Symbolic Methods for Solving Algebraic Systems of Equations and Applications for Testing the Structural Stability

Yacine Bouzidi, Fabrice Rouillier

Symbolic methods for solving algebraic systems of equations and applications for testing the structural stability

Yacine Bouzidi and Fabrice Rouillier

Abstract In this work, we provide an overview of the classical symbolic techniques for solving algebraic systems of equations and show the interest of such techniques in the study of some problems in dynamical system theory, namely testing the structural stability of multidimensional systems.

1 Introduction

In this work, we address the problem of solving algebraic system of equations of the form:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases} \tag{1}$$

where $f_1, f_2, \ldots, f_s$ are polynomials in the variables $x_1, \ldots, x_n$ with coefficients in the field of rational numbers $\mathbb{Q}$.

Before going further, a first and important question that shall be asked is: *what does solving algebraic systems means?* Actually, answering to this question clearly

Yacine Bouzidi
Inria, Lille-Nord Europe & Institut de Mathématiques de Jussieu - Paris Rive Gauche & Sorbonne Université & Université de Paris e-mail: Yacine.bouzidi@inria.fr

Fabrice Rouillier
Inria de Paris & Institut de Mathématiques de Jussieu - Paris Rive Gauche & Sorbonne Université & Université de Paris e-mail: Fabrice.rouillier@inria.fr

and in all generality is not an easy task. The answer depends often on various parame ters among which the nature of the solutions, the context of the computations as well as the field of applications for which the computations are perfomed.

In the case of univariate polynomial equations, i.e. equations of the form $f(x) = 0$ where f is a polynomial with arbitrary coefficients, since the work of Abel in the 19th century, it is known that there is no general algebraic formulas for the solutions (solutions in radicals) when the degree of f is higher than four. An usual way to obtain a representation of the solutions is then via numerical approximations. Several methods exist for getting such approximations. One can mention for example the classical Newton-Raphson method for approximating a root (see [1] and references therein), or the bissection methods based on inclusion/exclusion criterias (Sturm's theorem, Descartes' rule of sign...) for approximating all the roots (see [2] and references therein). In addition, in many applications, one would like to perform exact computations with the resulting roots, e.g., checking the vanishing of an algebraic expression, computing it sign, etc. A suitable representation that allows such kind of computations consists in a polynomial that vanishes on the root and an isolating interval that contains this root and no other roots of the polynomial. Such an interval can then be refined to obtain an approximation of the root up to an arbitrary precision.

When it comes to systems of polynomial equations in several variables, an important aspect that governs the study of the solutions concernes their nature. More precisely, two type of systems can be distinguished. Those which admit a finite number of solutions in the algebraic closure of $\mathbb{R}$, i.e. $\mathbb{C}$, and those admitting an infinite number of solutions in $\mathbb{C}$.

For systems that admit a finite number of solutions, similarly as for univariate polynomial equations, one generally aims at finding numerical approximations of all the solutions which now are given as vectors of intervals. Two family of methods emerge, those which start from the initial polynomial system and compute numerical approximations of the solutions using for example multivariate variants of Newton-Raphson methods, interval evaluation, inclusion/exclusion criteria, homotopy continuation, etc (see [3,4] and references therein), and those which first focus on the computation of a formal expression of the solutions such as a univariate parametrization, a Gröbner basis or triangular sets and then compute numerical approximations of the solutions from these expressions. Such formal expressions ease in general the computation of numerical approximation of the solutions by reducing the problem to that of computing approximations of the roots of a univariate polynomial. It is worth mentioning that while the former methods (purely numerical methods) search for the solutions locally (in a given region of the solutions' space) and require regularity assumption on the input system in order to return an exact result (e.g., the system need to be squarefree, i.e., devoid from multiple solution), the methods based on the computation of formal expressions of the solutions provide a description for all the solutions of the system and do not made any assumption on the input.

Finally, for systems with an infinite number of solutions, the question of solving becomes rather vague and the specification of the output difficult to establish. In many applications, a frequently asked question concerns the existence of real solutions of a given system. More generally, a central problem for systems with infinite number of solutions is the computation of one real point in each connected component.

In this chapter we review some classical techniques for solving systems of polynomial equations focusing our attention on the exact symbolic methods, that is, methods providing an exact and complete description of the solutions. In addition, in order to motivate the use of such methods in the context of dynamical systems theory, we present an application of the latter to the problem of testing the stability of multidimensional systems (e.g. [5]) which we give the general statement below.

Structural stability of multidimensional systems. Let consider a single-input single-output (SISO) multidimensional discret linear system, described withing the frequency domain by a transfert function

$$G(z_1, \ldots, z_n) = \frac{N(z_1, \ldots, z_n)}{D(z_1, \ldots, z_n)}, \tag{2}$$

where N and D are polynomials in the complex variables $z_1, \ldots, z_n$ with rational coefficients with $\gcd(N, D) = 1$. This system is said to be *structurally stable* if the denominator of its transfert function is devoid from zeros in the complex unit polydisc $\mathbb{D}^n := \prod_{k=1}^{n} \{z_k \in \mathbb{C} || z_k| \leq 1\}$, or in other words:

$$D(z_1, \ldots, z_n) \neq 0 \text{ for } |z_1| \leq 1, \ldots, |z_n| \leq 1. \tag{3}$$

In order to check the above condition, a first step consists in rewitting it under algebraic form (conditions that involve only algebraic systems of equations). The resulting conditions are then processed by means of solving systems algorithms. As we will see further in the text, depending on the dimension of the multidimensional system, the resulting algebraic systems admits, either a finite number of zeros (for one or two dimensional systems) or an infinite number of zeros (for n-dimensional systems with $n \geq 3$). In each case, dedicated solving algorithms are used for testing the resulting conditions.

The chapter is organized as follow. We first recall in Section 2 the basic mathematical material behind the problem of solving symbolically systems of polynomial equations. In Section 3, we present some basic results about the roots of univariate polynomials. In Section 4 we provide a short introduction to Gröbner basis, a key tool in the study of systems of polynomial equations. Section 5 is devoted to the problem of solving systems with finitely many solutions called *zero-dimensional* systems. Finally, we address in Section 6 the problem of solving algebraic systems with an infinite number of solutions. At the end of each Section, we illustrate the use of the presented techniques on the problem of testing the structural stability of multidimensional systems.

2 Preliminaries

In the sequel, we will borrow some elements from algebraic geometry and comutative algebra to address problem (1). This problem consists in studying the zero-sets of polynomial systems. Geometrically, such sets correspond to algebraic varieties such as curves, surfaces or object of higher dimension. The good algebraic framework to study these kind of object is the theory of polynomial ideals. After defining the concepts of ideal and variety, we recall a classical result about the the correspondence between them which is at the core of the solving systems theory. This correspondence allows one to translate any question about the zeros of a system into a question about ideals, so that it can be answered using symbolic algorithms.

Given a set of polynomials $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$, one can construct other polynomials as linear polynomial combinations of the latter. This leads to the following definition.

Definition 1. (**Ideal**) The set of polynomials of the form

$$\sum_{i=1}^{s} g_i\, f_i, \text{ with } g_i \in \mathbb{K}[x_1, \ldots, x_n]$$

is called the ideal generated by $f_1, \ldots, f_s$ and denoted $\langle f_1, \ldots, f_s \rangle$

The ideal $\langle f_1, \ldots, f_s \rangle$ contains $f_1, \ldots, f_s$ and is a stable subset under addition and multiplication by elements in $\mathbb{K}[x_1, \ldots, x_n]$. Actually, it is the smallest subset of $\mathbb{K}[x_1, \ldots, x_n]$ that satisfies this property. Another important property is that every ideal in $\mathbb{K}[x_1, \ldots, x_n]$ is generated by a finite number of polynomials. This property stems from the fact that $\mathbb{K}[x_1, \ldots, x_n]$ is *noetherian*. Another important consequence of the *noetherianity* of $\mathbb{K}[x_1, \ldots, x_n]$ is that every ascending chain of ideals $I_1 \subsetneq I_2 \subsetneq \cdots I_k \subsetneq \cdots$ in $\mathbb{K}[x_1, \ldots, x_n]$ stabilizes. From the computation point of view, this last property is crucial since it garantees the termination of algorithms involving polynomial ideals in $\mathbb{K}[x_1, \ldots, x_n]$.

The geometrical objects we are going to study are defined as the zero-sets of systems of polynomial equations called algebraic varieties. We further introduce in Section 6.1, the notion of semi-algebraic set that consists in the points of an algebraic variety which satisfy certain inequalities.

Definition 2. (**Algebraic variety**) Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Then, the set

$$\mathcal{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for all } i \in \{1, \ldots, s\}\}$$

is called the affine variety defined by $f_1, \ldots, f_s$

Hence, the affine variety defined by a set of polynomials $f_1, \ldots, f_s$ is the subset of the affine space $\mathbb{K}^n$ that forms the zeros of the polynomial system $\{f_1 = \cdots = f_s = 0\}$. This variety is also defined as the zero set of the the ideal $\langle f_1, \ldots, f_s \rangle$. In the sequel, we often consider $\mathbb{K} = \mathbb{Q}$ and study two kind of varieties: the complex variety $\mathcal{V}_{\mathbb{C}}$, i.e., the set of complex zeros of a given ideal, and the real variety $\mathcal{V}_{\mathbb{R}}$, i.e., the set of its real zeros.

Exemple. Consider the polynomial $f(x,y) = x^4 - x^2 + y^2 \in \mathbb{Q}[x,y]$. The variety $\mathcal{V}_{\mathbb{R}}(f)$ corresponds to the points of $\mathbb{R}^2$ that satisfy the equation $f(x,y) = 0$ (see Figure 1).

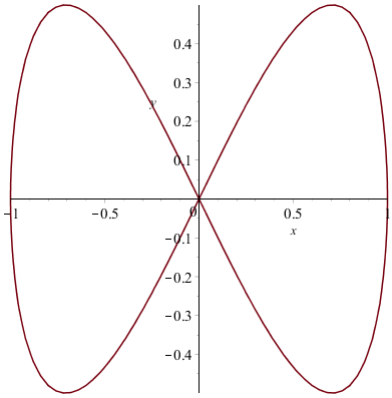

Fig. 1: The real variety associated to $x^4 - x^2 + y^2$

There exists an important correspondence between the algebraic concept of ideal and the geometric concept of variety. To understand this correspondence let start with the following definition.

Definition 3. Let V be an affine variety of $\mathbb{K}^n$. Define the set :

$$\mathcal{I}(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) : (a_1, \ldots, a_n) \in V\}.$$

The set $\mathcal{I}(V)$ is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. It is called the ideal of V.

Given an algebraic variety V, we can easily notice that the variety corresponding to the ideal of V is V itself, i.e., $\mathcal{V}(\mathcal{I}(V)) = V$. However, the reciprocal, i.e., $\mathcal{I}(\mathcal{V}(I)) = I$ is not always true as illustrated by the following example.

Example. Let consider the ideal $\langle (x-y)^2 \rangle \subset \mathbb{C}[x,y]$. $\mathcal{V}_{\mathbb{C}}(I)$ is the complex line given by the equation $x = y$ whose the corresponding ideal is $\langle x - y \rangle$, i.e., $\mathcal{I}(\mathcal{V}_{\mathbb{C}}(\langle (x-y)^2 \rangle)) \neq \langle (x-y)^2 \rangle$

In fact, the previous example shows that the correspondence between ideals and varieties is in general not one-to-one, different ideals can lead to the same variety. However, when $\mathbb{K}$ is an algebraically closed field, a fundamental result establishes a bijection between the set of varieties and the set of the so-called *radical* ideals.

Theorem 1. *[6, §4.1] If $\mathbb{K}$ is algebraically closed, then for any $I \subset \mathbb{K}[x_1, \ldots, x_n]$*

$$\mathcal{I}(V(I)) = \sqrt{I},$$

where $\sqrt{I} = \{g \in \mathbb{K}[x_1 \ldots, x_n] \mid \exists\, e \in \mathbb{N}, g^e \in I\}$ *is called the radical of* I.

The previous theorem, known as the *Hilbert Nullstelensatz theorem*, is the analogous of the fundamental theorem of algebra that relates a univariate polynomial to the set of its roots. It is at the core of the theory of solving algebraic systems of polynomials with coefficients in an algebraically closed field. In particular, it allows to translate any question about the solutions of an algebraic system of equations to a question about the radical ideal generated by this system.

Finally, when manipulating systems of algebraic equations, we are often interested in describing the nature of the corresponding zero-sets (algebraic varieties). For instance, the latter can consist in a finite number of points (e.g. the roots of a univariate polyomial), or an infinite number of points (e.g. the circle defined by the ideal $\langle x^2 + y^2 - 1\rangle$)). Intuitively, a convinient way to describe the nature of an algebraic variety is to consider the *degree of freedom* of an arbitrary point moving on it. In the case of a finite number of points, there is no way to move from a point to another point while remaining on the variety, the degree of freedom is thus zero. In the case of the variety defined by $\langle x^2 + y^2 - 1\rangle$, one can only move along the circle $x^2 + y^2 - 1 = 0$, the degree of freedom is equal to one. This notion of *degree of freedom* bears the name of *dimension* of an algebraic variety. It may be defined in various equivalent ways. The following definition gives an intuitive description of it. For more details on the dimension of an algebraic variety and how the latter can be computed, the reader may refer to [6, §9].

Definition 4. (*Dimension*) Let $V \subset \mathbb{K}^n$ be an affine variety. The dimension of V is the largest positive integer d such that there exists an affine variety $W \subset \mathbb{K}^d$ so that the projection

$$\begin{aligned} \mathbb{C}^n &\to \mathbb{C}^d \\ (x_1, \ldots, x_n) &\mapsto (x_{i_1}, \ldots, x_{i_d}), \end{aligned}$$

where $\{i_1, \ldots, i_d\}$ is a subset of $\{1, \ldots, n\}$, is surjective onto $\mathbb{C}^d/W$.

3 The univariate case

In this section, we start by recalling some classical tools and algorithms for the study of the roots of univariate polynomials. Beside the fact that such a material is a basic building block in solving systems problems, which are generally reduced to univariate ones (see Section 5.2), some of the presented results play also an important role in many algorithms that compute with multivariate polynomials considered as univariate polynomials with coefficients in polynomial rings (see Section 6.1).

3.1 GCD, Resultant, subresultants

Definition 5. (**Generalized remainder sequence**) Let $\mathbb{D}$ be a domain, $\mathbb{F}$ its fraction field and $f, g \in \mathbb{D}[x]$ with degree$(f) >$ degree(g). Consider the sequence $(\rho_i, r_i, q_i, s_i, t_i)_{i=0\ldots l}$ with $\rho_i \in \mathbb{F}^\star$, $r_i, q_i, s_i, t_i \in \mathbb{F}[x]$ such that:

- $\rho_0 r_0 = f \; s_0 = \rho_0^{-1} \; t_0 = 0$ and $\rho_1 r_1 = g \; s_1 = 0 \; t_1 = \rho_1$
- for $i \geqslant 1$, $r_{i-1} = q_i r_i + \rho_{i+1} r_{i+1}$, degree$(r_{i+1}) <$ degree(r_i)
- $l \in \mathbb{N}, r_l \neq 0 \wedge r_{l+1} = 0$
- $s_{i+1} := (s_{i-1} - q_i s_i)/\rho_{i+1}$, $t_{i+1} := (t_{i-1} - q_i t_i)/\rho_{i+1}$

It is important to point out that l, as well as the degree sequence does not depend on the choice of the ρ_i. In addition, we have :

- When $\rho_0 = \ldots = \rho_l = 1$, $(r_i)_{i=0\ldots l}$ is the **classical remainder sequence**.
- When $\rho_0 = 1, \rho_1 = 1, \rho_i = (-1)^{i+1}$, $(r_i)_{i=0\ldots l}$ is the so called **signed Euclidean remainder sequence** which corresponds, for $g = f'$ to the famous **Sturm sequence** (see Proposition 5).
- When the ρ_i's are recursively set as $\rho_i = \text{lc}(q_i r_i - r_{i-1})$, where lc$(.)$ denotes the leading coefficient, the $(r_i)_{i=0\ldots l}$ is the so called **monic remainder sequence**.

In all these cases, r_l is a GCD of f, g and $\forall i = 0 \ldots l$, $r_i = s_i f + t_i g$.

An important remark is that when f, g are in $\mathbb{D}[x]$, the polynomials r_i appearing in the above remainder sequences belong to $\mathbb{F}[x]$. In particular, if $\mathbb{D} = \mathbb{K}[y_1, \ldots, y_n]$ (i.e., the coefficients of f and g are polynomials in $y_1, \ldots, y_n$), then the sequence of r_i will have coefficients in $\mathbb{K}(y_1, \ldots, y_n)$ (i.e., rational fraction in $y_1, \ldots, y_n$). This fact prevents the remainders r_i from being specialized at any values of $y_1, \ldots, y_n$. More precisely, there exist $\alpha_1, \ldots, \alpha_n$ such that the i-th remainder of $f(\alpha_1, \ldots, \alpha_n, x)$ and $g(\alpha_1, \ldots, \alpha_n, x)$ is not equal to the specialization of the i-th remainder of $f(y_1, \ldots, y_n, x)$ and $g(y_1, \ldots, y_n, x)$. Such "bad" specializations correspond to the values of $y_1, \ldots, y_n$ that cancel the denominators of some coefficients appearing in the computation of r_i.

One way to overcome this specialization issue is to keep computations in the polynomial ring of coefficients. This can be done using the notion of subresultant sequence, which we define now.

Let $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$ with the convention that $f_i = g_i = 0$ if $i \leqslant 0$ and denote by $(r_i)_{i=0\ldots l}$ the monic remainder sequence of f and g as defined above. We introduce the following $(n + m - 2\,k)(n + m - k)$ matrix formed by the coefficients of f and g.

$$S_k = \begin{pmatrix} a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & & \\ & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & \\ & & \ddots & & & & & \ddots \\ & & & a_n & a_{n-1} & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & \cdots & b_0 & & \\ & b_m & b_{m-1} & \cdots & \cdots & \cdots & b_0 & \\ & & \ddots & & & & & \ddots \\ & & & b_m & b_{m-1} & \cdots & \cdots & b_0 \end{pmatrix},$$

and we set $\sigma_k = \det(S_k)$. Note that S_0 is the well known *Sylvester matrix*.

For each $i = 0 \dots l$, we denote by r_i the i-th monic remainder of f and g of degree d_i and we denote by $s_i, t_i \in \mathbb{D}[x]$ of degree respectively strictly less than $m - d_i - 1$ and $n - d_i - 1$, the unique solution of the system of linear equations

$$S_{d_i}^T (s_i, t_i)^T = (0, \dots, 0, 1)^T,$$

and thus, it turns out that $\sigma_{d_i} r_i = \sigma_{d_i} s_i f + \sigma_{d_i} t_i g$ when $r_i \neq 0$ is a non-zero remainder in the monic remainder sequence and $\sigma_{d_i} = 0$ otherwise.

Definition 6. (**Subresultants**) Let $f, g \in \mathbb{D}[x]$ with degree$(f) = n \geq m =$ degree(g).

- The sequence $(\sigma_i)_{i=0\dots m}$ is called the principal subresultant sequence associated to the couple (f, g).
- The sequence $(\text{Sres}_i(f, g) = \sigma_i r_{d_i})_{i=0\dots m}$ is called the polynomial subresultant sequence associated to (f, g). Sres_i is the polynomial subresultant of degree i.
- The polynomial subresultant of degree 0, Sres_0 is called the resultant of f and g, it belongs to the ideal generated by f and g.

The subresultant sequence has properties that are comparable to those of the classical remainder sequences.

Proposition 1. *Let $f, g \in \mathbb{D}[x]$, $f = a_0 + \dots + a_n x^n, g = b_0 + \dots + b_m x^m$ and denote by $\mathbb{F}$ the fraction field of $\mathbb{D}$. The following properties are equivalent:*

- *f, g have a commun root in $\overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$, or $a_n = b_m = 0$*
- *f, g have a non constant commun factor in $\mathbb{F}[x]$, or $a_m = b_n = 0$. If f, g have a non constant commun factor, then their* gcd *is proportional to the non-zero polynomial subresultant of minimal index.*
- *$\exists s, t \in \mathbb{F}[x]$ with degree$(s) < m$ and degree$(t) < n$ such that $sf + tg = 0$*
- *$\sigma_0 =$ Resultant$(f, g, x) = 0$*

In addition, as mentionned above, the subresultant sequence is well specialized.

Proposition 2. *Let $\mathbb{D}$ and $\mathbb{D}'$ be unique factorization domains and $\phi : \mathbb{D} \to \mathbb{D}'$ be a morphism. Let $f, g \in \mathbb{D}[x]$ and suppose that deg$(\phi(f)) =$ deg$(f) >$ deg$(g) =$ deg$(\phi(g))$. Then $\phi($Sres$_i(f, g)) =$ Sres$_i(\phi(f), \phi(g)), \forall i = 0 \dots$ deg(g).*

3.2 Real roots of univariate polynomials with real coefficients.

Let $P = \sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$ be a polynomial with real coefficients. We can easily bound the module of its (complex) roots as well as the distance between two roots.

Proposition 3. *[7, Prop. 10.9], [8, Thm. 1] If α is a complex root of P and if $a_n = 1$, then $|\alpha| < 1 + \max_{i=0}^{n}(|a_i|)$.*

If P has no multiple roots and if sep(P) denotes the distance between two roots of P, then sep$(P) \geq \sqrt{\frac{3}{n^n+2}} \cdot \frac{1}{||P||_2^{n-1}}$ with $||P||_2 = \sqrt{\sum_{i=0}^{d} a_i^2}$.

The above bounds give a straightforward exact algorithm to isolate the real roots of $P \in \mathbb{Q}[x]$.

Naive univariate isolation:

compute $\overline{P} := \frac{P}{\text{Gcd}(P, \partial P/\partial x)}$, the squarefree-part of P by Euclid's algorithm;
compute $M = 1 + \max_{i=0}^{n}(|\frac{a_i}{a_n}|)$;
compute any $m < \sqrt{\frac{3}{n^n+2}} \cdot \frac{1}{||P||_2^{n-1}}$;
compute the sign sequence sign $\left(\overline{P}\right)(-M + k\,m), 0 \leqslant i \leqslant \frac{2M}{m}$, and return the intervals in the form $(-M + k\,m, -M + (k+1)m)$ such that sign $\left(\overline{P}\right)(-M + k\,m)$sign $\left(\overline{P}\right)(-M + (k+1)m) < 0$ as well as the rational numbers $-M + k\,m$ such that sign $\left(\overline{P}\right)(-M + k\,m) = 0$.

However, such a simple algorithm would have an exponential behavior with respect to the degree n and the computation time would explode very quickly when increasing this degree. Alternatively, modern algorithms (and implementations) avoid the brutal partitioning of the interval $(-M, M)$ and use the so-called bissection strategies. The latter consist in iteratively subdividing the intial interval until getting isolating intervals around the roots. At each step, an interval of the form $I_{c,k} = \left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$ with $0 \leqslant c < 2^k$ is "visited", and some oracle is used to determine whether the polynomial has 0, 1 or more than one root in $I_{c,k}$ with respect to the following general principle:

General Bisection strategy:

List $= (0, 1)$;
while *List* $\neq \emptyset$ **do**
  Remove $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$ from List;
  If P has one root in $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$ add $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$ to the result;
  If P has more than one root in $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$, add $\left(\frac{2c}{2^{k+1}}, \frac{2c+1}{2^{k+1}}\right)$ and $\left(\frac{2c+1}{2^{k+1}}, \frac{2c+2}{2^{k+1}}\right)$ to List;
end

Hence, given an oracle for couting the number of real roots inside an interval (or at least deciding if there is 0, 1 or more than 1 real root), the above bissection strategy yields an algorithm for isolating the real roots of a univariate polynomial. A well known Oracle for that purpose is based on the so-called Sturm sequence.

Definition 7. Let $P \in \mathbb{R}[x]$. A Sturm sequence associated with P on a given interval $(a, b) \in \mathbb{R}$ is a sequence $f_0(x), \dots f_s(x) \in \mathbb{R}[x]$ such that :

- $f_0 = P$;
- f_s has no real root in (a, b);
- for $0 < i < s$, if $\alpha \in (a, b)$ is such that $f_i(\alpha) = 0$, then $f_{i-1}(\alpha) f_{i+1}(\alpha) < 0$;
- if $\alpha \in [a, b]$ is such that $f_0(\alpha) = 0$, then we have

$$\begin{cases} f_0 f_1(\alpha - \epsilon) < 0, \\ f_0 f_1(\alpha + \epsilon) > 0, \end{cases}$$

for any ϵ sufficiently small.

Proposition 4. *Let $P \in \mathbb{R}[x]$ and $f_0(x), \dots f_s(x)$ a Sturm sequence for P on (a, b). $V(a_1, \dots, a_s)$ denotes the number of sign changes in the sequence $a_1, \dots, a_s$ after removing zeros and $V_{stu}(P(c)) = V(f_0(c), \dots, f_s(c))$ then,*
$V_{stu}(P(b)) - V_{stu}(P(a))$ equals the number of real roots of P in (a, b).

A key point is that computing a Sturm sequence for a polynomial amounts essentially to computing a remainder sequence of this polynomial and its derivative.

Proposition 5. *[7, Thm. 2.50] Using Notation 5, the remainder sequence $(r_i)_{i=0\dots l}$ obtained when taking $\rho_0 = 1, \rho_1 = 1, \rho_i = (-1)^{i+1}, f = P, g = P'$ is a Sturm sequence for P on any interval (a, b).*

As for the classical remainder sequence, note that the Sturm sequence does not behave well under specialization, but, as for the classical remainder sequence, it suffices to multiply all the polynomials by the corresponding subresultants in order to solve the problem of specialization: if $(\mathrm{Stu}_i)_{i=0,\dots,l}$ is the Sturm sequence, then $(\sigma_{n_i}\mathrm{Stu}_i)_{i=0,\dots l}$ specializes well. Note that this new sequence, known as Sturm-Habicht sequence or signed subresultant sequence (see [7]), is not formally a Sturm sequence anymore but Proposition 4 can be adapted to get a well suited sign change counting for computing the roots of P in (a, b) using Sturm-Habicht sequences (see [7]).

The currently fastest implementations for the isolation of the real roots of univariate polynomials are not using Sturm (or Sturm-Habicht) sequences anymore but an Oracle based on Descartes' rule of signs:

Proposition 6. *[7, Thm. 2.33] Let $P = \sum_{i=0}^{n} a_n\, x^n \in \mathbb{R}[x]$ be a squarefree polynomial. The number of strictly positive real roots of P is dominated by $Var(P) = V(a_0, \dots, a_n)$ and equals $Var(P)$ modulo 2.*

In particular, if $\mathrm{Var}(P) = 0$, P has no positive roots, and if $\mathrm{Var}(P) = 1$, then P has exactly one positive root. This result can be adapted for inspecting the number of roots in an interval of the form $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$.

Corollary 1. *Let $P = \sum_{i=0}^{n} a_i\, x^i \in \mathbb{R}[x]$ be a squarefree polynomial and define the polynomials $P_{k,c} = 2^{kn} P\left(\frac{x+c}{2^k}\right)$, $R(P_{k,c}(x)) = x^n\, P_{k,c}(\frac{1}{x})$ and $T_1(R(P_{k,c})) = R(P_{k,c}(x+1))$. The number of strictly positive real roots of P in $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$ is dominated by $Var(T_1(R(P_{k,c})))$ and equals $Var(T_1(R(P_{k,c})))$ modulo 2.*

The formula in Corollary 1 is nowdays used in the general bissection algorithm in order to decide if a polynomial has $0, 1$ or more than one root in $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$. Unlike the Sturm-based strategy, Descartes rule of signs does not provide the exact number of roots but only a bound. However, the resulting algorithm still works since it has been shown (see [9]) that when the intervals $\left(\frac{c}{2^k}, \frac{c+1}{2^k}\right)$ are sufficiently small, then Descartes' rule of signs always return 0 or 1 and so allows to conclude.

4 Gröbner bases

Computing modulo ideals in the univariate ring $\mathbb{Q}[x]$ reduces to a simple Euclidean division. Indeed, given an ideal $I = (f_1, \ldots, f_n) \subset \mathbb{Q}[x]$ and a polynomial $p \in \mathbb{Q}[x]$, computing the reduction of p modulo I amounts to compute the remainder of the Euclidean division of p by the greatest common divisor of $\{f_1, \ldots, f_n\}$. When it comes to the multivariate polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$, computing the reduction of $p \in \mathbb{Q}[x_1, \ldots, x_n]$ modulo an ideal $I \subset \mathbb{Q}[x_1, \ldots, x_n]$ consists in obtaining a canonical representation of p in $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$. A Gröbner basis of an ideal I is a computable set of generators of I that allows to perform this operation.

In order to define Gröbner bases, a first step is to extend the usual Euclidean division, from polynomials in $\mathbb{Q}[x]$, to polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$. To do so, as for the Euclidean division in $\mathbb{Q}[x]$, one has to associate to each polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ a leading term with respect to which the reduction is made. This requires the introduction of the notion of *admissible ordering* on monomials in $\mathbb{Q}[x_1, \ldots, x_n]$. In the following, we denote by x^α the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ where $(\alpha = (\alpha_1, \ldots, \alpha_n))$.

Definition 8. An admissible monomial ordering in $\mathbb{Q}[x_1, \ldots, x_n]$ is a binary relation $<$ defined on the set of monomials x^α or equivalently on the set of $\alpha \in \mathbb{Z}^n_{\geq 0}$ such that

- $<$ is a total ordering relation.
- For any α, β and $\gamma \in \mathbb{Z}^n_{\geq 0}$, $\alpha < \beta \Longrightarrow \alpha + \gamma < \beta + \gamma$.
- For any $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, $\alpha < \alpha + \beta$.

These conditions imply Noetherianity, which means that every strictly decreasing sequence of monomials is finite.

In the following, we will mainly use the two following orderings and some others which we will define later.

- *Lexicographic order* (Lex):

$$\begin{aligned} & x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{\text{Lex}} x_1^{\beta_1} \cdots x_n^{\beta_n} \\ & \Leftrightarrow \exists i_0 \leq n, \quad \begin{cases} \alpha_i = \beta_i, & \text{for } i = 1, \ldots, i_0 - 1, \\ \alpha_{i_0} < \beta_{i_0}. \end{cases} \end{aligned} \tag{4}$$

- *Degree reverse lexicographic order (DRL)*:

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{\text{DRL}} x_1^{\beta_1} \cdots x_n^{\beta_n}$$

$$\Leftrightarrow \begin{cases} \sum_k^n \alpha_k < \sum_k^n \beta_k \\ \quad \text{or} \\ \sum_k^n \alpha_k = \sum_k^n \beta_k \text{ and } x_1^{-\alpha_n} \cdot \ldots \cdot x_n^{-\alpha_1} <_{\text{Lex}} x_1^{-\beta_n} \cdot \ldots \cdot x_n^{-\beta_1} \end{cases} \tag{5}$$

We also need the following notation.

Definition 9. Let $p = \sum_\alpha a_\alpha x^\alpha \in \mathbb{Q}[x_1, \ldots, x_n]$ and let $<$ be a monomial ordering. Then, we have:

- The multidegree of p is $\text{multideg}(p) = \max_<(\alpha \in \mathbb{Z}_{\geq 0}^n : a_\alpha \neq 0)$.
- The leading coefficient of p is $\text{LC}_<(p) = a_{\text{multideg}(p)} \in \mathbb{Q}$.
- The leading monomial of p is $\text{LM}_<(p) = x^{\text{multideg}(p)}$.
- The leading term of p is $\text{LT}_<(p) = \text{LC}(p)\,\text{LM}(p)$.

Given any admissible monomial ordering $<$, one can easily extend the classical Euclidean division to *reduce* a polynomial $p \in \mathbb{Q}[x_1, \ldots, x_n]$ by a set of polynomials F, performing the reduction with respect to each polynomial of F until getting an expression which cannot be further reduced (see [6] for details). This yields the following result.

Theorem 2. *Let $F = \{f_1, \ldots, f_n\}$ be a set of polynomials in $\mathbb{Q}[x_1 \ldots, x_n]$. For any $p \in \mathbb{Q}[x_1, \ldots, x_n]$, there exists $q_1, \ldots, q_n, r \in \mathbb{Q}[x_1, \ldots, x_n]$ such that*

$$p = q_1\, f_1 + \cdots + q_n\, f_n + r,$$

and none of the monomials of r is divisible by a leading term of $f_1, \ldots, f_n$.

The above reduction is denoted by $\texttt{Reduce}(p, F, <)$ (reduction of the polynomial p with respect to F). The polynomial r is the output of the function $\texttt{Reduce}(p, F, <)$ and is called the remainder of the reduction of p by F. Unlike the univariate case, this remainder polynomial now depends on the order in which the reductions by the polynomials of F are performed, and thus, the reduction is not canonical. In order to remedy this situation, the notion of *Gröbner basis* of an ideal has been introduced by Buchberger. Roughly speaking, a Gröbner basis G of an ideal I is a set of polynomials that generates the ideal and for which the function $\texttt{Reduce}(p, G, <)$ is canonical. In that case, the aforementioned remainder is refered to as the *normal form* of p with respect to G. The following definition of Gröbner basis is purely mathematical.

Definition 10. A set of polynomials G is a Gröbner basis of an ideal I with respect to a monomial ordering $<$ if for all $f \in I$ there exists $g \in G$ such that $\text{LM}_<(g)$ divides $\text{LM}_<(f)$.

Theorem 3. *[6, §2.6] Let I be an ideal in $\mathbb{Q}[x_1, \ldots, x_n]$ and G a Gröbner basis of I with respect to a fixed monomial ordering $<$. Then, for any $p \in \mathbb{Q}[x_1, \ldots, x_n]$, the reduction of f modulo G is uniquely determined. In particular, $p \in I$ iff this reduction is zero, i.e.,* $\texttt{Reduce}(p, F, <) = 0$.

Classical algorithms for computing Gröbner bases of ideals start from a set of generators and construct iteratively new sets of generators until obtaining a Gröbner basis. The most popular algorithm for computing Gröbner bases is Buchberger's algorithm [10]. It is implemented in most of computer algebra software such as `Maple` and `Mathematica`. This algorihtm has several variants and modern ones [11] make a large use of dedicated sparse linear algebra techniques and can be found in some general computer algebra systems such as `Magma` or `Maple` as well as in some dedicated systems like `FGb`.

4.1 Application of Gröbner basis

Gröbner bases are key objects for performing computations with polynomial ideals. As an illustration, we present in the following three important problems that can be solved through Gröbner bases computation.

The emptiness of the zero set: In several applications, a frequently asked question concerns the consistancy of an algebraic system of equations, that is, the existence of common zeros in the algebraic closure $\overline{\mathbb{K}}$ of the coefficients field $\mathbb{K}$. Given an ideal $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$, this problem translates into testing if the variety associated to the ideal I, that is, $\mathcal{V}(I) = \{\alpha \in \mathbb{C}^n \mid \forall f \in I,\ f(\alpha) = 0\}$ is empty. According to the *Nullstelensatz theorem*, $\mathcal{V}(I)$ is empty if and only if $1 \in I$. Given a Gröbner basis G of I, this condition is equivalent to the existence of an element of G that belongs to $\mathbb{Q}$.

The ideal membership problem: Given $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{Q}[x_0, \ldots, x_n]$ and a polynomial $p \in \mathbb{Q}[x_1, \ldots, x_n]$, an important question consists in testing whether the polynomial p belongs to the ideal I. In particular this implies that the polynomial vanishes at the zero-set corresponding to the ideal I. If G denotes the Gröbner basis associated to I, then according to Theorem 3, this can be done by computing the normal form of p modulo G and checking that the latter is zero.

An important question that stems from the membership problem is the representation of p. Indeed, if $p \in I$, then by definition, there exist polynomials $q_1, \ldots, q_s$ in $\mathbb{Q}[x_1, \ldots, x_n]$ such that $P = q_1\, f_1 + \ldots + q_s\, f_s$. An intersting problem is then to determine effectively the polynomials $q_1, \ldots, q_s$. One natural approach is to compute the reduction of p modulo the polynomials of the Gröbner basis $g_1, \ldots, g_l$, and then express each g_i as a polynomial combination of $f_1, \ldots, f_s$ using the calculations performed during the construction of the Gröbner basis. In such a computation, we are interested in polynomials $q_1, \ldots, q_s$ with the minimum degree. It was proved (see for instance [12]) that, in general, the degree of such $q_1, \ldots, q_s$ is bounded by

a value that is doubly exponential in the number of variables n, i.e. of the form d^{2^n} where d is the maximum degree of $p, f_1, \ldots, f_s$.

The elimination problem: If $I \subset \mathbb{Q}[x_1, \ldots, x_n]$ and i is an integer satisfying $1 \leq i \leq n$. The ideal $I_i = I \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$, consisting of the elements of I that do not depend on the variables $x_1, \ldots, x_i$, is called the *i-th elimination ideal* of I. These ideals play an important role in the computation with polynomial ideals and, in particular, for solving algebraic system of equations. Algorithmically, obtaining such ideals can be done by eliminating variables. A convinient way to do that is to compute Gröbner bases with respect to an approriate ordering called *elimination ordering.*

Definition 11. A monomial ordering $<$ in $\mathbb{Q}[x_1, \ldots, x_r, x_{r+1}, \ldots, x_n]$ is an elimination ordering with respect to the block $[x_1, \ldots, x_r]$ if for any polynomial $p \in \mathbb{Q}[x_1, \ldots, x_r, x_{r+1}, \ldots, x_n]$, we have

$$\mathrm{LT}_<(p) \in \mathbb{Q}[x_{r+1}, \ldots, x_n] \Rightarrow p \in \mathbb{Q}[x_{r+1}, \ldots, x_n]$$

Then, a fundamental result gives a description of elimination ideals using the Gröbner bases computed with respect to a given elimination ordering.

Theorem 4. *[6, §3.1] (**Elimination theorem**) Let I be an ideal of $\mathbb{Q}[x_1, \ldots, x_n]$ and $i \in \{1, \ldots, n\}$. If G is a Gröbner basis for an elimination ordering with respect to the block $[x_1, \ldots, x_{i-1}]$, then $G_i = G \cap \mathbb{Q}[x_i, \ldots, x_n]$ is a Gröbner basis of the elimination ideal $I_i = I \cap \mathbb{Q}[x_i, \ldots, x_n]$.*

A well known elimination ordering is the lexicographic ordering described above. The above theorem shows in particular that a Gröbner basis computed with respect to the lexicographic ordering eliminates not only the first variable but also the first two variables, the first three variables and so on. In the context of solving algebraic system of equations, this provides a way to obtain a triangular description of the solutions. In the case of system with finitely many solutions, such a method yields a generalization of the classical Gaussian elimination for solving algebraic systems of equations. Computing the solutions then consists in solving inductively the obtained equations. Starting from the isolation of the roots of the polynomial in the last variable, then the resulting intervals are substituted in the next polynomial, and the isolation is performed again and so on.

Two important operations that stem from the elimination orderings are the *projection* and the *localization*, which are summarized in Propositions 7 and 8. To facilitate their illustrations, the following notation is needed. Given any subset $\mathcal{V}$ of $\mathbb{C}^n$ (d is an arbitrary positive integer), we denote by $\overline{\mathcal{V}}$ its *Zariski closure*, that is, the smallest algebraic variety of $\mathbb{C}^n$ containing $\mathcal{V}$. If $\mathcal{V}$ is a *constructible set* (i.e., defined by equations and inequations), then $\overline{\mathcal{V}}$ is also the closure for the usual topology.

Proposition 7. *[6, §3.2] Let $I \subset \mathbb{Q}[x_1, \ldots, x_n]$ be an ideal and denote by $V(I) \subset \mathbb{C}^n$ the corresponding affine variety. Consider the following projection map*

$$\begin{array}{c} \Pi_i : \mathbb{C}^n \to \mathbb{C}^{n-i} \\ (\alpha_1, \ldots, \alpha_n) \in V(I) \mapsto (\alpha_{i+1}, \ldots, \alpha_n) \in \Pi_i(V_{\mathbb{C}}) \end{array}$$

Then, we have:

$$V(I_i) = \overline{\Pi_i(V)}$$

where I_i denotes the i-th elimination ideal of I.

Proposition 8. *[6, §3.2] Let $I \subset \mathbb{Q}[x_1, \ldots, x_n]$, $f \in \mathbb{Q}[x_1, \ldots, x_n]$, and t be a new indeterminate, then $\overline{V(I) \setminus V(f)} = V((I + \langle tf - 1 \rangle) \cap \mathbb{Q}[x_1, \ldots, x_n])$. Moreover, if $G' \subset \mathbb{Q}[t, x_1, \ldots, x_n]$ is a Gröbner basis of $I + \langle tf - 1 \rangle$ for an elimination ordering w.r.t to $[t]$, then $G' \cap \mathbb{Q}[x_1, \ldots, x_n]$ is a Gröbner basis of*

$$I : f^\infty := (I + \langle t\, f - 1 \rangle) \cap \mathbb{Q}[x_1, \ldots, x_n].$$

The variety $\overline{V(I) \setminus V(f)}$ and the ideal $I : f^\infty$ are usually called the localization of $V(I)$ and I by f.

5 Certified solutions of zero-dimensional systems

In this section, we study the case of zero-dimensional systems, that is, systems with finitely many solutions in the algebraic closure of the coefficient field. For such systems, we will see that the quotient algebra of the corresponding ideal is a finite dimensional vector space. This fundamental property allows one to translate most of the questions about zero-dimensional systems into linear algebra questions in the corresponding quotient algebra. These questions can then be answered using classical linear algebra algorithms. Hence, starting from a system of polynomial equations, we can obtain many information about its solutions, e.g., counting their number, computing their symbolic representation or determining their multiplicities.

5.1 The case of one variable

To give a first idea of the link between zero-dimensional systems and the corresponding quotient algebras, let us start by considering the simple case of univariate polynomials and let us recall a classical result about the computation of the roots of such polynomials.

Given a polynomial in $\mathbb{Q}[x]$, $P(x) = \sum_{i=0}^{D} a_i\, x^i$ with $a_D \neq 0$, the quotient algebra $\frac{\mathbb{Q}[x]}{\langle P \rangle}$ is a $\mathbb{Q}$-vector space of dimension D, in which one can define the endomorphism of the multiplication by x

$$\begin{array}{rccc} m_x : & \frac{\mathbb{Q}[x]}{\langle P \rangle} & \to & \frac{\mathbb{Q}[x]}{\langle P \rangle} \\ & u & \mapsto & \overline{x\, u}, \end{array}$$

which sends any u in $\frac{\mathbb{Q}[x]}{\langle P\rangle}$ to the remainder of the Euclidean division of $x\,u$ by P. We denote by $C(P)$ its matrix in the monomial basis $\{1, x, \ldots, x^{D-1}\}$, i.e.,:

$$C(f) = \begin{pmatrix} 0\,0\,0\ldots & -\frac{a_0}{a_D} \\ 1\,0\,0\ldots & -\frac{a_1}{a_D} \\ 0\,1\,0\ldots & -\frac{a_2}{a_D} \\ \vdots\,\vdots\,\vdots\,\ddots & \vdots \\ 0\,0\,0\ldots & -\frac{a_{D-1}}{a_D} \end{pmatrix}.$$

This matrix is known as the *Frobenius companion matrix* of P and its characteristic polynomial is the polynomial P itself.

Theorem 5. *The eigenvalues of $C(P)$ are exactly the roots of $P(x)$ with the same multiplicities.*

Consequently, one can compute the roots of a univariate polynomial $P(x)$ by simply computing the eigenvalues of its Frobenius companion matrix. This example exhibits the role of multiplication endomorphisms for the characterization of the roots of a univariate polynomial. In fact, this approach can be generalized for characterizing the solutions of a zero-dimensional system defined by an ideal I in $\mathbb{Q}[x_1, \ldots, x_n]$. As for the case of one univariate polynomial, the quotient algebra corresponding to I, i.e., $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ is a finite dimensional $\mathbb{Q}$-vector space, and a basis of it is given by the monomials that are irreducible modulo the ideal I [6]. The dimension of this vector space is the number of solutions of I counted with multiplicities, which we denote by D in the following.

The following result is a generalization of Theorem 5 for the case of ideals in $\mathbb{Q}[x_1, \ldots, x_n]$. The notation $\overline{P}$ denotes the normal form of P with respect to I.

Theorem 6. *[7] Let $h \in \mathbb{Q}[x_1, \ldots, x_n]$ and m_h be the multiplication endomorphism by h*

$$\begin{array}{rccc} m_h : & \frac{\mathbb{Q}[x_1,\ldots,x_n]}{I} & \to & \frac{\mathbb{Q}[x_1,\ldots,x_n]}{I} \\ & u & \mapsto & \overline{hu}. \end{array}$$

The eigenvalues of m_h are the $h(\alpha)$, where $\alpha \in V(I)$, with multiplicity $\mu(\alpha)$.

According to Theorem 6, providing a basis $\mathcal{B}$ of $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ and the matrices of the multiplication m_{x_i} by the variables $x_i, i = 1, \ldots, n$, one can compute all the coordinates of all the solutions $\alpha \in V(I)$. From the computation point of view, when $I \subset \mathbb{Q}[x_1, \ldots, x_n]$, one way to compute $\mathcal{B}$ as well as the matrices m_{x_i} is to use Gröbner bases.

Theorem 7. *[6] Let $I \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a zero-dimensional ideal and G a Gröbner basis of I with respect to any monomial ordering $<$. Then, we have:*

- *For all $i = 1, \ldots, n$, there exists a polynomial $g_j \in G$ and a positive integer n_j such that $x_i^{n_j} = LM_<(g_j)$.*

- $\mathcal{B} := \{t = x_1^{e_1} \cdots x_n^{e_n} | (e_1, \ldots, e_n) \in \mathbb{N}^n \text{ and } e_i \leq n_i\} = \{w_1, \ldots, w_D\}$ *is a basis of* $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ *as a* $\mathbb{Q}$*-vector space;*

Hence, given a Gröbner basis of a system, simply by looking at the leading terms of the basis, we are able to check if the system is zero-dimensional and, in the latter case, to deduce a basis of the corresponding quotient algebra. However, knowing all the coordinates of all the solutions of $V(I)$ is not sufficient since one needs to combine them suitably in order to get the actual solutions of $V(I)$, which is not an easy task. Alternatively, the usual approach, which we describe in the next section, is to compute a parametrization of the solutions.

Before going further, let mention the following important result which is a multivariate generalization of the Hermite's theorem for counting the number of distinct roots of univariate polynomials [7].

Theorem 8. *Let* $h \in \mathbb{Q}[x_1, \ldots, x_n]$ *and* Her_h *be the Hermite's quadratic form*

$$\begin{array}{rccc} Her_h : & \frac{\mathbb{Q}[x_1,\ldots,x_n]}{I} & \to & \mathbb{Q} \\ & f & \mapsto & Trace\left(m_{f^2 h}\right), \end{array}$$

Then, we have:

- $rank(Her_h) = \sharp\{x \in V(I) \mid h(x) \neq 0\}$.
- $signature(Her_h) = \sharp\{x \in V(I) \cap \mathbb{R}^n \mid h(x) > 0\} - \sharp\{x \in V(I) \cap \mathbb{R}^n | \, h(x) < 0\}$

where $\sharp$ *denotes the cardinality of a set.*

When $h = 1$, Theorem 8 yields an algorithm for counting the number of solutions in $V(I)$ as well as the number of solutions in $V(I) \cap \mathbb{R}^n$. This algorithm first constructs the matrix associated to Her_1 (the entries of this matrix are the $\text{Trace}(m_{w_i w_j})$ where w_k is an element of $\mathcal{B}$) and then compute its rank (resp. signature) to get the number of solutions in $V(I)$ (resp. the number of solutions in $V(I) \cap \mathbb{R}^n$).

5.2 Univariate representations of the solutions

Suppose that $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ is a $\mathbb{Q}$-vector space of dimension D and consider the vectors $1, \overline{x_1}, \ldots, \overline{x_1}^{D-1}$ in this vector space. If the latters are $\mathbb{Q}$-linearly independent, then they form a basis, and we can express $x_1^D, x_2, \ldots, x_n$ in $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ as a $\mathbb{Q}$-linear combination of them which yields the following parametrization:

$$\begin{cases} f(x_1) = 0, \\ x_2 = g_2(x_1), \\ \quad \vdots \\ x_n = g_n(x_1). \end{cases} \tag{6}$$

The polynomial $\{f, x_2 - g_2, \ldots, x_n - g_n\}$ forms a Gröbner basis of I for the lexicographic monomial ordering $<_{\text{lex}}$ with $x_1 <_{\text{lex}} \ldots <_{\text{lex}} x_n$ [6].

Up to an eventual permutation of the variable's index (considering the vectors $1, \overline{x_i}, \ldots, \overline{x_i}^{D-1}$), the case (8) is known as the *Shape position* case.

On the other hand, one can consider a polynomial $h \in \mathbb{Q}[x_1, \ldots, x_n]$, a new independent variable t, and define the ideal $I_h := I + \langle t - h \rangle \subset \mathbb{Q}[t, x_1, \ldots, x_n]$ so that $V(I_h) = \{(\alpha, h(\alpha)) \mid \alpha \in V(I)\}$ (one can easily remark that $V(I_h)$ and $V(I)$ are in one-to-one correspondence). If $1, \overline{h}, \ldots, \overline{h}^{D-1}$ are $\mathbb{Q}$-linearly independent in $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I_h}$, then, we can also express $x_1, \ldots, x_n$ in $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I_h}$ as a linear combination of $1, \overline{h}, \ldots, \overline{h}^{D-1}$, which yields the following parameterization:

$$\begin{cases} f(t) = 0, \\ x_1 = g_1(t), \\ \quad \vdots \\ x_n = g_n(t). \end{cases} \tag{7}$$

However, in some cases (see the above example), one cannot get parametrizations of the forms (8) or (9).

Example 1. Consider the ideal $I := \langle x_1^2, x_1\, x_2, x_2^2 \rangle$, which is already a Gröbner basis. According to Theorem 7, a basis of $\frac{\mathbb{Q}[x_1,x_2]}{I}$ is then $\mathcal{B}_{<_{\text{lex}}} := \{1, x_1, x_2\}$ and $D = \sharp\mathcal{B} = 3$ (the unique zero is $(0, 0)$ and has multiplicity 3).

As $x_1^2 \in I$ (resp. $x_2^2 \in I$), then $1, x_1, x_1^2$ (resp. $1, x_2, x_2^2$) are trivially $\mathbb{Q}$-linearly dependent in $\frac{\mathbb{Q}[x_1,x_2]}{I}$ and thus neither $1, x_1, \ldots, x_1^{D-1}$ nor $1, x_2, \ldots, x_2^{D-1}$ are linearly independent in $\frac{\mathbb{Q}[x_1,x_2]}{I}$. The ideal is not in *Shape position*. Let now take any $h \in \frac{\mathbb{Q}[x_1,x_2]}{I}$. The general expression of such an element is $h = ax_1 + bx_2 + c$, with $a, b, c \in \mathbb{Q}$, and it immediately turns out that $h^2 - 2ch - c^2 = 0$ in $\frac{\mathbb{Q}[x_1,x_2]}{I}$. Thus, for any $h \in \frac{\mathbb{C}[x_1,x_2]}{I}$, $1, h, \ldots, h^{D-1}$ are $\mathbb{Q}$-linearly dependent in $\frac{\mathbb{C}[x_1,x_2]}{I}$ which implies that the ideal I_h cannot be written under the form (9).

Mathematically, the two above situations ((8) and (9)) correspond to the case where the quotient algebra $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ is cyclic, that is, when it is generated by the successive powers of an element of $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$. Such an element is called a *primitive element* of $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$. When $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ is known to be cyclic, finding a primitive element is equivalent to finding what is called a *separating element* for the set of points defined by the variety $V(I)$.

Definition 12. Let h be a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$. Then, h is a separating element for $V(I)$ if and only if $x \in V(I) \mapsto h(x)$ is injective.

In adition a separating element can be found among a finite set of linear forms so as stated in the following theorem.

Theorem 9. *Suppose that $\sharp V(I) = d$. Then, the set*

$$\mathit{Sep}_d = \{x_1 + i\, x_2 + \cdots + i^{n-1} x_n, i = 0, \ldots, n\frac{d(d-1)}{2}\},$$

contains at least one separating element for $V(I)$.

The computation of such a primitive element can be done by computing for each $h \in \mathrm{Sep}_d$, the minimal integer d_h such that $1, \overline{h}, \ldots, \overline{h}^{d_h}$ are linearly dependent, and then selecting an h for which $d_h = D - 1$. The computation of the parametrization (9) then resumes to the computation of the coordinates of the vectors $x_1, x_2, \ldots, x_n$ in the basis $1, \overline{h}, \ldots, \overline{h^{D-1}}$. Note that another methods for obtaining such a parametrization is to compute a Gröbner basis of $I + \langle t - h\rangle$ with respect to the lexicographic monomial ordering $<_{\text{lex}}$ with $t < x_1 <_{\text{lex}} \ldots <_{\text{lex}} x_n$.

As mentionned before, the above strategy for computing a parametrization works only when a primitive element exists (i.e., $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ is cyclic). This is the case for example when the considered ideal is radical (all the solutions have multiplicity one).

When $\frac{\mathbb{Q}[x_1,\ldots,x_n]}{I}$ is not cyclic, one can still compute a parametrization of the solutions using the so-called *Rational Univariate Representation* (RUR) [13].

Definition 13. Given any $h \in \mathbb{Q}[x_1, \ldots, x_n]$, we define:

- $f_h(t) = \prod_{\alpha \in V(I)} (t - h(\alpha))^{\mu(\alpha)}$,
- $g_{h,1}(t) = \sum_{\alpha \in V(I)} \mu(\alpha)\ \prod_{\beta \in V(I), \beta \neq \alpha} (t - h(\beta))$,
- $g_{h,v}(t) = \sum_{\alpha \in V(I)} \mu(\alpha)\ v(\alpha)\ \prod_{\beta \in V(I), \beta \neq \alpha} (t - h(\beta))$ for $v \in \{x_1, \ldots, x_n\}$.

If h separates $V(I)$, then the univariate polynomials $\{f_h(t), g_{h,1}(t), \ldots, g_{h,x_n}(t)\}$ define the so called Rational Univariate Representation of I associated to h.

The Rational Univariate Representation of I bears important properties which we summarize below.

- $f_h(t), g_{h,1}(t), \ldots, g_{h,x_n}(t)$ are polynomials in $\mathbb{Q}[t]$.
- The application
$$\begin{array}{rcl} \phi_h : V(I) & \longrightarrow & V(f_h) \\ x & \longmapsto & h(x) \end{array}$$
defines a bijection between $V(I)$ and $V(f_h)$, whose reciprocal is given by:
$$\begin{array}{rcl} \phi_h^{-1} : V(f_h) & \longrightarrow & V(I) \\ x & \longmapsto & \left(\frac{g_{h,x_1}(x)}{g_{h,1}(x)}, \ldots, \frac{g_{h,x_n}(x)}{g_{h,1}(x)}\right). \end{array}$$
- ϕ_h preserves the multiplicities : $\mu(h(x)) = \mu(x)$.

The Rational Univariate Representation of an ideal I is a one-to-one mapping between the solutions of $V(I)$ and the roots of a univariate polynomial $f_h(t)$. This representation is uniquely defined up to a separating element. Moreover, unlike classical parametrizations, such a representation preserves the multiplicities of the solutions, in the sense that the multiplicity of a solution in I is the multiplicity of the

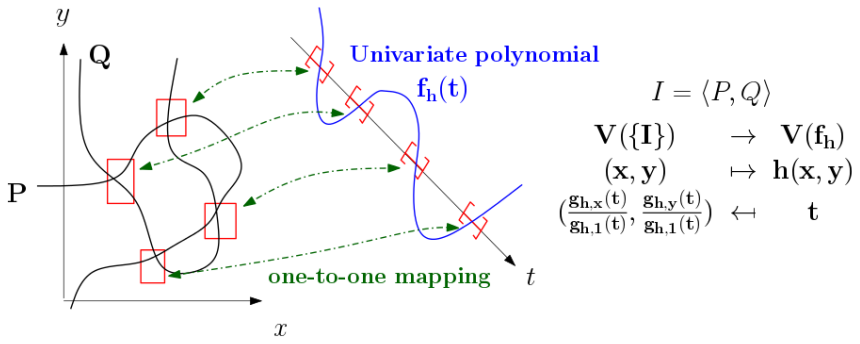

Fig. 2: A Rational Univariate Representation of a zero-dimensional bivariate system $I = \langle P, Q \rangle$

corresponding root in the polynomial $f_h(t)$. The latter property is critical in many problems where the information about the multiplicities is needed.

To compute a RUR, one has to solve the following two problems:

- Find a separating element h.
- Given any polynomial h, compute a RUR-Candidate $f_h, g_{h,1}, g_{h,x_1}, \ldots, g_{h,x_n}$ such that if h is a separating element, then the RUR-Candidate is a RUR.

According to [13], a RUR-Candidate can be explicitly computed when we know a suitable representation of $\mathbb{Q}[x_1, \ldots, x_n]/I$, which can be summarized as follows:

- $f_h = \sum_{i=0}^{D} a_i t^i$ is the characteristic polynomial of m_h. Let us denote by $\overline{f_h}$ its square-free part.
- For any $v \in \mathbb{Q}[X_1, \ldots, X_n]$, $g_{h,v} = g_{h,v}(t) = \sum_{i=0}^{d-1} \text{Trace}(m_{vh^i}) H_{d-i-1}(t)$, $d = \deg(\overline{f_h})$ and $H_j(T) = \sum_{i=0}^{j} a_i t^{i-j}$.

In [13], a strategy is proposed to compute a RUR for any system defined by a Gröbner basis for any ordering.

5.2.1 Application of the Rational Univariate Representation

From formal to numerical solutions. Computing a RUR reduces the resolution of a zero-dimensional system to solving a polynomial f_h with one variable and to evaluating n rational fractions $(\frac{g_{h,x_i}(t)}{g_{h,1}(t)}, i = 1 \ldots n)$ at the roots of f_h. The goal is thus to compute all the real roots of f_h providing a numerical approximation with an arbitrary precision of the coordinates.

The isolation of the real roots of f_h can be done using the algorithm proposed in [9]. The output will be a list l_{f_h} of intervals with rational bounds such that for each real root α of f_h, there exists a unique interval in l_{f_h} which contains α. The second step consists in refining each interval in order to ensure that it does not

contain any real root of $g_{h,1}$. Since f_h and $g_{h,1}$ are coprime, this computation is easy. Then, we can ensure that the rational functions can be evaluated by using interval arithmetics without any cancelation of the denominator. The last evaluation is performed by using multi-precision arithmetics (MPFI package - [14]). Moreover, the rational functions defined by the RUR are stable under numerical evaluation even if their coefficients are huge rational numbers. Thus, the isolation of the real roots does not involve huge compaction burden. To increase the precision of the result, it is only necessary to decrease the length of the intervals in l_{f_h} which can be easily done by bisection or using a certified Newton's algorithm. It is in particular quite simple to certify the sign of the coordinates.

Signs of polynomials at the roots of a system. Due to the presence of inequalities in semi-algebraic system, it is important to develop a method for computing the sign ($+, -, \neq$ or 0) of given multivariate polynomials at the real roots of a zero-dimensional system. Having a RUR $\{f_h, g_{h,1}, g_{h,x_1}, \ldots, g_{h,x_n}\}$ of I, one can translate the problem of computing the sign of a multivariate polynomial into a problem of computing the sign of a univariate polynomial. Indeed, let $P \in \mathbb{Q}[x_1, \ldots, x_n]$ be the polynomial to be evaluated at the real solution $\alpha = (\alpha_1, \ldots, \alpha_n) \in V(I)$ (α is the image of a root γ of $f_h(t)$ by the RUR mapping). One can define the polynomial $P_I(t)$ roughly as the numerator of the rational fraction $P\left(\frac{g_{h,x_1}}{g_{h,1}}, \ldots, \frac{g_{h,x_n}}{g_{h,1}}\right)$, that is the rational fraction obtained after substituting in P each variable x_i by $\frac{g_{h,x_i}}{g_{h,1}}$. Then the following result holds.

Theorem 10. *The sign of $P(x_1, \ldots, x_n)$ at the real solution $\alpha = (\alpha_1, \ldots, \alpha_n) \in V(I)$ is equal to the sign of $P_I(t)$ at the corresponding root γ of $f_h(t)$ via the RUR mapping.*

Accordingly, the problem of computing the sign of $P(x_1, \ldots, x_n)$ at a solution of $V(I)$ is reduced to the problem of computing the sign of $P_I(t)$ at a real root of $f_h(t)$. To solve the latter problem, a naive algorithm consists in isolating the real root of $f_h(t)$, so that the interval is also isolating for the product $P_I(t)\, f_h(t)$ and then evaluating the sign of $P_I(t)$ at the endpoints of this interval.

Consequently, in order to compute the sign of the polynomial $P(x_1, \ldots, x_n)$ at a solution of $V(I)$, it is sufficient to compute the sign of the polynomial $P_I(t)$ at a given root of $f_h(t)$.

Instead of straightforwardly *plugging* the formal coordinates provided by the RUR into P, we better extend the RUR by computing rational functions which coincide with the values of P at the roots of I. This can be done by using the general formula $g_{h,P} = \sum_{i=0}^{D-1} \text{Trace}(m_{P\,h^i}) H_{D-i-1}(t)$ given in [13]. One can directly compute the $\text{Trace}(Pt^i)$ by reusing the computations already done if the RUR has already been computed. Hence, it is not more costly to compute the extended RUR than the classical one.

5.3 Testing the structural stability: the zero-dimensional case

In the following, we are going to show how Rational Univariate Representations can be used in order to solve the stability test problem mentioned in the introduction. For one or two dimensional systems, the test of the structural stability can be reduced to the study of algebraic zero-dimensional systems. Indeed, in the case of one dimensional system the stability condition translates into

$$D(z) \neq 0 \text{ for } |z| \leq 1,$$

or equivalently, the subset of $\mathbb{C}$ defined by $E := \{z \in \mathbb{C} \mid D(z) = 0, |z| \leq 1\}$ is empty. The set E can be viewed as a semi-algebraic set of $\mathbb{R}^2$. Indeed, if we note $z = x + i\,y$, where x (resp., y) is the real part (resp., the imaginary part) of z and i the imaginary unit, then the polynomial $D(z)$ can be rewritten as $D(x, y) = \mathcal{R}(x, y) + i\,\mathcal{I}(x, y)$, where $\mathcal{R}, \mathcal{I} \in \mathbb{Q}[x, y]$, and the inequality $|z| \leq 1$ as $x^2+y^2 \leq 1$, which shows that:

$$\mathrm{E} \approx \{(x, y) \in \mathbb{R}^2 | \mathcal{R}(x, y) = 0, \mathcal{I}(x, y) = 0, x^2 + y^2 \leq 1\}.$$

Then, the problem of testing the stability reduces to that of testing that the above semi-algebraic set does not have real solutions. Without loss of generality the system $S := \{\mathcal{R}(x, y) = 0, \mathcal{I}(x, y) = 0\}$ can be assumed to be zero-dimensional (i.e., has a finite number of complex solutions). In that case, the problem resumes to compute the sign of the real solutions of S at the polynomial $x^2 + y^2 - 1$.

Example 2. We consider the polynomial $D(z) = \frac{3}{2}z^5 - \frac{27}{2}z^4 + \frac{57}{2}z^3 + \frac{7}{2}z^2 - \frac{9}{2}z + \frac{1}{2}$. We first compute the zero-dimensional system S whose real solutions are in bijection with the complex roots of $D(z)$.

$$S := \begin{cases} \mathcal{R}(x, y) = \frac{3}{2}x^5 - 15x^3y^2 + \frac{15}{2}x\,y^4 - \frac{27}{2}\,x^4 + 81x^2y^2 - \frac{27}{2}y^4 + \frac{57}{2}x^3 \\ \qquad\qquad -\frac{171}{2}x\,y^2 + \frac{7}{2}x^2 - \frac{7}{2}y^2 - \frac{9}{2}x + \frac{1}{2} = 0 \\ \\ \mathcal{I}(x, y) \;= \frac{171}{2}x^2y - \frac{9}{2}\,y - 15\,x^2y^3 + \frac{3}{2}\,y^5 + 54\,x\,y^3 - \frac{57}{2}y^3 + 7xy \\ \qquad\qquad -54x^3y + \frac{15}{2}\,x^4y = 0 \end{cases}$$

The system S is zero-dimensional and we can compute a Rational Univariate Representation of its solutions using the formulas given in Section 5.2 which yields:

$$\begin{aligned} f(t) = {} & 559872\,t^{25} - 25194240\,t^{24} + 544195584\,t^{23} - 7493513472\,t^{22} + 73628346816\,t^{21} \\ & -547311691584t^{20} + 3183535332864t^{19} - 14780593319616t^{18} + 55362880574208t^{17} \\ & -167896649845440\,t^{16} + 411029639424576\,t^{15} - 804050295433200\,t^{14} \\ & +1232226241447500\,t^{13} - 1428873627636324\,t^{12} + 1177034305128192\,t^{11} \\ & -603440918202276\,t^{10} + 126187803250443\,t^9 + 22809165295113\,t^8 \\ & -11098557635568\,t^7 + 17376699104892\,t^6 - 9925212685221\,t^5 + 2611676368585\,t^4 \\ & -821059361472\,t^3 + 262536537420\,t^2 - 42350188473\,t + 2455046453 \end{aligned}$$

$$
\begin{aligned}
g_x(t) = {} & 13996800\,t^{24} - 604661760\,t^{23} + 12516498432\,t^{22} - 164857296384\,t^{21} \\
& +1546195283136\,t^{20} - 10946233831680\,t^{19} + 60487171324416\,t^{18} \\
& -266050679753088\,t^{17} + 941168969761536\,t^{16} - 2686346397527040\,t^{15} \\
& +6165444591368640\,t^{14} - 11256704136064800\,t^{13} + 16018941138817500\,t^{12} \\
& -17146483531635888\,t^{11} + 12947377356410112\,t^{10} - 6034409182022760\,t^{9} \\
& +1135690229253987\,t^{8} + 182473322360904\,t^{7} - 77689903448976\,t^{6} \\
& +104260194629352\,t^{5} - 49626063426105\,t^{4} + 10446705474340\,t^{3} \\
& -2463178084416\,t^{2} + 525073074840\,t - 42350188473
\end{aligned}
$$

$$
\begin{aligned}
g_x(t) = {} & 25194240\,t^{24} - 1050879744\,t^{23} + 20976724224\,t^{22} - 265852699776\,t^{21} \\
& +2391835843008\,t^{20} - 16175589523776\,t^{19} + 84921114868416\,t^{18} \\
& -352340187356736\,t^{17} + 1164594239224128\,t^{16} - 3065803125993360\,t^{15} \\
& +6371804589628464\,t^{14} - 10251200537235576\,t^{13} + 12302401061993148\,t^{12} \\
& -10249204642846020\,t^{11} + 4995304129178172\,t^{10} - 576047210865300\,t^{9} \\
& -590896493514297\,t^{8} + 232387793555778\,t^{7} - 215336160313290\,t^{6} \\
& +124704312574422\,t^{5} - 32799357684699\,t^{4} + 9758271572934\,t^{3} \\
& -3373050489686\,t^{2} + 598205563056\,t - 37550186449
\end{aligned}
$$

$$
\begin{aligned}
g_y(t) = {} & -37511424\,t^{23} + 1503816192\,t^{22} - 28660687488\,t^{21} + 344722614912\,t^{20} \\
& -2925622473408\,t^{19} + 18543038368896\,t^{18} - 90562857236928\,t^{17} \\
& +346475609384832\,t^{16} - 1044493268252400\,t^{15} + 2472748660136736\,t^{14} \\
& -4535514360134424\,t^{13} + 6272956097279064\,t^{12} - 6229275628948668\,t^{11} \\
& +4056309643855968\,t^{10} - 1442957641141788\,t^{9} + 203140683497376\,t^{8} \\
& -32613756115554\,t^{7} - 114821122679658\,t^{6} + 73799941129998\,t^{5} \\
& -22045846055586\,t^{4} + 8305034379450\,t^{3} - 2665289870974\,t^{2} + 418198960296\,t \\
& -23825974876
\end{aligned}
$$

Isolating numerically the real roots of $f(t)$ and substituting in $\frac{g_x(t)}{g_1(t)}$ and $\frac{g_y(t)}{g_1(t)}$ yields the following five real solutions:

$[x = -0.45367372, y = 0], [x = 0.14614706, y = 0], [x = 0.25639717, y = 0],$
$[x = 3.59132461, y = 0], [x = 5.45980486, y = 0].$

and we can easily remark (without further symbolic computations) that the three first solutions correspond to the roots of $D(z)$ that are inside the unit disk while the two last solutions correspond to the roots of $D(z)$ that are outside the unit disk, which implies that the system is not stable.

In the case of two dimensional systems, according to DeCarlo et. al. [15], the structural stability condition, i.e.

$$D(z_1, z_2) \neq 0 \text{ for } |z_1| \leq 1, |z_2| \leq 1,$$

is equivalent to:

$$
\begin{cases}
D(z_1, 1) \neq 0 \ \text{ for } \ |z_1| \leq 1, \\
D(1, z_2) \neq 0 \ \text{ for } \ |z_2| \leq 1, \\
D(z_1, z_2) \neq 0 \ \text{ for } \ |z_1| = |z_2| = 1.
\end{cases}
$$

The two first conditions can easily be tested using classical stability tests (see for instance [16]), or the method presented above. For the last condition, if we note $z_j = x_j + i\,y_j$ testing the latter resumes to test that the following system

$$S := \begin{cases} \mathcal{R}(x_1, y_1, x_2, y_2) = 0, \\ \mathcal{I}(x_1, y_1, x_2, y_2) = 0, \\ x_1^2 + y_1^2 - 1 = 0, \\ x_2^2 + y_2^2 - 1 = 0, \end{cases}$$

where $D(x_1, y_1, x_2, y_2) = \mathcal{R}(x_1, y_1, x_2, y_2) + i\,\mathcal{I}(x_1, y_1, x_2, y_2)$, does not have real solutions. The system S consists of four polynomials in four variables and is generically zero-dimensional. One can thus compute the corresponding Rational Univariate Representation and use it to check the existence of real solutions.

Example. We consider the polynomial $D(z_1, z_2) = (12+10z_1+2z_1^2)+(6+5z_1+z_1^2)z_2$ which is shown to be devoid from complex zero in $\mathbb{D}^2$ [17]. This polynomial yields the following zero-dimensional system

$$S := \begin{cases} R(x_1, y_1, x_2, y_2) = x_1^2x_2 - 2x_1\,y_1y_2 - y_1^2x_2 + 2\,x_1^2 + 5x_1x_2 - 2y_1^2 \\ \qquad\qquad -5\,y_1y_2 + 10\,x_1 + 6x_2 + 12 = 0, \\ \\ C(x_1, y_1, x_2, y_2) = x_1^2y_2 + 2\,x_1y_1x_2 - y_1^2y_2 + 4\,x_1y_1 + 5\,x_1y_2 \\ \qquad\qquad +5\,y_1x_2 + 10\,y_1 + 6\,y_2 = 0, \\ \\ x_1^2 + y_1^2 - 1 \qquad = 0, \\ \\ x_2^2 + y_2^2 - 1 \qquad = 0, \end{cases}$$

whose solutions are encoded by the following Rational Univariate Representation

$f(t)= 144\,t^4 + 337\,t^2 + 144$, $g_1(t)= 1152\,t^3 + 1348\,t$, $g_{x_1}(t)= -1680\,t^3 - 1820\,t$, $g_{y_1}(t)= -1348\,t^2 - 1152$, $g_{x_2}(t)= -1440\,t^3 - 1685\,t$, $g_{y_2}(t)= 900\,t^2 + 900$.

Performing numerical isolation on the polynomial $f(t)$, we obtain that it does not admit real roots, which implies that the system S does not have real solutions, and thus that the initial system is stable.

Note finally that one can avoid doubling the number of variables by opting for special transformations such as Mobius transformation (see [18] for details).

6 Real roots of positive dimensional systems

In this section, we review the principal approaches for studying systems of polynomials equations that admit an infinite number of complex zeros. As mentionned in the introduction, various questions can be asked about the zero set of such systems: deciding the emptiness, computing points in each connected component of the variety, etc.

We distinguish between two general strategies. The first one, which is descibed in the next section, is based on the classical Cylindrical Algebraic Decomposition (CAD) algorithm [19]. This algorithm, based on variable elimination, one after the other, provides a partition of the real space into cells in which the given polynomials keep their sign constant. It allows one to answer to more general questions such

as deciding the truth of a first order formula, quantifier elimination, etc. However, its complexity, which is doubly exponential in the number of variable turns out to be its Achilles' heel, and prevents it from being used for system with more than two variables. The second strategy, described briefly in Section 6.2, is based on the determination of a function that reaches its extremum (at a finite number of points), on each connected component of the studied set. Putting in equation these extremum then allows one to reduce the problem to the study of zero-dimensional systems. These methods are referred as the critical point methods and lead to algorithms that have a single exponential complexity in the number of variables.

6.1 Cylindrical Algebraic Decomposition

Let start with some definitions that are used in the sequel.

A *semi-algebraic set* of $\mathbb{R}^n$ is a set of $\mathbb{R}^n$ that satisfies a logical combination of polynomial equations and inequalities with real coefficients. The set of semi-algebraic sets forms the smallest class $\mathcal{SA}_n$ of sets in $\mathbb{R}^n$ such that:

- If $P \in \mathbb{R}[x_1, \ldots, x_n]$, then $\{x \in \mathbb{R}^n \mid P(x) = 0\} \in \mathcal{SA}_n$.
- If $A \in \mathcal{SA}_n$ and $B \in \mathcal{SA}_n$, then $A \cup B$, $A \cap B$ and $\mathbb{R}^n \setminus A$ are in $\mathcal{SA}_n$.

Proposition 9. *Any semi-algebraic set of $\mathbb{R}^n$ is the union of a finite number of semi-algebraic sets of the form:*

$$\{x \in \mathbb{R}^n \mid \ P(x) = 0,\ Q_1(x) > 0, \ldots,\ Q_l(x) > 0\}$$

where $l \in \mathbb{N}$, and $P, Q_1, \ldots, Q_l \in \mathbb{R}[x_1, \ldots, x_n]$.

Definition 14. A function from $A \subset \mathbb{R}^m$ to $B \subset \mathbb{R}^n$ is *semi-algebraic* if the corresponding graph is semi-algebraic.

One knows that semi-algebraic sets of $\mathbb{R}$ decompose into an union of a finite number of points and open intervals. More generally, semi-algebraic sets of $\mathbb{R}^n$ decompose into a disjoint union of cells that are isomorphic to open hypercubes of different dimensions.

The demonstration of this property can be done by exhibing an algorithm which, given a set of polynomials, decomposes $\mathbb{R}^n$ in cells where the sign of these polynomials is invariant.

The resulting decomposition allows one to answer several questions about the zero of the system among which for example: Does the system admit real solutions?

Definition 15. A *Cylindrical Algebraic Decomposition* of $\mathbb{R}^n$ is a sequence $C_1, \ldots, C_n$ such that each C_i is a partition of $\mathbb{R}^i$ in a finite number of semi-algebraic sets satisfying:

1. Each cell C of C_1 is either a point or an open interval.

2. For any $1 \leq k < n$ and any $C \in C_k$, there exists a finite number of continuous semi-algebraic functions $\Psi_{C,1} < \ldots < \Psi_{C,l_C} \colon C \longrightarrow \mathbb{R}$ such that the cylinder $C \times \mathbb{R}$ is the disjoint union of cells in C_{k+1} that are:
   - either the graph of one the function Ψ_{C,i_C} :
   $$A_{C,j} = \{(x', x_{k+1}) \in \mathbb{C} \times \mathbb{R} \mid x_{k+1} = \Psi_{C,j}(x')\},$$
   - or the section of the cylinder bounded by the functions $\Psi_{C,j}$ et $\Psi_{C,j+1}$:
   $$B_{C,j} = \{(x', x_{k+1}) \in \mathbb{C} \times \mathbb{R} \mid \Psi_{C,j}(x') < x_{k+1} < \Psi_{C,j+1}(x')\}.$$

Proposition 10. *Every cell of a Cylindrical Algebraic Decomposition of $\mathbb{R}^n$ is semi-algebraically homeomorphic to an open hypercube of the form $(0,1)^k$.*

Given a set of polynomials F, a subset S of $\mathbb{R}^n$ is said to be *F-invariant* if the sign of each polynomial in F is constant inside S. In the following, we are going to show how to compute a Cylindrical Algebraic Decomposition adapted to a set of polynomial F, that is a decomposition of $\mathbb{R}^n$ into cells that are F-invariant. The resulting Cylindrical Algebraic Decomposition is then said to be F-invariant.

Example 3. Consider the polynomial $f = x - y^2 - 1$. We provide a Cylindrical Algebraic Decomposition adapted to f, that is, a partition of $\mathbb{R}^2$ into cells that are f-invariant.

The latter is given by the sequence C_1, C_2 where:

- C_1 is the partition of $\mathbb{R}$ that consists of $]-\infty, 1[, \{1\},]1, +\infty[$
- C_2 is the partition of $\mathbb{R}^2$ that consists of the following semi-algebraic set:
  - $C_{2,1} = \{(x,y) \in \mathbb{R}^2 | x < 1\}$,
  - $C_{2,2} = \{(x,y) \in \mathbb{R}^2 | x = 1, y < 0\}$,
  - $C_{2,2} = \{(x,y) \in \mathbb{R}^2 | x = 1, y = 0\}$,
  - $C_{2,3} = \{(x,y) \in \mathbb{R}^2 | x = 1, y > 0\}$,
  - $C_{2,4} = \{(x,y) \in \mathbb{R}^2 | x > 1, x^2 - y^2 - 1 > 0, y < 0\}$,
  - $C_{2,5} = \{(x,y) \in \mathbb{R}^2 | x > 1, x^2 - y^2 - 1 = 0, y < 0\}$,
  - $C_{2,6} = \{(x,y) \in \mathbb{R}^2 | x > 1, x^2 - y^2 - 1 < 0\}$,
  - $C_{2,7} = \{(x,y) \in \mathbb{R}^2 | x > 1, x^2 - y^2 - 1 = 0, y > 0\}$,
  - $C_{2,8} = \{(x,y) \in \mathbb{R}^2 | x > 1, x^2 - y^2 - 1 > 0, y > 0\}$,

and each cell $C_{2,i}$ for $i = 1, \ldots, 9$ is f-invariant.

If we have a look to the interval $]1, +\infty[$, the corresponding cylinder, that is, $\mathcal{C} :=]1, +\infty[\times \mathbb{R}$, is decomposed by means of the following semi-algebraic functions:

- $\Psi_{\mathcal{C},1} :]1, +\infty[\to \mathbb{R}$
  $y \mapsto -\sqrt{x-1}$,
- $\Psi_{\mathcal{C},2} :]1, +\infty[\to \mathbb{R}$
  $y \mapsto \sqrt{x-1}$.

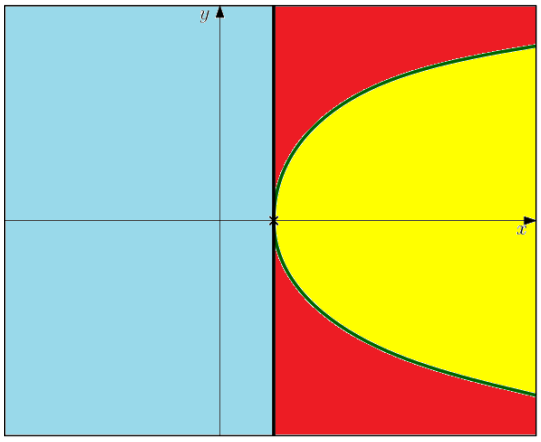

Fig. 3: Decomposition of $\mathbb{R}^2$ in $(x - y^2 - 1)$-invariant cells

More generally, we have the following result.

Proposition 11. *Let $P(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$, $C \subset \mathbb{R}^{n-1}$ be a connected semi-algebraic set and $k \leq d$ a positive integer such that for each point $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in C$, the polynomial $P(\alpha, x_n)$ has degree d and admits exactly k complex roots. Then, there exist $l \leq k$ continuous semi-algebraic functions $\Psi_1 < \ldots < \Psi_l : C \longrightarrow \mathbb{R}$, such that for each $\alpha \in C$, the set of real roots of $P(\alpha, x_n)$ is exactly $\{\Psi_1(\alpha), \ldots, \Psi_l(\alpha)\}$. Moreover, for $i = 1 \ldots l$, the multiplicity of the roots $\Psi_i(\alpha)$ is constant for $\alpha \in C$.*

Let now consider a set of polynomials. We need to obtain results about the relative positions of their zeros. A basic result is the following.

Proposition 12. *Let P and Q be two polynomials in $\mathbb{R}[x_1, \ldots, x_n]$ and C a connected component of a semi-algebraic set of $\mathbb{R}^{n-1}$. Let suppose that the degree and the number of distinct complex roots of P and Q are constant above C and so that for their gcd (finite number of common solutions). Let $\xi, \zeta : C \to \mathbb{R}$ be two continuous semi-algebraic functions such that $P(\alpha, \xi(\alpha)) = 0$ and $Q(\alpha, \zeta(\alpha)) = 0$ for all $\alpha \in C$. If there exists $\beta \in C$ such that $\xi(\beta) = \zeta(\beta)$, then $\xi(\alpha) = \zeta(\alpha)$ for all $\alpha \in C$.*

The two above propositions allow us to construct semi-algebraic functions that have the same properties as the functions used in a CAD of $\mathbb{R}^n$. These functions are actually the roots of P and Q with respect to the last variable. Hence, we almost reach the initial objectif since outside these semi-algebraic functions, and under the hypotheses of the above propositions, the sign of P and Q is constant. It remains thenceforth to address the cases where the hypotheses of the propositions are not satisfied, that is:

- The components where the degree of P and Q varies, i.e., where the leading term vanishes; In that case, we need to perform the same operation on P (resp. Q) deprived from its leading term.
- The components where the degree of the gcd of P and Q varies, i.e., where the resultant of these polynomials vanishes.

Definition 16. Let $P_1, \ldots, P_r$ be polynomials in $\mathbb{R}[x_1, \ldots, x_n]$. We denote by PROJ$(P_1, \ldots, P_r)$ the minimal set of polynomials in $\mathbb{R}[x_1, \ldots, x_n]$ that satisfies the following conditions:

- If $\deg_{x_n}(P_i) = d \leq 2$, PROJ$(P_1, \ldots, P_r)$ contains all the non constant polynomials among the principal subresultants (Definition 6), $\sigma_j(P_i, \frac{\partial P_i}{\partial x_n})$, $j = 0 \ldots d-1$ (variations of the number of roots of P_i).
- If $1 \leq d = \min(\deg_{x_n}(P_i), \deg_{x_n}(P_k))$, PROJ$(P_1, \ldots, P_r)$ contains all the non constant polynomials among the principal subresultants $\sigma_j(P_i, P_k)$, $j = 0 \ldots d$ (variation of the number of common roots of two polynomials).
- If $\deg_{x_n}(P_i) \geq 1$ and $\mathrm{lc}_{x_n}(P_i)$ is not constant, PROJ$(P_1, \ldots, P_r)$ contains $\mathrm{lc}_{x_n}(P_i)$ and the set PROJ$(P_1, \ldots, P_r, \text{Trunc}(P_i))$ [1] (case of non constant polynomials in x_n whose the leading term vanishes).
- If $\deg_{X_n}(P_i) = 0$ and P_i non constant, PROJ$(P_1, \ldots, P_r)$ contains P_i (constant polynomials in x_n).

A direct consequence of the propositions stated above is the following theorem:

Theorem 11. *Let $\{P_1, \ldots, P_r\}$ be a set of polynomials in $\mathbb{R}[x_1, \ldots, x_n]$ and C a connected semi-algebraic set $(P_1, \ldots, P_r)$-invariant. Then, there exist continuous semi-algebraic functions $\Psi_1 < \ldots < \Psi_l : C \to \mathbb{R}$ such that for any $\alpha \in C$, the set of $\{\Psi_1(\alpha), \ldots, \Psi_l(\alpha)\}$ is the set of roots of non-identically zero polynomials in $\{P_1, \ldots, P_r\}$. The graph of each Ψ_i and the sections of the cylinder $C \times \mathbb{R}$ bounded by the graphs of Ψ_i and Ψ_{i+1}, $i = 1, \ldots, l-1$ are connected semi-algebraic sets, homeomorphic to C or $C \times (0,1)$ respectively, and $(P_1, \ldots, P_r)$-invariants.*

Having constructed a CAD of $\mathbb{R}^{n-1}$ adapted to $\{P_1, \ldots, P_r\}$, the above theorem allows us to extend the latter to a CAD of $\mathbb{R}^n$ adapted to $\{P_1, \ldots, P_r\}$. By iteratively constructing the set PROJ$(.)$ from $P_1, \ldots, P_r$ (i.e. PROJ(PROJ(...))), one ends up, after $n-1$ steps, with a finite set of polynomials in x_1. The final step then consists in computing a CAD for these univariate polynomials. The real roots of these polynomials decompose the real axis into a finite number of points and open intervals. This algorithmical construction proves the following general result.

Theorem 12. *For any set of polynomials $\{P_1, \ldots, P_r\}$ in $\mathbb{R}[x_1, \ldots, x_n]$, there exists a CAD of $\mathbb{R}^n$ adapted to $\{P_1, \ldots, P_r\}$.*

Cylindrical Algebraic decomposition is implemented in most computer algebraic softwares such as `Maple` (in the package RegularChains[SemiAlgebraicSetTools]) or `Mathematica`.

[1] Trunc(P_i) refers to the polynomial obtained after reducing all the coefficients of P_i modulo $\mathrm{lc}_{x_n}(P_i)$.

6.1.1 CAD for testing the structural stability

Let us go back to the problem of testing the structural stability of multidimensional system and show how Cylindrical Algebraic Decomposition can be used in this context. Checking the structural stability of a two dimensional systems, i.e. $D(z_1, z_2) \neq 0$ for $|z_1| \leq 1, |z_2| \leq 1$, can be reduced, via the transformations $z_i = x_i + i\, y_i$, to testing that the following semi-algebraic set is empty.

$$S := \begin{cases} \mathcal{R}(x_1, y_1, x_2, y_2) = 0, \\ \mathcal{I}(x_1, y_1, x_2, y_2) = 0, \\ x_1^2 + y_1^2 \leq 1, \\ x_2^2 + y_2^2 \leq 1. \end{cases}$$

This can be done by computing a Cylindrical Algebraic Decomposition of $\mathbb{R}^4$ adapted to the polynomials $\mathcal{R}, \mathcal{I}$ and $x_i^2 + y_i^2 - 1$ for $i = 1, 2$, and then check if this decomposition contain cells satisfying the sign conditions of S.

Example 4. We consider the polynomial $D(z_1, z_2) = 6 + 5\, z_1 + z_2$. After transformation, the latter yields the following semi-algebraic set:

$$S := \begin{cases} \mathcal{R}(x_1, y_1, x_2, y_2) = 5\, x_1 + x_2 + 6 = 0, \\ \mathcal{I}(x_1, y_1, x_2, y_2) = 5\, y_1 + y_2 = 0, \\ x_1^2 + y_1^2 \leq 1, \\ x_2^2 + y_2^2 \leq 1. \end{cases}$$

Computing a CAD adapted to $\mathcal{I}, \mathcal{R}, x_1^2+y_1^2-1, x_2^2+y_2^2-1$ returns (after 2/3 minutes of computations) 1717 cells. Among these cells, 177 satisfy the above conditions which correspond to the real zeros of the system S. This implies that the input system is not stable.

If we consider the polynomial $D(z_1, z_2) = 2 - z_1\, z_2$, the CAD associated with the polynomials of the corresponding system S returns (after 30 minutes of computations) 31655 cells and outputs 3687 real points satisfying the condition of S. Again the system is not stable.

In practice, we can observe that when the polynomial D is bivariate with total degree larger than 2 or has more than 2 variables (which yields semi-algebraic systems with at least six variables), the previous CAD-based approach fails to return an answer in a reasonable time. This is mainly due to the size of the output (the number of cells) which is doubly exponential in the number of variables. However, when we are only interested in deciding the emptiness of a real semi-algebraic set, this doubly exponential behavior can be overcome by opting for alternative methods, which we will describe in the next section.

6.2 Critical points methods

When we are only interested in deciding if a system of positive complex dimension has (or not) real roots, the Cylindrical Algebraic Decomposition might answer but

this algorithm has a prohibitive complexity while it computes too much information. Alternatively, the so-called critical point methods allow one to compute at least one point in each semi-algebraically connected component of the studied semi-algebraic set and turn out to be, in general, much more efficient in practice.

Critical point methods are essentially based on the determination of a function that reaches its extrema (at a finite number of points), on each connected component of the studied set. Putting in equations these extremum then allow one to reduce the problem to the study of zero-dimensional systems which can be done using the algorithms described in Section 5 (which are known to be in a complexity that is single exponential in the number of variables). For a sake of simplicity, in the sequel, we will only consider the case of algebraic sets even if such methods can easily be extended to the case of semi-algebraic sets.

Let us start with some definitions needed in the sequel.

Definition 17. Let $V \subset \mathbb{C}^n$ be an algebraic variety and denote by $\mathcal{I}(V)$ the corresponding radical ideal (the set of polynomials that vanish on V).

- If f is a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$, the differential of f at a point $\alpha = (\alpha_1, \ldots, \alpha_n)$, denoted by $d_\alpha(f)$, is defined by,

$$d_\alpha(f) = \frac{\partial f}{\partial x_1}(x_1 - \alpha_1) + \cdots + \frac{\partial f}{\partial x_n}(x_n - \alpha_n).$$

- The tangent space of V at a point p, denoted by $T_\alpha(V)$, is the points of $\mathbb{C}^n$ on which the differential $d_\alpha(f)$ vanishes for all $f \in \mathcal{I}(V)$.

Definition 18. Let $V \subset \mathbb{C}^n$ be an algebraic variety, and $\varphi_1, \ldots, \varphi_s$ polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$. Define the following polynomial application:

$$\begin{aligned} \varphi : V &\longrightarrow \mathbb{C}^m \\ \alpha &\longmapsto (\varphi_1(\alpha), \ldots, \varphi_m(\alpha)). \end{aligned}$$

- The set of critical points of φ restricted to V is the set of points of V such that the differential map $d_\alpha(\varphi) : T_\alpha(V) \longrightarrow \mathbb{C}^m$ is not surjective, or in other words, such that the rank of $d_\alpha(\varphi)$ is strictly smaller than m.

A fundamental result concerns the critical points of an application restricted to a *compact* [2] algebraic variety.

Theorem 13. *[7] Let $V \subset \mathbb{C}^n$ be a compact algebraic variety and $\varphi : V \longrightarrow \mathbb{C}^m$ a polynomial application. Then the set of the critical points of φ restricted to V intersect $V \cap \mathbb{R}^n$ in each of its connected components.*

In some simple cases, one can easily derive an algebraic characterisation of the set of critical points of an application restricted to a variety. Indeed, given an algebraic variety $V \subset \mathbb{C}^n$ whose the corresponding radical ideal $\mathcal{I}(V)$ is generated by

[2] Here, the term compact is used for subsets of the Euclidean space $\mathbb{R}^n$, which are closed and bounded regarding to the classical Euclidean topology.

a finite number of polynomials $f_1, \ldots, f_s$. The tangent space at each point $p \in V$, $T_\alpha(V)$, is defined as the kernel of the linear application defined by the following matrix, which corresponds to the evalutation at α of the Jacobian matrix associated with the polynomials $f_1, \ldots, f_s$, namely:

$$\text{Jac}(f_1, \ldots, f_s)_\alpha := \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\alpha) & \cdots & \frac{\partial f_1}{\partial x_n}(\alpha) \\ \vdots & \vdots & \vdots \\ \frac{\partial f_s}{\partial x_1}(\alpha) & \cdots & \frac{\partial f_s}{\partial x_n}(\alpha) \end{pmatrix}$$

On the other hand, given a polynomial application $\varphi : V \longrightarrow \mathbb{C}^m$, the differential of φ at a point $\alpha \in V$ is the linear application which associates to each vector $v = (v_1, \ldots, v_n) \in T_\alpha(V)$, the vector $(d_\alpha(\varphi_1)(v), \ldots, d_\alpha(\varphi_m)(v))$, and whose matrix is defined by:

$$\text{Jac}(\varphi_1, \ldots, \varphi_m)_\alpha := \begin{pmatrix} \frac{\partial \varphi_1}{\partial x_1}(\alpha) & \cdots & \frac{\partial \varphi_1}{\partial x_n}(\alpha) \\ \vdots & \vdots & \vdots \\ \frac{\partial \varphi_m}{\partial x_1}(\alpha) & \cdots & \frac{\partial \varphi_m}{\partial x_n}(\alpha) \end{pmatrix}.$$

A point α is said to be *critical* for φ if the rank of the above matrix is strictly smaller than m or in other words if its kernel has dimension larger or equal than one. Consequently, α is a critical point if there exists $(v_1, \ldots, v_n) \neq (0, \ldots, 0)$ such that

$$\begin{cases} \frac{\partial \varphi_1}{\partial x_1}(\alpha)\, v_1 + \cdots + \frac{\partial \varphi_1}{\partial x_n}(\alpha) v_n = 0, \\ \qquad\qquad \vdots \\ \frac{\partial \varphi_m}{\partial x_1}(\alpha)\, v_1 + \cdots + \frac{\partial \varphi_m}{\partial x_n}(\alpha) v_n = 0, \end{cases}$$

under the following conditions that:

$$\begin{cases} \frac{\partial f_1}{\partial x_1}(\alpha)\, v_1 + \cdots + \frac{\partial f_1}{\partial x_n}(\alpha) v_n = 0, \\ \qquad\qquad \vdots \\ \frac{\partial f_s}{\partial x_1}(\alpha)\, v_1 + \cdots + \frac{\partial f_s}{\partial x_n}(\alpha) v_n = 0. \end{cases}$$

When the algebraic variety V is *smooth* and *equidimensional* of dimension d [3], the rank of the Jacobian matrix of $f_1, \ldots, f_s$ has dimension $n-d$, and a point $\alpha \in V$ is a critical point of φ if we have:

$$\text{Rank}(\text{Jac}(f_1, \ldots, f_s)_\alpha) + \text{Rank}(\text{Jac}(\varphi_1, \ldots, \varphi_m)_\alpha) < n - d + m,$$

that is, the rank of the following matrix

[3] An algebraic variety is said to be equidimensional if all it irreducible components have the same dimension.

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\alpha) & \cdots\cdots & \frac{\partial f_1}{\partial x_n}(\alpha) \\ \vdots & \vdots & \vdots \\ \frac{\partial f_s}{\partial x_1}(\alpha) & \cdots\cdots & \frac{\partial f_s}{\partial x_n}(\alpha) \\ \\ \frac{\partial \varphi_1}{\partial x_1}(\alpha) & \cdots\cdots & \frac{\partial \varphi_1}{\partial x_n}(\alpha) \\ \vdots & \vdots & \vdots \\ \frac{\partial \varphi_m}{\partial x_1}(\alpha) & \cdots\cdots & \frac{\partial \varphi_m}{\partial x_n}(\alpha) \end{pmatrix},$$

is strictly smaller than $n-d+m$, or equivalently, if all its $(n-d+m, n-d+m)$ minors vanish on p. This yields the following theorem which gives a characterization of the critical points of a polynomial application restricted to a smooth and equidimensional variety.

Theorem 14. *Let $V \subset \mathbb{C}^n$ be a smooth and equidimensional variety of dimension d that is defined as the zero set of the radical ideal $\langle f_1, \ldots, f_s \rangle$ and φ: $\alpha \in \mathbb{C}^n \longrightarrow (\varphi_1(\alpha), \ldots, \varphi_m(\alpha)) \in \mathbb{C}^m$ a polynomial application. The set of critical points of φ restricted to V is the zero-set of the algebraic system that consists of:*

1. *The equations $f_1 = \cdots = f_m = 0$.*
2. *The $(n-d-m, n-d-m)$ minors of the matrix Jac$(f_1, \ldots, f_s, \varphi_1, \ldots, \varphi_m)$.*

Moreover, the above system is zero-dimensional, i.e., admits a finite number of zeros in $\mathbb{C}^n$.

As an example, given an algebraic variety defined by a unique equation

$$V(f) = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n \mid f(\alpha_1, \ldots, \alpha_n) = 0\},$$

which we suppose *smooth* and *compact*, and considering the projection function $\Pi_{x_1} : (x_1, \ldots, x_n) \in \mathbb{C}^n \longrightarrow x_1 \in \mathbb{C}$, the set of critical points of Π_{x_1} restricted to $V(f)$ is finite and intersect each connected component of $V(f) \cap \mathbb{R}^n$. According to Theorem 14, this set of critical points can be defined as the zero-set of the system defined by $f = 0$ and the vanishing of $(2,2)$ minors of the matrix $\begin{pmatrix} \frac{\partial f}{\partial x_1} & \frac{\partial f}{\partial x_2} & \cdots & \frac{\partial f}{\partial x_n} \\ 1 & 0 & \cdots & 0 \end{pmatrix}$, that is, $\frac{\partial f}{\partial x_2} = 0, \ldots, \frac{\partial f}{\partial x_n} = 0$.

Example 5. Consider the sphere $\mathcal{S}$ defined by the equation $x^2+y^2+(z-1)^2-1=0$ and the projection $\Pi_x : (x, y, z) \in \mathbb{C}^3 \longrightarrow x$. According to Theorem 14, the critical points of Π_x restricted to $\mathcal{S}$ are the solutions of the following system

$$\begin{cases} x^2 + y^2 + (z-1)^2 - 1 = 0, \\ 2\,y = 0, \\ 2z - 2 = 0, \end{cases}$$

that is, the two real points $(1, 0, 1)$ and $(-1, 0, 1)$ of $\mathcal{S}$ (see Figure 4).

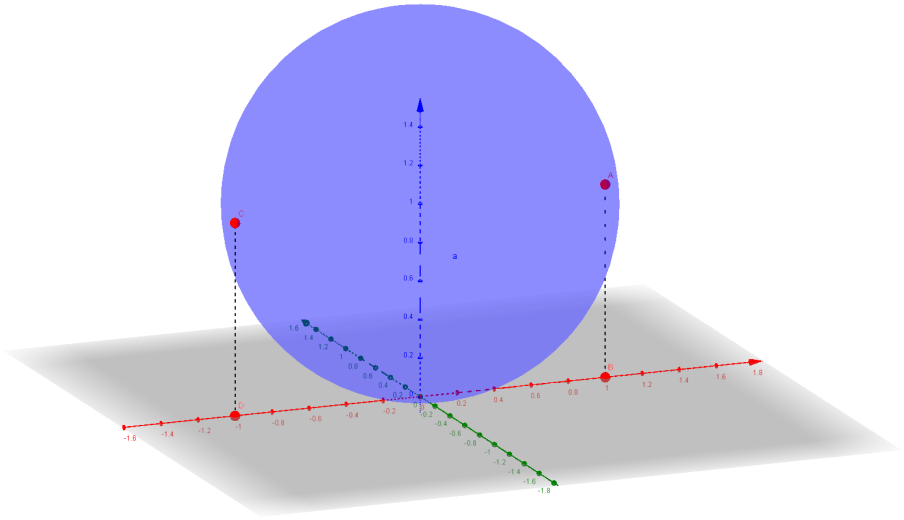

Fig. 4: Critical points of Π_x restricted to the variety $x^2+y^2+(z-1)^2-1=0$

Changing the function sometimes allows one to get rid of some asumptions. For example, to avoid the compactness assumption, one can consider the extrema of the distance function to some point A. When the point A is chosen *generic* enough and the set $V(f)$ is smooth, this allows one to reduce the problem to the resolution of a zero-dimensional. More precisely, the set of critical points of the distance function with respect to A is defined by

$$V(\mathcal{C}(A)) = \{p \in \mathbb{C}^n \mid f(p) = 0 \wedge \text{grad}_p(f) // \overrightarrow{\text{Ap}}\},$$

where $\text{grad}_p(f)$ is the gradient vector of f at the point $p=(p_1,\ldots,p_n)$. The points of $V(\mathcal{C}(A))$ are the zeros of the ideal generated by $\mathcal{C}(A) = \{f, f_{1,A}, \ldots, f_{r,A}\}$ where the $f_{i,A}$ are the 2×2 minors of the matrix $\begin{pmatrix} \frac{\partial f}{\partial x_1} & \cdots & \frac{\partial f}{\partial x_n} \\ x_1-a_1 & \cdots & x_n-a_n \end{pmatrix}$.

The main algorithmical problem when using such a general strategy is that the asumptions made on the system cannot easily be checked (compactness, smoothness and equidimensionality) and/or bypassed, and the situation becomes more involved when dealing with systems of equations of the form $\{f_1=0,\ldots,f_s=0\}$ rather than a unique one.

In [7] for instance, the authors first replace the system $\{f_1=0,\ldots,f_s=0\}$ by the unique equation $f=\sum f_i^2$, then add an infinitesimal Ω and a new variable to switch to a bounded variety $f_\Omega = f^2+(x_1^2+\ldots+x_n^2+x_{n+1}^2-(\frac{1}{\Omega})^2)$ and then add a second infinitesimal ϵ to get a smooth and bounded variety defined by a unique equation $f_{\Omega,\epsilon} = (1-\epsilon)f_\Omega+\epsilon\left(x_1^{2(d_1+1)}+\ldots+x_n^{2(d_n+1)}+x_{n+1}^6-3(\frac{1}{\Omega}-1)^{2(d_1+1)}\right)$.

The algorithm then becomes rather simple since it "suffices" to study the system $\left\{f_{\Omega,\epsilon} = 0, \frac{\partial f_{\Omega,\epsilon}}{\partial x_2} = 0, \ldots, \frac{\partial f_{\Omega,\epsilon}}{\partial x_{n+1}} = 0\right\}$ and then take the limits (when $\Omega, \epsilon \to 0$) of the solutions. However, such a strategy turns out to be quite inefficient in practice, mainly because of the costly computations induced by the infinitesimal deformations as well as the degree increase produced by the sum of squares.

In [20], the authors avoid computing sum of squares as well as infinitisimal deformations by considering the distance function and recursively computing the critical points of the singular locus (which is another algebraic variety of smaller dimension).

The current state of the art algorithms and implementations (see [21, 22]) use extended notions of critical points/values (generalized critical values) to avoid the compactness assumption and prevent as much as possible either recursive call and/or costly decompositions.

References

1. A. Neumaier, *Introduction to numerical analysis*. Cambridge University Press, 2001.
2. G. E. Collins and A. G. Akritas, "Polynomial real root isolation using descarte's rule of signs," in *Proceedings of the third ACM symposium on Symbolic and algebraic computation*. ACM, 1976, pp. 272–275.
3. W. C. Rheinboldt, *Methods for solving systems of nonlinear equations*. SIAM, 1998, vol. 70.
4. B. Mourrain and J. Pavone, "Subdivision methods for solving polynomial equations," *J. Symb. Comput.*, vol. 44, no. 3, pp. 292–306, 2009.
5. Y. Bouzidi, A. Quadrat, and F. Rouillier, "Computer algebra methods for testing the structural stability of multidimensional systems," in *Multidimensional (nD) Systems (nDS), 2015 IEEE 9th International Workshop on*. IEEE, 2015, pp. 1–6.
6. D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, 3rd ed., ser. Undergraduate Texts in Mathematics. New York: Springer-Verlag, 2007.
7. S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, 2nd ed., ser. Algorithms and Computation in Mathematics. Springer-Verlag, 2006, vol. 10.
8. I. Z. Emiris, B. Mourrain, and E. P. Tsigaridas, "The DMM bound: Multivariate (aggregate) separation bounds," in *ISSAC'10*, S. Watt, Ed. Munich, Germany: ACM, July 2010, pp. 243–250.
9. F. Rouillier and P. Zimmermann, "Efficient isolation of polynomial real roots," *J. of Computational and Applied Mathematics*, vol. 162, no. 1, pp. 33–50, 2003.
10. B. Buchberger, *Gröbner bases : An Algorithmic Method in Polynomial Ideal Theory*, ser. Recent Trends in Multidimensional Systems Theory. Reider ed. Bose, 1985.
11. J.-C. Faugère, "A new efficient algorithm for computing Gröbner bases (F_4)," *J. of Pure and Applied Algebra*, vol. 139, no. 1–3, pp. 61–88, June 1999.
12. W. D. Brownawell *et al.*, "A pure power product version of the hilbert nullstellensatz." *The Michigan Mathematical Journal*, vol. 45, no. 3, pp. 581–597, 1998.
13. F. Rouillier, "Solving zero-dimensional systems through the rational univariate representation," *J. of Applicable Algebra in Engineering, Communication and Computing*, vol. 9, no. 5, pp. 433–461, 1999.
14. N. Revol and F. Rouillier, "Motivations for an arbitrary precision interval arithmetic and the mpfi library," *Reliable Computing*, vol. 11, pp. 1–16, 2005.
15. R. A. Decarlo, J. Murray, and R. Saeks, "Multivariable Nyquist theory," *International Journal of Control*, vol. 25, no. 5, pp. 657–675, 1977.

16. Y. Bistritz, "Zero location with respect to the unit circle of discrete-time linear system polynomials," *Proceedings of the IEEE*, vol. 72, no. 9, pp. 1131–1142, 1984.
17. L. Li, L. Xu, and Z. Lin, "Stability and stabilisation of linear multidimensional discrete systems in the frequency domain," *International Journal of Control*, vol. 86, no. 11, pp. 1969–1989, 2013.
18. Y. Bouzidi and F. Rouillier, "Certified algorithms for proving the structural stability of two dimensional systems possibly with parameters," in *MNTS 2016-22nd International Symposium on Mathematical Theory of Networks and Systems*, 2016.
19. G. Collins, "Quantifier elimination for real closed fields by cylindrical algebraic decomposition," *Springer Lecture Notes in Computer Science 33*, vol. 33, pp. 515–532, 1975.
20. P. Aubry, F. Rouillier, and M. S. E. Din, "Real solving for positive dimensional systems," *Journal of Symbolic Computation*, vol. 34, no. 6, pp. 543 – 560, 2002. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747717102905638
21. "RAGLIB: A library for real solving polynomial systems of equations and inequalities," http://www-salsa.lip6.fr/~safey/RAGLib/.
22. M. Safey El Din and É. Schost, "Polar varieties and computation of one point in each connected component of a smooth real algebraic set," in *Proceedings of ISSAC 2003*. ACM, 2003, pp. 224–231.