J. Symbolic Computation (1988) **5**, 65–108

Complexity of Deciding Tarski Algebra

D. Yu GRIGOR'EV

Leningrad Department of Steklov Mathematical Institute
of the Academy of Sciences of the USSR,
Fontanka embankment 27, *Leningrad* 191011, *USSR*

(*Received* 20 *March* 1985)

Let a formula of Tarski algebra contain k atomic subformulas of the kind $(f_i \geqslant 0)$, $1 \leqslant i \leqslant k$, where the polynomials $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$ have degrees $\deg(f_i) < d$, let 2^M be an upper bound for the absolute value of every coefficient of the polynomials f_i, $1 \leqslant i \leqslant k$, let $a \leqslant n$ be the number of quantifier alternations in the prenex form of the formula. A decision method for Tarski algebra is described with the running time polynomial in $M(kd)^{(O(n))^{4a-2}}$. Previously known decision procedures have a time complexity polynomial in $(Mkd)^{2^{O(n)}}$.

Introduction

The decidability of the first order theory of real closed fields (or, in other words, Tarski algebra) was proved for the first time in Tarski (1951) (see also Seidenberg, 1954; Cohen 1969). Moreover, quantifier elimination methods for Tarski algebra were suggested in these papers. The running time, however, of the method from Tarski (1951) cannot be bounded by any finite tower of exponential functions. Collins (1975) (see also Monk, 1974; Wüthrich, 1976) proposes a quantifier elimination procedure for Tarski algebra with a running time bounded by $\mathscr{L}^{5^{O(n)}}$, where $\mathscr{L}$ denotes the size of an input formula and n is the number of variables occurring in the formula. In the present paper we present a decision algorithm for Tarski algebra that works within time $\mathscr{L}^{(O(n))^{4a-2}}$, where $a \leqslant n$ denotes the number of quantifier alternations in the input formula which can be assumed w.l.o.g. to be in the prenex form.

So the running time of the algorithm described is essentially better than that of the algorithms known earlier in the case of a small number a of quantifier alternations. One can observe that Fischer-Rabin (1974) prove an exponential lower bound on the complexity of deciding Tarski algebra for a sequence of formulas in which the order of growth of the number a of quantifier alternations is the same as the order of growth of the number n of variables. Thus, the number a of quantifier alternations makes the most essential contribution to the complexity of the decision problem. Further, the result of Fischer–Rabin was generalized in Berman (1980) to alternating Turing machines. Besides, EXPSPACE-completeness of the decision problem of Tarski algebra was proved in Mayr & Meyer (1982) and Ben-Or *et al.* (1984). The time bound of the algorithm from the latter paper is the same as in Collins (1975).

The present paper continues (Grigor'ev & Vorobjov, 1987) (see also Vorobjov & Grigor'ev, 1985) and uses its main result (see below, theorem 1 in section 1). One can even consider the present paper as a generalization of Grigor'ev & Vorobjov (1987), where an algorithm is described for finding real solutions of a given system of polynomial

0747–7171/88/010065+44 $03.00/0

© 1988 Academic Press Limited

inequalities (i.e. $a=1$ in the notations adopted in the present paper). In section 3 a certain construction from Chistov & Grigor'ev (1984) is involved. Chistov & Grigor'ev (1984) present a quantifier elimination method for the first-order theory of the algebraically closed fields with time-bound $\mathscr{L}^{(O(n))^{2a+1}}$.

Let

$$\exists X_{1,1} \dots \exists X_{1,s_1} \forall X_{2,1} \dots \forall X_{2,s_2} \dots \exists X_{a,1} \dots \exists X_{a,s_a}(P) \tag{1}$$

be a formula of Tarski algebra, where P is a quantifier-free formula with atomic subformulas $(f_i \geqslant 0)$, $1 \leqslant i \leqslant k$, and $f_i \in \mathbb{Z}[X_{1,1}, \dots, X_{1,s_1}, \dots, X_{a,1}, \dots, X_{a,s_a}]$. We denote by $n = s_1 + \dots + s_a$ the number of all the variables and by $a \leqslant n$ the number of quantifier alternations (in the presentation of the formula (1) a is odd, but this is not essential). The degrees $\deg_{X_{1,1},\dots,X_{a,s_a}}(f_i) < d$ and the absolute value of each integer coefficient of a polynomial f_i is supposed to be less than 2^M, $1 \leqslant i \leqslant k$. For a rational function $g \in \mathbb{Q}(X_1, \dots, X_n)$ we denote by $l(g)$ the maximum of the bit lengths of the coefficients in relatively prime polynomials $g_1, g_2 \in \mathbb{Z}[X_1, \dots, X_n]$, where $g = g_1/g_2$. In this notation $l(f_i) \leqslant M$, $1 \leqslant i \leqslant k$.

A decision method for Tarski algebra is an algorithm determining for any formula (1), whether it is valid. By validity of a formula we mean here validity over the field $\mathbb{R}$ of real numbers. On the other hand, one can consider validity over an arbitrary real closed field F (see e.g. Lang, 1965) by virtue of the following statement expressing the fact that all the real closed fields are elementary equivalent (Tarski, 1951) and that any extension of real closed fields is elementary.

Transfer principle. Let a formula (1) be such that the polynomials $f_i \in F[X_{1,1}, \dots, X_{a,s_a}]$ for some real closed field F, and let $F_1 \supset F$ be any other real closed field containing F. Then the truth values of the formula over the fields F and F_1, respectively, are the same.

The main purpose of the present paper is to prove the following theorem (see also Grigor'ev, 1985; Grigor'ev, 1987).

THEOREM. *One can design a decision algorithm for Tarski algebra which determines the truth value of a formula of the kind* (1) *within a time polynomial in* $M(kd)^{(O(n))^{4a-2}}$.

The latter estimate does not exceed $\mathscr{L}^{(O(n))^{4a-2}}$ where $\mathscr{L}$ denotes the size of the formula (1) (cf. Grigor'ev & Vorobjov, 1987).

We shall utilise the notation $g_1 \leqslant \mathscr{P}(g_2, \dots, g_m)$ for the functions $g_1 > 0, \dots, g_m > 0$ if for appropriate natural numbers p, q the inequality $g_1 \leqslant p(g_2 \dots g_m)^q$ holds.

Let us mention that the running time of the algorithm from Collins (1975) (and also Wüthrich, 1976) can be bounded by $\mathscr{P}((Mkd)^{2^{O(n)}})$.

Further, 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 zero characteristic fields are considered in the present paper and in order to avoid some swelling of formulas due to inseparable fields extensions we restrict ourselves herein to the zero characteristic case.

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

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

its minimal polynomial over $\mathbb{Q}(T_1, \ldots, T_e)$ with the 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. Let

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

Let $\deg_{X_m}(f) < \tau$, $deg_{T_j}(f) < \tau_2$, $\deg_{T_j}(\varphi) < \tau_1$, $\deg_Z(\varphi) < \tau_1$, $l(f) \leqslant M_2$, $l(\varphi) \leqslant M_1$ for all $1 \leqslant m \leqslant n$, $1 \leqslant j \leqslant e$. As a size $L_1(f)$ of the polynomial f we consider in proposition 1 a 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; Chistov, 1984; Grigor'ev, 1984; Chistov & 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 some coefficients equal to* 1, *the following bounds are true:*

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

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 an 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 $\deg_{X_1, \ldots, X_n}(f_i) < d$, $\deg_{T_1, \ldots, T_e, Z}(\varphi) < d_1$, $\deg_{T_1, \ldots, T_e}(f_i) < d_2$, $l(f_i) \leqslant M_2$ for all $1 \leqslant i \leqslant k$. As size of the system in proposition 2 we consider the value

$$L = kd^n d_1 d_2^e M_2 + d_1^{e+1} M_1.$$

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 in a union of 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 two ways: 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 fields isomorphism:

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

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 herein as the rational (coordinate) functions on the variety W. Under the isomorphism (*) $t_i \rightarrow X_{j_i}$ for suitable $1 \leqslant j_1 < \ldots < j_{n-m} \leqslant n$ where $1 \leqslant i \leqslant n - m$. Besides, θ is an 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 $c_1, \ldots, c_n$ together with 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*; Chistov, 1984; Grigor'ev, 1984; Chistov & 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 $n-m = \dim W_\alpha, \theta_\alpha = \theta, \Phi_\alpha = \Phi$ *(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,

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

and

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

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.

Let us briefly describe the further contents of the paper. In section 1 we present an algorithm for producing a representative set for the partition of the space $\mathbb{R}^n$ into maximal connected subsets on each of which a given family of polynomials has constant signs (lemma 2).

In Grigor'ev & Vorobjov (1987) (see also Vorobjov & Grigor'ev, 1985) a relevant tool for calculations with the infinitesimals was introduced. It is developed further in section 2. We ascertain some properties of semialgebraic curves over real closed fields; in addition some properties of the decomposition of a semi-algebraic set in its semialgebraic components of connectivity under passage to the limit (or standard part), i.e. when zeros are substituted for infinitesimals (lemmas 3, 4, 5).

In section 3 we describe a construction allowing to reduce a projection of a semialgebraic set along many variables to a projection along two variables (lemma 10). In this connection the question, whether a point belongs to the projection of a semi-algebraic set, is replaced by the question, whether a point infinitely close to the initial one belongs to the projection (lemma 6).

At the beginning of section 4 it is proved that the construction suggested in section 3 has a relevant additional property (lemma 11) which, together with sections 1 and 3, completes the description of the decision algorithm (lemma 13).

An outline and time analysis of the decision algorithm described is carried out in section 5. This completes the proof of the theorem.

As an application of the theorem we give a procedure to compute the dimension of a semialgebraic set within subexponential time in the last section 6.

If we were supplied with either a polynomial-time procedure for eliminating one quantifier in Tarski algebra or with a polynomial-time algorithm for finding the components of connectivity of a given semialgebraic set, then it would be possible to design a quantifier elimination method for Tarski algebra with the same time-bound as in the theorem. This follows from the construction in section 3 (see lemma 10). The author would like to conjecture the existence of a quantifier elimination procedure with the same time-bound as in the theorem.

1. Producing a Representative Set for a Semialgebraic Set

Let polynomials $f_1, \ldots, f_k \in \mathbb{Q}[X_1, \ldots, X_n]$ with rational coefficients be given, in addition $\deg(f_i) = \deg_{X_1,\ldots,X_n}(f_i) < d$ and bit lengths $l(f_i) \leqslant M$, $1 \leqslant i \leqslant k$. Let Π be a certain quantifier-free formula of Tarski algebra with atomic subformulas of the kind $(f_i \geqslant 0)$. Then the set, consisting of all points from $\mathbb{R}^n$ satisfying formula Π, is a semialgebraic set which we denote by $\{\Pi\} \subset \mathbb{R}^n$. The set $V = \{\Pi\} = \bigcup_j V_j$ coincides with the union of its components of connectivity V_j, each of which is also a semialgebraic set (see e.g. Collins, 1975; Wüthrich, 1976; and also Grigor'ev & Vorobjov, 1987). The procedures described in Collins (1975) and Wüthrich (1976) find quantifier-free formulas Π_j of Tarski algebra such that $V_j = \{\Pi_j\}$ within time $(Mkd)^{2^{O(n)}}$.

A finite set $\mathscr{S} \subset V$ is called a representative set for the set V if for every j the intersection $V_j \cap \mathscr{S} \neq \phi$. With the help of procedures from Collins (1975) and Wüthrich (1976) one can produce a representative set for V also within time $(Mkd)^{2^{O(n)}}$. Further, we need the main result from Grigor'ev & Vorobjov (1987) (see also Vorobjov & Grigor'ev, 1985) considerably improving the latter time-bound.

Theorem 1. *One can design an algorithm which, for an arbitrary semialgebraic set of the sort*

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

produces a representative set $\mathscr{S}$ with a number of points not greater than $\mathscr{P}((kd)^{n^2})$; the running time of the algorithm does not exceed $\mathscr{P}(M, (kd)^{n^2})$. Furthermore, for every point $(\xi_1, \ldots, \xi_n) \in \mathscr{S}$ the algorithm constructs a polynomial $\Phi \in \mathbb{Q}[Z]$ irreducible over the field $\mathbb{Q}$, and expressions

$$\xi_i = \xi_i(\theta) = \sum_{0 \leqslant j < \deg(\Phi)} \alpha_j^{(i)} \theta^j,$$

where $\alpha_j^{(i)} \in \mathbb{Q}$, $1 \leqslant i \leqslant n$, $0 \leqslant j < \deg(\Phi)$ and $\theta \in \mathbb{R}$, $\Phi(\theta) = 0$. Moreover, the algorithm yields a pair of rational numbers $b_1, b_2 \in \mathbb{Q}$ such that in the interval $(b_1, b_2) \subset \mathbb{R}$ θ is the unique real root of the polynomial Φ. Moreover,

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

for suitable natural numbers $1 \leqslant \lambda_i \leqslant \deg(\Phi)$. Finally, the following bounds are valid:

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

In particular, the coordinates of the points from $\mathscr{S}$ are real algebraic numbers.

Remark. Based on theorem 1 and on a result from Heindel (1971), one can find δ-approximations to the points of the representative set $\mathscr{S}$ within time $\mathscr{P}(\log(1/\delta), M, (kd)^{n^2})$.

Following Heintz (1983) we call $(\{f_i\}_{1 \leqslant i \leqslant k})$-cell any nonempty semialgebraic set of the form

$$\{\underset{i \in I}{\&} (f_i = 0) \& \underset{i_1 \in I_1}{\&} (f_{i_1} > 0) \& \underset{i_2 \in I_2}{\&} (f_{i_2} < 0)\},$$

where $I \cup I_1 \cup I_2 = \{1, \ldots, k\}$. The next lemma allows us to find all $(\{f_i\}_{1 \leqslant i \leqslant k})$-cells.

LEMMA 1. *One can enumerate all partitions of the set of indices* $I\cup I_1\cup I_2=\{1,\ldots,k\}$ *such that the corresponding semialgebraic set*

$$\{\mathop{\&}_{i\in I}(f_i=0)\&\mathop{\&}_{i_1\in I_1}(f_{i_1}>0)\&\mathop{\&}_{i_2\in I_2}(f_{i_2}<0)\}$$

is nonempty, i.e. is a $(\{f_i\}_{1\leqslant i\leqslant k})$*-cell, within time* $\mathscr{P}(M,(kd)^{n^2})$. *Furthermore, the number of* $(\{f_i\}_{1\leqslant i\leqslant k})$*-cells does not exceed* $\mathscr{P}((kd)^n)$.

PROOF. We shall conduct the enumeration of all $(\{f_i\}_{1\leqslant i\leqslant k})$-cells by recursion on k. Assume that all $(\{f_i\}_{1\leqslant i\leqslant j})$-cells are already selected for a certain $0\leqslant j<k$. For each $(\{f_i\}_{1\leqslant i\leqslant j})$-cell $K\subset\mathbb{R}^n$, the algorithm detects with the aid of theorem 1, what sets among the following three:

$$K\cap\{f_{j+1}=0\},\quad K\cap\{f_{j+1}>0\},\quad K\cap\{f_{j+1}<0\}$$

are nonempty, i.e. are $(\{f_i\}_{1\leqslant i\leqslant j+1})$-cells. Thus, all $(\{f_i\}_{1\leqslant i\leqslant j+1})$-cells will be enumerated.

Let us now estimate the number of all $(\{f_i\}_{1\leqslant i\leqslant k})$-cells. Any nonempty subset of $\mathbb{C}^n$ of the kind

$$\{\mathop{\&}_{i\in I}(f_i=0)\&\mathop{\&}_{i\notin I}(f_i\neq 0)\},$$

where $I\subset\{1,\ldots,k\}$ is called a complex $(\{f_i\}_{1\leqslant i\leqslant k})$-cell (see Heintz, 1983).

According to Heintz (1983) the number of complex $(\{f_i\}_{1\leqslant i\leqslant k})$-cells is less or equal to $(1+\sum_{1\leqslant i\leqslant k}\deg(f_i))^n$. For an arbitrary fixed subset of indices $I\subset\{1,\ldots,k\}$, the number of $(\{f_i\}_{1\leqslant i\leqslant k})$-cells of the sort

$$\{\mathop{\&}_{i\in I}(f_i=0)\&\mathop{\&}_{i_1\in I_1}(f_{i_1}>0)\&\mathop{\&}_{i_2\in I_2}(f_{i_2}<0)\}\subset\mathbb{R}^n$$

for all possible I_1, I_2 does not exceed the number of components of connectivity (in $\mathbb{R}^n$) of the semialgebraic set

$$\{\mathop{\&}_{i\in I}(f_i=0)\&\mathop{\&}_{i\notin I}(f_i\neq 0)\}\subset\mathbb{R}^n,$$

because on every such component of connectivity all the signs $\operatorname{sgn}(f_i)$, $1\leqslant i\leqslant k$ are constant. The set

$$\{\mathop{\&}_{i\in I}(f_i=0)\&\mathop{\&}_{i\notin I}(f_i\neq 0)\}$$

coincides with the projection of the semialgebraic set

$$V^{(1)}=\{\mathop{\&}_{i\in I}(f_i=0)\&(Z\prod_{i\notin I}f_i=1)\}\subset\mathbb{R}^{n+1}$$

along the variable Z. By virtue of Milnor (1964) the number of components of connectivity of the set $V^{(1)}$ is less or equal to $(2kd)^{n+1}$. Therefore, the whole number of $(\{f_i\}_{1\leqslant i\leqslant k})$-cells does not exceed

$$(1+\sum_{1\leqslant i\leqslant k}\deg(f_i))^n(2kd)^{n+1}\leqslant\mathscr{P}(kd)^n).$$

This entails also the required in the lemma time-bound in view of theorem 1 and completes the proof of the lemma.

Let the polynomials $g_1,\ldots,g_m\in\mathbb{R}[X_1,\ldots,X_n]$. Denote by $\mathscr{U}(\{g_i\}_{1\leqslant i\leqslant m})$ the partition of the space $\mathbb{R}^n$ into maximal connected subsets on each of which the signs $\operatorname{sgn}(g_i)$ are constant for every $1\leqslant i\leqslant m$ (cf. Wüthrich, 1976). Observe that the family of elements of the partition $\mathscr{U}(\{g_i\}_{1 \leqslant i \leqslant m})$ coincides with the family of components of connectivity of all possible $(\{g_i\}_{1 \leqslant i \leqslant m})$-cells. A finite set $\mathscr{S} \subset \mathbb{R}^n$ is called a *representative set* for the partition $\mathscr{U}(\{g_i\}_{1 \leqslant i \leqslant m})$ if each element of the partition contains at least one point from the set $\mathscr{S}$.

Consider now polynomials

$$g_1, \ldots, g_m \in \mathbb{Q}[Y_1, \ldots, Y_q, X_1, \ldots, X_n].$$

Let $y = (y_1, \ldots, y_q) \in \mathbb{R}^q$ be a real algebraic point given in the following form (cf. theorem 1): $\Phi_1(Z) \in \mathbb{Q}[Z]$ is a polynomial irreducible over $\mathbb{Q}$;

$$y_p = y_p(\theta_1) = \sum_{0 \leqslant j < \deg(\Phi_1)} \rho_j^{(p)} \theta_1^j$$

are expressions where $\rho_j^{(p)} \in \mathbb{Q}$, $1 \leqslant p \leqslant q$, $0 \leqslant j < \deg(\Phi_1)$ and $\theta_1 \in \mathbb{R}$, $\Phi_1(\theta_1) = 0$; furthermore, a pair of rational numbers $c_1, c_2 \in \mathbb{Q}$ is given such that in the interval $(c_1, c_2) \subset \mathbb{R}$, θ is the unique real root of the polynomial Φ_1. Moreover,

$$\theta_1 = \sum_{1 \leqslant p \leqslant q} \lambda_p^{(1)} y_p(\theta_1)$$

for some natural numbers $\lambda_p^{(1)}$, $1 \leqslant p \leqslant q$. In addition, the following bounds are fulfilled: $\deg(g_j) < d$; $l(g_j) \leqslant M$ for every $1 \leqslant j \leqslant m$ and $\deg(\Phi_1) < d_1$;

$$l(\Phi_1),\ l(y_p(\theta_1)),\ l(c_1),\ l(c_2) \leqslant M_1$$

for all $1 \leqslant p \leqslant q$. Introduce polynomials

$$\hat{g}_j(X_1, \ldots, X_n) = g_j(y_1, \ldots, y_q, X_1, \ldots, X_n) \in \mathbb{R}[X_1, \ldots, X_n], \quad 1 \leqslant j \leqslant m.$$

The following lemma allows us to produce a representative set for the partition $\mathscr{U}(\{\hat{g}_j\}_{1 \leqslant j \leqslant m})$.

Lemma 2. *One can design an algorithm which produces a representative set $\mathscr{S} \subset \mathbb{R}^n$ for the partition $\mathscr{U}(\{\hat{g}_j\}_{1 \leqslant j \leqslant m})$ within time $\mathscr{P}(M, M_1, q, (mdd_1)^{n^2})$, where $\mathscr{S}$ contains not more than $\mathscr{P}((mdd_1)^{n^2})$ points. Moreover, for every point $(\xi_1, \ldots, \xi_n) \in \mathscr{S}$ the algorithm constructs polynomial $\Phi \in \mathbb{Q}[Z]$ irreducible over $\mathbb{Q}$, and expressions*

$$\xi_i = \xi_i(\theta) = \sum_{0 \leqslant j < \deg(\Phi)} \alpha_j^{(i)} \theta^j,$$

where $\alpha_j^{(i)} \in \mathbb{Q}$, $1 \leqslant i \leqslant n$, $0 \leqslant j < \deg(\Phi)$ and $\theta \in \mathbb{R}$, $\Phi(\theta) = 0$; apart from that, the algorithm yields a pair of rational numbers $b_1, b_2 \in \mathbb{Q}$ such that in the interval $(b_1, b_2) \subset \mathbb{R}$ θ is the only real root of the polynomial Φ. Furthermore, the expressions

$$y_p = y_p(\theta) = \sum_{0 \leqslant j < \deg(\Phi)} \mu_j^{(p)} \theta^j$$

are constructed by the algorithm, where $\mu_j^{(p)} \in \mathbb{Q}$, $1 \leqslant p \leqslant q$, $0 \leqslant j < \deg(\Phi)$. In addition

$$\theta = \lambda_0 \theta_0 + \sum_{1 \leqslant i \leqslant n} \lambda_i \xi_i$$

for certain natural numbers $1 \leqslant \lambda_i \leqslant \deg(\Phi)$, $0 \leqslant i \leqslant n$. At last, we have the following bounds:

$$\deg(\Phi) = \mathscr{P}((mdd_1)^n)$$

and

$$l(\Phi),\ l(\xi_i(\theta)),\ l(y_p(\theta)),\ l(b_1),\ l(b_2) \leqslant (M + M_1 + q)\mathscr{P}((mdd_1)^n).$$

Proof. Consider the following family consisting of $(m+2)$ polynomials in $(n+1)$ variables $T, X_1, \ldots, X_n$ with rational coefficients:

$$\tilde{g}_j(T, X_1, \ldots, X_n) = g_j(y_1(T), \ldots, y_q(T), X_1, \ldots, X_n), \quad 1 \leqslant j \leqslant m;$$
$$\tilde{g}_{m+1}(T, X_1, \ldots, X_n) = \Phi_1(T); \qquad \tilde{g}_{m+2}(T, X_1, \ldots, X_n) = (T - c_1)(c_2 - T).$$

To begin with, let us enumerate all $(\{\tilde{g}_j\}_{1 \leqslant j \leqslant m+2})$-cells based on lemma 1. Next for every $(\{\tilde{g}_j\}_{1 \leqslant j \leqslant m+2})$-cell

$$\Big\{\mathop{\&}_{j \in J} (\tilde{g}_j = 0) \& \mathop{\&}_{j_1 \in J_1} (\tilde{g}_{j_1} > 0) \& \mathop{\&}_{j_2 \in J_2} (\tilde{g}_{j_2} < 0)\Big\}$$

such that the requirements $\tilde{g}_{m+1} = 0$, $\tilde{g}_{m+2} > 0$ are satisfied, i.e. $(m+1) \in J$, $(m+2) \in J_1$, the algorithm produces a representative set $\mathscr{S}_{J, J_1, J_2} \subset \mathbb{R}^{n+1}$ using theorem 1. Denote by $\pi\colon \mathbb{R}^{n+1} \to \mathbb{R}^n$ the linear projection defined by the formula $\pi(T, X_1, \ldots, X_n) = (X_1, \ldots, X_n)$ and put

$$\mathscr{S} = \bigcup_{J, J_1, J_2} \pi(\mathscr{S}_{J, J_1, J_2}) \subset \mathbb{R}^n,$$

where the union is taken over all $(\{\tilde{g}_j\}_{1 \leqslant j \leqslant m})$-cells satisfying the requirements stated above. Then $\mathscr{S}$ is a representative set for the partition $\mathscr{U}(\{\hat{g}_j\}_{1 \leqslant j \leqslant m})$, since the partition $\mathscr{U}(\{\hat{g}_j\}_{1 \leqslant j \leqslant m})$ is isomorphic by means of the projection π to the partition of the space $\mathbb{R}^{n+1} \cap \{T = \theta_1\} \simeq \mathbb{R}^n$ formed by the components of connectivity of all $(\{\tilde{g}_j\}_{1 \leqslant j \leqslant m+2})$-cells satisfying the requirements $(m+1) \in J, (m+2) \in J_1$, taking into account that the requirements $\tilde{g}_{m+1}(T) = 0$, $\tilde{g}_{m+2}(T) > 0$ imply the equality $T = \theta_1$.

Let a point $(\theta_1, \xi_1, \ldots, \xi_n) \in \mathscr{S}_{J, J_1, J_2}$. According to theorem 1, a polynomial $\Phi \in \mathbb{Q}[Z]$ irreducible over the field $\mathbb{Q}$ corresponds to the point, as well as expressions

$$\xi_i = \xi_i(\theta) = \sum_{0 \leqslant j < \deg(\Phi)} \alpha_j^{(i)} \theta^j, \quad 1 \leqslant i \leqslant n$$

and

$$\theta_1 = \theta_1(\theta) = \sum_{0 \leqslant j < \deg(\Phi)} \alpha_j^{(0)} \theta^j;$$

moreover, the algorithm from theorem 1 yields an interval $(b_1, b_2) \subset \mathbb{R}$ (with rational endpoints $b_1, b_2 \in \mathbb{Q}$) which contains a unique real root $\theta \in (b_1, b_2)$ of the polynomial Φ. Furthermore,

$$\theta = \lambda_0 \theta_1 + \sum_{1 \leqslant i \leqslant n} \lambda_i \xi_i$$

for appropriate natural numbers $1 \leqslant \lambda_i \leqslant \deg(\Phi)$, $0 \leqslant i \leqslant n$. Substituting the constructed expression $\theta_1(\theta)$ in the expressions $y_p(\theta_1), 1 \leqslant p \leqslant q$ we obtain the expressions $y_p(\theta), 1 \leqslant p \leqslant q$. Observe that $\deg_{T, X_1, \ldots, X_n}(\tilde{g}_j) < dd_1$, $1 \leqslant j \leqslant m+2$. Hence, the number of points in the set $\mathscr{S}_{J, J_1, J_2}$ is not greater than $\mathscr{P}((mdd_1)^{n^2})$ by virtue of theorem 1; on the other hand the number of $(\{\tilde{g}_j\}_{1 \leqslant j \leqslant m+2})$-cells does not exceed $\mathscr{P}((mdd_1)^n)$ in view of lemma 1. Therefore, the set $\mathscr{S}$ contains not more than $\mathscr{P}((mdd_1)^{n^2})$ points.

Theorem 1 entails the bound $\deg(\Phi) \leqslant \mathscr{P}((mdd_1)^n)$. The bit lengths of coefficients are bounded by

$$l(\tilde{g}_j) \leqslant M + M_1 d + d \log(d_1) + q \log(d);$$

from this we obtain the bounds:

$$l(\Phi), l(\xi_i(\theta)), l(\theta_1(\theta)), l(b_1), l(b_2) \leqslant (M + M_1 + q)\mathscr{P}((mdd_1)^n), \quad 1 \leqslant i \leqslant n;$$

thus,

$$l(y_p(\theta)) \leqslant (M + M_1 + q)\mathscr{P}((mdd_1)^n), \quad 1 \leqslant p \leqslant q.$$

Finally, the running time of the algorithm can be estimated by $\mathscr{P}(M, M_1, q, (mdd_1)^{n^2})$ by lemma 1 and theorem 1, this completes the proof of the lemma.

2. Semialgebraic Curves Over Real Closed Fields (With Infinitesimals)

First of all we shall recall some facts about real closed fields.

Throughout the present section, F denotes a real closed field. Consider the ordered field $F(\varepsilon)$, in which the order is defined by the condition $0 < \varepsilon < \beta$ for all $0 < \beta \in F$, in other words, the element ε is infinitesimal relatively to the elements of the field F. For any ordered field F_1 denote by $\tilde{F}_1 \supset F_1$ (defined uniquely up to an isomorphism of the ordered fields) the real closure of the field F_1 (see e.g. Lang, 1965). For instance, $\tilde{\mathbb{Q}} \subset \mathbb{R}$ is the field of real algebraic numbers.

A Puiseux series (or in other words, power-fractional series) is a series of the kind

$$b = \sum_{i \geqslant 0} \beta_i \varepsilon^{\nu_i/\mu},$$

where $0 \neq \beta_i \in F$ for each i, the integers $\nu_0 < \nu_1 < \ldots$ increase, the natural number $\mu \geqslant 1$ may depend on the series. The totality of all Puiseux series (with added zero) forms the field $F((\varepsilon^{1/\infty})) \supset \widetilde{F(\varepsilon)} \supset F(\varepsilon)$ containing the real closure $\widetilde{F(\varepsilon)}$ of the field $F(\varepsilon)$. The order in the field $F((\varepsilon^{1/\infty}))$ (that induces the order in the field $\widetilde{F(\varepsilon)}$) is lexicographical. Furthermore, the field

$$\bar{F}((\varepsilon^{1/\infty})) \supset \overline{F(\varepsilon)} = F(\varepsilon)[\sqrt{-1}]$$

of Puiseux series over the algebraic closure $\bar{F} = F[\sqrt{-1}]$ of the field F contains the algebraic closure $\overline{F(\varepsilon)}$ of the field $F(\varepsilon)$.

If $\nu_0 < 0$, then the element b is called *infinitely large* (relatively to the field F); if $\nu_0 > 0$, then b is *infinitesimal.* A vector $(b_1, \ldots, b_n) \in (F((\varepsilon^{1/\infty})))^n$ is called F-finite if every coordinate b_i is not infinitely large. For any F-finite element $b \in F((\varepsilon^{1/\infty}))$, its *standard part* $st(b) \in F$ is defined and is equal to β_0 in cases when $\nu_0 = 0$, or $st(b) = 0$ when $\nu_0 > 0$. For an F-finite vector $(b_1, \ldots, b_n) \in (F((\varepsilon^{1/\infty})))^n$, its standard part is

$$st(b_1, \ldots, b_n) = (st(b_1), \ldots, st(b_n)).$$

If each point from a set $V \subset (F((\varepsilon^{1/\infty})))^n$ is F-finite, then its standard part $st(V) \subset F^n$ is defined as the set of standard parts of all points from the set V. In the sequel, we deal with the subfield $\widetilde{F(\varepsilon)}$ of $F((\varepsilon^{1/\infty}))$ and apply to it the notions introduced.

Now we shall demonstrate how the transfer principle can work and show (a known fact) that any semialgebraic set over a real closed field F can be represented uniquely as a union of its components of connectivity, each in its turn being a semialgebraic set. Consider a semialgebraic set $W = \{\Pi\} \subset F^n$, determined by a quantifier-free formula Π of Tarski algebra with the atomic subformulas of the kind $(f \geqslant 0)$, where the polynomials $f \in F[X_1, \ldots, X_n]$. By a format of the formula Π we shall 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 $F = \mathbb{R}$, the set W is uniquely representable in a union of its components of connectivity $W = \bigcup_i W_i$, where every W_i is in its turn a semialgebraic set (and connected in the euclidean topology). From e.g. the papers by Collins (1975), and Wüthrich (1976), one can deduce the existence of a function $\mathfrak{N}$ such that if a format of a formula Π is less than $\mathscr{N}$, then the whole number of the components W_i is less than $\mathfrak{N}(\mathscr{N})$

and, moreover, one can find quantifier-free formulas Π_i of Tarski algebra each of the format less than $\mathfrak{N}(\mathscr{N})$ that $W_i = \{\Pi_i\}$. Indeed, the algorithms from Collins (1975) and Wüthrich (1976) allow to produce a cylindrical algebraic decomposition of a semialgebraic set and as a corollary to produce the decomposition on the components of connectivity. For a given format $\mathscr{N}$ 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 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; to any vertex with out-degree three corresponds a polynomial. The computation for arbitrary initial formula, with specified coefficients substituted instead of 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 $\mathscr{N}$, one can yield a formula $\Omega_{\mathscr{N}}$ of Tarski algebra (for the case of the field $F = \mathbb{R}$), expressing the existence of decomposition of any semialgebraic set $W = \{\Pi\}$, with the format of Π less than $\mathscr{N}$ into less than $\mathfrak{N}(\mathscr{N})$ its components of connectivity $W = \bigcup_i \{\Pi_i\}$, such that the format of every Π_i is less than $\mathfrak{N}(\mathscr{N})$. Moreover, the formula $\Omega_{\mathscr{N}}$ 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 $\Omega_{\mathscr{N}}$ claims the "connectedness" of every $\{\Pi_i\}$, this means that there do not exist two "separated" semialgebraic subsets of $\{\Pi_i\}$, each determined by a quantifier-free formula of Tarski algebra with the format less than $\mathfrak{N}(\mathfrak{N}(\mathscr{N}))$.

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

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

As usual, one can define a *semialgebraic curve* $C \subset F^n$ as a semialgebraic set for which there exists a linear projection on the line (i.e. on F), such that the inverse image of every point under the projection consists of a finite number of points and in addition the latter number is less than a certain number depending only on the curve C. A mapping $\varphi: V_1 \to V_2$ where $V_1 \subset F^n$, $V_2 \subset F^m$ are semialgebraic sets, is called semialgebraic if its graph is a semialgebraic subset in the space F^{m+n}. We shall utilise the terms continuous mapping, open and closed set in the sense of the topology with the base of all open balls. We denote by $\mathscr{D}_x(R)$ the closed ball of radius R with the centre in the point x.

We shall call a set $V \subset F^n$ *monotone* iff there exists a vector $(\delta_1, \ldots, \delta_n) \in \{-1, +1\}^n$ satisfying the following property: for any pair of points

$$v^{(1)} = (v_1^{(1)}, \ldots, v_n^{(1)}), \qquad v^{(2)} = (v_1^{(2)}, \ldots, v_n^{(2)}) \in V$$

either

$$\delta_1 v_1^{(1)} \geqslant \delta_1 v_1^{(2)}, \ldots, \delta_n v_n^{(1)} \geqslant \delta_n v_n^{(2)} \quad \text{or} \quad \delta_1 v_1^{(1)} \leqslant \delta_1 v_1^{(2)}, \ldots, \delta_n v_n^{(1)} \leqslant \delta_n v_n^{(2)}$$

are fulfilled.

One can prove the next lemma first for the case of the field $F = \mathbb{R}$ bounding the formats of the constructed semialgebraic sets (and their number) via the formats of the given semialgebraic sets, and after that make use of the transfer principle. The proof for the case $F = \mathbb{R}$ is quite cumbersome and routine, on the other hand, the reader can reproduce it for himself without great difficulties, therefore we omit the proof.

LEMMA 3.

(*a*) *The image of any connected semialgebraic curve under the action of a continuous curve on this semialgebraic mapping is also a connected semialgebraic curve.*

(*b*) *Any pair of points of a connected semialgebraic set can be joined by a closed connected semialgebraic curve entirely situated in this set and in a certain ball.*

(*c*) *One can represent any closed semialgebraic curve as a union of a finite number of monotone closed semialgebraic curves.*

Let the elements $\varepsilon_1 > \varepsilon_2 > \ldots > \varepsilon_m > 0$ be such that the element ε_{i+1} is infinitesimal relatively to the field $F(\varepsilon_1, \ldots, \varepsilon_i)$ for each $0 \leqslant i < m$. For every element $\alpha \in \widetilde{F(\varepsilon_1, \ldots, \varepsilon_m)}$ one can uniquely define its standard part $st(\alpha) \in F$ (provided that it exists) by recursion on m. We denote $F_m = \widetilde{F(\varepsilon_1, \ldots, \varepsilon_m)}$.

LEMMA 4.

(*a*) *Given a closed connected semialgebraic curve $C \subset \mathscr{D}_0(R) \subset F^n$, where $R \in F$, one can find a closed connected semialgebraic curve $C^{(\varepsilon)} \subset \mathscr{D}_0(R) \subset F_m^n$ such that $C^{(\varepsilon)} \supset st(C^{(\varepsilon)}) = C$ and, furthermore, for a certain quantifier-free formula Π of Tarski algebra both $C = \{\Pi\} \subset F^n$ and $C^{(\varepsilon)} = \{\Pi\} \subset F_m^n$ are true;*

(*b*) *Let $W \subset \mathscr{D}_0(R) \subset F_m^n$ be a connected semialgebraic set where $R \in F$. Assume that the set $st(W) \subset V \subset F^n$ for a certain semialgebraic set V. Then $st(W) \subset V_1$ for a suitable component of connectivity V_1 of the set V.*

REMARK. Under the conditions of item (b) it is apparently possible to prove that $st(W) \subset F^n$ is a semialgebraic set, but since we shall not need this further, we do not dwell on its proof.

PROOF. (a) By virtue of lemma (3c), one can represent C as a union of monotone closed curves and after that decompose each monotone curve on the components of connectivity. Thus, we obtain a representation $C = \bigcup_i C_i$ of C as a union of monotone closed connected curves C_i. Let $C_i = \{\Pi_i\}$ for an appropriate quantifier-free formula Π_i of Tarski algebra. We set

$$C_i^{(\varepsilon)} = \{\Pi_i\} \subset F_m^n, \qquad \Pi = \bigvee_i \Pi_i \quad \text{and} \quad C^{(\varepsilon)} = \{\Pi\} = \bigcup_i C_i^{(\varepsilon)}.$$

Evidently $C_i^{(\varepsilon)} \supset C_i$ and $st(C_i^{(\varepsilon)}) \supset C_i$. The transfer principle implies the inclusion $C_i^{(\varepsilon)} \subset \mathscr{D}_0(R)$, since it is equivalent to the formula $\forall\, x(\Pi_i(x) \Rightarrow \|x\| \leqslant R)$ of Tarski algebra.

We fix a curve C_i and we claim that $C_i^{(\varepsilon)} \subset F_m^n$ is a monotone closed connected semialgebraic curve and besides that $C_i = st(C_i^{(\varepsilon)})$. From this the statement of item (a) will be concluded easily.

The closedness of semialgebraic set $C_i^{(\varepsilon)}$ can be inferred from the transfer principle. Now we are going to prove that $C_i^{(\varepsilon)}$ is a monotone curve. Consider a linear projection π of the n-dimensional space on the line which is given by the formula

$$\pi(x_1, \ldots, x_n) = \sum_{1 \leqslant j \leqslant n} \delta_j x_j,$$

where $\delta_j = \pm 1$ are taken from the definition of monotonicity of curve C_i. In view of lemma (3a), the image $\pi(C_i) \subset F$ is a connected semialgebraic set, therefore, $\pi(C_i)$ is an interval. Moreover, in the case of the field $F = \mathbb{R}$, the image $\pi(C_i)$ of the compact set C_i is also a compact, in particular $\pi(C_i)$ is a closed interval. The transfer principle entails that $\pi(C_i) = [\gamma_1, \gamma_2]$ is a closed interval in the case of an arbitrary real closed field F. Moreover, the mapping π: $C_i \to [\gamma_1, \gamma_2]$ is bijective, since C_i is monotone. Henceforth, $\pi(C_i^{(\varepsilon)}) = [\gamma_1, \gamma_2] \subset F_m$ according to the transfer principle, furthermore, the mapping π: $C_i^{(\varepsilon)} \to [\gamma_1, \gamma_2]$ is bijective. In particular, we deduce that $C_i^{(\varepsilon)}$ is a semialgebraic curve and, in addition, it is monotone again by the transfer principle.

Now we shall check that $st(C_i^{(\varepsilon)}) \subset C_i$. Indeed, let a point $x = (x_1, \ldots, x_n) \in C_i^{(\varepsilon)}$; then there exists a point

$$y = (y_1, \ldots, y_n) \in C_i \subset C_i^{(\varepsilon)}$$

such that

$$\pi(y) = st(\pi(x)) \in [\gamma_1, \gamma_2] \subset F$$

(see above). The elements $\delta_j(x_j - y_j) \in F_m$ are either non-negative for all $1 \leqslant j \leqslant n$ or non-positive for all $1 \leqslant j \leqslant n$, since $C_i^{(\varepsilon)}$ is monotone. On the other hand,

$$st\Big(\sum_{1 \leqslant j \leqslant n} \delta_j(x_j - y_j)\Big) = st(\pi(x)) - \pi(y) = 0,$$

therefore,

$$st(x_j - y_j) = \delta_j\, st(\delta_j(x_j - y_j)) = 0$$

for all $1 \leqslant j \leqslant n$, i.e. $st(x) = y$, that proves the inclusion $st(C_i^{(\varepsilon)}) \subset C_i$.

At last, consider a semialgebraic mapping π^{-1}: $[\gamma_1, \gamma_2] \to C_i^{(\varepsilon)}$. The mapping is continuous by virtue of monotonicity of $C_i^{(\varepsilon)}$, henceforth, the curve $C_i^{(\varepsilon)}$ is connected in view of lemma (3a). Now we shall show that $C^{(\varepsilon)}$ is connected. Suppose the contrary. Then for some family I of indices the intersection

$$\Big(\bigcup_{i \in I} C_i^{(\varepsilon)}\Big) \cap \Big(\bigcup_{i \notin I} C_i^{(\varepsilon)}\Big) = \phi.$$

Taking into account that the curve C is connected and that curves C_i are closed, we deduce the existence of a point

$$x \in \Big(\bigcup_{i \in I} C_i\Big) \cap \Big(\bigcup_{i \notin I} C_i\Big) \subset \Big(\bigcup_{i \in I} C_i^{(\varepsilon)}\Big) \cap \Big(\bigcup_{i \notin I} C_i^{(\varepsilon)}\Big).$$

The obtained contradiction proves the connectivity of $C^{(\varepsilon)}$.

(b) For every component of connectivity V_i of the set V, consider the following semialgebraic set $U_i \subset F^n$ (cf. lemma 1 in Grigor'ev & Vorobjov, 1987). A point $x \in U_i$ iff there exist such $\tau_i^{(x)} \geqslant 0$, $\tau_{1i}^{(x)} > 0$ that the intersection $\mathscr{D}_x(\tau_i^{(x)}) \cap V_i \neq \phi$, and for each $j \neq i$ the intersection $\mathscr{D}_x(\tau_i^{(x)}+\tau_{1i}^{(x)}) \cap V_j = \phi$. Now we shall establish various properties of the set U_i, which is semialgebraic since it is represented by some formula of Tarski algebra.

(α) The inclusion $V_i \subset U_i$ is correct. Indeed, for any point $y \in V_i$, one can set $\tau_i^{(y)}=0$ and can take $\tau_{1i}^{(y)}$ from the definition of components of connectivity (see above).

(β) The set U_i is open. Let a point $x \in U_i$, we shall check that the ball $\mathscr{D}_x(\tau_{1i}^{(x)}/3) \subset U_i$. Actually, we assert that for any point $z \in \mathscr{D}_x(\tau_{1i}^{(x)}/3)$, one can take $\tau_i^{(z)}=\tau_i^{(x)}+\tau_{1i}^{(x)}/3$ and $\tau_{1i}^{(z)}=\tau_{1i}^{(x)}/3$. There is such a point $y \in V_i$ that the distance $\|y-x\| \leqslant \tau_i^{(x)}$, henceforth,

$$\|y-z\| \leqslant \|y-x\|+\|x-z\| \leqslant \tau_i^{(z)}.$$

Besides that, for any point $z_1 \in V_j$, where $j \neq i$ the inequalities

$$\|z_1-z\| \geqslant \|z_1-x\|-\|z-x\| > \tau_i^{(z)}+\tau_{1i}^{(z)}$$

are true.

(γ) For $i \neq j$ the intersection $U_i \cap U_j = \phi$. Suppose, on the contrary, that a certain point $x \in U_i \cap U_j$. There exist points $y_i \in V_i$, $y_j \in V_j$, for which $\|x-y_i\| \leqslant \tau_i^{(x)}$, $\|x-y_j\| \leqslant \tau_j^{(x)}$. On the other hand, $\|x-y_j\| > \tau_i^{(x)}+\tau_{1i}^{(x)}$ and $\|x-y_i\| > \tau_j^{(x)}+\tau_{1j}^{(x)}$, this leads to the contradiction.

Let $U_i=\{\Pi_i\}$ for each i for suitable quantifier-free formulas Π_i of Tarski algebra. Consider semialgebraic sets $U_i^{(\varepsilon)}=\{\Pi_i\} \subset F_m^n$, for which properties ($\alpha$), ($\beta$), ($\gamma$) are fulfilled according to the transfer principle.

Let an arbitrary point $w \in W$; then the point $st(w) \in V_{i_0}$ (which is defined since $\|w\| \leqslant R$) for an appropriate i_0. By virtue of (α), (β) the ball $\mathscr{D}_{st(w)}(\tau) \subset U_{i_0}$ for a suitable $0<\tau \in F$. In view of the transfer principle, the inclusion $\mathscr{D}_{st(w)}(\tau) \subset U_{i_0}^{(\varepsilon)}$ is valid in the space F_m^n. Therefore, $w \in \mathscr{D}_{st(w)}(\tau) \subset U_{i_0}^{(\varepsilon)}$. Thus,

$$W \subset \bigcup_i U_i^{(\varepsilon)}.$$

Since set W is connected, one can infer that $W \subset U_{i_1}^{(\varepsilon)}$ for a certain i_1, taking into account properties (β), (γ) of sets $U_i^{(\varepsilon)}$. This implies according to the proved above that $st(W) \subset V_{i_1}$. The lemma is proved.

Consider polynomials

$$p_i \in F[\varepsilon_1, \ldots, \varepsilon_m][X_1, \ldots, X_n], \quad 1 \leqslant i \leqslant k.$$

Write p_i in the form

$$p_i = \sum_{j_1, \ldots, j_m} p_i^{(j_1, \ldots, j_m)} \varepsilon^{j_1} \ldots \varepsilon_m^{j_m},$$

where $p_i^{(j_1, \ldots, j_m)}$ are polynomials in $F[X_1, \ldots, X_n]$.

LEMMA 5.

(*a*) *Let $W \subset F^n$ be an element of the partition $\mathscr{U}(\{p_i^{(j_1, \ldots, j_m)}\}_{1 \leqslant i \leqslant k;\, j_1, \ldots, j_m})$ (see section 1), and let $C \subset W \cap \mathscr{D}_0(R)$ be a closed connected semialgebraic curve, where $R \in F$. Furthermore, let $C^{(\varepsilon)} \subset \mathscr{D}_0(R) \subset F_m^n$ be a closed connected semialgebraic curve such that $C^{(\varepsilon)} \supset st(C^{(\varepsilon)}) = C$ and such that for a suitable quantifier-free formula Π of Tarski algebra equalities $C=\{\Pi\} \subset F^n$, $C^{(\varepsilon)}=\{\Pi\} \subset F_m^n$ are fulfilled (cf. lemma (4a)). Then $C^{(\varepsilon)} \subset W^{(\varepsilon)}$ for some unique element $W^{(\varepsilon)} \subset F_m^n$ of the partition $\mathscr{U}(\{p_i\}_{1 \leqslant i \leqslant k})$.*

(*b*) *For any element W of the partition $\mathscr{U}(\{p_i^{(j_1, \ldots, j_m)}\}_{1 \leqslant i \leqslant k;\, j_1, \ldots, j_m})$ there is a unique element $W^{(\varepsilon)}$ of the partition $\mathscr{U}(\{p_i\}_{1 \leqslant i \leqslant k})$ such that $W \subset W^{(\varepsilon)} \cap F^n$.*

(*c*) *Let $g_1, \ldots, g_k$ be polynomials in $F[X_1, \ldots, X_n]$, and let $W_1 \subset F^n$ be a certain component of connectivity of the semialgebraic set $\{(g_1 \geqslant 0) \& \ldots \& (g_k \geqslant 0)\} \subset F^n$.*

Then there exists a unique element $W_1^{(\varepsilon)} \subset F_3^n$ of the partition

$$\mathscr{U}(\{g_1+\varepsilon_1, \ldots, g_k+\varepsilon_1, (g_1+\varepsilon_1) \ldots (g_k+\varepsilon_1)-\varepsilon_3\})$$

which contains $W_1 \subset W_1^{(\varepsilon)}$.

PROOF. (a) Taking into account that the curve $C^{(\varepsilon)}$ is connected, it is sufficient to show that $C^{(\varepsilon)}$ is situated entirely in some $(\{p_i\}_{1 \leqslant i \leqslant k})$-cell (see section 1).

Assume that the polynomial $p_i^{(j'_1, \ldots, j'_m)}$ vanishes on the set W for some $j'_1, \ldots, j'_m$. Since the curve $C = \{\Pi\} \subset W$, the following statement is correct: if a point $x \in F^n$ satisfies the formula Π, then $p_i^{(j'_1, \ldots, j'_m)}(x) = 0$. The transfer principle entails that the polynomial $p_i^{(j'_1, \ldots, j'_m)}$ vanishes also on the curve $C^{(\varepsilon)} = \{\Pi\} \subset F_m^n$.

We introduce a lexicographical order on multi-indices setting $(j'_1, \ldots, j'_m) \prec (j_1, \ldots, j_m)$ if $j'_m = j_m, \ldots, j'_l = j_l$ and $j'_{l-1} < j_{l-1}$ for a certain $1 < l \leqslant m+1$. Let us denote $\text{least}(\text{p}_i) = p_i^{(j_1, \ldots, j_m)}$ iff the sign $\operatorname{sgn}(p_i^{(j_1, \ldots, j_m)})$ is different from zero on the set W (otherwise, if there is no such multi-index $(j_1, \ldots, j_m)$, then we set $\text{least}(p_i) = 0$) and in addition the sign $(p_i^{(j'_1, \ldots, j'_m)})$ is equal to zero for each multi-index $(j'_1, \ldots, j'_m) \prec (j_1, \ldots, j_m)$. We recall that sign $\operatorname{sgn}(p_i^{(j''_1, \ldots, j''_m)})$ is constant on W for every multi-index $(j''_1, \ldots, j''_m)$. Note that polynomial $p_i^{(j'_1, \ldots, j'_m)}$ vanishes on the curve $C^{(\varepsilon)}$, provided that $(j'_1, \ldots, j'_m) \prec (j_1, \ldots, j_m)$ by virtue of the facts proved above.

For any point $c \in C^{(\varepsilon)}$ we claim the equality

$$\operatorname{sgn}(p_i(c)) = \operatorname{sgn}((\text{least}(p_i))(st(c))), \quad 1 \leqslant i \leqslant k.$$

In the case when $\text{least}(p_i) = 0$, both sides of the claimed equality are zeros according to the ascertained above. If $\text{least}(p_i) = p_i^{(j_1, \ldots, j_m)} \neq 0$, then $p_i^{(j_1, \ldots, j_m)}(st(c)) \neq 0$ since $st(c) \in C \subset W$. Therefore, taking into account the equalities

$$\begin{aligned} p_i(c) &= p_i^{(j_1, \ldots, j_m)}(c)\varepsilon_1^{j_1} \ldots \varepsilon_m^{j_m} + w_1 \varepsilon_1^{j_1} \ldots \varepsilon_m^{j_m} \\ &= p_i^{(j_1, \ldots, j_m)}(st(c))\varepsilon_1^{j_1} \ldots \varepsilon_m^{j_m} + w_2 \varepsilon_1^{j_1} \ldots \varepsilon_m^{j_m} \end{aligned}$$

for suitable infinitesimals $w_1, w_2 \in F_m$ (relatively to the field F), one can deduce the desired equality

$$\operatorname{sgn}(p_i(c)) = \operatorname{sgn}(p_i^{(j_1, \ldots, j_m)}(st(c))) \neq 0.$$

Finally, for an arbitrary pair of points $c_1, c_2 \in C^{(\varepsilon)}$, points $st(c_1), st(c_2) \in C \subset W$. So the definition of the partition $\mathscr{U}(\{p_i^{(j_1, \ldots, j_m)}\}_{1 \leqslant j \leqslant k; j_1, \ldots, j_m})$ implies

$$\operatorname{sgn}((\text{least}(p_i))(st(c_1))) = \operatorname{sgn}((\text{least}(p_i))(st(c_2)))$$

for all $1 \leqslant i \leqslant k$, therefore, $\operatorname{sgn}(p_i(c_1)) = \operatorname{sgn}(p_i(c_2))$; $1 \leqslant i \leqslant k$ in view of the fact claimed above. Thus, arbitrary points $c_1, c_2 \in C^{(\varepsilon)}$ belong to the same $(\{p_i\}_{1 \leqslant i \leqslant k})$-cell, which was to be shown.

(b) Suppose that there are points $x_1 \in W_1^{(\varepsilon)} \cap W$, $x_2 \in W_2^{(\varepsilon)} \cap W$ for two distinct elements $W_1^{(\varepsilon)} \neq W_2^{(\varepsilon)}$ of the partition $\mathscr{U}(\{p_i\}_{1 \leqslant i \leqslant k})$. According to lemma 3(b), there exists a closed connected semialgebraic curve $C \subset W \cap \mathscr{D}_0(R)$ for some $R \in F$ which contains points $x_1, x_2 \in C$. By virtue of lemma (4a) one can find a closed connected semialgebraic curve $C^{(\varepsilon)} \subset \mathscr{D}_0(R) \subset F_m^n$ such that $C^{(\varepsilon)} \supset st(C^{(\varepsilon)}) = C$ and, furthermore, $C = \{\Pi\} \subset F^n$, $C^{(\varepsilon)} = \{\Pi\} \subset F_m^n$ for a suitable quantifier-free formula Π of Tarski algebra. Then $C^{(\varepsilon)} \subset W^{(\varepsilon)}$ for some unique element $W^{(\varepsilon)}$ of the partition $\mathscr{U}(\{p_i\}_{1 \leqslant i \leqslant k})$ in view of part (a) of the present lemma, in particular $x_1, x_2 \in W^{(\varepsilon)}$, which contradicts the hypothesis.

(c) One can uniquely decompose $W_1 = \bigcup_j W_{1j}$, where W_{1j} is an element of the partition $\mathscr{U}(\{g_i\}_{1 \leqslant i \leqslant k})$ for every j. Taking into account the equality of the partitions

$$\mathscr{U}(\{g_i\}_{1 \leqslant i \leqslant k}) = \mathscr{U}(\{g_i\}_{1 \leqslant i \leqslant k} \cup \{\prod_{i \in I} g_i\}_{I \subset \{1,\ldots,k\}}),$$

one deduces from part (b) of the present lemma that for each W_{1j} there is a unique element $W_{1j}^{(\varepsilon)} \subset F_3^n$ of the partition

$$\mathscr{U}(g_1+\varepsilon_1, \ldots, g_k+\varepsilon_1, (g_1+\varepsilon_1) \ldots (g_k+\varepsilon_1)-\varepsilon_3),$$

which contains $W_{1j} \subset W_{1j}^{(\varepsilon)}$.

Suppose that for some indices $j_1 \neq j_2$, elements $W_{1j}^{(\varepsilon)} \neq W_{1j_2}^{(\varepsilon)}$ are distinct. Let us pick out points $x_1 \in W_{1j_1}, x_2 \in W_{1j_2}$. According to lemma (3b), one can find a closed connected semialgebraic curve $C \subset W_1 \cap \mathscr{D}_0(R)$ for a suitable $R \in F$ such that $x_1, x_2 \in C$. By virtue of lemma (4a) there exists a quantifier-free formula Π of Tarski algebra which satisfies the following conditions: $C = \{\Pi\} \subset F^n$, the closed connected semialgebraic curve $C^{(\varepsilon)} = \{\Pi\} \subset \mathscr{D}_0(R) \subset F_3^n$ and $C^{(\varepsilon)} \supset st(C^{(\varepsilon)}) = C$. For any point $c \in C \subset W_1$, the inequalities $g_i(c) \geqslant 0$, $1 \leqslant i \leqslant k$ are valid. So for every point $c^{(\varepsilon)} \in C^{(\varepsilon)}$, the inequalities $g_i(c^{(\varepsilon)}) \geqslant 0$, $1 \leqslant i \leqslant k$ are also correct in view of the transfer principle, therefore $g_i(c^{(\varepsilon)})+\varepsilon_1 > 0$, $1 \leqslant i \leqslant k$ and

$$(g_1(c^{(\varepsilon)})+\varepsilon_1) \ldots (g_k(c^{(\varepsilon)})+\varepsilon_1)-\varepsilon_3 \geqslant \varepsilon_1^k-\varepsilon_3 > 0.$$

Since the curve $C^{(\varepsilon)}$ is connected, the inclusion $C^{(\varepsilon)} \subset W_1^{(\varepsilon)}$ is fulfilled for an appropriate element $W_1^{(\varepsilon)} \subset F_3^n$ of the partition $\mathscr{U}(g_1+\varepsilon_1, \ldots, g_k+\varepsilon_1, (g_1+\varepsilon_1) \ldots (g_k+\varepsilon_1)-\varepsilon_3)$, in particular, $x_1, x_2 \in W_1^{(\varepsilon)}$. We have obtained a contradiction which completes the proof of the lemma.

3. Projections of a Semialgebraic Set

Let a formula of Tarski algebra be given by

$$\exists X_1 \ldots \exists X_{s-1}((f_1 > 0) \& \ldots \& (f_m > 0) \& (f_{m+1} \geqslant 0) \& \ldots \& (f_{k-1} \geqslant 0)), \qquad (2)$$

where $f_1, \ldots, f_{k-1} \in \mathbb{Q}[Z_1, \ldots, Z_n, X_1, \ldots, X_{s-1}]$ are polynomials with $\deg(f_i) < d$, $l(f_i) \leqslant M$, $1 \leqslant i \leqslant k-1$. We add a new variable X_s, let $f_k = X_s f_1 \ldots f_m - 1$, and consider the formula

$$\exists X_1 \ldots \exists X_{s-1} \exists X_s((f_1 \geqslant 0) \& \ldots \& (f_{k-1} \geqslant 0) \& (f_k \geqslant 0)) \qquad (3)$$

equivalent to formula (2). We introduce one more variable Z_0, denote

$$f_0 = Z_0 - X_1^2 - \ldots - X_s^2$$

and consider the formula

$$\exists Z_0 \exists X_1 \ldots \exists X_{s-1} \exists X_s((f_0 \geqslant 0) \& (f_1 \geqslant 0) \& \ldots \& (f_{k-1} \geqslant 0) \& (f_k \geqslant 0)), \qquad (4)$$

which is equivalent to formulas (2) and (3).

In the present section we describe an algorithm which constructs (see lemma 10 below) a formula of the first-order theory of a certain real closed field F_3. The formula is of the form $\exists T(P_1)$, where P_1 is a quantifier-free formula with the coefficients in the field F_3, and is such that $\exists T(P_1)$ is equivalent (over the field $\tilde{\mathbb{Q}}$) to the formula

$$\exists X_1 \ldots \exists X_{s-1} \exists X_s((f_0 \geqslant 0) \& (f_1 \geqslant 0) \& \ldots \& (f_{k-1} \geqslant 0) \& (f_k \geqslant 0)), \qquad (5)$$

i.e. both formulas determine the same (semialgebraic) set in the space $\tilde{\mathbb{Q}}^{n+1}$; in other words a point $(z_0, z_1, \ldots, z_n) \in \tilde{\mathbb{Q}}^{n+1}$ satisfies (5) iff it satisfies the formula $\exists T(P_1)$. So, the algorithm reduces a projection along many variables (see formula (2)) to a projection along two variables Z_0, T, taking into account that formula (2) (and (4)) is equivalent to the formula $\exists\, Z_0 \in \tilde{\mathbb{Q}}\ \exists\, T \in F_3(P_1)$ (being not a formula of the first-order theory!)

We begin with the construction of the formula $\exists\, T(P_1)$. Let the element $\varepsilon_1 > 0$ be infinitesimal relatively to the field $\mathbb{Q}$, let the element $\varepsilon_2 > 0$ be infinitesimal relatively to $\mathbb{Q}(\varepsilon_1)$ and let the element $\varepsilon_3 > 0$ be infinitesimal relatively to $\mathbb{Q}(\varepsilon_1, \varepsilon_2)$. We denote $F_1 = \widetilde{\mathbb{Q}(\varepsilon_1)}$, $F_2 = \widetilde{\mathbb{Q}(\varepsilon_1, \varepsilon_2)}$, $F_3 = \widetilde{\mathbb{Q}(\varepsilon_1, \varepsilon_2, \varepsilon_3)}$ (see section 2). Consider the polynomial

$$g = (f_0+\varepsilon_1)(f_1+\varepsilon_1)\ldots(f_k+\varepsilon_1)-\varepsilon_3 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, Z_1, \ldots, Z_n, X_1, \ldots, X_s]$$

and the formula

$$\exists\, X_1 \ldots \exists\, X_s((g = 0)\&(f_0+\varepsilon_1 > 0)\& \ldots \&(f_k+\varepsilon_1 > 0)). \tag{6}$$

Consider points $z = (z_0, z_1, \ldots, z_n) \in \tilde{\mathbb{Q}}^{n+1}$ and $0 \neq v \in \tilde{\mathbb{Q}}^{n+1}$, and let $\tilde{z} = z+\varepsilon_2 v \in F_2^{n+1}$. We denote the semialgebraic sets

$$V = \{(f_0 \geqslant 0)\& \ldots \&(f_k \geqslant 0)\} \subset \tilde{\mathbb{Q}}^{s+n+1},$$
$$V^{(\varepsilon)} = \{(f_0+\varepsilon_1 > 0)\& \ldots \&(f_k+\varepsilon_1 > 0)\} \subset F_3^{s+n+1}.$$

LEMMA 6.

(*a*) *For an arbitrary* $0 < R \in \tilde{\mathbb{Q}}$, *the following three sets coincide:*

$$V \cap \mathscr{D}_0(R) = st(V^{(\varepsilon)} \cap \mathscr{D}_0(R))$$
$$= st(V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathscr{D}_0(R)) \subset (V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathscr{D}_0(R)) \subset F_3^{s+n+1};$$

(*b*) *The sign* $\operatorname{sgn}(f_i+\varepsilon_1)$ *is constant on any component of connectivity of the semialgebraic set* $\{g \geqslant 0\} \subset F_3^{s+n+1}$ *for each* $0 \leqslant i \leqslant k$;

(*c*) *Formula* (5) *is true at point* z *iff formula* (6) *is valid at point* $\tilde{z}$. *Moreover, if formula* (5) *is true at point* z *and some point* $(z, x) \in \tilde{\mathbb{Q}}^{s+n+1}$ *belongs to a certain component of connectivity* V_1 *of the set* V, *and by the same token* (*cf. part* (*a*) *of the present lemma*) *the point* (z, x) *belongs to a corresponding component of connectivity* $V_1^{(\varepsilon)}$ *of the set* $\{g \geqslant 0\}$, *then there exists a point* $(\tilde{z}, \tilde{x}) \in V_1^{(\varepsilon)}$ *such that* $g(\tilde{z}, \tilde{x}) = 0$ *and such that point* $(z, st(\tilde{x})) = st(\tilde{z}, \tilde{x}) \in \tilde{\mathbb{Q}}^{s+n+1}$ *is defined.*

PROOF. (a) (see also lemma 2 from Grigor'ev & Vorobjov, 1987). Let a point $u \in V^{(\varepsilon)} \cap \mathscr{D}_0(R)$, then $\|st(u)\| \leqslant R$ and $f_i(st(u)) \geqslant 0$ for every $0 \leqslant i \leqslant k$; this entails the inclusion $st(V^{(\varepsilon)} \cap \mathscr{D}_0(R)) \subset V \cap \mathscr{D}_0(R)$. Now consider a point $w \in V \cap \mathscr{D}_0(R)$, then $f_i(w)+\varepsilon_1 \geqslant \varepsilon_1 > 0$, $0 \leqslant i \leqslant k$ and $g(w) \geqslant \varepsilon_1^{k+1}-\varepsilon_3 > 0$, henceforth,

$$(V \cap \mathscr{D}_0(R)) \subset st(V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathscr{D}_0(R)) \cap (V^{(\varepsilon)} \cap \{g \geqslant 0\} \cap \mathscr{D}_0(R)).$$

(b) (see also lemma 2 from Grigor'ev & Vorobjov, 1987). Let $W_1 \subset \{g \geqslant 0\}$ be a component of connectivity of the semialgebraic set $\{g \geqslant 0\}$. If the sign $\operatorname{sgn}(f_i+\varepsilon_1)$ is not constant on W_1, then there exists a point $u \in W_1$ such that $f_i(u)+\varepsilon_1 = 0$. The inequality $g(u) = -\varepsilon_3 < 0$ leads to contradiction.

(c) Assume that formula (6) is valid at point $\tilde{z}$, then there exists a point $(\tilde{z}, \tilde{x}) \in V^{(\varepsilon)} \cap \{g = 0\}$. Since $f_0(\tilde{z}, \tilde{x})+\varepsilon_1 > 0$, i.e. $\|\tilde{x}\|^2 < z_0+2\varepsilon_1$, one concludes that the point $st(\tilde{x})$ is defined and $(z, st(\tilde{x})) \in V$ is fulfilled according to part (a) of this lemma, i.e. formula (5) is true at point z.

Conversely, suppose that formula (5) is valid at point z, then some point $(z, x) \in V$ belongs to an appropriate component of connectivity V_1 of the set V, whence $(z, x) \in V_1^{(\varepsilon)}$

for a suitable component of connectivity $V_1^{(\varepsilon)}$ of the set $V^{(\varepsilon)} \cap \{g \geqslant 0\}$ (see item (a) of this lemma). Note that $V_1 \subset V_1^{(\varepsilon)}$ by virtue of lemma 5(c). Since $f_i(z, x)+\varepsilon_1 \geqslant \varepsilon_1$, $0 \leqslant i \leqslant k$ and $g(z, x) \geqslant \varepsilon_1^{k+1}-\varepsilon_3$, there exists such a natural number q that for any point $(z', x') \in \mathscr{D}_{(z,x)}(\varepsilon_1^q)$ the inequalities $f_i(z', x')+\varepsilon_1 \geqslant \varepsilon_1/2$, $0 \leqslant i \leqslant k$ are correct; so $g(z', x') \geqslant (\varepsilon_1/2)^{k+1}-\varepsilon_3 > 0$, i.e. $\mathscr{D}_{(z,x)}(\varepsilon_1^q) \subset V_1^{(\varepsilon)}$. Obviously, $(\tilde{z}, x) \in \mathscr{D}_{(z,x)}(\varepsilon_1^q)$.

On the s-dimensional plane $\mathscr{L} = \{(\tilde{z}, x') \colon x' \in F_3^s\} \subset F_3^{s+n+1}$ we consider an arbitrary ray $\gamma \subset \mathscr{L}$ with endpoint $(\tilde{z}, x)$ and with a rational directing vector. The intersection $K_1 = \gamma \cap \{g < 0\}$ is not empty. Indeed, otherwise $\gamma \subset V_1^{(\varepsilon)}$ in view of part (b) of the present lemma; so for any point $(\tilde{z}, x') \in \gamma$ the inequality $\|x'\|^2 < z_0+2\varepsilon_1$ is fulfilled, which leads to a contradiction. The set K_1 is semialgebraic and, henceforth, K_1 is the union of a finite number of intervals. We denote by $(\tilde{z}, \tilde{x}) \in \gamma$ one of the endpoints of these intervals which is the nearest to the point $(\tilde{z}, x)$. Then $g(\tilde{z}, \tilde{x}) = 0$ since in an arbitrary neighbourhood (on the ray γ) of the point $(\tilde{z}, \tilde{x})$ there is a point in which the polynomial g has a negative value as well as a point in which g has a positive value.

The closed interval $J \subset \gamma$ with endpoints $(\tilde{z}, x)$ and $(\tilde{z}, \tilde{x})$ is contained in $V_1^{(\varepsilon)}$, according to part (b) of the present lemma, in particular $(\tilde{z}, \tilde{x}) \in V_1^{(\varepsilon)}$, this entails $\|\tilde{x}\|^2 < z_0+2\varepsilon_1$ and that the formula (6) is true at point $\tilde{z}$. It remains to show that $st(\tilde{z}, \tilde{x}) \in V_1$. The set $st(J) \subset \tilde{\mathbb{Q}}^{s+n+1}$ is well defined and coincides with the closed interval with endpoints (z, x) and $(z, st(\tilde{x}))$. Indeed, let $(u_1, \ldots, u_s) \in \mathbb{Q}^s$ be the directing vector of the ray γ. Then $\tilde{x} = x+\alpha(u_1, \ldots, u_s)$ for a certain $0 < \alpha \in F_3$ being $\mathbb{Q}$-finite by the facts proved above. For any $0 \leqslant \beta \leqslant \alpha$, $\beta \in F_3$, the equality

$$st(x+\beta(u_1, \ldots, u_s)) = x+st(\beta)(u_1, \ldots, u_s)$$

is correct. This implies that $st(J)$ is a closed interval. Finally, $st(J) \subset V$ by virtue of part (a) of the present lemma, henceforth, $st(J) \subset V_1$, which completes the proof of the lemma.

Now we return to the description of the algorithm. It involves the following construction from Grigor'ev & Vorobjov (1987) (see also Vorobjov & Grigor'ev, 1985). We denote by $\Gamma \subset \mathbb{Z}^{s-1}$ the family consisting of vectors of the kind $\gamma = (\gamma_2, \ldots, \gamma_s) \in \Gamma$, where γ_i, $2 \leqslant i \leqslant s$ run independently over all integers from 1 up to $N_2 = (2(k+1)d)^s$. For a point $z^{(2)} \in F_2^{n+1}$ we denote by $g(z^{(2)})$ the polynomial

$$g(z^{(2)}, X_1, \ldots, X_s) \in F_2[\varepsilon_3][X_1, \ldots, X_s].$$

The following lemma can be inferred from lemmas 4, 5 in Grigor'ev & Vorobjov (1987) (see there the corollary after lemma 5; cf. also Vorobjov & Grigor'ev, 1985).

Lemma 7. *Let a point* $z^{(2)} \in F_2^{n+1}$.

(*a*) *For each component of connectivity* V_2 *of the variety* $\{g(z^{(2)}) = 0\} \subset F_3^s$, *provided that* V_2 *is situated in a certain ball, and for every vector* $\gamma = (\gamma_2, \ldots, \gamma_s) \in \Gamma$ *the system of equations*

$$g(z^{(2)}) = \left(\frac{\partial g(z^{(2)})}{\partial X_2}\right)^2 - \frac{\gamma_2}{N_2 s} \sum_{1 \leqslant i \leqslant s} \left(\frac{\partial g(z^{(2)})}{\partial X_i}\right)^2 = \cdots$$
$$= \left(\frac{\partial g(z^{(2)})}{\partial X_s}\right)^2 - \frac{\gamma_s}{N_2 s} \sum_{1 \leqslant i \leqslant s} \left(\frac{\partial g(z^{(2)})}{\partial X_i}\right)^2 = 0 \qquad (7)$$

has a root in V_2.

(*b*) *There exists a vector* $\gamma = (\gamma_2, \ldots, \gamma_s) \in \Gamma$ *such that any solution of system* (7), *which belongs to the space* F_3^s, *is an isolated point of the algebraic variety consisting of all solutions of system* (7) *in the space* $\bar{F}_3^s$.

We recall that $\bar{F}_3 = F_3[\sqrt{-1}]$ is the algebraic closure of F_3. Lemma 7(b) entails, in particular, that for a relevant $\gamma \in \Gamma$, system (7) has only finite number of solutions in the space $\bar{F}_3^s$.

In order to verify formula (6) in a certain point $z^{(2)}$, it is sufficient to test, whether there exists a component of connectivity V_3 of the variety $\{g(z^{(2)})=0\} \subset F_3^s$ and a point $x \in V_3$ from some representative set for the variety $\{g(z^{(2)})=0\}$ (considered below) such that the inequalities $f_i(z^{(2)})(x)+\varepsilon_1 > 0, \quad 0 \leqslant i \leqslant k$ hold, taking into account that signs $\operatorname{sgn}(f_i(z^{(2)})+\varepsilon_1), \quad 0 \leqslant i \leqslant k$ are constant on V_3 according to lemma 6(b). As a representative set of the points x, the algorithm will take solutions of system (7) in the space F_3^s, this family of points x suffices in view of lemma 7(a) and the observation that if $\operatorname{sgn}(f_0(z^{(2)})(x^{(1)})+\varepsilon_1) > 0$ for points $x^{(1)} \in V_3$ belonging to some component of connectivity V_3 of the variety $\{g(z^{(2)})=0\} \subset F_3^s$, then $V_3 \subset \mathscr{D}_0((z_0+2\varepsilon_1)^{1/2})$.

Let us fix for the time being a vector $\gamma \in \Gamma$ and denote $h_1 = g$,

$$h_j = \left(\frac{\partial g}{\partial X_j}\right)^2 - \frac{\gamma_j}{N_2 s} \sum_{1 \leqslant i \leqslant s} \left(\frac{\partial g}{\partial X_i}\right)^2 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, X_1, \ldots, X_s]; \; 2 \leqslant j \leqslant s.$$

We introduce a new variable X_0 and polynomials

$$\bar{h}_j = X_0^{\deg_{X_1,\ldots,X_s}(h_j)} h_j(Z_0, \ldots, Z_n, X_1/X_0, \ldots, X_s/X_0), \quad 1 \leqslant j \leqslant s$$

homogeneous with respect to variables $X_0, X_1, \ldots, X_s$. Consider a certain point $z^{(3)} \in \bar{F}_3^{n+1}$, one more new variable Y and the following system of equations homogeneous with respect to variables $X_0, \ldots, X_s$ (cf. section 5 in Chistov & Grigor'ev, 1983*b*; Chistov & Grigor'ev, 1984):

$$\bar{h}_j(z^{(3)}) - Y X_j^{\deg_{X_0,\ldots,X_s}(\bar{h}_j)} = 0; \quad 1 \leqslant j \leqslant s \tag{8}$$

over a field $\bar{F}_3(Y)$.

Besides, consider a system of equations

$$\bar{h}_j - Y X_j^{\deg_{X_0,\ldots,X_s}(\bar{h}_j)} = 0; \quad 1 \leqslant j \leqslant s \tag{8'}$$

in the variables $X_0, \ldots, X_s$ over a field $\mathbb{Q}(\varepsilon_1, \varepsilon_3)(Y, Z_0, \ldots, Z_n)$. Further, we need some similar statements about both systems (8) and (8′). Thus, we consider an arbitrary field F (of zero characteristic), a vector $\mathscr{Z} \in F^{n+1}$ and a system

$$\bar{h}_j(\mathscr{Z}) - Y X_j^{\deg_{X_0,\ldots,X_s}(\bar{h}_j)} = 0; \quad 1 \leqslant j \leqslant s. \tag{8''}$$

Define the field $H_1 = F(Y)$. Later we consider two cases: $F = \bar{F}_3$ and $\mathscr{Z} = z^{(3)}$ or $F = \mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n)$ and $\mathscr{Z} = (Z_0, \ldots, Z_n)$.

Proposition 3. *System* (8′) *has a finite nonzero number of solutions in the projective space* $\mathbb{P}^s(\bar{H}_1)$ (*see section* 5 *in Chistov & Grigor'ev*, 1983*b and also Chistov & Grigor'ev*, 1984).

Proof. We define $T_1 = 1/Y$, then $H_1 = F(Y_1)$ and system (8″) is equivalent to a system

$$Y_1 \bar{h}_j(\mathscr{Z}) - X_j^{\deg_{X_0,\ldots,X_s}(\bar{h}_j)} = 0; \quad 1 \leqslant j \leqslant s$$

(i.e. the varieties of solutions of the latter system and system (8″) in the space $\mathbb{P}^s(\bar{H}_1)$ coincide). The latter system has a finite nonzero number of solutions iff its u-resultant $\mathscr{R}(Y_1) \in F[u_0, \ldots, u_s][Y_1]$ does not vanish identically. On the other hand, $\mathscr{R}(0) \neq 0$, taking into account that $\mathscr{R}(0)$ equals to the u-resultant of the system $X_j^{\deg_{X_0,\ldots,X_s}(\bar{h}_j)} = 0$; $1 \leqslant j \leqslant s$ having a finite number of solutions in $\mathbb{P}^s(\bar{F})$. This completes the proof of the proposition.

Consider now system (8″) in the variables $X_0, \ldots, X_s$, Y over the field F and the variety of its solutions $U_F \subset \bar{F}^{s+2}$.

Proposition 4. *The irreducible (over F) components $\mathscr{V}_t \subset \bar{F}^{s+2}$ of the variety U_F that are not situated in any union of a finite number of hyperplanes of the kind $\{Y = \beta\}$, where $\beta \in \bar{F}$, correspond bijectively to the classes of solutions conjugate over the field H_1 in the space $\mathbb{P}^s(\bar{H}_1)$ of the system (8″). Under this correspondence, if $J \subset F[Y, X_0, \ldots, X_s]$ is an ideal of a component $\mathscr{V}_t$, then $H_1 \otimes_F J \subset H_1[X_0, \ldots, X_s]$ is an ideal of the corresponding conjugate class. Furthermore, $\dim \mathscr{V}_t = 2$ for each t (see section 5 in Chistov & Grigor'ev, 1983b and also Chistov & Grigor'ev, 1984).*

Proof. Indeed, denote by J_{H_1} (resp. J_F) the ideal, generated by the polynomials $\bar{h}_j(\mathscr{X}) - YX_j^{\deg_{X_0, \ldots, X_s}(\bar{h}_j)}$ for $1 \leqslant j \leqslant s$ in the H_1-algebra $\Lambda_{H_1} = H_1[X_0, \ldots, X_s]$ (resp. in F-algebra $\Lambda_F = F[Y, X_0, \ldots, X_s]$). Then

$$\Lambda_{H_1} = H_1 \otimes_F \Lambda_F = (F[Y] \backslash \{0\})^{-1} \Lambda_F.$$

Therefore, there is a bijective correspondence preserving the inclusion relation between prime ideals $\mathscr{I}_{H_1}^{(i)} \subset \Lambda_{H_1}$, and on the other hand, prime ideals $\mathscr{I}_F^{(i)} \subset \Lambda_F$ such that $\mathscr{I}_F^{(i)} \cap F[Y] = \{0\}$; besides, under this correspondence $\mathscr{I}_{H_1}^{(i)} = H_1 \otimes_F \mathscr{I}_F^{(i)}$ (see Lang, 1965). Apart from that, to every prime ideal $\mathscr{I}_F^{(i)}$ such that $\mathscr{I}_F^{(i)} \cap F[Y] = \{0\}$ corresponds a variety $\mathscr{V}_{\mathscr{I}_F^{(i)}} \subset \bar{F}^{s+2}$ irreducible over F, which is not situated in any union of a finite number of hyperplanes of the kind $\{Y = \beta\}$ for $\beta \in F$ (and conversely). Denote by $\mathscr{V}_{\mathscr{I}_{H_1}^{(i)}} \subset \mathbb{P}^s(\bar{H}_1)$ a variety irreducible over H_1 corresponding to a homogeneous prime ideal $\mathscr{I}_{H_1}^{(i)}$, provided that $\mathscr{I}_{H_1}^{(i)} \neq (X_0, \ldots, X_s)$. Let $\mathscr{I}_{H_1}^{(i)} \supset J_{H_1}$ (resp. $\mathscr{I}_F^{(i)} \supset J_F$) be a certain prime ideal homogeneous (resp. homogeneous relatively to $X_0, \ldots, X_s$) and minimal among prime ideals containing J_{H_1} (resp. J_F). In other words, the factor ideal $\mathscr{I}_{H_1}^{(i)}/J_{H_1}$ (resp. $\mathscr{I}_F^{(i)}/J_F$) is a minimal prime ideal in the factorring Λ_{H_1}/J_{H_1} (resp. Λ_F/J_F). Hence, $\mathscr{V}_{\mathscr{I}_{H_1}^{(i)}}$ (resp. $\mathscr{V}_{\mathscr{I}_F^{(i)}}$) is an irreducible (over H_1, resp. F) component of the variety of roots of system (8″) in the space $\mathbb{P}^s(\bar{H}_1)$ (resp. $\bar{F}^{s+2}$), taking into account that $\mathscr{I}_{H_1}^{(i)} \neq (X_0, \ldots, X_s)$ since system (8″) has at least one root in the space $\mathbb{P}^s(\bar{H}_1)$ by proposition 3. This entails the correspondence claimed in proposition 4 between components $\mathscr{V}_t$ and, on the other hand, classes of solutions of system (8″) conjugate over H_1. Finally, for each $\mathscr{V}_t$ there is a suitable prime ideal $\mathscr{I}_F^{(i)}$ such that $\mathscr{V}_t = \mathscr{V}_{\mathscr{I}_F^{(i)}}$, therefore

$$\begin{aligned} \dim \mathscr{V}_t &= \deg tr_F(\Lambda_F/\mathscr{I}_F^{(i)}) = \deg tr_F((H_1 \otimes_F \Lambda_F)/(H_1 \otimes_F \mathscr{I}_F^{(i)})) \\ &= \deg tr_F(\Lambda_{H_1}/\mathscr{I}_{H_1}^{(i)}) = \deg tr_{H_1}(\Lambda_{H_1}/\mathscr{I}_{H_1}^{(i)}) + 1 = \dim \mathscr{V}_{\mathscr{I}_{H_1}^{(i)}} + 2 = 2 \end{aligned}$$

(the latter equality follows from proposition 3). The proposition is proved.

Proposition 5. *The variety*

$$\left(\bigcup_t \mathscr{V}_t\right) \cap \{Y = 0\} \subset \bar{F}^{s+1}$$

considered as a subvariety of the space $\bar{F}^{s+1}$ with coordinates $X_0, \ldots, X_s$ is a union of a finite number of lines passing through the origin of coordinates. Besides, for every isolated solution $(x_1, \ldots, x_s) \in \bar{F}^s$ of system $h_1(\mathscr{X}) = \ldots = h_s(\mathscr{X}) = 0$ (obtained from system (7) by replacing the point $z^{(2)}$ by the point $\mathscr{X}$) its cone (which is a line) $\{(\lambda, \lambda x_1, \ldots, \lambda x_s)_{\lambda \in \bar{F}}\} \subset \bar{F}^{s+1}$ is a component of the variety

$$\left(\bigcup_t \mathscr{V}_t\right) \cap \{Y = 0\}$$

irreducible over the field $\bar{F}$.

Proof. For each t, by virtue of proposition 4, $\dim \mathscr{V}_t = 2$. Apart from that, $\mathscr{V}_t \cap \{Y=0\} \subsetneqq \mathscr{V}_t$. Therefore, $\dim(\mathscr{V}_t \cap \{Y=0\}) = 1$ according to the theorem on the dimension of intersection (see Shafarevich, 1974). Furthermore, the variety $\mathscr{V}_t \cap \{Y=0\}$ is homogeneous since $\mathscr{V}_t$ is a component of the variety, consisting of solutions of system (8″), which is homogeneous relatively to the coordinates $X_0, \ldots, X_s$. Thus, $\mathscr{V}_t \cap \{Y=0\}$ is a union of a finite number of lines passing through the origin of coordinates.

Taking into account that con $= \{(\lambda, \lambda x_1, \ldots, \lambda x_s)_{\lambda \in \bar{F}}\} \subset U_F \cap \{Y=0\}$, one can infer that there exists a certain irreducible component $\mathscr{V} \subset U_F$ of the variety U_F which contains con $\subset \mathscr{V}$. If $\mathscr{V} = \mathscr{V}_t$ for some t, then con is a line being a component of $\mathscr{V}_t \cap \{Y=0\}$ and the required statement of the proposition is valid. Otherwise, $\mathscr{V}$ is situated in a union of a finite number of hyperplanes of the kind $\{Y=\beta\}$, therefore, $\mathscr{V} \subset \{Y=0\}$ because of the irreducibility of $\mathscr{V}$. Denote by $\mathscr{W} \subset \mathbb{P}^s(\bar{F})$ a projective irreducible variety such that the cone con$(\mathscr{W}) = \mathscr{V}$. According to theorem on the dimension of intersections (see Shafarevich, 1974), $\dim \mathscr{V} \geqslant 2$, hence $\dim \mathscr{W} \geqslant 1$. On the other hand, the point $(1 : x_1 : \ldots : x_s) \in \mathscr{W}$ is an isolated solution of a system $\bar{h}_1(\mathscr{X}) = \ldots = \bar{h}_s(\mathscr{X}) = 0$. This leads to a contradiction with the fact that $\mathscr{W}$ also satisfies the latter system. The proposition is proved.

In the sequel we shall make use of the following construction from Lazard (1981). Let $g_0, \ldots, g_{k-1} \in F[X_0, \ldots, X_s]$ be homogeneous polynomials of degrees $\delta_0 \geqslant \delta_1 \geqslant \ldots \geqslant \delta_{k-1}$, respectively. Introduce new variables $u_0, \ldots, u_s$ algebraically independent over a field $F(X_0, \ldots, X_s)$. Consider a polynomial $g_k = X_0 u_0 + \ldots + X_s u_s$ and set

$$D = \sum_{0 \leqslant i \leqslant s} \delta_i - s,$$

where $\delta_k = \ldots = \delta_s = 1$ if $k \leqslant s$. Denote by $\mathscr{B}_i$ (resp. $\mathscr{B}$) a space of homogeneous polynomials in the variables $X_0, \ldots, X_s$ of degree $D - \delta_i$ (resp. D) over the field $F(u_0, \ldots, u_s)$. Consider a linear mapping $\mathscr{A} : \mathscr{B}_0 \oplus \ldots \oplus \mathscr{B}_k \to \mathscr{B}$ over the field $F(u_0, \ldots, u_s)$ given by the formula

$$\mathscr{A}(b_0, \ldots, b_k) = \sum_{0 \leqslant i \leqslant k} g_i b_i.$$

Denote by

$$\rho_i = \binom{n+D-\delta_i}{n}, \quad \tau = \binom{n+D}{n}$$

binomial coefficients. One can write an arbitrary element $b = (b_0, \ldots, b_k) \in \mathscr{B}_0 \oplus \ldots \oplus \mathscr{B}_k$ in the form

$$b = (b_{0,1}, \ldots, b_{0,\rho_0}, b_{1,1}, \ldots, b_{1,\rho_1}, \ldots, b_{k,1}, \ldots, b_{k,\rho_k}),$$

where $b_{i,1}, \ldots, b_{i,\rho_i}$ are the coefficients of the polynomial b_i, provided that some numeration of monomials of degree $D - \delta_i$ is fixed. Similarly, one can write elements from the space $\mathscr{B}$. In a chosen coordinate system the mapping $\mathscr{A}$ has a matrix A of size $\tau \times (\sum_{0 \leqslant i \leqslant k} \rho_i)$. The matrix A can be uniquely represented in a form $A = (A^{(n)}, A^{(f)})$, where $A^{(n)}$ (we call it the number part of A) contains $\sum_{0 \leqslant i \leqslant k-1} \rho_i$ columns and $A^{(f)}$ (we call it the formal part of A) contains ρ_k columns; furthermore, the entries of $A^{(n)}$ belong to the field F, the entries of $A^{(f)}$ are linear forms in variables $u_0, \ldots, u_s$ over F.

The next proposition is a certain effective version of Hilbert's Nullstellensatz.

PROPOSITION 6. (Lazard, 1981). *A system* $g_0 = \ldots = g_{k-1} = 0$ *has no roots in* $\mathbb{P}^s(\bar{F})$ *iff the ideal* $(g_0, \ldots, g_{k-1}) \supset (X_0, \ldots, X_s)^D$.

The proof of the next proposition is based on the latter one.

PROPOSITION 7 (Lazard, 1981).

(*a*) *A system* $g_0 = \ldots = g_{k-1} = 0$ *has a finite number of roots in* $\mathbb{P}^s(\bar{F})$ *iff rank* rank $(A) = \tau$*; in parts* (*b*), (*c*), (*d*) *we suppose that rank* rank $(A) = \tau$.

(*b*) *All* $\tau \times \tau$ *minors* (*by a minor we mean the determinant of a submatrix*) *of matrix A generate a principal ideal whose generator* $R \in F[u_0, \ldots, u_s]$ *is their greatest common divisor.*

(*c*) *a form R homogeneous relatively to the variables* $u_0, \ldots, u_s$ *is a product*

$$R = \prod_{1 \leqslant i \leqslant D_2} L_i^{e_i}$$

of linear forms

$$L_i = \sum_{0 \leqslant j \leqslant s} \xi_j^{(i)} u_j, \quad 1 \leqslant i \leqslant D_2$$

with coefficients from $\bar{F}$, *furthermore,* $(\xi_0^{(i)} : \ldots : \xi_s^{(i)}) \in \mathbb{P}^s(\bar{F})$ *is a root of the system* $g_0 = \ldots = g_{k-1} = 0$ *with the multiplicity* e_i.

(*d*) *Let* Δ *be a nonsingular* $\tau \times \tau$ *submatrix of A containing* rank $(A^{(n)})$ *columns in the number part* $A^{(n)}$ (*obviously, such a submatrix exists*). *Then the determinant* $\det \Delta$ *equals to R up to a factor from* F^*, *besides,*

$$\deg R = D_1 = \sum_{1 \leqslant i \leqslant D_2} e_i = \tau - \operatorname{rank}(A^{(n)}).$$

We shall apply later this proposition in the case when $k = n$. In this case, R coincides with the classical u-resultant of the system of the polynomials $g_0, \ldots, g_{n-1}$. We shall make use of the suggested explicit form of R.

The algorithm constructs a matrix A with entries in the ring

$$\mathbb{Q}[\varepsilon_1, \varepsilon_3][Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s]$$

corresponding to system (8′) considered in the variables $X_0, \ldots, X_s$. Denote by $A_{(z^{(3)})}$ (resp. $A_{\mathscr{X}}$) a matrix corresponding to system (8) (resp. (8″)) and obtained from matrix A by substituting the coordinates of the vector $z^{(3)}$ (resp. $\mathscr{X}$) instead of the variables $Z_0, \ldots, Z_n$. Denote by

$$R \in \mathbb{Q}[\varepsilon_1, \varepsilon_3, Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s] \text{ (resp. } R_{(z^{(3)})} \in \bar{F}_3[Y, u_0, \ldots, u_s],$$

resp. $R_{\mathscr{X}} \in F[Y, u_0, \ldots, u_s]$) the u-resultant of system (8′) (resp. (8), resp. (8″)) (see proposition 7(b)). u-Resultants do not vanish because of proposition 3. One can assume w.l.o.g. that $Y \nmid R$, $Y \nmid R_{(z^{(3)})}$, $Y \nmid R_{\mathscr{X}}$, otherwise one divides the respective polynomial by the highest possible power of the variable Y.

Consider arbitrary polynomials $\Xi_0, \ldots, \Xi_\mu \in F[Y, X_0, \ldots, X_s]$ homogeneous in the variables $X_0, \ldots, X_s$ such that the variety $\bigcup_t \mathscr{V}_t$ (see proposition 4) coincides with the variety of all roots in the space $\bar{F}^{s+2}$ of the system $\Xi_0 = \ldots = \Xi_\mu = 0$. By virtue of proposition 4, the variety of all roots of the latter system over the field $\bar{H}_1$ coincides with the variety $U_{H_1} \subset \mathbb{P}^s(\bar{H}_1)$ of all roots of system (8″). Owing to proposition 3, U_{H_1} has a finite number of points; denote by $\hat{A}_{\mathscr{X}}$ a matrix with τ_1 rows corresponding to the system $\Xi_0 = \ldots = \Xi_\mu = 0$ and by $0 \neq \hat{R}_{\mathscr{X}} \in F[Y, u_0, \ldots, u_s]$ its u-resultant. Again, dividing $\hat{R}_{\mathscr{X}}$ by the highest possible power of Y, we can sssume w.l.o.g. that $Y \nmid \hat{R}_{\mathscr{X}}$.

Proposition 7(c) entails that

$$\hat{R}_{\mathscr{X}} = \prod_j (L_j^{(1)})^{\hat{\gamma}_j}, \quad R_{\mathscr{X}} = \prod_j (L_j^{(1)})^{\gamma_j},$$

where the linear forms $L_j^{(1)} = \xi_0^{(j)} u_0 + \ldots + \xi_s^{(j)} u_s$ correspond bijectively to the points $(\xi_0^{(j)} : \ldots : \xi_s^{(j)}) \in U_{H_1}$ of the variety U_{H_1}. Furthermore, the integers $\hat{\gamma}_j$, γ_j are positive. Hence, the relations $R_{\mathscr{X}} | (\hat{R}_{\mathscr{X}})^{\hat{\gamma}}$ and $\hat{R}_{\mathscr{X}} | (R_{\mathscr{X}})^{\gamma}$ are valid in the ring $H_1[u_0, \ldots, u_s]$ for relevant integers $\hat{\gamma}$, γ. Therefore,

$$R_{\mathscr{X}}(0, u_0, \ldots, u_s) | (\hat{R}_{\mathscr{X}}(0, u_0, \ldots, u_s))^{\hat{\gamma}} \text{ and } \hat{R}_{\mathscr{X}}(0, u_0, \ldots, u_s) | (R_{\mathscr{X}}(0, u_0, \ldots, u_s))^{\gamma}$$

are true in the ring $F[u_0, \ldots, u_s]$.

Consider a system

$$\Xi_0(0, X_0, \ldots, X_s) = \ldots = \Xi_\mu(0, X_0, \ldots, X_s) = 0.$$

It has a finite number of roots $\mathscr{W} \subset \mathbb{P}^s(\bar{F})$ and herewith the cone

$$\operatorname{con}(\mathscr{W}) = (\bigcup_t \mathscr{V}_t) \cap \{Y = 0\} \subset \bar{F}^{s+1}$$

(see proposition 5). The matrix $\hat{A}_{\mathscr{X}}(0)$, corresponding to the latter system is obtained from thc matrix $\hat{A}_{\mathscr{X}}$ by substituting 0 instead of Y. Let $\Delta(0)$ be a certain nonsingular $\tau_1 \times \tau_1$ submatrix of the matrix $\hat{A}_{\mathscr{X}}(0)$, containing the maximal possible number of columns in the number part of $\hat{A}_{\mathscr{X}}(0)$, then

$$\det(\Delta(0)) = \prod_i L_i^{\hat{c}_i}$$

is the u-resultant of the system

$$\Xi_0(0, X_0, \ldots, X_s) = \ldots = \Xi_\mu(0, X_0, \ldots, X_s) = 0,$$

where the linear forms L_i correspond bijectively to the points of the set $\mathscr{W}$ according to proposition 7(b). Denote by Δ the $\tau_1 \times \tau_1$ submatrix of the matrix $\hat{A}_{\mathscr{X}}$ formed by the same columns as the matrix $\Delta(0)$. Then $\det(\Delta) \neq 0$ and, by proposition 7(b), $\hat{R}_{\mathscr{X}} | \det(\Delta)$ in the ring $H_1[u_0, \ldots, u_s]$. Hence, $\hat{R}_{\mathscr{X}}(0, u_0, \ldots, u_s) | \det(\Delta(0))$. Thus

$$R_{\mathscr{X}}(0, u_0, \ldots, u_s) = \prod_i L_i^{c_i}$$

is fulfilled for suitable integers c_i. Our next purpose is to show that each $c_i > 0$.

Denote by $\mathscr{J}_F^{(t)} \subset F[Y, X_0, \ldots, X_s]$ the prime ideal defining the component $\mathscr{V}_t$, and by $\mathscr{J}_{H_1}^{(t)} \subset H_1[X_0, \ldots, X_s]$ the prime ideal defining the class of points of the variety U_{H_1} conjugate over the field H_1, that correspond to each other by proposition 4. Introduce a polynomial

$$E(Y, X_0, \ldots, X_s) = R_{\mathscr{X}}(Y, -\sum_{1 \leqslant i \leqslant s} u_i X_i, u_1 X_0, \ldots, u_s X_0) = \sum_I E_I u^I,$$

where the polynomials $E_I \in F[Y, X_0, \ldots, X_s]$ and $u^I = u_1^{I_1} \ldots u_s^{I_s}$ is a monomial respective to a multi-index $I = (I_1, \ldots, I_s)$. Let a point $(\xi_0 : \ldots : \xi_s) \in U_{H_1}$ and

$$L_{jo}^{(1)}(u_0, \ldots, u_s) = \xi_0 u_0 + \ldots + \xi_s u_s$$

be the corresponding linear form. Consider a polynomial

$$E_{jo}^{(1)}(X_0, \ldots, X_s) = L_{jo}^{(1)}(-\sum_{1 \leqslant i \leqslant s} u_i X_i, u_1 X_0, \ldots, u_s X_0)$$
$$= -\xi_0 \sum_{1 \leqslant i \leqslant s} u_i X_i + \xi_1 u_1 X_0 + \ldots + \xi_s u_s X_0 \in \bar{H}_1[X_0, \ldots, X_s, u_1, \ldots, u_s].$$

Obviously,

$$E(Y, X_0, \ldots, X_s) = \prod_j (E_j^{(1)}(X_0, \ldots, X_s))^{\gamma_j}.$$

Then

$$0 = E_{j_0}^{(1)}(\xi_0, \ldots, \xi_s) \in \bar{H}_1[u_1, \ldots, u_s],$$

and, conversely, if $E_{j_0}^{(1)}(\zeta_0, \ldots, \zeta_s) = 0$ and some of the $\zeta_0, \ldots, \zeta_s$ does not vanish, then the points

$$(\xi_0 : \ldots : \xi_s) = (\zeta_0 : \ldots : \zeta_s) \in \mathbb{P}^s(\bar{H}_1)$$

coincide. Therefore

$$0 = \prod_j (E_j^{(1)}(\hat{\xi}_0, \ldots, \hat{\xi}_s))^{\gamma_j} = E(Y, \hat{\xi}_0, \ldots, \hat{\xi}_s)$$

for every point $(\hat{\xi}_0 : \ldots : \hat{\xi}_s) \in U_{H_1}$. This implies that a polynomial $E_I \in \mathscr{I}_{H_1}^{(t)}$ for each I, t. Hence, by virtue of proposition 4, $E_I \in \mathscr{I}_F^{(t)}$. This means that the polynomial $E(Y, X_0, \ldots, X_s)$ vanishes on the variety $(\bigcup_t \mathscr{V}_t)$. Therefore, the polynomial $E(0, X_0, \ldots, X_s)$ vanishes on the variety

$$(\bigcup_t \mathscr{V}_t) \cap \{Y = 0\}.$$

By the above arguments, this entails that, for any point of the variety

$$(\bigcup_t \mathscr{V}_t) \cap \{Y = 0\}$$

and its corresponding linear form L_{i_0},

$$L_{i_0}^t | R_{\mathscr{Z}}(0, u_0, \ldots, u_s) = \prod_i L_i^{c_i}.$$

This completes the proof of the following

Proposition 8. *Let $R_{\mathscr{Z}}$ be the u-resultant of system* (8″). *Then*

$$R_{\mathscr{Z}}(0, u_0, \ldots, u_s) = \prod_i L_i^{c_i}$$

for appropriate positive integers c_i, where the linear forms $L_i = \zeta_0 u_0 + \ldots + \zeta_s u_s$ correspond bijectively to the points $(\zeta_0 : \ldots : \zeta_s) \in \mathscr{W}$ of the set $\mathscr{W} \subset \mathbb{P}^s(\bar{F})$ such that its cone

$$\operatorname{con}(\mathscr{W}) = (\bigcup_t \mathscr{V}_t) \cap \{Y = 0\}.$$

Applying lemma 7(a), (b), proposition 5 and proposition 8 to a point $\mathscr{Z} = z^{(2)} \in F_2^{n+1}$ one can infer the following

Corollary. *A point $z^{(2)} \in F_2^{n+1}$ satisfies formula* (6) *iff there exist a vector*

$$\gamma = (\gamma_2, \ldots, \gamma_s) \in \Gamma$$

and a linear form $\hat{L}_i = \xi_0^{(i)} u_0 + \ldots + \xi_s^{(i)} u_s$ such that *$\hat{L}_i | R_{z^{(2)}}(0, u_0, \ldots, u_s)$ and $\xi_0^{(i)} \neq 0$. Furthermore, the point $(\xi_1^{(i)}/\xi_0^{(i)}, \ldots, \xi_s^{(i)}/\xi_0^{(i)}) \in F_3^s$ belongs to the space F_3^s. Finally, the inequalities*

$$f_i(z^{(2)}, \xi_1^{(i)}/\xi_0^{(i)}, \ldots, \xi_s^{(i)}/\xi_0^{(i)}) + \varepsilon_1 > 0; \quad 0 \leqslant i \leqslant k$$

are fulfilled.

Our next aim is to contruct a polynomial

$$\psi_0(Z_0, \ldots, Z_n) \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, u_0, \ldots, u_s]$$

and a polynomial

$$P(Z_0, \ldots, Z_n) \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n]$$

such that

$$\psi_0(Z_0, \ldots, Z_n) = \lambda \prod_{i \in I} L_i^{c_i} | R(0, Z_0, \ldots, Z_n, u_0, \ldots, u_s)$$

is a product (up to a factor $\lambda \in \overline{F_3(Z_0, \ldots, Z_n)}^*$) of all linear forms $L_i = \zeta_0^{(i)} u_0 + \ldots + \zeta_s^{(i)} u_s$, $i \in I$ which are factors of the polynomial $R(0, Z_0, \ldots, Z_n, u_0, \ldots, u_s)$ such that $\zeta_j^{(i)} \in \overline{\mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n)}$, $\zeta_0^{(i)} \neq 0$ and, besides,

$$\psi_0(z^{(3)}) = \hat{\lambda} \prod_{i \in J} \hat{L}_i^{c_i} | R_{z^{(3)}}(0, u_0, \ldots, u_s)$$

is a product (up to a factor $\hat{\lambda} \in \bar{F}_3^*$) of all linear forms

$$\hat{L}_i = (\xi_0^{(i)} u_0 + \ldots + \xi_s^{(i)} u_s) | R_{z^{(3)}}(0, u_0, \ldots, u_s), \quad i \in J$$

such that $\xi_j^{(i)} \in \bar{F}_3$, $\xi_0^{(i)} \neq 0$, provided that $P(z^{(3)}) \neq 0$, where a point $z^{(3)} \in \bar{F}_3^{n+1}$ (cf. the construction from Chistov & Grigor'ev, 1984).

Now the algorithm applies the Gaussian algorithm to the matrix A. Let ρ steps of Gaussian algorithm be already carried out and let $(i_0, j_0), \ldots, (i_{\rho-1}, j_{\rho-1})$ be a sequence of leading entries, herewith $j_0 < \ldots < j_{\rho-1}$, and $i_\alpha \neq i_\beta$ when $\alpha \neq \beta$. By the current step the matrix A is reduced by elementary transformations to a matrix $A^{(\rho)} = (a_{ij}^{(\rho)})$ (at the beginning $A^{(0)} = A$) with entries from the field $\mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n, u_0, \ldots, u_s)$.

Moreover, $a_{ij}^{(\rho)} = 0$ if either $j_{\beta-1} < j < j_\beta$ for a certain $0 \leqslant \beta \leqslant \rho - 1$, or $j = j_\beta$ for some $0 \leqslant \beta \leqslant \rho - 1$ and $i \neq i_\alpha$ for all $0 \leqslant \alpha \leqslant \rho - 1$, or $j = j_\beta$ for some $0 \leqslant \beta \leqslant \rho - 1$ and $i = i_\alpha$ for some $0 \leqslant \beta < \alpha \leqslant \rho - 1$. The next leading entry (i_ρ, j_ρ) is picked out so that j_ρ is the least possible index such that $j_{\rho-1} < j_\rho$ and $a_{i_\rho, j_\rho}^{(\rho)} \neq 0$. For each i different from all $i_0, \ldots, i_\rho$ set the entry $a_{ij}^{(\rho+1)} = a_{ij}^{(\rho)} - a_{i_\rho, j}^{(\rho)} a_{i, j_\rho}^{(\rho)} / a_{i_\rho, j_\rho}^{(\rho)}$ (an elementary transformation over rows with the leading entry (i_ρ, j_ρ)). This completes the description of applying Gaussian algorithm to the matrix A and producing matrices $A = A^{(0)}, \ldots, A^{(\tau-1)}$, where τ is the number of rows in the matrix A, taking into account that $\operatorname{rank}(A) = \tau$ by virtue of proposition 3 and proposition 7(a).

Let $i \neq i_\alpha$ for all $0 \leqslant \alpha \leqslant \rho - 1$ and $j \neq j_\beta$ for all $0 \leqslant \beta \leqslant \rho - 1$. Denote by $\Delta_{ij}^{(\rho)}$ a submatrix of the matrix A, formed by the rows $i_0, \ldots, i_{\rho-1}, i$ and by the columns $j_0, \ldots, j_{\rho-1}, j_{(\rho)}$. It is well known (see e.g. Heintz, 1983) that $a_{ij} = \det(\Delta_{ij}^{(\rho)}) / \det(\Delta_{i_{\rho-1}, j_{\rho-1}}^{(\rho-1)})$. This statement, as usual, guarantees that the Gaussian algorithm can be realised within the available time (see section 5 below).

After carrying out the Gaussian algorithm, the algorithm under description calculates polynomials

$$\psi_1 = a_{i_0, j_0}^{(0)} \ldots a_{i_{\tau-1}, j_{\tau-1}}^{(\tau-1)} = \det(\Delta_{i_{\tau-1}, j_{\tau-1}}^{(\tau-1)})$$

and

$$P_1 = \prod_{0 \leqslant \rho \leqslant \tau - 1} (a_{i_\rho, j_\rho}^{(\rho)})^{\tau - \rho} = \prod_{0 \leqslant \rho \leqslant \tau - 1} \det(\Delta_{i_\rho, j_\rho}^{(\rho)})$$

from the ring $\mathbb{Q}[\varepsilon_1, \varepsilon_3][Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s]$. Denote by ρ_0 the unique number such that the entry $a_{i_{\rho 0 - 1}, j_{\rho 0 - 1}}^{(0)}$ belongs to the number part of the matrix A and the entry $a_{i_{\rho 0}, j_{\rho 0}}^{(0)}$ belongs to the formal part of A. Because of the choice of entry $a_{i_{\rho 0}, j_{\rho 0}}^{(\rho 0)}$ with the least possible $j_{\rho 0}$ one deduces that the rank of the number part of A equals ρ_0. Therefore, proposition 7(d) implies the coincidence of the polynomial ψ_1 with the u-resultant R of system (8′) up to a factor from $(\mathbb{Q}(\varepsilon_1, \varepsilon_3)(Y, Z_0, \ldots, Z_n))^*$. Observe that if

$$0 \neq P_1(z^{(3)}) \in \bar{F}_3[Y, u_0, \ldots, u_s],$$

then the polynomial $\psi_1(z^{(3)})$ coincides with the u-resultant $R_{z^{(3)}}$ of system (8) up to a factor from $(\bar{F}_3(Y))^*$ again according to proposition 7(d).

Let us write

$$\psi_1 = \sum_{j_0 \leqslant j} \psi_1^{(j)} Y^j,$$

where the polynomials

$$\psi_1^{(j)}(Z_0, \ldots, Z_n) \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, u_0, \ldots, u_s],$$

furthermore, $\psi_1^{(j_0)} \neq 0$. Then the polynomial

$$R(0, Z_0, \ldots, Z_n, u_0, \ldots, u_s) \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, u_0, \ldots, u_s]$$

coincides with the polynomial $\psi_1^{(j_0)}$ up to a factor from $(\mathbb{Q}\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n))^*$. If

$$0 \neq \psi_1^{(j_0)}(z^{(3)}) \in \bar{F}_3[u_0, \ldots, u_s]$$

and $P_1(z^{(3)}) \neq 0$, then the polynomial

$$R_{z^{(3)}}(0, u_0, \ldots, u_s) \in \bar{F}_3[u_0, \ldots, u_s]$$

coincides with the polynomial $\psi_1^{(j_0)}(z^{(3)})$ up to a factor from $\bar{F}_3^*$.

We write

$$\psi_1^{(j_0)} = \sum_{m \leqslant m_0} \psi_1^{(j_0, m)} u_0^m,$$

where the polynomials

$$\psi_1^{(j_0, m)}(Z_0, \ldots, Z_n) \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, u_1, \ldots, u_s],$$

furthermore, $\psi_1^{(j_0, m_0)} \neq 0$. Then a polynomial $\psi_1^{(j_0, m_0)}$ coincides up to a factor from $\overline{F_3(Z_0, \ldots, Z_n)}^*$ with the product

$$\prod_{i \notin I} L_i^{c_i} | R(0, Z_0, \ldots, Z_n, \ldots, Z_n, u_0, \ldots, u_s)$$

of all linear forms

$$L_i = \zeta_0^{(i)} u_0 + \ldots + \zeta_s^{(i)} u_s, \quad i \notin I$$

being factors of $R(0, Z_0, \ldots, Z_n, u_0, \ldots, u_s)$ such that $\zeta_0^{(i)} = 0$; $\zeta_j^{(i)} \in \overline{\mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n)}$ (see proposition 8). If

$$0 \neq \psi_1^{(j_0, m_0)}(z^{(3)}) \in \bar{F}_3[u_1, \ldots, u_s]$$

and $P_1(z^{(3)}) \neq 0$, then a polynomial $\psi_1^{(j_0, m_0)}(z^{(3)})$ coincides up to a factor from $\bar{F}_3^*$ with the product $\prod_{i \notin J} \hat{L}_i^{\hat{c}_i} | R_{z^{(3)}}(0, u_0, \ldots, u_s)$ of all linear forms

$$\hat{L}_i = \xi_0^{(i)} u_0 + \ldots + \xi_s^{(i)} u_s$$

being factors of $R_{z^{(3)}}(0, u_0, \ldots, u_s)$ such that $\xi_0^{(i)} = 0$; $\xi_j^{(i)} \in \bar{F}_3$ (see again proposition 8). Hence, the desired product

$$\prod_{i \in I} L_i^{c_i} | R(0, Z_0, \ldots, Z_n\ u_0, \ldots, u_s)$$

of all linear forms

$$L_i = \zeta_0^{(i)} u_0 + \ldots + \zeta_s^{(i)} u_s, \quad i \in I$$

such that $\zeta_0^{(i)} \neq 0$, coincides up to a factor from $\overline{F_3(Z_0, \ldots, Z_n)}^*$ with a quotient

$$\psi_1^{(j_0)} / \psi_1^{(j_0, m_0)} \in \mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n)[u_0, u_1, \ldots, u_s],$$

hence

$$\psi_1^{(j_0, m)} / \psi_1^{(j_0, m_0)} \in \mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n)[u_1, \ldots, u_s]$$

for each $m \leqslant m_0$. Similarly, the product

$$\prod_{i \in J} \hat{L}_i^{\hat{c}_i} | R_{z^{(3)}}(0, u_0, \ldots, u_s)$$

of all linear forms

$$\hat{L}_i = \xi_0^{(i)} u_0 + \ldots + \xi_s^{(i)} u_s, \quad i \in J$$

such that $\xi_0^{(i)} \neq 0$; $\xi_j^{(i)} \in \bar{F}_3$ coincides up to a factor from $\bar{F}_3^*$ with a quotient

$$(\psi_1^{(jo)}/\psi_1^{(jo,mo)})(z^{(3)}) \in \bar{F}_3[u_0, u_1, \ldots, u_s].$$

Hence,

$$(\psi_1^{(jo,m)}/\psi_1^{(jo,mo)}) \in \bar{F}_3[u_1, \ldots, u_s]$$

for each $m \leqslant m_0$, provided that $\psi_1^{(jo,mo)}(z^{(3)}) \neq 0$ and $P_1(z^{(3)}) \neq 0$.

After that the algorithm calculates the quotient $\psi_1^{(jo)}/\psi_1^{(jo,mo)}$ factoring both polynomials $\psi_1^{(jo)}, \psi_1^{(jo,mo)}$ over the field $\mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n)$ using proposition 1. The quotient $(\psi_1^{(jo)}/\psi_1^{(jo,mo)})(z^{(3)})$ is obtained by substituting in the quotient $(\psi_1^{(jo)}/\psi_1^{(jo,mo)})$ the coordinates of the point $z^{(3)}$ instead of the variables $Z_0, \ldots, Z_n$, provided that $\psi_1^{(jo,mo)}(z^{(3)}) \neq 0$, $P_1(z^{(3)}) \neq 0$. We represent $\psi_1^{(jo)}/\psi_1^{(jo,mo)} = \psi_0/P_2$ for a certain polynomial $P_2 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n]$ of the least possible degree and $\psi_0 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, u_0, \ldots, u_s]$. If $P_2(z^{(3)}) \neq 0$, $\psi_1^{(jo,mo)}(z^{(3)}) \neq 0$, $P_1(z^{(3)}) \neq 0$, then $\psi_0(z^{(3)})$ coincides with $(\psi_1^{(jo)}/\psi_1^{(jo,mo)})(z^{(3)})$ up to a factor from $\bar{F}_3^*$ and thus, with the product

$$\prod_{i \in J} \hat{L}_i^{\hat{c}_i} | R_{z^{(3)}}(0, u_0, \ldots, u_s)$$

of all linear forms

$$\hat{L}_i = \xi_0^{(i)} u_0 + \ldots + \xi_s^{(i)} u_s, \quad i \in J$$

such that $\xi_0^{(i)} = 0$, $\xi_j^{(i)} \in \bar{F}_3$ up to a factor from $\bar{F}_3^*$. So, the polynomial ψ_0 is constructed.

In order to produce a polynomial P, represent

$$P_1 = \sum_{K(1)} \delta_{K^{(1)}}^{(1)}(Z_0, \ldots, Z_n) u_0^{K_0^{(1)}} \ldots u_s^{K_s^{(1)}} Y^{K_{s+1}^{(1)}},$$

$$\psi_1^{(jo,mo)} = \sum_{K(2)} \delta_{K^{(2)}}^{(2)}(Z_0, \ldots, Z_n) u_1^{K_1^{(2)}} \ldots u_s^{K_s^{(2)}},$$

where

$$K^{(1)} = (K_0^{(1)}, \ldots, K_{s+1}^{(1)}), \qquad K^{(2)} = (K_1^{(2)}, \ldots, K_s^{(2)})$$

are multi-indices and the polynomials

$$\delta_{K^{(1)}}^{(1)}, \delta_{K^{(2)}}^{(2)} \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n].$$

Pick out some multi-indices $K^{(1)}, K^{(2)}$ for which $\delta_{K^{(1)}}^{(1)} \neq 0$ and $\delta_{K^{(2)}}^{(2)} \neq 0$. Finally, we put the polynomial $P = \delta_{K^{(1)}}^{(1)} \delta_{K^{(2)}}^{(2)} P_2$. If $P(z^{(3)}) \neq 0$, then $P_2(z^{(3)}) \neq 0$, $\psi_1^{(jo,mo)}(z^{(3)}) \neq 0$, $P_1(z^{(3)}) \neq 0$. This completes the construction of polynomials ψ_0, P.

Thus, based on the above corollary, we have proved the following

LEMMA 8. *A point $z^{(2)} \in F_2^{n+1}$ such that $P(z^{(2)}) \neq 0$ satisfies formula* (6) *iff there exist a vector $\gamma = (\gamma_2, \ldots, \gamma_s) \in \Gamma$ and a linear form $\hat{L}_i = \xi_0^{(i)} u_0 + \ldots + \xi_s^{(i)} u_s$ such that $\hat{L}_i | \psi_0(z^{(2)})$ (therefore $\xi_0^{(i)} \neq 0$). Furthermore, the point $(\xi_1^{(i)}/\xi_0^{(i)}, \ldots, \xi_s^{(i)}/\xi_0^{(i)}) \in F_3^s$ belongs to the space F_3^s, and, finally, the inequalities*

$$f_i(z^{(2)}, \xi_1^{(i)}/\xi_0^{(i)}, \ldots, \xi_s^{(i)}/\xi_0^{(i)}) + \varepsilon_1 > 0, \quad 0 \leqslant i \leqslant k$$

are fulfilled.

With the aid of proposition 1 (see introduction) the algorithm factorises the polynomial ψ_0 over the field $\mathbb{Q}$. Since ψ_0 is a product of linear forms, its irreducible factors $\Omega \in \mathbb{Q}[\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0, \ldots, u_s]$ correspond bijectively to classes of linear forms L_ν, which are conjugate over the field $H_2 = \mathbb{Q}(\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n)$, moreover, the product of all linear forms L_ν from the considered class corresponding to Ω, equals to Ω up to a factor from H_2.

Now fix Ω for the time being and define $D_1 = \deg_{u_0, \ldots, u_s}(\Omega)$. Let a linear form

$$L_\nu = (\zeta_0^{(\nu)} u_0 + \ldots + \zeta_s^{(\nu)} u_s) | \Omega$$

be a factor of Ω, consider a field

$$H_3^{(\nu)} = H_2(\zeta_1^{(\nu)}/\zeta_0^{(\nu)}, \ldots, \zeta_s^{(\nu)}/\zeta_0^{(\nu)})$$

being a finite extension of H_2. Let $\delta: H_3^{(\nu)} \to \bar{H}_2$ be any field embedding over H_2. Then

$$\delta(L_\nu/\zeta_0^{(\nu)}) = L_\mu/\zeta_0^{(\mu)} = u_0 + (\zeta_1^{(\mu)}/\zeta_0^{(\mu)}) u_1 + \ldots + (\zeta_s^{(\mu)}/\zeta_0^{(\mu)}) u_s$$

for a suitable unique index μ since $\delta(L_\nu/\zeta_0^{(\nu)}) | \Omega$. Therefore, there exist not more than D_1 embeddings, hence the field degree $[H_3^{(\nu)} : H_2] \leqslant D_1$ (see Lang, 1965). In fact, $[H_3^{(\nu)} : H_2] = D_1$, taking into account that a polynomial

$$\prod_\delta \delta(L_\nu/\zeta_0^{(\nu)}) \in H_2[u_0, \ldots, u_s]$$

is a factor of the polynomial Ω irreducible over H_2, where the product is taken over all embeddings $\delta: H_3^{(\nu)} \to \bar{H}_2$ over H_2. This entails the existence of integers $1 \leqslant \lambda_i \leqslant D_1$, $1 \leqslant i \leqslant s$ such that the element

$$\theta^{(\nu)} = \sum_{1 \leqslant i \leqslant s} \lambda_i (\zeta_i^{(\nu)}/\zeta_0^{(\nu)})$$

is primitive in the field $H_2[\theta^{(\nu)}] = H_3^{(\nu)}$ by virtue of the theorem on primitive elements (see Lang, 1965).

The algorithm considers all s-tuples $(\lambda_1^{(0)}, \ldots, \lambda_s^{(0)})$, where $1 \leqslant \lambda_i^{(0)} \leqslant D_1$, $1 \leqslant i \leqslant s$. For each s-tuple $(\lambda_1^{(0)}, \ldots, \lambda_s^{(0)})$ it checks, whether the element

$$\theta_0^{(\nu)} = \sum_{1 \leqslant i \leqslant s} \lambda_1^{(0)} (\zeta_i^{(\nu)}/\zeta_0^{(\nu)})$$

is primitive over the field H_2, in the following manner. Substitute in the polynomial Ω the vector $(-\lambda_1^{(0)}, \ldots, -\lambda_s^{(0)})$ instead of $(u_1, \ldots, u_s)$. Then a polynomial

$$\begin{aligned} \Omega_0(u_0) &= \Omega(u_0, -\lambda_1^{(0)}, \ldots, -\lambda_s^{(0)}) \\ &= \Big(\prod_\nu \zeta_0^{(\nu)}\Big)\Big(\prod_\nu (u_0 - \theta_0^{(\nu)})\Big) \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, u_0]. \end{aligned}$$

Since $\Omega_0(\theta_0^{(\nu)}) = 0$ and $\deg_{u_0}(\Omega_0) = D_1$, the element $\theta_0^{(\nu)}$ is primitive in the field $H_3^{(\nu)}$ iff the polynomial Ω_0 is irreducible over the field H_2. The algorithm tests its irreducibility with the help of proposition 1 and thus, finds a primitive element

$$\theta^{(\nu)} = \sum_{1 \leqslant i \leqslant s} \lambda_i (\zeta_i^{(\nu)}/\zeta_0^{(\nu)})$$

and its minimal polynomial

$$\Phi = \Omega_0 / \Big(\prod_\nu \zeta_0^{(\nu)}\Big).$$

Then the algorithm produces for each element

$$\zeta_i^{(\nu)}/\zeta_0^{(\nu)} = (\zeta_i^{(\nu)}/\zeta_0^{(\nu)})(\theta^{(\nu)}) = \sum_{0 \leqslant j \leqslant D_1} (a_j^{(i)}/b)(\theta^{(\nu)})^j \in H_2[\theta^{(\nu)}] = H_3^{(\nu)}$$

its expression via $\theta^{(\nu)}$, where the polynomials

$$a_j^{(i)}, b \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n].$$

For this goal consider a polynomial

$$\begin{aligned}\Omega_i &= \Omega(-\lambda_1, \ldots, -\lambda_{i-1}, -\lambda_i + u_i, -\lambda_{i+1}, \ldots, -\lambda_s)\\ &= (\prod_{\nu} \zeta_0^{(\nu)})(\prod_{\nu} (u_0 - \theta_0^{(\nu)} + (\zeta_i^{(\nu)}/\zeta_0^{(\nu)})u_i))\end{aligned}$$

and factorise it over the field $H_3^{(\nu)}$ based on proposition 1. Then we obtain a linear factor $u_0 - \theta^{(\nu)} + (\zeta_i^{(\nu)}/\zeta_0^{(\nu)})(\theta^{(\nu)})u_i$ of Ω_i and as a result the expression $(\zeta_i^{(\nu)}/\zeta_0^{(\nu)})(\theta^{(\nu)})$.

Thus, the algorithm has produced a polynomial

$$\Phi = \sum_{0 \leqslant j \leqslant D_1} (\alpha_j/\beta)T^j \in H_2[T]$$

irreducible over H_2, where $\alpha_j, \beta \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n]$ with the leading coefficient $lc_T(\Phi) = 1$. The expressions

$$(\zeta_i^{(\nu)}/\zeta_0^{(\nu)})(\theta^{(\nu)}) = \sum_{0 \leqslant j < D_1} (\alpha_j^{(i)}/b)(\theta^{(\nu)})^j \in H_2[\theta^{(\nu)}]$$

and the integers $1 \leqslant \lambda_i \leqslant D_1$, $1 \leqslant i \leqslant s$ satisfy the following properties. For each root $\theta_0 \in \bar{H}_2$ of the polynomial Φ the equality

$$\theta_0 = \sum_{1 \leqslant i \leqslant s} \lambda_i (\sum_{0 \leqslant j < D_1} (a_j^{(i)}/b)\theta_0^j)$$

holds, furthermore, a linear from

$$L^{(\theta_0)} = (u_0 + \sum_{1 \leqslant i \leqslant s} (\sum_{0 \leqslant j < D_1} (a_j^{(i)}/b)\theta_0^j)u_i) | \Omega$$

divides the polynomial Ω in the ring $H_2[\theta_0][u_0, \ldots, u_s]$ and $L^{(\theta_0)} = L_\nu/\zeta_0^{(\nu)}$ for an appropriate index ν; conversely, every linear form $L_\nu|\Omega$ dividing Ω equals $L_\nu = \zeta_0^{(\nu)}L^{(\theta_0)}$ for a suitable root θ_0 of the polynomial Ω. The fields

$$H_2[\theta_0] \simeq H_2[T]/(\Phi) \simeq H_2[\theta^{(\nu)}] = H_2(\zeta_1^{(\nu)}/\zeta_0^{(\nu)}, \ldots, \zeta_s^{(\nu)}/\zeta_0^{(\nu)})$$

are isomorphic. Further, we assume that any element $\eta \in H_2[\theta_0]$ is represented in the form

$$\eta = \sum_{0 \leqslant j < D_0} \eta_j \theta_0^j.$$

Then $\Omega = L^{(\theta_0)}\chi^{(\theta_0)}$ for a certain polynomial $\chi^{(\theta_0)} \in H_2[\theta_0][u_0, \ldots, u_s]$ homogeneous in variables $u_0, \ldots, u_s$ of degree $D_1 - 1$. The algorithm finds the coefficients of the polynomial $\chi^{(\theta_0)}$ factoring the polynomial Ω over the field $H_2[\theta_0]$ with the aid of proposition 1. Let us denote by $L^{(T)}, \chi^{(T)} \in H_2[T][u_0, \ldots, u_s]$ the polynomials obtained by replacing θ_0 by the variable T in the polynomials $L^{(\theta_0)}, \chi^{(\theta_0)}$, respectively. One can show that the polynomial

$$(\Omega - L^{(T)}\chi^{(T)}) = \Phi\tau_1 \in (\Phi) \subset H_2[T][u_0, \ldots, u_s]$$

belongs to the principal ideal (Φ). Analogously, taking into account the equality

$$\theta_0 = \sum_{1 \leqslant i \leqslant s} \lambda_i \zeta_i^{(\nu)}/\zeta_0^{(\nu)}$$

one deduces

$$T - \sum_{1 \leqslant i \leqslant s} \lambda_i \sum_j (a_j^{(i)}/b)T^j = \phi\tau_2 \in (\Phi).$$

Let us write

$$\chi^{(\theta_0)} = \sum_j (a_{j1}/b_1)\theta_0^j, \qquad \tau_1 = \sum_j (\alpha_{j1}/\beta_1)T^j, \qquad \tau_2 = \sum_j \frac{\alpha_{j2}T^j}{\beta_2},$$

where the polynomials $b_1, \beta_1, \beta_2 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n]$ and the polynomials

$$a_{j1}, \alpha_{j1}, \alpha_{j2} \in \mathbb{Q}[\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n][u_0, \ldots, u_s].$$

Assume that a certain point $z^{(3)} \in \bar{F}_3^{n+1}$ satisfies the following conditions:

$$((bb_1\beta\beta_1\beta_2)(z^{(3)}) \neq 0) \,\&\, (\bigvee_q (\varphi_q(z^{(3)}) \neq 0)),$$

and let $\theta^{(0)} \in \bar{F}_3$ be one of the roots of the polynomial $\Phi(z^{(3)})(T) \in \bar{F}_3[T]$. Then the linear form $L^{(\theta^{(0)})}(z^{(3)})|\Omega(z^{(3)})$ divides the polynomial $\Omega(z^{(3)})$ in the ring $\bar{F}_3[u_0, \ldots, u_s]$, since $(\Phi\tau_1)(z^{(3)})(\theta^{(0)}) = 0$. So the linear form $L^{(\theta^{(0)})}(z^{(3)})$ is collinear to one of the linear forms $\hat{L}_{\rho_1}$ in the factorisation

$$\Omega(z^{(3)}) = \prod_{\rho_1} \hat{L}_{\rho_1}^{\mu_{\rho_1}}$$

(cf. above the factorisation of $\psi_0(z^{(3)})$).

Let us denote by

$$D = \operatorname{Res}_T(\Phi, \Phi'_T) = (a_2/b_2) \in H_2$$

the discriminant of polynomial Φ, where a_2, b_2 are polynomials in $\mathbb{Q}[\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n]$.

Lemma 9. *Let a point $z^{(3)} \in \bar{F}_3^{n+1}$ satisfy the conditions*

$$((bb_1b_2\beta\beta_1\beta_2)(z^{(3)}) \neq 0) \,\&\, (\varphi_1(z^{(3)}) \neq 0) \,\&\, (D(z^{(3)}) \neq 0). \tag{9}$$

Then

$$\Omega(z^{(3)}) = \delta \prod_{\varkappa} L^{(\theta_\varkappa^{(0)})}(z^{(3)})$$

for an appropriate $0 \neq \delta \in \bar{F}_3$ where the product is taken over all roots $\theta_\varkappa^{(0)} \in \bar{F}_3$ of the polynomial $\phi(z^{(3)})(T)$. Moreover,

$$\theta_\varkappa^{(0)} = \sum_{1 \leqslant i \leqslant s} \lambda_i \Big(\sum_j \frac{a_j^{(i)}(z^{(3)})}{b(z^{(3)})} (\theta_\varkappa^{(0)})^j\Big)$$

where $\Phi(z^{(3)})(\theta_\varkappa^{(0)}) = 0$.

Proof. The linear form $L^{(\theta_\varkappa^{(0)})}(z^{(3)})|\Omega(z^{(3)})$ divides the polynomial $\Omega(z^{(3)})$ for all $\varkappa$ according to the facts proved above, furthermore $\theta_{\varkappa_1}^{(0)} \neq \theta_{\varkappa_2}^{(0)}$ when $\varkappa_1 \neq \varkappa_2$ since $D(z^{(3)}) \neq 0$.

Finally,

$$\theta_\varkappa^{(0)} = \sum_{1 \leqslant i \leqslant s} \lambda_i \left(\sum_j \frac{a_j^{(i)}(z^{(3)})}{b(z^{(3)})} (\theta_\varkappa^{(0)})^j\right),$$

in view of the equality $(\Phi\tau_2)(\mathrm{z}^{(3)})(\theta_\varkappa^{(0)}) = 0$. Therefore all linear forms $L^{(\theta_\varkappa^{(0)})}(z^{(3)})$ are pairwise distinct for diverse $\varkappa$, and so $\prod_\varkappa L^{(\theta_\varkappa^{(0)})}(z^{(3)})|\Omega(z^{(3)})$, where the degrees of both these polynomials are equal to $\deg_T(\Phi) = \deg_{u_0, \ldots, u_s}(\Omega)$. This completes the proof of the lemma.

The conditions (9) concern the case of a fixed vector $\gamma \in \Gamma$ and an irreducible factor $\Omega|\Psi_0$. We introduce a hypersurface $\mathscr{L}$ consisting of all points $z^{(3)} \in \bar{F}_3^{n+1}$ which do not satisfy the conditions similar to (9) for at least one vector $\gamma^{(1)} \in \Gamma$ and one irreducible factor $\Omega^{(1)} | \Psi_0$. Then the degree

$$\deg(\mathscr{L}) \leqslant N_1 = (\operatorname{card} \Gamma)((\deg \psi_0)(\deg (bb_1 b_2 \beta\beta_1 \beta_2 D)) \deg \varphi_1)$$

(an estimate on N_1 will be found below in section 5). Let us denote $N = N_1 n + 1$. It is easy to construct (see e.g. section 2 in Chistov & Grigor'ev, 1983*a*) linear forms $Y_1, \ldots, Y_N$ over integers in the variables $Z_0, \ldots, Z_n$ such that any $(n+1)$ among them are linearly independent (one can set, for example

$$Y_i = \sum_{0 \leqslant j \leqslant n} i^j Z_j).$$

Let us fix a certain point $z^{(3)} \in \bar{F}_3^{n+1}$. We assert the existence of indices $1 \leqslant i_1 < \ldots < i_n \leqslant N$ such that the line

$$(z^{(3)} + \lambda\{Y_{i_1} = \ldots = Y_{i_n} = 0\})_{\lambda \in \bar{F}_3} \subset \bar{F}_3^{n+1}$$

is not situated in the hypersurface $\mathscr{L}$ (cf. section 2 in Chistov & Grigor'ev, 1983*a*). Arguing by induction on $0 \leqslant j \leqslant n$, we assume that $j < n$ and indices $1 \leqslant i_1 \leqslant \ldots < i_j \leqslant N$ are already found, for which

$$\dim(\mathscr{L} \cap (z^{(3)} + \lambda\{Y_{i_1} = \ldots = Y_{i_j} = 0\})_{\lambda \in \bar{F}_3}) = n - j.$$

There is an index $1 \leqslant i \leqslant N$ such that the linear function $Y_i - Y_i(z^{(3)})$ does not vanish identically on any irreducible component of variety

$$\mathscr{L} \cap (z^{(3)} + \lambda\{Y_{i_1} = \ldots = Y_{i_j} = 0\})_{\lambda \in \bar{F}_3}.$$

Otherwise, on some irreducible component at least $(n+1)$ functions among $Y_1 - Y_1(z^{(3)}), \ldots, Y_N - Y_N(z^{(3)})$ vanish, taking into account that the number of irreducible components is less or equal to

$$\deg(\mathscr{L} \cap (z^{(3)} + \lambda\{Y_{i_1} = \ldots = Y_{i_j} = 0\})_{\lambda \in \bar{F}_3}) \leqslant \deg(\mathscr{L}) \leqslant N_1$$

by virtue of Bezout's inequality (see Shafarevich, 1974; Heintz, 1983). This leads to a contradiction with the property of linear forms $Y_1, \ldots, Y_N$ and proves the existence of the desired index $1 \leqslant i \leqslant N$. Let us add index i to indices $i_1, \ldots, i_j$, reorder them in increasing order and get the indices $1 \leqslant i_1 < \ldots < i_{j+1} \leqslant N$. Therefore, if a point $z^{(3)}$ is defined over the field $\overline{\mathbb{Q}(\varepsilon_1, \varepsilon_3)}$, then the intersection

$$\mathscr{L} \cap (z^{(3)} + \lambda\{Y_{i_1} = \ldots = Y_{i_n} = 0\})_{\lambda \in \bar{F}_3}$$

consists of a finite number of points which are defined over the field $\overline{\mathbb{Q}(\varepsilon_1, \varepsilon_3)}$.

For any sequence of indices $1 \leqslant i_1 < \ldots < i_n \leqslant N$, let us pick out an arbitrary vector $0 \neq v_{i_1, \ldots, i_n} \in \mathbb{Q}^{n+1}$ lying on the line $\{Y_{i_1} = \ldots = Y_{i_n} = 0\} \subset \bar{F}_3^{n+1}$. Furthermore, we require that one of the coefficients of vector $v_{i_1, \ldots, i_n}$ equals 1. Then for any point $z \in \mathbb{Q}^{n+1}$ there exists a sequence of indices $1 \leqslant i_1 < \ldots < i_n \leqslant N$ such that point $z^{(2)} = z + \varepsilon_2 v_{i_1, \ldots, i_n} \in F_2^{n+1}$ does not belong to the hypersurface $\mathscr{L}$, taking into account that the point $z^{(2)}$ is not defined over the field $\overline{\mathbb{Q}(\varepsilon_1, \varepsilon_3)}$. According to lemmas 8, 9 point $z^{(2)} \in F_2^{n+1} \backslash \mathscr{L}$ satisfies formula (6) iff there is a vector $\gamma \in \Gamma$, an irreducible factor $\Omega | \psi_0$ and a root $\theta^{(0)} \in F_3$ of the polynomial $\Phi(z^{(2)})(T) \in \tilde{\mathbb{Q}}(\varepsilon_1, \varepsilon_2, \varepsilon_3)[T]$ for which the inequalities

$$f_i\left(z^{(2)}, \sum_j \frac{a_j^{(1)}(z^{(2)})}{b(z^{(2)})} (\theta^{(0)})^j, \ldots, \sum_j \frac{a_j^{(s)}(z^{(2)})}{b(z^{(2)})} (\theta^{(0)})^j\right) + \varepsilon_1 > 0, \quad 0 \leqslant i \leqslant k$$

are valid. Here, we use the observation that the point

$$\left(\sum_j \frac{a_j^{(1)}(z^{(2)})}{b(z^{(2)})}(\theta^{(0)})^j, \ldots, \sum_j \frac{a_j^{(s)}(z^{(2)})}{b(z^{(2)})}(\theta^{(0)})^j\right) \in \bar{F}_3^s,$$

where $\Phi(z^{(2)})(\theta^{(0)}) = 0$, belongs to the space F_3^s iff $\theta^{(0)} \in F_3$ since

$$\theta^{(0)} = \sum_{1 \leqslant i \leqslant s} \lambda_i \left(\sum_j \frac{a_j^{(i)}(z^{(2)})}{b(z^{(2)})}(\theta^{(0)})^j\right)$$

by virtue of lemma 9. We recall also that lemma 9 implies that the linear form

$$L^{(\theta^{(0)})}(z^{(2)}) = \left(u_0 + \sum_{1 \leqslant i \leqslant s} \left(\sum_j \frac{a_j^{(i)}(z^{(2)})}{b(z^{(2)})}(\theta^{(0)})^j\right) u_i\right) \in F_3[u_0, \ldots, u_s]$$

divides the polynomial $\Omega(z^{(2)})$. Thus, in view of lemma 6(c) we have proved the following lemma, in which we use introduced above notations.

LEMMA 10. *A point $z \in \tilde{\mathbb{Q}}^{n+1}$ satisfies formula (5) iff there exist a sequence of indices $1 \leqslant i_1 < \ldots < i_n \leqslant N$ such that the point $z^{(2)} = z + \varepsilon_2 v_{i_1, \ldots, i_n} \notin \mathcal{L}$. Furthermore, a vector $\gamma \in \Gamma$, a factor Ω of Ψ_0 irreducible over $\mathbb{Q}$ and, finally, a root $T = \theta^{(0)} \in F_3$ of the polynomial $\phi(z^{(2)})(T)$, where the polynomial Φ is associated with the factor Ω, such that the inequalities*

$$f_i\left(z^{(2)}, \sum_j \frac{a_j^{(1)}(z^{(2)})}{b(z^{(2)})}(\theta^{(0)})^j, \ldots, \sum_j \frac{a_j^{(s)}(z^{(2)})}{b(z^{(2)})}(\theta^{(0)})^j\right) + \varepsilon_1 > 0, \quad 0 \leqslant i \leqslant k$$

are fulfilled. Here, the linear form

$$L^{(\theta)} = u_0 + \sum_{1 \leqslant i \leqslant s} \left(\sum_j \frac{a_j^{(i)}}{b}\theta^j\right) u_i$$

being a factor of the polynomial Ω was constructed by the algorithm described above. Furthermore, the point

$$\left(\sum_j \frac{a_j^{(1)}(z^{(2)})}{b(x^{(2)})}(\theta^{(1)})^j, \ldots, \sum_j \frac{a_j^{(s)}(z^{(2)})}{b(z^{(2)})}(\theta^{(1)})^j\right) \in \bar{F}_3^s$$

is a solution of system (7) for every root $\theta^{(1)} \in \bar{F}_3$ of the polynomial $\Phi(z^{(2)})(T)$.

4. Verifying Formulas of Tarski Algebra

In lemma 10 a formula of the kind $\exists\, T(P_1)$ is produced which is equivalent to formula (5) (over $\tilde{\mathbb{Q}}$, i.e. both formulas determine the same set in $\tilde{\mathbb{Q}}^{n+1}$), where P_1 is a quantifier-free formula of Tarski algebra with atomic subformulas of the sort $(g_j \geqslant 0)$, with polynomials $g_j \in \mathbb{Q}[\varepsilon_1, \varepsilon_2, \varepsilon_3][T, Z_0, \ldots, Z_n]$.

Applying the construction from section 2 in Wüthrich (1976) (see also Collins, 1975) to the family of polynomials $\{g_j\}_j$ (which are considered over the real closed field F_3) and to the variable T, one gets a family of polynomials $\{p_e\}_e$, where $p_e \in \mathbb{Q}[\varepsilon_1, \varepsilon_2, \varepsilon_3][Z_0, \ldots, Z_n]$ which satisfies the following property (see theorem 1 in Wüthrich, 1976 and theorem 5 in Collins, 1975). For every element $W^{(\varepsilon)} \subset F_3^{n+1}$ of the partition $\mathcal{U}(\{p_e\}_e)$ (see section 1) there exists a sequence of semialgebraic functions $q_1, \ldots, q_t \colon W^{(\varepsilon)} \to F_3$ continuous on $W^{(\varepsilon)}$ (with respect to the topology with the base of all open balls), such that $q_1 < \ldots < q_t$ and the partition, formed by the components of connectivity of the intersection of all elements of the partition $\mathscr{U}(\{g_j\}_j)$ with the cylinder $F_3 \times W^{(\varepsilon)} \subset F_3^{n+2}$, coincides with the following partition of the cylinder:

$$F_3 \times W^{(\varepsilon)} = \{T < q_1(Z_0, \ldots, Z_n)\} \cup \{T > q_t(Z_0, \ldots, Z_n)\} \cup \bigcup_{1 \leqslant i \leqslant t-1} \{q_i(Z_0, \ldots, Z_n) < T < q_{i+1}(Z_0, \ldots, Z_n)\} \cup \bigcup_{1 \leqslant i \leqslant t} \{T = q_i(Z_0, \ldots, Z_n)\}.$$

As above (see section 2), one bounds the formats of the semialgebraic functions $q_1, \ldots, q_t$ via the formats of $\{p_e\}_e$ in the case of the field $\mathbb{R}$ and then spread these bounds and the properties of $q_1, \ldots, q_t$ to the field F_3 according to the transfer principle.

Let us denote

$$p_e = \sum_{j_1, j_2, j_3} p_e^{(j_1, j_2, j_3)} \varepsilon_1^{j_1} \varepsilon_2^{j_2} \varepsilon_3^{j_3},$$

where the polynomials $p_e^{(j_1, j_2, j_3)} \in \mathbb{Q}[Z_0, \ldots, Z_n]$ (cf. section 2). We denote by $\pi_1 : \tilde{\mathbb{Q}}^{s+n+1} \to \tilde{\mathbb{Q}}^{n+1}$ the linear projection defined by the formula

$$\pi_1(Z_0, \ldots, Z_n, X_1, \ldots, X_s) = (Z_0, \ldots, Z_n).$$

In the following lemma we use the notations from the previous section.

Lemma 11. *Let a point $(z^{(0)}, x^{(0)}) = (z_0^{(0)}, \ldots, z_n^{(0)}, x_1^{(0)}, \ldots, x_s^{(0)})$ belong to some component of connectivity V_1 of the semialgebraic set*

$$V = \{(f_0 \geqslant 0) \& \ldots \& (f_k \geqslant 0)\} \subset \tilde{\mathbb{Q}}^{s+n+1}$$

and the point $z^{(0)} = \pi_1(z^{(0)}, x^{(0)}) \in W$, where $W \subset \tilde{\mathbb{Q}}^{n+1}$ is a certain element of the partition $\mathscr{U}(\{p_e^{(j_1, j_2, j_3)}\}_{e, j_1, j_2, j_3})$. Then the projection $\pi_1(V_1) \supset W$.

Proof. In view of the properties of the vectors $\{v_{i_1, \ldots, i_n}\}$ constructed in the previous section, there exist indices $1 \leqslant i_1 < \ldots < i_n \leqslant N$ such that $z^{(2)} = z^{(0)} + \varepsilon_2 v_{i_1, \ldots, i_n} \notin \mathscr{L}$ (cf. lemma 10). According to lemma 5(c) there is a unique element $V_2^{(\varepsilon)} \subset F_3^{s+n+1}$ of the partition $\mathscr{U}(g, f_0 + \varepsilon_1, \ldots, f_k + \varepsilon_1)$ which contains the component $V_1 \subset V_2^{(\varepsilon)}$. Lemma 6(a) entails the inclusion $V \subset \{g \geqslant 0\} \cap V^{(\varepsilon)}$, where

$$V^{(\varepsilon)} = \{(f_0 + \varepsilon_1 > 0) \& \ldots \& (f_k + \varepsilon_1 > 0)\} \subset F_3^{s+n+1},$$

therefore $V_2^{(\varepsilon)} \subset \{g \geqslant 0\} \cap V^{(\varepsilon)}$. Let us denote by $V_1^{(\varepsilon)}$ the unique component of connectivity of the semialgebraic set $\{g \geqslant 0\} \cap V^{(\varepsilon)}$ which contains the set $V_2^{(\varepsilon)} \subset V_1^{(\varepsilon)}$. Thus $V_1^{(\varepsilon)} \supset V_1$.

By virtue of lemma 6(c) one can find a point $(z^{(2)}, \tilde{x}) \in V_1^{(\varepsilon)}$ such that $g(z^{(2)}, \tilde{x}) = 0$ and $(z^{(0)}, st(\tilde{x})) \in V_1$. Let $V_3^{(\varepsilon)}$ be the unique component of connectivity of the variety $\{g = 0\} \subset F_3^{s+n+1}$, which contains the point $(z^{(2)}, \tilde{x}) \in V_3^{(\varepsilon)}$. Then $V_3^{(\varepsilon)} \subset V_1^{(\varepsilon)}$ in view of lemma 6(b). Consider the unique component of connectivity $V_4^{(\varepsilon)}$ of the semialgebraic set

$$\{(z^{(2)}, y) : y \in F_3^s, g(z^{(2)}, y) = 0\} \subset F_3^{s+n+1},$$

which contains point $(z^{(2)}, \tilde{x}) \in V_4^{(\varepsilon)}$. Obviously, $V_4^{(\varepsilon)} \subset V_3^{(\varepsilon)}$. Note that

$$V_4^{(\varepsilon)} \subset \mathscr{D}_{(z^{(2)}, 0)}((z_0^{(0)} + 2\varepsilon_1)^{1/2}),$$

since $f_0(u) + \varepsilon_1 > 0$ for any point $u \in V_4^{(\varepsilon)} \subset V_1^{(\varepsilon)}$.

Lemma 7(a), (b) implies the existence of a vector $\gamma \in \Gamma$ such that system (7) has a solution $x = (x_1, \ldots, x_s) \in F_3^s$ where point $(z^{(2)}, x) \in V_4^{(\varepsilon)}$. Moreover, point x is isolated in the variety of all the solutions of system (7) in the space $\bar{F}_3^s$. Hence, the linear form $u_0+x_1u_1+\ldots+x_su_s$ divides the polynomial $\psi_0(z^{(2)})$, where $\psi_0\in\mathbb{Q}[\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0, \ldots, u_s]$ (see systems (8), (8′) and lemma 8). Consider some irreducible (over $\mathbb{Q}$) factor $\Omega\in\mathbb{Q}[\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0, \ldots, u_s]$ of the polynomial ψ_0 for which $(u_0+x_1u_1+\ldots+x_su_s)|\Omega(z^{(2)})$.

Let $W^{(\varepsilon)}$ be the unique element of the partition $\mathscr{U}(\{p_e\}_e)$ such that $z^{(0)}\in W^{(\varepsilon)}$. Lemma 5(b) entails the inclusion $W\subset W^{(\varepsilon)}$. For a point $z\in W^{(\varepsilon)}$ and an element $\theta\in F_3$ we denote

$$(\theta, \mathrm{z})_{\gamma,\Omega,i_1,\ldots,i_n}=\left(z+\varepsilon_2 v_{i_1,\ldots,i_n}, \sum_j \frac{a_j^{(1)}(z+\varepsilon_2 v_{i_1,\ldots,i_n})}{b(z+\varepsilon_2 v_{i_1,\ldots,i_n})}\,\theta^j, \ldots,\right.$$

$$\left.\sum_j \frac{a_j^{(s)}(z+\varepsilon_2 v_{i_1,\ldots,i_n})}{\beta(z+\varepsilon_2 v_{i_1,\ldots,i_n})}\,\theta^j\right)\in F_3^{s+n+1}$$

(see lemma 10). According to lemma 9 and to the construction of a primitive element in section 3, there is a root $\theta^{(0)}\in F_3$ of polynomial $\Phi(z^{(2)})(T)$, for which $(z^{(2)}, x)=(\theta^{(0)}, z^{(0)})_{\gamma,\Omega,i_1,\ldots,i_n}$, furthermore,

$$\theta^{(0)}=\sum_{1\leqslant i\leqslant s}\lambda_i x_i$$

for suitable natural numbers $1\leqslant\lambda_i\leqslant\deg_{u_0,\ldots,u_s}(\Omega)$. Since point x is a solution of system (7), the following equality in particular is fulfilled:

$$g((\theta^{(0)}, z^{(0)})_{\gamma,\Omega,i_1,\ldots,i_n})=0. \tag{10}$$

Moreover, taking into account that point $(z^{(2)}, x)\in V_4^{(\varepsilon)}\subset V_1^{(\varepsilon)}\subset V^{(\varepsilon)}$ belongs to $V^{(\varepsilon)}$ the following inequalities are true:

$$f_i((\theta^{(0)}, z^{(0)})_{\gamma,\Omega,i_1,\ldots,i_n})+\varepsilon_1>0;\quad 0\leqslant i\leqslant k. \tag{11}$$

Consider the unique element $G_1\subset F_3^{n+2}$ of the partition $\mathscr{U}(\{g_j\}_j)$ which contains point $(\theta^{(0)}, z^{(0)})\in \mathrm{G}_1$. In view of the definition of partition $\mathscr{U}(\{g_j\}_j)$ and of lemma 10 for an arbitrary point $(\theta, z)\in G_1$ the value of polynomial $b(z+\varepsilon_2 v_{i_1,\ldots,i_n})\neq 0$ and, moreover, the conditions obtained from (10), (11) by replacing the point $(\theta^{(0)}, z^{(0)})$ by the point (θ, z), respectively, are valid for the given $\gamma, \Omega, i_1, \ldots, i_n$. Furthermore, $y\in F_3^s$, where

$$(z+\varepsilon_2 v_{i_1,\ldots,i_n}, y)=(\theta, z)_{\gamma,\Omega,i_1\ldots,i_n}$$

satisfies system (7) by virtue of lemmas 8, 9.

One can observe that the intersection $G_1\cap(F_3\times W^{(\varepsilon)})$ coincides with a union of some sets of the sort $\{(q_{m_1}(z), z)\}_{z\in W^{(\varepsilon)}}$, where z runs over all points of the set $W^{(\varepsilon)}$ for appropriate indices $1\leqslant m_1\leqslant t$ (see above the beginning of the present section). Otherwise, suppose that

$$G_1\cap(F_3\times W^{(\varepsilon)})\supset\{(\theta, z): q_{m_1}(z)<\theta<q_{m_1+1}(z)\}$$

for a certain m_1, then for any point $z\in W$ (for instance, one can take $z=z^{(0)}$), there are infinitely many points of the kind $(\theta^{(1)}, z)\in G_1$, but on the other hand, every such $\theta^{(1)}$ is a root of polynomial $\Phi(z+\varepsilon_2 v_{i_1,\ldots,i_n})(T)$ (see lemma 10), that leads to contradiction. Consider such unique index $1\leqslant m\leqslant t$ that

$$G_1\cap(F_3\times W^{(\varepsilon)})\supset\{(q_m(z), z)\}_{z\in W^{(\varepsilon)}}$$

and point $(\theta^{(0)}, z^{(0)})\in\{(q_m(z), z)\}_{z\in W^{(\varepsilon)}}$. Let us define $q=q_m$ for brevity.

For any point $z^{(1)}\in W$ the standard part $st((q(z^{(1)}), \mathrm{z}^{(1)})_{\gamma,\Omega,i_1,\ldots,i_n})\in\tilde{\mathbb{Q}}^{s+n+1}$ is defined, since $f_0((q(z^{(1)}), z^{(1)})_{\gamma,\Omega,i_1,\ldots,i_n})+\varepsilon_1>0$ (cf. (4)), taking into account that for a point $z\in W^{(\varepsilon)}$ a point $(q(z), z)\in G_1$ satisfies the inequalities obtained from (11) by replacing point $(\theta^{(0)}, z^{(0)})$ by point $(q(z), z)$. Therefore,

$$0\leqslant st(f_i((q(z), z)_{\gamma,\Omega,i_1,\ldots,i_n}))=f_i(st((q(z), z)_{\gamma,\Omega,i_1,\ldots,i_n})),\quad 0\leqslant i\leqslant k,$$

provided that $st((q(z), z)_{\gamma,\Omega,i_1,\ldots,i_n})$ is defined. This means that point $st((q(z), z)_{\gamma,\Omega,i_1,\ldots,i_n})\in V$. For the completion of the proof of the lemma it suffices to show that for any point $z^{(1)}\in W$ point $st((q(z^{(1)}), z^{(1)})_{\gamma,\Omega,i_1,\ldots,i_n})$ belongs to V_1, taking into account that

$$\pi_1(st((q(z^{(1)}), z^{(1)})_{\gamma,\Omega,i_1,\ldots,i_n}))=z^{(1)}.$$

Let us fix an arbitrary point $z^{(1)}\in W$. By means of lemma 3(b) one can join the points $z^{(0)}, z^{(1)}\in W$ by a closed connected semialgebraic curve $z^{(0)}, z^{(1)}\in C\subset W\cap\mathscr{D}_0(R)$, where $R\in\mathbb{Q}$. In view of lemmas 4(a), 5(a) there exists such a closed connected semialgebraic curve $C^{(\varepsilon)}\subset W^{(\varepsilon)}\cap\mathscr{D}_0(R)$ that $C^{(\varepsilon)}\supset st(C^{(\varepsilon)})=C$. Consider the image $\rho(C^{(\varepsilon)})$ of the curve $C^{(\varepsilon)}$ under the action of the continuous on $W^{(\varepsilon)}$ semialgebraic mapping

$$\rho: z\to(q(z), z)_{\gamma,\Omega,i_1,\ldots,i_n}\in F_3^{s+n+1}.$$

Lemma 3(a) entails that $\rho(C^{(\varepsilon)})\subset F_3^{s+n+1}$ is a connected semialgebraic curve.

We claim that $\rho(C^{(\varepsilon)})\subset\mathscr{D}_0(R+1)$. Indeed, let us denote

$$\rho(z)=\rho(z_0,\ldots,z_n)=(z+\varepsilon_2 v_{i_1,\ldots,i_n}, y)$$

for an arbitrary point $z\in C^{(\varepsilon)}$. Then the euclidean norm $\|z\|\leqslant R$, furthermore,

$$\|\rho(z)\|^2=\|z+\varepsilon_2 v_{i_1,\ldots,i_n}\|^2+\|y\|^2<\|z\|^2+z_0+2\varepsilon_1<R^2+R+1$$

by virtue of inequality (11) in the case $i=0$ for the point $(q(z), z)\in G_1$. This proves the claim. Hence, the standard part $st(\rho(C^{(\varepsilon)}))\subset\tilde{\mathbb{Q}}^{s+n+1}$ is defined and $st(\rho(C^{(\varepsilon)}))\subset V$, according to inequalities (11) (cf. above).

The projection $\pi_1(st(\rho(C^{(\varepsilon)})))\subset\tilde{\mathbb{Q}}^{n+1}$ contains both points $z^{(0)}, z^{(1)}$, since $C^{(\varepsilon)}\supset C$ and $\pi_1(st(\rho(z)))=z$ for any point $z\in C\subset W$. To complete the proof of the lemma it remains to show the inclusion $st(\rho(C^{(\varepsilon)}))\subset V_1$. In view of lemma 4(b) it suffices to check that $st(\rho(C^{(\varepsilon)}))\cap V_1\neq\phi$, taking into account that the curve $\rho(C^{(\varepsilon)})\subset\mathscr{D}_0(R+1)$ is connected and $st(\rho(C^{(\varepsilon)}))\subset V$. With the help of lemma 3(b) one can find a closed connected semialgebraic curve $C_1\subset V_4^{(\varepsilon)}$ joining the points $(z^{(2)}, x), (z^{(2)}, \tilde{x})\in C_1$. Then $C_1\subset V_4^{(\varepsilon)}\subset\mathscr{D}_{(z^{(2)},0)}((z_0^{(0)}+2\varepsilon_1)^{1/2})$ (see above). Lemma 6(a) implies the inclusion $st(C_1)\subset V$ since $C_1\subset V_4^{(\varepsilon)}\subset V_3^{(\varepsilon)}\subset V_1^{(\varepsilon)}\subset V^{(\varepsilon)}$. On the other hand, point $st(z^{(2)}, \tilde{x})\in V_1\cap st(C_1)$, hence $st(C_1)\subset V_1$ by virtue of lemma 4(b), in particular, point $st(z^{(2)}, x)\in V_1$. Finally, the equality $(z^{(2)}, x)=\rho(z^{(0)})$ entails

$$st(z^{(2)}, x)=st(\rho(z^{(0)}))\in st(\rho(C^{(\varepsilon)})),$$

i.e.

$$st(z^{(2)}, x)\in V_1\cap st(\rho(C^{(\varepsilon)}))\neq\phi.$$

The lemma is proved.

Now we proceed to the description of the algorithm which verifies formula (1). Let us first design by recursion on $0\leqslant\alpha\leqslant a-1$ (we remind the reader that a is the number of quantifier alternations in formula (1)), a certain procedure consisting of $a-1$ stages. Before the implementation of the first stage the algorithm sets polynomials $g_i^{(0)}=f_i$, $0\leqslant i\leqslant k$ (see formula (1)). As a result of the implementation of α stages of the procedure (we assume here that $\alpha \leqslant a-2$) a family of polynomials $\{g_j^{(\alpha)}\}_j$ is produced, where

$$g_j^{(\alpha)} \in \mathbb{Q}[X_{1,1}, \ldots, X_{1,s_1}, \ldots, X_{a-\alpha, s_{a-\alpha}}].$$

The algorithm enumerates all $(\{g_j^{(\alpha)}\}_j)$-cells $K_1, K_2, \ldots$ based on lemma 1 from section 1.

Let us fix for the time being a certain $(\{g_j^{(\alpha)}\}_j)$-cell K_t and let $K_t = \{\Pi_t\}$ for a suitable quantifier-free formula of Tarski algebra

$$\Pi_t = (\mathop{\&}_{j \in J} (g_j^{(\alpha)} = 0) \,\&\, \mathop{\&}_{j \in J_1} (g_{j_1}^{(\alpha)} > 0) \,\&\, \mathop{\&}_{j_2 \in J_2} (g_{j_2} < 0))$$

(see section 1). Consider the following formula of Tarski algebra

$$\exists X_{a-\alpha, 1} \ldots \exists X_{a-\alpha, s_{a-\alpha}} \Pi_t \tag{12}$$

and let us apply to it the construction from section 3, taking (12) as the input formula (i.e. (12) plays the role of the formula (2) in the construction from section 3). As a result, the algorithm produces a formula of the form $\exists\, T(P_t)$ (see lemma 10). Here the quantifier-free formula P_t has atomic subformulas of the form $(g_{m,t}^{(\alpha+1)} \geqslant 0)$, where the polynomials

$$g_{m,t}^{(\alpha+1)} \in \mathbb{Q}[\varepsilon_1, \varepsilon_2, \varepsilon_3][T, Z_0, X_{1,1}, \ldots, X_{1,s_1}, \ldots, X_{a-\alpha-1,1}, \ldots, X_{a-\alpha-1, s_{a-\alpha-1}}].$$

We recall that (see (4), (5)) formula (12) is equivalent (over the field $\tilde{\mathbb{Q}}$) to formula $\exists Z_0 \in \tilde{\mathbb{Q}}\, \exists\, T \in F_3(P_t)$ (being not a formula of the first-order theory). Observe, that we do not use the latter claim.

As in the beginning of the present section the procedure yields polynomials

$$p_{l,t}^{(\alpha+1)} \in \mathbb{Q}[\varepsilon_1, \varepsilon_2, \varepsilon_3][Z_0, X_{1,1}, \ldots, X_{a-\alpha-1, s_{a-\alpha-1}}]$$

by means of the construction from section 2 in Wüthrich (1976) (see also Collins, 1975), which is applied here to the family of polynomials $\{g_{m,t}^{(\alpha+1)}\}_m$ and to the variable T. Next, we write

$$p_{l,t}^{(\alpha+1)} = \sum_{j_1, j_2, j_3} p_{l,t}^{(\alpha+1)(j_1, j_2, j_3)} \varepsilon_1^{j_1} \varepsilon_2^{j_2} \varepsilon_3^{j_3},$$

as above, where the polynomials

$$p_{l,t}^{(\alpha+1)(j_1, j_2, j_3)} \in \mathbb{Q}[Z_0, X_{1,1}, \ldots, X_{a-\alpha-1, s_{a-\alpha-1}}].$$

Finally, the procedure applies again the construction from section 2 in Wüthrich (1976) to the family $\{p_{l,t}^{(\alpha+1)(j_1, j_2, j_3)}\}_{j_1, j_2, j_3, l, t}$ consisting of polynomials corresponding to the totality of $(\{g_j^{(\alpha)}\}_j)$-cells K_t (cf. formula (12)), and to variable Z_0. As a result, the procedure obtains a family $\{g_i^{(\alpha+1)}\}_i$ of polynomials

$$g_i^{(\alpha+1)} \in \mathbb{Q}[X_{1,1}, \ldots, X_{1,s_1}, \ldots, X_{a-\alpha-1,1}, \ldots, X_{a-\alpha-1, s_{a-\alpha-1}}].$$

This completes the description of the recursive procedure which produces the polynomials $\{g_j^{(\alpha)}\}_{j,\alpha}$. Let us denote by $\{K_t^{(\alpha)}\}_t$ the family of all $(\{g_j^{(\alpha)}\}_j)$-cells. Note that the procedure produces also this family. Let us adopt the convention that for $\alpha = a$, the families $\{K_t^{(a)}\}_t$ and $\{g_j^{(a)}\}_j$ are empty.

Lemma 12. *For any element W of partition $\mathcal{U}(\{g_j^{(\alpha)}\}_j)$ of the space $\tilde{\mathbb{Q}}^{s_1 + \cdots + s_{a-\alpha}}$ its natural projection onto the space $\tilde{\mathbb{Q}}^{s_1 + \cdots + s_{a-\alpha-1}}$ coincides with a union of a suitable collection of elements of partition $\mathcal{U}(\{g_i^{(\alpha+1)}\}_i)$.*

PROOF. Let us denote $n_1 = s_1 + \ldots + s_{a-\alpha-1}$ and consider a commutative diagram

$$\begin{tikzcd} \tilde{\mathbb{Q}}^{n_1+s_{a-\alpha}+2} \arrow[r, "\pi_1"] \arrow[d, "\sigma_2"'] & \tilde{\mathbb{Q}}^{n_1+1} \arrow[d, "\sigma_1"] \\ \tilde{\mathbb{Q}}^{n_1+s_{a-\alpha}} \arrow[r, "\pi_2"] & \tilde{\mathbb{Q}}^{n_1}, \end{tikzcd}$$

where all four mapping are linear projections. The space $\tilde{\mathbb{Q}}^{n_1}$ has coordinates $X_{1,1}, \ldots, X_{a-\alpha-1, s_{a-\alpha-1}}$; the space $\tilde{\mathbb{Q}}^{n_1+1}$ has the additional coordinate Z_0, the space $\tilde{\mathbb{Q}}^{n_1+s_{a-\alpha}}$ has coordinates $X_{1,1}, \ldots, X_{a-\alpha, s_{a-\alpha}}$ and at last the space $\tilde{\mathbb{Q}}^{n_1+s_{a-\alpha}+2}$ has coordinates $X_{1,1}, \ldots, X_{a-\alpha, s_{a-\alpha}}, X_{n_1+s_{a-\alpha}+1}, Z_0$.

The set $W \subset \tilde{\mathbb{Q}}^{n_1+s_{a-\alpha}}$ is a component of connectivity of a certain $(\{g_j^{(\alpha)}\}_j)$-cell K_t being given by a quantifier-free formula

$$\Pi_t = (\mathop{\&}_{j \in J} (g_j^{(\alpha)} = 0) \& \mathop{\&}_{j_1 \in J_1} (g_{j_1}^{(\alpha)} > 0) \& \mathop{\&}_{j_2 \in J_2} (g_{j_2}^{(a)} < 0))$$

(cf. (12) above). Let us introduce a semialgebraic set $U_t \subset \tilde{\mathbb{Q}}^{n_1+s_{a-\alpha}+2}$, which is given by a formula

$$\Pi_t \& (X_{n_1+s_{a-\alpha}+1} (\prod_{j_1 \in J_1} g_{j_1}^{(\alpha)})(\prod_{j_2 \in J_2} (-g_{j_2}^{(\alpha)})) \geqslant 1) \& \\ (Z_0 - X_{n_1+s_{a-\alpha}+1}^2 - X_{a-\alpha,1}^2 - \ldots - X_{a-\alpha, s_{a-\alpha}}^2 \geqslant 0)$$

(cf. formulas (3), (4), herein variable $X_{n_1+s_{a-\alpha}+1}$ plays a role similar to the role of variable X_s in formula (3)). Then $\sigma_2(U_t) = K_t$.

For any point $x \in K_t$ the intersection $\sigma_2^{-1}(x) \cap U_t \subset \sigma_2^{-1}(x) \simeq \tilde{\mathbb{Q}}^2$ of its inverse image with set U_t is a connected semialgebraic set. We show that semialgebraic set $\sigma_2^{-1}(W) \cap U_t \subset \tilde{\mathbb{Q}}^{n_1+s_{a-\alpha}+2}$ is connected. Indeed, let us pick out an arbitrary pair of points $x^{(1)}, x^{(2)} \in W$. According to lemma 3(b) one can find a closed connected semialgebraic curve $C \subset W \cap \mathcal{D}_0(R)$ joining the points $x^{(1)}, x^{(2)} \in C$ for a certain $R \in \mathbb{Q}$. Then set

$$\left\{\left(c = (x_{1,1}, \ldots, x_{a-\alpha, s_{a-\alpha}}), \left(\prod_{j_1 \in J_1} (g_{j_1}^{(\alpha)}(c)) \prod_{j_2 \in J_2} (-g_{j_2}^{(\alpha)}(c))\right)^{-1}, \right.\right. \\ \left.\left. \left(\prod_{j_1 \in J_1} (g_{j_1}^{(\alpha)}(c)) \prod_{j_2 \in J_2} (-g_{j_2}^{(\alpha)}(c))\right)^{-2} + x_{a-\alpha,1}^2 + \ldots + x_{a-\alpha, s_{a-\alpha}}^2\right)\right\}_{c \in C} \subset U_t$$

is a connected semialgebraic curve by virtue of lemma 3(a) and, furthermore, the projection of this curve under the projection σ_2 contains points $x^{(1)}, x^{(2)}$. This implies, in view of the arbitrariness of the choice of points $x^{(1)}, x^{(2)}$, that there is a unique component of connectivity $\mathscr{W}$ of the set U_t such that $\sigma_2(\mathscr{W}) = W$ and, moreover, $\sigma_2^{-1}(W) \cap U_t = \mathscr{W}$.

Lemma 11 entails that the projection

$$\pi_1(\mathscr{W}) = \bigcup_{\beta} \mathscr{V}_{\beta}^{(1)} \subset \tilde{\mathbb{Q}}^{n_1+1}$$

coincides with a union of an appropriate collection of elements $\mathscr{V}_{\beta}^{(1)}$ of the partition $\mathscr{U}(\{p_{l,t}^{(\alpha+1)(j_1, j_2, j_3)}\}_{j_1, j_2, j_3, l})$ for the given t. *A fortiori*

$$\pi_1(\mathscr{W}) = \bigcup_{\nu} \mathscr{V}_{\nu}$$

coincides with a union of a suitable collection of elements $\mathscr{V}_{\nu}$ of a finer partition $\mathscr{U}(\{p_{l,t}^{(\alpha+1)(j_1, j_2, j_3)}\}_{j_1, j_2, j_3, l, t})$. According to theorem 1 from Wüthrich (1976) (see also Collins, 1975), the projection

$$\sigma_1(\mathscr{V}_\nu) = \bigcup_{\varkappa} \mathscr{V}_{\nu,\varkappa} \subset \tilde{\mathbb{Q}}^{n_1}$$

coincides with a union of a certain collection of elements $\mathscr{V}_{\nu,\varkappa}$ of the partition $\mathscr{U}(\{g_i^{(\alpha+1)}\}_i)$. Thus,

$$\pi_2(W) = \pi_2\sigma_2(\mathscr{W}) = \sigma_1\pi_1(\mathscr{W}) = \bigcup_{\nu,\varkappa} \mathscr{V}_{\nu,\varkappa},$$

which completes the proof of the lemma.

Now we describe one more recursive process, consisting of a stages. At the first stage it applies lemma 2 from section 1 to a family of polynomials $\{g_i^{(a-1)}\}_i$. As a result, the process produces a representative set $\{w_{m_1}^{(a-1)}\}_{m_1} \subset \tilde{\mathbb{Q}}^{s_1}$ for the partition $\mathscr{U}(\{g_i^{(a-1)}\}_i)$ (see section 1).

Assume that for a certain $1 \leqslant \beta \leqslant a-1$ a finite set of points

$$\{w_{m_1,\ldots,m_\beta}^{(a-\beta)}\}_{m_1,\ldots,m_\beta} \subset \tilde{\mathbb{Q}}^{s_1+\ldots+s_\beta}$$

is already produced by recursion. For each point $w_{m_1,\ldots,m_\beta}^{(a-\beta)}$ the process applies lemma 2 to the intersection of partition $\mathscr{U}(\{g_i^{(a-\beta-1)}\}_i)$ with the $s_{\beta+1}$-dimensional plane

$$\Xi_{m_1,\ldots,m_\beta} = \{(w_{m_1,\ldots,m_\beta}^{(a-\beta)}, x) : x \in \tilde{\mathbb{Q}}^{s_{\beta+1}}\} \subset \tilde{\mathbb{Q}}^{s_1+\ldots+s_{\beta+1}},$$

in other words, lemma 2 is applied to a family of polynomials (in the notations of lemma 2)

$$\{\hat{g}_i\}_i = \{g_i^{(a-\beta-1)}(w_{m_1,\ldots,m_\beta}^{(a-\beta)}, X)\}_i,$$

where polynomial

$$g_i^{(a-\beta-1)}(w_{m_1,\ldots,m_\beta}^{(a-\beta)}, X) \in \tilde{\mathbb{Q}}[X_{\beta+1,1}, \ldots, X_{\beta+1,s_{\beta+1}}].$$

As a result, the process gets a representative set

$$\{(w_{m_1,\ldots,m_\beta}^{(a-\beta)}, w_{m_{\beta+1}})\}_{m_{\beta+1}} = \{w_{m_1,\ldots,m_\beta,m_{\beta+1}}^{(a-\beta-1)}\}_{m_{\beta+1}} \subset \tilde{\mathbb{Q}}^{s_1+\ldots+s_{\beta+1}}$$

for the partition formed by the components of connectivity of the intersections of all elements of partition $\mathscr{U}(\{g_i^{(a-\beta-1)}\}_i)$ with the plane $\Xi_{m_1,\ldots,m_\beta}$.

By means of the following lemma one can easily complete the decision algorithm for Tarski algebra (cf. theorem 3 in Wüthrich, 1976).

Lemma 13. *Formula* (1) *is equivalent to quantifier-free formula*

$$\bigvee_{m_1} \mathop{\&}_{m_2} \ldots \bigvee_{m_a} P(w_{m_1,m_2,\ldots,m_a}^{(0)}). \tag{13}$$

Proof. We shall prove by induction on $0 \leqslant \alpha \leqslant a$ that for all points $x, w_{m_1,\ldots,m_{a-\alpha}}^{(\alpha)} \in K_t^{(\alpha)}$, which belong to the same element of partition $\mathscr{U}(g_j^{(\alpha)}\}_j)$, the following formula of Tarski algebra (depending on point x)

$$\begin{gathered}\exists X_{a-\alpha+1,1} \ldots \exists X_{a-\alpha+1,s_{a-\alpha+1}} \exists X_{a-\alpha+2,1} \ldots \exists X_{a-\alpha+2,s_{a-\alpha+2}} \ldots \\ \exists X_{a,1} \ldots \exists X_{a,s_a}(P(x, X_{a-\alpha+1,1}, \ldots, X_{a-\alpha+1,s_{a-\alpha+1}}, \ldots, X_{a,1}, \ldots, X_{a,s_a}))\end{gathered} \tag{$1_x^{(\alpha)}$}$$

is equivalent to the quantifier-free formula (depending on indices $m_1, \ldots, m_{a-\alpha}$)

$$\bigvee_{m_{a-\alpha+1}} \neg \bigvee_{m_{a-\alpha+2}} \neg \ldots \bigvee_{m_a} (P(w_{m_1,\ldots,m_a}^{(0)})) \tag{$13_{m_1,\ldots,m_{a-\alpha}}^{(\alpha)}$}$$

Note that formula $(1^{(a)})$ (respectively $(13^{(a)})$) is identical with formula (1) (respectively with (13)).

The induction basis for $\alpha = 0$ can be deduced from the fact that the truth value of formula $P(x)$ for a point $x \in \tilde{\mathbb{Q}}^{s_1 + \dots + s_a}$ is determined uniquely by signs

$$\operatorname{sgn} f_i(x) = \operatorname{sgn} g_i^{(0)}(x) = \operatorname{sgn} g_i^{(0)}(w^{(0)}_{m_1, \dots, m_a}) = \operatorname{sgn} f_i(w^{(0)}_{m_1, \dots, m_a})$$

for all $1 \leqslant i \leqslant k$. Let us observe that here we did not exploit the statement that in every element of partition $\mathscr{U}(\{g_i^{(0)}\}_i)$ one can find at least one point of the sort $w^{(0)}_{m_1, \dots, m_a}$ (a proof of this statement can be extracted from the further proof of the present lemma).

Suppose that the equivalence of formulas $(1_y^{(\alpha)})$ and $(13^{(\alpha)}_{m_1, \dots, m_{a-\alpha}})$ is already proved for arbitrary points y and $w^{(\alpha)}_{m_1, \dots, m_{a-\alpha}}$ which belong to the same element of the partition $\mathscr{U}(\{g_j^{(\alpha)}\}_j)$. Consider points $x, w^{(\alpha+1)}_{m_1, \dots, m_{a-\alpha-1}} \in \mathscr{W}$, where $\mathscr{W}$ is a certain element of partition $\mathscr{U}(\{g_i^{(\alpha+1)}\}_i)$. Assume that the plane $\Xi_{m_1, \dots, m_{a-\alpha-1}}$ has a nonempty intersection with some element W of partition $\mathscr{U}(\{\beta_j^{(\alpha)}\}_j)$. The image $\pi_2(W)$ under projection

$$\pi_2 : \tilde{\mathbb{Q}}^{s_1 + \dots + s_{a-\alpha}} \rightarrow \tilde{\mathbb{Q}}^{s_1 + \dots + a_{a-\alpha-1}}$$

coincides with a union

$$\pi_2(W) = \bigcup_{\nu, \varkappa} \mathscr{V}_{\nu, \varkappa}$$

of a suitable collection of elements $\mathscr{V}_{\nu, \varkappa}$ of partition $\mathscr{U}(\{g_i^{(\alpha+1)}\}_i)$ by virtue of lemma 12.

According to the process of construction of the points $\{w^{(\alpha)}_{m_1, \dots, m_{a-\alpha-1}, m_{a-\alpha}}\}_{m_{a-\alpha}}$ there exists such an index m that

$$w^{(\alpha)}_{m_1, \dots, m_{a-\alpha-1}, m} \in W \cap \Xi_{m_1, \dots, m_{a-\alpha-1}}.$$

Since

$$\pi_2(w^{(\alpha)}_{m_1, \dots, m_{a-\alpha-1}, m}) = w^{(\alpha+1)}_{m_1, \dots, m_{a-\alpha-1}},$$

the intersection $\pi_2(W) \cap \mathscr{W} \neq \phi$. Hence, $\mathscr{W} = \mathscr{V}_{\nu, \varkappa} \subset \pi_2(W)$ for appropriate indices $\nu, \varkappa$. Therefore, one can find a point $x_W \in W$ with the projection $\pi_2(x_W) = x$.

So assume that formula $(13^{(\alpha+1)}_{m_1, \dots, m_{a-\alpha-1}})$ is valid, then for a suitable index $m_{a-\alpha}$ the formula $(13^{(\alpha)}_{m_1, \dots, m_{a-\alpha-1}, m_{a-\alpha}})$ is false. Let point $w^{(\alpha)}_{m_1, \dots, m_{a-\alpha-1}, m_{a-\alpha}} \in W_1$ for a relevant element W_1 of partition $\mathscr{U}(g_j^{(\alpha)}\}_j)$. Then $\pi_2(x_{W_1}) = x$ for a certaint $x_{W_1} \in W_1$ in view of the fact proved above. The inductive hypothesis implies that formula $(1^{(\alpha)}_{x_{w1}})$ is false. This entails the truth of formula $(1_x^{(\alpha+1)})$, which was to be shown.

Conversely, suppose that formula $(1_x^{(\alpha+1)})$ is valid, then there exist $x_1, \dots, x_{s_{a-\alpha}} \in \tilde{\mathbb{Q}}$ such that formula $(1_{\tilde{x}}^{(\alpha)})$ is false, where we denote a point

$$\tilde{x} = (x, (x_1, \dots, x_{s_{a-\alpha}})) \in \tilde{\mathbb{Q}}^{s_1 + \dots + s_{a-\alpha}}.$$

Let the point $\tilde{x} \in W_1$ for a suitable element W_1 of the partition $\mathscr{U}(\{g_j^{(\alpha)}\}_j)$. Taking into account that $\pi_2(\tilde{x}) = x$, one concludes that $\pi_2(W_1) \cap \mathscr{W} \neq \phi$, whence $\mathscr{W} \subset \pi_2(W_1)$ by virtue of lemma 12 (cf. above), in particular point $w^{(\alpha+1)}_{m_1, \dots, m_{a-\alpha-1}} \in \pi_2(W_1)$. Thus, there is an index $m_{a-\alpha}$ for which point $w^{(\alpha)}_{m_1, \dots, m_{a-\alpha-1}, m_{a-\alpha}} \in W_1$ (see above). Then formula $(13^{(\alpha)}_{m_1, \dots, m_{a-\alpha-1}, m_{a-\alpha}})$ is false according to the inductive hypothesis. Therefore, formula $(13^{(\alpha+1)}_{m_1, \dots, m_{a-\alpha-1}})$ is true, which completes the proof of the lemma.

5. Time Analysis of the Decision Algorithm

First of all we estimate the time required for the algorithm in section 3 constructing the formula $\exists\, T(P_1)$ (see lemma 10) and the size of this formula. Let formula (2) be given. In the beginning, the algorithm yields the family of vectors $\Gamma \subset \mathbb{Z}^{s-1}$. According to Grigor'ev & Vorobjov (1987) (see also Vorobjov & Grigor'ev, 1985) $\operatorname{card}(\Gamma) \leqslant \mathscr{P}((kd)^{s^2})$.

Furthermore, for each vector $(\gamma_2, \ldots, \gamma_s) \in \Gamma$ the inequalities $1 \leqslant \gamma_i \leqslant \mathscr{P}((kd)^s)$, $2 \leqslant i \leqslant s$ are correct; finally, the algorithm yields the family Γ within time $\mathscr{P}((kd)^{s^2})$.

Next, the algorithm constructs the matrix A with entries in the ring $\mathbb{Q}[\varepsilon_1, \varepsilon_3][Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s]$ corresponding to system (8′) (see proposition 7) and applies to it the Gaussian algorithm. As a result, the polynomials

$$\psi_1, P_1 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s]$$

are produced. The number τ of rows of the matrix $A = (a_{ij})$ can be estimated by $\tau \leqslant \mathscr{P}((kd)^s)$, each entry a_{ij} of A is of degree

$$\deg_{\varepsilon_1, \varepsilon_3, Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s}(a_{ij}) \leqslant 0(kd)$$

and the size $l(a_{ij}) \leqslant 0(M + n\log(kd))$. Taking into account that both ψ_1, P_1 are the products of not more than τ minors of the matrix A we obtain the bounds

$$\deg_{\varepsilon_1, \varepsilon_3, Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s}(\psi_1), \deg_{\varepsilon_1, \varepsilon_3, Y, Z_0, \ldots, Z_n, u_0, \ldots, u_s}(P_1) \leqslant \mathscr{P}((kd)^s);$$

$$l(\psi_1), l(P_1) \leqslant (M+n)\mathscr{P}((kd)^s).$$

Similar bounds are valid for the polynomials $\psi_1^{(j_0)}, \psi_1^{(j_0, m_0)}$. Since executing the Gaussian algorithm with the matrix A requires $\mathscr{P}((kd)^s)$ arithmetical operations with entries $a_{ij}^{(\rho)}$ of intermediate matrices $A^{(\rho)}$, and taking into account that the bit sizes of rational functions

$$a_{ij}^{(\rho)} = \det(\Delta_{ij}^{(\rho)})/\det(\Delta_{i_{p-1}, j_{\rho-1}}^{(\rho-1)}) \in \mathbb{Q}(\varepsilon_1, \varepsilon_3)(Z_0, \ldots, Z_n, u_0, \ldots, u_s)$$

do not exceed $\mathscr{P}(M, (kd)^{s(n+s)})$ according to the bounds obtained on degrees and on sizes l, one concludes that the time necessary to construct the matrix A and the polynomials $\psi_1, P_1, \psi_1^{(j_0)}, \psi_1^{(j_0, m_0)}$ can be estimated by $\mathscr{P}(M, (kd)^{s(n+s)})$.

Then the algorithm calculates the quotient $\psi_1^{(j_0)}/\psi_1^{(j_0, m_0)} = \psi_0/P_2$, where polynomials $P_2 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n]$ and $\psi_0 \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n, u_0, \ldots, u_s]$ with the help of proposition 1 factoring polynomials $\psi_1^{(j_0)}$ and $\psi_1^{(j_0, m_0)}$. Then the algorithm computes the polynomial $P = \delta_{K(1)}^{(1)} \delta_{K(2)}^{(2)} P_2$, where $\delta_{K(1)}^{(1)}, \delta_{K(2)}^{(2)} \in \mathbb{Q}[\varepsilon_1, \varepsilon_3][Z_0, \ldots, Z_n]$ are some nonzero coefficients of the polynomials $\mathrm{P}_1, \psi_1^{(j_0, m_0)}$ respectively. Proposition 1 implies the bounds

$$\deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n}(P), \deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0, \ldots, u_s}(\psi_0) \leqslant \mathscr{P}((kd)^s);$$

$$l(P), l(\psi_0) \leqslant (M+n)\mathscr{P}((kd)^s)$$

and the time required to produce P, ψ_0 does not exceed $\mathscr{P}(M, (kd)^{s(n+s)})$.

After that the algorithm factorises the polynomial ψ_0 over the field $\mathbb{Q}$, picks out a factor $\Omega | \psi_0$ of the polynomial ψ_0 irreducible over $\mathbb{Q}$. By virtue of proposition 1

$$\deg_{\varepsilon_1, \varepsilon_3, Z_0, Z_n}(\Omega) \leqslant \mathscr{P}((kd)^s); \quad l(\Omega) \leqslant (M+n)\mathscr{P}((kd)^s)$$

and the algorithm yields Ω within time $\mathscr{P}(M, (kd)^{s(n+s)})$. Then for each s-tuple $(\lambda_1^{(0)}, \ldots, \lambda_s^{(0)})$, where

$$1 \leqslant \lambda_i^{(0)} \leqslant D_1 = \deg_{u_0, \ldots, u_s}(\Omega) \leqslant \tau; \quad 1 \leqslant i \leqslant s$$

the algorithm tests irreducibility over the field H_2 of the polynomial

$$\Omega_0(u_0) = \Omega(u_0, -\lambda_1^{(0)}, \ldots, -\lambda_s^{(0)})$$

within time $\mathscr{P}(M, (kd)^{sn})$ again by proposition 1 and the bounds

$$\deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0}(\Omega_0) \leqslant \mathscr{P}((kd)^s), \quad l(\Omega_0) \leqslant (M+n)\mathscr{P}((kd)^s).$$

Since the whole number of s-tuples $(\lambda_1^{(0)}, \ldots, \lambda_s^{(0)})$ is less than $\mathscr{P}((kd)^{s^2})$, one concludes that the algorithm produces a primitive element

$$\theta^{(v)} = \sum_{1 \leqslant i \leqslant s} \lambda_i(\zeta_i^{(v)}/\zeta_0^{(v)})$$

and its minimal polynomial

$$\Phi = \sum_{0 \leqslant j \leqslant D_1} (\alpha_j/\beta)T^j \in H_2[T]$$

within time $\mathscr{P}(M, (kd)^{s(n+s)})$, herewith

$$\deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, T}(\phi) \leqslant \mathscr{P}(kd)^s), \qquad l(\Phi) \leqslant (M+n)\mathscr{P}((kd)^s).$$

Next, the algorithm finds the expressions $(\zeta_i^{(v)}/\zeta_0^{(v)})(\theta^{(v)})$ again by proposition 1 factoring the polynomial

$$\Omega_i = \Omega(-\lambda_1^{(0)}, \ldots, -\lambda_{i-1}^{(0)}, -\lambda_i^{(0)}+u_i, -\lambda_{i+1}^{(0)}, \ldots, -\lambda_s^{(0)}).$$

Hence,

$$\deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n}((\zeta_i^{(v)}/\zeta_0^{(v)})(\theta^{(v)})) \leqslant \mathscr{P}((kd)^s), \quad l((\zeta_i^{(v)}/\zeta_0^{(v)})(\theta^{(v)})) \leqslant (M+n)\mathscr{P}((kd)^s)$$

and the required time for finding $(\zeta_i^{(v)}/\zeta_0^{(v)})(\theta^{(v)})$ does not exceed $\mathscr{P}(M, (kd)^{s(s+n)})$.

After that the algorithm yields a polynomial $\chi^{(\theta_0)} = \Omega/L^{(\theta_0)}$ factoring the polynomial Ω over the field $H_2[\theta_0]$ based on proposition 1. Proposition 1 entails the bounds

$$\deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0, \ldots, u_s, T}(\chi^{(T)}) \leqslant \mathscr{P}((kd)^s), \qquad l(\chi^{(T)}) \leqslant (M+n)\mathscr{P}((kd)^s)$$

and that the time required to produce $\chi^{(T)}$ can be estimated by $\mathscr{P}(M, (kd)^{s(n+s)})$.

Thereupon, the algorithm finds the polynomials

$$\tau_1 = (\Omega - L^{(T)}\chi^{(T)})/\Phi,$$

$$\tau_2 = \left(T - \sum_{1 \leqslant i \leqslant s} \lambda_i \sum_j (a_j^{(i)}/b)T^j\right)\Big/\Phi \in H_2[T][u_0, \ldots, u_s]$$

dividing each coefficient at a monomial in the variables $u_0, \ldots, u_s$ on the polynomial Φ in the ring $H_2[T]$. It takes time $\mathscr{P}(M, (kd)^{s(n+s)})$ by virtue of, e.g. proposition 1 (though this is a rather strong tool to use it for dividing polynomials), and the following bounds are true:

$$\deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0, \ldots, u_s, T}(\tau_1), \deg_{\varepsilon_1, \varepsilon_3, Z_0, \ldots, Z_n, u_0, \ldots, u_s, T}(\tau_2) \leqslant \mathscr{P}((kd)^s);$$

$$l(\tau_1), l(\tau_2) \leqslant (M+n)\mathscr{P}((kd)^s).$$

After that the algorithm finds the hypersurface $\mathscr{L} \subset \bar{F}_3^{n+1}$ (see (9)). It is given by not more than $(\operatorname{card}\Gamma)(\deg\psi_0) \leqslant \mathscr{P}((kd)^{s^2})$ polynomials, each of degree less or equal to $\mathscr{P}((kd)^s)$. Hence, $N_1 \leqslant \mathscr{P}((kd)^{s^2})$, $N \leqslant n\mathscr{P}((kd)^{s^2})$. The algorithm finds the hypersurface $\mathscr{L}$ within time $\mathscr{P}(M, (kd)^{s(n+s)})$. At last, the algorithm produces the family of linear forms $Y_1, \ldots, Y_N$ and the family of vectors $\{v_{i_1, \ldots, i_n}\}_{1 \leqslant i_1 < \ldots < i_n \leqslant N}$ over the rationals. Then $l(v_{i_1, \ldots, i_n}) \leqslant \mathscr{P}(n, s, \log(kd))$; in addition, the whole number of vectors $\{v_{i_1, \ldots, i_n}\}$ and the time for producing them do not exceed

$$\mathscr{P}\left(\binom{N}{n}\right) \leqslant \mathscr{P}((kd)^{s^2n})$$

(cf. section 2 in Chistov & Grigor'ev, 1983*a*).

Thus, we have proved the following

LEMMA 14. *For a given formula* (2), *the algorithm, described in section* 3, *yields a formula of the form* $\exists\, T(P_1)$ (*see lemma* 10) *which is equivalent to formula* (5), *within time*

$\mathscr{P}(M, (kd)^{s^2n})$. Furthermore, the quantifier-free formula P_1 contains $\mathscr{P}((kd)^{s^2n})$ atomic subformulas of the sort $(g_j \geqslant 0)$ where polynomials $g_j \in \mathbb{Q}[\varepsilon_1, \varepsilon_2, \varepsilon_3][T, Z_0, Z_1, \ldots, Z_n]$, with

$$\deg(g_j) \leqslant \mathscr{P}((kd)^s); \qquad l(g_j) \leqslant M\mathscr{P}(n, (kd)^s).$$

We recall that the decision algorithm for Tarski algebra described in section 4, after implementation of α stages of the procedure enumerates first all $(\{g_j^{(\alpha)}\}_j)$-cells. Let us introduce the notations: $k^{(\alpha)}$ is the number of polynomials $g_j^{(\alpha)}$, i.e. $1 \leqslant j \leqslant k^{(\alpha)}$; next

$$d^{(\alpha)} = \max_{1 \leqslant j \leqslant k(\alpha)} \deg(g_j^{(\alpha)}), \qquad M^{(\alpha)} = \max_{1 \leqslant j \leqslant k(\alpha)} l(g_j^{(\alpha)}).$$

Based on lemma 1 the algorithm enumerates all $(\{g_j^{(\alpha)}\}_j)$-cells within time $\mathscr{P}(M^{(\alpha)}, (k^{(\alpha)}d^{(\alpha)})^{n^2}$, where $n = s_1 + \ldots + s_a$. Note that the whole number of all $(\{g_j^{(\alpha)}\}_j)$-cells does not exceed $\mathscr{P}((k^{(\alpha)}d^{(\alpha)})^n)$ in view of lemma 1.

Next, the algorithm applies the construction from section 3 to a formula of the form (12) and outputs a formula of the sort $\exists\, T(P_t)$ within time $\mathscr{P}(M^{(\alpha)}, (k^{(\alpha)}d^{(\alpha)})^{s_a^2 - \alpha n})$ according to lemma 14. The quantifier-free formula P_t contains atomic subformulas $(g_{m,t}^{(\alpha+1)} \geqslant 0)$. By virtue of lemma 14 the following bounds are true:

$$m \leqslant \mathscr{P}((k^{(\alpha)}d^{(\alpha)})^{s_a^2 - \alpha n}), \qquad \deg(g_{m,t}^{(\alpha+1)}) \leqslant \mathscr{P}((k^{(\alpha)}d^{(\alpha)})^{s_a - \alpha}),$$
$$l(g_{m,t}^{(\alpha+1)}) \leqslant M^{(\alpha)}\mathscr{P}(n, (k^{(\alpha)}d^{(\alpha)})^{s_a - \alpha}), \tag{14}$$

moreover, the polynomials "hidden" in the notations $\mathscr{P}$ do not depend on α.

In the next step the algorithm produces polynomials $\{P_{l,t}^{(\alpha+1)}\}_l$ within the same time-bound $\mathscr{P}(M^{(\alpha)}, (k^{(\alpha)}d^{(\alpha)})^{s_a^2 - \alpha n})$, where bounds similar to (14) are correct for the polynomials $P_{l,t}^{(\alpha+1)}$ in view of the construction in theorem 1 in Wüthrich (1976). Hence, the same time-bound and the bounds similar to (14) are satisfied for polynomials $P_{l,t}^{(\alpha+1)(j_1, j_2, j_3)}$. Finally, the algorithm applies the construction from Wüthrich (1976) to the family of polynomials $\{p_{l,t}^{(\alpha+1)(j_1, j_2, j_3)}\}_{j_1, j_2, j_3, l, t}$ and obtains, as a result, polynomials $\{g_i^{(\alpha+1)}\}_i$ within the same time-bound. In addition, the polynomials $g_i^{(\alpha+1)}$ again satisfy bounds analogous to (14) and, as above, the polynomials "hidden" in the notations $\mathscr{P}$ do not depend on α.

Let us denote $N^{(\alpha)} = k^{(\alpha)}d^{(\alpha)}$. One can infer by induction on α (taking into account for the induction basis $\alpha = O$ the estimates on the parameters of formula (1)) inequalities

$$N^{(\alpha+1)} \leqslant \mathscr{P}((N^{(\alpha)})^{s_a^2 - \alpha n}) \leqslant (kd)^{(O(n))^{3(\alpha+1)}}$$

(see 14)), where the constant factor "hidden" in the notation $O(n)$ does not depend on α. In addition,

$$M^{(\alpha+1)} \leqslant M(kd)^{(O(n))^{3\alpha}s_{a-\alpha}} \leqslant M(kd)^{(O(n))^{3\alpha+1}}.$$

The algorithm produces polynomials $\{g_j^{(\alpha)}\}$ for all j, $0 \leqslant \alpha \leqslant a-1$ within time $\mathscr{P}(M, (kd)^{(O(n))^{3(a-1)}})$.

Thereafter, the algorithm produces by recursion on $1 \leqslant \beta \leqslant a$ the representative set of points $\{w_{m_1, \ldots, m_\beta}^{(a-\beta)}\}_{m_1, \ldots, m_\beta}$. Assume that for a certain $0 \leqslant \beta < a$ the algorithm has constructed for each β-tuple of indices $m_1, \ldots, m_\beta$ a polynomial

$$\Phi_\beta(Z) = \Phi_{m_1, \ldots, m_\beta}(Z) \in \mathbb{Q}[Z],$$

irreducible over $\mathbb{Q}$, and expressions

$$w_\beta^{(p)}(\theta_1) = \sum_{0 \leqslant j < \deg(\Phi_\beta)} \rho_j^{(p)} \theta_1^j$$

for the coordinates of the point

$$w^{(a-\beta)}_{m_1,\dots,m_\beta} = (w^{(1)}_\beta(\theta_1), \dots, w^{(s_1+\dots+s_\beta)}_\beta(\theta_1)) \in (\mathbb{Q}[\theta_1])^{s_1+\dots+s_\beta},$$

where

$$\rho^{(p)}_j \in \mathbb{Q},\ 1 \leqslant p \leqslant s_1 + \dots + s_\beta,\ 0 \leqslant j < \deg(\Phi_\beta) \quad \text{and} \quad \theta_1 \in \tilde{\mathbb{Q}},\ \Phi_\beta(\theta_1) = 0.$$

Furthermore,

$$\theta_1 = \sum_{1 \leqslant p \leqslant s_1 + \dots + s_\beta} \lambda^{(1)}_p w^{(p)}_\beta(\theta_1)$$

for certain natural numbers $1 \leqslant \lambda^{(1)}_p \leqslant \deg(\Phi_\beta)$. Besides, we assume that the algorithm has found a pair of rational numbers $c_1, c_2 \in \mathbb{Q}$ such that in the interval $(c_1, c_2) \subset \mathbb{R}$, θ_1 is the only root of the polynomial Φ_β. Let us define

$$d_\beta = \deg(\Phi_\beta), \qquad M_\beta = \max_p \{l(\Phi_\beta), l(w^{(p)}_\beta(\theta_1)), l(c_1), l(c_2)\}.$$

Applying lemma 2 to the family of polynomials

$$\{\hat{g}_i\}_i = \{g^{(a-\beta-1}_i(w^{(a-\beta)}_{m_1,\dots,m_\beta}, X)\}_i$$

the algorithm produces for given $m_1, \dots, m_\beta$ the set of points

$$\{w^{(a-\beta-1)}_{m_1,\dots,m_\beta,m_{\beta+1}}\}_{m_{\beta+1}} \subset \tilde{\mathbb{Q}}^{s_1+\dots+s_\beta+s_{\beta+1}},$$

a corresponding polynomial

$$\Phi_{\beta+1} = \Phi_{m_1,\dots,m_{\beta+1}} \in \mathbb{Q}[Z],$$

expressions

$$w^{(l)}_{\beta+1}(\theta) \in \mathbb{Q}[\theta],\ \Phi_{\beta+1}(\theta) = 0 \quad \text{for} \quad 1 \leqslant l \leqslant s_1 + \dots + s_{\beta+1}$$

(cf. above) and, finally, a pair of rational numbers $b_1, b_2 \in \mathbb{Q}$ such that in the interval $(b_1, b_2) \subset \mathbb{R}$, θ is the unique root of the polynomial $\Phi_{\beta+1}$. Lemma 2 implies the following bounds (taking into account the inequalities for $N^{(\alpha)}$, $M^{(\alpha)}$ proved above):

$$d_{\beta+1} \leqslant \mathscr{P}((N^{(a-\beta-1)}d_\beta)^n); \qquad M_{\beta+1} \leqslant (M^{(a-\beta-1)} + M_{\beta+n})\mathscr{P}((N^{(a-\beta-1)}d_\beta)^n).$$

From this one can deduce by induction on β the bounds

$$d_{\beta+1} \leqslant (kd)^{(O(n))^{3a+\beta-2}}; \qquad M_{\beta+1} \leqslant M(kd)^{(O(n))^{3a+\beta-2}}.$$

Moreover, the constant factors "hidden" in the notations $O(n)$, do not depend on β (cf. above).

By virtue of lemma 2, for given $m_1, \dots, m_\beta$, the number of points in the set $\{w^{(a-\beta-1)}_{m_1,\dots,m_\beta,m_{\beta+1}}\}_{m_{\beta+1}}$ does not exceed $(kd)^{(O(n))^{3a+\beta-1}}$. The algorithm can produce the set $\{w^{(a-\beta-1)}_{m_1,\dots,m_\beta,m_{\beta+1}}\}_{m_{\beta+1}}$ within time $\mathscr{P}(M, (kd)^{(O(n))^{3a+\beta-1}})$, again according to lemma 2 and to the bounds on d_β, M_β obtained above. Thus, the number of all points from the representative set $\{w^{(0)}_{m_1,\dots,m_a}\}_{m_1,\dots,m_a}$ is not greater than $(kd)^{(O(n))^{4a-2}}$, the time for the construction of this set can be estimated by $\mathscr{P}(M, (kd)^{(O(n))^{4a-2}})$.

At the end of its work the algorithm evaluates the signs $\operatorname{sgn}(f_j(w^{(0)}_{m_1,\dots,m_a}))$ for all $1 \leqslant j \leqslant k$; $m_1, \dots,, m_a$, and thereby verifies formula (13) (see lemma 13). One can evaluate the sign $\operatorname{sgn}(f_j(w^{(0)}_{m_1,\dots,m_a}))$ for given $j, m_1, \dots, m_a$ in the following way. First, the algorithm replaces the coordinates of the point $w^{(0)}_{m_1,\dots,m_a} \in (\mathbb{Q}[\theta_0])^n$ by their expressions via appropriate real root $\theta_0 \in \tilde{\mathbb{Q}}$ of polynomial Φ_a (see above the representation of points $w^{(a-\beta)}_{m_1,\dots,m_\beta}$). So, the algorithm gets the expression $f(w^{(0)}_{m_1,\dots,m_a}) = h_j(\theta_0)$ for a suitable polynomial $h_j(Z) \in \mathbb{Q}[Z]$. Obviously, $f(w^{(0)}_{m_1,\dots,m_a}) = 0$ is valid iff polynomial $\Phi_a | h_j$. If the latter relation is false, the algorithm finds a suitable rational approximation $\omega_0 \in \mathbb{Q}$ to the root θ_0 in order to guarantee the equality $\operatorname{sgn} h_j(\omega_0) = \operatorname{sgn} h_j(\theta_0) \neq 0$ (cf. section 3 in Grigor'ev & Vorobjov, 1987). The rational approximation can be found, e.g. by means of Heindel (1971) within time $\mathscr{P}(M, (kd)^{(O(n))^{4a-3}})$ in view of the bounds on d_a, M_a proved above. This completes the proof of the theorem (see the introduction).

6. Computing the Dimension of a Semialgebraic Set

Let $V = \{\Pi\} \subset \mathbb{R}^n$ be a semialgebraic set, given by a quantifier-free formula Π of Tarski algebra. We shall prove the following statement: If the dimension $\dim V = m < n$, then there is an index $1 \leqslant j \leqslant n$ such that $\dim (\pi^{(j)}(V)) = m$, where π^j denotes the projection onto the coordinates $X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n$. We conduct the proof by induction on m. When $m = 0$, the statement is trivial, so we assume further that $m \geqslant 1$. For any number $x \in \mathbb{R}$ consider a semialgebraic set $V^{(x)} = V \cap \{X_1 = x\}$. If for a certain $x_0 \in \mathbb{R}$ the equality $\dim V^{(x_0)} = m$ is valid, then one can take $j = 1$. Suppose that, on the contrary, $\dim V^{(x)} \leqslant m-1$ for all $x \in \mathbb{R}$. Let us denote by $W \subset \mathbb{R}$ the semialgebraic set, which consists of all numbers $x \in \mathbb{R}$ such that $\dim (V^{(x)}) = m-1$ (the set W is semialgebraic since the condition $x \in W$ can be written as a suitable formula of Tarski algebra). Then W contains some interval, taking into account that $\dim V = m$. For each $2 \leqslant i \leqslant n$ we introduce the semialgebraic set $W^{(i)} \subset W$ consisting of all points $x \in W$ for which $\dim (\pi^{(i)}(V^{(x)})) = m-1$. The inductive hypothesis entails the equality

$$W = \bigcup_{2 \leqslant i \leqslant n} W^{(i)}.$$

Therefore, for a suitable $2 \leqslant i_0 \leqslant n$, the set $W^{(i_0)}$ contains a certain interval. Setting $j = i_0$ completes the proof of the statement.

One concludes from the statement that $\dim V = m$ iff m is the greatest natural number such that there exist indices $1 \leqslant i_1 < \ldots < i_m \leqslant n$, for which $\dim (\pi_{i_1, \ldots, i_m}(V)) = m$ where $\pi_{i_1, \ldots, i_m} : \mathbb{R}^n \to \mathbb{R}^m$ denotes the projection onto the coordinates $X_{i_1}, \ldots, X_{i_m}$. On the other hand, for given $i_1, \ldots, i_m$, the condition $\dim (\pi_{i_1, \ldots, i_m}(V)) = m$ is equivalent to the requirement that the semialgebraic set $\pi_{i_1, \ldots, i_m}(V) \subset \mathbb{R}^m$ contains some m-dimensional ball. The latter requirement is equivalent in turn to the following formula of Tarski algebra

$$\exists\, w \in \mathbb{R}^m\, \exists\, \tau > 0\, \forall\, w_1 \in \mathbb{R}^m\, \exists\, v_1 \in \mathbb{R}^{n-m}((\|w_1 - w\| \leqslant \tau) \Rightarrow (\langle w_1, v_1 \rangle \in V))$$

in $n+m+1$ variables with the number of quantifier alternations $a = 3$. Here, $\langle w_1, v_1 \rangle = (u^{(1)}, \ldots, u^{(n)}) \in \mathbb{R}^n$ denotes the unique vector such that $\pi_{i_1, \ldots, i_m}(\langle w_1, v_1 \rangle) = w_1$ and $u^{(j_l)} = v_1^{(l)}$ for $1 \leqslant l \leqslant n-m$, where

$$\{i_1, \ldots, i_m\} \cup \{j_1, \ldots, j_{n-m}\} = \{1, \ldots, n\},$$

indices $j_1 < \ldots < j_{n-m}$, point $v_1 = (v_1^{(1)}, \ldots, v_1^{(n-m)})$. The algorithm verifies for every m and set of indices $i_1, \ldots, i_m$ the designed formula of Tarski algebra based on the theorem (see the introduction) and thereby determines $\dim V$. Thus, the following corollary is true.

Corollary. *Let Π be a quantifier-free formula of Tarski algebra, which contains k atomic subformulas $(f_i \geqslant 0)$, where f_i are polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ with $\deg (f_i) < d$, $l(f_i) \leqslant M$, $1 \leqslant i \leqslant k$. Then one can compute the dimension $\dim \{\Pi\}$ within time $\mathscr{P}(M, (kd)^{(O(n))^{10}})$.*

References

Ben-Or, M., Kozen, D., Reif, J. (1984). The complexity of elementary algebra and geometry. *Proc. 16 ACM Symp. Th. Comput.* 457–464.

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., Grigor'ev, D. Yu. (1984). Complexity of quantifier elimination in the theory of algebraically closed fields. *Springer Lec. Notes Comp. Sci.* **176,** 17–31.

Chistov, A. L. (1984). Polynomial-time factoring of polynomials and finding compounds of a variety within the 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.)

Cohen, P. (1969). Decision procedures for real and p-adic fields. *Commun. Pure Appl. Math.* **22,** 131–153.

Collins, G. E. (1975). Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Automata Theory and Formal Languages 2nd GI Conf., Kaiserslautern (Brakhage, H., ed.). *Springer Lec. Notes Comp. Sci.* **33,** 134–183.

Fischer, M., Rabin, M. (1974). Super-exponential complexity of Presburger arithmetic. In: *Complexity of Computations* (SIAM–AMS Proc., 7), pp. 27–41.

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. (1985). Complexity of deciding first-order theory of real closed fields. *Proc. All-Union Conf. Appl. Logic, Novosibirsk*, 64–66 (in Russian).

Grigor'ev, D. Yu. (1987). Computational Complexity in Polynomial Algebra. Proc. International Congress of Mathematicians, Berkeley, California.

Grigor'ev, D. Yu., Vorobjov, N. N., Jr (1987). Solving systems of polynomial inequalities in subexponential time. (Submitted.)

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 fields. *Theor. Comp. Sci.* **24,** 239–278.

Lang, S. (1965). *Algebra.* New York: Addison-Wesley.

Lazard, D. (1981). Résolution des systèmes d'équation algébriques. *Theor. Comp. Sci.* **15,** 77–110.

Lenstra, A. K. (1984). Factoring multivariable polynomials over algebraic number fields. *Springer Lec. Notes Comp. Sci.* **176,** 389–396.

Mayr, E. W., Meyer, A. R. (1982). The complexity of the word problem for commutative semigroups and polynomial ideals. *Adv. Math.* **46,** 305–329.

Milnor, J. (1964). On a Betti numbers of real varieties. *Proc. Amer. Math. Soc.* **15**(2), 275–280.

Monk, L. (1974). *An Elementary-recursive Decision Procedure for Th(R, +,·).* Ph.D. Thesis, Berkeley.

Seidenberg, A. (1954). A new decision method for elementary algebra and geometry. *Ann. Math.* **60,** 365–374.

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.

Vorobjov, N. N. Jr, Grigor'ev, D. Yu. (1985). Finding real solutions of systems of algebraic inequalities in subexponential time. *Soviet Math. Dokl.* **32(1),** 316–320.

Wüthrich, H. (1976). Ein Entscheidungsverfahren für die Theorie der reel-abgeschlossenen Körper. In Komplexität von Entscheidungs-Problemen. (Specker, E., Strassen, V., Eds). *Springer Lec. Notes Comp. Sci.* **43,** 138–162.