Finding at least one point in each connected component of a real algebraic set defined by a single equation

F. Rouillier, M.-F. Roy, M. Safey El Din

-

Abstract

Deciding efficiently the emptiness of a real algebraic set defined by a single equation is a fundamental problem of computational real algebraic geometry. We propose an algorithm for this test. We find, when the algebraic set is non empty, at least one point on each semi-algebraically connected component. The problem is reduced to deciding the existence of real critical points of the distance function and computing them.

1 Introduction

The first algorithms for deciding the truth of a first order formula over the reals, and, as a particular case, deciding the emptiness of a semi-algebraic set, follow from Tarski and Seidenberg's work [30, 29]. The complexity of their algorithms was not elementary recursive.

The Cylindrical Algebraic Decomposition of Collins [8] has much better complexity (polynomial in the degrees and number of polynomials, doubly exponential in the number of variables). It is the first algorithm deciding the truth of a first order formula over the reals, and, as a particular case, deciding the emptiness of a semi-algebraic set, to have been implemented. This algorithm is based on the elimination of the variables one after the other and is considered as inefficient in practice when the number of variables is

greater than 2 or 3. Other implementations based on the algorithms of Weipsfenning [32, 33, 34] are being developed.

Grigoriev and Vorobjov [15] proposed an algorithm which decides the emptiness of a semi-algebraic set with single exponential complexity in the number of variables. Rather than making iterated projections, their method is based on the computation of a finite number of points, the critical points of a well chosen function. Several other algorithms with single exponential complexity, based on variants of the critical point method, have been proposed more recently [21, 6, 16, 2, 3]. However, these algorithms are inefficient in practice due to the introduction of several infinitesimals. Ideas to improve the practical complexity appear in [17] and have been developed in [24] (see also [7, 9]).

The strategy we propose for efficiently solving systems of inequalities over the reals is based on the progressive construction of the following subroutines [28, 14, 25]:

- a) find real solutions of univariate polynomials,
- b) find real solutions of systems of equations which have only a finite number of complex solutions,
- c) find real points on every semi-algebraically connected component of a real algebraic set defined by a single equation, using the critical point method,
- d) find real points on every semi-algebraically connected component of a real algebraic set defined by several equations,
- e) find real points on every semi-algebraically connected component of a semi-algebraic set.

Typically, for example, problem b) can be reduced to problem a) by a convenient Rational Univariate Representation using a separating element (see [1, 24, 25, 14]).

Problem c) can be reduced to problem b) by various techniques (see for example [2, 3, 28, 24, 4]) using infinitesimals. The reduction of d) to c) is done by taking sums of squares [2]. The theoretical complexity of taking sums of squares is good but the method is not adapted to practical computations

since the degrees and the size of coefficients are multiplied by 2, singularities are introduced and infinitesimals are systematically needed for the reduction of c) to b). Other techniques are proposed in [9, 26].

The aim of the present paper is to design a new efficient algorithm for solving the problem c): testing whether the zero set of a polynomial has real points and if it does compute a point at least on every semi-algebraically connected component.

This problem can be reduced to problem b) by studying the critical points of the projection function on a coordinate (see [2, 3, 28]). In these papers, at least two infinitesimals are introduced to deform the hypersurface so that there are a finite number of critical points for this coordinate. Then techniques for polynomial system solving have to be used in a ring with these infinitesimals.

To obtain an efficient algorithm in practice, we keep in mind that integer arithmetic is critical for :

- a) very efficient implementations of Gröbner basis (see [11, 12]),
- b) efficient implementation of Rational Univariate Representation which is, in part, based on a modular guess of a separating element (see [24, 25]),
- c) efficient real root counting and description of the real roots of a univariate polynomial [27].

Thus, we try to limit the use of infinitesimals in our algorithms. We use them only for special cases, rare in practice, and we use at most one infinitesimal.

Our main algorithm, described in section 3, presents a variant of the critical point method, coming back to a classical idea of Seidenberg [29]. We search the critical points of the distance function, getting a point in every connected component, even unbounded ones. We introduce only one infinitesimal, and only when the number of singular points is infinite.

Since the resolution of zero-dimensional systems is essential (from a practical and a theoretical point of view) for the algorithm that we design, we recall in section 2 some basic results about them and in particular the definition and the properties of the Rational Univariate Representation.

In section 4, we present an algorithm to detect the real bounded roots of univariate polynomials with infinitesimal coefficients.

In section 5, we present various improvements of computations with infinitesimals.

In section 6, we present some experimental results of our algorithm.

We would like to thank R. Rioboo for updating his implementation of CAD for these computations and R. Pollack for his help in the proof of Lemma 4.6.

2 Zero-dimensional systems

The resolution of zero-dimensional systems is a key point in our algorithms. This section is devoted to the description of the tools we use in practice. In this section, we introduce and recall some basic results about zero-dimensional systems.

In all the paper K is an ordered field, R is a real closed field containing the ordered field K and $C = R[i]$ is an algebraically closed field containing the field K. It is helpful to think of K, R, C as the fields of rational, real and complex numbers.

A *polynomial system* S in $K[X_1, \ldots, X_k]$, is a finite subset of $K[X_1, \ldots, X_k]$, $\langle S \rangle$ denotes the ideal generated by S,

$$\mathcal{Z}(S) = \{X \in C^k \mid \forall P \in S \ P(x) = 0\}$$

the solutions of S in C^k and

$$Z(S) = \{X \in R^k \mid \forall P \in S \ P(x) = 0\}$$

the solutions of S in R^k.

A *zero-dimensional polynomial system* of S in $K[X_1, \ldots, X_k]$, is a finite subset of $K[X_1, \ldots, X_k]$ with a finite number of solutions in C^k.

In the algorithms described in this paper, we need black boxes for different purposes :

- **GröbnerCompute** computes a Gröbner basis for the ideal generated by a polynomial system S in $K[X_1, \ldots, X_k]$ (for any admissible order on the monomials) (see an efficient version in [12]) .

- **Test-Dim** takes as input a Gröbner basis and returns *false* if it is not zero-dimensional, else it returns *true*.
- **Test-Radical** tests if the ideal generated by a zero-dimensional polynomial system is radical,
- **RUR** takes as input a zero-dimensional Gröbner basis G with coefficients in K, and returns a representation of the solutions of G in C (this will be detailed in the remainder of this section).
- **RealRootCount** which counts and describes the roots in R of a univariate polynomial with coefficients in K (see the various existing methods in [27, 28]).

The second item follows easily from a Gröbner basis of $I = \langle S \rangle$ for any admissible monomial ordering. If G denotes such a Gröbner basis, it is well known (see [10] for example) that S is zero-dimensional if and only if for each $i = 1 \dots k$ there exists a polynomial g in G such that its leading monomial is in the form $X_i^{n_i}$ where n_i is a positive integer.

If S is zero-dimensional and $I = \langle S \rangle$, the quotient algebra $K[X_1, \dots, X_k]/I$ is a K-vector space whose dimension is equal to the number of solutions of S in C^k counted with multiplicities. Consequently, the third item can be done by comparing the dimensions of the finite dimensional K-vector spaces $K[X_1, \dots, X_k]/I$ and $K[X_1, \dots, X_k]/\sqrt{I}$. The dimension of $K[X_1, \dots, X_k]/I$ can be computed from a Gröbner basis G of I for any admissible monomial ordering : it is equal to the number of monomials that cannot be reduced modulo G. The dimension of the K-vector space $K[X_1, \dots, X_k]/\sqrt{I}$ is equal to the number of distinct solutions of S in C^k which can be explicitly and efficiently (see [24, 14]) computed knowing G by constructing and reducing Hermite's quadratic form: its rank is exactly equal to the number of solutions of S in C^k.

A convenient representation of the solutions of a zero- dimensional is given by the Rational Univariate Representation (RUR) (see [25, 14]).

Let S be a zero-dimensional polynomial system in $K[X_1, \dots, X_k]$, for any $x = (x_1, \dots, x_k) \in \mathcal{Z}(S)$, we denote by $\mu(x)$ the multiplicity of x (i.e. the dimension of the localization of $C[X_1, \dots, X_k]/I$ at x, with $I = \langle S \rangle$).

Proposition 2.1 *Given any $u \in K[X_1, \dots, X_k]$ we define:*

- $f_u(T) = \prod_{x \in \mathcal{Z}(S)} (T - u(x))^{\mu(x)}$
- $g_0(T) = \sum_{x \in \mathcal{Z}(S)} \mu(x) \prod_{y \in \mathcal{Z}(S), u(y) \neq u(x)} (T - u(y))$
- $g_i(T) = \sum_{x \in \mathcal{Z}(S)} \mu(x) x_i \prod_{y \in \mathcal{Z}(S), u(y) \neq u(x)} (T - u(y))$

for $i = 1, \ldots, k$.

If u *separates* S *(i.e. if* $\forall (x, y) \in \mathcal{Z}(S)^2, x \neq y \Rightarrow u(x) \neq u(y)$*), then the univariate polynomials*

$$\{f_u(T), g_0(T), g_1(T), \ldots, g_k(T)\}$$

define the so called Rational Univariate Representation (RUR) of S associated to u.

The RUR of S *has the following properties (see [25]) :*

- $f_u(T), g_0(T), g_1(T), \ldots, g_k(T)$ *are all elements of* $K[X_1, \ldots, X_k]$
- *the application :*

$$\begin{array}{rccc} \Pi_u : & C^k & \longrightarrow & C \\ & x & \longmapsto & u(x) \end{array}$$

  defines a bijection between $\mathcal{Z}(S)$ *and* $\mathcal{Z}(f_u)$*, whose reciprocal is given by :*

$$\begin{array}{rccc} \Pi_u^{-1} : & \mathcal{Z}(f_u) & \longrightarrow & \mathcal{Z}(S) \\ & a & \longmapsto & (\frac{g_1(a)}{g_0(a)}, \ldots, \frac{g_k(a)}{g_0(a)}) \end{array}$$

- Π_u *preserves the multiplicities (*$\mu(u(x)) = \mu(x)$*).*

Moreover, a separating element u *for* S *can be chosen among the elements of the family*

$$\mathcal{U} = \{X_1 + jX_2 + \ldots + j^{k-1}X_k, j = 0 \ldots kD(D-1)/2\},$$

where D *is the dimension of* $K[X_1, \ldots, X_k]/\langle S \rangle$ *as a* K*-vector space.*

The point $(\frac{g_1(a)}{g_0(a)}, \ldots, \frac{g_k(a)}{g_0(a)})$ of $\mathcal{Z}(S)$ is *associated* to the root a of f_u.
The computation of a RUR can be decomposed into two steps :

- finding a separating element,
- computing a RUR knowing a separating element.

According to the proposition above, we can proceed as follows for checking if a given element is separating and finding a separating element of a zero-dimensional system S of $K[X_1, \ldots, X_k]$:

ChecksepElement

- **Input :** A zero-dimensional system S of $K[X_1, \ldots, X_k]$, a Gröbner basis G of $I = \langle S \rangle$ for any admissible monomial ordering, the number $\sharp\mathcal{Z}(S)$ of distinct solutions of the system and an element $u \in K[X_1, \ldots, X_k]$
- **Output :** *true* if u is separating for S and *false* if it is not.
- Compare the degree of the square-free part of the minimal polynomial of the multiplication by u (abusing notation and identifying u and its image in $K[X_1, \ldots, X_k]/I$) and $\sharp\mathcal{Z}(S)$. If these two numbers are equal return *true*, otherwise return *false*.

sepElement

- **Input :** A zero dimension system S of $K[X_1, \ldots, X_k]$ and a Gröbner basis G of $I = \langle S \rangle$ for any admissible monomial ordering.
- **Output :** a separating element for S.

1. Compute $\sharp\mathcal{Z}(S)$ by constructing and reducing Hermite's quadratic form.
2. Choose $u \in \mathcal{U}$. Remove u from $\mathcal{U}$.
3. Perform ChecksepElement on u. If the output is *false*, go to step 2 again.
4. Return(u)

In the particular case when $I = \langle S \rangle$ is radical, step 1 is not needed since $\sharp\mathcal{Z}(S)$ is exactly the dimension of the K-vector space $K[X_1, \ldots, X_k]/I$.

The RUR itself can be computed using different strategies. For example, when the ideal is known to be radical, a separating element u is a primitive element of $K[X_1, \ldots, X_k]/I$, and the computation of a RUR consists in expressing the coordinates $X_i, i = 1 \ldots k$ with respect to the algebraic extension $K[u]$ (done by inverting the matrix whose columns are the coordinates of $1, u, \ldots, u^{D-1}$ in $K[X_1, \ldots, X_k]/I$).

In the general case (the ideal is not supposed to be radical), an algorithm for computing a RUR is described (see [25]). All the coefficients of all the polynomials in the RUR can be deduced from the scalars Trace$(u^i \cdot X_j), i = 0 \ldots D, j = 1 \ldots n$ where u is the chosen separating element, and, Trace(P), for any $P \in K[X_1, \ldots, X_k]/I$, is the trace of the K-linear map of $K[X_1, \ldots, X_k]/I : f \longmapsto f\dot{P}$. This method allows in particular to choose an arbitrary element u and check after the computation if u is separating or not. In the particular case of systems with rational coefficients, an optimized method, based on modular computations, for the full computation (including the search of a separating element) is also proposed in [25].

For an efficient use of the existing tools for solving zero-dimensional systems, one will try as much as possible to deal with radical ideals (separating element easier to find) and, as much as possible, rational coefficients (the RUR is easier to compute). In any case, we denote by **RUR** the following:

RUR

- **Input :** A zero-dimensional polynomial system S in $K[X_1, \ldots, X_k]$ and a Gröbner basis G of $\langle S \rangle$.
- **Output :**A Rational Univariate Representation of S.

1. Construct the multiplication table of $K[X_1, \ldots, X_k]/I$.
2. Use sepElement to obtain a separating element.
3. Compute a RUR $(f_u(T), g_0(T), g_1(T), \ldots, g_k(T))$ for this separating element.

Finally, counting and describing the solutions of the polynomial system in R^k is equivalent to counting and describing the roots in R of the first element of the RUR $f_u(T)$ (see [24, 25]) which is a univariate polynomial with rational coefficients. This is done by RealRootCount .

The following variant, called ARUR [1], will be useful in the last sections

of the paper. We suppose we know already a separating element.

Definition 2.2 *Given any separating $u \in K[X_1, \ldots, X_k]$ we define:*

- $f_u(T) = \prod_{x \in \mathcal{Z}(S)} (T - u(x))^{\mu(x)}$
- $\tilde{g}_0(T) = \sum_{x \in \mathcal{Z}(S)} \mu(x)(T - u(x))^{\mu(x)-1} \prod_{y \in \mathcal{Z}(S) \setminus \{x\}} (T - u(y))^{\mu(y)}$
- $\tilde{g}_i(T) = \sum_{x \in \mathcal{Z}(S)} \mu(x) x_i (T - u(x))^{\mu(x)-1} \prod_{y \in \mathcal{Z}(S) \setminus \{x\}} (T - u(y))^{\mu(y)}$

for $i = 1, \ldots, k$. Note that $\tilde{g}_0$ is the derivative of f_u.

The univariate polynomials

$$\{f_u(T), \tilde{g}_0(T), \tilde{g}_1(T), \ldots, \tilde{g}_k(T)\}$$

define the so called Antique Rational Univariate Representation (ARUR) of S associated to u.

The ARUR of S has the following properties:

- *$f_u(T), \tilde{g}_0(T), \tilde{g}_1(T), \ldots, \tilde{g}_k(T)$ are all elements of $K[X_1, \ldots, X_k]$*
- *the application :*

$$\begin{array}{rccc} \Pi_u : & C^k & \longrightarrow & C \\ & x & \longmapsto & u(x) \end{array}$$

defines a bijection between $\mathcal{Z}(S)$ and $\mathcal{Z}(f_u)$, whose reciprocal is given by :

$$\begin{array}{rccc} \Pi_u^{-1} : & \mathcal{Z}(f_u) & \longrightarrow & \mathcal{Z}(S) \\ & a & \longmapsto & (\frac{\tilde{g}_1^{(\mu-1)}(a)}{\tilde{g}_0^{(\mu-1)}(a)}, \ldots, \frac{\tilde{g}_k^{(\mu-1)}(a)}{\tilde{g}_0^{(\mu-1)}(a)}) \end{array}$$

where μ is the multiplicity of a as a root of f_u.

All the coefficients of all the polynomials in the ARUR can be deduced from the scalars $\mathrm{Trace}(u^i \cdot X_j), i = 0 \ldots D, j = 1 \ldots n$.

3 The main algorithm

In the following, P is a polynomial in $K[X_1, \ldots, X_k]$, and $A = (a_1, \ldots, a_k)$ is a point of K^k such that $P(A) \neq 0$.

We give now an algebraic description of an algebraic set containing the points of $Z(P)$ at minimal distance from A.

We consider the polynomial system $\mathcal{C}(A)$ defined by

$$P(M) = 0,\ \overrightarrow{\text{grad}}_M\ (P) /\!/\ \overrightarrow{AM},$$

where $M = (X_1, \ldots, X_k)$. The condition $\overrightarrow{\text{grad}}_M\ (P) /\!/\ \overrightarrow{AM}$ is expressed by setting the $(2,2)$ determinants of the matrix whose columns are the vectors $\overrightarrow{\text{grad}}_M\ (P)$ and $\overrightarrow{AM}$ to 0.

A point M is *singular* if

$$P(M) = 0,\ \overrightarrow{\text{grad}}_M\ (P) = 0,$$

so that all singular points belong to $\mathcal{Z}(\mathcal{C}(A))$.

It is clear that a semi-algebraically connected component of $Z(\mathcal{C}(A))$ is contained in a semi-algebraically connected component of $Z(P)$.

Lemma 3.1 *Every semi-algebraically connected component of $Z(P)$ meets $Z(\mathcal{C}(A))$.*

Proof: Consider a semi-algebraically connected component D of $Z(P)$ and denote by M a point of D at minimum distance from A. Let d be the distance from A to M. If the point M is singular, $M \in Z(\mathcal{C}(A))$ since $\overrightarrow{\text{grad}}_M\ (P) = \overrightarrow{0}$. If it is regular, $\overrightarrow{\text{grad}}_M\ (P) \neq \overrightarrow{0}$ and there exists a hyperplane H which is tangent to $Z(P)$ at M. Since M is a point at minimum distance from the origin on D, the interior of the sphere of center A and of radius d contains no point of D. Thus, the sphere of center A and of radius d is tangent to H, and $\overrightarrow{AM}\ /\!/\ \overrightarrow{\text{grad}}_M\ (P)$. □

3.1 Case 1

Lemma 3.1 gives immediately an algorithm to decide if $Z(P)$ is empty and to find a point in every semi-algebraically connected component of $Z(P)$ when $\mathcal{Z}(\mathcal{C}(A))$ is finite.

Algorithm 1

- **Input:** a polynomial $P \in K[X_1, \ldots, X_k]$ and a point $A \in K^k$.
- **Output:** *no answer* if $\mathcal{Z}(\mathcal{C}(A))$ is infinite, *false* if $Z(P)$ is empty, *true* and at least one point on each semi-algebraically connected component if $Z(P)$ is not empty.

1. Set G be the output of GröbnerCompute on $\mathcal{C}(A)$.
2. Use Test-Dim on G. If it returns *false*, then return *no answer*.
3. Else use RUR on G. Set $(f_u(T), g_0(T), g_1(T), \ldots, g_k(T))$ to the output.
4. Use RealRootCount on $f_u(T)$.

3.2 Case 2

When $\mathcal{Z}(\mathcal{C}(A))$ is infinite, we consider the system $\mathcal{G}$ defined by

$$P(M) = 0, \ \overrightarrow{\text{grad}}_M(P) = 0,$$

the set $\mathcal{Z}(\mathcal{G})$ is the set of singular points of $\mathcal{Z}(P)$ In this section, we suppose that $\mathcal{Z}(\mathcal{G})$ is finite.

We say that $B = (b_1, \ldots, b_k) \in C^k$ is a *good center* for P if $\mathcal{Z}(\mathcal{C}(B))$ is finite.

We are going to prove that the set of $B \in C^k$ which are not good centers for P is contained in a strict algebraic subset of C^k. As a consequence, the set of $B \in K^k$ which are not good centers for P is contained in a strict algebraic subset of K^k.

Let

$$Q_1 = \lambda \frac{\partial P}{\partial X_1} - X_1,$$

$$\vdots$$

$$Q_k = \lambda \frac{\partial P}{\partial X_k} - X_k.$$

Consider the system $\mathcal{C}'(B)$ defined by

$$P = 0,$$

$$Q_1 + b_1 = 0,$$
$$\vdots$$
$$Q_k + b_k = 0$$

It is clear that $\mathcal{Z}(\mathcal{C}(B)) = \mathcal{Z}(\mathcal{G}) \cup \pi(\mathcal{Z}(\mathcal{C}'(B)))$ where π is the projection of $(x_1, \ldots, x_k, \lambda)$ on $(x_1, \ldots, x_k)$.

Lemma 3.2 *Let P be a polynomial and*

$$\mathcal{H} = \{(M, \lambda) \in C^{k+1} \mid P(M) = 0, \overrightarrow{\text{grad}}_M\ (P) \neq \overrightarrow{0}\}.$$

$$\mathcal{A} = \{B = (b_1, \ldots, b_k) \in C^k \mid$$
$$\mathcal{H} \cap \mathcal{Z}(Q_1 + b_1, \ldots, Q_k + b_k, Jac(P, Q_1 + b_1, \ldots, Q_k + b_k)) \neq \emptyset\}$$

is contained in a strict algebraic subset of C^k.

Proof: Consider the application F from $\mathcal{H}$ to C^k which associates to (M, λ) $Q_1(M, \lambda), \ldots, Q_k(M, \lambda)$. The critical values of F are the points $B = (b_1, \ldots, b_k)$ of C^k such that $\mathcal{Z}(Q_1 + b_1, \ldots, Q_k + b_k, Jac(P, Q_1 + b_1, \ldots, Q_k + b_k)) \neq \emptyset$. ¿From Sard's theorem over $\mathbb{C}$ [20] and the transfer principle [5] it follows that $\mathcal{A}$ is a constructible set of dimension $< k$ of C^k. □

Corollary 3.3 *A point $A \notin \mathcal{A}$ is a good center for P. Moreover, the zeroes of $\mathcal{C}'(A)$ are simple.*

Proof: Let $A = (a_1, \ldots, a_k) \notin \mathcal{A}$. Since the rank of the Jacobian matrix is maximal at the solutions of the system $\mathcal{C}'(A)$, these solutions are isolated and non singular. So, $\mathcal{Z}(\mathcal{C}'(A))$ is finite and contains only simple zeroes. □

It is well known that

Lemma 3.4 *Let g be a non null polynomial in $R[X_1, \ldots, X_k]$ of degree d, one can find a point A in $\{0, \ldots, d\}^k$ such that $g(A) \neq 0$.*

Thus, one can choose successive values of $B = (b_1, \ldots, b_k)$ in a box $\{0, \ldots, d\}^k$ and guarantee that for one of these choices the zero set of $\mathcal{C}'(B)$ is composed of a finite number of simple zeroes. Since we do not have a precise

bound on the degree of the algebraic set defining $\mathcal{A}$, we have to be careful in the way we exhaust this box.

If $\mathcal{Z}(\mathcal{C}(A))$ is infinite and $\mathcal{Z}(\mathcal{G})$ is finite, we need to find a point B such that the system $P = 0,\ \lambda\ \overrightarrow{\text{grad}}_M\ (P)//\ \overrightarrow{BM}$ is zero-dimensional.

change-center

- **Input:** A polynomial $P \in K[X_1, \ldots, X_k]$ such that $\mathcal{Z}(\mathcal{G})$ is finite.
- **Output:** A point B such that $\mathcal{C}(B)$ is zero-dimensional, and a Gröbner basis G of $\langle \mathcal{C}(B) \rangle$

1. Choose a point B in $\{0, \ldots, d\}^k \setminus \{0, \ldots, d-1\}^k$.
2. Perform GröbnerCompute on $\mathcal{C}(B)$. Set G to the output.
3. Use Test-Dim on G. If it returns *true*, return G.
4. Else, if all the points of $\{0, \ldots, d\}^k$ have been tested, take $d := d + 1$ and go to 1.

Now, we are ready to describe the **Algorithm 2** which tests the emptiness of $Z(P)$ (and returns at least one point on each semi-algebraically connected component if it is not empty) in the case where $\mathcal{Z}(\mathcal{C}(A))$ is infinite and $\mathcal{Z}(\mathcal{G})$ is finite.

Algorithm 2

- **Input:** a polynomial $P \in K[X_1, \ldots, X_k]$.
- **Output:** *no answer* if $\mathcal{Z}(\mathcal{G})$ is infinite, *false* if $Z(P)$ is empty, *true and at least one point on each semi-algebraically connected component* if $Z(P)$ is not empty.

1. Perform GröbnerCompute on $\mathcal{G}$. Set $\widetilde{G}$ to the output.
2. Use Test-Dim on $\widetilde{G}$. If it returns *false*, then return *no answer*.
3. Use change-center on P. Then perform RUR on the returned Gröbner basis of $\mathcal{C}(B)$.
4. Perform RealRootCount on the first polynomial of the computed RUR.

Note that any point B taken at random is good, so the change of center part of the algorithm is not used much in practice.

3.3 Case 3

Now, we deal with the last case, when $\mathcal{Z}(\mathcal{G})$ is infinite.

The idea for this case is to make an infinitesimal deformation of our algebraic set $Z(P)$ to get a smooth hypersurface, to solve the problem after deformation and to come back to the original problem.

We denote by $R\langle\varepsilon\rangle$ (resp. $C\langle\varepsilon\rangle$) the real closed field (resp. algebraically closed field) of *algebraic Puiseux series with coefficients in R (resp. C)* (see [5, 31]). Let $\alpha = \sum_{i\geq i_0} a_i\varepsilon^{i/q}$ be an element of $R\langle\varepsilon\rangle$ (resp. $C\langle\varepsilon\rangle$) where $i_0 \in \mathbb{Z}$, $q \in \mathbb{N}$ and $a_i \in R$ (resp. C), $a_{i_0} \neq 0$ (by convention, $a_i = 0$ if $i < i_0$). The rational $o(\alpha) = i_0/q$ is the *order* of α, the *initial coefficient* $\mathrm{in}(\alpha)$ of α is the coefficient of $\varepsilon^{O(\alpha)}$ in α. The element α is said to be *bounded over R (resp. C)* if $o(\alpha)$ is non negative. The elements of $R\langle\varepsilon\rangle$ (resp. $C\langle\varepsilon\rangle$) bounded over R (resp. over C) form a valuation ring $R_b\langle\varepsilon\rangle$ (resp. $C_b\langle\varepsilon\rangle$), the function $\lim_0$, from $R_b\langle\varepsilon\rangle$ to R (resp. $C_b\langle\varepsilon\rangle$ to C) defined by $\lim_0(\alpha) = a_0$ is a ring homomorphism. The element α is said to be *infinitesimal* over R (resp. C) if $o(\alpha)$ is positive. Points $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$ in $R\langle\varepsilon\rangle^k$ (resp. $C\langle\varepsilon\rangle^k$) are *infinitesimally close* if for all $i = 1, \ldots, k$, $x_i - y_i$ is infinitesimal.

If $S_\varepsilon \subset R[\varepsilon][X_1, \ldots, X_k]$ is a zero-dimensional polynomial system, we denote by $\mathcal{Z}_b(S_\varepsilon) \subset C\langle\varepsilon\rangle^k$ (resp. $Z_b(S_\varepsilon) \subset R\langle\varepsilon\rangle^k$) the set of bounded solutions of S_ε, with coordinates in $R_b\langle varepsilon\rangle^k$ (resp. $C_b\langle\varepsilon\rangle^k$). Note that $\lim_0(\mathcal{Z}_b(S_\varepsilon)) = \lim_0(\mathcal{Z}_b(S_{-\varepsilon}))$, where $S_{-\varepsilon}$ is the polynomial system obtained by substituting $-\varepsilon$ to ε in the elements of S_ε. Note also that

$$\lim_0(Z_b(S_\varepsilon) \cup Z_b(S_{-\varepsilon})) \subset \lim_0(\mathcal{Z}(S_\varepsilon)) \cap R^k.$$

The following result is a well known consequence of Sard's theorem.

Lemma 3.5 *The algebraic sets defined by $P - \varepsilon = 0$ (resp. $P + \varepsilon = 0$) in C^k are smooth hypersurfaces (i.e. their set of singular points is empty).*

We are going to explain how the bounded points of the algebraic sets defined by $P - \varepsilon = 0$ and $P + \varepsilon = 0$ are related to the algebraic set defined by P.

Lemma 3.6

$$\lim_0(Z_b(P - \varepsilon) \cup Z_b(P + \varepsilon)) = \lim_0(\mathcal{Z}_b(P - \varepsilon) \cap R^k = \\ = \{M \in R^k \mid P(M) = 0\}.$$

Proof:

- Take $M \in R^k$ such that $P(M) = 0$. In all the balls of R^k of center M, there exists a point N such that $P(N) \neq 0$. So according to the curve selection lemma, there exists a semi- algebraic function from $[0,1]$ to R^k, with $\phi(0) = M$, $P^2(\phi(x)) > 0$ for $x \in]0,1]$. So denoting by ϕ_ε the extension of ϕ to $R\langle\varepsilon\rangle$, and using the intermediate value theorem, there exists y with $P(\phi_\varepsilon(y))^2 = \varepsilon^2$. Since $\lim_0(P(\phi_\varepsilon(y))) = P(\phi(\lim_0(y))) = 0$, $\lim_0(y) = 0$ and $\lim_0(\phi_\varepsilon(y)) = M$. It is clear that $\phi_\varepsilon(y)$ is bounded over R.

- Let $N \in C\langle\varepsilon\rangle^k$ be a bounded point such that $P(N) - \varepsilon = 0$. We denote $M = \lim_0(N)$. By applying the ring homomorphism $\lim_0$, we have $P(M) = 0$.

□

Let $\mathcal{C}_\varepsilon(A)$ be the polynomial system defined by

$$P = \varepsilon,\ \overrightarrow{\text{grad}}_M\ (P) /\!/\ \overrightarrow{AM}\ .$$

and $\mathcal{I}_{\varepsilon,A} = \langle \mathcal{C}_\varepsilon(A)\rangle$.

Lemma 3.7 $\lim_0(\mathcal{Z}_b(\mathcal{C}_\varepsilon)(A)) \cap R^k$ *meets every semi-algebraically connected component of* $Z(P)$.

Proof: Let D be a semi-algebraically connected component of $Z(P)$ and $\mathcal{M}$ be the subset of points of D at minimal distance from the origin. Let $r > 0$ be small enough so that the closed and bounded semi algebraic set

$$T = \{x \in R^k \mid \exists y \in \mathcal{M}\ \text{dist}(x, \mathcal{M}) \leq r\}$$

does not intersect $Z(P) \setminus D$. According to Lemma 3.6, there exists $N \in Z_b(P^2 - \varepsilon^2)$ with $\lim_0(N) \in \mathcal{M}$. Denoting

$$T' = \{x \in R^k \mid \exists y \in \mathcal{M}\ \text{dist}(x, \mathcal{M}) = r\}$$

we notice that the points of $Z_b(P^2 - \varepsilon^2) \cap T'$ are infinitesimally closed of points of $Z(P) \cap T'$ which are not at minimal distance from A. So the minimal distance from A to $Z(P^2 - \varepsilon^2) \cap T$ is not obtained on T'. Thus this minimal distance is obtained at a bounded point N which is a critical point of the distance function to A on $Z(P^2 - \varepsilon^2)$. It is clear that $\lim_0(N) \in \mathcal{M}$. □

According to the preceding results, if we find a point A such that $\mathcal{C}_\varepsilon(A)$ is zero-dimensional and design a black box which computes $\lim_0(\mathcal{Z}_b(\mathcal{C}_\varepsilon(A))) \cap R^k$, we get a point in every semi-algebraically connected component of the zero set of P.

We denote by **DetectBounded Roots Algo** the following blackbox :

- It takes as input S_ε a zero-dimensional polynomial system of $K[\varepsilon][X_1, \ldots, X_k]$ and a Gröbner basis G_ε of $I_\varepsilon = \langle S_\varepsilon \rangle$ for any admissible monomial ordering.
- It returns a list of Rational Univariate Representations with coefficients in K, counts and describes the solutions in R of their first polynomial.

The set of points associated in C^k to these RUR is $\lim_0(\mathcal{Z}_b(S_\varepsilon))$, while the set of points associated in R^k to these RUR is equal to $\lim_0(\mathcal{Z}_b(S_\varepsilon)) \cap R^k$.

In section 4, we design a version of this black box. It is optimized in section 5.3. Modulo these blackboxes we have the following algorithm.

Algorithm 3

- **Input:** a polynomial $P \in K[X_1, \ldots, X_k]$.
- **Output:** *false* if $Z(P)$ is empty, *true and at least one point on each semi-algebraically connected component* if $Z(P)$ is not empty.

1. Perform GröbnerCompute on $\mathcal{G}$, defined by
$$P(M) = 0,\ \overrightarrow{\text{grad}}_M\ (P) = 0.$$
Set $\widetilde{G}$ to the output. Use Test-Dim on $\widetilde{G}$. If it returns *false*, go to 3.
2. Use change-center . Then perform RUR on the returned Gröbner basis. Use RealRootCount on the first polynomial of the computed RUR.
3. Use change-center with input $P - \varepsilon$, return a good center B and a Gröbner basis G_ε of $\mathcal{I}_{\varepsilon,B}$.
4. Use DetectBounded Roots Algo on $\mathcal{C}_\varepsilon(B)$.

4 Computing limits of bounded solutions

In this section we describe an algorithm performing **DetectBounded Roots Algo**. An optimized version of this black box is designed in the next section.

Let S_ε be a zero-dimensional polynomial system in $K[\varepsilon][X_1, \ldots, X_k]$ and $A_\varepsilon = K(\varepsilon)[X_1, \ldots, X_k]/\langle S_\varepsilon \rangle$.

We are going to explain how to compute a list of Rational Univariate Representations with coefficients in K, such that the set of points associated in C^k to these RUR will be $\lim_0(\mathcal{Z}_b(S_\varepsilon))$, while the set of points associated in R^k to these RUR will be equal to $\lim_0(\mathcal{Z}_b(S_\varepsilon)) \cap R^k$.

We give full details about this blackbox in this paper since the algorithms designed to solve this problem [3, 28] are not correct.

Note that since u is with coefficients in K, the image by u of bounded elements of $\mathcal{Z}(S_\varepsilon)$ in $C\langle\varepsilon\rangle^k$ are bounded. We denote by $Z = \lim_0(\mathcal{Z}_b(S_\varepsilon))$.

Definition 4.1 *A* well separating element $u = \sum_{i=1,\ldots,k} u_i X_i$, $u_i \in K$ *for* S_ε *is a separating element such that* u *is a bijection from* Z *to the bounded roots of* $f_u(\varepsilon, T)$.

In order to illustrate the phenomena that can appear in the $\lim_0$ process, we consider the following examples :

- **Example 1 :** Consider the polynomial system $XY = 1, X = \varepsilon$, the only solution is
$$(\varepsilon, \frac{1}{\varepsilon})$$
which is unbounded, $u = X$ sends this solution to ε which is bounded, so X is separating.

- **Example 2 :** Consider the polynomial system $X^2 + Y^2 - 1 = 0, \varepsilon Y = X$, the only solutions are
$$(\frac{\varepsilon}{(1+\varepsilon^2)^{1/2}}, \frac{1}{(1+\varepsilon^2)^{1/2}}), (\frac{-\varepsilon}{(1+\varepsilon^2)^{1/2}}, \frac{-1}{(1+\varepsilon^2)^{1/2}})$$
which are bounded and not infinitesimally close, $u = X$ sends these solutions to
$$\frac{\varepsilon}{(1+\varepsilon^2)^{1/2}}, \frac{-\varepsilon}{(1+\varepsilon^2)^{1/2}},$$
which are infinitesimally close. So $f_u(\varepsilon, T)$ has one single bounded root while Z has two points.

In examples 1 and 2, X is not well separating while Y is.

We explain now how to find a well separating element.

A rational function f in $K(\varepsilon)$ can be uniquely written under the form $\varepsilon^{o(f)}\frac{a(\varepsilon)}{b(\varepsilon)}$ with $\nu \in \mathbb{Z}$, $a(0)b(0) \neq 0$. The integer number $o(f)$ is the order of f. We denote by $K_b(\varepsilon)$ the ring of elements of $K(\varepsilon)$ with a positive order.

Let $u = u_1X_1 + \ldots + u_kX_k$, $u_i \in K$, be a separating element of S_ε. Since the polynomial system S_ε is contained in $K[\varepsilon][X_1, \ldots, X_k]$, the polynomials

$$(f_u(\varepsilon, T), \tilde{g}_0(\varepsilon, T), \tilde{g}_1(\varepsilon, T), \ldots, \tilde{g}_k(\varepsilon, T))$$

of the ARUR associated to u are elements of $K(\varepsilon)[T]$. Note that $f_u(\varepsilon, T)$ is monic. Let ν be the smallest integer such that $\varepsilon^\nu f_u(\varepsilon, T)$ to $K_b(\varepsilon)[T]$, We define

$$(F_u(\varepsilon, T), G_0(\varepsilon, T), G_1(\varepsilon, T), \ldots, G_k(\varepsilon, T)),$$

the Normalized Rational Univariate Representation (NRUR) as

$$(\varepsilon^\nu f_u(\varepsilon, T), \varepsilon^\nu \tilde{g}_0(\varepsilon, T), \varepsilon^\nu \tilde{g}_1(\varepsilon, T), \ldots, \varepsilon^\nu \tilde{g}_k(\varepsilon, T)).$$

This NRUR describes the same points as the initial RUR.

Note that $G_0(\varepsilon, T)$ is the derivative of $F_u(\varepsilon, T) = \varepsilon^\nu f_u(\varepsilon, T)$, so $G_0(\varepsilon, T) \in K_b(\varepsilon)[T]$ while it may happen that some $G_i(\varepsilon, T)$ do not belong to $K_b(\varepsilon)[T]$.

In example 1

$$G_0(\varepsilon, T) = 1, G_1(\varepsilon, T) = \varepsilon, G_2(\varepsilon, T) = \frac{1}{\varepsilon}.$$

Similarly to separating element (see last item of Proposition 2.1), well separating elements can be chosen in a set $\mathcal{U}'$ defined in advance.

Lemma 4.2 *A well separating element u for S_ε can be chosen among the elements of the family*

$$\mathcal{U}' = \{X_1 + jX_2 + \ldots + j^{k-1}X_k, j = 0 \ldots (k-1)D^2\}.$$

Proof : Define

1. $\mathcal{W}_1$, of cardinality $\leq D(D-1)/2$, to be the set of vectors $x - y$ with x and y distinct solutions of S_ε in $C\langle\varepsilon\rangle^k$,

2. $\mathcal{W}_2$, of cardinality $\leq D$, to be the set of vectors $c = (c_1, \ldots, c_k)$ with c_i the coefficient of $\varepsilon^{\min_{i=1,\ldots,k}(o(x_i))}$ in x_i,

3. $\mathcal{W}_3$, of cardinality $\leq D(D-1)/2$, to be the set of vectors $\lim_0(x) - \lim_0(y)$ with x and y distinct non infinitesimally close bounded solutions of S_ε in $C\langle\varepsilon\rangle^k$,

4. $\mathcal{W} = \mathcal{W}_1 \cup \mathcal{W}_2 \cup \mathcal{W}_3$. Note that $\mathcal{W}$ is of cardinality $\leq D^2$.

Since $o(u(x)) = \min_{i=1,\ldots,k}(o(x_i))$ for every $x \in \mathcal{Z}(S_\varepsilon)$ implies that the polynomials $G_1(\varepsilon, T), \ldots, G_k(\varepsilon, T)$ belong to $K_b(\varepsilon)[T]$, an element $u = X_1 + \ldots + j^{k-1}X_k$ is well separating if for every $w \in \mathcal{W}$, $w_1 + \ldots + j^{k-1}w_k \neq 0$. For a fixed $w \in \mathcal{W}$, there are at most $k-1$ elements of $\mathcal{U}'$ which satisfy $w_1 + \ldots + j^{k-1}w_k = 0$. This is because an element $X_1 + jX_2 + \ldots + j^{k-1}X_k$ satisfying $w_1 + \ldots + j^{k-1}w_k = 0$ is such that $P_w(j) = 0$, with $P_w(T) = w_1 + Tw_2 + \ldots + T^{k-1}w_k$ and $P_w(T)$, which is non zero, has at most $k-1$ roots. So the result is clear by the pigeon-hole principle. □

We relate now roots of $f_u(\varepsilon, T)$ in $C\langle\varepsilon\rangle$ and roots of $F_u(0, T)$ when u is well separating.

Lemma 4.3 *Let u be a well separating element for S_ε.*

- *The polynomial $f_u(\varepsilon, T)$ has unbounded roots in $C\langle\varepsilon\rangle$ if and only if $\deg_T(F_u(0, T)) < \deg_T(f_u(\varepsilon, T))$,*
- *$\nu = \sum_{j=\ell+1,\ldots,p} -o(\alpha_j)\mu_j$ where $\alpha_{\ell+1}, \ldots, \alpha_p$ are the unbounded roots of $f_u(\varepsilon, T)$ with negative orders $o(\alpha_j)$ and multiplicities μ_j,*
- *if α is a root of $f(\varepsilon, T)$ in $C\langle\varepsilon\rangle$ bounded over C, then $a = \lim_0(\alpha)$ is a root of $F_u(0, T)$.*

Proof : Let $\alpha_1, \ldots, \alpha_\ell$ be the bounded roots of $f_u(\varepsilon, T)$, with multiplicities μ_j. We have

$$f_u(\varepsilon, T) = \prod_{j=1}^{\ell}(T - \alpha_j)^{\mu_j} \prod_{j=\ell+1}^{p}(T - \alpha_j)^{\mu_j} \in K(\varepsilon)[T],$$

and it is clear that the order of the coefficient of $T^{\sum_{j=1}^{\ell}\mu_j}$ in $f_u(\varepsilon, T)$ is exactly $\sum_{j=\ell+1}^{p}\mu_j o(\alpha_j)$, and that the order of any other coefficient of $f_u(\varepsilon, T)$ is

smaller than $\sum_{j=\ell+1}^{p} \mu_j o(\alpha_j)$. Denoting $\varepsilon_j = \varepsilon^{-o(\alpha_j)}$ (for $j = \ell+1, \ldots, p$), it is clear that

$$F_u(\varepsilon, T) = \prod_{j=\ell+1}^{p} (\varepsilon_j T - \varepsilon_j \alpha_j)^{\mu_j} \prod_{j=1}^{\ell} (T - \alpha_j)^{\mu_j} \in K_b(\varepsilon)[T].$$

Denoting $a_j = \lim_0(\alpha_j)$ for $j = 1, \ldots, \ell$, $c = \prod_{j=\ell+1}^{p} (-\mathrm{in}(\alpha_j))^{\mu_j}$,

$$F_u(0, T) = c \prod_{j=1}^{\ell} (T - a_j)^{\mu_j}.$$

□

Lemma 4.4 *If $u = u_1 X_1 + \ldots + u_k X_k$, $u_i \in K$, is separating, such that $\varepsilon^\nu g_1(\varepsilon, T) \ldots, \varepsilon^\nu g_k(\varepsilon, T) \in K_b(\varepsilon)[T]$, and u is injective on the bounded zeros of $\mathcal{S}_\varepsilon$ in $C\langle\varepsilon\rangle^k$, then u is well separating for $\mathcal{S}_\varepsilon$.*

More precisely if t is a root of $F_u(0, T)$ with multiplicity n then, there exists a root τ of $f_u(\varepsilon, T)$ in $C\langle\varepsilon\rangle$ with $\lim_0(\alpha) = a$. Moreover for every bounded τ root of $f_u(\varepsilon, T)$ in $C\langle\varepsilon\rangle$ of multiplicity μ with $\lim_0(\alpha) = a$,

$$\lim_0 \left(\frac{g_i^{\mu-1}(\varepsilon, \alpha)}{g_0^{\mu-1}(\varepsilon, \alpha)} \right) = \frac{g_i^{(n-1)}(0, a)}{g_0^{(n-1)}(0, a)}.$$

Proof : With the same notation as above,

$$G_0(0, T) = c(\sum_{j=1}^{l} \mu_j (T - a_j)^{\mu_j - 1} \prod_{m \in \{1, \ldots, \ell\} \setminus \{j\}} (T - a_m)^{\mu_m}).$$

Suppose that $a = \lim_0(\alpha_1) = \ldots = \lim_0(\alpha_s)$, $a \neq \lim_0(\alpha_j), j > s$, then

$$G_0^{(n-1)}(0, a) = c.n! \prod_{j=n+1}^{\ell} (a - a_j),$$

where $n = \mu_1 + \ldots + \mu_s$.

Denoting by ξ_j the unique point of $\mathcal{Z}(S_\varepsilon)$ such that $u(\xi_j) = \alpha_j$, and ξ_{ij} the i-th coordinate of ξ_j, we have also

$$\tilde{g}_i(\varepsilon, T) = \sum_{j=1}^{p} \xi_{ij}\mu_j (T-\alpha_j)^{\mu_j - 1} \prod_{m\in\{1,\dots p\}\setminus\{j\}} (T-\alpha_m)^{\mu_m}$$

$$G_i(\varepsilon, T) = \sum_{j=1}^{\ell} \xi_{ij}\mu_j (T-\alpha_j)^{\mu_j - 1} \prod_{m\in\{1,\dots \ell\}\setminus\{j\}} (T-\alpha_m)^{\mu_m} \prod_{m=\ell+1}^{p} (\varepsilon_m T - \varepsilon_m\alpha_m)^{\mu_m}$$

$$+ \prod_{m=1}^{\ell} (T-\alpha_m)^{\mu_m} \Big(\sum_{j=\ell+1}^{p} \varepsilon_j \xi_{ij}\mu_j (\varepsilon_j T - \varepsilon_j\alpha_j)^{\mu_j - 1} \prod_{m\in\{\ell+1,\dots p\}\setminus\{j\}} (\varepsilon_m T - \varepsilon_m\alpha_m)^{\mu_m} \Big).$$

It is clear that

$$A = \sum_{j=1}^{\ell} \xi_{ij}\mu_j (T-\alpha_j)^{\mu_j - 1} \prod_{m\in\{1,\dots \ell\}\setminus\{j\}} (T-\alpha_m)^{\mu_m} \prod_{m=\ell+1}^{p} (\varepsilon_m T - \varepsilon_m\alpha_m)^{\mu_m} \in C_b\langle\varepsilon\rangle[T].$$

Since $G_i(\varepsilon, T) \in K_b(\varepsilon)[T]$, $\prod_{m=1}^{\ell} (T-\alpha_m)^{\mu_m} \in C_b\langle\varepsilon\rangle[T]$ is monic,

$$G_i(\varepsilon, T) = A + \prod_{m=1}^{\ell} (T-\alpha_m)^{\mu_m} B$$

with $B \in C_b\langle\varepsilon\rangle[T]$. So that

$$G_i(0, T) = \bar{A} + \prod_{m=1}^{\ell} (T-a_m)^{\mu_m} \bar{B},$$

with $\lim_0(\alpha_j) = a_j$, $\bar{A}$ and $\bar{B}$ the polynomials of $C[T]$, obtained by replacing each coefficient c of A and B by $\lim_0(c)$. So, since $a = \lim_0(\alpha_1) = \dots = \lim_0(\alpha_s)$, $a \neq \lim_0(\alpha_j), j > s$, denoting by $x = \lim_0(\xi_1) = \dots = \lim_0(\xi_s)$, with $u(\xi_i) = \alpha_i$,

$$G_i^{(n-1)}(0, a) = c.n! x_i \prod_{j=n+1}^{\ell} (a - a_j),$$

where $n = \mu_1 + \ldots + \mu_s$ and finally

$$x_i = \frac{G_i^{(n-1)}(0,a)}{G_0^{(n-1)}(0,a)}.$$

□

The following naive-and inefficient- algorithm can be used to find a well separating element :

Naivewell-sepElement

- **Input :** A zero-dimensional S_ε of $K[\varepsilon][X_1,\ldots,X_k]$ and a Gröbner basis G_ε of the ideal I_ε generated by S_ε, for any admissible monomial ordering.
- **Output :** a well separating element u of S_ε, a square free decomposition of $F_u(0,T)$ and
$$(G_0(0,T), G_1(0,T), \ldots, G_k(0,T))$$
the NRUR for u.

1. For every $u \in \mathcal{U}'$
   - Check if u is separating using ChecksepElement.
   - Compute the NRUR associated to u
   $$(F_u(\varepsilon,T), G_0(\varepsilon,T), G_1(\varepsilon,T), \ldots, G_k(\varepsilon,T)),$$
   keep u only if the NRUR belongs to $K_b(\varepsilon)[T]$.
2. Choose among elements of $\mathcal{U}'$ kept in Step 1 u such that the degree of the square-free part of $F_u(0,T)$ is maximum.
3. Compute the square free decomposition of $F_u(0,T)$
$$F_u(0,T) = f_1 f_2^2 \ldots f_m^m.$$
4. Return $(u, f_1, \ldots, f_m)$ and
$$(G_0(0,T), G_1(0,T), \ldots, G_k(0,T)).$$

The multiplicity of a point x of Z is the sum of the multiplicities of the points $\xi \in \mathcal{Z}(S_\varepsilon)$ such that $\lim_0(\xi) = x$.

Lemma 4.5 *Let $u = u_1X_1 + \ldots + u_kX_k$, $u_i \in K$, be such that the NRUR belongs to $K_b(\varepsilon)[T]$. Let $h_i(\varepsilon, \Lambda_i)$ be the characteristic polynomial of the map of multiplication by X_i in A_ε, and $H_i \in K_b(\varepsilon)[\Lambda_i], H_i \notin \varepsilon K_b(\varepsilon)[\Lambda_i]$ a convenient multiple of h_i, called a normalized characteristic polynomial of X_i. Let $F_u(0,T) = f_1 f_2^2 \ldots f_m^m$, with all f_n square free, be the square-free decomposition of $F_u(0,T)$. The element u is well separating if and only if, defining*

$$K_i(\Lambda_i) = \prod_{n=1}^{m} \mathrm{Res}(G_0(0,T)^{(n-1)}\Lambda_i - G_i(0,T)^{(n-1)}, f_n)^n,$$

K_i divides $H_i(0, \Lambda_i)$.

Proof : If u is well separating, the roots of K_i are roots of the form

$$x_i = \frac{G_i^{(n-1)}(0,a)}{G_0^{(n-1)}(0,a)}$$

where a is a root of f_n (i.e. a root of multiplicity n of $F_u(0,T)$) and $u(x) = a$. So the roots of K_i are roots of $H_i(0,\Lambda_i)$ with the same multiplicities.

Conversely, if u is not well separating, there exists a root a of $G(0,T)$ with $x_1, \ldots, x_s$ elements of Z of multiplicities $n_1, \ldots, n_s$ and $u(x_1) = \ldots = u(x_s) = a$. Let $n = n_1 + \ldots + n_s$, then it is clear from the definitions that

$$\frac{G_i^{(n-1)}(0,a)}{G_0^{(n-1)}(0,a)} = \frac{n_1x_1 + \ldots + n_sx_s}{n}.$$

So the s-tuple $x_1, \ldots, x_s$ is replaced by the barycenter b of the points x_i with weights n_i. We can conclude using next lemma that there exists a root x_i of some $H_i(0,\Lambda_i)$ of multiplicity n whose multiplicity in K_i is $> n$. □

Lemma 4.6 *Let Z be a finite multiset consisting of points $x \in C^k$ with multiplicities $\mu(x)$. We denote by $\Pi_i(Z)$ the multiset obtained by projecting points of Z on their i-th coordinate (adding the multiplicities if points have the same i-th coordinate). Let Z'be a multiset obtained by replacing finite disjoint subsets of Z by their barycenter (taking into account multiplicities). Then $Z \neq Z'$ if and only if there exists an i such that $\Pi_i(Z) \neq \Pi_i(Z')$.*

Proof : Suppose that $Z \neq Z'$ and denote by W the subset of points of Z that are no more in Z', and let H be the convex hull of W. Let x be any extreme point of H, and i such that x_i is distinct from the i-th coordinate of the barycenter replacing it. Since a barycenter of points is contained in the interior of the convex hull of these points, the multiplicity of $\Pi_i(Z')$ at x_i is strictly smaller that the multiplicity of $\Pi_i(Z)$ at x_i. It follows that there is a point y such that the multiplicity of $\Pi_i(Z')$ at y_i is strictly bigger than the multiplicity of $\Pi_i(Z)$ at y_i. □

According to the above Lemmas, the following **well-sepElement Algo** can be used for producing a well separating element.

well-sepElement Algo

- **Input :** A zero-dimensional S_ε of $K[\varepsilon][X_1, \ldots, X_k]$ and a Gröbner basis G_ε of the ideal generated by S_ε, for any admissible monomial ordering.
- **Output :** a well separating element u of S_ε, a square free decomposition of $F_u(0,T)$ and
$$(G_0(0,T), G_1(0,T), \ldots, G_k(0,T))$$
the NRUR for u.

1. Compute for every i H_i a normalized characteristic polynomials of X_i in A_ε.
2. Choose $u \in \mathcal{U}'$. Remove u from $\mathcal{U}'$.
3. Check if u is separating, using ChecksepElement.
4. Compute the NRUR
$$(F_u(\varepsilon,T), G_0(\varepsilon,T), G_1(\varepsilon,T), \ldots, G_k(\varepsilon,T)),$$
if it is not in $K_b(\varepsilon)[T]$, go to 2.
5. Compute the square free-decomposition
$$F_u(0,T) = f_1 f_2^2 \ldots f_m^m.$$
Compute
$$K_i(\Lambda_i) = \prod_{n=1}^{m} \mathrm{Res}(G_0(0,T)^{(n-1)}\Lambda_i - G_i(0,T)^{(n-1)}, f_n)^n,$$
If there exists i such that K_i does not divide $H_i(0,\Lambda_i)$, go to 1.
6. Return$(u, , f_1, \ldots, f_m)$ and
$$(G_0(0,T), G_1(0,T), \ldots, G_k(0,T)).$$

In example 2, when $u = X$, $F_u(\varepsilon,T) = (1+\varepsilon^2)T^2 - \varepsilon^2$ is square-free and $F_u(0,T) = T^2$. The normalized characteristic polynomial $H_2(\varepsilon,\Lambda_2)$ of the multiplication by Y is $(1+\varepsilon^2)\Lambda_2^2 - 1$, so $H_2(0,\Lambda_1) = \Lambda_2^2 - 1$, while $G_0(\varepsilon,T) = 2(1+\varepsilon^2)T$, $G_0(0,T) = 2T$, $G_1(\varepsilon,T) = 2\varepsilon^2$ $G_2(0,T) = 0$, $K_2(0,\Lambda_2) = \Lambda_2^2$. So we can conclude (without looking at the roots) that $u = X$ is not a well separating element.

Now, we explain how $Z = \lim_0(\mathcal{Z}_b(S_\varepsilon))$ can be computed from a well separating element.

Detect-Bounded Roots Algo

- **Input :** S_ε be a zero-dimensional polynomial system of $K[\varepsilon][X_1,\ldots,X_k]$ and G_ε a Gröbner basis of the ideal I_ε generated by S_ε for any admissible monomial ordering.
- **Output :**A list of real solutions of rational univariate representations containing the limits of the bounded roots in $R\langle\varepsilon\rangle$ of I_ε.
- Use well-sepElement Algo.
- Return($listrurs = \{(f_n, G_0(0,T)^{(n-1)}, G_1(0,T)^{(n-1)}\ldots, G_k(0,T)^{(n-1)})\}$),
- For every element of $listrurs$ use RealRootCount on its first polynomial.

Example 3. We are going to prove that the zero set of the equation $Y^2+(XY-1)^2$ is empty by studying $Y^2+(XY-1)^2-\varepsilon$. It is easy to check that the variable X is a separating element For the polynomial system

$$P(X,Y)=\varepsilon,\ \overrightarrow{\text{grad}}_{X,Y}\ (P)//(X,Y).$$

Its characteristic polynomial is

$$F(\varepsilon,X)=\varepsilon X^{10}+(4\varepsilon-1)X^8+(-3-2\varepsilon^2+4\varepsilon)X^6+(10\varepsilon-1-4\varepsilon^2)X^4$$
$$+(10\varepsilon-7+\varepsilon^3-4\varepsilon^2)X^2-\varepsilon^2+2\varepsilon-1$$

We have :

$$G_0(\varepsilon,X)=10\varepsilon X^9+8(4\varepsilon-1)X^7+6(-3-2\varepsilon^2+4\varepsilon)X^5$$
$$+4(10\varepsilon-1-4\varepsilon^2)X^3+2(10\varepsilon-7+\varepsilon^3-4\varepsilon^2)X,$$
$$G_1(\varepsilon,X)=10\varepsilon X^8+(16\varepsilon-8)X^6+(4\varepsilon^2-10\varepsilon-4)X^4$$
$$+(-8\varepsilon^2-4\varepsilon+12)X^2+2(\varepsilon-1)(\varepsilon^2-2\varepsilon+1),$$
$$G_2(\varepsilon,X)=(-8\varepsilon+2)X^8+(12+8\varepsilon^2-16\varepsilon)X^6+(-60\varepsilon+6+24\varepsilon^2)X^4$$
$$+(-80\varepsilon+56-8\varepsilon^3+32\varepsilon^2)X^2+10\varepsilon^2-20\varepsilon+10.$$

So, we have :

$$F(0,X)=-X^8-3X^6-X^4-7X^2-1$$
$$G_0(O,X)=-8X^7-18X^5-4X^3-14X$$
$$G_1(0,X)=-8X^6-4X^4+12X^2-2$$
$$G_2(0,X)=2X^8+12X^6+6X^4+56X^2+10$$

The normalized characteristic polynomial $H_1(\varepsilon, \Lambda_1)$ is equal to :

$$H_1(\varepsilon, \Lambda_1) = \Lambda_1^{10} - \varepsilon\Lambda_1^8 + (-2\varepsilon - 2)\Lambda_1^6 + (2\varepsilon + 1 + 2\varepsilon^2)\Lambda_1^4 + (\varepsilon^2 - 2\varepsilon + 1)\Lambda_1^2 - \varepsilon - \varepsilon^3 + 2\varepsilon^2$$

and

$$H_1(0, \Lambda_1) = \Lambda_1^{10} - 2\Lambda_1^6 + \Lambda_1^4 + \Lambda_1^2.$$

Now, we can compute $K_1(\Lambda_1)$ and $K_2(\Lambda_2)$ to check if the variable X is a well separating element.

$$K_1(\Lambda_1) \text{ is proportional to } -\Lambda_1^8 + 2\Lambda_1^4 - \Lambda_1^2 - 1$$
$$K_2(\Lambda_2) = F(0, \Lambda_2).$$

Since K_1 divides $H_1(0, \Lambda_1)$ and $K_2 = H_1(0, \Lambda_1)$, X is a well separating element.

Since $F(0, X)$ has no real roots, one can conclude that $Y^2 + (XY - 1)^2$ has no real roots.

5 Optimizations

We improve now Algorithm 3 in Section 3 to avoid as much as possible computations with infinitesimals.

5.1 Computing a Gröbner basis in $R\langle\varepsilon\rangle[X_1, \ldots, X_k]$

We need a Gröbner basis of the ideal generated by $\mathcal{C}_\varepsilon(B)$ in $R\langle\varepsilon\rangle[X_1, \ldots, X_k]$ in order to decide if B is a good center for $P - \varepsilon$ and to compute a Rational Univariate Representation of $\mathcal{Z}(\mathcal{C}_\varepsilon(B))$.

Since $\mathcal{C}_\varepsilon(B) \subset K[\varepsilon][X_1, \ldots, X_k]$ we can proceed as follows.

Definition 5.1 *An E-specialization* Φ *is a homomorphism*

$$\Phi : R[E] \longrightarrow R,$$

it is defined by the image e *of* E *by* Φ*.*

We consider an order eliminating the variables $X_1, \ldots, X_k$ on the monomials of $R[E, X_1, \ldots, X_k]$ (i.e. E is smaller than all the X_i), and the restriction of this order to $X_1, \ldots, X_k$, we denote by $\mathrm{lm}_{X_1,\ldots,X_k}(P)$ the leading monomial of P for this order and by $\mathrm{lt}_{X_1,\ldots,X_k}(P)$ the leading term.

Definition 5.2 *For all P in $R[E, X_1, \ldots, X_k]$, we define,*

$$P = \mathrm{lc}(P)X^A + Q$$

with $\mathrm{lc}(P) \in R[E]$ *and* $\mathrm{lm}_{X_1,\ldots,X_k}(Q) < \mathrm{lm}_{X_1,\ldots,X_k}(P) = X^A$. *Then, if* $e \in R$ *is not a root of* $\mathrm{lc}(P)$, *denoting* $c = \mathrm{lc}(P(e))$,

$$\mathrm{lm}_{X_1,\ldots,X_k}(P_e) = X^A$$

$$\mathrm{lt}(P_e) = cX^A.$$

Given a zero-dimensional polynomial system S_ε in $K[\varepsilon][X_1, \ldots, X_k]$, denote by $\mathcal{L}$ the polynomials in the variable E which are the coefficients of the leading monomials of the Groebner basis of $I_E = \langle S_E \rangle$ for an order eliminating $X_1, \ldots, X_k$.

Lemma 5.3 *[13] Let Φ be the E-specialization which sends E to e, and G a Gröbner basis (according to an elimination order of $X_1, \ldots, X_k$) of I_E. If e is not a root of a polynomial in $\mathcal{L}$, then $\Phi(G)$ is a Gröbner basis for $\Phi(I_E)$.*

ε-Gröbner Compute

- **Input:** a polynomial system in $K[\varepsilon][X_1, \ldots, X_k]$, and an elimination order for E.
- **Output:** a non-reduced Gröbner basis in $K(\varepsilon)[X_1, \ldots, X_k]$ for the polynomial system.

1. Replace the input system by the system obtained by substituting to ε a new variable E.
2. Compute a Gröbner basis for the preceding system with respect to an order eliminating $X_1, \ldots, X_k$.
3. Specialize the variable E to ε in the obtained Gröbner basis.

We easily deduce from this εTest-Dim which tests if a polynomial system with coefficients in $K[\varepsilon]$ is zero-dimensional.

5.2 Finding a separating element and a good center

In the Rational Univariate Representation , we find a separating element by choosing an element in $\mathcal{U}$ and checking whether it is separating. Our input polynomials are now in $K[\varepsilon][X_1, \ldots, X_k]$, but we are going to chose a separating element performing computations exclusively in $K[X_1, \ldots, X_k]$. When K is the field of rational numbers, the use of modular arithmetic for checking that an element is separating is particularly efficient.

Suppose that the polynomial system $S_\varepsilon \subset K[\varepsilon][X_1, \ldots, X_k]$ is zero-dimensional and denote $I_\varepsilon = \langle S_\varepsilon \rangle$. Denote by S_e ($e \in K$) the polynomial system obtained by substituting e to ε in S_ε and denote $I_e = \langle S_e \rangle$

Using the notations of the last paragraph, an element e of K which is not a root of a polynomial in $\mathcal{L}$ is such that $\dim(K[X_1, \ldots, X_k]/I_e) = \dim(K\langle\varepsilon\rangle[X_1, \ldots, X_k]/I_\varepsilon)$. Denote by $\mathcal{E}$ the set of elements of C which are not roots of a polynomial in $\mathcal{L}$. It is clear that the complement of $\mathcal{E}$ contains at most a finite number of elements of K.

Lemma 5.4 *The following are equivalent*

a) I_ε is radical,

b) There exists $e_0 \in \mathcal{E} \cap K$ such that I_{e_0} is radical,

c) The complement of $\mathcal{E}' = \{e \in \mathcal{E} \mid I_e$ is radical,$\}$ is finite.

Proof: b) implies c): Obviously, $\mathcal{E}'$ is not empty because $e_0 \in \mathcal{E}'$. Let e be an element of $\mathcal{E}'$. Since I_e is radical, all the solutions of I_e are simple solutions. Moreover, in a neighborhood U of e, the dimension of the quotient is fixed for every $e' \in U$. Thus, the solutions vary continuously. So, there exists a neighborhood of e in which the solutions are simple solutions. Thus, we have proved that $\mathcal{E}'$ is an open set for the euclidean topology. Moreover, since it can be described by a first order formula, $\mathcal{E}'$ is constructible for the Zariski topology. The complement of $\mathcal{E}'$ is a subset of C which is constructible and closed, thus finite.
c) implies a): Since the complement of $\mathcal{E}'$ is finite, there exists an open interval of the type $(0, \alpha)$ (where $\alpha \in R$) such that $\forall e \in (0, \alpha)$, e is an element of $\mathcal{E}'$. Thus, if we denote by $\mathcal{E}'$ the extension of $\mathcal{E}'$ to $R\langle\varepsilon\rangle$, $\varepsilon \in \mathcal{E}'$.
a) implies b): The extension of the open constructible set $\mathcal{E}' = \{e \in \mathcal{E} \mid I_e$ is radical$\}$ to $C\langle\varepsilon\rangle$ contains ε and is non empty. Thus the complement of $\mathcal{E}'$ is finite and $\mathcal{E}' \cap K$ is non empty. □

Let $e_0 \in \mathcal{E} \cap K$, such that S_{e_0} is 0-dimensional and I_{e_0} is radical . Let u be a separating element for S_{e_0}.

Lemma 5.5 *The ideal I_ε is radical and u is a separating element for S_ε.*

Proof: Since the zeroes of I_{e_0} are simple, and the zeroes of I_e remain simple and vary continuously for $e \in \mathcal{E}$ in a neighborhood of e_0, if u is separating for S_{e_0}, then u remains a separating element for S_e in a neighborhood of e.

Consider

$$\mathcal{E}'' = \{e \in \mathcal{E}' \mid I_e \text{ is radical}, u \text{ is separating for} S_e\}.$$

The set $\mathcal{E}''$ is a non empty and open set for the euclidean topology. It is constructible for the Zariski topology as defined by a first order formula. Thus, the complement of $\mathcal{E}''$ which is closed and constructible is a finite set of points. So, $\varepsilon \in \mathcal{E}''$. Then I_ε is a radical ideal and u is a separating element for S_ε. □

Finally we have an improved way of checking that a given element is separating for S_ε in a special case.

ε-ChecksepElement

- **Input :** A zero-dimensional system S_ε of $K[\varepsilon][X_1, \ldots, X_k]$, a Gröbner basis G_ε of $I_\varepsilon = \langle S_\varepsilon \rangle$ for any admissible monomial ordering, an element $e \in K$ such that I_e is radical, $\dim(K[X_1, \ldots, X_k]/I_e) = \dim(K\langle\varepsilon\rangle[X_1, \ldots, X_k]/I_\varepsilon)$, G_e is a Gröebner basis of I_e, and an element $u \in K[X_1, \ldots, X_k]$.
- **Output :** *true* if u is separating for S and *false* if it is not.
- Use ChecksepElement on S_e.

A *good pair* $(B, e) \in R^k \times R$ for P is such that :

- the polynomial system $\mathcal{C}_\varepsilon(B)$ defined by $P - \varepsilon$, $\overrightarrow{\text{grad}}_M\ (P)//\ \overrightarrow{BM}$ is zero-dimensional,
- the polynomial system $\mathcal{C}_e(B)$ $P-e$, $\overrightarrow{\text{grad}}_M\ (P)//\ \overrightarrow{BM}$ is zero-dimensional and the ideal $\mathcal{I}_{B,e} = \langle \mathcal{C}_e(B) \rangle$, is radical,

- $\dim(K[X_1,\ldots,X_k]/\mathcal{I}_{B,e}) = \dim(K\langle\varepsilon\rangle[X_1,\ldots,X_k]/\mathcal{I}_{B,\varepsilon})$ where $\mathcal{I}_{B,\varepsilon} = \langle\mathcal{C}_\varepsilon(B)\rangle$.

Note that a pair (B,e) chosen at random is good.

According to the preceding results and results of section 2, the following strategy finds a good center for $P-\varepsilon$.

ε change-center

- **Input:** $P \in K[X_1,\ldots,X_k]$ such that $\mathcal{Z}(\mathcal{G})$ is infinite.
- **Output:** A good center B for $P-\varepsilon$, a Gröbner basis G_ε of $\mathcal{I}_{B,\varepsilon}$, an element e such that $\mathcal{I}_{B,e}$ is radical, $\dim(K[X_1,\ldots,X_k]/\mathcal{I}_{B,e}) = \dim(K\langle\varepsilon\rangle[X_1,\ldots,X_k]/\mathcal{I}_{B,\varepsilon})$ and G_e is a Gröbner basis of $\mathcal{I}_{B,e}$.

1. Initialize $d=1$.
2. For $B \in \{0,\ldots,d\}^k, e=d$ and $B \in \{0,\ldots,d\}^k \setminus \{0,\ldots,d-1\}^k, e \in \{1,\ldots,d-1\}$, use Test-dim and Test-radical to test if $\mathcal{C}_e(B)$ is zero-dimensional and $\mathcal{I}_{B,e}$ radical.
3. Check that $\mathcal{C}_\varepsilon(B)$ is zero-dimensional by using εTest-Dim .
4. As soon as a pair (B,e) is good, return this pair and the corresponding Gröebner basis of $\mathcal{I}_{B,e}$, G_e.
5. If there is no good pair, increase d by 1 , and return to 2.
6. Return B, a Gröbner basis G_ε of $\mathcal{I}_{B,\varepsilon}$, and e.

5.3 Using infinitesimals with a fixed precision

In the algorithms described before, ε is treated as an independent variable.

Since ε is an infinitesimal, there are steps of the computation where the terms of high degree in ε are not used for the final result. It is then possible to truncate the computation by setting $\varepsilon^p = 0$ for a convenient p. In most cases, setting $\varepsilon^2 = 0$ is sufficient. For any $h(\varepsilon,T) \in K[\varepsilon][X_1,\ldots,X_k]$, we note :

- $h(\varepsilon,T) = \sum_{i\geq 0}^{\text{degree}_\varepsilon(h)} h_i\varepsilon^i$
- $\overline{h}(\varepsilon,T) = \sum_{i\geq 0}^{min(\text{degree}_\varepsilon(h),p)} h_i\varepsilon^i$.

If $G_\varepsilon \subset K[\varepsilon][X_1, \ldots, X_k]$ we define $\bar{G}_\varepsilon = \{\bar{P} \mid P \in G_\varepsilon\}$.

Using such a fixed precision is not possible for the Gröbner basis computation since it could create errors when deciding whether ideals are zero-dimensional. In any case, if the algorithm described in [12] is used for the Gröbner basis computation, the costly part is the Rational Univariate Representation of the ideal I_ε generated by S_ε.

So we compute the Gröbner basis $G_\varepsilon \subset K[\varepsilon][X_1, \ldots, X_k]$ of the ideal I_ε. We obtain, inspecting the Gröbner basis, a precision p_0 such that p_0 is the smallest integer p so that fixing $\varepsilon^p = 0$ the staircase of G_ε and of $\bar{G}_\varepsilon$ coincide.

The fixed precision can be used inside **DetectBounded Roots Algo** computation as we explain now.

We denote by $(F_u(\varepsilon, T), G_0(\varepsilon, T), \ldots, G_k(\varepsilon, T))$ the NRUR of I_ε. If $p < \nu$, the computation of the RUR with fixed precision fails because a division by zero appears somewhere in the computation. So we need to take the precision equal at least to ν.

This gives a new algorithm for the computation of the representation of the bounded solutions of a zero-dimensional system S_ε of $K[\varepsilon][X_1, \ldots, X_k]$ which improves the blackbox **DetectBounded Roots Algo**.

We start by improving the blackbox which find a well separating element.

FixedPrecisionwell-sepElement Algo

- **Input :** A zero-dimensional polynomial system S_ε and a Gröbner basis G_ε of the ideal I_ε generated by S_ε for any admissible monomial ordering, an element $e \in K$ such that I_e is radical, $\dim(K[X_1,\ldots,X_k]/I_e) = \dim(K\langle\varepsilon\rangle[X_1,\ldots,X_k]/I_\varepsilon)$, G_e is a Gröebner basis of I_e.
- **Output :** a well separating element of S_ε, a precision p, a square free decomposition of $F_u(0,T)$ and
$$(\bar{G}_0(0,T), \bar{G}_1(0,T), \ldots, \bar{G}_k(0,T))$$
the NRUR for u and the precision p.

1. Compute the initial precision p_0 from the Gröbner basis, set $p = p_0$, so that $\varepsilon^p = 0$.
2. Compute for every i $\bar{H}_i$ where H_i is a normalized characteristic polynomial of the multiplication by X_i in A_ε.
3. If the computation fails because a division by 0 was needed, set $p := p+1$, fix the new precision $\varepsilon^p = 0$, go to 2.
4. Choose $u \in \mathcal{U}'$. Remove u from $\mathcal{U}'$.
5. Check if u is separating, using ε-ChecksepElement .
6. Compute the NRUR for this precision
$$(\bar{F}_u(\varepsilon,T), \bar{G}_0(\varepsilon,T), \bar{G}_1(\varepsilon,T), \ldots, \bar{G}_k(\varepsilon,T)).$$
7. If the computation fails because a division by 0 was needed, set $p := p+1$, fix the new precision $\varepsilon^p = 0$, go to 6.
8. If the NRUR is not in $K_b(\varepsilon)[T]$, go to 4.
9. Compute the square free-decomposition
$$\bar{F}_u(0,T) = f_1 f_2^2 \ldots f_m^m.$$
Compute
$$K_i(\Lambda_i) = \prod_{n=1}^{m} \mathrm{Res}(\bar{G}_0^{(n-1)}(0,T)\Lambda_i - \bar{G}_i(0,T)^{(n-1)}, f_n)^n,$$
If there exists i such that K_i does not divide $\bar{H}_i(0,\Lambda_i)$, go to 2.
10. Return$(u, f_1, \ldots, f_m)$ and
$$(\bar{G}_0(0,T), \bar{G}_1(0,T), \ldots, \bar{G}_k(0,T)),$$

Finally we have the following algorithm :

FixedPrecision Detect-Bounded Roots Algo

- **Input :** S_ε be a zero-dimensional system of $K[\varepsilon][X_1, \ldots, X_k]$, G_ε a Gröbner basis of the ideal I_ε generated by S_ε for any admissible monomial ordering, an element $e \in K$ such that I_e is radical, $\dim(K[X_1, \ldots, X_k]/I_e) = \dim(K\langle\varepsilon\rangle[X_1, \ldots, X_k]/I_\varepsilon)$, G_e is a Gröebner basis of I_e.
- **Output :**A list of real solutions of rational univariate representations containing the limits of the bounded solutions in $R\langle\varepsilon\rangle$ of S_ε.
- Use FixedPrecisionwell-sepElement Algo.
- Return($listrurs = \{(f_n, \bar{G}_0(0,T)^{(n-1)}, \bar{G}_1(0,T)^{(n-1)} \ldots, \bar{G}_k(0,T)^{(n-1)})\}$).
- For every element of $listrurs$ use RealRootCount on its first polynomial.

We are now ready to describe the improved algorithm which deals with all cases.

The Improved Algorithm

- **Input:** a polynomial P in $K[X_1, \ldots, X_k]$.
- **Output:** *false* if $Z(P)$ is empty, *true and at least one point on each semi-algebraically connected component* if $Z(P)$ is non empty.

1. Use Test-Dim for the polynomial system $P = 0$, $\overrightarrow{\text{grad}}_M(P) = \overrightarrow{0}$. If $\mathcal{Z}(\mathcal{G})$ is infinite go to 3.
2. Use change-center . Then use RUR on the returned Gröbner basis. Use RealRoot-Count on the first polynomial of the RUR output.
3. Perform ε change-center on $P - \varepsilon$.
4. Use FixedPrecision DetectBounded Roots Algo on $\mathcal{C}_\varepsilon(B)$ and G_ε.

6 Some examples

The following computations have been made in order to illustrate our method. The software we used are preliminary versions of FGb (devoted to Gröbner basis computations and developped by J.-C. Faugère) and RS (devoted to the computation of RURs and the study of Real Roots, developped by F.

Rouillier). We compare our method with the Cylindrical Algebraic Decomposition implemented in the Axiom Computer Algebra System by R. Rioboo. This implementation is based on :

- Mc Callum's projection (see [19, 22]) : at the i-th step of projection, a list $\mathcal{L}_i$ of polynomials in $R[X_{i+1}, \ldots, X_k]$ is obtained. The list $\mathcal{L}_{i+1}$ is obtained by taking the square-free basis and the gcd-basis of the list obtained by computing the discriminants of the polynomials in $\mathcal{L}_i$, the resultants of pairs of these polynomials and their coefficients (the polynomials being considered as univariate in the variable X_{i+1}).

- An implementation of the Real Closure (see [23]) : it is used to perform the extension step of CAD. Each cell produced by CAD is represented by a real algebraic number.

Since FGb and RS are very optimized software compared with Axiom, comparing computation times would make no sense. The fact that there are examples where with one method the computation ends in few seconds and with the other method the computation does not end after several hours is in our opinion a relevant information.

Cylindrical Algebraic Decomposition proceeds by elimination of variables one after the other and produces many cells. These cells give a lot of information, more than what is needed to decide only the emptiness of the real hypersurface defined by the input polynomial. This additional information spoils the practical computations since the size of the output is huge. Critical Point Method has been introduced to avoid this problem of CAD. The information output is smaller and more specific.

In the following we give the the number of cells obtained by CAD, the number of points output by our method (as well as the degree of the first polynomial of the computed RUR) and the computation time for our method. All the computations have been performed on a PC Bi-Pentium II (2×400 MHz) with 512 Meg of RAM from CNRS UMS Medicis.

Example 1

Consider

```
P:=2*u6^2*u5*u4*u3*u2+4*u6^2*u5*u4*u3+4*u6^2*u5*u4*u2+
4*u6^2*u5*u3*u2-1
```

The CAD returns 277 cells and outputs 74 real points on the hypersurface. Our method outputs 24 real points on the hypersurface. The degree of the univariate polynomial in the RUR is 150. Our computation time is :

```
FGb : 0,5 sec., RS : 14 sec.
```

Example 2

Consider

```
P:=36*u5^2*u4^2*u3^2*u2^2+88*u5^2*u4^2*u3^2*u2
+32*u5^2*u4^2*u3^2+32*u5^2*u4^2*u3*u2^3
+152*u5^2*u4^2*u3*u2^2-1
```

The CAD returns 203 cells and outputs 60 real points on the hypersurface. Our method outputs 20 real points on the hypersurface. The degree of the univariate polynomial in the RUR is 144. Our computation time is :

```
FGb : 2 sec., RS : 14 sec.
```

Example 3

Consider

```
P:=36*u5^2*u4^2*u3^2*u2^2+88*u5^2*u4^2*u3^2*u2
+32*u5^2*u4^2*u3^2+32*u5^2*u4^2*u3*u2^3
+152*u5^2*u4^2*u3*u2^2+64*u5^2*u4^2*u3*u2
+64*u5^2*u4^2*u2^3+32*u5^2*u4^2*u2^2+32*u5^2*u4*u3^3*u2^2-1
```

The CAD returns 1399 cells and outputs 394 real points on the hypersurface. Our method outputs 18 real points on the hypersurface. The degree of the univariate polynomial in the RUR is 236. Our computation time is :

```
FGb : 14 sec., RS : 90 sec.
```

Example 4

```
552*u2*u3^2*u4+62208*u2+1492992*u3+2799360*u4-3*u2^2*u4^2
-7842*u2*u3*u4+420*u2*u3*u4^2-314*u2^2*u3*u4+3*u2^2*u3^2*u4
-62208*u2^2+429*u4^3+20736*u3^2-4*u2^3*u3^2-1157*u2^2*u3^2
-18801*u2^2*u3-83520*u2*u3^2+39744*u2*u3+3*u2*u4^2+864*u2*u4
+17280*u3^2*u4+60912*u4^2-864*u2^2*u4-207*u2^3*u3
+1152*u3^2*u4^2+156*u4^3*u3+18540*u3*u4^2-554688*u3*u4
+8*u2*u3^2*u4^2+2*u2^3*u3*u4-2*u2*u3*u4^3+u4^4-8957952
```

The projection step of CAD does not end on this example. Our method outputs 10 real points on the hypersurface. The degree of the univariate polynomial in the RUR is 84. Our computation time is :

```
FGb : 1 sec., RS : 26 sec.
```

Example 5

Consider

```
P:=110*u5^2*u4*u3+190*u5*u4^2*u3+80*u4^3*u3+80*u5^2*u3^2+
270*u5*u4*u3^2+160*u4^2*u3^2+80*u5*u3^3+80*u4*u3^3-
32*u4*u3^2*u2-32*u3^3*u2-80*u5^2*u2^2-128*u5*u4*u2^2-
160*u5*u3*u2^2-112*u4*u3*u2^2-64*u3^2*u2^2-80*u5*u2^3-
32*u3*u2^3+60*u5^2*u4+220*u5*u4^2+160*u4^3+67*u5*u4*u3+
136*u4^2*u3-24*u5*u3^2-88*u4*u3^2-64*u3^3-100*u5^2*u2+
32*u5*u4*u2+96*u4^2*u2-228*u5*u3*u2-108*u4*u3*u2-
120*u3^2*u2+20*u5*u2^2+96*u4*u2^2-56*u3*u2^2+110*u5*u4+
80*u4^2+48*u4*u3-32*u3^2+30*u5*u2+48*u4*u2-20*u3*u2
```

The projection step of CAD does not end on this example. Our method outputs 26 real points on the hypersurface. The degree of the univariate polynomial in the RUR is 151. Our computation time is :

```
FGb : 47,2 sec., RS : 1800 sec.
```

In conclusion, it seems that our algorithm is able to solve some problems which are not reachable by the Cylindrical Algebraic Decomposition.

Note that in all these examples, only Algorithm 1 has been used (O is a good center and the set of singular points is not infinite).

7 Remarks on practical and theoretical complexity

The number of connected components of a real algebraic set defined by polynomials of degree d in k variables is $0(d)^k$, and this is bound is reached for some examples [5]. Using Bezout theorem, it is clear that the degrees of the polynomials we obtained in the RUR are $O(d)^k$. So in terms of the number of points output, our algorithm has a good behavior.

In terms of computation time, the theoretical complexity of our algorithm is worse than $d^{O(k)}$ reached in [6, 21, 2]. The reason for that is the need to find a good center and Gröbner basis computations. As presented above, the computation time of our algorithm could even be doubly exponential, because of the Gröbner basis computations. The algorithm can be easily modified (truncating polynomials to avoid double exponential degrees in Gröbner basis computations) to get an algorithm with complexity $d^{k^{O(1)}}$.

Note that algorithms in [6, 21, 2] were either not implemented or not efficient in practice. The tricks used in these papers to get a good theoretical complexity are in conflict with efficient computations. Adding a fixed number of infinitesimals does not modify the theoretical complexity but spoils the practical computations.

Developing efficient algorithms in practice and designing algorithms with good theoretical complexity are two complementary aspects of research in computer algebra.

We are convinced that in computational real algebraic geometry and in many other parts of computer algebra, algorithms with good theoretical complexity can and will inspire practical algorithms.

References

[1] M. E. Alonso, E. Becker, M.-F. Roy. T. Wormann, *Zeroes, Multiplicities and Idempotents for Zero Dimensional Systems,* in Algorithms in Algebraic Geometry and Applications, Laureano Gonzalez Vega and Tomas Recio Eds., 6-16, Birkhauser (1996).

[2] S. Basu, R. Pollack, M.-F. Roy, *A New Algorithm to Find a Point in Every Cell Defined by a Family of Polynomials,* in Quantifier Elimi-

nation and Cylindrical Algebraic Decomposition, Texts and Monographs in Symbolic Computation, B. Caviness and J. Johnson, Eds. 341-349, Springer-Verlag, Wien, New York (1998).

[3] S. Basu, R. Pollack, M.-F. Roy, *On the combinatorial and algebraic complexity of Quantifier elimination*. J. Assoc. Comput. Machin., 43, 1002–1045, (1996).

[4] E. Becker, V. Powers, *Deciding positivity of real polynomials.* Proceeding of the RAGOS conference, to appear in Contemp, Math.

[5] J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry,* Springer-Verlag (1999).

[6] J. Canny , *Some Algebraic and Geometric Computations in PSPACE,* Proc. Twentieth ACM Symp. on Theory of Computing, 460-467, (1988).

[7] J. Canny , *A toolkit for nonlinear algebra,* Goldberg, Ken (ed.) et al., Algorithmic foundations of robotics, Proceedings of the workshop on the algorithmic foundations of robotics, WAFR '94, held in San Francisco, CA, USA, 17-19 February, 1994. Wellesley, MA: A. K. Peters.

[8] G. E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition,* Springer Lecture Notes in Computer Science 33, 515- 532, (1975).

[9] P. Conti, C. Traverso, *Algorithms for the real radical,* unpublished manuscript

[10] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms,* Springer-Verlag (1991)

[11] J.C. Faugère *http://www-calfor.lip6.fr/ jcf*

[12] J.C. Faugère *A new efficient Algorithm for computing Gröbner bases*, To appear in Journal of Pure and Applied Algebra.

[13] P.Gianni, *Properties of Gröbner basis under specializations,* Lecture Notes in Computer Science, Vol. 378, 293-297 (1987)

[14] L. Gonzalez-Vega, F. Rouillier, M.-F. Roy, G. Trujillo, *Symbolic Recipes for Real Solutions,* In: Sometapas of computer algebra, A. Cohen ed. Springer, 121-167, (1999).

[15] D. Grigor'ev, N. Vorobjov , *Solving Systems of Polynomial Inequalities in Subexponential Time,* J. Symbolic Comput., 5:37–64, (1988).

[16] J. Heintz, M.-F. Roy, P. Solernó , *On the Complexity of Semi-Algebraic Sets,* Proc. IFIP 89, San Francisco. North-Holland 293-298 (1989).

[17] J. Heintz, M.-F. Roy, P. Solerno, *On the theoretical and practical complexity of the existential theory of the reals,* Comput. J. 36, No.5, 427–431 (1993).

[18] Z. Ligatsikas, R. Rioboo and M.F. Roy, (1993). *Generic Computation of the Real Closure of an Ordered Field*. Proceedings of IMACS 93 (Lille, may 1993), 203–208.

[19] S. Mc Callum, *An improved projection operator for Cylindrical Algebraic Decomposition*, Doctoral Thesis, University of Wisconsin- Madison, 1984.

[20] D. Mumford *Algebraic Geometry I, Complex projective varieties*, Berlin, Heildelberg, New York : Springer Verlag (1976).

[21] J. Renegar *On the computational complexity and geometry of the first order theory of the reals,* J. of Symbolic Comput.13(3):255-352, (1992).

[22] R. Rioboo, *Quelques aspects du calcul exact avec les nombres réels*, Doctoral Thesis, University of Paris 6, 1992.

[23] R. Rioboo, (1992). *Algebraic Closure of an Ordered Field, Implementation in Axiom*. Proc. of Issac'92 (Berkeley, july 1992).

[24] F. Rouillier, *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux,* Doctoral Thesis, University of Rennes I (1996).

[25] F. Rouillier, *Solving Zero-Dimensional Systems through the Rational Univariate Representation,* AAECC Journal.9 : 433-461 (1999).

[26] F. Rouillier, M.-F. Roy, M. Safey El Din, *Testing emptiness of real hypersurfaces, real algebraic sets and semi-algebraic sets* FRISCO Report Month 23 (1998).

[27] F. Rouillier, P. Zimmermann, *Uspensky's algorithm : improvements and applications,* in preparation (1999).

[28] M.-F. Roy, *Basic algorithms in real algebraic geometry: from Sturm theorem to the existential theory of reals,* Lectures on Real Geometry in memoriam of Mario Raimondo, Expositions in Mathematics 23, 1- 67. Berlin, New York: de Gruyter (1996).

[29] A. Seidenberg, *A new decision method for elementary algebra,* Annals of Mathematics, 60:365–374, (1954).

[30] A. Tarski, *A Decision method for elementary algebra and geometry,* University of California Press (1951).

[31] R. J. Walker *Algebraic Curves*, Princeton University Press (1950).

[32] V. Weispfenning, *Solving parametric polynomial equations and inequalities by symbolic algorithms,* Computer Algebra in Science and Engineering, 163–179, World Scientific (1995).

[33] V. Weispfenning *Quantifier elimination for real algebra – the quadratic case and beyond,* J. of AAECC, 8, 85-101 (1997).

[34] V. Weispfenning, *A new approach to quantifier elimination for real algebra,* 376-392 In Quantifier Elimination and Cylindrical Algebraic Decomposition. Texts and Monographs in Symbolic Computation (Springer-Verlag) (1998).