant (M + \log R)\mathscr{P}(d^n).$$

PROOF. Represent $\theta' = q(\theta)$ for a suitable polynomial $q(Z) \in \mathbb{Q}(\varepsilon_1, \varepsilon)[Z]$, making use of the expressions $\xi_i(\theta)$, then the following bounds are true:

$$\deg_{\varepsilon_1, \varepsilon}(q) \leqslant \mathscr{P}(d^n) \quad \text{and} \quad l(q) \leqslant (M + \log R)\mathscr{P}(d^n).$$

From the latter bounds the following ones for the powers q^e, $1 \leqslant e \leqslant \deg_z(\Phi)$ can be deduced:

$$\deg_{\varepsilon_1, \varepsilon}(q^e) \leqslant \mathscr{P}(d^n, \deg_z(\Phi)) \leqslant \mathscr{P}(d^n) \quad \text{and} \quad l(q^e) \leqslant (M + \log R)\mathscr{P}(d^n).$$

For the remainders rem (q^e, Φ) of dividing polynomial q^e by polynomial Φ over the field $\mathbb{Q}(\varepsilon_1, \varepsilon)$ the same bounds are correct. The following inequality is obvious:

$$\deg_z(\Phi^{(1)}) = [\mathbb{Q}(\varepsilon_1, \varepsilon)[\theta'] : \mathbb{Q}(\varepsilon_1, \varepsilon)] \leqslant [\mathbb{Q}(\varepsilon_1, \varepsilon)(\xi_1, \ldots, \xi_n) : \mathbb{Q}(\varepsilon_1, \varepsilon)] = \deg_z(\Phi)$$

(here and further $[H_1 : H_2]$ for a finite extension $H_2 \subset H_1$ of a field denotes its degree). The equality

$$\sum_{0 \leqslant e \leqslant \deg(\Phi^{(1)})} \alpha_e \operatorname{rem}(q^e, \Phi) = 0,$$

where $\alpha_e \in \mathbb{Z}[\varepsilon_1, \varepsilon]$ are the coefficients of the polynomial $\Phi^{(1)}$, gives a system of homogeneous linear equations in the indeterminates α_e having a one-dimensional space of solutions. Involving Cramer's rule one can infer the bounds

$$\deg_{\varepsilon_1, \varepsilon}(\alpha_e) \leqslant \mathscr{P}(d^n) \quad \text{and} \quad l(\alpha_e) \leqslant (M + \log R)\mathscr{P}(d^n),$$

which completes the proof of the lemma.

Consider an arbitrary element of the sort

$$\tau = \sum_{1 \leqslant i \leqslant n} \lambda_i' st(\xi_i) \in \bar{F}_1,$$

provided that $st(\xi_i) \in F_1$, $1 \leqslant i \leqslant n$ are defined, where the natural numbers $1 \leqslant \lambda_i' \leqslant \deg_z(\Phi)$, $1 \leqslant i \leqslant n$. Then according to lemma 6, for an irreducible (over $\mathbb{Z}$) polynomial $\Phi^{(1)}(Z) \in \mathbb{Z}[\varepsilon_1, \varepsilon][Z]$ such that

$$\Phi^{(1)}\left(\sum_{1 \leqslant i \leqslant n} \lambda_i' \xi_i\right) = 0,$$

the bounds

$$\deg_Z(\Phi^{(1)}) \leqslant \deg_Z(\Phi); \quad \deg_{\varepsilon_1, \varepsilon}(\Phi^{(1)}) \leqslant \mathscr{P}(d^n) \quad \text{and} \quad l(\Phi^{(1)}) \leqslant (M + \log R)\mathscr{P}(d^n)$$

are valid. Evidently $(st(\Phi^{(1)}))(\tau) = 0$ where the polynomial $st(\Phi^{(1)}) \in \mathbb{Z}[\varepsilon_1][Z]$. Therefore, for an irreducible (over $\mathbb{Z}$) polynomial $\psi^{(1)}(Z) \in \mathbb{Z}[\varepsilon_1][Z]$ such that $\psi^{(1)}(\tau) = 0$, the following bounds are fulfilled:

$$\deg_Z(\Psi^{(1)}) \leqslant \deg_Z(\Phi^{(1)}); \quad \deg_{\varepsilon_1}(\psi^{(1)}) \leqslant p_1(d^n) \quad \text{and} \quad l(\psi^{(1)}) \leqslant (M + \log R).$$

$p_2(d^n)$ for certain polynomials p_1, p_2 by virtue of proposition 1 (cf. also Mignotte, 1974), taking into account that the polynomial $\psi^{(1)}$ divides $st(\Phi^{(1)})$.

Now let

$$\tau^{(2)} = \sum_{1 \leqslant i \leqslant n} \lambda_i^{(2)} st(\xi_i), \quad \tau^{(3)} = \sum_{1 \leqslant i \leqslant n} \lambda_i^{(3)} st(\xi_i),$$

where the natural numbers $1 \leqslant \lambda_i^{(2)}, \lambda_i^{(3)} \leqslant \deg_Z(\Phi)$, $1 \leqslant i \leqslant n$. Assume that

$$\tau^{(3)} = q(\tau^{(2)}) \in \mathbb{Q}(\varepsilon_1)[\tau^{(2)}]$$

for a polynomial $q(Z) \in \mathbb{Q}(\varepsilon_1)[Z]$ such that

$$\deg_Z(q) < [\mathbb{Q}(\varepsilon_1)[\tau^{(2)}] : \mathbb{Q}(\varepsilon_1)].$$

Let us show that $\deg_{\varepsilon_1}(q) \leqslant \mathscr{P}(d^n)$ and $l(q) \leqslant (M+\log R)\mathscr{P}(d^n)$. Indeed, suppose that $\psi^{(2)}(\tau^{(2)})=0$, $\psi^{(3)}(\tau^{(3)})=0$ for some irreducible (over $\mathbb{Z}$) polynomials $\psi^{(2)}, \psi^{(3)} \in \mathbb{Z}[\varepsilon_1][Z]$, then

$$\deg_{\varepsilon_1}(\psi^{(2)}), \deg_{\varepsilon_1}(\psi^{(3)}) \leqslant \mathscr{P}(d^n) \quad \text{and} \quad l(\psi^{(2)}), l(\psi^{(3)}) \leqslant (M+\log R)\mathscr{P}(d^n)$$

in view of lemma 6 and what was proved just after it. Polynomial $\psi^{(3)}$ has a root $\tau^{(3)} = q(\tau^{(2)})$ in the field $\mathbb{Q}(\varepsilon_1)[\tau^{(2)}] = \mathbb{Q}(\varepsilon_1)[Z]/(\psi^{(2)})$. Hence, $\deg_{\varepsilon_1}(q) \leqslant p_3(d^n)$ and $l(q) \leqslant (M+\log R)p_4(d^n)$ for the relevant polynomials p_3, p_4 according to proposition 1, since a polynomial $(Z-\tau^{(3)})$ divides the polynomial $\psi^{(3)}$ over the field $\mathbb{Q}(\varepsilon_1)[Z]/(\psi^{(2)})$.

Now we pass to describing a procedure which produces a family of some classes of vectors $(\zeta_1, \ldots, \zeta_n) \in \bar{F}_1^n$ conjugate over the field $\mathbb{Q}(\varepsilon_1)$ such that $\psi_i(\zeta_i)=0$, $1 \leqslant i \leqslant n$ (let us recall that $\psi_i = st(\Phi_i)$) and, furthermore, the produced family contains vectors of the kind $(st(\xi_1), \ldots, st(\xi_n)) \in \bar{F}_1^n$ for all points $(\xi_1, \ldots, \xi_n) \in \bar{V}_j^{(\varepsilon)} \subset \bar{F}^n$ of the null-dimensional irreducible component $\bar{V}_j^{(\varepsilon)}$ of the variety $\bar{V}^{(\varepsilon)}$ constructed earlier, provided that $(st(\xi_1), \ldots, st(\xi_n))$ is definable.

In the first step, the procedure factorises the polynomial

$$\psi_1 = \prod_j \psi_{1j}^{e_j}$$

over the field $\mathbb{Q}(\varepsilon_1)$ by proposition 1 (see also Lenstra, 1984). Here, the multipliers $\psi_{1j} \in \mathbb{Q}(\varepsilon_1)[Z]$. For each multiplier ψ_{1j} we introduce the field

$$\Xi_1^{(j)} = \mathbb{Q}(\varepsilon_1)[Z]/(\psi_{1j}) \supset \mathbb{Q}(\varepsilon_1),$$

which is a finite extension of the field $\mathbb{Q}(\varepsilon_1)$. Let $\psi_{1j}(\theta_1^{(j)})=0$ for a certain $\theta_1^{(j)} \in \Xi_1^{(j)}$, then $\Xi_1^{(j)} \simeq \mathbb{Q}(\varepsilon_1)[\theta_1^{(j)}]$. Put $\psi_1^{(j)} = \psi_{1j}$.

Assume that by recursion on i the following objects are already constructed by the procedure: a family of fields $\{\Xi_i^{(m)}\}_m$, for every field $\Xi_i^{(m)}$ an irreducible (over the field $\mathbb{Q}(\varepsilon_1)$) polynomial $\psi_i^{(m)} \in \mathbb{Q}(\varepsilon_1)[Z]$ such that

$$\Xi_i^{(m)} = \mathbb{Q}(\varepsilon_1)[\theta_i^{(m)}] \simeq \mathbb{Q}(\varepsilon_1)[Z]/(\psi_i^{(m)}),$$

where $\psi_i^{(m)}(\theta_i^{(m)})=0$, and a primitive element

$$\theta_i^{(m)} = \sum_{1 \leqslant e \leqslant i} \mu_e \zeta_e \in \Xi_i^{(m)},$$

with $\psi_e(\zeta_e)=0$ and the natural numbers

$$1 \leqslant \mu_e \leqslant [\Xi_e^{(m_e)} : \mathbb{Q}(\varepsilon_1)] \leqslant \deg_Z(\Phi)$$

for suitable indices m_e, $1 \leqslant e \leqslant i$. Apart from that the procedure yields the expressions

$$\zeta_e = \sum_{0 \leqslant s < \deg_Z(\psi_i^{(m)})} \rho_{i,e,s}^{(m)} (\theta_i^{(m)})^s$$

for appropriate $\rho_{i,e,s}^{(m)} \in \mathbb{Q}(\varepsilon_1)$. Each root of the polynomial $\psi_i^{(m)}$ is of the same form as $\theta_i^{(m)}$, in addition the different roots generate fields conjugate (over the field $\mathbb{Q}(\varepsilon_1)$) to the field $\mathbb{Q}(\varepsilon_1)[\theta_i^{(m)}]$.

For the realisation of the $(i+1)$th step of the procedure we fix a field $\Xi_i^{(m)}$ and factorise the polynomial

$$\psi_{i+1} = \prod_j \psi_{i+1,j}$$

over the field $\Xi_i^{(m)}$ by proposition 1, where $\psi_{i+1,j} \in \Xi_i^{(m)}[Z]$. For every factor $\psi_{i+1,t}$ consider the field $\Xi_{i+1}^{(t)} = \Xi_i^{(m)}[Z]/(\psi_{i+1,t})$ (for brevity we omit in its notation the dependence on m), provided that the product of degrees

$$[\Xi_i^{(m)} : \mathbb{Q}(\varepsilon_1)] \deg_Z(\psi_{i+1,t}) \leqslant \deg_Z(\Phi),$$

otherwise the procedure does not construct the field $\Xi_{i+1}^{(t)}$. Let $\psi_{i+1,t}(\zeta_{i+1})=0$ for a certain $\zeta_{i+1}\in\Xi_{i+1}^{(t)}$. Among the elements of the sort $\theta_i^{(m)}+\mu\zeta_{i+1}$ for all natural numbers

$$1\leqslant\mu\leqslant[\Xi_i^{(m)}:\mathbb{Q}(\varepsilon_1)]\deg_Z(\psi_{i+1,t})=[\Xi_{i+1}^{(t)}:\mathbb{Q}(\varepsilon_1)]\leqslant\deg_Z(\Phi),$$

one can find a primitive element of the field $\Xi_{i+1}^{(t)}$ over the field $\mathbb{Q}(\varepsilon_1)$ (see e.g. Lang, 1965).

The procedure finds for each element of the sort $\theta_i^{(m)}+\mu\zeta_{i+1}$ its minimal polynomial over the field $\mathbb{Q}(\varepsilon_1)$. For this goal, for any fixed $1\leqslant s\leqslant[\Xi_{i+1}^{(t)}:\mathbb{Q}(\varepsilon_1)]$, the procedure checks whether there exist elements $\alpha_0,\ldots,\alpha_s\in\mathbb{Q}(\varepsilon_1)$ such that

$$\sum_{0\leqslant e\leqslant s}\alpha_e(\theta_i^{(m)}+\mu\zeta_{i+1})^e=0,$$

solving the system of linear equations over the field $\mathbb{Q}(\varepsilon_1)$ which arises from the latter equality. Namely, in order to obtain the system remove the parenthesis in the binoms $(\theta_i^{(m)}+\mu\zeta_{i+1})^e$ and compute the polynomials

$$\operatorname{rem}(Z^{e_1},\psi_i^{(m)}(Z))\in\mathbb{Q}(\varepsilon_1)[Z],\quad \operatorname{rem}(Z^{e_2},\psi_{i+1,t}(Z))\in\Xi_i^{(m)}[Z]$$

for all

$$0\leqslant e,e_1,e_2<[\Xi_{i+1}^{(t)}:\mathbb{Q}(\varepsilon_1)].$$

As a result, we obtain expressions of the powers $(\theta_i^{(m)}+\mu\zeta_{i+1})^e$ via the basis

$$(\theta_i^{(m)})^{d_1}(\zeta_{i+1})^{d_2},\quad 0\leqslant d_1<\deg_Z(\psi_i^{(m)}),\quad 0\leqslant d_2<\deg_Z(\psi_{i+1,t})$$

of the field $\Xi_{i+1}^{(t)}$ over the field $\mathbb{Q}(\varepsilon_1)$. The desired system of linear equations is obtained by setting the coefficients at the monomials $(\theta_i^{(m)})^{d_1}(\zeta_{i+1})^{d_2}$ in the equality

$$\sum_{0\leqslant e\leqslant s}\alpha_e(\theta_i^{(m)}+\mu\zeta_{i+1})^e=0$$

equal to zero. The element $\theta_{i+1}^{(t)}=\theta_i^{(m)}+\mu_{i+1}\zeta_{i+1}$, for which the degree of its minimal polynomial $\psi_{i+1}^{(t)}$ is maximal, is primitive.

If at least one of the two inequalities

$$\deg_{\varepsilon_1}(\psi_{i+1}^{(t)})\leqslant p_1(d^n)\quad\text{or}\quad l(\psi_{i+1}^{(t)})\leqslant(M+\log R)p_2(d^n)$$

is not satisfied (cf. above), then the procedure does not construct the field $\Xi_{i+1}^{(t)}$.

The above procedure has produced the transforming matrix from the basis $(\theta_i^{(m)})^{d_1}(\zeta_{i+1})^{d_2}$ to the basis $(\theta_{i+1}^{(t)})^e$. Inverting this matrix, the procedure yields the expression of the former basis in terms of the latter one, in particular the expressions

$$\zeta_{i+1}=\sum_{0\leqslant s<\deg_Z(\psi_{i+1}^{(t)})}\rho_{i+1,i+1,s}^{(t)}(\theta_{i+1}^{(t)})^s\quad\text{and}\quad(\theta_i^{(m)})^l=\sum_{0\leqslant s<\deg_Z(\psi_{i+1}^{(t)})}\sigma_{i,s,l}^{(t)}(\theta_{i+1}^{(t)})^s.$$

Substituting the latter expressions in the equalities obtained in the previous step of the recursion, we compute the expressions

$$\zeta_e=\sum_{0\leqslant s<\deg_Z(\psi_{i+1}^{(t)})}\rho_{i+1,e,s}^{(t)}(\theta_{i+1}^{(t)})^s,\quad 1\leqslant\rho\leqslant i.$$

If at least one of the following inequalities

$$\deg_{\varepsilon_1}(\zeta_e(\theta_{i+1}^{(t)}))\leqslant p_3(d^n)\quad\text{or}\quad l(\zeta_e(\theta_{i+1}^{(t)}))\leqslant(M+\log R)p_4(d^n)$$

is not fulfilled (cf. above), then the procedure does not construct the field $\Xi_{i+1}^{(t)}$.

Thus, the procedure constructs the field $\Xi_{i+1}^{(t)}$ iff all the above inequalities are valid. This completes the recursive construction of the family of fields $\{\Xi_i^{(m)}\}_{m;1\leqslant j\leqslant n}$. Observe that for every point $(\xi_1,\ldots,\xi_n)\in\bar{V}_j^{(e)}\subset\bar{F}^n$ from the null-dimensional irreducible component $\bar{V}_j^{(\varepsilon)}$ of the variety $\bar{V}^{(\varepsilon)}$, to vector $(st(\xi_1), \ldots, st(\xi_n)) \in \bar{F}_1^n$ (provided that it is definable), corresponds a certain field among the fields

$$\Xi_n^{(m)} = \mathbb{Q}(\varepsilon_1)(st(\zeta_1), \ldots, st(\xi_n))$$

constructed. In addition, the vector

$$(st(\xi_1), \ldots, st(\xi_n)) = (\zeta_1, \ldots, \zeta_n)$$

in view of the above-mentioned properties of the polynomials p_1, p_2, p_3, p_4.

Thereby, the following lemma is actually proved.

LEMMA 7. *Let a polynomial $\Phi \in H[\varepsilon][Z]$ be irreducible over an ordered field H, with $\varepsilon > 0$ infinitesimal relatively to H. Assume that the expressions*

$$\xi_i = \xi_i(\theta) = \sum_{0 \leqslant j < \deg_Z(\phi)} \beta_i^{(j)} \theta^j,$$

where $\beta_i^{(j)} \in H(\varepsilon)$, $1 \leqslant i \leqslant n$, $0 \leqslant j < \deg_Z(\Phi)$, yield a class of conjugate points over the field $H(\varepsilon)$ of the kind $(\xi_1(\theta), \ldots, \xi_n(\theta)) \in \overline{H(\varepsilon)}^n$, where $\phi(\theta) = 0$. In addition

$$\theta = \sum_{1 \leqslant i \leqslant n} \lambda_i \xi_i$$

for certain natural numbers $1 \leqslant \lambda_i \leqslant \deg_Z(\Phi)$, i.e. the field

$$H(\varepsilon)(\xi_1, \ldots, \xi_n) = H(\varepsilon)[\theta] \simeq H(\varepsilon)[Z]/(\phi).$$

Then one can produce a set $\mathscr{R} \subset \bar{H}^n$, containing the set of standard parts $(st(\xi_1), \ldots, st(\xi_n)) \in \bar{H}^n$ of all those points from the above-mentioned class of conjugates such that the standard part is definable. Besides that, $\mathscr{R}$ is a union of classes of conjugate points over the field H $(\zeta_1, \ldots, \zeta_n) \in \bar{H}^n$. Here each class is represented analogously as the class of points $(\xi_1(\theta), \ldots, \xi_n(\theta))$ above.

Note that the proof of lemma 7 was conducted for the field $H = \mathbb{Q}(\varepsilon_1)$, but one can easily carry it over to arbitrary ordered effectively given fields. We shall not make the meaning of the latter claim more precise, since in the present paper we apply lemma 8 only to the case of the field $H = \mathbb{Q}(\varepsilon_1)$ (in this section) and to the case of the field $H = \mathbb{Q}$ (in section 3). Estimations on the parameters of the points belonging to $\mathscr{R}$ were, in fact, given earlier in the case of the field $H = \mathbb{Q}(\varepsilon_1)$ (see the properties of polynomials p_1, p_2, p_3, p_4), in the case of the field $H = \mathbb{Q}$, the estimations on the bit lengths of the coefficients are the same; a time-bound on producing $\mathscr{R}$ will be obtained below in the case $H = \mathbb{Q}(\varepsilon_1)$ (cf. lemma 8), in the case $H = \mathbb{Q}$ the time-bound is the same.

Now we shall continue to describe the algorithm that produces a representative set for the semi-algebraic set V_0. Fix a certain class of conjugate vectors

$$(\zeta_1, \ldots, \zeta_n) \in \mathscr{R} \cap (\Xi_n^{(m)})^n$$

over the field $\mathbb{Q}(\varepsilon_1)$, which was constructed above (see lemma 7). Denote by $\eta = \theta_n^{(m)} \in \Xi_n^{(m)}$ the primitive element and by $\psi = \psi_n^{(m)} \in \mathbb{Q}(\varepsilon_1)[Z]$ its minimal polynomial over the field $\mathbb{Q}(\varepsilon_1)$. The algorithm tests, whether an equality $g(\zeta_1, \ldots, \zeta_n) = 0$ is fulfilled (observe that the fulfilment of this equality is independent of the choice of the particular vector in the conjugate class). Namely, involving expressions $\zeta_i(\eta) \in \mathbb{Q}(\varepsilon_1)[\eta]$ (see the proof of lemma 7) one can obtain a representation

$$g(\zeta_1(\eta), \ldots, \zeta_n(\eta)) = h(\eta)$$

for a certain polynomial $h(Z)\in\mathbb{Q}(\varepsilon_1)[Z]$. Then $g(\zeta_1,\ldots,\zeta_n)=0$ iff ψ divides the polynomial h.

Suppose that $g(\zeta_1,\ldots,\zeta_n)=0$. Determine whether ψ has at least one root in the field F_1, with the help of Sturm sequence (Lang, 1965; see also Heindel, 1971). If ψ has a root $\eta_0\in F_1$, then the corresponding point

$$(\zeta_1(\eta_0),\ldots,\zeta_n(\eta_0))\in V_0=\{g=0\}\subset F_1^n,$$

and the representative set $\mathscr{S}'$, which is produced by the algorithm described, consists of the points of the kind

$$(\zeta_1(\eta_1),\ldots,\zeta_n(\eta_1))\in\mathscr{R}\cap F_1^n$$

for all roots $\eta_1\in F_1$ of the polynomial ψ, all possible classes of conjugate points $(\zeta_1,\ldots,\zeta_n)\in F_1^n$, where $g(\zeta_1,\ldots,\zeta_n)=0$; $(\xi_1,\ldots,\xi_n)\in F^n$, and lastly all vectors $\gamma\in\Gamma$.

Now we shall prove that $\mathscr{S}'$ is really a representative set for V_0. Lemma 3 from section 1 entails that $V_0=st(V_\varepsilon)$. Let us consider an arbitrary component of connectivity V_1 of the set V_0 and make sure that the intersection $V_1\cap\mathscr{S}'\neq\phi$. By virtue of lemma 1(b) from section 1 there exist components of connectivity $W_1,\ldots,W_e$ of the set V_ε such that $V_1=st(W_1\cup\ldots\cup W_e)$. According to the corollary of lemma 5, one can find a vector $\gamma\in\Gamma$, such that for any component of connectivity W_s of the set V_ε, there exists a null-dimensional irreducible component $\bar{V}_j^{(\varepsilon)}$ of the variety $\bar{V}^{(\varepsilon)}\subset\bar{F}^n$ of all roots of the system (4n), corresponding to the vector $\gamma\in\Gamma$ under consideration, for which $W_s\cap\bar{V}_j^{(\varepsilon)}\neq\phi$. This means that

$$\Big(\bigcup_{\gamma\in\Gamma;\dim(\bar{V}_j^{(\varepsilon)})=0}\bar{V}_j^{(\varepsilon)}\Big)\cap F^n$$

is a representative set for the set V_ε (see above). Fix some $1\leqslant s\leqslant e$ and let a point $(\xi_1,\ldots,\xi_n)\in W_s\cap\bar{V}_j^{(\varepsilon)}$. Hence, $st(\xi_1,\ldots,\xi_n)\in V_1$. Starting with the class $\bar{V}_j^{(\varepsilon)}$ of conjugate points (see the proof of lemma 7), the above procedure constructs a polynomial $\psi\in\mathbb{Q}(\varepsilon_1)[Z]$, expressions $\zeta_i(\eta)\in\mathbb{Q}(\varepsilon_1)[\eta]$ and a set $\mathscr{R}\subset\bar{F}_1^n$ such that for an appropriate root

$$\eta_0=\sum_{1\leqslant i\leqslant n}\lambda_i^{(4)}\zeta_i(\eta_0)\in F_1$$

of the polynomial ψ, where the natural numbers $1\leqslant\lambda_i^{(4)}\leqslant\deg_Z(\psi)$ for $1\leqslant i\leqslant n$, the equality

$$st(\xi_1,\ldots,\xi_n)=(\zeta_1(\eta_0),\ldots,\zeta_n(\eta_0))\in\mathscr{R}$$

holds. (Note that $st(\xi_1,\ldots,\xi_n)$ is definable since $(\xi_1,\ldots,\xi_n)\in V_\varepsilon\subset\mathscr{D}_0(R+1)$.) Thus, the point $st(\xi_1,\ldots,\xi_n)\in\mathscr{S}'\cap V_1$, which completes the proof of the fact that $\mathscr{S}'$ is a representative set for the set V_0.

Now we proceed to the time analysis of the algorithm suggested in the present section.

At the beginning of its work the algorithm scans all vectors $\gamma\in\Gamma=\{1,\ldots,(4d)^n\}^{n-1}$. For this time $\mathscr{P}(d^{n^2})$ is sufficient. After that the algorithm from proposition 2 is applied to the system (4n) (producing a representative set for the set V_ε), its running time can be bounded by $\mathscr{P}(M,\log R,\mathrm{d}^{n^2})$. Then, recursively, the above procedure constructs a family of fields $\Xi_i^{(m)}$ and expressions $\zeta_e(\theta_i^{(m)})$ (see the proof of lemma 7). The field $\Xi_{i+1}^{(t)}=\Xi_i^{(m)}[Z]/(\psi_{i+1,t})$, where the polynomial $\psi_{i+1,t}\in\Xi_i^{(m)}[Z]$ is a certain factor of the polynomial $\psi_{i+1}=st(\Phi_{i+1})$ irreducible over $\Xi_i^{(m)}$. According to proposition 1, lemma 6 and the properties of the polynomials p_1,p_2, one can construct the polynomial $\psi_{i+1,t}$ within time $\mathscr{P}(M,\log R,d^n)$, furthermore, $\deg_{\varepsilon_1}(\psi_{i+1,t})\leqslant\mathscr{P}(d^n)$ and

$$l(\psi_{i+1,t})\leqslant(M+\log R)\mathscr{P}(d^n).$$

Next, the procedure searches for a primitive element $\theta_{i+1}^{(t)}$, solving for every element

$$\theta_i^{(m)}+\mu\zeta_{i+1},\quad 1\leqslant\mu\leqslant[\Xi_{i+1}^{(t)}:\mathbb{Q}(\varepsilon_1)]\leqslant\deg_Z(\Phi)$$

the respective system of linear equations by means of which the procedure finds the minimal polynomial of the element $\theta_i^{(m)}+\mu\zeta_{i+1}$ over the field $\mathbb{Q}(\varepsilon_1)$. The size of the system and, incidentally, the time for its solution can be estimated by $\mathscr{P}(M, \log R, d^n)$ in view of the properties of the polynomials p_1, p_2 and the bounds on $\deg_{\varepsilon_1}(\psi_{i+1,t})$, $l(\psi_{i+1,t})$ (see above). Therefore, the procedure constructs the expressions $\zeta_{i+1}(\theta_{i+1}^{(t)})$, $(\theta_i^{(m)})^l(\theta_{i+1}^{(t)})$ also within time $\mathscr{P}(M, \log R, d^n)$ and by virtue of the properties of the polynomials p_3, p_4 all expressions $\zeta_e(\theta_i^{(m)})$ can be constructed within the same time-bound. Thus, the whole computing time of the procedure constructing the set $\mathscr{R}$ mentioned in lemma 7 does not exceed $\mathscr{P}(\mathrm{M}, \log R, d^{n^2})$ taking into account that the total number of fields of the kind $\Xi_n^{(m)}$ is less or equal to the product $\deg_Z(\psi_1)\ldots\deg_Z(\psi_n)\leqslant\mathscr{P}(d^{n^2})$.

After that, for each class $(\zeta_1, \ldots, \zeta_n)\in\mathscr{R}$ of conjugate points the algorithm checks, whether $g(\zeta_1, \ldots, \zeta_n)=0$ is true, making use of the constructed expressions $\zeta_i(\eta)$, $1\leqslant i\leqslant n$, where $\eta=\theta_n^{(m)}$ for an appropriate m. For this time $\mathscr{P}(M, \log R, d^n)$ is sufficient. Then the algorithm determines, whether the polynomial $\psi=\psi_n^{(m)}$ has a root in the field F_1, using Sturm sequence (see e.g. Lang, 1965). This requires also not more than $\mathscr{P}(M, \log R, d^n)$ time according, e.g. to Heindel (1971).

Summarising the results of this section we arrive at the following

Lemma 8. *One can design an algorithm which, for a given polynomial* $g_1\in\mathbb{Z}[\varepsilon_1][X_1, \ldots, X_{n-1}]$ *and for a natural number* $R\geqslant 1$, *produces a representative set* $\mathscr{S}\subset F_1^{n-1}$ *for the intersection* $\{g_1=0\}\cap\mathscr{D}_0(R)$. *The number of points in* $\mathscr{S}$ *does not exceed* $\mathscr{P}(d^{n^2})$. *Here, the algorithm outputs the set* $\mathscr{S}$ *as a union of classes* $(\zeta_1, \ldots, \zeta_{n-1})$ *of points conjugate over the field* $\mathbb{Q}(\varepsilon_1)$. *For every class the algorithm constructs a certain polynomial* $\psi\in\mathbb{Z}[\varepsilon_1][Z]$ *irreducible over* $\mathbb{Q}(\varepsilon_1)$ *and expressions*

$$\zeta_i(\eta)=\sum_j \rho_i^{(j)}\eta^j,$$

where

$$\eta\in F_1,\quad \rho_i^{(j)}\in\mathbb{Q}(\varepsilon_1),\quad 1\leqslant i\leqslant n-1,\quad 0\leqslant j<\deg_Z(\psi),$$

in addition $\psi(\eta)=0$ *and*

$$\eta=\sum_{1\leqslant i\leqslant n-1}\lambda_i'\zeta_i(\eta)$$

for suitable natural numbers $1\leqslant\lambda_i'\leqslant\deg_Z(\psi)$, $1\leqslant i\leqslant n-1$. *The set* $\mathscr{S}$ *coincides with a family of points of the sort* $(\zeta_1(\eta), \ldots, \zeta_{n-1}(\eta))\in F_1^{n-1}$, *where* η *runs over all roots* $\eta\in F_1$ *of the polynomial* ψ *and* $(\zeta_1, \ldots, \zeta_{n-1})$ *runs over all classes of conjugate points. Besides that, the following bounds are valid:*

$$\deg_{\varepsilon_1, Z}(\psi), \deg_{\varepsilon_1}(\zeta_i(\eta))\leqslant\mathscr{P}(d^n)\quad\textit{and}\quad l(\psi), l(\zeta_i(\eta))\leqslant(M+\log R)\mathscr{P}(d^n).$$

The algorithm works within time $\mathscr{P}(M, \log R, d^{n^2})$.

3. Finding Solutions of a System of Polynomial Inequalities

We turn now to considering the general case and complete the proof of the theorem (see the introduction).

Let the input system of polynomial inequalities $f_1>0, \ldots, f_m>0, f_{m+1}\geqslant 0, \ldots, f_k\geqslant 0$ be given (cf. (1)), where the polynomials $f_1, \ldots, f_k\in\mathbb{Z}[X_2, \ldots, X_n]$ satisfy the bounds

$\deg_{X_2,\ldots,X_n}(f_i)<d$; $l(f_i)\leqslant M$, $1\leqslant i\leqslant k$ (see (2)). Introduce a new variable X_1 and a polynomial $f_{k+1}=X_1 f_1,\ldots f_m-1$. Denote by π_1 a linear projection defined by the formula $\pi_1(X_1,\ldots,X_n)=(X_2,\ldots,X_n)$. Consider the semi-algebraic set

$$V=\{(f_1\geqslant 0)\&\ldots\&(f_m\geqslant 0)\&(f_{m+1}\geqslant 0)\&\ldots\&(f_k\geqslant 0)\&(f_{k+1}\geqslant 0)\}\subset\tilde{\mathbb{Q}}^n.$$

Then

$$\mathscr{V}=\pi_1(V)=\{(f_1>0)\&\ldots\&(f_m>0)\&(f_{m+1}\geqslant 0)\&\ldots\&(f_k\geqslant 0)\}\subset\tilde{\mathbb{Q}}^{n-1}$$

and it is sufficient to produce a representative set $\mathscr{T}'$ for the set V, in this case $\mathscr{T}=\pi_1(\mathscr{T}')$ is the representative set for the set $\mathscr{V}=\pi_1(V)$ as desired in the theorem. Below, the standard part st concerns the situation $K=\tilde{\mathbb{Q}}$ (see section 1), i.e. for an element $a\in F_1$ its standard part $st(a)\in\tilde{\mathbb{Q}}$, provided that $st(a)$ is definable.

The following bound on real roots of a polynomial was originally proved in Vorobjov (1984). Here we expose a shorter proof.

LEMMA 9. *Let a polynomial $h\in\mathbb{Z}[X_1,\ldots,X_n]$ satisfy the inequalities $\deg_{X_1,\ldots,X_n}(h)<d$ and $l(h)\leqslant M$. Then any component of connectivity U_0 of the semi-algebraic set $\{h=0\}\subset\tilde{\mathbb{Q}}^n$ has non-empty intersection with the ball $\mathscr{D}_0(R)$, where the natural number $R\leqslant\exp(M\mathscr{P}(d^n))$.*

Let us conduct the proof by induction on n. The base for $n=1$ is well known (see e.g. Lang, 1965). Consider an arbitrary n. If U_0 has a non-empty intersection with one of the coordinate hyperplanes $\{X_i=0\}$, where $1\leqslant i\leqslant n$, then the statement of the lemma follows from the inductive hypothesis. So we can assume the opposite. In this case U_0 is situated in some cone of the kind

$$\Big\{\mathop{\&}_{1\leqslant i\leqslant n}(\delta_i X_i>0)\Big\},$$

where $\delta_i\in\{-1,+1\}$, $1\leqslant i\leqslant n$. Suppose for definiteness that

$$U_0\subset\Big\{\mathop{\&}_{1\leqslant i\leqslant n}(X_i<0)\Big\}.$$

We can assume w.l.o.g. that $h(x)\geqslant 0$ for all $x\in\tilde{\mathbb{Q}}^n$, squaring polynomial h if necessary.

Lemma 5 implies that one can find a vector $\gamma=(\gamma_2,\ldots,\gamma_n)\in\Gamma$ such that any solution from the space F_1^n of the system

$$h-\varepsilon_1=\left(\frac{\partial h}{\partial X_2}\right)^2-\frac{\gamma_2}{Nn}\sum_{1\leqslant j\leqslant n}\left(\frac{\partial h}{\partial X_j}\right)^2=\ldots=\left(\frac{\partial h}{\partial X_n}\right)^2-\frac{\gamma_n}{Nn}\sum_{1\leqslant j\leqslant n}\left(\frac{\partial h}{\partial X_j}\right)^2=0 \qquad (5)$$

is an isolated point in the variety $\bar{W}^{(\varepsilon_1)}$ consisting of all solutions of the system from the space $\bar{F}_1^n$. Define

$$\alpha_j=\sqrt{\gamma_j/Nn}>0,\ 2\leqslant j\leqslant n \quad\text{and}\quad \alpha_1=\sqrt{1-\sum_{2\leqslant j\leqslant n}\alpha_j^2}>0.$$

Introduce the linear function

$$q(X_1,\ldots,X_n)=\alpha_1 X_1+\ldots+\alpha_n X_n.$$

Let us pick a certain point $x^{(0)}=(x_1^{(0)},\ldots,x_n^{(0)})\in U_0$. Consider the closed simplex

$$S=\Big\{\mathop{\&}_{1\leqslant i\leqslant n}(X_i\leqslant 0)\&q(X_1,\ldots,X_n)\geqslant q(x^{(0)})\Big\}.$$

Then $x^{(0)}\in U_0\cap S$ and the function q has the maximal value $0>q_0\in\tilde{\mathbb{Q}}$ on the limited closed set $U_0\cap S$. Moreover, q_0 is the maximal value of q on the whole component U_0.

A set

$$A = \{q(X_1, \ldots, X_n) = q_0\} \cap U_0 \subset \tilde{\mathbb{Q}}^n$$

lies in the simplex

$$\Big\{ \mathop{\&}_{1 \leqslant i \leqslant n} (X_i \leqslant 0) \,\&\, (q(X_1, \ldots, X_n) = q_0) \Big\}$$

and therefore $A \subset \mathcal{D}_0(\tau)$ for an appropriate $\tau \in \mathbb{Q}$. Lemma 3 entails the coincidence of the sets

$$st(\{h = \varepsilon_1\} \cap \mathcal{D}_0(\tau + 1)) = (\{h = 0\} \cap \mathcal{D}_0(\tau + 1)) \subset \tilde{\mathbb{Q}}^n.$$

Let $U_0^{(1)} \subset \tilde{\mathbb{Q}}^n$ be a component of connectivity of the semi-algebraic set $\{h = 0\} \cap \mathcal{D}_0(\tau + 1)$ such that $A^{(1)} = A \cap U_0^{(1)} \neq \phi$. Obviously $U_0^{(1)} \subset U_0$. By virtue of lemma 1(b) there exist components of connectivity $W_1, \ldots, W_e$ of the semi-algebraic set

$$(\{h = \varepsilon_1\} \cap \mathcal{D}_0(\tau + 1)) \subset F_1^n$$

such that the equality $st(W_1 \cup \ldots \cup W_e) = U_0^{(1)}$ is true.

The function q has the maximal value $q_1 \in F_1$ on the closed limited semi-algebraic set $(W_1 \cup \ldots \cup W_e) \subset \mathcal{D}_0(\tau + 1)$ in view of the transfer principle (see section 1). Introduce the semi-algebraic set

$$B = \{q(X_1, \ldots, X_n) = q_1\} \cap (W_1 \cup \ldots \cup W_e).$$

Let us show that $st(B) \subset A^{(1)}$. For this purpose it is sufficient to check for any point $y^{(1)} \in B$ that $q(st(y^{(1)})) = q_0$. Indeed, pick a point $x \in A^{(1)} \subset U_0^{(1)}$, then there is a point $y \in W_1 \cup \ldots \cup W_e$ such that $st(y) = x$. Hence,

$$q_0 = q(x) = st(q(y)) \leqslant st(q(y^{(1)})) = st(q_1)$$

taking into account the definition of the set B. On the other hand, $st(y^{(1)}) \in U_0^{(1)} \subset U_0$, therefore $q(st(y^{(1)})) \leqslant q_0$, which was to be shown. One concludes in particular that $B \subset \mathcal{D}_0(\tau + 1/2)$.

The following proposition is well known (see e.g. Thorpe, 1979). Let a polynomial $\rho \in \mathbb{R}[X_1, \ldots, X_n]$ and a point $y^{(2)} \in \{\rho = 0\} \subset \mathbb{R}^n$ be such that the gradient

$$\left(\frac{\partial \rho}{\partial X_1}(y^{(2)}), \ldots, \frac{\partial \rho}{\partial X_n}(y^{(2)})\right) \neq 0$$

and, apart from that, the linear form q reaches the maximum in the point $y^{(2)}$ on the set $\{\rho = 0\} \cap \mathcal{D}_{y^{(2)}}(\tau^{(2)})$ for a certain $\tau^{(2)} > 0$. Then

$$\left(\frac{\partial \rho}{\partial X_1}(y^{(2)}), \ldots, \frac{\partial \rho}{\partial X_n}(y^{(2)})\right)$$

is collinear to the vector $(\alpha_1, \ldots, \alpha_n)$. According to the transfer principle this proposition remains also correct if we replace $\mathbb{R}$ by an arbitrary real closed field K.

Apply the proposition to the polynomial $\rho = h - \varepsilon_1$, the field $K = F_1$ and an arbitrary point $y^{(2)} \in B$. Since $y^{(2)} \in B \subset \{h = \varepsilon_1\}$, the gradient

$$\left(\frac{\partial h}{\partial X_1}(y^{(2)}), \ldots, \frac{\partial h}{\partial X_n}(y^{(2)})\right) \neq 0$$

by virtue of lemma 4(a). As radius $\tau^{(2)}$ one can take $0 < \tau^{(2)} < 1/2$ such that

$$\mathcal{D}_{y^{(2)}}(\tau^{(2)}) \cap (W_1 \cup \ldots \cup W_e) = \mathcal{D}_{y^{(2)}}(\tau^{(2)}) \cap \{h = \varepsilon_1\} \subset \mathcal{D}_0(\tau + 1).$$

The proposition implies that the gradient

$$\left(\frac{\partial h}{\partial X_1}(y^{(2)}), \ldots, \frac{\partial h}{\partial X_n}(y^{(2)})\right)$$

is collinear to the vector $(\alpha_1, \ldots, \alpha_n)$. Therefore, the point $y^{(2)}$ satisfies the system (5). Besides that, $y^{(2)}$ is an isolated point in the variety $\bar{W}^{(\varepsilon_1)} \subset \bar{F}_1^n$ (see above) and the point $st(y^{(2)}) \in A^{(1)} \subset A \subset U_0$, since $y^{(2)} \in B$.

As in section 2, applying the algorithm from proposition 2, one can produce a null-dimensional component $\bar{W}_1^{(\varepsilon_1)}$ of the variety $\bar{W}^{(\varepsilon_1)}$ irreducible over the field $\mathbb{Q}(\varepsilon_1)$ such that the point $y^{(2)} = (y_1^{(2)}, \ldots, y_n^{(2)}) \in \bar{W}_1^{(\varepsilon_1)}$. The algorithm constructs polynomials $\Phi_1, \ldots, \Phi_n \in \mathbb{Q}[\varepsilon_1][Z]$ for which $\Phi_i(y_i^{(2)}) = 0$, $1 \leqslant i \leqslant n$, furthermore, the bounds $\deg_{\varepsilon_1, Z}(\Phi_i) \leqslant \mathscr{P}(d^n)$ and $l(\Phi_i) \leqslant M\mathscr{P}(d^n)$ are fulfilled. Finally, $(st(\Phi_i))(st(y_i^{(2)})) = 0$ (remark that $st(y_i^{(2)})$ is definable, taking into account that the point $y^{(2)} \in B \subset \mathscr{D}_0(\tau + 1/2)$). Hence, $|st(y_i^{(2)})| \leqslant \exp(M\mathscr{P}(d^n))$ (see e.g. Lang, 1965; also Heindel, 1971), i.e. the point

$$st(y^{(2)}) \in U_0 \cap \mathscr{D}_0(\exp(M\mathscr{P}(d^n))),$$

which completes the proof of the lemma.

Let the polynomials $h_1, \ldots, h_k \in \mathbb{Z}[X_1, \ldots, X_n]$ satisfy the bounds $\deg h_i < d$; $l(h_i) \leqslant M$, $1 \leqslant i \leqslant k$. Consider an arbitrary component of connectivity W of the semi-algebraic set

$$\{(h_1 \geqslant 0) \& \ldots \& (h_k \geqslant 0)\} \subsetneqq \tilde{\mathbb{Q}}^n.$$

The following lemma generalises lemma 9 and estimates real solutions of a system of polynomial inequalities.

LEMMA 10. *For a suitable natural number*

$$R \leqslant \exp((M + \log k)\mathscr{P}(d^n))$$

both $\mathscr{D}_0(R) \cap W \neq \phi$ *and* $\mathscr{D}_0(R) \backslash W \neq \phi$ *are valid.*

PROOF. By virtue of lemma 9, for a suitable natural number

$$R \leqslant \exp((M + \log k)\mathscr{P}(d^n)),$$

if a polynomial $h \in \mathbb{Z}[X_1, \ldots, X_{n+1}]$ satisfies the bounds $\deg h \leqslant 2d$ and

$$l(h) \leqslant M + n \log d + \log k,$$

then any component of connectivity of the semi-algebraic set $\{h = 0\} \subset \tilde{\mathbb{Q}}^n$ has non-empty intersection with the ball $\mathscr{D}_0(R)$. We claim that this R is the one desired in the lemma.

At first we show that $W \cap \mathscr{D}_0(R) \neq \phi$. Take a set of indices $I \subset \{1, \ldots, k\}$ maximal with respect to inclusion, such that there exists a point $z \in W$ for which $h_i(z) = 0$ for every $i \in I$.

Consider the component of connectivity $U_1 \subset \tilde{\mathbb{Q}}^n$ of the semi-algebraic set $\left\{\sum_{i \in I} h_i^2 = 0\right\}$ that contains the point $z \in U_1$ (if $I = \phi$ then $U_1 = \tilde{\mathbb{Q}}^n$). Lemma 9 entails that $U_1 \cap \mathscr{D}_0(R) \neq \phi$ taking into account that

$$l\left(\sum_{i \in I} h_i^2\right) \leqslant M + n \log d + \log k.$$

We assert that $U_1 \subset W$ (in the case when $I = \{1, \ldots, k\}$ the latter inclusion is trivial, so w.l.o.g. we assume further that $I \subsetneqq \{1, \ldots, k\}$). Suppose the contrary. Since U_1 is connected, there exists a point $z_0 \in U_1$ such that for any $\tau > 0$ the intersection $U_1 \cap \mathscr{D}_0(\tau)$

contains points from $U_1 \cap W$ as well as points not belonging to W. (In the case of the field $\mathbb{R}$, the latter statement is obvious, for an arbitrary real closed field one has to make use of the transfer principle.) Then $z_0 \in W$, since the semi-algebraic set

$$\{(h_1 \geqslant 0) \& \ldots \& (h_k \geqslant 0)\} \supset W$$

is determined by only unstrict inequalities and, hence, W is closed in the topology generated by the base consisting of all open balls.

On the other hand, there exists an index $j_0 \notin I$ for which $h_{j_0}(z_0) = 0$. Otherwise, for an appropriate $\tau_0 > 0$ and every point $v \in \mathscr{D}_{z_0}(\tau_0)$, the inequality $h_j(v) > 0$ is true for each $j \notin I$. Consider the component of connectivity U_2 of the intersection $U_1 \cap \mathscr{D}_{z_0}(\tau_0)$ which contains the point $z_0 \in U_2$. Then $U_2 \subset W$ taking into account that W is a component of connectivity of the set $\{(h_1 \geqslant 0) \& \ldots \& (h_k \geqslant 0)\}$. For a suitable τ_1 satisfying the inequalities $\tau_0 > \tau_1 > 0$, any component of connectivity (except U_2) of the intersection $U_1 \cap \mathscr{D}_{z_0}(\tau_0)$ has no common points with the ball $\mathscr{D}_{z_0}(\tau_1)$. This leads to a contradiction to the assumption that the intersection $U_1 \cap \mathscr{D}_{z_0}(\tau_1)$ has at least one point not belonging to W.

Thus, we have proved the existence of $j_0 \notin I$ such that $h_{j_0}(z_0) = 0$. This contradicts to the maximality of the set I of indices, therefore

$$W \cap \mathscr{D}_0(R) \supset U_1 \cap \mathscr{D}_0(R) \neq \phi.$$

From the above one can infer that if U is a component of connectivity of some non-empty semi-algebraic set

$$\{(h_1 > 0) \& \ldots \& (h_m > 0) \& (h_{m+1} \geqslant 0) \& \ldots \& (h_k \geqslant 0)\} \subset \tilde{\mathbb{Q}}^n,$$

then for a suitable natural number

$$R_1 \leqslant \exp((M+k)\mathscr{P}((md)^n)),$$

the intersection $U \cap \mathscr{D}_0(R_1) \neq \phi$. Indeed, introduce a new variable X_{n+1} and a semi-algebraic set

$$\{(X_{n+1}h_1 \ldots h_m - 1 \geqslant 0) \& (h_1 \geqslant 0) \& \ldots \& (h_m \geqslant 0) \& (h_{m+1} \geqslant 0) \& \ldots \& (h_k \geqslant 0)\} \subset \tilde{\mathbb{Q}}^{n+1}$$

(cf. beginning of the section). There exists a unique component of connectivity $U^{(1)}$ of the latter semi-algebraic set such that $\pi_2(U^{(1)}) = U$, where the linear projection π_2 is defined by the formula

$$\pi_2(X_1, \ldots, X_n, X_{n+1}) = (X_1, \ldots, X_n).$$

According to what we proved above, $U^{(1)} \cap \mathscr{D}_0(R_1) \neq \phi$ is fulfilled taking into account the bound

$$l(X_{n+1}h_1 \ldots h_m - 1) \leqslant M + kn \log d.$$

Hence, $U \cap \mathscr{D}_0(R_1) \neq \phi$.

Assume now that $\mathscr{D}_0(R) \subset W$. Then $h_i(x) \geqslant 0$ is valid for each point $x \in \mathscr{D}_0(R)$ and each $1 \leqslant i \leqslant k$. We can suppose w.l.o.g. that the polynomial h_1 is not non-negative everywhere on $\tilde{\mathbb{Q}}^n$. (Otherwise, if $h_i \geqslant 0$ on $\tilde{\mathbb{Q}}^n$ for each $1 \leqslant i \leqslant k$, then

$$\{(h_1 \geqslant 0) \& \ldots \& (h_k \geqslant 0)\} = \tilde{\mathbb{Q}}^n.)$$

Then the intersection $\{h_1 < 0\} \cap \mathscr{D}_0(R) \neq \phi$ by virtue of what we proved above. This contradicts to the assumption and completes the proof of the lemma.

Introduce now the polynomial

$$g_1 = (f_1 + \varepsilon_1) \ldots (f_{k+1} + \varepsilon_1) - \varepsilon_1^{k+1} \in \mathbb{Z}[\varepsilon_1][X_1, \ldots, X_n].$$

Apply the algorithm from section 2 (see lemma 8) to this polynomial and to the natural number $R+1$, where $R \leqslant \exp(M\mathscr{P}(kd)^n)$ is obtained from lemma 10, in which the polynomials $f_1, \ldots, f_{k+1}$ are taken as $h_1, \ldots, h_k$. As a result, the algorithm produces a representative set $\mathscr{S} \subset F_1^n$ for the semi-algebraic set $\{g_1 = 0\} \cap \mathscr{D}_0(R+1)$. The set $\mathscr{S}$ is a union of classes of points conjugate over the field $\mathbb{Q}(\varepsilon_1)$ (see lemma 8). Any class of conjugate points from the set $\mathscr{S}$ is given by a polynomial $\psi \in \mathbb{Z}[\varepsilon_1][Z]$ irreducible over field $\mathbb{Q}(\varepsilon_1)$ and by expressions for the coordinates

$$\zeta_i(\eta) = \sum_j \rho_i^{(j)} \eta^j \ (1 \leqslant i \leqslant n),$$

where $\rho_i^{(j)} \in \mathbb{Q}(\varepsilon_1)$, $0 \leqslant j < \deg_Z(\psi)$ and $\eta \in F_1$, $\psi(\eta) = 0$. Apart from that, the following bounds are valid:

$$\deg_{\varepsilon_1, Z}(\psi), \deg_{\varepsilon_1}(\zeta_i(\eta)) \leqslant \mathscr{P}((kd)^n) \quad \text{and} \quad l(\psi), l(\zeta_i(\eta)) \leqslant M\mathscr{P}(kd)^n).$$

Apply the algorithm from lemma 7 in the case of the field $H = \mathbb{Q}$ to each class of conjugate points $(\zeta_1(\eta), \ldots, \zeta_n(\eta))$ from the set $\mathscr{S}$. Thus, a finite set $\mathscr{R} \subset \bar{\mathbb{Q}}^n$ is obtained which contains the standard part of every point from the set $\mathscr{S}$, provided that the standard part is definable. Analogously, the set $\mathscr{R}$ is a union of classes of points conjugate over the field $\mathbb{Q}$ (see lemma 7).

Fix a certain class of conjugate points from $\mathscr{R}$ which is given by polynomial $\Phi \in \mathbb{Q}[Z]$ irreducible over the field $\mathbb{Q}$ and by expressions for the coordinates

$$\chi_i(\omega) = \sum_j \beta_i^{(j)} \omega^j,$$

where $\beta_i^{(j)} \in \mathbb{Q}$, $1 \leqslant i \leqslant n$, $0 \leqslant j < \deg_Z(\Phi)$ and $\omega \in \tilde{\mathbb{Q}}$, $\Phi(\omega) = 0$. Besides that, the following bounds are true:

$$\deg_Z(\Phi) \leqslant \mathscr{P}(kd)^n) \quad \text{and} \quad l(\Phi), l(\chi_i(\omega)) \leqslant M\mathscr{P}((kd)^n)$$

(see the proof of lemma 7). Write

$$q_e(\omega) = f_e(\chi_1(\omega), \ldots, \chi_n(\omega)), \quad 1 \leqslant e \leqslant k+1$$

for suitable polynomials $q_e \in \mathbb{Q}[Z]$. If the polynomial Φ divides the polynomial q_e for some $1 \leqslant e \leqslant k+1$, then $q_e(\omega) = 0$ and vice versa. Select all such polynomials q_e. Assume that $q_{e_0}(\omega) \neq 0$ for a certain $1 \leqslant e_0 \leqslant k+1$. Following, e.g. Heindel (1971), one can find a polynomial p_5 such that the inequalities

$$|\omega'' - \omega'|, |\omega' - \omega_1| > 2^{(-Mp_5((kd)^n))} = C$$

are correct for all roots $\omega_1 \in \tilde{\mathbb{Q}}$ of polynomial q_{e_0} and each pair of distinct real roots $\omega' \neq \omega''$ of polynomial the Φ. Here we make use of the inequalities

$$\deg_Z(q_e) \leqslant \mathscr{P}((kd)^n) \quad \text{and} \quad)l(q_e) \leqslant M\mathscr{P}((kd)^n).$$

Following, e.g. Heindel (1971), the algorithm yields for every real root $\omega_0 \in \tilde{\mathbb{Q}}$ of the polynomial Φ its rational approximation $\omega_2 \in \mathbb{Q}$ which satisfies the inequality $|\omega_0 - \omega_2| < C/2$. Hence, an interval $(\omega_2 - C/2, \omega_2 + C/2) \subset \tilde{\mathbb{Q}}$ with the rational endpoints contains only one root ω_0 of the polynomial Φ. After that the algorithm evaluates $q_{e_0}(\omega_2)$ for all indices $1 \leqslant e_0 \leqslant k+1$ such that $q_{e_0}(\omega) \neq 0$ (observe that the latter is valid iff $q_{e_0}(\omega_0) \neq 0$). If $q_{e_0}(\omega_2) > 0$ is fulfilled for an index e_0, then the algorithm includes the point $(\chi_1(\omega_0), \ldots, \chi_n(\omega_0))$ into the set $\mathscr{T}'$, where $\mathscr{T}' \subset \mathscr{R}$ is the required representative set of the semi-algebraic set

$$V = \{(f_1 \geqslant 0) \& \ldots \& (f_{k+1} \geqslant 0)\} \subset \tilde{\mathbb{Q}}^n$$

(see the beginning of the present section). This completes the description of the algorithm.

Now we shall show that $\mathcal{T}'$ is really a representative set for the set V. Furthermore, we determine bounds on the parameters of the points from $\mathcal{T}'$ and on the running time of the algorithm which produces $\mathcal{T}'$. These bounds are similar to the corresponding bounds in the theorem (see the introduction). Let us check at first that $\mathcal{R} \cap V = \mathcal{T}'$. Let a point $(\chi_1(\omega_0), \ldots, \chi_n(\omega_0)) \in \mathcal{T}'$. Assume that $q_{e_0}(\omega_0) \neq 0$ for a certain $1 \leqslant e_0 \leqslant k+1$ (see above). Suppose that $q_{e_0}(\omega_0) < 0$. Then there exists a root $\omega_3 \in \tilde{\mathbb{Q}}$ of the polynomial q_{e_0} which lies between ω_0 and ω_2 since $q_{e_0}(\omega_2) > 0$. Therefore $|\omega_0 - \omega_3| < C/2$, so the supposition leads to a contradiction taking into account that $\Phi(\omega_0) = 0$. Hence,

$$f_{e_0}(\chi_1(\omega_0), \ldots, \chi_n(\omega_0)) = q_{e_0}(\omega_0) > 0$$

for all $1 \leqslant e_0 \leqslant k+1$ such that $q_{e_0}(\omega_0) \neq 0$, i.e. $(\chi_1(\omega_0), \ldots, \chi_n(\omega_0)) \in V$, thus $\mathcal{T}' \subset \mathcal{R} \cap V$.

Conversely, let a point

$$\chi = (\chi_1(\omega_0), \ldots, \chi_n(\omega_0)) \in \mathcal{R} \cap V.$$

Then

$$\omega_0 = \sum_{1 \leqslant j \leqslant n} \lambda_j' \chi_j(\omega_0)$$

for the appropriate natural numbers λ_j' (see lemma 7), therefore $\omega_0 \in \tilde{\mathbb{Q}}$. Assume that the point $\chi \notin \mathcal{T}'$. Then one can find an index $1 \leqslant e_0 \leqslant k+1$ such that $q_{e_0}(\omega_0) \neq 0$ and $q_{e_0}(\omega_2) < 0$ (see the construction of $\mathcal{T}'$ above). On the other hand, $q_{e_0}(\omega_0) > 0$ since $\chi \in V$. Hence, there exists a real root of the polynomial q_{e_0} between the numbers ω_0 and ω_2, which leads to a contradiction similar to the above.

Let us consider now an arbitrary component of connectivity $V^{(1)}$ of the semi-algebraic set V and prove that $V^{(1)} \cap \mathcal{T}' \neq \phi$. Remark that the set $V^{(1)}$ is closed (see the proof of lemma 10 above). Lemma 10 implies that $\mathcal{D}_0(R) \cap V^{(1)} \neq \phi$ and $\mathcal{D}_0(R) \backslash V^{(1)} \neq \phi$. Therefore, one can find a certain point

$$x \in (\partial V^{(1)}) \cap \mathcal{D}_0(R) \subset V^{(1)} \cap \mathcal{D}_0(R).$$

Denote by $V^{(2)}$ the unique component of connectivity of the semi-algebraic set $V \cap \mathcal{D}_0(R+1)$ that contains the point $x \in V^{(2)}$. Observe that $V^{(2)} \subset V^{(1)}$ in view of the connectivity of $V^{(1)}$.

Introduce the semi-algebraic set

$$W = \{(f_1 + \varepsilon_1 > 0) \& \ldots \& (f_{k+1} + \varepsilon_1 > 0) \& (g_1 \geqslant 0)\} \subset F_1^n.$$

Lemma 2(d) entails the existence of a point $z \in W \cap \{g_1 = 0\}$ such that each coordinate of the point $(z - x)$ is infinitesimal relatively to the field $\mathbb{Q}$. In particular, the point $z \in \mathcal{D}_0(R+1)$. According to lemma 2(a),

$$st(W \cap \mathcal{D}_0(R+1)) = (V \cap \mathcal{D}_0(R+1)).$$

Pick all components of connectivity $W^{(1)}, \ldots, W^{(e)}$ of the semi-algebraic set $W \cap \mathcal{D}_0(R+1)$, for which

$$st(W^{(j)}) \subset V^{(2)}, \quad 1 \leqslant j \leqslant e.$$

Then by virtue of lemma 1(b),

$$V^{(2)} = st(W^{(1)} \cup \ldots \cup W^{(e)}).$$

Taking into account that $st(z) = x$, we deduce by lemma 1(b) that the point $z \in W^{(1)} \cup \ldots \cup W^{(e)}$. Let w.l.o.g. $z \in W^{(1)}$.

Denote by U the unique component of connectivity of the semi-algebraic set $\{g_1 = 0\} \cap \mathcal{D}_0(R+1)$ that contains the point $z \in U$. One can infer that $U \subset W \cap \mathcal{D}_0(R+1)$ by lemma 2(c) since $z \in U \cap W^{(1)}$. This implies the inclusion $U \subset W^{(1)}$ in view of the connectivity of U. Hence, $st(U) \subset V^{(2)}$.

Involving lemma 8 from section 2, the algorithm described above produces a representative set $\mathscr{S}$ for the semi-algebraic set $\{g_1=0\}\cap\mathscr{D}_0(R+1)$. In particular, there is a certain point $u\in U\cap\mathscr{S}$. Then $st(u)\in V^{(2)}\subset V^{(1)}$ by what we proved above. Besides that, $st(u)\in\mathscr{R}$ according to the construction of $\mathscr{R}$ (cf. lemma 7). Thus, the point $st(u)\in\mathscr{T}'\cap V^{(1)}$. So we have shown that $\mathscr{T}'$ is a representative set for the set V.

To complete the proof of the theorem (see the introduction), it remains to estimate the running time of the algorithm and the parameters of the points (and their number) in the set $\mathscr{T}'$. For producing the representative set $\mathscr{S}$ for the set $\{g_1=0\}\cap\mathscr{D}_0(R+1)$ the algorithm works within time $\mathscr{P}(M(kd)^{n^2})$ by lemma 8. The running time of the algorithm from lemma 7, which constructs the set $\mathscr{R}$, can be estimated by the same bound. Thereby the algorithm yields a rational approximation $\omega_2\in\mathbb{Q}$ to a real root $\omega_0\in\tilde{\mathbb{Q}}$ of the polynomial Φ such that $|\omega_0-\omega_2|<C/2$. This requires no more time than $\mathscr{P}(M(kd)^n)$ (see e.g. Heindel, 1971). Also, within the latter time-bound one can evalute $q_{e_0}(\omega_2)$. Thus, the time-bound desired in the theorem is guaranteed.

The number of points in the set $\mathscr{S}$ does not exceed $\mathscr{P}((kd)^{n^2})$, according to lemma 8. Hence, the number of points in the set $\mathscr{T}'$ also is bounded by $\mathscr{P}((kd)^{n^2})$ in view of the construction in the proof of lemma 7. The estimations for $\deg_Z(\Phi)$ and $l(\Phi)$, $l(\chi_i(\omega))$ were obtained earlier. Based on Heindel (1971), we get the inequalities $l(C)$, $l(\omega_2)\leqslant M\mathscr{P}((kd)^n)$. This entails the bounds on $l(b_1)$, $l(b_2)$, where $b_1=\omega_2-C/2$, $b_2=\omega_2+C/2\in\mathbb{Q}$ (see above). This completes the proof of the theorem.

In conclusion we make a remark that the theorem allows a direct generalisation to input polynomials $f_1,\ldots,f_k\in H[X_1,\ldots,X_n]$, where the field H is, for example, of the kind $H=\mathbb{Q}(\varepsilon_1,\ldots,\varepsilon_s)$, where ε_{i+1} is infinitesimal relatively to the field $\mathbb{Q}(\varepsilon_1,\ldots,\varepsilon_i)$ for $0\leqslant i<s$. The method of the proof and all the above constructions are the same, only the form of the necessary bounds has to be changed respectively.

4. General Outline of the Algorithm

Before implementing the algorithm one has to fulfil the following routine work (fortunately, this has only to be done once). Namely, one has to determine the bounds in the proofs of propositions 1, 2, lemmas 9, 10 "hidden" in the denotation $\mathscr{P}$ and, as a result, to obtain a specified polynomial $p\in\mathbb{Z}[Z]$ with non-negative coefficients satisfying the following property (cf. lemma 10).

Let some polynomials $h_1,\ldots,h_k\in\mathbb{Z}[X_1,\ldots,X_n]$ satisfy the bounds $\deg h_i<d$; $l(h_i)\leqslant M$, $1\leqslant i\leqslant k$. Let us set the integer $R=3^{((M+[\log k])p(d^n))}$. Then for each component of connectivity W of the semi-algebraic set

$$\{(h_1\geqslant 0)\&\ldots\&(h_k\geqslant 0)\}\subsetneqq\tilde{\mathbb{Q}}^n$$

both $\mathscr{D}_0(R)\cap W\neq\phi$ and $\mathscr{D}_0(R)\backslash W\neq\phi$ are valid.

Now we proceed to exposing an outline of the algorithm.

Let an input system of inequalities

$$f_1>0,\ldots,f_m>0,f_{m+1}\geqslant 0,\ldots,f_k\geqslant 0$$

be given (see (1)), where the polynomials $f_1,\ldots,f_k\in\mathbb{Z}[X_2,\ldots,X_{n-1}]$ satisfy the bounds

$$\deg_{X_2,\ldots,X_{n-1}}(f_i)<d;\quad l(f_i)\leqslant M,\quad 1\leqslant i\leqslant k$$

(see (2)). Introduce a new variable X_1 and a polynomial $f_{k+1}=X_1f_1\ldots f_m-1$. Denote by π_1 a linear projection defined by the formula

$$\pi_1(X_1,\ldots,X_{n-1})=(X_2,\ldots,X_{n-1}).$$

The algorithm then yields a representative set $\mathscr{T}' \subset \tilde{\mathbb{Q}}^{n-1}$ for the system

$$f_1 \geqslant 0, \ldots, f_m \geqslant 0, f_{m+1} \geqslant 0, \ldots, f_k \geqslant 0, f_{k+1} \geqslant 0.$$

Then as the representative set $\mathscr{T}$ required in the theorem, the algorithm takes $\mathscr{T} = \pi_1(\mathscr{T}')$.

As at the beginning of the present section we take R corresponding to the polynomials $f_1, \ldots, f_{k+1}$.

Let us introduce new variables ε_1, ε, X_n and a polynomial

$$g_1 = (f_1 + \varepsilon_1) \ldots (f_{k+1} + \varepsilon_1) - \varepsilon_1^{k+1} \in \mathbb{Z}[\varepsilon_1][X_1, \ldots, X_{n-1}].$$

Consider now the polynomial

$$g = g_1^2 + (X_1^2 + \ldots + X_n^2 - (R+1))^2 \in \mathbb{Z}[\varepsilon_1][X_1, \ldots, X_n].$$

Define $N = (8kd)^n$ and introduce a family $\Gamma \subset \mathbb{Z}^{n-1}$ consisting of N^{n-1} integer vectors $\Gamma = \{\gamma = (\gamma_2, \ldots, \gamma_n)\}$, where each γ_i ranges independently over all values $1, \ldots, N$. The algorithm looks over all elements of Γ. Let us fix a vector $\gamma = (\gamma_2, \ldots, \gamma_n) \in \Gamma$, and consider the following system of equations where

$\Delta = \sum_{1 \leqslant j \leqslant n} (\partial g / \partial X_j)^2$ (cf. (4n)):

$$g - \varepsilon = \left(\frac{\partial g}{\partial X_2}\right)^2 - \frac{\gamma_2}{Nn}\Delta = \ldots = \left(\frac{\partial g}{\partial X_n}\right)^2 - \frac{\gamma_n}{Nn}\Delta = 0. \tag{6}$$

Denote by $\bar{V}^{(\varepsilon)} \subset \bar{F}^n$ the variety of solutions of the latter system. Now the algorithm from proposition 2 is applied to system (6) and, as a result, components $\bar{V}_j^{(\varepsilon)}$ of the variety

$$\bar{V}^{(\varepsilon)} = \bigcup_j \bar{V}_j^{(\varepsilon)}.$$

irreducible over the field $\mathbb{Q}(\varepsilon_1, \varepsilon)$ are produced. After that the algorithm selects all the null-dimensional components.

Then the algorithm, at first for each null-dimensional component, yields a certain finite family $\mathscr{R}_1 \subset \bar{F}_1^n$ containing the standard part (relatively to ε) of every point (for which the standard part is definable) from this component. The procedure for obtaining such an $\mathscr{R}_1$ is described in details in section 2 (see lemma 7). Then the algorithm selects the points from $\mathscr{R}_1$ lying in the semi-algebraic set $\{g = 0\} \cap F_1^n$ (see section 2). Collecting the points produced for all vectors $\gamma \in \Gamma$ and for all null-dimensional components $\bar{V}_j^{(\varepsilon)}$, the algorithm gets a representative set $\mathscr{S}' \subset F_1^n$ for the equation $g = 0$ (see lemma 8). Denote by π a linear projection defined by a formula

$$\pi(X_1, \ldots, X_n) = (X_1, \ldots, X_{n-1}).$$

The algorithm produces the set $\mathscr{S} = \pi(\mathscr{S}') \subset F_1^{n-1}$.

After that the algorithm applies the analogous procedure to the points from the set $\mathscr{S}$. As a result the algorithm obtains a finite set $\mathscr{R} \subset \bar{\mathbb{Q}}^{n-1}$ containing the standard part (relative to ε_1) of every point (for which the standard part is definable) from the set $\mathscr{S}$ (see section 3).

Finally, the algorithm constructs the required set $\mathscr{T}' \subset \mathscr{R}$ as a subset of $\mathscr{R}$ consisting of all those points from $\mathscr{R}$ that belong to the space $\tilde{\mathbb{Q}}^{n-1}$ (i.e. have real coordinates) and satisfy inequalities $f_1 \geqslant 0, \ldots, f_k \geqslant 0, f_{k+1} \geqslant 0$ (see section 3). At last, set $\mathscr{T} = \pi_1(\mathscr{T}')$.

References

Chistov, A. L., Grigor'ev, D. Yu. (1982). *Polynomial-time factoring of multivariable polynomials over a global field.* Preprint LOMI E–5–82, Leningrad.

Chistov, A. L., Grigor'ev, D. Yu. (1983*a*). *Subexponential-time solving systems of algebraic equations. I.* Preprint LOMI E-9-83, Leningrad.
Chistov, A. L., Grigor'ev, D. Yu. (1983*b*). *Subexponential-time solving systems of algebraic equations. II.* Preprint LOMI E-10-83, Leningrad.
Chistov, A. L. (1984). Polynomial-time factoring of polynomials and finding compounds of a variety within subexponential time. *Notes of Sci. Seminars of Leningrad Department of Math. Steklov Inst.* **137,** 124–188 (in Russian, English transl. to appear in J. Soviet Math.).
Chistov, A. L., Grigor'ev, D. Yu. (1984). Complexity of quantifier elimination in the theory of algebraically closed fields. *Springer Lec. Notes Comp. Sci.* **176,** 17–31.
Collins, G. E. (1975). Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Springer Lec. Notes Comp. Sci.* **33,** 134–183.
Grigor'ev, D. Yu. (1984). Factoring multivariable polynomials over a finite field and solving systems of algebraic equations. *Notes of Sci. Seminars of Leningrad Department of Math. Steklov Inst.* **137,** 20–79 (in Russian, English transl. to appear in J. Soviet Math.).
Grigor'ev, D. Yu. (1987). Computational complexity in polynomial algebra. Proc. Intern. Congress of Mathematicians, Berkeley.
Heindel, L. E. (1971). Integer arithmetic algorithms for polynomial real zero determination. *J. Assoc. Comp. Mach.* **18/4,** 533–548.
Heintz, J. (1983). Definability and fast quantifier elimination in algebraically closed field. *Theor. Comp. Sci.* **24,** 239–278.
Khachian, L. G. (1979). A polynomial algorithm in linear programming. *Soviet Math. Doklady* **20/1,** 191–194.
Lang, S. (1965). *Algebra.* New York: Addison-Wesley.
Lenstra, A. R. (1984). Factoring multivariable polynomials over algebraic number fields. *Springer Lec. Notes Comp. Sci.* **176,** 389–396.
Milnor, J. (1964). On the Betti numbers of real varieties. *Proc. Amer. Math. Soc.* **15/2,** 275–280.
Milnor, J. (1965). *Topology from the Differentiable Viewpoint.* University Press of Virginia.
Mignotte, M. (1974). An inequality about factors of polynomials. *Math. Comput.* **28/128,** 1153–1157.
Shafarevich, I. R. (1974). *Basic Algebraic Geometry.* Berlin: Springer-Verlag.
Tarski, A. (1951). *A Decision Method for Elementary Algebra and Geometry.* University of California Press.
Thorpe, J. A. (1979). *Elementary Topics in Differential Geometry.* Berlin: Springer-Verlag.
Vorobjov, N. N., Jr. (1984). Bounds of real roots of a system of algebraic equations. *Notes of Sci. Seminars of Leningrad Department of Math. Steklov Inst.* **137,** 7–19 (in Russian, English transl. to appear in J. Soviet Math.).
Vorobjov, N. N., Jr., Grigor'ev, D. Yu. (1985). Finding real solutions of systems of algebraic inequalities within the subexponential time. *Soviet Math. Dokl.* **32** (1), 316–320.
Wüthrich, H. R. (1976). Ein Entscheidungsverfahren für die Theorie der reell-abgeschlossenen Körper. In: Komplexität von Entschiedungs Problemen, (Specker, E, Strassen, V., Eds). *Springer Lec. Notes Comp. Sci.* **43,** 138–162.