École Doctorale Sciences et Technologies de Versailles

THÈSE
pour obtenir le grade de

DOCTEUR de l'UNIVERSITÉ de VERSAILLES-SAINT-QUENTIN
Spécialité Mathématiques

Présentée par

Aurélien Greuet

Optimisation polynomiale et variétés polaires : théorie, algorithmes et implantations.

Thèse soutenue le 5 décembre 2013 devant le jury composé de

Vincent Cossart	Professeur - Université de Versailles (Directeur)
Jean-Charles Faugère	Directeur de Recherche Inria - CRI Paris-Rocquencourt
Stéphane Gaubert	Directeur de Recherche Inria - CRI Saclay
Marc Giusti	Directeur de Recherche CNRS - École Polytechnique (Président)
Didier Henrion	Directeur de Recherche CNRS - LAAS-CNRS (Rapporteur)
Mohab Safey El Din	Professeur - Université Pierre et Marie Curie (Directeur)
Markus Schweighofer	Professeur - Université de Constance (Rapporteur)

Résumé

Le calcul de l'infimum global $f^\star$ d'un polynôme à n variables sous contraintes est une question centrale qui apparaît dans de nombreux domaines des sciences de l'ingénieur. Pour certaines applications, il est important d'obtenir des résultats fiables. De nombreuses techniques ont été développées dans le cas où les contraintes sont données par des inéquations polynomiales.
Dans cette thèse, on se concentre sur le problème d'optimisation d'un polynôme à n variables sous des contraintes définies par des équations polynomiales à n variables. Notre but est d'obtenir des outils, algorithmes et implémentations efficaces et fiables pour résoudre ces problèmes d'optimisation.

Notre stratégie est de ramener le problème d'optimisation sous des contraintes qui définissent des ensembles algébriques de dimension quelconque à un problème équivalent, sous des nouvelles contraintes dont on maîtrise la dimension. La variété algébrique définie par ces nouvelles contraintes est l'union du lieu critique du polynôme objectif et d'un ensemble algébrique de dimension au plus 1. Pour cela, on utilise des objets géométriques définis comme lieux critiques de projections linéaires.

Grâce au bon contrôle de la dimension, on prouve l'existence de certificats pour des bornes inférieures sur $f^\star$ sur nos nouvelles variétés. Ces certificats sont donnés par des sommes de carrés et on ne suppose pas que $f^\star$ est atteint.

De même, on utilise les propriétés de nos objets géométriques pour concevoir un algorithme exact pour le calcul de $f^\star$. S'il existe, l'algorithme renvoie aussi un minimiseur. Pour un problème avec s contraintes et des polynômes de degrés au plus D, la complexité est essentiellement cubique en $(sD)^n$ et linéaire en la complexité d'évaluation des entrées. L'implantation, disponible sous forme de bibliothèque Maple, reflète cette complexité. Elle a permis de résoudre des problèmes inatteignables par les autres algorithmes exacts.

Abstract

Computing the global infimum $f^\star$ of a multivariate polynomial subject to some constraints is a central question since it appears in many areas of engineering science. For some particular applications, it is of first importance to obtain reliable results. A lot of techniques has emerged to deal with constraints defined by polynomial inequalities.
In this thesis, we focus on the optimization problem of a n-variate polynomial subject to constraints defined by n-variate polynomial equations. Our goal is to obtain reliable and efficient tools, algorithms and implementations to solve polynomial optimization problems.

To do that, our strategy is to reduce the optimization problem subject to constraints defining algebraic sets of arbitrary dimension to an equivalent optimization problem, subject to constraints defining algebraic sets whose dimension is well-controlled. The algebraic variety defined by these new constraints is the union of the critical locus of the objective polynomial and an algebraic set of dimension at most 1. This is done by means of geometric objects defined as critical loci of linear projections.

Since the dimension is well-controlled, the existence of certificates for lower bounds on $f^\star$ can be proved on this new variety. This is done by means of sums of squares and it does not require that $f^\star$ is reached.

Likewise, we use the properties of our geometric objects to design an exact algorithm computing $f^\star$. If it exists, a minimizer is also returned. If there are s constraints and if all the polynomials have degree at most D, its complexity is essentially cubic in $(sD)^n$ and linear in the evaluation complexity of the input. Its implementation, available as a Maple library, reflects the theoretical complexity. It solves problems unreachable by previous exact algorithms.

Contents

Introduction

Problem Statement

Let $\mathbf{X} = \{X_1, \ldots, X_n\}$ be a set of indeterminates and $\mathbf{F} = \{f_1, \ldots, f_s\}$ be a sequence of polynomials in $\mathbb{Q}[\mathbf{X}]$ of degree at most D. Let $\mathcal{S}$ be the semi-algebraic set

$$\mathcal{S} = \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}.$$

Let $f \in \mathbb{Q}[\mathbf{X}]$ be another polynomial of degree at most D. The global polynomial optimization problem is the following.

Given $f \in \mathbb{Q}[\mathbf{X}]$ and a semi-algebraic set $\mathcal{S} \subset \mathbb{R}^n$ as above, solve *the global optimization problem*

$$f^\star = \inf_{x \in \mathcal{S}} f(x).$$

The real algebraic number $f^\star$ can lie in an extension of $\mathbb{Q}$ whose degree is exponential in n. Hence, it can be hard to give an exact representation. In the sequel, an algebraic representation of $f^\star$ is defined by a polynomial $P \in \mathbb{Q}[T]$ and an interval $I \subset \mathbb{R}$ such that P has only one root in I, that is $f^\star$.

Let $V \subset \mathbb{C}^n$ be the algebraic variety $\mathbb{V}(\mathbf{F}) = \{x \in \mathbb{C}^n \mid f_1(x) = \cdots = f_s(x) = 0\}$. In this thesis, we focus on the global optimization problem when $\mathcal{S} = V \cap \mathbb{R}^n$.

Given $f \in \mathbb{Q}[\mathbf{X}]$ and an algebraic variety $V \subset \mathbb{C}^n$ as above, solve *the global polynomial optimization problem*

$$f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x).$$

Solving the optimization problem may have several meanings:

(A) Computing certificates for lower bounds on $f^\star$.

(B) Deciding the finiteness and computing an algebraic representation of $f^\star$.

(C) Deciding whether there exists $x^\star \in V \cap \mathbb{R}^n$ such that $f(x^\star) = f^\star$ and computing a rational parametrization of $x^\star$.

These problems are NP-hard (see [98]). For some applications such as program verification, it is important to obtain reliable results. The goal of this thesis is to provide efficient tools, algorithms and implementations for solving problems (A), (B) and (C). Furthermore, our goal is to combine practical efficiency with reliability.

Motivations and Goal of the Thesis

Motivations

Polynomial optimization appears in various areas of engineering sciences. For instance, it is natural to deal with optimization in economics or in control theory [60, 62].

It also appears in static analysis of programs [36, 95], where the correctness of some particular programs can be reduced to a polynomial optimization problem. Likewise, some combinatorial problems can be translated into polynomial optimization problems [34]. Applications of these problems can be found in very-large-scale integration circuit design and statistical physics [40, 48].

Geometric problems such as the computation of the Fermat-Weber point can be translated to polynomial optimization problems. Given points $p_1, \ldots, p_s \in \mathbb{R}^n$, the goal is to find a point $p \in \mathbb{R}^n$ that minimizes $\sum_{1 \leq i \leq s} \|p - p_i\|_2$. Introducing new variables and using elimination techniques, the problem can be reduced to the minimization of a new variable d on a set of constraints defined by polynomial equations in the variables $\mathbf{X}$ and d. This problem appears when we try to find the best place to locate a firm in a given region [49].

The polynomial optimization problem also appears in computer vision. Consider the triangulation problem, that is a fundamental problem in multi-view geometry [56]. The space of pictures of three-dimensional objects seen from more than two cameras has an algebraic description. Then the triangulation problem can be translated to an optimization problem with constraints defined by polynomial equations [3, 4].

State of the Art

Methods based on sum of squares decomposition have been developed to tackle problem (A). A non-negative univariate polynomial can always be written as a sum of squares [128]. This is not true for the multivariate case. However, if a sum of squares representation exists, an approximation can be computed using semidefinite programming [61, 84, 103, 135]. Furthermore, there exist methods to compute rational certificates by rationalizing a numerical certificate obtained by semidefinite programming [75, 105]. The idea is then to add constraints to ensure the existence of certificates. It has been done in [39, 101] when $f^\star$ is reached. In [141], existence of certificates on a semi-algebraic set is obtained without assuming that $f^\star$ is reached. However, because many auxiliary constraints are introduced and because they have high degree, the SOS relaxations can be hard to solve. It is then relevant to obtain simpler constraints, without the assumption that $f^\star$ is reached. In [1, 2, 99, 100], hierarchies of semidefinite relaxations, based on Lasserre's relaxations, are presented. If $f^\star$ is reached, these relaxations converge to $f^\star$ in a finite number of steps.

Problems (B) and (C) are quantifier elimination problems over the reals. They can be solved by the cylindrical algebraic decomposition [22, 31, 32, 33, 67, 94]. However, its complexity is doubly exponential in the number of variables. Practically, it can not deal

with non-trivial problems of more than 4 variables. In [68], an algorithm for a variant of quantifier elimination is presented. It requires extra conditions on the inputs. These conditions are naturally satisfied in many real-life applications. Likewise, the output is almost equivalent to the input formula, this is sufficient for many applications. It allows to solve problems unreachable with quantifier elimination solvers.

A quantifier elimination algorithm designed to solve problems (B) and (C) whose complexity is $D^{O(n)}$ for n-variate polynomials of degree at most D is presented in [16, Section 14.2]. However, the constant in the exponent of the complexity is not known. The only known algorithm whose complexity is singly exponential and well-controlled to solve problem (B), namely $O\left(n^7 D^{4n}\right)$, is given in [118]. It deals with the unconstrained case.

In [13], a study of the intrinsic complexity in polynomial optimization is given. It is done with constraints defined by polynomial equations satisfying some assumptions of regularity.

In this thesis, we generalize the gradient variety approach so that $f^\star$ is not assumed to be reached. The introduced constraints and the certificates are simpler and with smaller degree than [141].

We generalize [118] to solve problems (B) and (C) in the constrained case. We design a dedicated algorithm whose complexity is essentially $(sD)^{3n}$. Its implementation reflects its complexity.

Methodology

We transform efficiently the previous problems to equivalent problems of small dimension. To this end, we construct geometric objects defined as critical loci of linear projections. These objects are close to the polar varieties. Polar varieties have been introduced by Severi [132, 133] and Todd [139, 140] at the beginning of the century. Then, they have been studied in the context of computer algebra by Bank, Giusti, Heintz, Mbakop and Pardo (see e.g. [9, 11, 12]).

We prove that the union of our geometric objects is the union of the critical locus of f and a variety of dimension 1, on which the infimum of f is $f^\star$. Hence, problems (A), (B) and (C) can be considered these new varieties, whose dimension is essentially 1.

In order to solve problem (A), we follow the approach introduced in [101]. To this end, we use the fact that the dimension of our varieties is essentially 1. We are then able to prove that the set of values of f at infinity on our varieties is finite and use results from [130]. Hence, we prove the existence of certificates without assuming that $f^\star$ is reached.

To solve problem (B) we take into account asymptotic phenomena. To compute the set of potential values of $f^\star$, a set of values of f at infinity is computed. Since we can work on a set whose dimension is essentially 1, they can be computed by seeing them as a set of non-properness (see [70, 120]).

Problem (C) can be solved by computing a finite set meeting each connected component of the critical locus of f. We prove that such a set can be obtained from our geometric objects.

Main Results

Modified Polar Varieties

Solving problems (A), (B) and (C) is easier on a variety of small dimension. We present tools to construct a variety that is the union of the critical locus of f and an algebraic set of dimension 1. Furthermore, the infimum on $V \cap \mathbb{R}^n$ and on this new variety are the same.

Let $f \in \mathbb{Q}[\mathbf{X}]$ and let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ such that the ideal $\langle \mathbf{F} \rangle$ is radical and the variety $V = \mathbb{V}(\mathbf{F})$ is d-equidimensional with finitely many singular points.

We define the modified polar varieties as follows: for $1 \leq i \leq d-1$, let $\mathscr{C}(f, \mathbf{F}, i)$ be the algebraic variety defined by

- $f_1 = \cdots = f_s = 0$,
- the vanishing of all minors of size $n - d + 1$ of the Jacobian matrix of $f, f_1, \ldots, f_s$ with respect to the variables $X_{i+1}, \ldots, X_n$,
- and $X_1 = \cdots = X_{i-1} = 0$.

By convention, $\mathscr{C}(f, \mathbf{F}, d) = V \cap \mathbb{V}(X_1, \ldots, X_{d-1})$. Let $\mathscr{C}(f, \mathbf{F})$ be the union

$$\mathscr{C}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{C}(f, \mathbf{F}, i).$$

In the sequel, given $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, we denote by $f^{\mathbf{A}}$ the polynomial $f(\mathbf{AX})$. Likewise, let $\mathbf{F}^{\mathbf{A}} = \left\{f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}\right\}$ and $V^{\mathbf{A}} = \mathbb{V}\left(\mathbf{F}^{\mathbf{A}}\right)$.

Main Result 1. *There exists a non-empty Zariski-open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$,*

- $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x) = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$,
- $\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}}$ *has dimension at most* 1,
- $\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, F^{\mathbf{A}}\right)$ *has dimension at most* 0 *and contains, for each critical value of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$* that is not isolated *in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, at least one corresponding critical point.*

Furthermore, for $1 \leq i \leq d$, the algebraic varieties $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ and

$$\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$$

have degree bounded by

$$D\left((n - d + 1)(D - 1)\right)^n.$$

From this result, the optimization problems (A), (B) and (C) can be solved on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ instead of the original variety $V \cap \mathbb{R}^n$. Because of this reduction of dimension, the asymptotic phenomena are better controlled. More precisely, since $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension 1, f has finitely many asymptotic values on this set. Thanks to Sard's theorem, f has finitely many value on $\mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$. Finally, this means that f has finitely many asymptotic values on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$.

Exact Algorithm for Global Polynomial Optimization

The second main result is an algorithm solving problems (B) and (C) and an implementation of the algorithm. It is based on symbolic computation. A real algebraic number α is represented by a polynomial $P \in \mathbb{Q}[T]$ and an isolating interval I. This means that P has only one root in I, that is α. Let Y be a real finite variety. It can be represented by a rational parametrization. This is a sequence of polynomials $q, q_0, q_1, \ldots, q_n \in \mathbb{Q}[U]$ such that for each $x = (x_1, \ldots, x_n) \in Y$, there is a unique $u \in \mathbb{R}$ such that

$$\begin{cases} q(u) &= 0 \\ x_1 &= q_1(u)/q_0(u) \\ &\vdots \\ x_n &= q_n(u)/q_0(u) \end{cases}$$

In other words, there is a bijection between the roots of q and the points in Y. Thus, a single point in $x \in Y$ can be represented by $q, q_0, q_1, \ldots, q_n$ and an interval isolating the root of q corresponding with x.

Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ and $f \in \mathbb{Q}[\mathbf{X}]$. Assume that

- the ideal $\langle \mathbf{F} \rangle$ is radical,
- $\mathbb{V}(\mathbf{F})$ is equidimensional of dimension $d > 0$,
- $\mathbb{V}(\mathbf{F})$ has finitely many singular points.

Note that these assumptions are far from being restrictive since they often hold in practice. For instance, any set of polynomials $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ whose Jacobian matrix has full rank satisfies them.

We design an exact probabilistic algorithm taking as input f and $\mathbf{F}$ satisfying the above assumptions and that returns

- $-\infty$ if f is not bounded from below,
- $+\infty$ if $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is empty,
- an algebraic representation of $f^\star = \inf_{x \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n} f(x)$ if $f^\star$ is finite,
- if and only if $f^\star$ is reached, an algebraic representation of a point $x^\star \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ such that $f(x^\star) = f^\star$.

The algorithm solves problems (B) and (C). It exploits properties that are satisfied up to a generic change of coordinates. Practically, a random change of coordinates is chosen. However, we provide some routines to test if it is suitable, which removes the probabilistic aspect.

The implementation is available as a Maple library. It can be downloaded at `http://www-polsys.lip6.fr/~greuet/`. With this implementation, we are able to solve problems unreachable with other algorithms. For instance, it solved random problems in 7 variables in several hours and problems coming from applications in 10 variables in less than a minute. Furthermore, problems that seem difficult with numerical approaches are solved efficiently too. Others implementations solving problems (B) and (C) are based on the cylindrical algebraic decomposition. Practically, they can not deal with problems of more than 4 variables.

To illustrate its theoretical efficiency, we state the main result in a simpler case, that is a bit more restrictive than the general case. We use the soft-O notation: $\widetilde{O}(a)$ indicates the omission of polylogarithmic factors in a.

Main Result 2. *There exists a probabilistic algorithm taking as input*

- $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ *that generates a radical ideal of dimension* $n - s$ *such that the Jacobian matrix associated with* $f_1, \ldots, f_s$ *has rank* s,
- $f \in \mathbb{Q}[\mathbf{X}]$,

and that returns $-\infty$ *if* f *is not bounded from below,* $+\infty$ *if* $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ *is empty, an algebraic representation of* $f^\star = \inf_{x \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n} f(x)$ *if it is finite. If* $f^\star$ *is reached, it also returns an algebraic representation of* $x^\star \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ *such that* $f(x^\star) = f^\star$. *Moreover, assume that the input polynomials have degree bounded by* D *and are represented by a straight-line program of length* $\leq L$. *Then the algorithm performs*

$$\widetilde{O}\left(LD^6\left(\sqrt[3]{2}\,(s+1)\,(D-1)\right)^{3n}\right)$$

arithmetic operations in $\mathbb{Q}$.

Our algorithm follows a classical pattern. It first performs a change of coordinates to ensure some technical assumptions that are satisfied in general position. Then, roughly speaking, it computes a finite set of real points containing $f^\star$. Moreover, for any interval between two consecutive real points in this set is either contained in $f(\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n)$ or has an empty intersection with $f(\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n)$. The computation and the properties of these sets rely on the modified polar varieties.

Algebraic Certificates of Positivity

The third main result is about solving problem (A). It is done by reducing the problem to the problem of finding certificates on the union of the modified polar varieties.

Let I by an ideal of $\mathbb{R}[\mathbf{X}]$, $f \in \mathbb{R}[\mathbf{X}]$ and $f_I^\star = \inf_{x \in \mathbb{V}(I) \cap \mathbb{R}^n} f(x)$. Using semidefinite programming, one can compute successive lower bounds on the number f_I^{sos} defined as

$$f_I^{\mathsf{sos}} = \sup \left\{ a \in \mathbb{R} \,|\, \exists \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2, f - a = \sigma_0 + \sigma_1 (B - f) \mod \langle I \rangle \right\},$$

where $B \in f(\mathbb{V}(I) \cap \mathbb{R}^n)$. In general, $f_I^{\mathsf{sos}} \leq f_I^\star$ but $f_I^{\mathsf{sos}} \neq f_I^\star$. However, assume that on $\mathbb{V}(I)$, any positive polynomial can be written $\sigma_0 + \sigma_1 (B - f) \mod \langle I \rangle$, where σ_0 and σ_1 are sums of squares of polynomials in $\mathbb{R}[\mathbf{X}]$. Since for any $\varepsilon > 0$, $f - f^\star + \varepsilon > 0$, f_I^{sos} is actually equal to $f_I^\star$. Hence, one can focus on proving the existence of such a sum of squares identity for positive polynomials.

Let $f \in \mathbb{Q}[\mathbf{X}]$ and let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ such that the ideal $\langle \mathbf{F} \rangle$ is radical and the variety $V = \mathbb{V}(\mathbf{F})$ is d-equidimensional with finitely many singular points. Let $\mathscr{C}(f, \mathbf{F})$ be the union of our modified polar varieties. We prove that the original optimization problem can be reduced to the optimization problem on $\mathscr{C}(f, \mathbf{F})$ and that there exist certificates of positivity on $\mathscr{C}(f, \mathbf{F})$ by means of sum of squares.

Main Result 3. *There exists a non-empty Zariski-open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, $f^{\mathbf{A}} \geq 0$ on $V \cap \mathbb{R}^n$ if and only if for all $\varepsilon > 0$, there exist a sum of squares of real polynomials $S^{\mathbf{A}}$ and $T^{\mathbf{A}}$ such that, for any $B \in f(V \cap \mathbb{R}^n)$,*

$$f^{\mathbf{A}} + \varepsilon = S^{\mathbf{A}} + T^{\mathbf{A}} \left(B - f^{\mathbf{A}}\right) \mod \mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right).$$

Assume that $\mathbf{A} \in \mathscr{O} \cap \mathrm{GL}_n(\mathbb{Q})$. Note that it is true if $\mathbf{A}$ is generic enough, *e.g.* randomly chosen. Using semidefinite programming, this leads to the computation of a sequence of lower bounds on $f^\star$. This sequence is monotonically increasing and tends to $f^\star$. Remark that in this statement, $V \cap \mathbb{R}^n$ is not assumed to be compact.

Conclusion

In this thesis, we adapt the definition of the classical polar varieties in order to deal with the optimization problem. This leads to considering the modified polar varieties. By studying their geometric properties, we prove that the optimization problem can be reduced to a new optimization problem on a variety of smaller dimension. It allows to take into account asymptotic phenomena in the optimization problem. We use these properties to solve the optimization problem in two ways.

First, we deduce an exact algorithm solving the optimization problem. It can compute an algebraic representation of the infimum of a polynomial on an algebraic variety under some assumptions of regularity. Moreover, it can decide whether this infimum is reached or not. If so, an algebraic representation of a minimizer is also returned. Its correctness and its complexity rely on the properties of the modified polar varieties. We prove that it is singly exponential in the number of variables. A major part of this work consists of an efficient implementation of this algorithm. It is available as a Maple library, downloaded from `http://www-polsys.lip6.fr/~greuet/` and can be used free of charge. Experiments on random inputs and toy examples show that it is practically

efficient, even for problem hard to solve using numerical approaches or for problem with huge coefficients, substantial degree or substantial number of variables. As far as we know, this is the first exact dedicated algorithm solving the optimization problem in the constrained case.

The second application is the existence of algebraic certificates of positivity. We prove that a positive polynomial f on an algebraic variety admits a sum of squares representation on its associated modified polar varieties. Such a representation can be numerically approximated using semidefinite programming. Then, we expect that a rational identity can be recovered from the numerical one. We do not require that the given variety is compact or that the infimum of f is reached.

Perspectives

We first focus on problems for which the properties of the modified polar varieties should be used. Sharp bounds on the value and the degree of the infimum should be obtained by using the modified polar varieties, even if $f^\star$ is not reached. Likewise, the existence of rational certificates of positivity should be obtained on the modified polar varieties. When $f^\star$ is reached, the computation of such certificates should be done by reducing the problem to the univariate case.

Then we are interested in the computation of asymptotic critical values. This should be useful to improve the algorithmic resolution of problem (B) and (C).

Finally, we discuss the resolution of problems (B) and (C) with constraints defined by polynomial inequalities.

Bounds and Degree of the Infimum

Consider the infimum of a polynomial with rational coefficients on a semi-algebraic set defined by inequalities of polynomials with rational coefficients. Under the assumption that it is reached, bounds on its degree and on its absolute value are given in [73]. These bounds are sharp. They can be computed from the degrees and the coefficients of the involved polynomials.

It is straightforward that a lower bound on the absolute value of the infimum gives information for the optimization problems (A), (B) and (C). Likewise, an upper bound on its degree should allow to obtain useful information about the degree of the polynomials involved in a sum of squares representation.

In this context, our goal would be to get analogous bounds when the infimum is not supposed to be reached. This could be done by reducing the problem on the modified polar varieties.

Rational Sum of Squares and Computation

In Chapter 7, we prove the existence of certificates of positivity by means of sum of squares on an algebraic variety. Our input polynomials have rational coefficients whereas the result gives the existence of sum of squares with real coefficients.

It would be interesting to obtain the existence of rational certificates. Such results have been proved in the unconstrained case [64] and on the constrained case, when the semi-algebraic set defined by the constraints is compact [107]. To deal with a more general case, without the assumption of compactness, one can try to adapt the results of real algebra in [129, 130] to the rational case. Then, they can be used to prove the existence of rational certificates on the modified polar varieties.

To compute rational certificates, rationalizing a numerical certificate obtained by semidefinite programming can be done [75, 105]. However, since it relies on numerical solvers, numerical instabilities can occur. From the results in [55], one can decide whether a polynomial with rational coefficient has a rational sum of squares representation. For the optimization problem (A), we can expect to be able to compute rational certificates for lower bounds on $f^\star$.

Assume that the critical locus of f is 0-dimensional and $f^\star$ is reached. Using a rational parametrization, a rational sum of squares representation on the gradient variety [101] can be transformed into a univariate sum of squares identity. Hence, the algorithm from [128] can compute such a rational certificate.

If the gradient variety is not 0-dimensional, the modified polar varieties should be used to get an equivalent problem on a 0-dimensional variety.

Computation of Asymptotic Critical Values

The set of generalized critical values is the union of classical critical values and their analogous at infinity, the asymptotic critical values (see [71, 72, 80]). It is a fundamental mathematical notion, that appears naturally in optimization. Indeed, in [118], it is proved that the infimum of a polynomial over $\mathbb{R}^n$ is necessarily a generalized critical value. This result is based on topological properties of the generalized critical values given in [80]. These topological properties still hold in the constrained case, thus the result should be generalized to the constrained case. Hence, it would be interesting to be able to compute efficiently these values.

The computation of a set containing the classical critical values can be done using Gröbner bases. However, computing the asymptotic critical values is not straightforward. In [118], the author deals with the unconstrained case. To this end, the computation of the asymptotic critical values is reduced to the computation of the set of non-properness of a projection restricted to a curve. To ensure an assumption of Noether position, a generic change of variables is performed. It is then computable using Gröbner bases, but the change of variable can make the computations harder.

A view of this problem through the projective space could lead us to get information at infinity. In particular, one expects to be able to replace the Noether position assumption with a test of dimension, that is much faster in practice.

Exact Algorithm on Semi-Algebraic Sets

The exact algorithm presented in Chapter 6 solves the optimization problems (B) and (C) with constraints that define an algebraic variety. For some applications, it is necessary to

be able to deal with semi-algebraic sets. A first step would be the generalization of our approach to semi-algebraic sets defined by equations and non-strict inequalities. In our algorithm, we can actually get the values of all extrema. Thus, adapting it to the semi-algebraic case where the infimum is reached should be straightforward. Nevertheless, since our goal is still to provide a general algorithm, we want to avoid the assumption that the infimum is reached. To this end, the goal would be to be able to compute the values attained by a polynomial "at infinity" on a semi-algebraic set.

Organization of the Thesis

In Chapter 1, we recall some notions of algebraic and semi-algebraic geometry. In particular, we recall algorithms to compute algebraic representations of geometric objects such as union, intersection, difference, projection of algebraic varieties, using Gröbner bases in Section 1.2. Likewise, we present a method to test the Noether position using Gröbner bases. We also mention tools used to estimate the complexity of these geometric operations in Section 1.3. Then we introduce quantifier elimination over the reals and its connection with global optimization. Then, we present a state of the art of the techniques coming from computational real algebraic geometry that can be used to solve symbolically the optimization problems (B) and (C).

In Chapter 3, we first present the context of real algebra and the historical results about certificates of positivity. Then we show that the problem of finding such a certificate can be relaxed to a semidefinite program. Thus if the existence of certificates is ensured then accurate lower bounds for the infimum can be computed numerically. Finally, we present a state of the art of the recent result about the existence of certificates.

Chapter 4 is devoted to introduce the (classical) polar varieties. Given an algebraic variety, these objects are defined as critical loci of some projection restricted to the given variety. This leads to the computation of varieties of smaller dimension. From these varieties, a finite set of points that meets each connected component of the real trace of the given variety can be computed. It will be used in our algorithms to compute some critical points and to test the emptiness of real varieties.

In the second part of the thesis, we present our contributions. Most parts of the contribution are published or submitted, but our presentation does not follow the chronology of the publications. Indeed, some results are generalization of some previous works, so that the old result becomes a particular instance of the new one.

In Chapter 5, we define and study the properties of the modified polar varieties. This is a synthesis of some of our results coming from [53] and [52].

Chapter 6 is devoted to present an exact algorithm solving problems (B) and (C). It can compute the infimum of a polynomial under constraints defining a regular algebraic variety and decide whether it is reached or not. This algorithm has been implemented and is available as a Maple package at `http://www-polsys.lip6.fr/~greuet/`. This implementation can solve instances of global optimization problems that were not tractable with previous algebraic algorithms. This work can be found in [52] and contains the one given in [51].

Finally, in Chapter 7, we show how the modified polar varieties can be used to obtain the existence of certificates of positivity, be means of sum of squares. This work has been published in [53].

Part I

Prerequisites

Chapter 1

Algebraic and Semi-Algebraic Geometry

In this chapter, we introduce notions and properties of algebraic and semi-algebraic geometry. Basic definitions and notations are given in Section 1.1. Then we present in Section 1.2 the Gröbner bases and explain how to use them to perform geometric operations like computing the intersection, the union, the difference of two varieties or the projection of an algebraic variety (about the projection, see [37, Chapter 4]). We also show how to check whether an ideal is in Noether position (a notion described in [7, Chapter 5]). Gröbner bases can also be used to compute a rational parametrization of a finite algebraic set of points in $\mathbb{R}^n$ [115]. Likewise, the geometric resolution algorithm is presented in Section 1.3. It is a probabilistic algorithm that can perform the above geometric operations [43, 50, 91, 126]. Furthermore, it provides a complexity estimate that will be useful for our complexity analyses. Finally, we introduce the definitions of infinitesimals and Puiseux series in Section 1.4. They will be used to consider deformations of an algebraic variety.

1.1 Definitions and Notations

This section is devoted to introduce algebraic varieties, the Zariski-topology and the connection between polynomial ideals and algebraic varieties. These definitions and properties will be used throughout this thesis. Without more precision, $f_1, \ldots, f_s$ are polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ and $\mathbf{F}$ is the set of polynomials $\{f_1, \ldots, f_s\}$.

Basic definitions. For simplicity, $\mathbf{X}$ is the set of indeterminates $\{X_1, \ldots, X_n\}$, $\mathbf{X}_{\leq i}$ the set $\{X_1, \ldots, X_i\}$ and $\mathbf{X}_{>i} = \{X_{i+1}, \ldots, X_n\}$. An ideal I is a subset of $\mathbb{Q}[\mathbf{X}]$ such that

- $0 \in I$;
- if $f \in I$, $g \in I$ then $f + g \in I$;

- if $f \in I$, $g \in \mathbb{Q}[\mathbf{X}]$ then $gf \in I$.

Let $S \subset \mathbb{Q}[\mathbf{X}]$. Then $\langle S \rangle$ stands for the ideal generated by S, that is the smallest ideal containing S.

An algebraic variety is the complex solution set of a set of polynomial equations. Given $S \subset \mathbb{Q}[\mathbf{X}]$, we can define the algebraic variety $\mathbb{V}(S)$ as the set of common zeros in $\mathbb{C}^n$ of the polynomial equations in S in indeterminates $X_1, \ldots, X_n$. More precisely,

$$\mathbb{V}(S) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \,|\, \forall f \in S,\, f(x_1, \ldots, x_n) = 0\}.$$

Given a variety V, we denote by

$$\mathbb{I}(V) = \{f \in \mathbb{C}[\mathbf{X}] \,|\, \forall (x_1, \ldots, \mathbf{x}_n) \in V,\, f(x_1, \ldots, \mathbf{x}_n) = 0\}.$$

It is an ideal and it is called the ideal of the variety V. An algebraic variety V is *reducible* if it can be written as the union of two proper algebraic varieties, *irreducible* else. For any algebraic variety V, there exist irreducible varieties $V_1, \ldots, V_s$ such that for $i \neq j$, $V_i \not\subset V_j$ and such that $V = V_1 \cup \cdots \cup V_s$. The algebraic varieties V_i are the irreducible components of V. The decomposition of V as the union of its irreducible components is unique.

Proposition-Definition 1.1 (Zariski topology)**.** *A topology can be defined on $\mathbb{C}^n$ specifying that its closed sets are the algebraic varieties. This topology is called the* Zariski topology .

In the sequel we show the connection between an ideal and the ideal associated with its associated variety. Let I be an ideal of $\mathbb{Q}[\mathbf{X}]$. The radical of I is defined as

$$\sqrt{I} = \left\{f \in \mathbb{Q}[\mathbf{X}] \,|\, \exists N \in \mathbb{N}^*,\, f^N \in I\right\}.$$

It is easy to show that the radical of an ideal is an ideal itself.

Theorem 1.2. *[83, Chapter 9, §1, Theorem 1.5 p. 380] Let k be a field and let K be an algebraic closure of k. Let I be an ideal in $k[\mathbf{X}]$. Let f be a polynomial in $k[\mathbf{X}]$ such that $f(c) = 0$ for all $c \in \{x \in K^n \,|\, \forall g \in I,\, g(x) = 0\}$. Then there exists an integer $m > 0$ such that $f^m \in I$.*

In particular, if $f_1, \ldots, f_s \in \mathbb{Q}[\mathbf{X}]$ then $\mathbb{I}(\mathbb{V}(f_1, \ldots, f_s)) \cap \mathbb{Q}[\mathbf{X}] = \sqrt{\langle f_1, \ldots, f_s \rangle}$.

Given an arbitrary set $A \subset \mathbb{C}^n$, the *Zariski-closure* of A is the smallest algebraic variety containing A. It will be denoted by $\overline{A}^{\mathcal{Z}}$. The following lemma gives information about the closure of a union and will be helpful in the sequel.

Lemma 1.3. *Let A and B be two subset of $\mathbb{C}^n$. Then $\overline{A \cup B}^{\mathcal{Z}} = \overline{A}^{\mathcal{Z}} \cup \overline{B}^{\mathcal{Z}}$.*

Proof. Since $A \subset \overline{A}^{\mathcal{Z}}$ and $B \subset \overline{B}^{\mathcal{Z}}$, $\overline{A}^{\mathcal{Z}} \cup \overline{B}^{\mathcal{Z}}$ is a closed set (as a union of two closed sets) containing $A \cup B$. By definition, $\overline{A \cup B}^{\mathcal{Z}}$ is the smallest closed set containing $A \cup B$. In particular, this implies that $\overline{A \cup B}^{\mathcal{Z}} \subset \overline{A}^{\mathcal{Z}} \cup \overline{B}^{\mathcal{Z}}$.

Conversely, let $x \in \overline{A}^{\mathcal{Z}} \cup \overline{B}^{\mathcal{Z}}$. Then either $x \in \overline{A}^{\mathcal{Z}}$ or $x \in \overline{B}^{\mathcal{Z}}$. In the first case, every neighbourhood of x meets A, thus it also meets $A \cup B$ then x lies in the closure of $A \cup B$. Likewise if $x \in \overline{B}^{\mathcal{Z}}$, every neighbourhood of x meets $B \subset A \cup B$ meaning that $x \in \overline{A \cup B}^{\mathcal{Z}}$. Finally, $\overline{A}^{\mathcal{Z}} \cup \overline{B}^{\mathcal{Z}} \subset \overline{A \cup B}^{\mathcal{Z}}$ □

1.2 Gröbner Bases

We present a short introduction (and refer to [37] for further details) of the notion of Gröbner basis, that is a "good" representation of a polynomial ideal. We will see that Gröbner bases allow to

- test whether a set of polynomial define an empty complex variety;
- compute the intersection, the union and the Zariski-closure of the difference of two varieties;
- compute the Zariski-closure of the projection of a variety to a linear subspace;
- test whether a variety is in Noether position;
- compute an exact representation of a finite algebraic set.

In order to define a Gröbner basis, we first fix an order on the monomials. A monomial ordering $\succ$ is a total ordering on the set of monomials compatible with the multiplication ($\alpha \succ \beta \Rightarrow \alpha\gamma \succ \beta\gamma$) and for which there is no strictly decreasing sequence. Given $f \in \mathbb{Q}[\mathbf{X}]$, $\mathrm{LT}(f)$ stands for the greatest monomial term in f with respect to $\succ$ and $\mathrm{LC}(f)$ the coefficient of $\mathrm{LT}(f)$.

Let $I \subset \mathbb{Q}[\mathbf{X}]$ be an ideal and denote by $\langle \mathrm{LT}(I) \rangle$ the ideal generated by $\mathrm{LT}(f)$ for all $f \in I$. A finite subset $\{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if $I = \langle g_1, \ldots, g_t \rangle$ and $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.

Proposition-Definition 1.4. *Let $I \subset \mathbb{Q}[\mathbf{X}]$ be an ideal. Then I has a unique* reduced *Gröbner basis, that is a basis G such that for all $g \in G$, $LC(g) = 1$ and no monomial of g lies in $\langle LT(G \setminus \{g\}) \rangle$.*

Note that there exist algorithms to compute Gröbner bases (see e.g. [26] for the historical Buchberger algorithm, [46], [47] for Faugère's F4 and F5 algorithms). Implementations of Faugère's algorithms are available in computer algebra systems, or as a standalone library at `http://www-polsys.lip6.fr/~jcf/Software/`.

In the sequel, let $V = \mathbb{V}(f_1, \ldots, f_s)$ and $W = \mathbb{V}(g_1, \ldots, g_p)$, where all polynomials f_i and g_j are in $\mathbb{Q}[\mathbf{X}]$. Denote by I_V the ideal $\langle f_1, \ldots, f_s \rangle$ and by I_W the ideal $\langle g_1, \ldots, g_p \rangle$.

Testing the emptiness.

Hilbert's weak Nullstellensatz (see [37, Chapter 4, §1, Theorem 1, p. 170]) gives a theoretical answer to decide the emptiness of a complex algebraic variety.

Theorem 1.5 (Hilbert's Weak Nullstellensatz)**.** *Let k be a field and let K be an algebraic closure of k. Let I be an ideal in $k[\mathbf{X}]$. Then $\{x \in K^n \mid \forall g \in I,\, g(x) = 0\} = \varnothing$ if and only if $I = \langle 1 \rangle$.*

Then testing the emptiness of $\mathbb{V}(I)$ is equivalent to test whether $I = \langle 1 \rangle$. That can be achieved using Gröbner bases. Indeed, it is easy to verify that $\{1\}$ is a reduced Gröbner basis of the ideal $\langle 1 \rangle$. Then a consequence of Proposition-Definition 1.4 and Theorem 1.5 is the following.

Proposition 1.6 (Testing the (complex) emptiness)**.** *Let $f_1, \ldots, f_p \subset \mathbb{Q}[\mathbf{X}]$ and G be a reduced Gröbner basis of $\langle f_1, \ldots, f_p \rangle$. Then $\mathbb{V}(f_1, \ldots, f_p) = \varnothing$ if and only if $G = \{1\}$.*

Geometric Operations.

In this section, we show how to perform some basic geometric operations on varieties represented by a set of polynomials. The first one allows to compute a set of polynomials that define the intersection of two varieties that are given by sets of polynomials.

Proposition 1.7. *[37, Chapter 4, §3, Theorem 4, p.184] The variety defined by*

$$I_V + I_W = \langle f_1, \ldots, f_s, g_1, \ldots, g_p \rangle$$

is the variety $V \cap W$.

Then we are interested in the computation of the union of two varieties.

Proposition 1.8. *[37, Chapter 4, §3, Theorem 7, p.185] The variety defined by*

$$I_V.I_W = \langle f_i g_j,\ 1 \leq i \leq s,\ 1 \leq j \leq p \rangle$$

is the variety $V \cup W$.

The projection of an algebraic variety is not necessarily an algebraic variety. However, an ideal defining its Zariski-closure can be computed.

Proposition 1.9. *[37, Chapter 3, §2, Theorem 3, p.125] The variety V_{elim} defined by*

$$I_{elim} = I_V \cap \mathbb{Q}[X_{\ell+1}, \ldots, X_n]$$

is the Zariski-closure $\overline{\pi_{>\ell}(V)}^{\mathcal{Z}}$ of the projection of V to $X_{\ell+1}, \ldots, X_n$.

Since we are now able to characterize the ideal of the Zariski-closure of a projection, we are interested in computing generators of this ideal. This can be done using Gröbner bases with an elimination order. A monomial order on $\mathbb{Q}[\mathbf{X}]$ such that any monomial involving one of the indeterminates $x_1, \ldots, x_\ell$ is greater than any monomial in $\mathbb{Q}[x_{\ell+1}, \ldots, x_n]$ is called an order eliminating $\{x_1, \ldots, x_\ell\}$.

Proposition 1.10. *[37, Chapter 3, §1, Theorem 2, p.116] Let G be a Gröbner basis of I_V with respect to an order eliminating $\{x_1, \ldots, x_\ell\}$. Then $G_{elim} = G \cap \mathbb{Q}[X_{\ell+1}, \ldots, X_n]$ is a Gröbner basis of the ideal $I_{elim} = I_V \cap \mathbb{Q}[X_{\ell+1}, \ldots, X_n]$.*

Practically, the elimination ordering used is the block grevlex order. The grevlex order compares the total degree first, then compares exponents of the last indeterminate X_n but reversing the outcome (so the monomial with smaller exponent is larger in the ordering), followed (as always only in case of a tie) by a similar comparison of X_{n-1}, and so forth ending with x_1. For the block grevlex order, indeterminates are splitted into two blocks, $[x_1, \ldots, x_\ell]$ and $[x_{\ell+1}, \ldots, x_n]$. Monomials are first compared with respect to the grevlex ordering on the first block. In case of a tie, they are compared with respect to the grevlex ordering on the second block.

Like the image of a projection, the difference of two varieties is not necessarily a variety. Nevertheless, its Zariski-closure can be seen as the one of a projection. Hence, its computation can be done by elimination. We first present the case of the difference by a hypersurface. Since any algebraic variety is the intersection of finitely many hypersurfaces, the general case is obtained by induction.

Proposition 1.11. *[37, Chapter 4, §4, Exercice 9, p. 195] Let $g \in \mathbb{Q}[\mathbf{X}]$ and L be a new indeterminate. Then the variety defined by the ideal*

$$I_{elim} = (I_V + \langle L \times g - 1 \rangle) \cap \mathbb{Q}[\mathbf{X}]$$

is the variety $\overline{V \setminus \mathbb{V}(g)}^{\mathcal{Z}}$.

Assume now that I_W is given by an arbitrary finite number of generators. In order to compute the difference of a variety by the one defined by I_W, we use the fact that if W_1, W_2 are any varieties then

$$\begin{aligned} V \setminus (W_1 \cap W_2) &= V \cap {}^c(W_1 \cap W_2) \\ &= V \cap ({}^cW_1 \cup {}^cW_2) \\ &= (V \cap {}^cW_1) \cup (V \cap {}^cW_2) \\ &= (V \setminus W_1) \cup (V \setminus W_2) \end{aligned}$$

Then considering the Zariski-closure and using Lemma 1.3, we obtain

$$\overline{V \setminus (W_1 \cap W_2)}^{\mathcal{Z}} = \overline{(V \setminus W_1)}^{\mathcal{Z}} \cup \overline{(V \setminus W_2)}^{\mathcal{Z}}.$$

Test for the Noether position.

We first introduce the basic notions to define the Noether position of an ideal. Recall that a map $f\colon V \subset \mathbb{C}^n \to \mathbb{C}^i$ is proper at $y \in \mathbb{C}^i$ if there exists a closed neighborhood $\mathcal{U}$ of y such that $f^{-1}(\mathcal{U})$ is compact.

We will see that the notion Noether position is strongly related to the notion of properness of projections to linear subspaces. In our algorithms, the Noether position of ideals is sometimes required. Hence, is is fundamental to be able to test it. For a complete introduction to the algebraic notions related to the Noether position see [7, Chapter 5]. For an effective point of view of the Noether position, see [42, Section 2.2].

Noether position and properness. Let R be a ring and $A \subset R$ be a subring of R. An element $x \in R$ is integral over A if it is a root of a monic polynomial with coefficients in A. The ring R is an integral extension of A if every element $x \in R$ is integral over A.

The dimension of $V = \mathbb{V}(f_1, \ldots, f_s)$ is the Krull dimension of its coordinate ring, that is the maximal length of the chains $p_0 \subset p_1 \subset \cdots \subset p_d$ of prime ideals of the quotient ring $\mathbb{C}[\mathbf{X}] / \langle f_1, \ldots, f_s \rangle$ (see [44, Chapter 8]). We write $\dim V = d$. The variety is *equidimensional* of dimension d if its irreducible components have dimension d.

An ideal $I \subset \mathbb{C}[X_1, \ldots, X_n]$ such that $\mathbb{V}(I)$ has dimension d is in Noether position if the ring extension $\mathbb{C}[X_1, \ldots, X_d] \longrightarrow \mathbb{C}[X_1, \ldots, X_n] / I$ is integral.

Example 1.12. *Let $I = \langle X_1^2 - X_2 \rangle \subset \mathbb{C}[X_1, X_2]$. It has dimension 1 and X_2 is integral over $\mathbb{C}[X_1, X_2] / I$: it is a root of the monic polynomial $T - X_1^2 \in \mathbb{C}[X_1]$ modulo I. Then I is in Noether position.*

Let $J = \langle X_1 X_2 - 1 \rangle \subset \mathbb{C}[X_1, X_2]$, of dimension 1. It is not in Noether position since X_2 is not integral over $\mathbb{C}[X_1, X_2] / J$. Indeed, it is a root of $X_1 T - 1 \in \mathbb{C}[X_1]$ modulo I, meaning that it can not be the root of a monic polynomial in $\mathbb{C}[X_1]$.

Remark 1.13. *Assume that f is a polynomial mapping and let $y \in \mathbb{C}^i$ be a point at which f is not proper. This means that for all neighborhood $\mathcal{O}$ of y, the preimage $f^{-1}(\overline{\mathcal{O}})$ is not bounded. In particular, one can construct, by induction, a sequence $(x_k)_k$ in V that is not bounded such that $f(x_k) \underset{k \to +\infty}{\longrightarrow} y$.*

Then we exhibit the relationship between Noether position and properness of projections.

Proposition 1.14. *Assume that I_V is such that $V = \mathbb{V}(I_V)$ has dimension d. Then I_V is in Noether position if and only if the projection*

$$\begin{aligned} \pi_{\leq d} : \quad V \subset \mathbb{C}^n &\longrightarrow \mathbb{C}^d \\ (x_1, \ldots, x_n) &\longmapsto (x_1, \ldots, x_d) \end{aligned}$$

is proper.

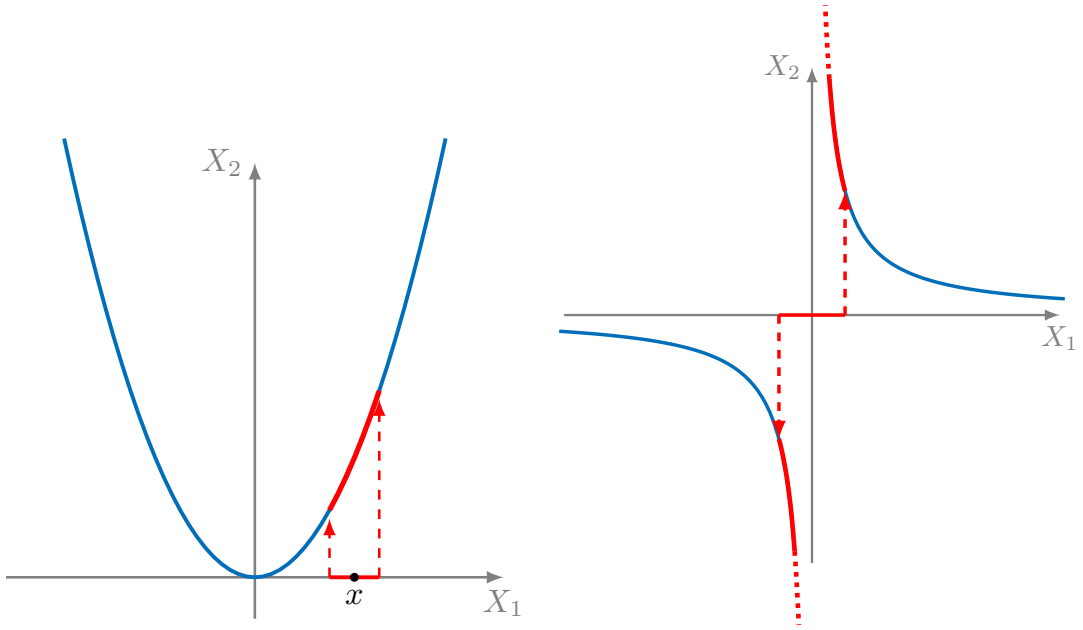
Proof. Let $\pi_{\leq d}$ be the above projection. Denote by $\mathbb{C}[V]$ the coordinate ring of V, that is the quotient ring $\mathbb{C}[X_1, \ldots, X_n] / I_V$. According to [70, Proposition 3.2], $\pi_{\leq d}$ is proper if and only if the map

$$\begin{aligned} (\pi_{\leq d})_* : \mathbb{C}[X_1, \ldots, X_d] &\longrightarrow \mathbb{C}[V] \\ h &\longmapsto h \circ \pi_{\leq d} \end{aligned}$$

is finite, i.e. its fibers are finite. By [70, Proposition 3.2], this is equivalent to say that $(\pi_{\leq d})_* \mathbb{C}[X_1, \ldots, X_d] \subset \mathbb{C}[X_1, \ldots, X_n] / I_V$ is an integral extension. In our case, the map $(\pi_{\leq d})_*$ is the identity. □

Example 1.15. *Let us consider the ideals given in Example 1.12. The ideal $I = \langle X_1^2 - X_2 \rangle \subset \mathbb{C}[X_1, X_2]$ is in Noether position. Geometrically, the associated variety is the parabola in Figure 1.1(a), for which the projection to X_1 is proper.*

The ideal $J = \langle X_1X_2 - 1\rangle \subset \mathbb{C}[X_1, X_2]$ *is not in Noether position. Geometrically, the associated variety is the parabola in Figure 1.1(b), for which the projection to* X_1 *is not proper at* 0.



(a) For all $x \in \mathbb{R}$ and all $\varepsilon > 0$, the preimage of $[x - \varepsilon, x + \varepsilon]$ by the projection to X_1 is compact.

(b) For all $\varepsilon > 0$, the preimage of $[-\varepsilon, \varepsilon]$ by the projection to X_1 contains an unbounded branch of the hyperbola.

Figure 1.1: Polar varieties with properness.

Test for the Properness. According to the previous result, it is sufficient to test the properness of a given projection restricted to the variety. To this end, we will check the existence of points at infinity using homogenization with respect to a block of indeterminates. Given $f \in \mathbb{Q}[\mathbf{X}]$, denote by $\deg_{X_{d+1},\ldots,X_n}(f)$ the degree of f with respect to the indeterminates $X_{d+1}, \ldots, X_n$.

The homogenization of f with respect to the indeterminates $X_{d+1}, \ldots, X_n$ is the polynomial $X_0^{\deg_{X_{d+1},\ldots,X_n}} f\left(X_1, \ldots, X_d, \frac{X_{d+1}}{X_0}, \ldots, \frac{X_n}{X_0}\right)$. Likewise, given an ideal $I \subset \mathbb{Q}[\mathbf{X}]$, the homogenization of I with respect to the indeterminates $X_{d+1}, \ldots, X_n$ is the ideal of $\mathbb{Q}[X_0, X_1, \ldots, X_n]$ of all the polynomials

$$X_0^{\deg_{X_{d+1},\ldots,X_n}} f\left(X_1, \ldots, X_d, \frac{X_{d+1}}{X_0}, \ldots, \frac{X_n}{X_0}\right),$$

for each $f \in I$.

An algorithm to compute the set of non-properness is given in [96, Theorem 1]. In order to test whether a projection is proper, we obtain the following.

Proposition 1.16. *[96, Theorem 1] Let I_V^h be the homogenization of I_V with respect to the set of indeterminates $X_{d+1}, \ldots, X_n$, and $V^h = \mathbb{V}\left(I_V^h\right)$. Then the restriction of $\pi_{\leq d}$ to V is proper if and only if the set*

$$\left(\overline{V^h \setminus \mathbb{V}(X_0)}^{\mathcal{Z}} \cap \mathbb{V}(X_0)\right) \setminus \mathbb{V}(X_{d+1}, \ldots, X_n)$$

is empty.

Representation of finite algebraic varieties.

An objective in this thesis is to design an exact algorithm computing algebraic representations of $f^\star$ and a minimizer $x^\star$, if such a minimizer exists. To this end, finite algebraic sets are represented by a rational parametrization. Such a representation can be computed from a Gröbner basis (see [115]). Let $Y \subset \mathbb{R}^n$ be a finite algebraic set defined by polynomials in $\mathbb{Q}[\mathbf{X}]$. A rational parametrization of Y is a sequence of polynomials $q, q_0, q_1, \ldots, q_n \in \mathbb{Q}[U]$ such that for all $x = (x_1, \ldots, x_n) \in Y$, there exists a unique $u \in \mathbb{R}$ such that

$$\begin{cases} q(u) &= 0 \\ x_1 &= q_1(u)/q_0(u) \\ &\vdots \\ x_n &= q_n(u)/q_0(u) \end{cases}$$

In other words, there is a bijection between the roots of q and the points in Y. Thus, a single point in $x \in Y$ can be represented by $q, q_0, q_1, \ldots, q_n$ and an interval isolating the root of q corresponding with x. Then, box isolating a single point can be computed.

Likewise, an algebraic number $\alpha \in \mathbb{R}$ is represented by a univariate polynomial P and an isolating interval I: P has only one root in I, that is α.

Example 1.17. *Consider the intersection of the circle $x^2 + y^2 = 1$ and the line $y = 2x$. This is the 0-dimensional variety*

$$\mathbb{V}\left(x^2 + y^2 - 1, y - 2x\right) = \left\{\left(\frac{-1}{\sqrt{5}}, \frac{-2}{\sqrt{5}}\right), \left(\frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}}\right)\right\},$$

that can be parametrized by

$$\begin{cases} 5u^2 - 4 &= 0 \\ x &= 2/5u \\ y &= 4/5u \end{cases}$$

The point $\left(\frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}}\right)$ is characterized by the isolating intervals $I_0 = \left[\frac{1}{2}, 1\right]$, $I_1 = \left[\frac{2}{5}, \frac{4}{5}\right]$ and $I_2 = \left[\frac{4}{5}, \frac{8}{5}\right]$. Indeed, the polynomial $5U^2 - 4$ has only one root u in $\left[\frac{1}{2}, 1\right]$. The corresponding point $(2/5u, 4/5u)$ is the only point of $\mathbb{V}\left(x^2 + y^2 - 1, y - 2x\right)$ in the rectangle $I_1 \times I_2$.

Likewise, the point $\left(\frac{-1}{\sqrt{5}}, \frac{-2}{\sqrt{5}}\right)$ *is characterized by the isolating intervals* $I'_0 = \left[-1, -\frac{1}{2}\right]$, $I'_1 = \left[-\frac{4}{5}, -\frac{2}{5}\right]$ *and* $I'_2 = \left[-\frac{8}{5}, -\frac{4}{5}\right]$ *(see Figure 1.2, the upper rectangle being* $I_1 \times I_2$ *and the other one* $I'_1 \times I'_2$*).*

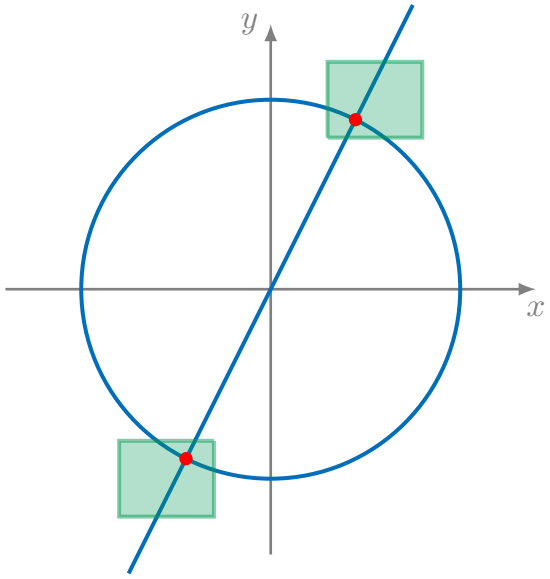


Figure 1.2: Isolation of each point in $\mathbb{V}\left(x^2 + y^2 - 1, y - 2x\right)$.

1.3 Geometric Resolution

The geometric operations presented in Section 1.2 can be performed by the geometric resolution algorithm. This algorithm can be used to compute a parametrization of a finite algebraic set too. The geometric resolution algorithm is a classical routine in polynomial system solving solvers.

Let $C \subset \mathbb{C}^n$ be an irreducible variety. Its geometric degree $\deg C$ is the maximum finite cardinal of $C \cap \mathscr{L}$, for every linear subspace $\mathscr{L} \subset \mathbb{C}^n$. If V is a reducible variety, $\deg V = \sum \deg C$ where the sum is over each irreducible component C of V. The geometric degree of a hypersurface $V(f)$ is bounded by $\deg f$. Given a variety $V = \mathbb{V}(g_1, \ldots, g_p)$, we denote by $\delta(V)$ the maximum of the degrees $\deg(V(g_1, \ldots, g_i))$, for $1 \leq i \leq p$.

The geometric resolution algorithm takes advantage of the representation of polynomials as *straight-line programs*. To perform geometric operations on a variety V, the complexity is essentially cubic in $\delta(V)$. Then it can be used to obtain complexity estimates.

We recall the basic definitions and then recall the complexity results of the subroutines we will use in our complexity estimates. For further details, see [43, 50, 90, 91, 126].

Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$, $g \in \mathbb{Q}[\mathbf{X}]$. Assume that the polynomials f_i and g have degree $\leq D$, that they are given by a straight-line program of size L and $\mathbb{V}(\mathbf{F})$ has dimension d.

In the sequel, a geometric resolution is a representation of a variety by a parametrization. A lifting fiber is a data from which a geometric resolution can be recovered. We refer to [50, 90, 91, 126] for precise statements.

The subroutines required to estimate the complexity of our algorithm are the following.

- GeometricSolveRRS [50]: let $\mathbf{F} = \{f_1, \ldots, f_n\}$ and g as above. Assume that $\mathbf{F}$ defines a reduced regular sequence in the open subset $\{g \neq 0\}$. In case of success, the procedure returns a geometric resolution of $\overline{\mathbb{V}(\mathbf{F}) \setminus \mathbb{V}(g)}^{\mathcal{Z}}$ in time

$$\widetilde{O}\left(\left(nL + n^4\right)\left(D\delta\left(\mathbb{V}(\mathbf{F})\right)\right)^2\right).$$

- GeometricSolve [91]: let $\mathbf{F}$ and g as above. In case of success, the procedure returns an equidimensional decomposition of $\overline{\mathbb{V}(\mathbf{F}) \setminus \mathbb{V}(g)}^{\mathcal{Z}}$, encoded by a set of irreducible lifting fibers in time

$$\widetilde{O}\left(sn^4\left(nL + n^4\right)\left(D\delta\left(\mathbb{V}(\mathbf{F})\right)\right)^3\right).$$

- LiftCurve [91]: given an irreducible lifting fiber F of the above output, in case of success, the routine returns a rational parametrization of the lifted curve of F in time

$$\widetilde{O}\left(sn^4\left(nL + n^4\right)\left(D\delta\left(\mathbb{V}(\mathbf{F})\right)\right)^2\right).$$

- OneDimensionalIntersect [50]: let $\langle \mathbf{F} \rangle$ be a 1-dimensional ideal, $\mathfrak{I}$ be a geometric resolution of $\langle \mathbf{F} \rangle$, and f and g be polynomials. In case of success, the routine returns a rational parametrization of $\overline{\mathbb{V}(\mathfrak{I} + f) \cap \mathbb{V}(g)}^{\mathcal{Z}}$ in time

$$\widetilde{O}\left(n\left(L + n^2\right)\left(D\delta\left(\mathbb{V}(\mathbf{F})\right)^2\right)\right).$$

- LiftParameter [126]: let T be a parameter and let $\mathcal{P}_T$ be a set of polynomials in $\mathbb{Q}(T)[X_1, \ldots, X_n]$. Let $t \in \mathbb{R}$ be a generic point and $\mathcal{P}_t$ be the polynomial system specialized at t. If $\mathbb{V}(\mathcal{P}_t)$ is 0-dimensional, the routine takes as input a geometric resolution of $\mathcal{P}_t$ and returns a parametric geometric resolution of $\mathcal{P}_t$ in time

$$\widetilde{O}\left(\left(nL + n^4 + n\right)\delta\left(\mathbb{V}(\mathcal{P}_t)\right)\left(4\delta\left(\mathbb{V}(\mathcal{P}_T)\right) + 1\right)\right).$$

1.4 Infinitesimals, Puiseux Series

In order to formally consider small deformations of algebraic varieties, we introduce infinitesimals and Puiseux series. In this section, $\mathbb{K}$ stands for $\mathbb{R}$ or $\mathbb{C}$. We refer to [16, Chapter 2.6] and [16, Chapter 12.5] for precise statements and properties of the notions presented in the sequel.

Let $F \subset F'$ be two ordered fields. An element $\varepsilon \in F'$ is infinitesimal over F if for any $x > 0$ in F, $0 < |\varepsilon| < x$.

Let ε be an infinitesimal and denote by $\mathbb{K}\langle\varepsilon\rangle$ the field of algebraic Puiseux series in ε with coefficients in $\mathbb{K}$, that is the set of series

$$\sum_{i \geq k} a_i \varepsilon^{i/q}, \text{ with } k \in \mathbb{Z},\ i \in \mathbb{Z},\ a_i \in \mathbb{K},\ q \in \mathbb{N}^*$$

that are algebraic over $\mathbb{K}(\varepsilon)$.

Proposition 1.18. *[16, Corollary 2.98 p. 81] The field $\mathbb{R}\langle\varepsilon\rangle$ is a real closed field and $\mathbb{C}\langle\varepsilon\rangle$ is an algebraically closed field.*

An element $\sum_{i \geq k} a_i \varepsilon^{i/q} \in \mathbb{K}\langle\varepsilon\rangle$ such that $k \in \mathbb{N}$ is *bounded* . The set of bounded elements in $\mathbb{K}\langle\varepsilon\rangle$ is denoted by $\mathbb{K}\langle\varepsilon\rangle_b$. If $\alpha = \sum_{i \geq k} a_i \varepsilon^{i/q} \in \mathbb{K}\langle\varepsilon\rangle_b$ then we define $\lim_0 \alpha = a_0$. We also denote by $\lim_0$ the mapping $\mathbb{K}\langle\varepsilon\rangle_b^n \longrightarrow \mathbb{K}^n$ that apply $\lim_0$ on each coordinate.

Let $S \subset \mathbb{R}^n$ defined by a system of polynomial equations and inequalities. We will denote by $\mathsf{ext}(S, \mathbb{R}\langle\varepsilon\rangle)$ the solution set in $\mathbb{R}\langle\varepsilon\rangle^n$ of the same system.

Chapter 2

Symbolic Algorithms for Optimization

Let $\mathbf{X} = \{X_1, \ldots, X_n\}$ be a set of indeterminates and $\mathbf{F} = \{f_1, \ldots, f_s\}$ be a sequence of polynomials in $\mathbb{Q}[\mathbf{X}]$ of degree at most D. Let $V \subset \mathbb{C}^n$ be the algebraic variety $\mathbb{V}(\mathbf{F}) = \{x \in \mathbb{C}^n \mid f_1(x) = \cdots = f_s(x) = 0\}$. Given another polynomial $f \in \mathbb{Q}[\mathbf{X}]$ of degree at most D, we denote by $f^\star$ the infimum $\inf_{x \in V \cap \mathbb{R}^n} f(x)$.

We present a state of the art of algorithms solving the following problems.

(B) Deciding the finiteness and computing an algebraic representation of $f^\star$.

(C) Deciding whether there exists $x^\star \in V \cap \mathbb{R}^n$ such that $f(x^\star) = f^\star$ and computing a rational parametrization of $x^\star$.

To this end, we first introduce the real quantifier elimination in Section 2.1 and we show that problems (B) and (C) are actually quantifier elimination problems.

In 1930, Tarski has proved that a quantifier-free equivalent formula always exists and has given an algorithm to compute it [138]. In Section 2.2, we present the cylindrical algebraic decomposition (CAD). It has provided a new and more efficient symbolic algorithm to solve the quantifier elimination problem. The CAD has been introduced by Collins in 1973 and described in [31]. The first complete implementation, done in 1981, is described in [5]. Then in the 1990s, several works have provided improvements and simplifications of the CAD, see e.g. [22, 32, 33, 67, 94]. The main drawback of this approach is its complexity that is doubly exponential in the number of variables. Practically, its best implementations are limited to non-trivial problems involving 4 variables at most.

In Section 2.3, we present algorithms based on the critical point method. In Section 2.3.1, we present a brief introduction to a quantifier elimination algorithm based on critical point methods [15]. Its theoretical complexity is singly exponential in the number of variables but there is no practical implementation. Finally, Section 2.3.2 is devoted to present a dedicated algorithm solving problem (B) without constraints. Unlike the previous methods, that are general quantifier elimination solvers, it take into account the structure of the optimization problem to solve it. This algorithm is singly exponential

in the number of variables. Furthermore, its implementation has a good behavior in practice, allowing to solve problems intractable with the previous methods.

2.1 Real Quantifier Elimination

In this section, we give a short introduction to real quantifier elimination (QE). Then we show how problems (B) and (C) can be seen as QE problems. Since there exist symbolic algorithms to solve the quantifier elimination problem, they can be used to solve problems (B) and (C). These algorithms are briefly presented in Sections 2.2 and 2.3.

We refer to [16], [20] and [35] for more details about semi-algebraic geometry, real fields and real quantifier elimination.

A first order formula is a formula constructed from the following rules.

- If $f \in \mathbb{Q}[\mathbf{X}]$ then $f = 0$ and $f > 0$ are formulas;
- if ϕ_1 and ϕ_2 are formulas then $\phi_1 \wedge \phi_2$ and $\phi_1 \vee \phi_2$ are formulas;
- if ϕ is a formula then so is $\neg\phi$;
- if X is a variable and ϕ a formula then $\exists X\, \phi$ and $\forall X\, \phi$ are formulas.

A quantifier-free formula is a formula in which there is no quantifier such as $\exists$ or $\forall$. Remark that since $(\phi_1 \Rightarrow \phi_2) \Leftrightarrow (\neg\phi_1 \vee \phi_2)$, if ϕ_1 and ϕ_2 are formulas then so is $(\phi_1 \Rightarrow \phi_2)$. Given a first order formula $\phi(X_1, \ldots, X_n)$ with quantifiers, the goal of quantifier elimination is to find an equivalent quantifier-free formula.

We show the connection with optimization with an example. Let $f = (xy-1)^2 + y^2 + z^2 \in \mathbb{Q}[x, y, z]$ and $V = \mathbb{V}(z-2)$. The optimization problem "compute $\inf_{x \in V \cap \mathbb{R}^n} f(x)$" can be rephrased as

$$\text{"compute the greatest } t \in \mathbb{R} \text{ such that } \forall (x, y, z) \in \mathbb{R}^3, \big(z - 2 = 0 \Longrightarrow f \geq t\big)."$$

The formula $\forall (x, y, z) \in \mathbb{R}^3, \big(z - 2 = 0 \Longrightarrow f \geq t\big)$ is equivalent to the quantifier-free formula $t - 4 \leq 0$, meaning that $f^\star = 4$. We can check that $f \geq 4$ on V. Furthermore, $f\left(x, \frac{1}{x}, 2\right) = \frac{1}{x^2} + 4$ tends to 4 when $x \to \infty$.

In general, the existence of an equivalent quantifier-free formula is given by the following theorem that we state in the special case of the real closed field $\mathbb{R}$.

Theorem 2.1. *[16, Theorem 2.77 p. 69] Let $\phi(X_1, \ldots, X_n)$ be a formula with coefficients in an ordered subring R of $\mathbb{R}$. Then there is a quantifier-free formula $\psi(X_1, \ldots, X_n)$ with coefficients in R such that for every $x \in \mathbb{R}^n$, the formula $\phi(x)$ is true if and only if $\psi(x)$ is true.*

2.2 Cylindrical Algebraic Decomposition

The cylindrical algebraic decomposition is an algorithm that allows to perform a quantifier elimination over the reals. Furthermore, there exists implementations available in

computer algebra systems like Maple, Mathematica or Redlog, or as a standalone interactive command-line program like QEPCAD. However, because of the intrinsic doubly exponential complexity, computing an infimum involving polynomials of more than 4 variables is intractable with this method. See e.g. [16, 31, 32, 33] for further reading about the cylindrical algebraic decomposition.

Definition 2.2. *Let $S \subset \mathbb{R}^n$ and let $\mathbf{F}$ be a finite set of polynomials in $\mathbb{R}[X_1, \ldots, X_n]$. The set S is said to be $\mathbf{F}$-invariant if for all $P \in \mathbf{F}$, P has a constant sign on S (that is $P > 0$, $P < 0$ or $P = 0$).*

A cylindrical algebraic decomposition (CAD) of $\mathbb{R}^n$ adapted to $\mathbf{F}$ is a partition of $\mathbb{R}^n$ into semi-algebraic sets called cells, such that each cell is $\mathbf{F}$-invariant.

The following theorem ensures the existence of such a decomposition.

Theorem 2.3. *([16, Theorem 5.6 p. 163] For every finite set $\mathcal{P} \subset \mathbb{R}[X_1, \ldots, X_n]$, there is a cylindrical algebraic decomposition of $\mathbb{R}^k$ adapted to $\mathcal{P}$.*

Collins has given an algorithm to compute a CAD (see [31] for the historical algorithm, [32, 67, 94] for improvements). The algorithm is based on two steps. The first one is a step of recursive projections. It is based on subresultant computations, which is a variant of Euclidean remainder sequence. At each step, the degree is squared. Since the depth of the recursion is the number of variables, this leads to a complexity at least doubly exponential in the number of variables. The second step is a lifting step: an explicit representation of the decomposition is build from the previous projections.

Adding slight modifications in the algorithm, the CAD can be adapted to perform a quantifier elimination (see [22] and [16, Section 11.3]). This leads to the following theorem.

Theorem 2.4. *There exists an algorithm solving the quantifier elimination problem by computing a cylindrical algebraic decomposition.*

Several implementations of the cylindrical algebraic decomposition are available. All of them can perform a quantifier elimination based on the CAD.

- Maple (`http://www.maplesoft.com/`, SemiAlgebraicSetTools package, implemented by C. Chen, M. Moreno Maza, B. Xia and L. Yang [28]).
- Mathematica (`http://www.wolfram.com/mathematica/`, implementation due to A. Strzebonski [137]).
- QEPCAD (`http://www.usna.edu/cs/~qepcad/B/QEPCAD.html`, due to H. Hong and subsequently added on to by C. W. Brown, G. E. Collins, M. J. Encarnacion, J. R. Johnson, W. Krandick, S. McCallum, S. Steinberg, R. Liska, N. Robidoux [23]).
- Redlog (`http://www.redlog.eu`, implemented by A. Seidl and T. Sturm [41, 131]).

2.3 Critical Point Method

In this section, we denote by D an upper bound on the degree of the involved polynomials.

2.3.1 Critical Point Method for Quantifier Elimination

We mention, without details, a critical point method to solve problems (B) and (C). We refer to [15] and [16, Section 14] for more precise information.

Given a polynomial family $\mathbf{F} \subset \mathbb{R}[X_1, \ldots, X_n]$, it allows to compute a tree of realizable sign conditions of $\mathbf{F}$ in singly exponential time. Then it can be used to decide the truth of a given formula ([15], [16, Section 14.1]), to perform a quantifier elimination ([16, Section 14.3]) and more particularly to solve problems (B) and (C) ([16, Section 14.2]). In this last case, the complexity is $D^{O(n)}$.

However, the techniques that allow to obtain such complexity results such as infinitesimal deformations did not provide yet practical results that reflect this complexity gain. Furthermore, the constant factors are not precised and seem to be high in practice. Then this algorithm is not usable for the size of our problems.

2.3.2 Dedicated Algorithm for Optimization

In this section, we present a dedicated algorithm for solving problem (B), coming from [118]. This is a probabilistic algorithm for the unconstrained case, that is computing $f^\star = \inf_{x \in \mathbb{R}^n} f(x)$. It is a symbolic algorithm, that requires $\widetilde{O}\left(D^{4n}\right)$ arithmetic operations in $\mathbb{Q}$. Furthermore, its implementation, that relies on Gröbner bases, is efficient in practice and has solved problems intractable before (up to 6 variables).

To this end, the potential values for $f^\star$ are characterized, using the notion of generalized critical value. The generalized critical values are introduced in [81]. The infimum $f^\star$ is necessarily a generalized critical value. Then, the problem is reduced to the computation of the smallest generalized critical value. The computation of a set that contains the critical values can be done using Gröbner bases. Moreover, the computation of the asymptotic values can be reduced to the computation of the set of non-properness of a projection restricted to an algebraic variety of dimension at most 1. Hence, it can be done using Gröbner bases or the geometric resolution algorithm. Since the set of values computed can strictly contain the critical values, one must be able to detect an eventual redundant value. This is done by using the fact that f is a locally trivial fibration outside the generalized critical values. Thus the detection of a redundant value is reduced to testing the emptiness of finitely many sets of the form $f^{-1}(t) \cap \mathbb{R}^n$ for $t \in \mathbb{Q}$.

Let $f \in \mathbb{Q}[\mathbf{X}]$. We recall that a real number c is a *real critical value* of f if and only if there exists $x \in \mathbb{R}^n$ such that

- $f(x) = c$;
- $\dfrac{\partial f}{\partial X_1}(x) = \cdots = \dfrac{\partial f}{\partial X_n}(x) = 0.$

A real number c is a *real asymptotic critical value* of f if and only if there exists a sequence $(x_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{R}^n$ such that

- $f(x_\ell)$ tends to c when ℓ tends to ∞;
- $\|x_\ell\|$ tends to ∞ when ℓ tends to ∞;
- for all $(i,j) \in \{1,\ldots,n\}^2$, $\|X_i(x_\ell)\| \left\| \dfrac{\partial f}{\partial X_j}(x_\ell) \right\|$ tends to 0 when ℓ tends to ∞.

The set of *real generalized critical values* of f is the union of real critical values and the real asymptotic critical values.

Using the result of [81] stating that outside its set of generalized critical values, a polynomial mapping realizes a locally trivial fibration, we can obtain the following characterization for the infimum.

Theorem 2.5. *[118, Theorem 5] Let $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathcal{E} = \{e_1,\ldots,e_\ell\}$ (with $e_1 < \ldots < e_\ell$) be the set of real generalized critical values of f. Then $\inf\limits_{x\in\mathbb{R}^n} f(x)$ is finite if and only if there exists $i_0 \in \{1,\ldots,\ell\}$ such that $\inf\limits_{x\in\mathbb{R}^n} f(x) = e_{i_0}$.*

Since the infimum is necessarily a real generalized critical value, the next step is the computation of a set that contain the real asymptotic critical values.

Theorem 2.6. *[117, Theorem 3.6] There exists a Zariski-open set $\mathscr{O} \subsetneq GL_n(\mathbb{C})$ such that for all $\mathbf{A} \in GL_n(\mathbb{Q}) \cap \mathscr{O}$, the set of asymptotic critical values of f is contained in the set of non-properness of the projection*

$$\begin{aligned} \pi_T : \quad \mathbb{C}^{n+1} &\longrightarrow \mathbb{C} \\ (x_1,\ldots,x_n,t) &\longmapsto t \end{aligned}$$

restricted to the Zariski-closure of the constructible set defined by

$$W^{\mathbf{A}} = \left\{ f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0 \right\}.$$

Example 2.7. *Let $f = (xy-1)^2 + y^2$. The Zariski-closure of $\left\{ \frac{\partial f}{\partial x} = 0, \frac{\partial f}{\partial y} \neq 0 \right\}$ is the variety $\mathbb{V}(y(xy-1))$. The above theorem ensures that if there exists an asymptotic critical value $c \in \mathbb{R}$, then there exists a sequence $(x_k)_k \subset \mathbb{V}(y(xy-1))$ such that $f(x_k) \underset{k\to+\infty}{\longrightarrow} c$. One can check that 0 is an asymptotic critical value and that it is the limit of the evaluation by f of the sequence $\left(k, \dfrac{1}{k}\right) \in \mathbb{V}(y(xy-1))$.*

The algebraic variety $W^{\mathbf{A}}$ has dimension at most 1, thus the set of non-properness of any polynomial restricted to $W^{\mathbf{A}}$ is finite. In particular, the above set of non-properness can be computed using [120, Lemma 4].

However, it can contain useless values. To detect these values, the following topological property is used.

Theorem 2.8. *[118, Theorem 6] Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ and $\mathcal{E} = \{e_1, \ldots, e_\ell\}$ be the set of its real generalized critical values as above. Consider $\{r_0, \ldots, r_\ell\}$ a set of rationals such that*

$$r_0 < e_1 < r_1 < \cdots < r_{\ell-1} < e_\ell < r_\ell$$

The infimum $\inf_{x \in \mathbb{R}^n} f(x)$ is finite if and only if there exists $i_0 \in \{1, \ldots, \ell\}$ such that

$$\{x \in \mathbb{R}^n \mid f(x) = r_{i_0}\} \neq \varnothing$$

and for all $j \leq i_0 - 1$,

$$\{x \in \mathbb{R}^n \mid f(x) = r_j\} = \varnothing$$

In this case, we have $\inf_{x \in \mathbb{R}^n} f(x) = e_{i_0}$.

It is then sufficient to test the emptiness of some real fibers between the computed set to detect which value is the infimum. Finally, the following theorem is obtained.

Theorem 2.9. *([118, Theorem 7]) There exists a probabilistic algorithm computing the global infimum of a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree D with a complexity within $\widetilde{O}\left(D^{4n}\right)$.*

Note that its implementation has solved some problems not tractable before (up to 6 variables).

Chapter 3

Real Algebra

We first introduce some tools and results coming from real algebra in Section 3.1. We present results about the existence of a representations as sum of squares of rational functions or of polynomials for a non-negative polynomial. Since there is not bound on the degree of the denominators in a representation as a sum of squares of rational functions, we focus on the representation as sum of squares of polynomial. Nevertheless, all non-negative polynomials can not be expressed as a sum of squares of polynomials. Though, the existence of certificates on a semi-algebraic set can be obtained.

In Section 3.2.1, we explain how to compute approximations of sums of squares. Writing the condition of being a sum of squares in terms of linear matrix inequalities, numerical semidefinite programming solvers can be used for practical computations. In general, this provides a sequence of certificates for lower bounds on $f^\star$. A natural question is then to know when these computed lower bounds tends to or are close to $f^\star$.

Then in Section 3.2.2, we are interested in the computation of certificates with rational coefficients.

To prove the existence of certificates, constraints can be added to reduce the problem to an equivalent one on a semi-algebraic set on which being a sum of squares is equivalent to being non-negative. We present a state of the art of this approach in Section 3.3.

3.1 Real Algebra and Sums of Squares

In the context of real algebra, the goal is to characterize a non-negative element by writing it as a sum of squares. A real non-negative polynomial is a sum of squares of rational functions. However, because there are no bounds on the degree of these rational functions, from a computational point of view, we focus on writing a non-negative polynomial as a sum of squares of *polynomials*. All non-negative polynomials can not be expressed as a sum of squares of polynomials.

However, assume that a polynomial f can be written $f = \sigma_0 + \sum_{1 \leq i \leq s} \sigma_i f_i$, where each f_i is a polynomial and each σ_i is a sum of squares. Then f is necessarily non-negative on the semi-algebraic set defined by $f_1 \geq 0, \ldots, f_s \geq 0$. The aim of Schmüdgen's and

Putinar's Positivstellensatz is to ensure the existence of this type of certificate.

3.1.1 Positivstellensatz

In this section, we present historical results dealing with the positivity of polynomial. In the context of real algebra, the goal is to obtain a certificate of positivity using expressions with sums of squares. Indeed, in his 17th problem, Hilbert asked whether a real non-negative polynomial in several variables is a sum of squares of rational functions. Artin solved this problem in 1927 [6]: the answer is yes. However, his proof was not constructive. Given a set $\mathcal{S}$, $f > 0$ (resp. $f \geq 0$) on $\mathcal{S}$ means that for all $x \in \mathcal{S}$, $f(x) > 0$ (resp. $f(x) > 0$). For $\mathbb{K} = \mathbb{R}$ or $\mathbb{Q}$, one denotes by $\sum \mathbb{K}[\mathbf{X}]^2$ the set of sums of squares of polynomials in $\mathbb{K}[\mathbf{X}]$.

Krivine [78] and Stengle [136] independently got a refinement of Artin result, from which the following is a consequence.

Theorem 3.1 (Positivstellensatz). *Let* $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{R}[X_1, \ldots, X_n]$ *and let*

$$\mathcal{S} = \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}.$$

Then $f > 0$ *on* $\mathcal{S}$ *if and only if* f *can be written in the form*

$$f = \frac{1 + \sum_{\delta \in \{0,1\}^s} \sigma_\delta f_1^{\delta_1} \ldots f_s^{\delta_s}}{1 + \sum_{\delta \in \{0,1\}^s} \theta_\delta f_1^{\delta_1} \ldots f_s^{\delta_s}},$$

where $\delta = (\delta_1, \ldots, \delta_s)$ *and* σ_δ, $\theta_\delta \in \sum \mathbb{R}[\mathbf{X}]^2$.

To compute such a representation, the degrees of the numerator and denominator are chosen. Nevertheless, as far as we know, there are no praticable information about the degree of the involved polynomials in Theorem 3.1. Indeed, bounds on the degree of the Positivstellensatz on $\mathbb{R}^n$ depending only in the number of variables and the degree of f are either non-explicit (see e.g. [110, Theorem A]) or explicit but too large for practical computation (see [124, Chapter 11, Theorem 11.14] for a n-fold exponential bound in n and in the degree of f). Lombardi, Perrucci and Roy recently announced a 5-fold bound in n and in the degree of f. However the results is not published yet.

3.1.2 Sum of Squares

To avoid the Positivstellensatz issue about the degree, we consider the representation of a positive polynomial as a sum of squares of polynomials. Indeed, if a polynomial f of degree $2d$ is a sum of squares of polynomials g_i then each g_i has degree at most d. Then it provides a natural bound on the degree of the polynomials involved in the decomposition as a sum of squares. In general, there exist non-negative polynomials that are not a sum of squares. However, the existence of certificates of positivity on semi-algebraic set $\mathcal{S}$ can be obtained under additional assumptions.

In 1888, Hilbert [63] prove that $f \geq 0$ over $\mathbb{R}^n$ is necessarily a sum of squares only when

- $n = 1$ or
- f has degree 2 or
- $n = 2$ and f has degree ≤ 4.

Counterexamples can be constructed in all other cases (see [29, 97, 114] for some special cases and [113] for a survey).

According to Blekherman [19], "there are significantly more non-negative polynomials than sums of squares".

Theorem 3.2. *[19] For every fixed degree, the volume of the set of sums of squares of polynomials in the set of non-negative polynomials tends to* 0 *when the number of variables increases.*

However, the Positivstellensatz can be generalized without denominators over a semi-algebraic set under some assumptions. We present the first historical results about the existence of sum of squares decompositions. Some recent results, that have been studied in the context of global optimization, are presented in Section 3.3.

Theorem 3.3 (Schmüdgen's Positivstellensatz [125])**.** *Let* $f_1, \ldots, f_s \in \mathbb{R}[\mathbf{X}]$ *and*

$$\mathcal{S} = \{x \in \mathbb{R}^n \,|\, f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}.$$

Assume that $\mathcal{S}$ *is* compact*. Then* $f > 0$ *on* $\mathcal{S}$ *if and only if* f *can be written in the form*

$$f = \sum_{\delta \in \{0,1\}^s} \sigma_\delta f_1^{\delta_1} \ldots f_s^{\delta_s},$$

where $\delta = (\delta_1, \ldots, \delta_s)$ *and* $\sigma_\delta \in \sum \mathbb{R}[\mathbf{X}]^2$.

Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{R}[\mathbf{X}]$. The quadratic module $M(\mathbf{F})$ generated by $\mathbf{F}$ is the set

$$M(\mathbf{F}) = \left\{ \sigma_0 + \sum_{1 \leq i \leq s} \sigma_i f_i \,|\, \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2 \right\}.$$

The quadratic module $M(\mathbf{F}) \subset \mathbb{R}[\mathbf{X}]$ is archimedean if there exists $N \in \mathbb{N}$ such that $N - \|\mathbf{X}\|^2 \in M(\mathbf{F})$. Note that if $M(\mathbf{F})$ is archimedean then $\mathcal{S}$ is compact (see [111] or [102]).

Theorem 3.4 (Putinar's Positivstellensatz)**.** *Let* $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{R}[\mathbf{X}]$ *and*

$$\mathcal{S} = \{x \in \mathbb{R}^n \,|\, f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}.$$

Assume that $M(\mathbf{F})$ is archimedean. Then $f > 0$ on $\mathcal{S}$ if and only if f can be written in the form

$$f = \sigma_0 + \sum_{1 \leq i \leq s} \sigma_i f_i,$$

where $\sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2$.

These results require the compactness of the semi-algebraic set. In Section 3.3, we present existence of algebraic certificates of positivity results that do not require the compactness.

3.2 Computation of Sum of Squares Representations

We present now the practical aspect of the real algebra approach. From the previous section, we know the theoretical existence of certificate of positivity as sum of squares in some cases. The goal is to compute practically such a certificate of positivity in order to obtain information for the optimization problem

First, we introduce semidefinite programming. Then we show the connection between optimization and sum of squares problem. This sum of squares problem can be expressed as a semidefinite program. Hence, successive approximations of a sum of squares certificate can be numerically obtained. This provides a sequence of certified lower bounds on $f^\star$.

Finally, we present two approaches that can be used to compute a sum of squares identity with rational coefficients.

In this section, we denote by $\mathrm{Sym}_n(\mathbb{R})$ the set of symmetric matrices of size n with real coefficients. Given $X \in \mathrm{Sym}_n(\mathbb{R})$, we write $X \succeq 0$ if and only if X is positive semidefinite, that is if $z^T X z \geq 0$ for all vector $z \in \mathbb{R}^n$.

3.2.1 Semidefinite Programming and Sum of Squares

This section is devoted to define a semidefinite program (SDP) and present softwares solving this problem. Then we show how to relax the optimization problem to a sum of squares problem, that itself can be expressed as a SDP problem.

Semidefinite programming.

We refer to [86] for a general survey on semidefinite programming and the computation of sums of squares of polynomials.

A semidefinite program (SDP) is a problem of the form

$$\begin{aligned} \text{minimize } & \langle C, X \rangle = \mathrm{Tr}(CX) \\ \text{s.t. } & \mathrm{Tr}(A_i X) = b_i, \quad i = 1, \ldots, m \\ & X \succeq 0 \end{aligned}$$

where the unknown X lies in $\mathrm{Sym}_n(\mathbb{R})$ and $C \in \mathrm{Sym}_n(\mathbb{R})$, $A_i \in \mathrm{Sym}_n(\mathbb{R})$ and $b_i \in \mathbb{R}$ are given entries.

There exist numerical algorithms solving this problem.

- ConicBundle: `http://www-user.tu-chemnitz.de/~helmberg/ConicBundle/`
- CSDP: `http://infohost.nmt.edu/~borchers/csdp.html`,
- DSDP: `http://www.mcs.anl.gov/hs/software/DSDP/`,
- PENSDP: `http://www.penopt.com/pensdp.html`,
- SeDuMi: `http://sedumi.ie.lehigh.edu/`
- SDPA: `http://sdpa.sourceforge.net/`,
- SDPLR: `http://dollar.biz.uiowa.edu/~sburer/`,
- SDPT3: `http://www.math.nus.edu.sg/~mattohkc/sdpt3.html`,

Most of them are based on interior point methods: a barrier function is associated with the problem. It depends on the variables of the original problem and a parameter μ. It is a convex function for $\mu > 0$. As $\mu \to 0$, the minimum of the barrier function tends to a solution of the original problem. To compute the minimum of the barrier function, Newton's method is used to approximate a point at which the necessary optimality conditions for the function are satisfied (see e.g. [21, Section 4] and [38] for more details on interior point methods).

ConicBundle is based on another approach. The semidefinite program is transformed into a problem of eigenvalue optimization [59]. To solve this eigenvalue optimization problem, bundle methods are used [58, 65, 66, 76, 127].

Sum of Squares Relaxations.

Let $f \in \mathbb{R}[\mathbf{X}]$. We consider the SOS relaxation

$$f^{\mathsf{sos}} = \sup\left\{a \in \mathbb{R} \,|\, \exists \sigma \in \sum \mathbb{R}[\mathbf{X}]^2, f(x) - a = \sigma\right\}.$$

The number f^{sos} gives a lower bound on $f^\star = \inf_{x \in \mathbb{R}^n} f(x)$. Furthermore, writing a polynomial as a sum of squares of polynomials is strongly related with the theory of positive semidefinite matrices. In the sequel, given $t \in \mathbb{N}$, we denote by $\mathbb{N}^n_t$ the set

$$\mathbb{N}^n_t = \left\{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \mid \sum_{1 \le i \le n} \alpha_i \le t\right\}.$$

Lemma 3.5. *[87, Lemma 3.8] Let* $f = \sum_{\alpha \in \mathbb{N}^n_{2D}} f_\alpha \mathbf{X}^\alpha \in \mathbb{R}[\mathbf{X}]$ *of degree* $\leq 2D$. *Then* $f \in \sum \mathbb{R}[\mathbf{X}]^2$ *if and there exists a matrix* $X = (X_{\alpha,\beta})_{\alpha,\beta \in \mathbb{N}^n_D}$ *such that*

$$\begin{cases} X \succeq 0 \\ \sum_{\substack{\beta,\gamma \in \mathbb{N}^n_D \\ \beta+\gamma=\alpha}} X_{\beta,\gamma} = f_\alpha \end{cases}$$

Example 3.6. *Let* $f = 2x_1^2 + x_2^2 - 2x_1x_2 + 2x_1 + 1$. *It can be written*

$$\underbrace{\begin{pmatrix} 1 & x_1 & x_2 \end{pmatrix}}_{z_1^T} \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}}_{X} \underbrace{\begin{pmatrix} 1 \\ x_1 \\ x_2 \end{pmatrix}}_{z_1}.$$

The eigenvalues of the matrix X *are* 0, 1 *and* 3. *Hence, it is positive semidefinite. We compute the Cholesky decomposition of* X. *We get* $X = U^T.U$ *with*

$$U = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence, $f = (Uz_1)^T (Uz_1) = \begin{pmatrix} 1+x_1 & x_1 - x_2 & 0 \end{pmatrix} \begin{pmatrix} 1+x_1 \\ x_1 - x_2 \\ 0 \end{pmatrix} = (1+x_1)^2 + (x_1 - x_2)^2$.

Thanks to this connection between sums of squares and semidefinite matrices, the problem of computing f^{sos} can be expressed as a SDP, see e.g. [29]. Let $\mathbb{N}^n_{2D} = \left\{ \alpha \in \mathbb{N}^n \mid \sum_{1 \leq i \leq n} \alpha_i < 2D \right\}$. Let z_d be the vector of all monomials of degree $\leq d$. In the sequel, we denote by E_{ij} the matrix whose entries are 0 except for the (i,j)-coefficient, that is 1.

Proposition 3.7. *[104, Lemma 3.1] Computing* f^{sos} *is equivalent to solving the semidefinite program:*

$$\begin{aligned} \text{minimize } & \langle C, X \rangle = \operatorname{Tr}(CX) \\ \text{s.t. } & \operatorname{Tr}(A_\alpha X) = f_\alpha, \quad \alpha \in \mathbb{N}^n_{2D} \\ & X \succeq 0 \end{aligned}$$

with $C = E_{11}$ *and* A_α *such that* $\sum_{\substack{\beta,\gamma \in \mathbb{N}^n_D \\ \beta+\gamma=\alpha}} X_{\beta,\gamma} = \operatorname{Tr}(A_\alpha X)$, *that can be obtained by equating the coefficients of the two polynomials* f *and* $z_d^T X z_d$.

Example 3.8. *Let* $f = 2x_1^2 + x_2^2 - 2x_1x_2 + 2x_1$ *and* $z_1 = \begin{pmatrix} 1 \\ x_1 \\ x_2 \end{pmatrix}$. *We want to compute*

$$f^{\mathsf{sos}} = \sup\left\{a \in \mathbb{R} \,|\, \exists \sigma \in \sum \mathbb{R}\left[\mathbf{X}\right]^2, f\left(x\right) - a = \sigma\right\}.$$

According to Lemma 3.5, $f - a$ *is a sum of squares if and only if there exists a positive semidefinite matrix* X *such that* $f - a = z_1^T X z_1$. *By equating the coefficients, we see that* $X = \begin{pmatrix} -a & 1 & 0 \\ 1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$. *Thus we want to find a matrix* $X \succeq 0$ *such that* $X = \begin{pmatrix} -a & 1 & 0 \\ 1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$, *where the coefficient* a *is maximal. In order to formulate this problem as a SDP, we translate the condition* $X = \begin{pmatrix} -a & 1 & 0 \\ 1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$ *in terms of* $\mathrm{Tr}\left(AX\right)$ *for symmetric matrices* A.

Remark that the matrix $(E_{ij} + E_{ji})$ *is symmetric and that*

$$\mathrm{Tr}\left((E_{ij} + E_{ji}) \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & x_{23} \\ x_{13} & x_{23} & x_{33} \end{pmatrix}\right) = 2x_{ij}.$$

Then the condition $X = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & x_{23} \\ x_{13} & x_{23} & x_{33} \end{pmatrix} = \begin{pmatrix} -a & 1 & 0 \\ 1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$ *can be written*

$$\begin{cases} \mathrm{Tr}\left(E_{11}X\right) = x_{11} = -a \\ \mathrm{Tr}\left(E_{22}X\right) = x_{22} = 2 \\ \mathrm{Tr}\left(E_{33}X\right) = x_{33} = 1 \\ \mathrm{Tr}\left(\left(E_{12} + E_{21}\right)X\right) = 2x_{12} = 2 \\ \mathrm{Tr}\left(\left(E_{13} + E_{31}\right)X\right) = 2x_{13} = 0 \\ \mathrm{Tr}\left(\left(E_{23} + E_{32}\right)X\right) = 2x_{23} = -2 \end{cases}$$

Finally, minimizing $-a$ *such that* $f - a$ *is a sum of squares is equivalent to the following SDP formulation.*

$$\begin{aligned} \textit{minimize} \quad & \mathrm{Tr}\left(E_{11}X\right) \\ \textit{s.t.} \quad & \mathrm{Tr}\left(E_{22}X\right) = 2 \\ & \mathrm{Tr}\left(E_{33}X\right) = 1 \\ & \mathrm{Tr}\left(\left(E_{12} + E_{21}\right)X\right) = 2 \\ & \mathrm{Tr}\left(\left(E_{13} + E_{31}\right)X\right) = 0 \\ & \mathrm{Tr}\left(\left(E_{23} + E_{32}\right)X\right) = -2 \\ & X \succeq 0 \end{aligned}$$

Using YALMIP [92], we get the solution $\begin{pmatrix} 1.0 & 1.0 & 0.0 \\ 1.0 & 2.0 & -1.0 \\ 0.0 & -1.0 & 1.0 \end{pmatrix}$, *meaning that* $f^{\mathsf{sos}} = -1$.

As seen in the previous section, a non-negative polynomial is not necessarily a sum of squares. However, results like Schmüdgen's or Putinar's Positivstellensatz ensure the existence of certificates of positivity by means of sums of squares on a semi-algebraic set. Hence, given $f_1, \ldots, f_s \in \mathbb{R}[\mathbf{X}]$, we can try to compute

$$f^{\mathsf{sos}} = \sup \left\{ a \in \mathbb{R} \,|\, \exists \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2, f(x) - a = \sigma_0 + \sum_{1 \leq i \leq s} \sigma_i f_i \right\}.$$

However, this problem can not be expressed as a SDP. Indeed, the degrees of the sums of squares σ_i are not known *a priori*. Nevertheless, fixing an upper bound on these degrees allows to translate the problem into a SDP. We show how to get a SDP problem in the following example.

Example 3.9. *Let f be a polynomial of degree $\leq 2d$ and g a polynomial of degree $\leq 2\delta$.*

Given $t \in \mathbb{N}$, we want to find sums of squares σ and τ such that $f - a = \sigma + \tau g$, with $\deg \sigma \leq 2t$ and $\deg \tau g \leq 2t$. This is equivalent to finding positive semidefinite matrices X_1 and X_2 such that

$$f - a = z_t^T X_1 z_t + z_{t-\delta}^T X_2 z_{t-\delta} g. \tag{3.1}$$

To satisfy such an equation, the matrices X_1 and X_2 are subject to constraints obtained by equating the coefficients, as in example 3.8. Let $X_1 = \left(X^{(1)}_{\beta,\gamma}\right)_{\beta,\gamma \in \mathbb{N}^n_t}$, $X_2 = \left(X^{(2)}_{\beta,\gamma}\right)_{\beta,\gamma \in \mathbb{N}^n_{t-\delta}}$, $g = \sum_{\alpha} g_{\alpha \in \mathbb{N}^n_{2\delta}} x^\alpha$ and $f = \sum_{\alpha \in \mathbb{N}^n_{2d}} f_\alpha x^\alpha$. By equating the coefficients, Equation 3.1 is equivalent to the problem

$$\begin{cases} X \succeq 0 \\ X^{(1)}_{\mathbf{0},\mathbf{0}} + X^{(2)}_{\mathbf{0},\mathbf{0}} \times g_{\mathbf{0}} = f_{\mathbf{0}} - a \\ \sum\limits_{\substack{\beta,\gamma \in \mathbb{N}^n_t \\ \beta+\gamma=\alpha}} X^{(1)}_{\beta,\gamma} + \sum\limits_{\substack{b,c \in \mathbb{N}^n_{2\delta} \\ b+c=\alpha}} g_b \sum\limits_{\substack{a,b \in \mathbb{N}^n_{t-\delta} \\ a+b=c}} X^{(2)}_{a,b} = f_\alpha \end{cases}$$

Since $X = \left(\begin{array}{c|c} X_1 & \mathbf{0} \\ \hline \mathbf{0} & X_2 \end{array}\right) \succeq 0$ is equivalent to $X_1 \succeq 0$ and $X_2 \succeq 0$, the computation of f^{sos} is a semidefinite program.

Then we can consider the following sequence of relaxations:

$$f_t^{\mathsf{sos}} = \sup \left\{ a \in \mathbb{R} \,|\, \exists \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2, f(x) - a = \sigma_0 + \sum_{1 \leq i \leq s} \sigma_i f_i, \deg(\sigma_0), \deg(\sigma_i f_i) \leq 2t \right\},$$

Since the above set become larger as t grows, $f_t^{\mathsf{sos}} < f_{t'}^{\mathsf{sos}}$ if $t < t'$, leading to a hierarchy of relaxations.

We present now Matlab implementations that translate an SOS problem into a SDP and use a SDP solver to solve it:

- Gloptipoly3: `http://homepages.laas.fr/henrion/software/gloptipoly/`,
- SOSTOOLS: `http://www.cds.caltech.edu/sostools/`,
- SparsePOP: `http://www.is.titech.ac.jp/~kojima/SparsePOP/`,
- YALMIP: `http://users.isy.liu.se/johanl/yalmip/`.

Hence the computation of an approximation of f^{sos} (resp. f_t^{sos} in the constrained case) is possible. In Section 3.3, we present results that, under some assumptions on $f_1, \ldots, f_s$, ensure that $f^{\mathsf{sos}} = f^\star$. In this case, the sequence $(f_t^{\mathsf{sos}})_t$ converges monotonically increasing to $f^\star$. This leads to methods that compute successive approximations of $f^\star$, that are more and more accurate.

3.2.2 Computation of Rational Certificates

As explained before, using SDP to solve SOS relaxations leads to the computation of approximations of representations as sums of squares. Let f be a polynomial of degree $2d$ and

$$f^{\mathsf{sos}} = \sup\left\{a \in \mathbb{R} \,|\, \exists \sigma \in \sum \mathbb{R}\left[\mathbf{X}\right]^2, f\left(x\right) - a = \sigma\right\}.$$

Assume that there exists $\sigma \in \sum \mathbb{R}\left[\mathbf{X}\right]^2$ with algebraic coefficients such that $f - f^{\mathsf{sos}} = \sigma$. Then using semidefinite programming, an approximation with floating point coefficients of the form $f - \widetilde{f}^{\mathsf{sos}} \simeq \widetilde{\sigma}$ is computed. In this section, we want to compute an approximation with rational coefficients. We present two methods to obtain such rational certificates.

Method based on numerical computation.

The first method comes from [75] and [105]. In this section, let $N = \binom{n+d}{d}$, that is the size of the vector z_d of all monomials of degree $\leq d$. The main steps are the following.

1. Compute a representation $f - \widetilde{f}^{\mathsf{sos}} \simeq z_d^T \widetilde{Q} z_d$, where $\widetilde{f}^{\mathsf{sos}}$ and $\widetilde{Q}$ have floating point coefficients, using semidefinite programming;
2. Approximate $\widetilde{f}^{\mathsf{sos}}$ by a rational number $r' \leq \widetilde{f}^{\mathsf{sos}}$ and convert $\widetilde{Q}$ to a rational matrix Q';
3. Compute $\Pi\left(Q'\right)$, the orthogonal projection of Q' to the linear affine hyperplane

$$\left\{Q \in \mathrm{Sym}_N\left(\mathbb{R}\right) \,|\, f - r' = z_d^T Q z_d\right\}.$$

According to [75, Section 2.2] and [105, Proposition 7], since $\Pi(Q')$ is an orthogonal projection, its coefficients can be computed exactly from the coefficients of Q'. Since Q' is a rational matrix, so is $\Pi(Q')$.

If $\Pi(Q') \succeq 0$, then a rational certificate $f - r' = z_d^T \Pi(Q') z_d$ is obtained for r', that is a certified lower bound on f^{sos}. Else, we start again with a better precision or with a lower r'.

In [75], the representation of Step 1 is refined using Gauss-Newton iterations before Step 2.

In [105], it is suggested to use continued fractions in order to convert $\widetilde{Q}$ to a rational matrix. Furthermore, conditions are given to ensure that the projection $\Pi(Q')$ is positive semidefinite. In the sequel, dist is the Euclidean distance between two matrices.

Proposition 3.10. *[105, Proposition 8] Let $Q \in \mathrm{Sym}_N(\mathbb{R})$ and Q' a rational matrix in $\mathrm{Sym}_N(\mathbb{R})$. Assume that there exist $\tau, \varepsilon, \delta \in \mathbb{R}_+$ such that $\tau^2 + \delta^2 \leq \varepsilon^2$ and*

- *every eigenvalue of Q is greater than or equal to ε,*
- *$\mathsf{dist}(Q, \Pi(Q)) \leq \delta$,*
- *and $\mathsf{dist}(Q, Q') \leq \tau$.*

Then $\Pi(Q')$ is positive semidefinite.

If the SDP is strictly feasible then one can choose $\varepsilon > 0$. Then if $\delta^2 < \varepsilon^2$, this proves that it is possible to compute a rational certificate using sufficiently many digits. Up to considering the dual form of the SDP problem, it is proved in [105, Proposition 9] that it is always possible to get $\delta = 0$.

Direct computation.

In this paragraph, we briefly introduce results that leads to the computation of rational certificates.

Univariate case. In the univariate case, a recursive algorithm is given in [128]. Let $f \in \mathbb{Q}[T]$ such that for all $t \in \mathbb{R}$, $f(t) \geq 0$. The algorithm is based on the following results.

1. if f has degree 2 then this is a sum of squares or rational polynomials;
2. if f is not square-free, it is enough to consider its square-free part;
3. if f is square-free of degree D, then there exists $t \in \mathbb{Q}$ and a polynomial $f_t \in \mathbb{Q}[T]$ of degree 2 such that
   - $f \geq f_t \geq 0$ on $\mathbb{R}$;
   - the square-free part of $f - f_t \geq 0$ has degree $\leq D - 2$.

Assertion 1 comes from [128, Lemma 2.25], where an expression of a sum of squares depending on the coefficients of f is given. Assertion 3 from [128, Theorem 2.27]. An expression of f_t depending on f and f' is given.

Hence, one can compute recursively a rational sum of squares: if f has degree 2, then we return the rational sum of squares expression of f. Else, we consider the square-free part of f and we compute the polynomial $f - f_t$. It is non-negative on $\mathbb{R}$, then one can call the algorithm on its square-free part, that has degree $D - 2$. Then we obtain a rational representation as a sum of squares of the square-free part of $f - f_t$. Since f_t has degree 2 and is non-negative on $\mathbb{R}$, it has a representation as a rational sum of squares. This leads to a representation as a rational sum of squares for $f - f_t$.

Computing rational solution of LMI. This algorithm comes from [55]. Given a symmetric matrix A whose entries are linear forms in $\mathbb{Q}[\mathbf{X}]$, it computes a rational point in $\mathbb{Q}^n$ that is a solution of the Linear Matrix Inequality $A \succeq 0$, if and only if such a solution exists. Let $f \in \mathbb{Q}[\mathbf{X}]$ of degree $2d$. Since the constraints in Lemma 3.5 are linear, this algorithm can be used to compute a rational symmetric matrix $Q \succeq 0$ such that $f = z_d^T Q z_d$. Such an equation gives a representation as a rational sum of squares for f.

The algorithm is based on the one in [122], that computes rational points in a convex semi-algebraic set. Linear Matrix Inequalities define convex semi-algebraic sets since they can be seen as sign conditions on the coefficients of characteristic polynomials [108].

Let $\mathcal{S} \subset \mathbb{R}^k$ be a semi-algebraic set. In the sequel, a set of sample points of $\mathcal{S}$ is a finite set of points that meets each connected component of $\mathcal{S}$ (see [15, Section 3] and [16, Chapter 5] for an algorithm computing a set of sample points). The algorithm is based on the following results.

1. if $\mathcal{S} \subset \mathbb{R}^k$ has dimension k then it has rational points and the proof of [15, Theorem 4.1.2 page 1032] leads to an algorithm computing such a point;

2. if $k = 1$ and $\mathcal{S}$ has dimension < 1 then it is either empty or a single point. By computing a set of sample points of $\mathcal{S}$, we obtain either an empty set, meaning that $\mathcal{S}$ is empty or a single point if it is not empty. It is then sufficient to test whether this single point is rational or not;

3. if $k > 1$ and $\mathcal{S} \subset \mathbb{R}^k$ has dimension $< k$ then it is included in an hyperplane $\mathcal{H}$ of $\mathbb{R}^k$. Hence, we can consider the intersection $\mathcal{S} \cap \mathcal{H}$. This leads to considering a new convex semi-algebraic set $\mathcal{S}' \subset \mathbb{R}^{k-1}$ such that $\mathcal{S}'$ has rational points if and only if $\mathcal{S}$ has rational points. Furthermore, one can recover a rational point in $\mathcal{S}$ from a rational point in $\mathcal{S}'$.

Assertion 1 comes from [122, Section 2.1]. Assertion 2 and 3 are explained in [122, Section 3.2].

This leads to a recursive algorithm that computes a rational point in $\mathcal{S}$ if and only if such a point exists: if $\mathcal{S}$ has dimension k, then we can compute rational points. If $k = 1$ and $\mathcal{S}$ has dimension < 1, then one can compute a rational point in $\mathcal{S}$ if and only if such

a point exists. If $\mathcal{S}$ has dimension $< k$ then from Assertion 3, we can call the algorithm with a new convex semi-algebraic set $\mathcal{S}' \subset \mathbb{R}^{k-1}$. Then at each step of the recursion, the dimension of the ambient space decrease. From Assertions 1 and 2, the algorithm terminates and return a rational point in $\mathcal{S}$ if and only if such a point exists.

This algorithm can be used to compute a rational solution of a LMI $A \succeq 0$. Its description for this special case is given in [55]. Furthermore, assume that A has size $N \times N$ and that its coefficients are linear forms in $\mathbb{Q}[\mathbf{X}]$, with coefficients of bit size $\leq \tau$. Then according to [55, Section 4], the algorithm runs within $(n\tau)^{O(1)} 2^{O\left(\min(n,N)N^2\right)} N^{O\left(N^2\right)}$ bit operations and its output has bit size dominated by $\tau^{O(1)} 2^{O\left(\min(n,N)N^2\right)}$.

3.3 Existence of Certificates

In this section, recent results providing the existence of certificates of positivity by means of sums of squares are presented. These results have been developed in order to compute lower bounds on the infimum of a polynomial. Indeed, following the approach described in Section 3.2.1, if the existence of certificates is proved then a sequence of lower bounds converging to $f^\star$ can be computed. This is done by constructing a hierarchy of sum of squares relaxations. These relaxations lead to semidefinite relaxations, that can be solved numerically using SDP solvers.

The relaxations are splitted into three families. In Section 3.3.1, we present results that can be used in the unconstrained case, that is when $f^\star = \inf_{x \in \mathbb{R}^n} f(x)$. Section 3.3.2 deals with the constrained case, that is $f^\star = \inf_{x \in \mathcal{S}} f(x)$, where $\mathcal{S} \subset \mathbb{R}^n$ is a semi-algebraic or a real algebraic set.

The idea is to add constraints to ensure that over the set defined by these new constraints,

- a positive polynomial is necessarily a sum of squares and
- if a polynomial is positive over these new constraints then it is positive over the original set.

Finally in Section 3.3.3, results about the existence of rational certificates are presented.

3.3.1 Unconstrained Case

"Big ball" method.

This method is due to Lasserre [84], using the following theorem (that is a special case of Schmüdgen's Positivstellensatz and that has been proved by Cassier [27]).

Given $R \geq 0$, let $\overline{B}(0, R)$ be the closed ball centered at 0 of radius R.

Theorem 3.11. *[84, Theorem 3.4] Let $f \in \mathbb{R}[\mathbf{X}]$ and $R \geq 0$. Then $f \geq 0$ over $\overline{B}(0, R)$ if and only if for all $\varepsilon > 0$, $f + \varepsilon$ can be written*

$$f + \varepsilon = \sigma + \theta\left(R^2 - \|x\|^2\right),$$

where $\sigma, \theta \in \sum \mathbb{R}[\mathbf{X}]^2$.

If $f^\star$ is reached on the ball $\overline{B}(0,R)$ then $f^{\mathsf{sos}} = \inf_{\overline{B}(0,R)} f(x) = f^\star$, so that this method allows to approximate $f^\star$.

Gradient variety.

Let $\nabla f = \left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right)$. Demmel, Nie and Sturmfels [101] proved the following result, that allows to approximate $\inf_{x \in \mathbb{V}(\nabla f)} f(x)$.

Theorem 3.12. *[101, Theorem 9] Let* $f \in \mathbb{R}[\mathbf{X}]$. *Then* $f \geq 0$ *over* $\mathbb{V}(\nabla f)$ *if and only if for all* $\varepsilon > 0$, $f + \varepsilon$ *can be written as*

$$f + \varepsilon = \sigma + \sum_{1 \leq i \leq n} \phi_i \frac{\partial f}{\partial X_i},$$

where $\sigma \in \sum \mathbb{R}[\mathbf{X}]^2$ *and* $\phi_i \in \mathbb{R}[\mathbf{X}]$.

If $f^\star$ is reached on $\mathbb{R}^n$, then it is at a critical point. In this case, $\inf_{x \in \mathbb{R}^n} f(x) = \inf_{x \in \mathbb{V}(\nabla f)} f(x)$. Then the above theorem make possible to compute an approximation of $f^\star$. However, the infimum $f^\star$ is not necessarily reached so that the approximation can be inaccurate.

Example 3.13. *Let* $f = (XY-1)^2 + X^2$. *Solving the system* $\frac{\partial f}{\partial X} = \frac{\partial f}{\partial Y} = 0$, *we get that* $\mathbb{V}(\nabla f) = \{(0,0)\}$. *Since* $f(0,0) = 1$, *this means that* $\inf_{x \in \mathbb{V}(\nabla f)} f(x) = 1$.

However, $f^\star = 0$. *Indeed, as a sum of squares,* $f \geq 0$. *Moreover, the sequence* $f\left(\frac{1}{k}, k\right) = \frac{1}{k^2}$ *tends to* 0 *when* k *tends to infinity, thus* $f^\star = 0$.

Gradient tentacle.

In [130, Theorem 9], real algebra tools from [129] generalizing Schmüdgen's Positivstellensatz are used to give the following characterization for the existence of certificates. Let S be the semi-algebraic set $\{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}$.

Notation 3.14. *In the sequel, we denote by*

- $R_\infty(f, S)$ *the set of values* $t \in \mathbb{R}$ *such that there exists a sequence* $(x_k)_{k \in \mathbb{N}} \subset S$ *such that* $\|x_k\| \underset{k \to +\infty}{\longrightarrow} \infty$ *and* $f(x_k) \underset{k \to +\infty}{\longrightarrow} t$,
- $S(\nabla f)$ *the set* $\left\{x \in \mathbb{R}^n \mid \|\nabla f(x)\|^2 \|x\|^2 \leq 1\right\}$.

Definition 3.15. *Let $f \in \mathbb{C}[\mathbf{X}]$. We denote by f_i its homogeneous component of degree i. The polynomial f has only isolated singularities at infinity if it is constant or if it has degree $d \geq 1$ and there are finitely many $z \in \mathbb{P}^{n-1}(\mathbb{C})$ such that*

$$\frac{\partial f_d}{\partial X_1}(z) = \cdots = \frac{\partial f_d}{\partial X_n}(z) = f_{d-1}(z) = 0.$$

Theorem 3.16. *[130, Theorem 9] Assume that f is bounded on S and that $R_\infty(f,S)$ is a finite subset of $]0,+\infty[$. Then $f > 0$ on S if and only if it can be written in the form*

$$f = \sum_{\delta \in \{0,1\}^s} \sigma_\delta f_1^{\delta_1} \dots f_s^{\delta_s},$$

where $\delta = (\delta_1, \dots, \delta_s)$ and $\sigma_\delta \in \sum \mathbb{R}[\mathbf{X}]^2$.

Applying this result, the following theorem is obtained.

Theorem 3.17. *[130, Theorem 25] Let $f \in \mathbb{R}[\mathbf{X}]$ bounded from below and assume that f has only isolated singularities at infinity or that $S(\nabla f)$ is compact. Then $f \geq 0$ on $\mathbb{R}^n$ if and only if for all $\varepsilon > 0$, $f + \varepsilon$ can be written*

$$f + \varepsilon = \sigma + \theta\left(1 - \|\nabla f(x)\|^2 \|x\|^2\right),$$

where $\sigma, \theta \in \sum \mathbb{R}[\mathbf{X}]^2$.

As far as we know, this result is the first one where $f^\star$ is not assumed to be reached over $\mathbb{R}^n$. It requires that f has only isolated singularities at infinity. According to a private communication with the author, the computation of certificates seems to work for polynomials that do not satisfy this assumption. However, since there is no proof of this fact, one can introduce the *higher gradient tentacles*. The gradient tentacle $S(\nabla f, N)$ of order N is defined as the semi-algebraic set $\left\{x \in \mathbb{R}^n \mid \|\nabla f(x)\|^{2N}\left(1 + \|x\|^2\right)^{N+1} \leq 1\right\}$. Then the analogous of Theorem 3.17, without the assumption on the number of isolated singularities at infinity, can be proved.

High order perturbation method.

This method, due to Lasserre [85], is more general than its previous "big ball" method since it does not require the assumption that $f^\star$ is reached. It is based on the following theorem.

Theorem 3.18. *[85, Theorem 4.1] Let $f \in \mathbb{R}[\mathbf{X}]$. Then $f \geq 0$ on $\mathbb{R}^n$ if and only if for all $\varepsilon > 0$, there exists $r \in \mathbb{N}$ such that*

$$f + \varepsilon \sum_{1 \leq i \leq n} \sum_{0 \leq k \leq r} \frac{X_i^{2k}}{k!} = \sigma,$$

where $\sigma \in \sum \mathbb{R}[\mathbf{X}]^2$.

Generalized critical values.

In [54], the notion of generalized critical values and Schweighofer's Theorem 3.16 are used. Furthermore, a method improving the convergence of the sum of squares relaxations when $f^\star$ is not attained on $\mathbb{R}^n$ is presented.

Theorem 3.19. *[54, Theorem 3.3] Let $f \in \mathbb{R}[\mathbf{X}]$. There exists a non-empty Zariski open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, $f^{\mathbf{A}} \geq 0$ on $\mathbb{R}^n$ if and only if for all $\varepsilon > 0$, $f^{\mathbf{A}} + \varepsilon$ can be written*

$$f^{\mathbf{A}} + \varepsilon = \sigma + \theta\left(M - f^{\mathbf{A}}\right) + \sum_{1 \leq i \leq n-1} \phi_i \frac{\partial f^{\mathbf{A}}}{\partial X_i}.$$

where $\sigma, \theta \in \sum \mathbb{R}[\mathbf{X}]^2$ and $M \in f(\mathbb{R}^n)$.

More precisely, computing certificates on $\mathbb{R}^n$ can be reduced to computing certificates on a set whose dimension is well controlled. The critical locus of f

$$W_0^{\mathbf{A}} = \left\{ x \in \mathbb{C},\ \frac{\partial f^{\mathbf{A}}}{\partial X_1}(x) = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n}(x) = 0 \right\}$$

and the constructible set

$$W_1^{\mathbf{A}} = \left\{ x \in \mathbb{C},\ \frac{\partial f^{\mathbf{A}}}{\partial X_1}(x) = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}}(x) = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n}(x) \neq 0 \right\}.$$

are considered.

According to [117], there exists a non-empty Zariski open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, the Zariski-closure of $W_1^{\mathbf{A}}$ has dimension 1. This implies that $R_\infty\left(f^{\mathbf{A}}, W_1^{\mathbf{A}}\right)$ is finite. The set $R_\infty\left(f^{\mathbf{A}}, W_0^{\mathbf{A}}\right)$ is a subset of the set of critical values of f, that is finite by Sard's theorem. Hence, Schweighofer's theorem can be applied on $W^{\mathbf{A}} = W_0^{\mathbf{A}} \cup W_1^{\mathbf{A}}$. To conclude, it is proved that finding the infimum on $W^{\mathbf{A}} \cap \mathbb{R}^n$ is equivalent to finding the one on $\mathbb{R}^n$.

Lemma 3.20. *([54, Lemma 3.1]) There exists a non-empty Zariski open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$,*

$$\inf_{x \in \mathbb{R}^n} f^{\mathbf{A}}(x) = \inf_{x \in W^{\mathbf{A}} \cap \mathbb{R}^n} f^{\mathbf{A}}(x).$$

Remark that Theorem 3.19 does not require that $f^\star$ is reached on $\mathbb{R}^n$.

3.3.2 Constrained Case

KKT ideals.

In this section, let $S = \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}$, where $f_i \in \mathbb{R}[\mathbf{X}]$. Demmel, Nie and Powers [39] generalized the gradient variety approach to get certificates of positivity over S.

Let $I_{KKT} \subset \mathbb{R}[\mathbf{X}, \lambda_1, \ldots, \lambda_s]$ be the Karush-Kuhn-Tucker ideal defined by

$$I_{KKT} = \left\langle \frac{\partial f}{\partial X_1} - \sum_{1 \leq j \leq s} \frac{\partial f_j}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} - \sum_{1 \leq j \leq s} \frac{\partial f_j}{\partial X_n}, \lambda_1 f_1, \ldots, \lambda_n f_n \right\rangle.$$

Theorem 3.21. *[39, Theorem 3.5] Let $f \in \mathbb{R}[\mathbf{X}]$. Then $f > 0$ over $\mathbb{V}(I_{KKT})$ if and only if for all $\varepsilon > 0$, $f + \varepsilon$ can be written as*

$$f + \varepsilon = \sum_{\delta \in \{0,1\}^s} \sigma_\delta f_1^{\delta_1} \ldots f_s^{\delta_s} + \sum_i \phi_i h_i,$$

where $\delta = (\delta_1, \ldots, \delta_s)$, $\sigma_\delta \in \sum \mathbb{R}[\mathbf{X}]^2$, $\phi_i \in \mathbb{R}[\mathbf{X}, \lambda_1, \ldots, \lambda_s]$ and $h_i \in \mathbb{R}[\mathbf{X}, \lambda_1, \ldots, \lambda_s]$ are the generators of I_{KKT}.

If $f^\star$ is reached, then it is reached at a KKT point. Thus, it is attained on $\mathbb{V}(I_{KKT})$ where the existence of certificates is ensured, so that $f^\star = \inf_{x \in \mathbb{V}(I_{KKT})} f(x)$ can be approximated by a sequence of SDP relaxations. However, as in Example 3.13, $f^\star$ may be a limit that is not reached. In this case, $f^\star \neq \inf_{x \in \mathbb{V}(I_{KKT})} f(x)$, so that the computed approximation may be far away from $f^\star$.

Truncated tangency variety.

Hà and Phạm [141] used Schweighofer's Theorem 3.16 to prove the existence of certificates with constraints.

In this section, let $S = \{x \in \mathbb{R}^n \mid g_i(x) = 0, 1 \leq i \leq l \text{ and } h_j(x) \geq 0, 1 \leq j \leq m\}$, where $g_i, h_j \in \mathbb{R}[\mathbf{X}]$.

Definition 3.22. *Let $J(x)$ be the set of indices j such that $h_j(x) = 0$. Then the set S is regular if all $x \in S$, for $1 \leq i \leq j$ and $j \in J(x)$, the vectors ∇g_i, ∇h_j are linearly independent.*

Theorem 3.23. *[141, Theorem 4.1] Let $f \in \mathbb{R}[\mathbf{X}]$ and $M \in f(\mathbb{R}^n)$ and assume that S is regular. Then $f \geq 0$ on S if and only if for all $\varepsilon > 0$,*

$$f + \varepsilon = \sigma + \theta(M - f) + \sum_{1 \leq i \leq l} \phi_i g_i + \sum_{1 \leq j \leq m} \tau_j h_j + \sum_{J \subset \{1, \ldots, m\}} \psi_J h_J p_{J^c},$$

where p_{J^c} is a polynomial constructed from the partial derivatives of f, g_i and some h_i. Moreover, $\sigma, \theta, \tau_j \in \sum \mathbb{R}[\mathbf{X}]^2$ and $\phi_i, \psi_J \in \mathbb{R}[\mathbf{X}]$.

In the above theorem, $f^\star$ is not assumed to be reached. In Section 7.2, we will also deal in the case where $f^\star$ is not necessarily reached. Indeed, we will prove the existence of certificates on a set on which the infimum is $f^\star$. Then even if if is not reached, this will allow to compute an approximation converging to $f^\star$. Furthermore, the new constraints we introduce and the certificates are simpler and with smaller degree than [141].

3.3.3 Existence of Rational Certificates

Since the methods and algorithms presented in Section 3.2.2 can be used to compute a rational certificate, we want to prove the existence of rational certificates instead of real certificates. For the univariate case, the existence of rational certificates is known, see [82, 106] and the algorithm in [128], presented in Section 3.2.2.

In the multivariate case, Sturmfels asked whether all polynomials with rational coefficients that are sums of squares in $\mathbb{R}[\mathbf{X}]$ are also sums of squares in $\mathbb{Q}[\mathbf{X}]$. Scheiderer gave a counterexample in [123]. However, the existence of rational sums of squares on a semi-algebraic set can be proved in some cases.

Rational Positivstellensatz. In [18, Theorem 4.1] a generalization of Schmüdgen's Positivstellensatz is given. The statement of Theorem 3.3 remains true when $\mathbb{R}[\mathbf{X}]$ is replaced by any affine algebra on a field K. In particular with $K = \mathbb{Q}$ and the affine algebra $\mathbb{Q}[\mathbf{X}]$, we get the following.

Theorem 3.24. *[18, Theorem 4.1, Corollary 4.4] Let* $f_1, \ldots, f_s \in \mathbb{Q}[\mathbf{X}]$ *and*

$$\mathcal{S} = \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}.$$

Assume that $\mathcal{S}$ *is* compact. *Then* $f > 0$ *on* $\mathcal{S}$ *if and only if* f *can be written in the form*

$$f = a + \sum_{\delta \in \{0,1\}^s} \sigma_\delta f_1^{\delta_1} \ldots f_s^{\delta_s},$$

where $0 < a \in \mathbb{Q}$, $\delta = (\delta_1, \ldots, \delta_s)$ *and* $\sigma_\delta \in \sum \mathbb{Q}[\mathbf{X}]^2$.

Likewise, a generalization of Putinar's Positivstellensatz is given in [69, Theorem 6]. The statement of Theorem 3.4 remains true when $\mathbb{R}[\mathbf{X}]$ is replaced by any affine algebra on an archimedean ordered field.

We recall that

$$M(\mathbf{F}) = \left\{ \sigma_0 + \sum_{1 \leq i \leq s} \sigma_i f_i \mid \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2 \right\}$$

is the quadratic module generated by $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$.

Then [69, Theorem 6] with $K = \mathbb{Q}$ and the affine algebra $\mathbb{Q}[\mathbf{X}]$ gives the following.

Theorem 3.25. *[69, Theorem 6] Let* $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ *and*

$$\mathcal{S} = \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}.$$

Assume that $M(\mathbf{F})$ *contains* $N - \sum_{1 \leq i \leq n} X_i^2$ *for some* $N \in \mathbb{N}$. *Then* $f > 0$ *on* $\mathcal{S}$ *if and only if* f *can be written in the form*

$$f = \sigma_0 + \sum_{1 \leq i \leq s} \sigma_i f_i + \sigma \left(N - \sum_{1 \leq i \leq n} X_i^2 \right),$$

where $\sigma_i, \sigma \in \sum \mathbb{Q}[\mathbf{X}]^2$.

These special cases of Jacobi's and Berr and Wörmann about rational certificates has also been presented in [107].

Sums of squares over totally real fields. Let K be a totally real number field. Then in [64], it is proved that if $f \in \mathbb{Q}[\mathbf{X}]$ is a sum of squares in $K[\mathbf{X}]$ then f is a sum of squares with rational coefficients. Furthermore, a results that ensure the existence of a rational sum of squares decomposition is given.

Let $f \in \mathbb{Q}[\mathbf{X}]$ of degree $2d$ and $N = \binom{n+d}{d}$ be the size of the vector z_d of all monomials of degree $\leq d$.

Theorem 3.26. *[64, Theorem 1.2] If there exists an invertible positive semidefinite matrix* $Q \in \mathrm{Sym}_N(\mathbb{R})$ *such that* $f = z_d^T Q z_d$ *then there exists a positive semidefinite matrix* $Q' \in \mathrm{Sym}_N(\mathbb{Q})$ *such that* $f = z_d^T Q' z_d$.

Then, the existence of rational sums of squares for polynomials in a totally real number field is given.

Theorem 3.27. *[64, Theorem 1.4] Let* K *be a totally real number field with Galois closure* L. *If* $f \in \mathbb{Q}[\mathbf{X}]$ *is a sum of* m *squares in* $K[\mathbf{X}]$, *then* f *is a sum of*

$$4m \cdot 2^{[L:\mathbb{Q}]+1} \binom{[L:\mathbb{Q}]+1}{2}$$

squares in $\mathbb{Q}[\mathbf{X}]$.

A refinement of this last result is presented in [112].

Theorem 3.28. *[112, Theorem 3.1] Let* K *be a totally real Galois extension of* $\mathbb{Q}$. *Let* $f \in \mathbb{Q}[\mathbf{X}]$ *be a sum of* m *squares in* $K[\mathbf{X}]$. *Then* f *is a sum of* $(4[K:\mathbb{Q}]-3).m$ *squares in* $\mathbb{Q}[\mathbf{X}]$.

Chapter 4

Polar Varieties

We present the polar varieties. Polar varieties have been introduced by Severi [132, 133] and Todd [139, 140] at the beginning of the century. Then, they have been studied in the context of computer algebra by Bank, Giusti, Heintz, Mbakop and Pardo (see e.g. [9, 11, 12] and [14]). Geometric objects close to the notion of polar varieties are used in [13] in the context of global optimization.

Given an algebraic variety V, the polar varieties are defined as the critical loci of the canonical projections restricted to V. Polar varieties are a core notion in real polynomial system solving. They have been studied in a computer algebra context in order to compute at least a point in each connected component of the real trace of an algebraic variety. Thus testing the emptiness of a real algebraic variety given by a polynomial equations can be done using polar varieties. In [9], the authors studied the case were the variety is a smooth hypersurface such that its real part is compact. Then in [11], the authors extend the properties of polar varieties to a real smooth and compact real variety, given by a reduced regular sequence. In [119], the compactness assumption is removed, replaced by an assumption of properness. This assumption can be ensured up to a generic change of coordinates. This leads to an algorithm singly exponential in the number of variables that compute a set of representative points of each connected component of a real algebraic variety. We present the results of [119] that will be used in our algorithms.

4.1 Definition and Properties

Regular and critical points. This section is devoted to define the critical points and critical values of a polynomial mapping defined on an algebraic variety.

The *Zariski-tangent space* to a variety V at $x \in V$ is the vector space T_xV defined by the equations

$$\frac{\partial f}{\partial X_1}(x)v_1 + \cdots + \frac{\partial f}{\partial X_n}(x)v_n = 0,$$

for all polynomials f that vanish on V.

Given a polynomial f, ∇f, is the gradient vector $\left(\frac{\partial f}{\partial X_1} \quad \dots \quad \frac{\partial f}{\partial X_n}\right)$. The Jacobian matrix of the system $\mathbf{F} = \{f_1, \dots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ is the $(s \times n)$-matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \cdots & \vdots \\ \frac{\partial f_s}{\partial X_1} & \cdots & \frac{\partial f_s}{\partial X_n} \end{bmatrix}.$$

This Jacobian matrix will be denoted by $\mathsf{Jac}(\mathbf{F}, \mathbf{X})$ or simply $\mathsf{Jac}(\mathbf{F})$. Likewise, $\mathsf{Jac}(\mathbf{F}, k)$ denotes the truncated Jacobian matrix of size $p \times (n - k + 1)$ with respect to the variables $X_k, \dots, X_n$.

Given a matrix M of size $s \times p$ and an integer $m \leq \min\{s, p\}$, we denote by $\mathsf{Minors}(M, m)$ the set of all minors of size $m \times m$ of M. In the sequel we assume that the polynomials in $\mathbf{F}$ generate a radical ideal and that the variety $\mathbb{V}(\mathbf{F})$ is equidimensional. Under these assumptions, the singular points are defined by polynomial equations.

Assume that V is equidimensional of dimension d and that the ideal $\langle \mathbf{F} \rangle$ is radical. The set of *singular points* in V is $\mathbb{V}(\mathbf{F}, \mathsf{Minors}(\mathsf{Jac}(\mathbf{F}), n - d))$. The *regular points* are all other points of V. We denote by $\mathrm{Reg}(V)$ the set of regular points of V and by $\mathrm{Sing}(V)$ its set of singular points. A variety V is smooth if $\mathrm{Sing}(V) = \varnothing$.

We can now define the critical points and critical values of a polynomial mapping f defined on an algebraic variety V. The set of critical points of $f_{|V}$, denoted by $\mathrm{Crit}(f, V)$, is the set of points in $\mathrm{Reg}(V)$ where the differential $d_x f \colon T_x(V) \to \mathbb{C}^n$ is not a surjection. A value $c \in \mathbb{R}$ is a critical value of $f_{|V \cap \mathbb{R}^n}$ if there exists a critical point $x_c \in V \cap \mathbb{R}^n$ such that $f(x_c) = c$.

Remark 4.1. *If the algebraic variety V is smooth then* $\mathrm{Crit}(f, V)$ *is the variety defined by* $\mathbf{F}$ *and* $\mathsf{Minors}(\mathsf{Jac}(f, \mathbf{F}), n - d + 1)$. *If V is not smooth, it defines the union* $\mathrm{Crit}(f, V) \cup \mathrm{Sing}(V)$.

The computation of the critical points is relevant when considering an optimization problem: it is well known that if a point $x \in V \cap \mathbb{R}^n$ is such that $f(x)$ is a local extremum then $x \in \mathrm{Crit}(f, V)$.

Moreover, according to Sard's theorem (algebraic version), the set of complex critical values is a 0-dimensional algebraic variety of $\mathbb{C}$. In other words, it is a finite algebraic set. The following statement is a consequence of [44, Corollary 16.23, p. 409].

Theorem 4.2 (Sard). *Let $f \colon V \longrightarrow \mathbb{C}$. Then the set of critical values of f is an algebraic variety strictly contained in $\mathbb{C}$.*

Projections. We will manipulate geometric object constructed as the critical locus of projections to linear subspaces, that we define now.

Given $1 \leq \ell \leq n$, let $\pi_{>\ell}$ be the projection

$$\begin{aligned} \pi_{>\ell} : \quad \mathbb{C}^n &\longrightarrow \mathbb{C}^{n-\ell} \\ (x_1, \dots, x_n) &\longmapsto (x_{\ell+1}, \dots, x_n) \end{aligned}.$$

Likewise, we define the projection $\pi_{\leq \ell}$

$$\begin{array}{rccc} \pi_{\leq \ell}: & \mathbb{C}^n & \longrightarrow & \mathbb{C}^\ell \\ & (x_1, \ldots, x_n) & \longmapsto & (x_1, \ldots, x_\ell) \end{array}.$$

Sometimes, we will keep the notation $\pi_{\leq \ell}$ for the projection

$$\begin{array}{rccc} \pi_{\leq \ell}: & \mathbb{C}^n \times \mathbb{C} & \longrightarrow & \mathbb{C}^\ell \times \mathbb{C} \\ & (x_1, \ldots, x_n, t) & \longmapsto & (x_1, \ldots, x_\ell, t) \end{array}.$$

Finally, if $\{X_{i_1}, \ldots, X_{i_s}\}$ is a subset of $\mathbf{X}$ then $\pi_{X_{i_1},\ldots,X_{i_s}}$ denotes the projection

$$\begin{array}{rccc} \pi_{X_{i_1},\ldots,X_{i_s}}: & \mathbb{C}^n & \longrightarrow & \mathbb{C}^s \\ & (x_1, \ldots, x_n) & \longmapsto & (x_{i_1}, \ldots, x_{i_s}) \end{array}.$$

Change of coordinates. The correctness of the results presented in Chapters 5, 6 and 7 depends on some properties that are satisfied up to a generic change of variables. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$. In this thesis, we denote by $f^{\mathbf{A}}$ the polynomial $f\left(\mathbf{A}\mathbf{X}^T\right)$ and $\mathbf{F}^{\mathbf{A}}$ the set $\{f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}\}$. Likewise, if $V = \mathbb{V}(\mathbf{F})$ then $V^{\mathbf{A}}$ is the algebraic variety $\mathbb{V}\left(\mathbf{F}^{\mathbf{A}}\right)$.

Polar varieties. Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ and $V = \mathbb{V}(\mathbf{F})$. The polar varieties associated with V are defined as critical loci of projections to linear subspaces. In order to compute these critical loci, one assumes that $\langle \mathbf{F} \rangle$ is a radical ideal and that V is smooth and equidimensional of dimension d.

Under these assumptions, we are able to define the polar varieties by polynomial equations constructed from the input system $\mathbf{F}$.

Definition 4.3 (Polar variety)**.** *For $1 \leq i \leq d$, let $\Delta_i = \langle \mathbf{F}, \mathsf{Minors}(\mathsf{Jac}(\mathbf{F}, i+1), n-d) \rangle$, that is the ideal defining the critical locus of $\pi_{\leq i}$ restricted to V.*

The $(d+1)$-th polar variety W_{d+1}, by convention, is V itself. For $1 \leq i \leq d$, the i-th polar variety is $W_i = \mathbb{V}(\Delta_i)$.

Remark 4.4. *Under the assumptions that $\langle \mathbf{F} \rangle$ is radical and that V is smooth and equidimensional of dimension d, the polar variety W_i is the critical locus of*

$$\begin{array}{rccc} \pi_{\leq i}: & V & \longrightarrow & \mathbb{C} \\ & (x_1, \ldots, x_n) & \longmapsto & (x_1, \ldots, x_i) \end{array}.$$

We refer to [11] for the results on the dimension and properties of polar varieties when $V \cap \mathbb{R}^n$ is assumed to be compact.

We focus on the generalization in [119]. The compactness assumption is replaced with an assumption of properness of canonical projections.

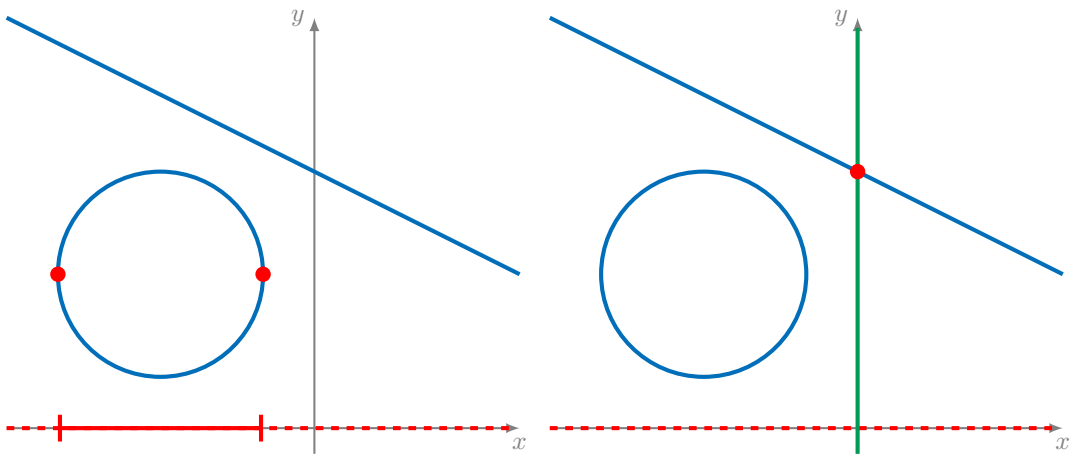
Theorem 4.5. *[119, Theorem 2] Assume that W_1 has dimension at most 0 and that for $1 \leq i \leq d$, the restriction of $\pi_{\leq i}$ to W_{i+1} is proper. Then each $W_i \cap \mathbb{V}(\mathbf{X}_{\leq i})$ is empty or 0-dimensional.*

Furthermore, the union $\bigcup_{1 \leq i \leq d+1} W_i \cap \mathbb{V}(\mathbf{X}_{\leq i})$ meets every connected component of $V \cap \mathbb{R}^n$.

Example 4.6. *Consider the algebraic variety defined as the union of the circle and the line drawn in Figure 4.1. Consider the projection of this variety to the x-axis, that is proper.*

The projection of the circle has two critical points, at each extremity (Figure 4.1(a)). Then the polar variety W_1, that is the union of these two points, is 0-dimensional and contains at least one point in the circle.

The projection of the line has no critical points. This means that the image of the projection is the entire x-axis. Therefore, the intersection of this line with any line orthogonal to the x-axis is non-empty. Hence, $W_2 \cap \mathbb{V}(x)$ is 0-dimensional and contains a point in the line (Figure 4.1(b)).



(a) Critical points of the projection to x. (b) Intersection with the y-axis.

Figure 4.1: Polar varieties with properness.

Remark 4.7. *The properness assumption is required. Consider the hyperbola in Figure 4.2. Its projection to the x-axis is the x-axis without the origin, that is a point of non-properness. Hence, the intersection of the hyperbola with the y-axis $\mathbb{V}(x)$ is empty.*

Nevertheless, after a generic change of coordinates, the projection is on another axis, that is proper. Then the situation is reduced to one of those of Example 4.6. If the new projection has no critical points, because of the properness, the intersection of the hyperbola with any line orthogonal to the axis of projection is non-empty and meets each connected component of the hyperbola (Figure 4.3(a)). If the new projection has critical points, then each connected component contains such a critical point (Figure 4.3(b)).

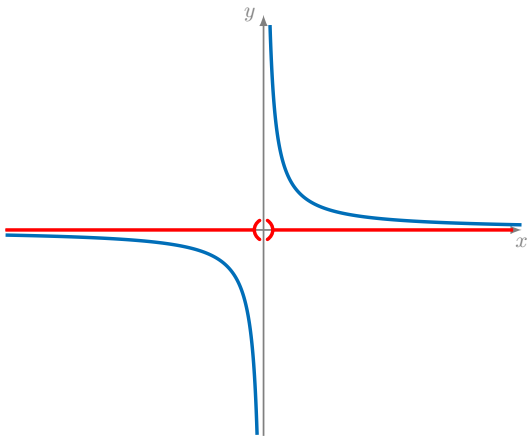
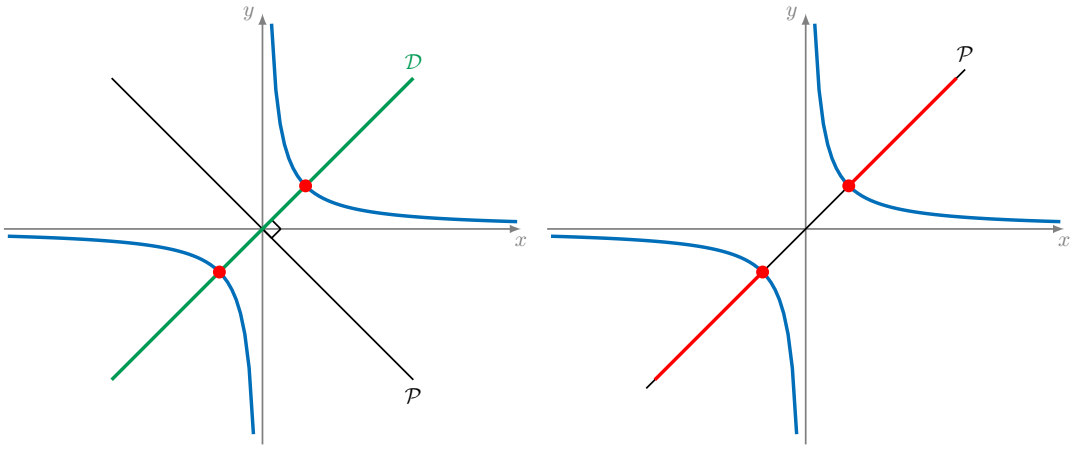


Figure 4.2: Polar varieties without properness: no critical point for the projection to x but the projection is not the entire axis.



(a) No critical points but any line $\mathcal{D}$ orthogonal to the axis of projection $\mathcal{P}$ meets each connected component of the variety.

(b) Critical points for the projection to $\mathcal{P}$, at least one in each connected component of the variety.

Figure 4.3: Polar varieties after a generic change of coordinates.

It is known (see for instance [42, Section 2.4]) that the Noether position can be obtained by performing a generic linear change of coordinates. Then from Proposition 1.14, this means that the properness of a projection to a linear subspace is a generic property.

However in Theorem 4.5, it is necessary to obtain a change of coordinates that gives the properness of each projection.

The following ensures that assuming the properness of all projections is not a loss of generality since it can always be ensured, up to a linear change of coordinates.

Theorem 4.8. *[119, Theorem 1] There exists a Zariski-open set* $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ *such that for all* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, $W_1^{\mathbf{A}}$ *has dimension at most* 0 *and that for* $1 \leq i \leq d$, *the restriction of* $\pi_{\leq i}$ *to* $W_{i+1}^{\mathbf{A}}$ *is proper.*

4.2 Computing a set of Sample Points

Given a variety V, a set of sample points of $V \cap \mathbb{R}^n$ is a finite set that contains at least one point in each connected component of $V \cap \mathbb{R}^n$.

From Theorem 4.5 and Theorem 4.8, the computation of a set of sample points of $V \cap \mathbb{R}^n$ is reduced to compute the solutions of a 0-dimensional system in generic coordinates. It can be done using Gröbner bases but to obtain a complexity estimate, the computations can be performed by the geometric resolution algorithm.

Theorem 4.9. *([119, Theorem 1]) There exists a probabilistic algorithm computing a geometric resolution of a* 0*-dimensional set containing at least one point in each connected component of* $V \cap \mathbb{R}^n$. *Its complexity is* singly exponential *in the number of variables.*

An implementation based on the results presented in this section is distributed in the Maple package RAGlib by Safey El Din. This Maple package can be downloaded at `http://www-polsys.lip6.fr/~safey/RAGLib/`. It relies on the computation of suitable sections of polar varieties. These sections are computed with Gröbner bases, using Faugère's FGb package, available at `http://www-polsys.lip6.fr/~jcf/Software/FGb/`.

Part II

Contributions

Chapter 5

Modified Polar Varieties

5.1 Introduction

This chapter is part of the submitted paper [52]. It contains a strong generalization of [51], where geometric results used to test the reachability of the global infimum of a polynomial on $\mathbb{R}^n$ are presented.

Motivation and prior work

Let $f, f_1, \ldots, f_s$ be n-variate polynomials with rational coefficients. For the moment, we assume that the ideal $\langle f_1, \ldots, f_s \rangle$ is radical and that $V = \mathbb{V}(f_1, \ldots, f_s)$ is equidimensional with finitely many singular points. Let $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x)$. Recall that our goal in this thesis is to solve problems:

(A) Computing certificates for lower bounds on $f^\star$.

(B) Deciding the finiteness and computing an algebraic representation of $f^\star$.

(C) Deciding whether there exists $x^\star \in V \cap \mathbb{R}^n$ such that $f(x^\star) = f^\star$ and computing a rational parametrization of $x^\star$.

In this context, the set of critical values of the restriction of f to $V \cap \mathbb{R}^n$ plays a crucial role. Indeed, if $f^\star$ is reached, then it is a critical value. However, consider the polynomial $f = (xy-1)^2 + x^2$ on $\mathbb{R}^n$. Its set of critical values is $\{1\}$. Since $f\left(k/\left(1+k^2\right), k\right) \underset{k \to +\infty}{\longrightarrow} 0$ and $f \geq 0$ as a sum of squares, we see that $f^\star = 0$, that is not a critical value. This is actually a real *asymptotic critical value*. A value $c \in \mathbb{R}$ is an asymptotic critical value if there exists a sequence $(x_k)_{k \in \mathbb{N}} \subset \mathbb{R}^n$ such that $f(x_k) \underset{k \to +\infty}{\longrightarrow} c$, $\|x_k\| \underset{k \to +\infty}{\longrightarrow} \infty$ and for all $(i,j) \in \{1, \ldots, n\}^2$, $\|X_i(x_k)\| \left\| \frac{\partial f}{\partial X_j}(x_k) \right\| \underset{k \to +\infty}{\longrightarrow} 0$. This notion is introduced in [72, 81].

Asymptotic critical values are taken into account in [118] to solve problem (B), where $f^\star = \inf_{x \in \mathbb{R}^n} f(x)$. It is proved that $f^\star$ is either a critical value or an asymptotic critical value. To compute these values, an algebraic set of dimension 1 is constructed. Then

computing asymptotic critical values is reduced to computing the set of non-properness of the restriction of a projection to this algebraic set of dimension 1.

To solve problem (A) without assuming that $f^\star$ is reached, Schweighofer's results [130] can be used. They ensure the existence of certificates under the assumption that f has finitely many asymptotic values. This is done in [54] to prove the existence of certificate on $\mathbb{R}^n$. To this end, an algebraic variety C such that $\inf_{x\in\mathbb{R}^n} f(x) = \inf_{x\in C\cap\mathbb{R}^n} f(x)$ is constructed. Furthermore, C is the union of the critical locus of f and an algebraic set of dimension one. This is sufficient to prove that f has finitely many asymptotic values on $C\cap\mathbb{R}^n$.

Solving problem (C) can be done by computing at least one point in each connected component of $\mathrm{Crit}(f,V)\cap\mathbb{R}^n$. Nevertheless, efficient methods based on polar varieties [9, 11, 119] require some properties of regularity. These properties can not be ensured for $\mathrm{Crit}(f,V)$ so that these methods can not be applied to answer this question. We give a first answer in [51] to compute a minimizer when $f^\star = \inf_{x\in\mathbb{R}^n} f(x)$ is reached. To this end, we construct a set that is generically finite and that intersect each connected component of $\mathrm{Crit}(f)\cap\mathbb{R}^n$.

We see that the common idea is to reduce the original problem to an equivalent problem on a set of smaller dimension, on which asymptotic phenomena are well controlled. This chapter is devoted to construct an algebraic set $\mathscr{C}(f,\mathbf{F})\subset V$ such that $f^\star = \inf_{x\in\mathscr{C}(f,\mathbf{F})\cap\mathbb{R}^n}$ and such that $\overline{\mathscr{C}(f,\mathbf{F})\setminus\mathrm{Crit}(f,V)}^{\mathcal{Z}}$ has dimension 1. Since $f^\star = \inf_{x\in\mathscr{C}(f,\mathbf{F})\cap\mathbb{R}^n}$, computing the infimum of f on $V\cap\mathbb{R}^n$ is equivalent to computing it on $\mathscr{C}(f,\mathbf{F})\cap\mathbb{R}^n$. Since $\overline{\mathscr{C}(f,\mathbf{F})\setminus\mathrm{Crit}(f,V)}^{\mathcal{Z}}$ has dimension 1, asymptotic phenomena and computation of minimizers can be managed on $\mathscr{C}(f,\mathbf{F})$.

Problem statement

Let $f\in\mathbb{Q}[\mathbf{X}]$ and let $\mathbf{F}=\{f_1,\ldots,f_s\}\subset\mathbb{Q}[\mathbf{X}]$. The problem in this chapter is to construct a new algebraic set $\mathscr{C}(f,\mathbf{F})$ such that

- $f^\star = \inf_{x\in V\cap\mathbb{R}^n} f(x) = \inf_{x\in\mathscr{C}(f,\mathbf{F})\cap\mathbb{R}^n} f(x)$,
- $\overline{\mathscr{C}(f,\mathbf{F})\setminus\mathrm{Crit}(f,V)}^{\mathcal{Z}}$ has dimension at most 1,
- $\overline{\mathscr{C}(f,\mathbf{F})\setminus\mathrm{Crit}(f,V)}^{\mathcal{Z}}\cap\mathrm{Crit}(f,V)$ has dimension at most 0 and contains at least one point in each connected component of $\mathrm{Crit}(f,V)\cap\mathbb{R}^n$.

To this end, it is natural to consider some objects related to polar varieties. Indeed, the dimension of the polar varieties is well controlled while information about the original object are kept (see Chapter 4). We use geometric objects which are close to the notion of polar varieties. We refer to [13] for geometric objects similar to the ones we manipulate in a more restrictive context.

Main results

Let $f \in \mathbb{Q}[\mathbf{X}]$ and let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ such that the ideal $\langle \mathbf{F} \rangle$ is radical and the variety $V = \mathbb{V}(\mathbf{F})$ is d-equidimensional with finitely many singular points.

We define the modified polar varieties as follows: for $1 \leq i \leq d-1$, let $\mathscr{C}(f, \mathbf{F}, i)$ be the algebraic variety defined as the vanishing set of

- the polynomials in $\mathbf{F}$,
- the minors of size $n-d+1$ of $\mathsf{Jac}([f, \mathbf{F}], i+1)$,
- and the variables $X_1, \ldots, X_{i-1}$.

By convention, $\mathscr{C}(f, \mathbf{F}, d) = V \cap \mathbb{V}(X_1, \ldots, X_{d-1})$. Let $\mathscr{C}(f, \mathbf{F})$ be the union

$$\mathscr{C}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{C}(f, \mathbf{F}, i).$$

Then we are able to prove the following, that is a summary of Theorems 5.9, 5.11 and 5.12 page 65.

Theorem 5.1. *There exists a non-empty Zariski-open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$,*

- $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x) = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$,
- $\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}}$ *has dimension at most* 1,
- $\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, F^{\mathbf{A}}\right)$ *has dimension at most* 0 *and contains, for each critical value of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$* that is not isolated *in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, at least one corresponding critical point.*

Note that we are able to compute critical points associated with critical values that are not isolated. However, critical points associated with isolated critical values can be obtained by computing a point in each connected component of $V \cap \mathbb{R}^n$ (see Proposition 6.7).

Furthermore, Proposition 5.22 page 76 gives a bound on the maximum geometric degree attained in the computation of each modified polar variety. More precisely, given a variety $V = \mathbb{V}(g_1, \ldots, g_p)$, we denote by $\delta(V)$ the maximum of the degrees $\deg(V(g_1, \ldots, g_i))$, for $1 \leq i \leq p$. Then the following is obtained. Remark that this bound in singly exponential in the number of variables.

Proposition 5.2. *For all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, for $1 \leq i \leq d$, $\delta\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ and $\delta\left(\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)\right)$ are bounded by*

$$D\left((n-d+1)(D-1)\right)^n.$$

Organization of the chapter

In Section 5.2, we define the modified polar varieties $\mathscr{C}(f, \mathbf{F}, i)$ and their union $\mathscr{C}(f, \mathbf{F})$. Section 5.3 is devoted to state and prove the properties of our modified polar varieties. We prove that for a generic matrix $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, $f^\star = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$. Then we prove that the dimension of $\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}}$ is at most one. Furthermore, the algebraic set

$$\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, F^{\mathbf{A}}\right)$$

is finite and contains at least one critical point for each critical value of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ that is not an isolated value in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$.

Finally, we give bounds on the maximum geometric degree attained in the computation of the modified polar varieties in Section 5.4. It will be useful in order to estimate the complexity of the algorithms, since it depends on these degrees.

5.2 Definition

We define the modified polar varieties. In order to obtain the expected properties and to be able to perform computations, we make some assumptions on the input set of polynomials $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$. Then we give an algebraic definition of our modified polar varieties. Finally, we explain the geometric meaning of these definitions and the connection with the classical polar varieties.

Notation 5.3. *A set $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ is said to satisfy assumptions $\mathbf{R}$ if:*

- *the ideal $\langle \mathbf{F} \rangle$ is radical,*
- *the variety $V = \mathbb{V}(\mathbf{F}) \subset \mathbb{C}^n$ is equidimensional of dimension $d > 0$,*
- *$V = \mathbb{V}(\mathbf{F})$ has finitely many singular points.*

In this thesis, we fix $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$ so that the definitions of regular, singular, critical points, etc. as solutions of polynomial systems given in Section 4.1 can be used.

Definition 5.4. *For $1 \leq i \leq d-1$, let $\mathscr{C}(f, \mathbf{F}, i)$ be the algebraic variety defined as the vanishing set of*

- *the polynomials in $\mathbf{F}$,*
- *the minors of size $n - d + 1$ of $\mathsf{Jac}([f, \mathbf{F}], i+1)$,*
- *and the variables $X_1, \ldots, X_{i-1}$.*

By convention, $\mathscr{C}(f, \mathbf{F}, d) = V \cap \mathbb{V}(X_1, \ldots, X_{d-1})$. *Let* $\mathscr{C}(f, \mathbf{F})$ *be the union*

$$\mathscr{C}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{C}(f, \mathbf{F}, i).$$

For $1 \leq i \leq d-1$, *let* $\mathscr{P}(f, \mathbf{F}, i) = \overline{\mathscr{C}(f, \mathbf{F}, i) \setminus \mathrm{Crit}(f, V)}^{\mathcal{Z}} \cap \mathrm{Crit}(f, V)$. *For* $i = d$, *let* $\mathscr{P}(f, \mathbf{F}, d) = \mathscr{C}(f, \mathbf{F}, d)$. *Finally, let*

$$\mathscr{P}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{P}(f, \mathbf{F}, i).$$

Example 5.5. *Let* $f = x_2 \in \mathbb{Q}[x_1, x_2, x_3]$ *and* $V = \mathbb{V}\left(x_1^2 + x_2^2 + (x_3 - 1)^2 - 1\right)$. *The first modified polar variety,* $\mathscr{C}(f, \mathbf{F}, 1)$, *is the variety* $\mathbb{V}\left(x_1^2 + x_2^2 + (x_3 - 1)^2 - 1, x_3 - 1\right)$, *of dimension* 1 *(see Figure 5.1(a)).*

The second modified polar variety is $\mathscr{C}(f, \mathbf{F}, 2) = \mathbb{V}\left(x_1^2 + x_2^2 + (x_3 - 1)^2 - 1, x_1\right)$, *of dimension* 1 *(see Figure 5.1(b)).*

Remark that the critical locus of $f_{|V \cap \mathbb{R}^n}$, *that is* $\{(0, 1, 1), (0, -1, 1)\}$ *is contained in each modified polar variety.*

Remark 5.6. *Since the critical locus* $\mathrm{Crit}(f, V)$ *is the algebraic variety defined by* $\mathbf{F}$ *and the minors of size* $n - d + 1$ *of* $\mathsf{Jac}([f, \mathbf{F}])$, *if* $x \in \mathrm{Crit}(f, V)$ *then any minor of size* $n - d + 1$ *of* $\mathsf{Jac}([f, \mathbf{F}], i + 1)$ *vanish at* x. *In particular, under assumptions* $\mathbf{R}$,

$$\mathrm{Crit}(f, V) \subset \mathscr{C}(f, \mathbf{F}, 1).$$

Definition 5.7. *For* $1 \leq i \leq d$, *let* $\mathscr{P}(f, \mathbf{F}, i) = \overline{\mathscr{C}(f, \mathbf{F}, i) \setminus \mathrm{Crit}(f, V)}^{\mathcal{Z}} \cap \mathrm{Crit}(f, V)$ *and let* $\mathscr{P}(f, \mathbf{F})$ *be the union*

$$\mathscr{P}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{P}(f, \mathbf{F}, i).$$

Example 5.8. *Let* $f = x_2 \in \mathbb{Q}[x_1, x_2, x_3]$ *and* $V = \mathbb{V}\left(x_1^2 + x_2^2 + (x_3 - 1)^2 - 1\right)$ *as in Example 5.5. Then* $\mathscr{P}(f, \mathbf{F}, 1)$, *is the variety*

$$\mathbb{V}\left(x_1^2 + x_2^2 + (x_3 - 1)^2 - 1, x_3 - 1, x_1\right) = \{(0, 1, 1), (0, -1, 1)\}.$$

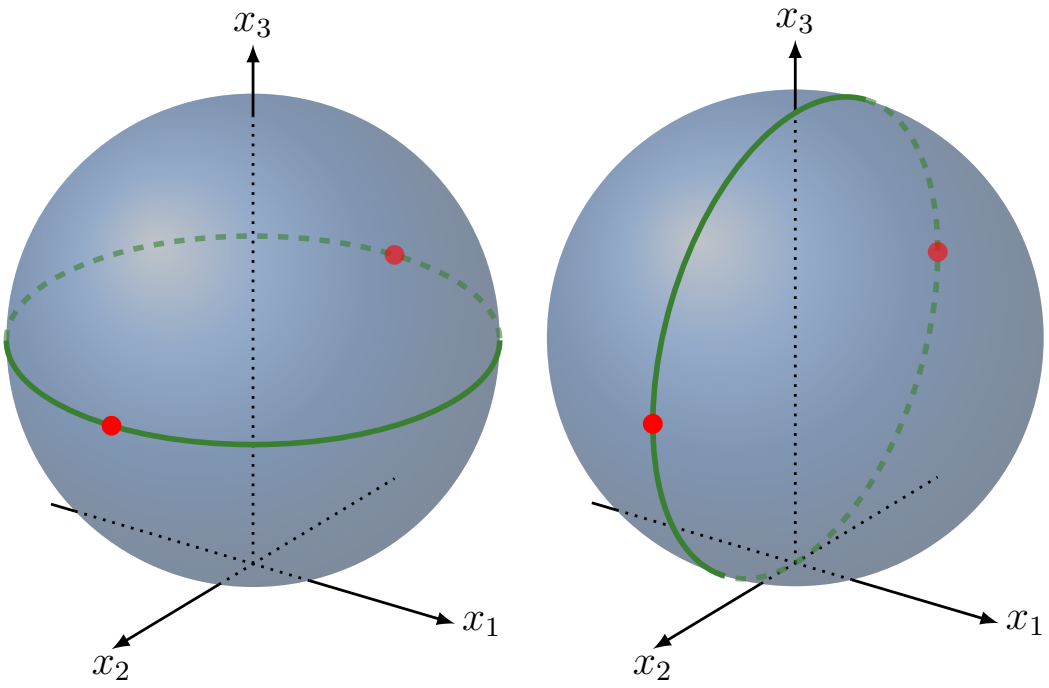
Its dimension is 0 *and it contains all the critical points of* $f_{|V \cap \mathbb{R}^n}$.

In this example, $\mathscr{P}(f, \mathbf{F}, 2) = \mathscr{P}(f, \mathbf{F}, 1)$. *Then the union* $\mathscr{P}(f, \mathbf{F}, 1) \cup \mathscr{P}(f, \mathbf{F}, 2)$ *contains at least one critical point for each critical value of* $f_{|V \cap \mathbb{R}^n}$. *We prove in the next section that it is always true up to a generic change of coordinates.*

In this Section, $\pi_{\leq i}$ stands for the projection, where T is a new indeterminate,

$$\pi_{\leq i} : \begin{array}{l} \mathbb{V}(f - T) \cap V \longrightarrow \mathbb{C}^{i+1} \\ (x_1, \ldots, x_n, t) \longmapsto (x_1, \ldots, x_i, t). \end{array}$$

Remark that since $\mathbf{F}$ satisfies assumptions $\mathbf{R}$, the variety $\mathscr{C}(f, \mathbf{F})$ is the union of



(a) $\mathscr{C}(f, \mathbf{F}, 1)$ (b) $\mathscr{C}(f, \mathbf{F}, 2)$

Figure 5.1: Modified polar varieties for $f = x_2$ and $\mathbf{F} = \left\{x_1^2 + x_2^2 + (x_3 - 1)^2 - 1\right\}$. The two points are the critical points of $f_{|V \cap \mathbb{R}^n}$.

- the set of singular points $\pi_{\mathbf{X}}(\mathrm{Sing}(V \cap \mathbb{V}(f - T))) = \mathrm{Sing}(V)$,
- the projection to $\mathbf{X}$ of the intersection of the linear subspace $\mathbb{V}(X_1, \ldots, X_i)$ and the critical locus of the projection $\pi_{\leq i}$ restricted to $V \cap \mathbb{V}(f - T)$, for $1 \leq i \leq d$.

Roughly speaking, the idea is to consider the section of the polar varieties of $V \cap \mathbb{V}(f - T)$ with linear subspaces, where T is a parameter, in order to obtain at least one point in each connected component of $V \cap \mathbb{V}(f - T) \cap \mathbb{R}^n$. Then we project on $\mathbf{X}$ in order to eliminate the parameter T, so that we obtain an object that contains information about the values of the objective polynomial f.

Moreover, $\mathscr{P}(f, \mathbf{F})$ is the intersection of $\mathrm{Crit}(f, V)$ and the components of $\mathscr{C}(f, \mathbf{F})$ that are not included in $\mathrm{Crit}(f, V)$.

5.3 Generic Properties

In this section the properties that will be used to solve optimization problems (A), (B) and (C) are stated. We first show that the original problem can be reduced to an optimization problem on the union of the modified polar varieties. Then we explain how to compute,

using these modified polar varieties, at least one critical point for each critical value. It will be useful in order to test whether $f^\star$ is reached or not. Finally, we state the results about the dimension of our objects. The proofs of these results are given in Section 5.3.2.

5.3.1 Statements

Theorem 5.9. *There exists a non-empty Zariski-open set $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, there exists a non-empty Zariski-open set $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ such that for all $t \in \mathbb{R} \cap \mathcal{Q}^{\mathbf{A}}$, $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ is empty if and only if $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ is empty too.*

This theorem ensures that the computation of $f^\star$ can be done on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ instead of $V^{\mathbf{A}} \cap \mathbb{R}^n$. Indeed, assume first that $f^\star$ is reached. It is then necessarily a critical value. By Remark 5.6, the critical points lie in $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, so that $f^\star = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$. If $f^\star$ is not reached, it is the limit of an infinite sequence of points in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$. By the above Theorem 5.9, up to removing the values in $\mathbb{R} \setminus \mathcal{Q}^{\mathbf{A}}$, that are finitely many, this sequence lies in $f^{\mathbf{A}}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n\right)$. Then $f^\star$ is in the closure (for the strong topology) of $f^{\mathbf{A}}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n\right)$, thus in this case, we also have

$$f^\star = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x).$$

Example 5.10. *Let $f = x_2 \in \mathbb{Q}[x_1, x_2, x_3]$ and $V = \mathbb{V}\left(x_1^2 + x_2^2 + (x_3 - 1)^2 - 1\right)$ as in Example 5.5 63. One can check on Figure 5.2(a) that for all $t \in \mathbb{R}$, $V \cap \mathbb{V}(f - t) \cap \mathbb{R}^n$ is empty if and only if $\mathscr{C}(f, \mathbf{F}) \cap \mathbb{V}(f - t) \cap \mathbb{R}^n$.*

The following shows that computing critical points of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ that correspond to non-isolated critical values can be reduced to computing critical points in $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ instead of $V^{\mathbf{A}} \cap \mathbb{R}^n$.

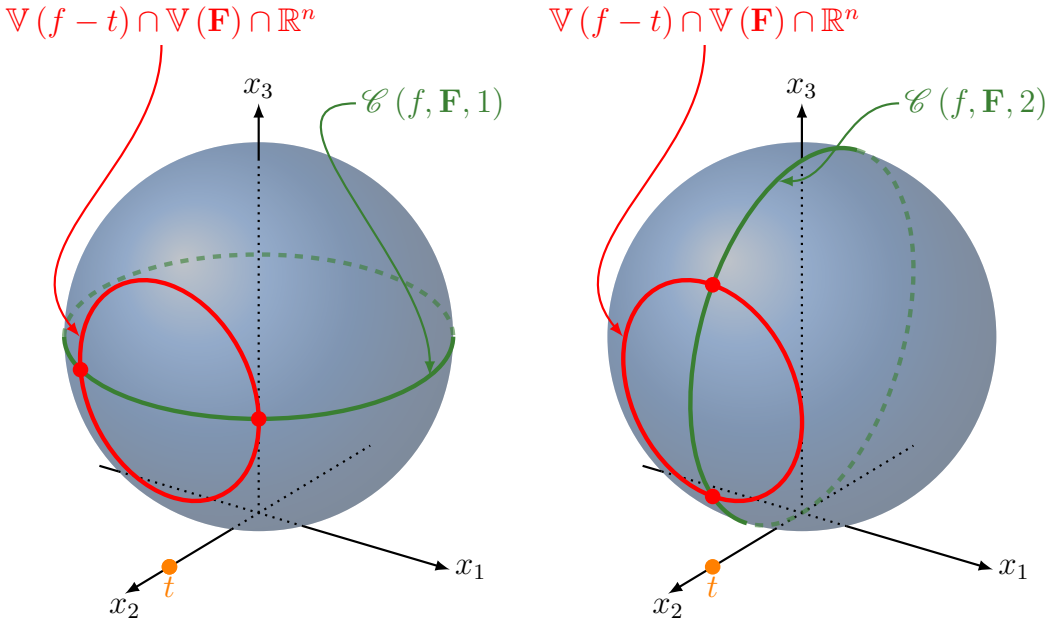
Theorem 5.11. *There exists a non-empty Zariski-open set $\mathscr{O}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$, for any critical value c of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ that is not isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, there exists $x_c \in \mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ such that $f^{\mathbf{A}}(x_c) = c$.*

We will see in Chapter 6 that the values corresponding to isolated critical values can be reached by computing at least one point in each connected component of $V \cap \mathbb{R}^n$.

Finally, the dimensions of the objects are known.

Theorem 5.12. *There exists a non-empty Zariski-open set $\mathscr{O}_3 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_3$,*

- $\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}}$ *has dimension at most* 1,
- $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ *has dimension at most* 0.



(a) $\mathscr{C}(f,\mathbf{F},1)$ (b) $\mathscr{C}(f,\mathbf{F},2)$

Figure 5.2: $V\cap\mathbb{V}(f-t)\cap\mathbb{R}^n$ is empty if and only if $\mathscr{C}(f,\mathbf{F})\cap\mathbb{V}(f-t)\cap\mathbb{R}^n$.

5.3.2 Proofs

Proof of Theorem 5.9.

This proof has been published in [53] in the case where $\mathbf{F}$ is supposed to define a smooth variety. It is a generalization of [119].

We first prove intermediate results before concluding with the proof of Theorem 5.9.

Lemma 5.13. *Let $\mathbf{F}\subset\mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$. For all real number t not in $f(\mathrm{Crit}(f,V)\cup\mathrm{Sing}(V))$,*

- *$\mathbb{V}(\mathbf{F},f-t)$ is either empty or equidimensional of dimension $d-1$,*
- *$\mathbb{V}(\mathbf{F},f-t)$ is smooth,*
- *the ideal $\langle\mathbf{F},f-t\rangle$ is radical.*

Proof. Let $t\in\mathbb{R}\setminus f(\mathrm{Crit}(f,V)\cup\mathrm{Sing}(V))$. Since $\pi_{\mathbf{X}}(\mathrm{Sing}(V\cap\mathbb{V}(f-T)))=\mathrm{Sing}(V)$ and $t\notin f(\mathrm{Crit}(f,V)\cup\mathrm{Sing}(V))$, t is neither a value of f at a point in

$$\pi_{\mathbf{X}}(\mathrm{Sing}(V\cap\mathbb{V}(f-T)))$$

nor a critical value of f. Then at every $(x,t=f(x))\in V\cap\mathbb{V}(f-t)$, the matrix $\mathsf{Jac}([\mathbf{F},f-t])$ has rank $n-d+1$. Let Z_t be an irreducible component of $V\cap\mathbb{V}(f-t)$.

Then, there exists an irreducible component Z of V such that Z_t is an irreducible component of $Z \cap \mathbb{V}(f-t)$. Since assumptions **R** is satisfied, V is equidimensional of dimension d so that Z has dimension d. Remark that since t is not a critical value of $f_{|V\cap\mathbb{R}^n}$, $Z \not\subset \mathbb{V}(f-t)$. By Krull's Principal Ideal Theorem [79, Corollary 3.2 p. 131], this means that Z_t is either empty or is equidimensional of dimension $d-1$. Since $V \cap \mathbb{V}(f-t)$ has finitely many irreducible components, this proves that for all $t \in \mathbb{R} \setminus f(\mathrm{Crit}(f,V) \cup \mathrm{Sing}(V))$, $V \cap \mathbb{V}(f-t)$ is either empty or equidimensional of dimension $d-1$.

To prove that $\mathbb{V}(\mathbf{F}, f-t)$ is smooth, remark that x is a singular point of $\mathbb{V}(\mathbf{F}, f-t)$ if and only $\mathsf{Jac}(f,\mathbf{F})$ has a rank defect at x. In other words, x is a singular point of $\mathbb{V}(\mathbf{F}, f-t)$ if and only if it is a singular point of V or a point such that $t = f(x)$ is a critical value of $f_{|V}$. This is not possible since $t \in \mathbb{R} \setminus f(\mathrm{Crit}(f,V) \cup \mathrm{Sing}(V))$.

To prove that $I_t = \langle \mathbf{F}, f-t\rangle$ is radical, assume that $I_t \neq \langle 1\rangle$ (otherwise the announced claim is immediate). Let $I_t = Q_1 \cap \cdots \cap Q_r \cap Q_{r+1} \cap \cdots \cap Q_s$ be a minimal primary decomposition of I_t. We assume that the Q_i's are isolated for $0 \leq i \leq r$. It is then sufficient to prove that for $1 \leq i \leq r$, Q_i is a prime ideal.

Let $i \in \{1,\ldots,r\}$. There exists $x \in \mathbb{V}(Q_i)$ such that $x \notin \mathbb{V}\left(\bigcap_{i\neq j} Q_j\right)$. Let $\mathfrak{m}$ be the maximal ideal at x. For an ideal I (resp. a ring R), we denote by $I_\mathfrak{m}$ (resp. $R_\mathfrak{m}$) its localization at $\mathfrak{m}$.

Since $V \cap \mathbb{V}(f-t)$ is smooth, $\mathsf{Jac}([\mathbf{F}, f-t])$ has rank $n-d+1$ at all points of $V \cap \mathbb{V}(f-t)$. According to [44, Theorem 16.19, Chapter 16, p. 404], $\dfrac{\mathbb{Q}[X_1,\ldots,X_n]_\mathfrak{m}}{(I_t)_\mathfrak{m}}$ is a regular ring. Hence, by [7, Lemma 11.23 p. 123]), it is integral, which implies that the ideal $(I_t)_\mathfrak{m}$ is prime. Note that, since Q_i is the unique isolated primary component contained in $\mathfrak{m}$, the following equalities hold:

$$(I_t)_\mathfrak{m} = (Q_i)_\mathfrak{m} \cap \bigcap_{\substack{Q_j \subset \mathfrak{m} \\ j \geq r+1}} (Q_j)_\mathfrak{m} = (Q_i)_\mathfrak{m}.$$

Thus $(Q_i)_\mathfrak{m} = (I_t)_\mathfrak{m}$ is also prime and using [7, Proposition 3.11 p. 41], we conclude that so is Q_i. Finally, as an intersection of prime ideals, I_t is a radical ideal. □

In the sequel, our goal is to prove that generically, the restriction of $\pi_{\leq i-1}$ to $V^\mathbf{A} \cap \mathbb{V}\left(f^\mathbf{A} - t\right) \cap \mathscr{C}\left(f^\mathbf{A}, \mathbf{F}^\mathbf{A}, i\right)$ is proper, that is stated in Lemma 5.17. To this end, we will use several intermediate results. They are strongly inspired by the results in [119, Theorem 1] and uses its intermediate results. For clarity and simplicity we refer to those results which can be used *mutatis mutandis* and focus on steps requiring a specific treatment to prove Lemma 5.17.

Notation 5.14. *In the sequel, we denote by*

- $\mathfrak{A}$ *a* $n \times n$ *matrix whose entries are new indeterminates* $(\mathfrak{A}_{i,j})_{1\leq i,j\leq n}$,
- $\mathfrak{t}$ *a new indeterminate,*

- $\Delta_d^{\mathfrak{A}}(\mathfrak{t})$ *the ideal* $\left\langle \mathbf{F}^{\mathfrak{A}}, f^{\mathfrak{A}} - \mathfrak{t} \right\rangle$,
- $\Delta_i^{\mathfrak{A}}(\mathfrak{t})$, *for* $1 \leq i \leq d-1$, *the ideal generated by* $\mathbf{F}^{\mathfrak{A}}, f^{\mathfrak{A}} - \mathfrak{t}$ *and the minors of size* $n-d+1$ *of* $\mathsf{Jac}\left(\left[\mathbf{F}^{\mathfrak{A}}, f^{\mathfrak{A}}\right], i+1\right)$.

Then we can restate [119, Section 2.3, Proposition 1], replacing $\mathbb{Q}$ with $\mathbb{Q}(\mathfrak{t})$. Indeed, the tools used in this proof, namely Nœther normalization, Krull's Principal Ideal Theorem, Quillen-Suslin's Theorem and algebraic Bertini's Theorem can be used with any field of characteristic 0.

Lemma 5.15. *Let* $i \in \{1, \ldots, d\}$, *let* $P_{\mathfrak{t}}$ *be a prime components of* $\sqrt{\Delta_i^{\mathfrak{A}}(\mathfrak{t})}$ *and let* r *be its dimension. Then* r *is at most* $i-1$ *and the extension* $\mathbb{Q}(\mathfrak{t})(\mathfrak{A}_{i,j})[X_1, \ldots, X_r] \to \mathbb{Q}(\mathfrak{t})(\mathfrak{A}_{i,j})[\mathbf{X}]/P_{\mathfrak{t}}$ *is integral.*

The next Proposition shows that this result remains true specializing the indeterminates $\mathfrak{A}_{i,j}$ and $\mathfrak{t}$ in a suitable non-empty Zariski-open set. This is similar to [119, Proposition 2], except that we manage the parameter $\mathfrak{t}$.

Lemma 5.16. *There exists a non-empty Zariski-open set* $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ *such that for all* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, *there exists a non-empty Zariski-open set* $\mathcal{T}^{\mathbf{A}} \subset \mathbb{C}$ *such that for all* $t \in \mathbb{R} \cap \mathcal{T}^{\mathbf{A}}$, *the following holds:*

- *Let* $i \in \{1, \ldots, d\}$, *let* $P_t^{\mathbf{A}}$ *be a prime components of* $\sqrt{\Delta_i^{\mathbf{A}}(t)}$ *and* r *its dimension. Then* r *is at most* $i-1$ *and the extension* $\mathbb{C}[X_1, \ldots, X_r] \to \mathbb{C}[X_1, \ldots, X_n]/P_t^{\mathbf{A}}$ *is integral.*

Proof. Let i be in $\{1, \ldots, d\}$. Since i is fixed, we write $\Delta = \Delta_i^{\mathfrak{A}}(\mathfrak{t})$. Applying [119, Proposition 2] with $\mathbb{C}(\mathfrak{t})$ as a ground field yields the existence of a non-empty Zariski-open set $\mathscr{O}_1$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$ and all prime component P of $\Delta^{\mathbf{A}}$ the following holds:

- the dimension r of P is at most $i-1$;
- the extension $\mathbb{C}(\mathfrak{t})[X_1, \ldots, X_r] \to \mathbb{C}(\mathfrak{t})[X_1, \ldots, X_n]/P$ is integral.

Thus it is sufficient to prove that the ideal P_t obtained specializing $\mathfrak{t}$ to t contains a monic polynomial in X_r. Since the extension $\mathbb{C}(\mathfrak{t})[X_1, \ldots, X_r] \to \mathbb{C}(\mathfrak{t})[X_1, \ldots, X_n]/P$ is integral, as an ideal in $\mathbb{Q}(\mathfrak{t})[X_1, \ldots, X_n]$, P contains a monic polynomial, that lies in $\mathbb{Q}(\mathfrak{t})[X_1, \ldots, X_{r-1}][X_r]$ non-identically zero, that we denote by m_P. Let $\alpha(\mathfrak{t}) \in \mathbb{Q}[\mathfrak{t}]$ be the least common multiple of the denominators of m_P in $\mathbb{Q}[\mathfrak{t}]$.

Now, let $\mathscr{U}_P^{\mathbf{A}}$ be the non-empty Zariski-open set such that for all $t \in \mathscr{U}_P^{\mathbf{A}}$, P_t is equidimensional of dimension the one of P and contains the polynomial $m_{P,t}$ obtained when instantiating $\mathfrak{t}$ to t in m_P: such a Zariski-open set exists since

- one can perform equidimensional decomposition without factorization;
- one can decide that a polynomial lies in an ideal without factorization.

Thus, $\mathscr{U}_P^{\mathbf{A}}$ can be obtained as the non-vanishing of all the denominators appearing in the execution of such algorithms with input polynomials defining P for the first algorithm and a Gröbner basis of P and m_P for the second algorithm.

Consider now the non-empty Zariski open set $\mathscr{V}_{\mathbf{A},P}$ defined by the non-vanishing of α and let $\mathcal{T}_P^{\mathbf{A}}$ be $\mathscr{U}_P^{\mathbf{A}} \cap \mathscr{V}_{\mathbf{A},P}$. For $t \in \mathcal{T}_P^{\mathbf{A}}$, we instantiate $\mathfrak{t}$ to t: since $t \in \mathscr{U}_P^{\mathbf{A}}$, P_t is equidimensional and contains $m_{P,t}$. Moreover, since $t \in \mathscr{V}_{\mathbf{A},P}$, $m_{P,t}$ is monic.

Consequently, for all $t \in \mathcal{T}_P^{\mathbf{A}}$, the extension $\mathbb{C}[X_1, \ldots, X_r] \to \mathbb{C}[X_1, \ldots, X_n]/P_t$ is integral. We conclude by defining $\mathcal{T}^{\mathbf{A}} = \bigcap \mathscr{U}_{\mathbf{A},P}$, where the intersection is taken for the finitely many prime components of $\Delta^{\mathbf{A}}$. □

We are now able to prove the following.

Lemma 5.17. *There exists a non-empty Zariski-open set $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, there exists a non-empty Zariski-open set $\mathcal{T}^{\mathbf{A}} \subset \mathbb{C}$ such that for all $t \in \mathbb{R} \cap \mathcal{T}^{\mathbf{A}}$, the restriction of $\pi_{\leq i-1}$ to $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is proper for $1 \leq i \leq d$.*

Proof. According to Lemma 5.16 for $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$ and $t \in \mathcal{T}^{\mathbf{A}}$, the following holds: for any prime component $P_t^{\mathbf{A}}$ of dimension r of $\sqrt{\Delta_i^{\mathbf{A}}(t)}$, then r is at most $i-1$ and the extension $\mathbb{C}[X_1, \ldots, X_r] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]/P_t^{\mathbf{A}}$ is integral.

Then according to Proposition 1.14, this is true if and only if the restriction of $\pi_{\leq i-1}$ to $\mathbb{V}\left(\Delta_i^{\mathbf{A}}(t)\right) = V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is proper. □

We can now prove Theorem 5.9.

Proof of Theorem 5.9. By Lemma 5.17, there exists a non-empty Zariski-open set $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ such that, for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, there exists a non-empty Zariski-open set $\mathcal{T}^{\mathbf{A}} \subset \mathbb{C}$ such that for all $t \in \mathbb{R} \cap \mathcal{T}^{\mathbf{A}}$, the restriction of $\pi_{\leq i-1}$ to $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is proper for $1 \leq i \leq d$.

Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$ and $\mathcal{Q}^{\mathbf{A}} = \mathcal{T}^{\mathbf{A}} \setminus f^{\mathbf{A}}\left(\mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right) \cup \mathrm{Sing}\left(V^{\mathbf{A}}\right)\right)$. By Sard's theorem, $f^{\mathbf{A}}\left(\mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)\right)$ is finite. Because of assumptions **R**, $f^{\mathbf{A}}\left(\mathrm{Sing}\left(V^{\mathbf{A}}\right)\right)$ is finite too. Then $\mathcal{Q}^{\mathbf{A}}$ is a Zariski-open set.

By Lemma 5.13 applied to $\mathbf{F}^{\mathbf{A}}$ and $f^{\mathbf{A}}$, for all $t \in \mathbb{R} \cap \mathcal{Q}^{\mathbf{A}}$, the ideal $\left\langle \mathbf{F}^{\mathbf{A}}, f^{\mathbf{A}} - t \right\rangle$ is radical, $\mathbb{V}\left(\mathbf{F}^{\mathbf{A}}, f^{\mathbf{A}} - t\right)$ is either empty or smooth and equidimensional of dimension $d-1$. Moreover, for all $t \in \mathbb{R} \cap \mathcal{T}^{\mathbf{A}}$, the restriction of $\pi_{\leq i-1}$ to $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is proper.

Then [119, Theorem 2] can be applied to $\mathbf{F}^{\mathbf{A}}, f^{\mathbf{A}} - t$ for all $t \in \mathbb{R} \cap \mathcal{Q}^{\mathbf{A}}$. It states that for $1 \leq i \leq d$, $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ have a non-empty intersection with each connected component of $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ and dimension at most 0. □

Proof of Theorem 5.11.

This is a generalization of [51] where the proof is done when $V \cap \mathbb{R}^n = \mathbb{R}^n$ and has been published in [52].

We will use the following result, that has been proved in [51, Theorem 3, page 134].

Theorem 5.18. *Let $V \subset \mathbb{C}^n$ be an algebraic variety of dimension d. There exists a non-empty Zariski-open set $\mathscr{O}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$ and $0 \leq i \leq d$, there exist algebraic sets $V_i^{\mathbf{A}} \subset V^{\mathbf{A}}$ such that for all connected component $C^{\mathbf{A}}$ of $V^{\mathbf{A}} \cap \mathbb{R}^n$,*

(i) the restriction of $\pi_{\leq i}$ to $V_i^{\mathbf{A}}$ is proper;

(ii) the boundary of $\pi_{\leq i}\left(C^{\mathbf{A}}\right)$ is contained in $\pi_{\leq i}\left(C^{\mathbf{A}} \cap V_{i-1}^{\mathbf{A}}\right)$.

Its proof is a consequence of Lemma 5.19, Lemma 5.20 and Proposition 5.21 below.

We give the intuition of the proof. It consists of constructing recursively $V_{i-1}^{\mathbf{A}}$ from $V_i^{\mathbf{A}}$ with $V_d^{\mathbf{A}} = V^{\mathbf{A}}$. Suppose that we have found $\mathbf{A}$ such that properties *(i)* and *(ii)* are satisfied by $V_i^{\mathbf{A}}$. Then, we construct $V_{i-1}^{\mathbf{A}}$ such that the boundary of $\pi_{\leq i}(C^{\mathbf{A}})$ is contained in $\pi_{\leq i}(C^{\mathbf{A}} \cap V_{i-1}^{\mathbf{A}})$. We will see that we can construct $V_{i-1}^{\mathbf{A}}$ as the union of

- the j-equidimensional components of $V_i^{\mathbf{A}}$ for $1 \leq j \leq i-1$
- the singular locus of the i-equidimensional component of $V_i^{\mathbf{A}}$.
- the critical locus of the restriction of $\pi_{\leq i}$ to the i-equidimensional component of $V_i^{\mathbf{A}}$;

Nevertheless, for this matrix $\mathbf{A}$, the restriction of $\pi_{\leq i-1}$ to $V_{i-1}^{\mathbf{A}}$ may not be proper. Then, a generic change of variables on the coordinates $X_1, \ldots, X_i$ will not alter $V_{i-1}^{\mathbf{A}}$ but will restore the properness property of $\pi_{\leq i-1}$.

This proof is widely inspired by the one of [119, Theorem 1 and Proposition 2]. We introduce some notations and preliminary results.

In the sequel, we denote by $\mathfrak{A}$ a $n \times n$ matrix whose entries are new indeterminates $(\mathfrak{A}_{i,j})_{1 \leq i,j \leq n}$, $\mathfrak{k}$ an algebraic closure of $\mathbb{Q}(\mathfrak{A}_{i,j})$ and $\mathbf{B}_r \in \mathrm{GL}_n(\mathbb{Q})$ a matrix of the form $\mathbf{B}_r = \begin{bmatrix} \mathbf{B}' & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-r} \end{bmatrix}$, where $\mathbf{B}'$ is square of size r and $\mathbf{I}_{n-r}$ is the identity matrix of size $n-r$. Then, $\mathfrak{B} = \mathfrak{A}\mathbf{B}_r$, whose entries are linear forms in the entries of $\mathfrak{A}$. $\mathsf{Subs}_{\mathfrak{B}}(g)$ stands for the polynomial obtained by substituting in g the entries of $\mathfrak{A}$ by those of $\mathfrak{B}$, for $g \in \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$. Given an ideal $I \subset \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$, $I^{\mathbf{B}_r}$ is defined as the ideal $\{f(\mathbf{B}_r\mathbf{X}) \mid f \in I\}$. Given an ideal $I \subset \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$, we denote by $\mathsf{Subs}_{\mathfrak{B}}(I)$ the ideal $\{\mathsf{Subs}_{\mathfrak{B}}(f) \mid f \in I\}$. Finally, $\mathbf{G}(I)$ denotes a finite system of generator of the ideal I, e.g. a Gröbner basis.

Then we define recursively the ideals defining

- the j-equidimensional components of $V_i^{\mathbf{A}}$ for $1 \leq j \leq i-1$
- the singular locus of the i-equidimensional component of $V_i^{\mathbf{A}}$.
- the critical locus of the restriction of $\pi_{\leq i}$ to the i-equidimensional component of $V_i^{\mathbf{A}}$;

To this end, we use the following notations: let $\Delta_d^{\mathfrak{A}}$ be the ideal $\left\langle \mathbf{F}^{\mathfrak{A}} \right\rangle \subset \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$. Then $\Delta_{d,i}^{\mathfrak{A}}$ is either

- the intersection of the prime ideals of dimension i associated to $\Delta_d^{\mathfrak{A}}$ if such prime ideals exist,
- or $\langle 1 \rangle$ if there is no such prime ideals.

Then we define $\Delta_{d,\leq k}^{\mathfrak{A}}$ as the intersection $\bigcap_{0 \leq i \leq k} \Delta_{d,i}^{\mathfrak{A}}$ and $\mathfrak{V}_{i,i}$ as the i-equidimensional component of the algebraic set defined by $\Delta_{i,i}^{\mathfrak{A}}$ in $\mathfrak{k}^n$. The ideal $\mathsf{M}_i^{\mathfrak{A}}$ is defined either as

- $\langle 1 \rangle$ if $\Delta_{i,i}^{\mathfrak{A}} = \langle 1 \rangle$
- or as the ideal generated by the $n-i$-minors of $\mathsf{Jac}\left(\mathbf{G}\left(\Delta_{i,i}^{\mathfrak{A}}\right), i+1\right)$ else.

Finally, let $\Sigma_{i-1}^{\mathfrak{A}}$ be the radical ideal $\sqrt{\Delta_{i,i}^{\mathfrak{A}} + \mathsf{M}_i^{\mathfrak{A}}}$ and $\Delta_{i-1}^{\mathfrak{A}} = \Sigma_{i-1}^{\mathfrak{A}} \cap \Delta_{i,\leq i-1}^{\mathfrak{A}}$.

By construction, the ideal $\Sigma_{i-1}^{\mathfrak{A}}$ is the ideal associated with the union of the singular locus of $\mathfrak{V}_{i,i}$ and the critical locus of the restriction of $\pi_{\leq i}$ to $\mathfrak{V}_{i,i}$. Thus, the definition of $\Sigma_{i-1}^{\mathfrak{A}}$ does not depend on $\mathbf{G}\left(\Delta_{i-1}^{\mathfrak{A}}\right)$.

Lemma 5.19. *Let $r \leq i$. If $\Delta_i^{\mathfrak{A}\mathbf{B}_r} = \mathsf{Subs}_{\mathfrak{B}}\left(\Delta_i^{\mathfrak{A}}\right)$, then $\Delta_{i-1}^{\mathfrak{A}\mathbf{B}_r} = \mathsf{Subs}_{\mathfrak{B}}\left(\Delta_{i-1}^{\mathfrak{A}}\right)$.*

Proof. The proof is done by induction. We detail below the induction; the initialization step being obtained by substituting i by d in the sequel.

By assumption $\Delta_i^{\mathfrak{A}\mathbf{B}_r} = \mathsf{Subs}_{\mathfrak{B}}\left(\Delta_i^{\mathfrak{A}}\right)$. Since these ideals are radical, the uniqueness of prime decomposition implies that $\Delta_{i,i}^{\mathfrak{A}\mathbf{B}_\mathbf{r}} = \mathsf{Subs}_{\mathfrak{B}}\left(\Delta_{i,i}^{\mathfrak{A}}\right)$ and $\Delta_{i,\leq i-1}^{\mathfrak{A}\mathbf{B}_r} = \mathsf{Subs}_{\mathfrak{B}}\left(\Delta_{i,\leq i-1}^{\mathfrak{A}}\right)$. Thus, to conclude it remains to prove that $\Sigma_{i-1}^{\mathfrak{A}\mathbf{B}_r} = \mathsf{Subs}_{\mathfrak{B}}\left(\Sigma_{i-1}^{\mathfrak{A}}\right)$. Let $\mathbf{G} = \mathbf{G}\left(\Delta_{i,i}^{\mathfrak{A}}\right)$. Since $\Delta_{i,i}^{\mathfrak{A}\mathbf{B}_r} = \mathsf{Subs}_{\mathfrak{B}}\left(\Delta_{i,i}^{\mathfrak{A}}\right)$, we get $\left\langle \mathbf{G}^{\mathbf{B}_r} \right\rangle = \langle \mathsf{Subs}_{\mathfrak{B}}(\mathbf{G}) \rangle$. Because of the equality $\left\langle \mathbf{G}^{\mathbf{B}_r} \right\rangle = \langle \mathsf{Subs}_{\mathfrak{B}}(\mathbf{G}) \rangle$, both ideals define the same algebraic variety $\mathfrak{V}$ in $\mathfrak{k}^n$. By construction, the ideal $\Sigma_{i-1}^{\mathfrak{A}\mathbf{B}_r}$ is the ideal associated to the union of the singular locus of $\mathfrak{V}$ and the critical locus of the restriction of $\pi_{\leq i}$ to $\mathfrak{V}$. The same statement occurs for $\mathsf{Subs}_{\mathfrak{B}}\left(\Sigma_{i-1}^{\mathfrak{A}}\right)$ so these ideals coincide. □

Lemma 5.20. *Let $i \in \{0, \ldots, d\}$ and P be a prime ideal appearing in the prime decomposition of $\sqrt{\Delta_i^{\mathfrak{A}}}$ and r its dimension. Then $r \leq i-1$ and the extension $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}] \longrightarrow \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}]/P$ is integral.*

Proof. We prove the property by decreasing induction on $i = d, \ldots, 0$. The case $i = d$ is obtained following the Noether Normalization Theorem.

In the sequel, we say that $\mathcal{R}\left(\Delta_i^{\mathfrak{A}}\right)$ holds if for all prime ideal P of dimension r appearing in the prime decomposition of $\Delta_i^{\mathfrak{A}}$, the extension $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}] \longrightarrow \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}]/P$ is integral.

Let us now assume that the property holds for index i, and prove it for index $i-1$. We first establish property $\mathcal{R}\left(\Delta_i^{\mathfrak{A}}\right)$. The dimension property will follow from it since it implies that $\pi_{\leq i}$ restricted the variety defined by $\Delta_i^{\mathfrak{A}}$ is a finite map. Then, the algebraic Bertini-Sard theorem allows us to conclude.

Recall that $\Delta_{i-1}^{\mathfrak{A}} = \Sigma_{i-1}^{\mathfrak{A}} \cap \Delta_{i,\leq i-1}^{\mathfrak{A}}$. Since $\mathcal{R}\left(\Delta_i^{\mathfrak{A}}\right)$ holds by assumption, $\mathcal{R}\left(\Delta_{i,\leq i-1}^{\mathfrak{A}}\right)$ holds trivially. Thus, it is sufficient to prove that $\mathcal{R}\left(\Sigma_{i-1}^{\mathfrak{A}}\right)$ holds. Recall also that $\Sigma_{i-1}^{\mathfrak{A}}$ is the radical of $\Delta_{i,i}^{\mathfrak{A}} + \mathsf{M}_i^{\mathfrak{A}}$ where $\mathsf{M}_i^{\mathfrak{A}}$ is the ideal generated by the $(n-i)$-minors $M_1, \ldots, M_N$ of $\mathsf{Jac}\left(\mathbf{G}\left(\Delta_{i,i}^{\mathfrak{A}}\right), i+1\right)$. We will consider this intersection process incrementally since for proving that $\mathcal{R}\left(\Delta_{i,i}^{\mathfrak{A}} + \mathsf{M}_i^{\mathfrak{A}}\right)$ holds, it is enough to prove that property $\mathcal{R}\left(\Delta_{i,i}^{\mathfrak{A}} + \langle M_1, \ldots, M_j\rangle\right)$ holds for $1 \leq j \leq N$. Note that by assumption $\mathcal{R}\left(\Delta_i^{\mathfrak{A}}\right)$ holds and we prove below by increasing induction that if $\mathcal{R}\left(\Delta_{i,i}^{\mathfrak{A}} + \langle M_1, \ldots, M_j\rangle\right)$ holds then $\mathcal{R}\left(\Delta_{i,i}^{\mathfrak{A}} + \langle M_1, \ldots, M_{j+1}\rangle\right)$ holds. To simplify notations, we fix $\Delta = \Delta_{i,i}^{\mathfrak{A}} + \langle M_1, \ldots, M_j\rangle$, $M = M_{j+1}$ and $\Delta' = \Delta + \langle M\rangle$ for $0 \leq j \leq N-1$.

Consider now the prime decomposition $\bigcap_{\ell \leq L} P_\ell$ of $\sqrt{\Delta}$ for some L and remark that the set of prime components of $\sqrt{\Delta'}$ is the union of the prime components of $\sqrt{P_\ell + \langle M\rangle}$ for $1 \leq \ell \leq L$. Consequently, it is enough to prove that $P_\ell + \langle M\rangle$ satisfies property $\mathcal{R}$ for those ℓ such that $P_\ell + \langle M\rangle \neq \langle 1\rangle$. Thus, as in [119], we partition $\{1, \ldots, L\}$ in four subsets:

- $\ell \in L^+$ if $\dim(P_\ell) = r$ and $M \in P_\ell$,
- $\ell \in L^-$ if $\dim(P_\ell) = r$, $M \notin P_\ell$ and $P_\ell + \langle M\rangle \neq \langle 1\rangle$,
- $\ell \in S$ if $\dim(P_\ell) = r$, $M \notin P_\ell$ and $P_\ell + \langle M\rangle = \langle 1\rangle$,
- $\ell \in R$ if $\dim(P_\ell) \neq r$.

We will prove that $\mathcal{R}(P_\ell + \langle M\rangle)$ holds for $\ell \in L^+ \cup L^-$ while letting $r \leq i$ vary will conclude the proof.

For $\ell \in L^+$, $M \in P_\ell$, since $P_\ell + \langle M\rangle = P_\ell$ while $\mathcal{R}(P_\ell)$ holds by assumption, the conclusion follows. Suppose now that $\ell \in L^-$. Since P_ℓ is prime, by Krull's Principal Ideal Theorem, $P_\ell + \langle M\rangle$ has dimension $r-1$ and is equidimensional. By [119, Lemma 1], it is sufficient to prove that the extension $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r-1}] \to \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r-1}]/(P_\ell + \langle M\rangle)$ is integral which is what we do below.

This step of the proof is common with the one of [119, Proposition 1]. We summarize it. By assumption, the extension

$$\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}] \to A_\ell = \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}]/P_\ell$$

is integral, it only remains to prove that $P_\ell + \langle M\rangle$ contains a monic polynomial that lies in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r-1}][\mathbf{X}_r]$. To this end, the characteristic polynomial of the multiplication by M in A_ℓ is naturally considered and more particularly, we consider its constant term α_ℓ. Since $\ell \in L^-$, M does not divide zero in A_ℓ and α_ℓ is not a constant and hence it is not zero. Moreover, by Cayley-Hamilton's Theorem, $\alpha_\ell \in P_\ell + \langle M\rangle$. This polynomial α_ℓ is proved to be monic in X_r hereafter.

Consider a matrix $\mathbf{B} = \mathrm{GL}_n(\mathbb{Q})$ which lets invariant the last $n-r$ variables and such that $\alpha_\ell(\mathbf{BX})$ is monic in X_r (recall that $r \leq i$). Following *mutatis mutandis* the reasoning of [119, Section 2.3] (paragraph entitled *Introduction of a change of variables*), we get that

- the constant term of the multiplication by $M(\mathbf{BX})$ modulo $P_\ell^{\mathbf{B}}$ is $\alpha_\ell(\mathbf{BX})$;
- the one of the multiplication by $\mathsf{Subs}_{\mathfrak{B}}(M)$ modulo $\mathsf{Subs}_{\mathfrak{B}}(P_\ell)$ is $\mathsf{Subs}_{\mathfrak{B}}(\alpha_\ell)$;

Note that we have chosen $\mathbf{B}$ such that $\alpha_\ell(\mathbf{BX})$ is monic in X_r. Thus, if we prove that $\alpha_\ell(\mathbf{BX}) = \mathsf{Subs}_{\mathfrak{B}}(\alpha_\ell)$, we are done (recall that $\mathsf{Subs}_{\mathfrak{B}}(.)$ only consists in substituting the entries of $\mathfrak{A}_{i,j}$ with those of $\mathfrak{AB}$ which do not depend on $X_1, \ldots, X_n$).

Since $\mathbf{B}$ lets invariant the last $n-r$ variables $X_{r+1}, \ldots, X_n$, Lemma 5.19 implies that $\Delta^{\mathbf{B}} = \mathsf{Subs}_{\mathfrak{B}}(\Delta)$ and $M^{\mathbf{B}} = \mathsf{Subs}_{\mathfrak{B}}(M)$. The uniqueness of prime decomposition implies that $\left\{P_\ell^{\mathbf{B}}, \ell \in L\right\} = \left\{\mathsf{Subs}_{\mathfrak{B}}(P_\ell), \ell \in L\right\}$. Moreover, since $\dim\left(\mathsf{Subs}_{\mathfrak{B}}(P_\ell)\right) = \dim\left(P_\ell^{\mathbf{B}}\right) = \dim(P_\ell)$, we also have

$$\left\{P_\ell^{\mathbf{B}}, \ell \in L^+ \cup L^- \cup S\right\} = \left\{\mathsf{Subs}_{\mathfrak{B}}(P_\ell), \ell \in L^+ \cup L^- \cup S\right\}.$$

The rest of the reasoning is the same as the one of [119]. Indeed, the above equality implies that for $\ell \in L^-$, there exists $\ell' \in L^+ \cup L^- \cup S$ such that $\mathsf{Subs}_{\mathfrak{B}}(P_\ell) = P_\ell^{\mathbf{B}}$. Since $M^{\mathbf{B}} = \mathsf{Subs}_{\mathfrak{B}}(M)$, the characteristic polynomials of $M^{\mathbf{B}}$ modulo $P_{\ell'}^{\mathbf{B}}$ coincides with the characteristic polynomial of $\mathsf{Subs}_{\mathfrak{B}}(M)$ modulo $\mathsf{Subs}_{\mathfrak{B}}(P_\ell)$, so $\mathsf{Subs}_{\mathfrak{B}}(\alpha_\ell) = \alpha_{\ell'}(\mathbf{BX})$. Recall now that α_ℓ is neither 0 nor a constant, then $\ell' \in L^-$. Thus, $\mathsf{Subs}_{\mathfrak{B}}(\alpha_\ell) = \alpha_{\ell'}(\mathbf{BX})$ is monic in X_r as requested. □

As in [119, Section 6.4], this property specializes. For $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, we denote by $\Delta_i^{\mathbf{A}}$ the ideal obtained by substituting the entries of $\mathfrak{A}$ by those of $\mathbf{A}$. The proof of the result below is skipped but follows *mutatis mutandis* the one of [119, Proposition 2].

Proposition 5.21. *There exists a non-empty Zariski open set $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ such that for $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, the following holds. Let $0 \leq i \leq d$, $P^{\mathbf{A}}$ be one of the prime components of $\Delta_i^{\mathbf{A}}$, and r its dimension. Then $\mathbb{C}[\mathbf{X}_{\leq r}] \longrightarrow \mathbb{C}[\mathbf{X}]/P^{\mathbf{A}}$ is integral.*

We can deduce the proof of Theorem 5.18.

Proof of Theorem 5.18. We use Proposition 1.14 page 20, that gives a connection between the properness property and the above normalization result to prove the first assertion.

For the second assertion, we define $V_i^{\mathbf{A}} \subset \mathbb{C}^n$ as the algebraic variety associated to $\Delta_i^{\mathbf{A}}$ for $0 \leq i \leq d$. For $j \leq i$, we denote by $V_{i,j}^{\mathbf{A}} \subset \mathbb{C}^n$ (resp. $V_{i,\leq j}^{\mathbf{A}} \subset \mathbb{C}^n$) the algebraic variety associated to $\Delta_{i,j}^{\mathbf{A}}$ (resp. $\Delta_{i,\leq j}^{\mathbf{A}}$). Consider now a connected component $C^{\mathbf{A}}$ of $V_i^{\mathbf{A}} \cap \mathbb{R}^n$. It is the union of some connected components $C_1^{\mathbf{A}}, \ldots, C_k^{\mathbf{A}}$ of the real algebraic sets $V_{i,j_1}^{\mathbf{A}} \cap \mathbb{R}^n, \ldots, V_{i,j_k}^{\mathbf{A}} \cap \mathbb{R}^n$. Consequently, the boundary of $\pi_{\leq i}(C)$ is contained in the boundary of $\bigcup_{1 \leq \ell \leq k} \pi_{\leq i}(C_\ell)$. By construction of $V_{i-1}^{\mathbf{A}}$, if $j_\ell > i$ then the boundary of

$\pi_{\leq i}(C_\ell)$ is contained in $\pi_{\leq i}\left(V_{i-1}^{\mathbf{A}}\right)$. By construction of $V_{i-1}^{\mathbf{A}}$, the variety $V_{i-1,i-1}^{\mathbf{A}}$ is the union of the singular points of $V_{i,i}^{\mathbf{A}}$ and the critical locus of $\pi_{\leq i}$ restricted to $V_{i,i}^{\mathbf{A}}$. Thus, if $j_\ell = i$, the properness of $\pi_{\leq i}$ restricted to $V_{i,i}^{\mathbf{A}}$ implies that the boundary of $\pi_{\leq i}(C_i)$ is contained in the image by $\pi_{\leq i}$ of $C^{\mathbf{A}} \cap V_{i-1,i-1}^{\mathbf{A}}$. □

We are now able to give a proof of Theorem 5.11.

Proof of Theorem 5.11. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$ and c be a critical value of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$. We prove that there exists $x_c \in \mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}(x_c) = c$. Let $C^{\mathbf{A}}$ be a connected component of $\mathbb{V}\left(f^{\mathbf{A}} - c\right) \cap V^{\mathbf{A}} \cap \mathbb{R}^n$.

Consider the largest $i \in \{1, \ldots, d\}$ such that $C^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i-1}) \neq \varnothing$ while $C^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i}) = \varnothing$.

Let φ_i be the projection $\begin{array}{rcl} \varphi_i : & \mathbb{C}^n & \longrightarrow \mathbb{C} \\ & (x_1, \ldots, x_n) & \longmapsto x_i \end{array}$. Then $\varphi_i\left(C^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i-1})\right) \subset \mathbb{R}^*$ is a strict subset of $\mathbb{R}$. Moreover, it is closed because of (i) and (ii) in Theorem 5.18. Then every extremum of the projection is reached. Since $\varphi_i\left(C^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i-1})\right) \neq \mathbb{R}$, there exists at least either a minimizer or a maximizer of φ_i. Without loss of generality, we assume that it is a local minimizer, denoted by $x^\star$.

Since c is not an isolated point in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, the set

$$\left(\mathbb{V}\left(f^{\mathbf{A}} - c - \varepsilon\right) \cup \mathbb{V}\left(f^{\mathbf{A}} - c + \varepsilon\right)\right) \cap V^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i-1}) \cap \mathbb{R}^n$$

is non-empty. Then by [116, Lemma 3.6], the following sets coincide:

- $\mathbb{V}\left(f^{\mathbf{A}} - c\right) \cap V^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i-1}) \cap \mathbb{R}^n$
- $\lim_0 \left(\mathbb{V}\left(f^{\mathbf{A}} - c \pm \varepsilon\right) \cap V^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i-1})\right) \cap \mathbb{R}^n$

Then, there exists a connected component $C_\varepsilon^{\mathbf{A}} \subset \mathbb{R}\langle\varepsilon\rangle^n$ of

$$\mathbb{V}\left(f^{\mathbf{A}} - c \pm \varepsilon\right) \cap V^{\mathbf{A}} \cap \mathbb{V}(\mathbf{X}_{\leq i-1}) \cap \mathbb{R}\langle\varepsilon\rangle^n$$

such that $C_\varepsilon^{\mathbf{A}}$ contains a x_ε such that $\lim_0(x_\varepsilon) = x^\star$. Furthermore, one can assume that x_ε minimize the projection φ_i over $C_\varepsilon^{\mathbf{A}}$. Indeed, in the converse, there exists $x'_\varepsilon \in C_\varepsilon^{\mathbf{A}}$ such that $\varphi_i(x'_\varepsilon) < \varphi_i(x_\varepsilon)$, that implies $\lim_0 \varphi_i(x'_\varepsilon) \leq \varphi_i(x^\star)$. Since $x^\star$ is a minimizer, this implies that $\lim_0 \varphi_i(x'_\varepsilon) = \varphi_i(x^\star)$ and we replace x_ε with x'_ε.

As a minimizer of the projection, x_ε lies in the algebraic set defined as the vanishing set of

- the polynomials in $\mathbf{F}^{\mathbf{A}}$,
- the minors of size $n - d + 1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}} - c \pm \varepsilon, \mathbf{F}^{\mathbf{A}}\right], i + 1\right)$,
- and $X_1, \ldots, X_{i-1}$.

Since $\mathsf{Jac}\left(\left[f^{\mathbf{A}}-c\pm\varepsilon,\mathbf{F}^{\mathbf{A}}\right],i+1\right)=\mathsf{Jac}\left(\left[f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right],i+1\right)$, this algebraic set is actually $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$. Furthermore, since ε is an infinitesimal, $c\pm\varepsilon$ is not a critical value of $f^{\mathbf{A}}$. Then $x_\varepsilon\notin\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$. This means that $x^\star$ is the limit of points that lies in $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. Hence $x^\star\in\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ too. Moreover since $f^{\mathbf{A}}(x^\star)=c$ that is a local extremum of $f^{\mathbf{A}}_{|V^{\mathbf{A}}\cap\mathbb{R}^n}$, $x^\star\in\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$. In other words,

$$x^\star\in\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\cap\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)=\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right),$$

that concludes the proof. □

Proof of Theorem 5.12.

This proof has been published in [52].

Proof of Theorem 5.12. Let $\mathscr{O}_3=\mathscr{O}_1\cap\mathscr{O}_2$ and $\mathbf{A}\in\mathrm{GL}_n(\mathbb{Q})\cap\mathscr{O}_3$ and $1\leq i\leq d$. We first prove that $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ have dimension at most 1.

Since $\mathbf{A}\in\mathscr{O}_3$, the properties in Theorem 5.9 and 5.11 hold. Thus there exists $\mathcal{Q}^{\mathbf{A}}\subset\mathbb{C}$ such that for all $t\in\mathcal{Q}^{\mathbf{A}}$, the algebraic set $\mathbb{V}\left(f^{\mathbf{A}}-t\right)\cap\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ has dimension at most zero.

Now let $Z^{\mathbf{A}}$ be an irreducible component of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. In particular, $Z^{\mathbf{A}}$ is an irreducible component of $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ that is not contained in $\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$. Consider the restriction $f^{\mathbf{A}}_{|C^{\mathbf{A}}}\colon Z^{\mathbf{A}}\longrightarrow\mathbb{C}$. Its image has a Zariski-closure of dimension 0 or 1.

Assume first that $f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ is 0-dimensional. Then as a continuous function, $f^{\mathbf{A}}_{|C^{\mathbf{A}}}$ is locally constant. This implies that $Z^{\mathbf{A}}$ is contained in critical locus of $f^{\mathbf{A}}_{|V^{\mathbf{A}}}$. In particular, this means that $Z^{\mathbf{A}}\subset\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$, a contradiction.

Then assume $\overline{f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension 1. From the Theorem on the dimension of fibers ([134, Theorem 7, Chapter 1, pp. 76]), there exists an Zariski-open set $U\subset\mathbb{C}$ such that for all $y\in U$, $\dim\left(f^{\mathbf{A}}\right)^{-1}=\dim Z^{\mathbf{A}}-1$. In particular if t lies in the non-empty Zariski-open set $U\cap\mathcal{Q}^{\mathbf{A}}$, we obtain

$$0\geq\dim\left(f^{\mathbf{A}}\right)^{-1}=\dim Z^{\mathbf{A}}-1.$$

Then every irreducible component $Z^{\mathbf{A}}$ of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension ≤ 1, so that $\dim\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\leq 1$.

Now let $Z_1^{\mathbf{A}}\cup\cdots\cup Z_\alpha^{\mathbf{A}}\cup\cdots\cup Z_\beta^{\mathbf{A}}$ be the decomposition of $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ as a union of irreducible components. Up to reordering, assume that

- for $1\leq i\leq\alpha$, $Z_i^{\mathbf{A}}\not\subset\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$,
- for $\alpha+1\leq j\leq\beta$, $Z_i^{\mathbf{A}}\subset\operatorname{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$.

Then the decomposition of $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ as a union of irreducible components is $Z_1^{\mathbf{A}} \cup \cdots \cup Z_\alpha^{\mathbf{A}}$.

Let $1 \leq i \leq \alpha$ and consider $Z_i^{\mathbf{A}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$. If it is non-empty, since $Z_i^{\mathbf{A}} \not\subset \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$, [79, Corollary 3.2 p. 131] implies that $Z_i^{\mathbf{A}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$ has dimension less than or equal to $\dim Z_i^{\mathbf{A}} - 1 \leq 1 - 1 = 0$. Finally, this prove that

$$\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}} \cap \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$$

has dimension ≤ 0. □

5.4 Degree Bounds

In this section, we assume that the polynomial f and the polynomials f_i have degree $\leq D$. Recall that the degree of an irreducible algebraic variety $V \subset \mathbb{C}^n$ is defined as the maximum finite cardinal of $V \cap L$ for every linear subspace $L \subset \mathbb{C}^n$. If V is reducible, $\deg V = \sum \deg Z$ where the sum is over every irreducible component Z of V. The degree of a hypersurface $\mathbb{V}(f)$ is bounded by $\deg f$. Given a variety $V = \mathbb{V}(g_1, \ldots, g_p)$, we denote by $\delta(V)$ the maximum of the degrees $\deg(V(g_1, \ldots, g_i))$, for $1 \leq i \leq p$.

As explained in Section 1.3, we will use the geometric resolution to estimate the complexity of our algorithms. Since its complexity of the computation of a variety V depends essentially on $\delta(V)$, it is relevant to give a bound on these degrees. We prove that $\delta\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ and $\delta\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ are bounded by a quantity that is singly exponential in the number of variables. Since the complexity of the geometric resolution is polynomial in the maximum geometric degree, this means that we can expect our algorithms to be singly exponential in the number of variables.

Proposition 5.22. *For all* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, *for* $1 \leq i \leq d$, $\delta\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ *and* $\delta\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ *are bounded by* $D\left((n-d+1)(D-1)\right)^n$.

Proof. Let $E_1 = \mathbb{V}\left(f^{\mathbf{A}}\right)$ and denote by $E_2, E_3, \ldots, E_p$ the zero-sets of each polynomial in $\mathbf{F}^{\mathbf{A}}$ and each minor of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right], i+1\right)$. Then for $2 \leq j \leq p$, each E_j has degree bounded by $(n-d+1)(D-1)$. Moreover, E_1 has degree bounded by D and dimension $n-1$. Let $1 \leq k \leq p$. Then using [57, Proposition 2.3] we get

$$\deg\left(\bigcap_{1 \leq j \leq k} E_j\right) \leq \deg E_1 \left(\max_{1 < j \leq k} \deg E_j\right)^{\dim E_1}. \tag{5.1}$$

In particular,

$$\deg\left(\bigcap_{1 \leq j \leq k} E_j\right) \leq D\left((n-d+1)(D-1)\right)^{n-1}.$$

By Bézout's inequality ([57, Proposition 2.3]), it follows that $\bigcap_{1\leq j\leq k} E_j \cap \mathbb{V}(\mathbf{X}_{\leq i-1})$ has also its degree bounded by $D((n-d+1)(D-1))^{n-1}$. Finally, this means that

$$\delta\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right) \leq D((n-d+1)(D-1))^{n-1}. \tag{5.2}$$

It remains to prove that $\delta\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right) \leq D((n-d+1)(D-1))^{n}$. From the above inequality 5.2, we deduce that

$$\delta\left(\overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}}\right) \leq D((n-d+1)(D-1))^{n-1}.$$

Finally, we apply [57, Proposition 2.3] with the varieties $F_1, \ldots, F_t$, where

$$F_1 = \overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}}$$

and $F_2, F_3, \ldots, F_t$ are the zero-sets of each minor defining $\mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$. Since these minors have degree bounded by $(n-d+1)(D-1)$, so are their associated varieties. By Proposition 6.8, $F_1 = \overline{\mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) \setminus \mathrm{Crit}(f^{\mathbf{A}}, V^{\mathbf{A}})}^{\mathcal{Z}}$ has dimension 1. Then inequality 5.1 becomes

$$\deg\left(\bigcap_{1\leq j\leq t} F_j\right) \leq D((n-d+1)(D-1))^{n-1} \times (n-d+1)(D-1).$$

This means that

$$\delta\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right) \leq D((n-d+1)(D-1))^{n}.$$

□

Chapter 6

Algorithm for Global Optimization

6.1 Introduction

This chapter is part of the submitted paper [52]. It is a strong generalization of our paper [51], where an algorithm testing the reachability of the global infimum of a polynomial on $\mathbb{R}^n$ is presented.

Motivation and prior work

Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ and $V = \mathbb{V}(\mathbf{F}) \subset \mathbb{C}^n$. Given another polynomial $f \in \mathbb{Q}[\mathbf{X}]$, let $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x)$. By convention, if $V \cap \mathbb{R}^n$ is empty then $f^\star = +\infty$.

In this chapter, we present an algorithm solving the following problems.

(B) Deciding the finiteness and computing an algebraic representation of $f^\star$.

(C) Deciding whether there exists $x^\star \in V \cap \mathbb{R}^n$ such that $f(x^\star) = f^\star$ and computing a rational parametrization of $x^\star$.

The goal is to obtain a dedicated algorithm whose complexity meets the best known bounds and whose practical behaviour reflects its complexity to solve problems

The problem of computing such algebraic representations is a quantifier elimination problem over the reals. Hence, it can be solved by the cylindrical algebraic decomposition algorithm, that is a general solver (see e.g. [22, 31, 32, 33, 67, 94]). This algorithm is able to decide whether $f^\star$ is finite. If so, it can compute an algebraic representation of $f^\star$ and if it exists, of a minimizer. However, its complexity is intrinsically doubly exponential in the number of variables. Practically, it can not deal with problems of more than 4 variables.

In [16], an algorithm whose complexity is singly exponential in the number of quantifiers alternates is presented. For problems (B) and (C) with a n-variate polynomial of degree D, this complexity becomes $D^{O(n)}$. Nevertheless, the techniques that allow to obtain such complexity results, such as infinitesimal deformations, did not provide yet practical results that reflect this complexity gain.

In [1, 2], criteria to decide whether the infimum is reached are given, when there are finitely many minimizers. If so, the set of minimizers can be represented by a border basis. However, there is no information about the complexity.

Thus, our goal is to obtain an algorithm for solving problems (B) and (C) with good control on the complexity constant in the exponent. We allow to have regularity assumptions on the input that are reasonable in practice (e.g. rank conditions on the Jacobian matrix of the input equality constraints). We also allow probabilistic algorithms provided that probabilistic aspects do not depend on the input but on random choices performed when running the algorithm.

A first attempt towards this goal is presented in [118]. Given a n-variate polynomial f of degree D, a probabilistic algorithm computing $\inf_{x\in\mathbb{R}^n} f(x)$ in $O\left(n^7D^{4n}\right)$ operations in $\mathbb{Q}$ is given. Furthermore, it is practically efficient and has solved problems intractable before (up to 6 variables).

In [13], algorithm and a study of the intrinsic complexity for polynomial optimization are given. It is done with constraints defined by polynomial equations satisfying some assumptions of regularity.

Our goal is to generalize these two approaches to the case of equality constraints and design an algorithm whose complexity is essentially cubic in $(sD)^n$ and linear in the evaluation complexity of the input.

Problem statement

Algebraic representation In the sequel, a real algebraic number α is represented by a polynomial $P \in \mathbb{Q}[t]$ and an isolating interval I. This means that P has only one root in I, that is α. Likewise, a finite real algebraic set $Y \subset \mathbb{R}^n$ defined by polynomials in $\mathbb{Q}[\mathbf{X}]$ can be represented by a rational parametrization. This is a sequence of polynomials $q, q_0, q_1, \ldots, q_n \in \mathbb{Q}[U]$ such that for all $x = (x_1, \ldots, x_n) \in Y$, there is a unique $u \in \mathbb{R}$ such that

$$\begin{cases} q(u) &= 0 \\ x_1 &= q_1(u)/q_0(u) \\ &\vdots \\ x_n &= q_n(u)/q_0(u) \end{cases}$$

In other words, there is a bijection between the roots of q and the points in Y. Thus, a single point in $x \in Y$ can be represented by $q, q_0, q_1, \ldots, q_n$ and an interval isolating the root of q corresponding with x. Note that such a representation can be computed from a Gröbner basis [115] and algorithms computing such a representation are implemented in computer algebra systems.

Algorithm specification Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ and $f \in \mathbb{Q}[\mathbf{X}]$. The goal of this chapter is to provide an algorithm taking as input f and $\mathbf{F}$ and that returns

- an algebraic representation of $f^\star = \inf_{x\in\mathbb{V}(\mathbf{F})\cap\mathbb{R}^n} f(x)$ if $f^\star$ is finite,

- if $f^\star$ is finite and reached, an algebraic representation of a point $x^\star \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ such that $f(x^\star) = f^\star$.

Note that a point $x^\star$ is returned if and only if $f^\star$ is reached so that its reachability can be decided.

Furthermore, our goal is to obtain an algorithm with good control on the complexity constant in the exponent and whose behaviour in practice reflects its complexity.

Main results

Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ and $f \in \mathbb{Q}[\mathbf{X}]$. We provide a symbolic algorithm computing $f^\star = \inf_{x \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n} f(x)$ and deciding whether it is reached or not under the following assumptions $\mathbf{R}$:

- the ideal $\langle \mathbf{F} \rangle$ is radical,
- $\mathbb{V}(\mathbf{F})$ is equidimensional of dimension $d > 0$,
- $\mathbb{V}(\mathbf{F})$ has finitely many singular points.

These assumptions are far from being restrictive since they often hold in practice. For instance, they are satisfied by any set of polynomials $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ whose Jacobian matrix has full rank.

For clarity, we state the main result in a simpler case. See also Section 6.5 for a complexity estimate in the general case. We count arithmetic operations $+, -, \times, \div$ in $\mathbb{Q}$ and sign evaluation at unit cost. We use the soft-O notation: $\widetilde{O}(a)$ indicates the omission of polylogarithmic factors in a.

Theorem 6.1. *There exists a probabilistic Las Vegas algorithm taking as input*

- $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ *defining a reduced regular sequence,*
- $f \in \mathbb{Q}[\mathbf{X}]$,

and that returns an algebraic representation of $f^\star = \inf_{x \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n} f(x)$. *If* $f^\star$ *is reached, it also returns an algebraic representation of* $x^\star \in \mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ *such that* $f(x^\star) = f^\star$. *Moreover, assume that the input polynomials have degree bounded by* D *and are represented by a straight-line program of size less than* L. *Then the algorithm performs*

$$\widetilde{O}\left(LD^7\left(\sqrt[3]{2}\,(s+1)\,(D-1)\right)^{3n}\right)$$

arithmetic operations in $\mathbb{Q}$.

We present the sketch of the algorithm.

Optimize$(f, \mathbf{F})$.

1. Perform a generic change of coordinates;
2. Compute a finite subset of $\mathbb{R}$ containing all the local extrema;
3. Decide which value in the previous set is $f^\star$;
4. Compute a finite set that intersect each connected component of $\mathrm{Crit}\,(f, V) \cap \mathbb{R}^n$;
   - if $f^\star$ is the image by f of a point $x^\star$ in this set then return $f^\star$ and $x^\star$.
   - else return $f^\star$, that is not reached.

Let $\mathscr{C}\,(f, \mathbf{F})$ be the union of the modified polar varieties defined in Chapter 5.

Step 2 is done by computing the critical values of $f_{|V\cap\mathbb{R}^n}$ and the asymptotic values of f on $\mathscr{C}\,(f, \mathbf{F})$. To this end, we prove that they are values of non-properness of a projection restricted to $\mathscr{C}\,(f, \mathbf{F})$.

To perform step 3, we use a topological property. This property reduces the problem of deciding the value of $f^\star$ among the local extrema to testing the emptiness of finitely many real algebraic varieties.

Finally, step 4 can be done by computing $\overline{\mathscr{C}\,(f, \mathbf{F}) \setminus \mathrm{Crit}\,(f, V)}^{\mathcal{Z}} \cap \mathrm{Crit}\,(f, V)$ and a set of sample points of $V \cap \mathbb{R}^n$. Indeed, the union of these two sets is finite and contains at least one point in each connected component of $\mathrm{Crit}\,(f, V)$.

We provide an implementation of this algorithm, available as a Maple library at `http://www-polsys.lip6.fr/~greuet/`. Its practical behaviour reflects its complexity and allows to solve problems that are either hard from the numerical point of view or unreachable by previous algorithms based on symbolic computation.

As an example, considering an objective polynomial and one constraint, both of degree 2 and increasing the number of variables, our implementation can solve problems with up to 32 variables in 4 hours. With two constraints, our implementation can solve problems with up to 11 variables in 5.3 hours. With a linear objective polynomial subject to one constraint of degree 4, both in 5 variables it takes 34 minutes.

We also considered examples coming from applications. We are able to solve problems with 5 constraints of degree 2 and 10 variables in less than 1 minute. Likewise, we solved an unconstrained problem with an objective polynomial in 6 variables of degree 8.

Note that this algorithm is a strong generalization of [118].

Organization of the chapter

In Section 6.2 definitions and notations that will be used throughout the chapter are introduced. Then the specifications and the description of the algorithm and its subroutines are presented in Section 6.3. Their proofs of correctness are presented in Section 6.4. A complexity analysis of the algorithm is given in Section 6.5. Practical results are presented in Section 6.6. The examples used in this section are detailed in Section 6.7.

6.2 Basic Definitions

6.2.1 Definitions

Assumptions of regularity. Let $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ be a polynomial family such that $\langle \mathbf{F} \rangle$ is radical and $V = \mathbb{V}(\mathbf{F})$ is equidimensional of dimension d. In this context, the set of singular points of V is the variety $\mathrm{Sing}(V)$ defined as the vanishing set of

- the polynomials in $\mathbf{F}$
- and the minors of size $n - d$ of $\mathsf{Jac}(\mathbf{F})$.

If $\mathrm{Sing}(V) = \varnothing$ then V is said to be *smooth*.

The polynomial family $\mathbf{F}$ satisfies assumptions $\mathbf{R}$ if

- the ideal $\langle \mathbf{F} \rangle$ is radical,
- $\mathbb{V}(\mathbf{F})$ is equidimensional of dimension $d > 0$,
- $\mathbb{V}(\mathbf{F})$ has finitely many singular points.

In this chapter, we consider a polynomial family $\mathbf{F} = \{f_1, \ldots, f_s\}$ that satisfies assumptions $\mathbf{R}$.

Sample points and modified polar varieties. We will denote by $\mathscr{S}(\mathbf{F})$ any finite set that contains at least a point in each connected component of $V \cap \mathbb{R}^n$. Such a set can be computed using [119].

We recall the definition of the modified polar varieties.

Definition 6.2. *For $1 \leq i \leq d-1$, let $\mathscr{C}(f, \mathbf{F}, i)$ be the algebraic variety defined as the vanishing set of*

- *the polynomials in $\mathbf{F}$,*
- *the minors of size $n - d + 1$ of $\mathsf{Jac}([f, \mathbf{F}], i + 1)$,*
- *and the variables $X_1, \ldots, X_{i-1}$.*

By convention, $\mathscr{C}(f, \mathbf{F}, d) = V \cap \mathbb{V}(X_1, \ldots, X_{d-1})$. Let $\mathscr{C}(f, \mathbf{F})$ be the union

$$\mathscr{C}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{C}(f, \mathbf{F}, i).$$

For $1 \leq i \leq d-1$, let $\mathscr{P}(f, \mathbf{F}, i) = \overline{\mathscr{C}(f, \mathbf{F}, i) \setminus \mathrm{Crit}(f, V)}^{\mathcal{Z}} \cap \mathrm{Crit}(f, V)$. For $i = d$, let $\mathscr{P}(f, \mathbf{F}, d) = \mathscr{C}(f, \mathbf{F}, d)$. Finally, let

$$\mathscr{P}(f, \mathbf{F}) = \bigcup_{1 \leq i \leq d} \mathscr{P}(f, \mathbf{F}, i).$$

6.2.2 Some Properties for Optimization

We state the properties we will request to solve problems (B) and (C).

Definition 6.3. *Given a set W, we say that property $Opt(W)$ holds if:*

- *W is finite,*
- *W contains every local extremum of $f_{|V\cap\mathbb{R}^n}$,*
- *let $W = \{a_1, \ldots, a_k\}$, $a_0 = -\infty$ and $a_{k+1} = +\infty$. There exists a non-empty Zariski-open set $\mathcal{Q} \subset \mathbb{C}$ such that for all $0 \leq i \leq k$:*
  - *either for all $t \in]a_i, a_{i+1}[\cap \mathcal{Q}$, $(f)^{-1}(t) \cap V \cap \mathbb{R}^n = \varnothing$,*
  - *or for all $t \in]a_i, a_{i+1}[\cap \mathcal{Q}$, $(f)^{-1}(t) \cap V \cap \mathbb{R}^n \neq \varnothing$.*

6.2.3 Genericity Properties

In the sequel we will assume some properties that are proved to be generically true. A value $c \in \mathbb{R}$ is isolated in $f(V \cap \mathbb{R}^n)$ if and only if there exists a neighborhood $\mathcal{B}$ of c such that $\mathcal{B} \cap f(V \cap \mathbb{R}^n) = \{c\}$. For simplicity, given $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$, we will denote by

- $\mathfrak{R}(f, \mathbf{F})$: for all $t \in \mathbb{R} \setminus f(\mathrm{Crit}(f, V) \cup \mathrm{Sing}(V))$, the ideal $\langle \mathbf{F}, f - t\rangle$ is radical, equidimensional and $\mathbb{V}(\mathbf{F}, f - t)$ is either smooth, of dimension $d-1$ or is empty.
- $\mathfrak{P}_1(f, \mathbf{F})$: there exists a non-empty Zariski-open set $\mathcal{Q} \subset \mathbb{C}$ such that for all $t \in \mathbb{R} \cap \mathcal{Q}$, the restriction of $\pi_{\leq i-1}$ to $V \cap \mathbb{V}(f - t) \cap \mathscr{C}(f, \mathbf{F}, i)$ is proper for $1 \leq i \leq d$.
- $\mathfrak{P}_2(f, \mathbf{F})$: for any critical value c of $f_{|V\cap\mathbb{R}^n}$ that is not isolated in $f(V \cap \mathbb{R}^n)$, there exists $x_c \in \mathscr{P}(f, \mathbf{F})$ such that $f(x_c) = c$.

Note that these properties are consequences of properties of modified polar varieties. Indeed, we proved, up to a generic change of coordinates, that:

- $\mathfrak{R}(f, \mathbf{F})$ holds in Lemma 5.13 page 66;
- $\mathfrak{P}_1(f, \mathbf{F})$ holds in Lemma 5.17 page 69;
- $\mathfrak{P}_2(f, \mathbf{F})$ holds in Theorem 5.11 page 65;

6.3 Algorithm

6.3.1 Specifications

In the descriptions of the algorithms, a polynomial family $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ is represented by the list $[f_1, \ldots, f_s]$. Likewise, an ideal (resp. an algebraic variety) is represented by a finite list of polynomials generating it (resp. defining it), for instance a Gröbner basis.

Let $Y \subset \mathbb{R}^n$ be a finite set defined by polynomials in $\mathbb{Q}[\mathbf{X}]$. It will be represented by a rational parametrization, that is a sequence of polynomials $q, q_0, q_1, \ldots, q_n \in \mathbb{Q}[U]$ such that for all $x = (x_1, \ldots, x_n) \in Y$, there exists a unique $u \in \mathbb{R}$ such that

$$\begin{cases} q(u) &= 0 \\ x_1 &= q_1(u)/q_0(u) \\ &\vdots \\ x_n &= q_n(u)/q_0(u) \end{cases}$$

In other words, there is a bijection between the roots of q and the points in Y. Thus, a single point in $x \in Y$ can be represented by $q, q_0, q_1, \ldots, q_n$ and an interval isolating the root of q corresponding with x. Such an algebraic representation can be computed from a Gröbner basis ([115]) and algorithms computing such a representation are implemented in computer algebra systems. Likewise, a real algebraic number α is represented by a univariate polynomial P and an isolating interval I.

6.3.2 Main Algorithm

One introduces the subroutines used in the description of the main algorithm. A complete description will be given in the sequel. Given a univariate polynomial P, $\mathrm{Roots}_{\mathbb{R}}(P)$ denotes its set of real roots.

The routine SetContainingLocalExtrema**.** This routine takes as input $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$. If $\mathfrak{P}_1(f, \mathbf{F})$, $\mathfrak{P}_2(f, \mathbf{F})$ and $\mathfrak{R}(f, \mathbf{F})$ hold, it returns a list ListSamplePoints $\subset \mathbb{Q}[\mathbf{X}]$, a list ListCriticalPoints $\subset \mathbb{Q}[\mathbf{X}]$ and a polynomial $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ such that, denoting by W the set

$$W = f(\mathbb{V}(\mathsf{ListSamplePoints})) \cup f(\mathbb{V}(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}}),$$

property $\mathrm{Opt}(W)$ holds.

The routine FindInfimum**.** This routine takes as input $f \in \mathbb{Q}[\mathbf{X}]$, $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, a list ListSamplePoints $\subset \mathbb{Q}[\mathbf{X}]$, a list ListCriticalPoints $\subset \mathbb{Q}[\mathbf{X}]$ and a polynomial $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ such that, denoting by W the set

$$W = f(\mathbb{V}(\mathsf{ListSamplePoints})) \cup f(\mathbb{V}(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}}),$$

property $\mathrm{Opt}(W)$ holds. If $\mathfrak{R}(f, \mathbf{F})$ holds, it returns

- $+\infty$ if $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is empty;
- $-\infty$ if f is not bounded below on $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$;
- if $f^\star > -\infty$ is not reached: $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ and an interval I such that $f^\star$ is the only root of P_{NP} in I;

- if $f^\star$ is reached, a rational parametrization with isolating intervals representing $f^\star$ and a minimizer $x^\star$.

The main routine Optimize takes as input $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$. It returns

- $+\infty$ if $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is empty;
- $-\infty$ if f is not bounded below over $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$;
- if $f^\star > -\infty$ is not reached: $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ and an interval I isolating $f^\star$;
- if $f^\star$ is reached, a rational parametrization encoding $x^\star$ and $f^\star(x^\star)$.

We give the description of Optimize.

Optimize$(f, \mathbf{F})$

- $\mathbf{A} \leftarrow$ a random matrix in $\mathrm{GL}_n(\mathbb{Q})$;
- $(\mathsf{ListSamplePoints}^{\mathbf{A}}, \mathsf{ListCriticalPoints}^{\mathbf{A}}, P_{\mathsf{NP}}^{\mathbf{A}}) \leftarrow \mathsf{SetContainingLocalExtrema}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$;
- $\mathsf{Infimum} \leftarrow \mathsf{FindInfimum}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, \mathsf{ListSamplePoints}^{\mathbf{A}}, \mathsf{ListCriticalPoints}^{\mathbf{A}}, P_{\mathsf{NP}}^{\mathbf{A}}\right)$;
- return Infimum.

Example 6.4. *Let* $f = (xy-1)^2 + y^2 + z^2 + 1$ *and* $V = \mathbb{V}(z)$. *After the change of variables, the routine* SetContainingLocalExtrema *returns* $\mathsf{ListSamplePoints}^{\mathbf{A}} = [x, y, z]$, $\mathsf{ListCriticalPoints}^{\mathbf{A}} = [x, y, z]$ *and* $P_{\mathsf{NP}}^{\mathbf{A}} = T - 1$. *This means that the point* $(0,0,0)$ *is a critical point, with associated critical value* 2, *and that* 1 *is potentially a value at infinity. The set containing the local extrema is* $\{1, 2\}$.

The next step is to decide which value in this set is the infimum. To this end, FindInfimum *test whether* f *reaches values in* $]-\infty, 1[$, $\{1\}$ *and* $]1, 2[$. *The way to test such a property is described in the next section. In this example,* f *does not reach any value in* $]-\infty, 1[$, $\{1\}$ *but reaches all the values in* $]1, 2[$ *(see Figure 6.1). This means that* $f^\star = 1$, *that is not attained.*

6.3.3 Subroutines

We describe the subroutines SetContainingLocalExtrema and FindInfimum. They are themselves based on other standard subroutines. The algorithm SetContainingLocalExtrema uses the subroutines RealSamplePoints and SetOfNonProperness described below.

The routine RealSamplePoints**.** Given $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, RealSamplePoints returns a list of equations ListSamplePoints $\subset \mathbb{Q}[\mathbf{X}]$ such that $\mathbb{V}(\mathsf{ListSamplePoints})$ contains at least a point in each connected component of $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$. Such an algorithm is given in [119].

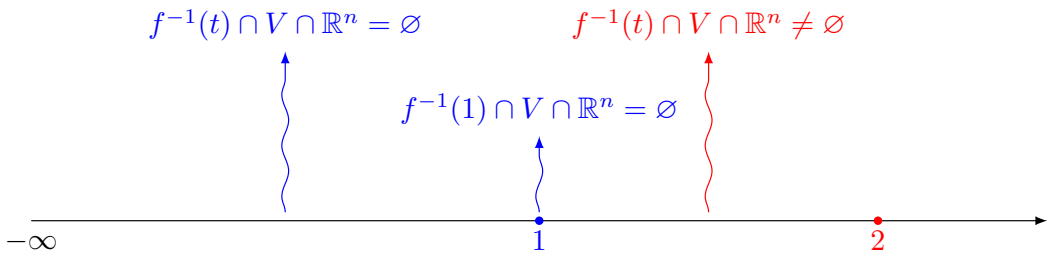


Figure 6.1: f does not reach any value ≤ 1 but reaches each value in $]1, 2[$. Thus $f^\star = 1$.

The routine SetOfNonProperness**.** It takes as input $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{G} \subset \mathbb{Q}[\mathbf{X}]$ such that the set of non-properness of the projection π_T restricted to $\mathbb{V}(f - T) \cap \mathbb{V}(\mathbf{G})$ is finite. It returns a univariate polynomial in T whose set of roots contains the set of non-properness of the restriction of π_T to $\mathbb{V}(f - T) \cap \mathbb{V}(\mathbf{G})$. Such an algorithm is given in [89, 117, 120].

The algorithm SetContainingLocalExtrema is described below. It takes as input $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, $\mathfrak{P}_1(f, \mathbf{F})$, $\mathfrak{P}_2(f, \mathbf{F})$ and $\mathfrak{R}(f, \mathbf{F})$. It returns a list ListSamplePoints $\subset \mathbb{Q}[\mathbf{X}]$, a list ListCriticalPoints $\subset \mathbb{Q}[\mathbf{X}]$ and a polynomial $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ such that property

$$\mathrm{Opt}\left(f\left(\mathbb{V}\left(\mathsf{ListSamplePoints}\right)\right) \cup f\left(\mathbb{V}\left(\mathsf{ListCriticalPoints}\right)\right) \cup \mathrm{Roots}_{\mathbb{R}}\left(P_{\mathsf{NP}}\right)\right)$$

holds.

To this end, a list containing polynomials that generates a 0-dimensional set of sample points of V is first computed, using the subroutine RealSamplePoints. Then, for $1 \leq i \leq d$, it computes a list of polynomials generating $\mathscr{C}(f, \mathbf{F}, i)$. Afterward, a polynomial whose set of roots contains the set of non-properness $\mathsf{NP}(\pi_T, \mathscr{C}(f, \mathbf{F}, i))$ is computed by SetOfNonProperness. It is multiplied by the polynomial obtained at the previous step. Then at step i, a polynomial whose set of roots contains $\bigcup_{j \leq i} \mathsf{NP}(\pi_T, \mathscr{C}(f, \mathbf{F}, j))$ is obtained. Finally, a list of equations defining $\mathscr{P}(f, \mathbf{F}, i)$ is computed from the one defining $\mathscr{C}(f, \mathbf{F}, i)$. Now we can describe the algorithm.

SetContainingLocalExtrema$(f, \mathbf{F})$

- ListSamplePoints $\leftarrow$ RealSamplePoints$(\mathbf{F})$;
- $P_{\mathsf{NP}} \leftarrow 1$;
- for $1 \leq i \leq d$ do
  - $\mathsf{L}_{\mathscr{C}}[i] \leftarrow$ a list of equations defining $\mathscr{C}(f, \mathbf{F}, i)$;
  - $P_{\mathsf{NP}} \leftarrow$ the univariate polynomial $P_{\mathsf{NP}} \times$ SetOfNonProperness$(f, \mathscr{C}(f, \mathbf{F}, i))$;
  - ListCriticalPoints$[i] \leftarrow$ a list of equations defining $\mathscr{P}(f, \mathbf{F}, i)$.

- return $(\mathsf{ListSamplePoints}, \mathsf{ListCriticalPoints}, P_{\mathsf{NP}})$;

Its correctness is stated in Proposition 6.6. Its proof relies on intermediate results presented in Section 6.4.1.

The routine FindInfimum uses the following subroutine.

The routine IsEmpty. Given $\mathbf{G} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$, this routine returns either true if $\mathbb{V}(\mathbf{G}) \cap \mathbb{R}^n$ is empty of false if it is non-empty. The routine SamplePoints, based on [119], can be adapted to provide such an algorithm.

Finally, we present the routine FindInfimum. It takes as input:

- $f \in \mathbb{Q}[\mathbf{X}]$,
- $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$ and $\mathfrak{R}(f, \mathbf{F})$,
- $\mathsf{ListSamplePoints} \subset \mathbb{Q}[\mathbf{X}]$, $\mathsf{ListCriticalPoints} \subset \mathbb{Q}[\mathbf{X}]$ and $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ such that $\mathrm{Opt}(W)$ holds with $W = f(\mathbb{V}(\mathsf{ListSamplePoints})) \cup f(\mathbb{V}(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}})$.

It returns

- $+\infty$ if $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is empty;
- $-\infty$ if f is not bounded below over $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$;
- if $f^\star > -\infty$ is not reached: $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ and an interval I isolating $f^\star$;
- if $f^\star$ is reached, a rational parametrization encoding $x^\star$ and $f^\star(x^\star)$.

Let $W = f(\mathbb{V}(\mathsf{ListSamplePoints})) \cup f(\mathbb{V}(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}})$. By definition, $f^\star$ is the smallest value c in $V \cap \mathbb{R}^n$ such that

(i) if $t < c$ then $t \notin f(V \cap \mathbb{R}^n)$ and

(ii) for all $t \geq c$, $[c, t]$ meets $V \cap \mathbb{R}^n$.

Since $\mathrm{Opt}(W)$ holds, $f^\star \in W$. Then we explain how to find the smallest value in W satisfying the above condition. We consider $a_0 = -\infty$, $a_1 < \cdots < a_k$ the values in W and $a_{k+1} = +\infty$. If the algorithm get in step i then this means that $f^\star \notin \{a_0, \ldots, a_{i-1}\}$. Then it first checks whether a_i is the image of a point $x^\star$ in $\mathsf{RealSamplePoints}(\mathbf{F})$ or in $\mathscr{C}(f, \mathbf{F})$. If it is, then the minimizer $x^\star$ and $a_i = f^\star$ are returned. Else, it checks whether a_i satisfies condition (ii). To this end, because of the last point in property $\mathrm{Opt}(W)$, it is sufficient to test the emptiness of $f^{-1}(t) \cap V \cap \mathbb{R}^n$ for only one value of $t \in]a_i, a_{i+1}[$. If $f^{-1}(q_i) \cap V \cap \mathbb{R}^n$ is not empty for some random rational $q_i \in]a_i, a_{i+1}[$ then $f^\star = a_i$ and it is not reached. Else, $a_i \neq f^\star$ and we go on with a_{i+1}. If the algorithm leaves step

k without returning a finite value for $f^\star$, this means that f takes no value on $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$, so that $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is empty. Hence, $+\infty$ is returned. Now we can describe the algorithm.

FindInfimum$(f, \mathbf{F}, \mathsf{ListSamplePoints}, \mathsf{ListCriticalPoints}, P_{\mathsf{NP}})$

- $a_1 < \cdots < a_k \leftarrow f(\mathbb{V}(\mathsf{ListSamplePoints})) \cup f(\mathbb{V}(\mathsf{ListCriticalPoints})) \cup \mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}})$;
- $a_{k+1} = +\infty$;
- $q_0 \leftarrow$ a random rational $< a_1$;
- if IsEmpty$(\{f - q_0, \mathbf{F}\})$=false then
  - return $-\infty$;
- $i \leftarrow 1$;
- while $i \leq k$ do
  - if $a_i \in f(\mathbb{V}(\mathsf{ListSamplePoints})) \cup f(\mathbb{V}(\mathsf{ListCriticalPoints}))$ then
    - RP $\leftarrow$ a rational parametrization encoding a minimizer $x^\star$ and $f(x^\star) = a_i$;
    - return RP

    else
    - $q_i \leftarrow$ a random rational in $]a_i, a_{i+1}[$;
    - if IsEmpty$(\{f - q_i, \mathbf{F}\})$=false then
      - return $(P_{\mathsf{NP}},]q_{i-1}, q_i[)$

      else
      - $i \leftarrow i + 1$
- return a_{k+1}

Its proof of correctness is given by Proposition 6.10 in Section 6.10.

By assumption on the inputs, the variety $\mathbb{V}(\mathsf{ListSamplePoints}) \cup \mathbb{V}(\mathsf{ListCriticalPoints})$ is finite. As explained in Section 6.3.1, a single point x that lies in this variety can be represented by a rational parametrization $q, q_0, q_1, \ldots, q_n$ and an interval isolating the corresponding root of q. From this parametrization and the isolating interval, an interval isolating $f(x)$ can be computed. Likewise, the values in $\mathrm{Roots}_{\mathbb{R}}(P_{\mathsf{NP}})$ are represented by isolating intervals. These intervals can be computed such that they do not intersect. Hence, they can be sorted so that the i-th interval corresponds with a_i.

Then, testing whether $a_i \in f(\mathbb{V}(\mathsf{ListSamplePoints})) \cup f(\mathbb{V}(\mathsf{ListCriticalPoints}))$ is done by testing whether the interval corresponding with a_i comes from the parametrization of $\mathbb{V}(\mathsf{ListSamplePoints}) \cup \mathbb{V}(\mathsf{ListCriticalPoints})$. If so, the parametrization and the isolating interval of q corresponding with a_i are an encoding for a_i and a point x_{a_i} such that $f(x_{a_i}) = a_i$.

6.4 Proof of Correctness of Optimize

We first consider the following theorem, stating that under assumptions $\mathbf{R}$, the properties $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold up to a generic change of coordinates.

Theorem 6.5. *Let $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$. There exists a non-empty Zariski-open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, properties $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold.*

Proof. This is a consequence of the properties of the modified polar varieties.

Property $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$. We proved in Lemma 5.13 that for all real number t not in $f(\mathrm{Crit}(f, V) \cup \mathrm{Sing}(V))$,

- $\mathbb{V}(\mathbf{F}, f - t)$ is either empty or equidimensional of dimension $d - 1$,
- $\mathbb{V}(\mathbf{F}, f - t)$ is smooth,
- the ideal $\langle \mathbf{F}, f - t \rangle$ is radical.

This means that property $\mathfrak{R}(f, \mathbf{F})$ holds. In particular, for any change of coordinates $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, property $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds.

Property $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$. According to Lemma 5.17, there exists a non-empty Zariski-open set $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, there exists a non-empty Zariski-open set $\mathcal{T}^{\mathbf{A}} \subset \mathbb{C}$ such that for all $t \in \mathbb{R} \cap \mathcal{T}^{\mathbf{A}}$, the restriction of $\pi_{\leq i-1}$ to $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is proper for $1 \leq i \leq d$. In particular, for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$, property $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds.

Property $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$. We proved in Theorem 5.11 that there exists a non-empty Zariski-open set $\mathscr{O}_2 \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$, for any critical value c of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ that is not isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, there exists $x_c \in \mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ such that $f^{\mathbf{A}}(x_c) = c$. In particular, for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_2$, property $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds.

Finally, let $\mathscr{O} = \mathscr{O}_1 \cap \mathscr{O}_2$. Since $\mathscr{O}_1$ and $\mathscr{O}_2$ are non-empty Zariski-open sets, so is $\mathscr{O}$. Furthermore, for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, properties $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold. □

Let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski-open set given in Theorem 6.5. We prove in the sequel that if the random matrix chosen in Optimize lies in $\mathscr{O}$ then Optimize is correct.

Given $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, let $W^{\mathbf{A}}$ be the set of values

$$W^{\mathbf{A}} = f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right) \cup f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right) \cup \mathsf{NP}\left(\pi_T, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right) \subset \mathbb{C}.$$

The correctness of Optimize is an immediate consequence of the correctness of the subroutines SetContainingLocalExtrema and FindInfimum. The correctness of SetContainingLocalExtrema is given in Section 6.4.1 below while the one of FindInfimum is given in Section 6.4.2 page 95.

6.4.1 Correctness of SetContainingLocalExtrema

We first state the correctness of SetContainingLocalExtrema $\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$.

Proposition 6.6. *Let $f \in \mathbb{Q}[\mathbf{X}]$ and $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ satisfying assumptions $\mathbf{R}$. Let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski-open set given in Theorem 6.5. Then for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$,* SetContainingLocalExtrema $\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ *is correct.*

Proving the above proposition is equivalent to prove that $\mathrm{Opt}\left(W^{\mathbf{A}}\right)$ holds. That is the purpose of Propositions 6.7, 6.8 and 6.9 below.

Since $V^{\mathbf{A}}$ is an algebraic variety, the image $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ is a semi-algebraic subset of $\mathbb{R}$. Hence, it is a finite union of real disjoint intervals. They are either of the form $[b_i, b_{i+1}]$, $[b_i, b_{i+1}[$, $]b_i, b_{i+1}]$ or $\{b_i\}$, for some $b_0 \in \mathbb{R} \cup \{-\infty\}$ and $b_1, \ldots, b_r \in \mathbb{R}$. Then the local extrema of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ are exactly the b_i. If b_i is an endpoint included in the interval, then it is reached, meaning that it is either a minimum or a maximum. If the interval is a single point then b_i is isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$. Else, it is not isolated. If b_i is an endpoint that is not included in the interval, then $b_i \notin f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ is an extremum that is not reached. Remark that our goal is to find b_0, that is necessarily $f^\star$.

Proposition 6.7. *For all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, the set $W^{\mathbf{A}}$ contains every local extremum of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$. More precisely, let $\ell \in \mathbb{R}$ be a local extremum of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$.*

1. *If ℓ is a value that is isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ then $\ell \in f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right)$;*
2. *if ℓ is a value that is not isolated in $f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ such that there exists $x_\ell \in V^{\mathbf{A}} \cap \mathbb{R}^n$ with $f^{\mathbf{A}}(x_\ell) = \ell$ then $\ell \in f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$;*
3. *if $\ell \notin f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ then $\ell \in \mathsf{NP}\left(\pi_T, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$.*

Proof. Let $\ell \in \mathbb{R}$ be a local extremum.

Case 1. Since ℓ is isolated, there exists $x_\ell \in V^{\mathbf{A}} \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}(x_\ell) = \ell$. Let $C^{\mathbf{A}}$ be the connected component of $V^{\mathbf{A}} \cap \mathbb{R}^n$ containing x_ℓ. We prove that $f^{\mathbf{A}}$ is constant on $C^{\mathbf{A}}$. Let $x' \in C^{\mathbf{A}}$ and assume that $f^{\mathbf{A}}(x') \neq \ell$. Since ℓ is isolated, there exists a neighborhood $\mathcal{B}$ of ℓ such that $f^{\mathbf{A}}\left(C^{\mathbf{A}}\right)$ would be the union of $\{\ell\}$ and some set S that contains $f^{\mathbf{A}}(x')$ but that does not meet $\mathcal{B}$. In particular, $f^{\mathbf{A}}\left(C^{\mathbf{A}}\right)$ would not be connected. This is a contradiction since $f^{\mathbf{A}}$ is continuous and $C^{\mathbf{A}}$ connected.

The set $\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)$ is a set containing at least a point in each connected component of $V^{\mathbf{A}} \cap \mathbb{R}^n$. In particular it contains a point y in the connected component $C^{\mathbf{A}}$ of x_ℓ. Since the restriction of $f^{\mathbf{A}}$ to $C^{\mathbf{A}}$ is constant, $f^{\mathbf{A}}(y) = \ell$, so that $\ell \in f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right)$.

Case 2. Since $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, property $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds. This means that there exists $x_\ell \in \mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ such that $f^{\mathbf{A}}(x_\ell) = \ell$, that is $\ell \in f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$.

Case 3. If $\ell \notin f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$, by definition, as a local extremum, there exists a closed neighborhood $\mathcal{U}$ of ℓ such that we can construct a sequence $(x^{(k)})_{k\in\mathbb{N}} \subset \left(f^{\mathbf{A}}\right)^{-1}(\mathcal{U}) \cap V^{\mathbf{A}} \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}\left(x^{(k)}\right) \to \ell$. We first prove that we can not extract a converging subsequence from $(x^{(k)})$. Indeed, assume that there exists a converging subsequence $(x'^{(k)})$ and denote by x its limit. Since $V^{\mathbf{A}} \cap \mathbb{R}^n$ and $\left(f^{\mathbf{A}}\right)^{-1}(\mathcal{U}) \cap \mathbb{R}^n$ are closed sets for the euclidean topology, x lies in $\left(f^{\mathbf{A}}\right)^{-1}(\mathcal{U}) \cap V^{\mathbf{A}} \cap \mathbb{R}^n$.

As a subsequence of $f^{\mathbf{A}}\left(x^{(k)}\right)$, the sequence $f^{\mathbf{A}}\left(x'^{(k)}\right)$ tends to ℓ. Moreover, by continuity of $f^{\mathbf{A}}$, $f^{\mathbf{A}}\left(x'^{(k)}\right)$ tends to $f^{\mathbf{A}}(x)$. This would imply that $f^{\mathbf{A}}(x) = \ell$, that is ℓ is attained, which is a contradiction. Since this is true for all converging subsequence $(x'^{(k)})$ of $(x^{(k)})$, this implies that $(x^{(k)})$ can not be bounded. Finally, this proves that $\|(x^{(k)})\|$ tends to ∞.

Let $\varepsilon > 0$. There exists $k_0 \in \mathbb{N}$ such that for all $k \geq k_0$, $f^{\mathbf{A}}\left(x^{(k)}\right) \in [\ell - \varepsilon, \ell + \varepsilon]$. By construction of $x^{(k)}$, $\left(f^{\mathbf{A}}\right)^{-1}\left(f^{\mathbf{A}}\left(x^{(k)}\right)\right) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing$.

By Theorem 6.5 and since by assumption, $\mathbf{A} \in \mathscr{O}$, properties $\mathfrak{R}\left(\mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold. Thus Theorem 5.9 ensures that for all $t \in \mathbb{R} \cap \mathcal{Q}^{\mathbf{A}}$, $V^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ is empty if and only if $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ is empty.

Then $\left(f^{\mathbf{A}}\right)^{-1}\left(f^{\mathbf{A}}\left(x^{(k)}\right)\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n \neq \varnothing$. Picking a point $\widetilde{x}_k$ in this last set, for each $k \geq k_0$, leads to the construction of a sequence of points $(\widetilde{x}_k)$ in $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$, that converges to ℓ. Since $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \subset V^{\mathbf{A}}$ and ℓ is not reached, this sequence is unbounded. Then considering the sequence $\left(\widetilde{x}_k, t = f^{\mathbf{A}}(\widetilde{x}_k)\right)$ proves that π_T restricted to $\mathbb{V}\left(f^{\mathbf{A}} - T\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ is not proper at ℓ. □

Proposition 6.8. *For all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, the set $W^{\mathbf{A}}$ is finite.*

Proof. Since $W^{\mathbf{A}} = f^{\mathbf{A}}\left(\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)\right) \cup f^{\mathbf{A}}\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right) \cup \mathsf{NP}\left(\pi_T, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$, it is sufficient to prove that

1. $\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)$ is finite,
2. for $1 \leq i \leq d$, $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is finite and
3. $\mathsf{NP}\left(\pi_T, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$ is finite.

The first assertion is true for all $\mathbf{A}$, since by assumption, $\mathscr{S}\left(\mathbf{F}^{\mathbf{A}}\right)$ is a finite set and the second assertion is proved in Theorem 5.12 page 65. Let us prove the third assertion.

By Theorem 6.5 and since $\mathbf{A} \in \mathscr{O}$, $\mathfrak{R}\left(\mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds.

We first prove that the set of values $t \in \mathbb{C}$ such that there exists a sequence $(x^{(k)})_{k\in\mathbb{N}} \subset \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ satisfying $\lim_{k\to+\infty} ||x^{(k)}|| = +\infty$ and $\lim_{k\to+\infty} f^{\mathbf{A}}(x^{(k)}) = t$ is finite.

Let $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski-open set given in Theorem 5.9 and $\mathscr{O}_3 \subset \mathrm{GL}_n(\mathbb{C})$ the Zariski-open set given in Theorem 5.12 (page 65). Let $\mathscr{O} = \mathscr{O}_1 \cap \mathscr{O}_3$ and let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$. Let $Z^{\mathbf{A}}$ be an irreducible component of $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and consider the map $x \in Z^{\mathbf{A}} \to f^{\mathbf{A}}(x) \in \mathbb{C}$.

Suppose first that $f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ has dimension 0. Then, $R_\infty\left(f^{\mathbf{A}}, Z^{\mathbf{A}}\right) \subset f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ which has dimension 0.

Suppose now that $f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ has dimension 1. By the theorem on the dimension of fibers, [134, Theorem 7, Chapter 1, p. 76], there exists a non-empty Zariski-open set $\mathscr{W} \subset \mathbb{C}$ such that for all $t \in \mathscr{W}$, $\dim\left(Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)\right) = \dim\left(Z^{\mathbf{A}}\right) - 1$.

Let $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ be the Zariski-open set given in Theorem 5.9. According to Lemma 7.2, if t belongs to $\mathbb{R} \cap \mathcal{Q}^{\mathbf{A}}$ then $Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)$ is either empty or 0-dimensional.

Hence, two situations may occur:

- either $Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)$ is empty and then $\dim\left(Z^{\mathbf{A}}\right) = 0$ which is not possible since, by assumption, $\dim\left(f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)\right) = 1$;
- or $Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)$ has dimension 0 and then $\dim\left(Z^{\mathbf{A}}\right) = 1$. This implies that the set $R_\infty\left(f^{\mathbf{A}}, Z^{\mathbf{A}}\right) \subset \mathbb{C}$ is the set of non-properness of the map $x \in Z^{\mathbf{A}} \longmapsto f^{\mathbf{A}}(x)$. Since $Z^{\mathbf{A}}$ has dimension 1, this set of non-properness has dimension at most 0 by [70, Theorem 3.8].

Since $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ has finitely many irreducible components, the lemma is proved.

Finally, we prove in the sequel that a value $t \in \mathbb{C}$ such that there exists a sequence $(x^{(k)})_{k\in\mathbb{N}} \subset \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ satisfying $\lim\limits_{k\to+\infty} ||x^{(k)}|| = +\infty$ and $\lim\limits_{k\to+\infty} f^{\mathbf{A}}(x^{(k)}) = t$ lies in $\mathsf{NP}\left(\pi_T, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$ and conversely.

Let $t_0 \in \mathbb{C}$ and $\left(x^{(k)}\right) = \left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ be a sequence of points in $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ satisfying $\lim\limits_{k\to+\infty} \left\|x^{(k)}\right\| = +\infty$ and $\lim\limits_{k\to+\infty} f^{\mathbf{A}}\left(x^{(k)}\right) = t_0$.

Let $\varepsilon > 0$. There exists $N \in \mathbb{N}$ such that for all $k \geq N$, $\left|f^{\mathbf{A}}\left(x^{(k)}\right) - t_0\right| \leq \varepsilon$. In particular, for all $k \geq N$, $\left(f^{\mathbf{A}}\right)\left(x^{(k)}\right)$ lies in the closed ball $\overline{B}\left(t_0, \varepsilon\right)$. This means that $\pi_T^{-1}\left(\overline{B}\left(t_0, \varepsilon\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - T\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ contains all the points

$$\left(x_1^{(k)}, \ldots, x_n^{(k)}, t = f^{\mathbf{A}}\left(x^{(k)}\right)\right)$$

for $k \geq N$. Since $\left(x^{(k)}\right)$ is not bounded,

$$\pi_T^{-1}\left(\overline{B}\left(t_0, \varepsilon\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - T\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right),$$

contains points that are not bounded. By the definition of properness, this means that t_0 is a point where the projection π_T restricted to $\mathbb{V}\left(f^{\mathbf{A}} - T\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is not proper.

Conversely, if $t_0 \in \mathbb{C}$ is such that for all $\varepsilon > 0$,

$$\pi_T^{-1}\left(\overline{B}\left(t_0, \varepsilon\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - T\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$$

is not bounded, we can construct by induction a sequence $\left(\left(x^{(k)}, f^{\mathbf{A}}\left(x^{(k)}\right)\right)\right)_{k\in\mathbb{N}}$, such that:

- for all $k \in \mathbb{N}$, $\left(x^{(k)}, f^{\mathbf{A}}\left(x^{(k)}\right)\right) \in \pi_T^{-1}\left(\overline{B}\left(t_0, \frac{1}{k}\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - T\right) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$;
- for all $k \in \mathbb{N}$, $\|x_{k+1}\| > 2\left\|x^{(k)}\right\|$.

In particular, $\left(x^{(k)}\right)_{k\in\mathbb{N}} \subset \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$, $\lim_{k\to+\infty} \left\|x^{(k)}\right\| = +\infty$ and $\lim_{k\to+\infty} f^{\mathbf{A}}(x^{(k)}) = t_0$. □

Proposition 6.9. *For all* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, *writing* $W^{\mathbf{A}} = \{a_1, \ldots, a_k\}$, $a_0 = -\infty$ *and* $a_{k+1} = +\infty$, *there exists a non-empty Zariski-open set* $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ *such that for all* $0 \leq i \leq k$:

- *either for all* $t \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$, $\left(f^{\mathbf{A}}\right)^{-1}(t) \cap V^{\mathbf{A}} \cap \mathbb{R}^n = \varnothing$,
- *or for all* $t \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$, $\left(f^{\mathbf{A}}\right)^{-1}(t) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing$.

Proof. Assume on the contrary that there exists i such that there exists $a \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$ such that $\left(f^{\mathbf{A}}\right)^{-1}(a) \cap V^{\mathbf{A}} \cap \mathbb{R}^n = \varnothing$ and $b \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$ such that $\left(f^{\mathbf{A}}\right)^{-1}(b) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing$. Then without loss of generality, we can assume that $a < b$ and

$$b = \inf\left\{t \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}} \text{ s.t. } \left(f^{\mathbf{A}}\right)^{-1}(t) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing\right\}.$$

Then b is a local infimum of $f^{\mathbf{A}}_{|V^{\mathbf{A}}\cap\mathbb{R}^n}$. According to Proposition 6.7, b lies in $W^{\mathbf{A}}$. Hence there exists i such that $b = a_i$, which is a contradiction. □

We are now able to give a proof of correctness of SetContainingLocalExtrema, that relies on the above propositions.

Proof of Proposition 6.6. Let $\mathsf{ListSamplePoints} \subset \mathbb{Q}[\mathbf{X}]$, $\mathsf{ListCriticalPoints} \subset \mathbb{Q}[\mathbf{X}]$ and $P_{\mathsf{NP}} \in \mathbb{Q}[T]$ be the output of $\mathsf{SetContainingLocalExtrema}(f, \mathbf{F})$. Denote by W the set

$$f\left(\mathbb{V}\left(\mathsf{ListSamplePoints}\right)\right) \cup f\left(\mathbb{V}\left(\mathsf{ListCriticalPoints}\right)\right) \cup \mathrm{Roots}_{\mathbb{R}}\left(P_{\mathsf{NP}}\right).$$

The routine SetContainingLocalExtrema is correct if property $\mathrm{Opt}(W)$ holds. Then we prove that

1. W is finite,
2. W contains every local extremum of $f_{|V\cap\mathbb{R}^n}$,
3. let $W = \{a_1, \ldots, a_k\}$, $a_0 = -\infty$ and $a_{k+1} = +\infty$. There exists a non-empty Zariski-open set $\mathcal{Q} \subset \mathbb{C}$ such that for all $0 \leq i \leq k$:
   - either for all $t \in]a_i, a_{i+1}[\cap \mathcal{Q}$, $(f)^{-1}(t) \cap V \cap \mathbb{R}^n = \varnothing$,
   - or for all $t \in]a_i, a_{i+1}[\cap \mathcal{Q}$, $(f)^{-1}(t) \cap V \cap \mathbb{R}^n \neq \varnothing$.

The first assertion comes from Proposition 6.8. The second one is a consequence of Proposition 6.7. Finally, the last assertion is given by Proposition 6.9. □

6.4.2 Correctness of FindInfimum

Finally, we prove that FindInfimum is correct.

Proposition 6.10. *Let* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, $f \in \mathbb{Q}[\mathbf{X}]$, $\mathbf{F} \subset \mathbb{Q}[\mathbf{X}]$ *satisfying assumptions* $\mathbf{R}$, $\mathsf{ListSamplePoints}^{\mathbf{A}} \subset \mathbb{Q}[\mathbf{X}]$, $\mathsf{ListCriticalPoints}^{\mathbf{A}} \subset \mathbb{Q}[\mathbf{X}]$ *and* $P^{\mathbf{A}}_{\mathsf{NP}} \in \mathbb{Q}[T]$. *Let* $W^{\mathbf{A}} = \{a_1, \ldots, a_k\}$, *be the finite algebraic set*

$$f^{\mathbf{A}}\left(\mathbb{V}\left(\mathsf{ListSamplePoints}^{\mathbf{A}}\right)\right) \cup f\left(\mathbb{V}\left(\mathsf{ListCriticalPoints}^{\mathbf{A}}\right)\right) \cup \mathrm{Roots}_{\mathbb{R}}\left(P^{\mathbf{A}}_{\mathsf{NP}}\right),$$

and assume that Opt $\left(W^{\mathbf{A}}\right)$ *is satisfied. Then let* $a_0 = -\infty$, $a_{k+1} = +\infty$ *and let* $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ *be the Zariski-open set satisfying, for all* $0 \leq i \leq k$*:*

- *either for all* $t \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$, $\left(f^{\mathbf{A}}\right)^{-1}(t) \cap V^{\mathbf{A}} \cap \mathbb{R}^n = \varnothing$,
- *or for all* $t \in]a_i, a_{i+1}[\cap \mathcal{Q}^{\mathbf{A}}$, $\left(f^{\mathbf{A}}\right)^{-1}(t) \cap V^{\mathbf{A}} \cap \mathbb{R}^n \neq \varnothing$.

If the random rational numbers computed in FindInfimum *lie in* $\mathcal{Q}^{\mathbf{A}}$ *then* FindInfimum *is correct.*

Proof. Since we assumed Theorem 6.5 and $\mathbf{A} \in \mathscr{O}$, property $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ is satisfied. Hence IsEmpty is always called with a correct input.

If $f^\star = -\infty$ then because of assertion 3 of Opt $\left(W^{\mathbf{A}}\right)$, the fiber of $f^{\mathbf{A}}$ at a rational $q_0 \in \mathcal{Q}^{\mathbf{A}}$ such that $q_0 < a_1$ is not empty. Hence the first call of IsEmpty returns false so that FindInfimum returns $-\infty$.

If $f^\star$ is finite, because the second assertion of Opt $\left(W^{\mathbf{A}}\right)$ holds, it is sufficient to know the smallest local extremum of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ in $W^{\mathbf{A}}$. To this end, we want to detect an eventual redundant value in $W^{\mathbf{A}}$. Such a redundant value, say a_i, is such that the interval $[a_i, a_{i+1}[$ does not contain any value reached by $f^{\mathbf{A}}$. In particular, it is a value that is not in $f^{\mathbf{A}}\left(\mathbb{V}\left(\mathsf{ListSamplePoints}^{\mathbf{A}}\right)\right) \cup f\left(\mathbb{V}\left(\mathsf{ListCriticalPoints}^{\mathbf{A}}\right)\right)$ and such that $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ does not reach any value in the interval $]a_i, a_{i+1}[$. Because of assertion 3 of Opt $\left(W^{\mathbf{A}}\right)$, testing this last point is equivalent to test the emptiness of the real fiber of $f^{\mathbf{A}}$ at some rational $q_i \in \mathcal{Q}^{\mathbf{A}} \cap]a_i, a_{i+1}[$.

If $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is empty then $\mathbb{V}\left(\mathsf{ListSamplePoints}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ and $\mathbb{V}\left(\mathsf{ListCriticalPoints}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ are empty. Since $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is empty, each call of the routine IsEmpty in the loop returns false. Hence, the algorithm leaves the loop without returning any value, so that $a_{k+1} = +\infty$ is returned.

Finally, this proves that the routine FindInfimum is correct. □

6.5 Complexity Analysis

Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$. Let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$, f and g in $\mathbb{Q}[\mathbf{X}]$ of degree bounded by D. Assume that each polynomial is given by a straight-line program (SLP) of size at most L. Recall that d denotes the dimension of $V = \mathbb{V}(\mathbf{F})$.

We study the complexity of the subroutines SetContainingLocalExtrema and FindInfimum. Gröbner bases can be used to compute the geometric objects. However, to estimate

the complexity, we use the Geometric Resolution subroutines GeometricSolve, LiftCurve and OneDimensionalIntersect presented in Section 1.3. We first estimate the size of the SLP representing the polynomials involved in the computations.

Size of SLP.

We want to estimate some parameters depending on the inputs of the Geometric Resolution routines, that are the polynomials defining the algebraic varieties $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ and $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$. Since bounds on $\delta\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ and $\delta\left(\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ have been obtained in Section 5.4, it remains to estimates the size of the straight-line programs representing these polynomials. These polynomials are either a polynomial $f^{\mathbf{A}}$ or $f_i^{\mathbf{A}}$ or a minor of size $n-d+1$ of the Jacobian matrix $\mathsf{Jac}\left(\left[f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right], i+1\right)$. The polynomials f and f_i are given as a SLP of size L. Then $f^{\mathbf{A}}$ and $f_i^{\mathbf{A}}$, can be represented by a SLP of size $O\left(L+n^2\right)$. Then we estimate the size of the minors. Let ω be the matrix-multiplication exponent.

Proposition 6.11. *Each minors of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right], i+1\right)$ can be represented by a SLP of size $\widetilde{O}\left((n-d+1)^{\omega/2+2}\left(L+n^2\right)\right)$.*

Proof. The partial derivatives appearing in the Jacobian matrix come from $f^{\mathbf{A}}$ and $f_i^{\mathbf{A}}$, represented by a SLP of size $O\left(L+n^2\right)$. According to [17], each partial derivative $\frac{\partial f_i^{\mathbf{A}}}{\partial x_j}$ and $\frac{\partial f^{\mathbf{A}}}{\partial x_j}$ can be represented by a SLP of size $O\left(L+n^2\right)$. Moreover, according to [74], the determinant of an $n \times n$ matrix can be computed using only $+$, $-$ and $\times$ in $\widetilde{O}\left((n-d+1)^{\omega/2+2}\right)$ operations. We combine these two results to conclude the proof. □

Remark 6.12. *Recall that $\omega \leq 3$. In the sequel, to lighten the expressions of complexity, we replace the above complexity $\widetilde{O}\left((n-d+1)^{\omega/2+2}\left(L+n^2\right)\right)$ with $\widetilde{O}\left(n^4\left(L+n^2\right)\right)$, that is less accurate but that dominates the first one.*

Is the sequel we use the routines of the geometric resolution, described in Section 1.3.

Computing $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$.

Recall that $\mathscr{C}\left(f^{\mathbf{A}}, F^{\mathbf{A}}, i\right)$ is defined as the vanishing set of

- the polynomials $f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}$,
- the minors of size $n-d+1$ of $\mathsf{Jac}\left(\left[f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right], i+1\right)$,
- and the variables $X_1, \ldots, X_{i-1}$.

Practically, $X_1, \ldots, X_{i-1}$ are set to 0. Hence, $\mathscr{C}\left(f^{\mathbf{A}}, F^{\mathbf{A}}, i\right)$ can be computed by GeometricSolve called with $s+\binom{s+1}{n-d+1}\binom{n-i}{n-d+1} = O\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right)$ polynomials in $n-i = O(n)$ variables. Each polynomial is given by a SLP of size $\widetilde{O}\left(n^4\left(L+n^2\right)\right)$. By

Proposition 5.22, $\delta\left(\mathscr{C}\left(f^{\mathbf{A}}, F^{\mathbf{A}}, i\right)\right)$ is bounded by $D\left((n-d+1)(D-1)\right)^n$. Hence, the computation can be done within

$$\widetilde{O}\left(\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right) LD^6\left((n-d+1)(D-1)\right)^{3n}\right)$$

arithmetic operations in $\mathbb{Q}$. Since $s \leq n$ and $\binom{n}{n-d+1} \leq 2^n$, we get the following result.

Lemma 6.13. *There exists a probabilistic algorithm that takes as input $f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}$ and i and that returns an equidimensional decomposition of $\mathscr{C}\left(f^{\mathbf{A}}, F^{\mathbf{A}}, i\right)$, encoded by a set of irreducible lifting fibers. In case of success, the algorithm has a complexity dominated by*

$$\widetilde{O}\left(2^n\binom{s+1}{n-d+1} LD^6\left((n-d+1)(D-1)\right)^{3n}\right).$$

Computing $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$.

Since $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ is defined as $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \operatorname{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}} \cap \operatorname{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$, a geometric resolution of $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ can be obtained from the lifting fibers of $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \operatorname{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. There are at most $D\left((n-d+1)(D-1)\right)$ lifting fibers. The routine LiftCurve is used on each fiber in order to obtain a parametrization of each component of the curve $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \operatorname{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. Lifting one fiber is done in

$$\widetilde{O}\left(\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right) LD^4\left((n-d+1)(D-1)\right)^{2n}\right).$$

From such a parametrization, the routine OneDimensionalIntersect is used with every polynomial that defines $\operatorname{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)$. There are $\binom{s+1}{n-d+1}\binom{n}{n-d+1}$ such polynomials, so that the cost is at most

$$\widetilde{O}\left(\binom{s+1}{n-d+1}\binom{n}{n-d+1} LD^4\left((n-d+1)(D-1)\right)^{2n}\right).$$

Finally, the total cost for the $D\left((n-d+1)(D-1)\right)$ lifting fibers is dominated by

$$\widetilde{O}\left(\left(s+\binom{s+1}{n-d+1}\binom{n}{n-d+1}\right) LD^5\left((n-d+1)(D-1)\right)^{3n}\right).$$

Since $s \leq n$ and $\binom{n}{n-d+1} \leq 2^n$, we get the following result.

Lemma 6.14. *There exists a probabilistic algorithm that takes as input a set of lifting fibers of $\overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \setminus \operatorname{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ and that returns a rational parametrization of $\mathscr{P}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$. In case of success, the algorithm has a complexity dominated by*

$$\widetilde{O}\left(2^n\binom{s+1}{n-d+1} LD^5\left((n-d+1)(D-1)\right)^{3n}\right).$$

Complexity of SetOfNonProperness**.**

As explained in [117], the computation of the set of non-properness of the restriction of $f^{\mathbf{A}}$ to $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ from the representation of $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ can be done using a parametric geometric resolution [126]. Indeed, from a set of lifting fibers of $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$, obtained by the routine GeometricSolve, one can compute a geometric resolution of the variety $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)$ for a generic $t \in \mathbb{R}$. Since there are at most $D\left((n-d+1)(D-1)\right)$ lifting fibers, this can be done using OneDimensionalIntersect on all the fibers in $\widetilde{O}\left(LD^5\left((n-d+1)(D-1)\right)^{3n}\right)$. From these geometric resolutions, LiftParameter computes a parametric geometric resolution of $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - T\right)$, where T is a parameter, in $\widetilde{O}\left(LD^3\left((n-d+1)(D-1)\right)^{3n}\right)$. Each coordinate in the parametrization is represented as a a rational function with coefficients in $\mathbb{Q}(T)$. Each of these rational function has the same denominator q_0, that is a univariate polynomial with coefficients in $\mathbb{Q}(T)$. Then the set of non-properness is contained in the set of roots of the least common multiple of the denominators that appears in the coefficients of q_0. Finally, we get the following.

Lemma 6.15. *There exists a probabilistic algorithm that takes as input a set of lifting fibers of $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$ and that returns a polynomial whose set of roots contains the set of non-properness of the projection π_T restricted to $\mathbb{V}(f-T) \cap \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$. In case of success, the algorithm has a complexity dominated by*

$$\widetilde{O}\left(LD^5\left((n-d+1)(D-1)\right)\right)^{3n}.$$

Complexity of RealSamplePoints **and** IsEmpty**.**

Given $\mathbf{F} = \{f_1, \ldots, f_s\}$, an algorithm computing a set of real sample points of $\mathbb{V}(\mathbf{F}) \cap \mathbb{R}^n$ is given in [119], using the polar varieties. Using techniques described in [10, 11, 121] and [14, Section 3], a local description of the polar varieties as a complete intersection can be obtained. Assume that $\mathbb{V}(\mathbf{F})$ is equidimensional of dimension d. Such a local description depends on the choice of a minor of size $n-d$ of the Jacobian matrix $\mathsf{Jac}(\mathbf{F})$. Since there are $\binom{s}{n-d}\binom{n}{n-d}$ minors of size $n-d$ in $\mathsf{Jac}(\mathbf{F})$, a full description of the polar varieties is obtained by computing the $\binom{s}{n-d}\binom{n}{n-d}$ possible localizations. Each local description is given by a reduced regular sequence involving $n-d$ polynomials in $\mathbf{F}$ and minors of degree bounded by $(n-d+1)(D-1)$. Hence, the routine GeometricSolveRRS computes one local description in $\widetilde{O}\left(LD^6\left((n-d+1)(D-1)\right)^{2n}\right)$. The cost for all localizations is then in $\widetilde{O}\left(\binom{s}{n-d}\binom{n}{n-d}LD^6\left((n-d+1)(D-1)\right)^{2n}\right)$. Since $\binom{n}{n-d} \leq 2^n$, this leads to the following complexity result.

Lemma 6.16. *There exists a probabilistic algorithm that takes as input $\mathbf{F}$ satisfying assumptions $\mathbf{R}$ and that returns a set of real sample points of $\mathbb{V}(F) \cap \mathbb{R}^n$, encoded by a rational parametrization. In case of success, the algorithm has a complexity dominated*

by

$$\widetilde{O}\left(2^n\binom{s}{n-d}LD^6\left((n-d+1)\left(D-1\right)\right)^{2n}\right).$$

Complexity of SetContainingLocalExtrema**.**

The first step in SetContainingLocalExtrema is the computation of a set of real sample points of $\mathbb{V}\left(\mathbf{F}^{\mathbf{A}}\right)\cap\mathbb{R}^n$. Its complexity is given in Lemma 6.16. Then at the i-th step of the loop, $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$, the set of non-properness of the projection π_T restricted to $\mathbb{V}\left(f-T\right)\cap\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$ and $\mathscr{P}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)$. The costs are given in Lemma 6.13, Lemma 6.15 and Lemma 6.14. The complexity for one step is then in $\widetilde{O}\left(2^n\binom{s+1}{n-d+1}LD^7\left((n-d+1)\left(D-1\right)\right)^{3n}\right)$. Finally, for the d steps, using that $d\leq n$ can be omitted, we get the following complexity.

Lemma 6.17. *In case of success, the routine* SetContainingLocalExtrema *performs at most*

$$\widetilde{O}\left(2^n\binom{s+1}{n-d+1}LD^6\left((n-d+1)\left(D-1\right)\right)^{3n}\right)$$

arithmetic operations in $\mathbb{Q}$.

Complexity of FindInfimum**.**

The most expensive steps in this routine are the calls to IsEmpty. There are at most k such steps, where k is the number of points of non-properness, of critical values and of real sample points. Using the Bézout inequality, k lies in $\widetilde{O}\left(D\left((n-d+1)\left(D-1\right)\right)^n\right)$. Using the complexity estimate given in Lemma 6.16, this leads to the following.

Lemma 6.18. *In case of success, the routine* FindInfimum *performs at most*

$$\widetilde{O}\left(2^n\binom{s}{n-d}LD^7\left((n-d+1)\left(D-1\right)\right)^{3n}\right).$$

Complexity of the Algorithm.

Finally, the complexity of Optimize comes from Lemma 6.17 and Lemma 6.18, using that $\binom{s}{n-d}\leq\binom{s+1}{n-d+1}$.

Theorem 6.19. *In case of success, the algorithm* Optimize *performs*

$$\widetilde{O}\left(2^n\binom{s+1}{n-d+1}LD^7\left((n-d+1)\left(D-1\right)\right)^{3n}\right)$$

arithmetic operations in $\mathbb{Q}$.

Remark that if $\mathbf{F}$ is a reduced regular sequence then the above complexity is simpler.

Theorem 6.20. *If* $\mathbf{F}$ *is a reduced regular sequence, the algorithm* Optimize *performs, in case of success,*

$$\widetilde{O}\left(LD^7\left(\sqrt[3]{2}\,(s+1)\,(D-1)\right)^{3n}\right)$$

arithmetic operations in $\mathbb{Q}$.

6.6 Implementation and Practical Experiments

We give details about our implementation in Section 6.6.1. Instead of using the geometric resolution algorithm [50] for algebraic elimination, we use Gröbner bases that still allow to perform all geometric operations needed to implement the algorithm. Moreover, there exist deterministic algorithms for computing Gröbner bases [46, 47]. This way, the probabilistic aspect of our algorithm relies on the random choice of a linear change of variables. In practice, we check if a given linear change of variables is suitable so that the exactness can be guaranteed. This is explained in Section 6.6.1.

In Sections 6.6.2 and 6.6.3, we present practical experiments. First, we run our implementation with random dense polynomials, that is the hardest case for the inputs. As an example, considering an objective polynomial and one constraint, both of degree 2 and increasing the number of variables, our implementation can solve problems with up to 32 variables in 4 hours. With two constraints, our implementation can solve problems with up to 11 variables in 5.3 hours. With a linear objective polynomial subject to one constraint of degree 4, both in 5 variables it takes 34 minutes. These results show that our implementation outperforms general solvers based on the Cylindrical Algebraic Decomposition.

Then we run examples coming from applications. Some of these examples can be solved by QEPCAD. The timings are given in Section 6.6.3.

We do not report timings of methods based on sums of squares or numerical procedures, e.g. [61, 92, 109] since their outputs are numerical approximation while we look for exact representations.

6.6.1 Implementation

Since our algorithm depends on the choice of a matrix that defines a change of coordinates, it is probabilistic. However, we present a technique to make sure that this choice is a correct one. This technique is used in our implementation.

As stated in Section 6.4, the algorithm is correct if the subroutines SetContainingLocalExtrema and FindInfimum are correct. According to Proposition 6.6, if the random matrix chosen at the first step of Optimize is such that $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold, then SetContainingLocalExtrema is correct. Then its output satisfies property Opt (W). Hence, FindInfimum can be called with the output of SetContainingLocalExtrema.

Then the choice of the matrix $\mathbf{A}$ leads to a correct output if $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$, $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ hold.

Property $\mathfrak{R}(f, \mathbf{F})$ always holds if $\mathbf{F}$ satisfies assumptions $\mathbf{R}$. Since for any change of coordinates, $\mathbf{F}$ satisfies assumptions $\mathbf{R}$ if and only if $\mathbf{F}^{\mathbf{A}}$ does, $\mathfrak{R}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ holds for any $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$. Then it remains to check $\mathfrak{P}_1\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ and $\mathfrak{P}_2\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$. Both properties depend on the properness of projections of the form

$$\begin{aligned} \pi_{\leq d} : \quad W \subset \mathbb{C}^n &\longrightarrow \mathbb{C}^d \\ (x_1, \ldots, x_n) &\longmapsto (x_1, \ldots, x_d) \end{aligned}$$

where W is an algebraic variety. According to [70, Proposition 3.2], if I_V is an ideal such that $V = \mathbb{V}(I_V)$ has dimension d then the projection

$$\begin{aligned} \pi_{\leq d} : \quad V \subset \mathbb{C}^n &\longrightarrow \mathbb{C}^d \\ (x_1, \ldots, x_n) &\longmapsto (x_1, \ldots, x_d) \end{aligned}$$

is proper if and only if I_V is in Noether position.

Thus we choose the matrix $\mathbf{A}$ such that after the change of variables, the ideals are in Noether position. This can be done using techniques described in [77, Section 4.1.2] and [93]. These techniques are used in our implementation to obtain a matrix as sparse as possible that makes SetContainingLocalExtrema correct.

6.6.2 Practical Experiments

The analysis of the degree of the algebraic varieties involved in the computations provides a singly exponential bound in the number of indeterminates. This matches the best complexity bounds for algorithms computing an algebraic representation of $f^\star$ and a minimizer using quantifier elimination. Our implementation is written in Maple. Gröbner bases are computed using the package FGb (`http://www-polsys.lip6.fr/~jcf/Software/`.)

The computations were performed on a Intel Xeon CPU E7540 @ 2.00GHz and 250GB of RAM.

The notations below are used in the following tables :

- d: degree of the objective polynomial f;
- D: upper bound for the degree of the constraints;
- n: number of indeterminates;
- s: number of constraints;
- obj terms: number of terms in the objective polynomial;
- terms: average number of terms.

To test the behavior of the algorithm, we run it with randomly generated polynomials and constraints as inputs.

Considering an objective polynomial and one constraint, both of degree 2 and increasing the number of variables, our implementation can solve problems with up to 32 variables in 4 hours. For this special case, the algorithm seems to be sub-exponential.

Constraints of degree 2.

n	d	D	s	obj terms	terms	time
8	2	2	1	44	45	9 sec.
12	2	2	1	91	91	30 sec.
16	2	2	1	153	153	2 min..
20	2	2	1	229	231	8 min.
24	2	2	1	323	323	27 min.
28	2	2	1	433	433	1.5 hours
32	2	2	1	559	557	4 hours
7	2	2	2	36	36	92 sec.
8	2	2	2	45	45	7 min.
9	2	2	2	55	55	27 min.
10	2	2	2	65	66	1.6 hours
11	2	2	2	78	78	5.3 hours

Constraints of degree 3.

n	d	D	s	obj terms	terms	time
4	2	3	1	15	34	4 sec.
5	2	3	1	21	55	28 sec.
6	2	3	1	27	84	9 min.
7	2	3	1	36	120	3.5 hours
4	2	3	2	15	34	81 sec.
5	2	3	2	21	56	2.2 hours

Constraints of degree 4.

n	d	D	s	obj terms	terms	time
2	3	4	1	10	14	2 sec.
3	3	4	1	20	34	4 sec.
4	3	4	1	34	70	7 min.
3	3	4	2	20	35	22 sec.
4	3	4	2	35	70	4.8 hours.
2	2	4	1	6	15	1 sec.
3	2	4	1	10	35	2 sec.
4	2	4	1	15	68	83 sec.

Linear objective function.

n	d	D	s	obj terms	terms	time
4	1	3	1	5	34	3 sec.
4	1	4	1	5	69	30 sec.
4	1	5	1	5	126	13 min.
5	1	3	1	6	56	7 sec.
5	1	4	1	6	126	34 min.
5	1	5	1	6	252	87 hours
6	1	3	1	7	84	68 sec.
6	1	4	1	7	207	62 hours
4	1	3	2	5	35	36 sec.
4	1	4	2	5	70	1 hour
4	1	5	2	5	126	33 hours

6.6.3 Examples coming from Applications

We consider simple examples coming from applications to compare the execution time of our algorithm with a cylindrical algebraic decomposition algorithm. These decompositions are computed using QEPCAD version B 1.69[1]

Some of these problems cause issues to numerical algorithm because the infimum is not reached.

	n	d	D	p	obj terms	terms	time	QEPCAD
nonreached	3	4	1	1	4	1	2.3 sec.	0.03 sec.
nonreached2	3	10	3	1	5	5	2 sec.	∞
isolated	2	4	3	1	2	2	0.8 sec.	0.04 sec.
reachedasymp	3	14	1	1	3	1	1 sec.	7.3 sec.
GGSZ2012	2	2	3	1	2	2	0.6 sec.	10.5 sec.
Nie2010	3	6	1	1	7	4	1.3 sec.	∞
LaxLax	4	4	1	3	5	2	0.6 sec.	∞
maxcut5-1	5	2	2	5	11	2	0.3 sec.	∞
maxcut5-2	5	2	2	5	11	2	0.3 sec.	∞
Coleman5	8	2	2	4	8	4	5 sec.	∞
Coleman6	10	2	2	5	10	4	33 sec.	∞
Vor1	6	8	n/a	0	63	n/a	2 min.	∞

6.7 Description of Examples

In this section we give detailed descriptions of the examples coming from applications considered in the previous section. They are available as a plain text file, that can be opened with Maple, at `http://www-polsys.lip6.fr/~greuet/`.

[1]Implementation originally due to H. Hong, and subsequently added on to by C. W. Brown, G. E. Collins, M. J. Encarnacion, J. R. Johnson, W. Krandick, S. McCallum, S. Steinberg, R. Liska, N. Robidoux. Latest version is available at `http://www.usna.edu/cs/~qepcad/`.

Example 6.21 (nonreached, nonreached2). *Let* $g(x_1,x_2,x_3) = x_1^2 - x_1x_2 + x_1x_2x_3 + x_2 + 3$. *They cause instabilities to numerical algorithms because their infima are not reached. The only way to get close to them is to evaluate the objective polynomial at a sequence of the form* $\left(x_1, \frac{1}{x_1}, x_3\right)$, *where* x_1 *tends to infinity:*

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & (x_1x_2-1)^2 + x_2^2 + x_3^2 + 42 \\ s.t. & x_3 = 0. \end{cases}$$

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & (x_1x_2-1)^2 + x_2^2 + x_3^2 g + (x_1+1)\, g^3 + 42 \\ s.t. & g(x_1,x_2,x_3) = 0. \end{cases}$$

Example 6.22 (isolated). *It is a toy example:* $f^\star$ *is isolated in* $f(V \cap \mathbb{R}^n)$.

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^2} & \left(x_1^2+x_2^2-2\right)\left(x_1^2+x_2^2\right) \\ s.t. & \left(x_1^2+x_2^2-1\right)(x_1-3) = 0. \end{cases}$$

Over $V \cap \mathbb{R}^n$, *either* $x_1^2 + x_2^2 = 1$ *or* $x_1 = 3$, *so that the objective polynomial is either equal to* -1 *or* $\left(7+x_2^2\right)\left(9+x_2^2\right)$. *The second expression is positive over the reals.*

Example 6.23 (reachedasympt). *The infimum is both attained and an asymptotic value. Indeed,* $f^\star = 42$ *is reached at any point* $(x_1,0,0)$, *but is also the limit of sequences of the form* $\left(x_1, \frac{1}{x_1}, 0\right)$ *when* x_1 *tends to infinity. Some iterative methods do not return a minimizer close to* $(x_1,0,0)$.

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & \left(10000\left(x_1x_2-1\right)^4 + x_1^6\right)x_2^6 + \frac{1}{124}x_3^2 + 42 \\ s.t. & x_3 = 0. \end{cases}$$

Example 6.24 (GGSZ2012). *It comes from [53] (Example 4.4). The minimizer does not satisfy the KKT conditions.*

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^2} & (x_1+1)^2 + x_2^2 \\ s.t. & x_1^3 = x_2^2. \end{cases}$$

Example 6.25 (Nie2011). *It comes from [100] (Example 5.2) and has been studied in [53] because of the numerical instabilities that occurs with numerical algorithms.*

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^3} & x_1^6 + x_2^6 + x_3^6 + 3x_1^2x_2^2x_3^2 - x_1^2(x_2^4+x_3^4) - x_2^2(x_3^4+x_1^4) - x_3^2(x_1^4+x_2^4) \\ s.t. & x_1 + x_2 + x_3 - 1 = 0. \end{cases}$$

Example 6.26 (LaxLax). *The objective polynomial appears in [88] and [75]. Its infimum is* 0 *and is reached over* $V(x_1, x_2-x_3, x_3-x_4) \cap \mathbb{R}^n$.

$$\begin{cases} \inf\limits_{(x)\in\mathbb{R}^4} & x_1x_2x_3x_4 - x_1(x_2-x_1)(x_3-x_1)(x_4-x_1) \\ & -x_2(x_1-x_2)(x_3-x_2)(x_4-x_2) - x_3(x_1-x_3)(x_2-x_3)(x_4-x_3) \\ & -x_4(x_1-x_4)(x_2-x_4)(x_3-x_4) \\ s.t. & x_1 = x_2 - x_3 = x_3 - x_4 = 0. \end{cases}$$

Example 6.27 (maxcut5-1/5-2). *A cut of a graph with weighted edges is a partition of the vertices into two disjoint subsets. Its weight is the sum of the weights of the edges crossing the cut. The maxcut problem is to find a cut whose weight is greater than or equal to any other cut. This problem has applications, among other, in Very-large-scale integration circuit design and statistical physics ([40, 48]). It can be reformulated has a constrained polynomial optimization problem ([34]). For a graph of p vertices and weight w_{ij} for the edge joining the i-th vertex to the j-th one, it is equivalent to solve*

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^p} & -\dfrac{1}{2}\displaystyle\sum_{1\leq i<j\leq p} w_{ij}\left(1-x_ix_j\right) \\ s.t. & x_i^2-1=0,\ \textit{for } i\in\{1,\ldots,p\}\,, \end{cases}$$

We use the set of weight W_{G5-1} and W_{G5-2} in [8], that leads to solve

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^5} & -98+\frac{23}{2}x_1x_2+8x_1x_3+9x_1x_4+\frac{17}{2}x_1x_5+\frac{25}{2}x_2x_3 \\ & +13x_2x_4+\frac{23}{2}x_2x_5+7x_3x_4+12x_3x_5+5x_4x_5 \\ s.t. & x_i^2-1=0,\ \textit{for } i\in\{1,\ldots,5\}\,. \end{cases}$$

and

$$\begin{cases} \inf\limits_{x\in\mathbb{R}^5} & -31+3x_1x_2+3x_1x_3+4x_1x_4+5x_1y_5+\frac{5}{2}x_2x_3+\frac{5}{2}x_2x_4+3x_2x_5 \\ & +2x_3x_4+3x_3x_5+3x_4x_5 \\ s.t. & x_i^2-1=0,\ \textit{for } i\in\{1,\ldots,5\}\,. \end{cases}$$

Example 6.28 (coleman5/6). *They come from optimal control problems and appears in [30]. For $M\in\{5,6\}$, let $x_1,\ldots,x_{M-1}$ and $y_1,\ldots,y_{M-1}$ be the indeterminates.*

$$\begin{cases} \inf\limits_{(x,y)\in\mathbb{R}^{2M}} & \dfrac{1}{M}\displaystyle\sum_{i=1}^{M-1} x_i^2+y_i^2 \\ s.t. & y_1-1=y_{i+1}-y_i-\frac{1}{M-1}\left(y_i^2-x_i\right)=0,\ \textit{for } i\in\{1,\ldots,M-2\}\,. \end{cases}$$

Example 6.29 (Vor1). *It comes from [45] and have no constraints.*
$Vor1\,(a,\alpha,\beta,u,x,y) = -16a^3u^3\alpha\beta+16a^2u^3x\alpha+16a^2u^3y\beta-16au^3\alpha\beta-8u^2x\beta a^3-24u^2a\alpha\beta+24u^2y\beta a^2-24u^2\alpha\beta a^3-8u^2ax\beta+24u^2x\alpha a^2-8u^2ya^3\alpha-8u^2ay\alpha-12u\alpha\beta a^3-8uya^3\alpha+4u\alpha a^4x+12uy\beta a^2-4uya^3x-8uax\beta+12ux\alpha a^2-4uaxy-12ua\alpha\beta-8uay\alpha-8ux\beta a^3+a^4\alpha^2+y^2a^2+x^2a^2+a^2\beta^2+a^2\alpha^2+a^4x^2+32a^2u^3+4u^2\beta^2+16u^2a^2+2\beta y+16a^2u^4+4u\beta^2+\beta^2+y^2+4u\beta y+8ua^2\beta^2+4u^2x^2a^2+4u^2y^2a^2-2ya^3x+2\alpha a^4x+4ua^4\alpha^2-2axy+8ua^2\alpha^2+4uy^2a^2-2ya^3\alpha-2ay\alpha+16a^2u^4\alpha^2+16a^2u^4\beta^2+32a^2u^3\beta^2+24u^2a^2\beta^2+24u^2a^2\alpha^2+4u^2a^4\alpha^2+32a^2u^3\alpha^2+4ux^2a^2-2a\alpha\beta-2x\beta a^3+2y\beta a^2-2\alpha\beta a^3-2ax\beta+2x\alpha a^2.$

Chapter 7

SOS Certificates of Positivity

7.1 Introduction

This chapter is based on the article [53]. In this paper, we assumed that the algebraic variety defined by the constraints is smooth.

However, we will use results presented in Chapter 5 and in [52] that allow to present a bit more general statements. In this Chapter, the results are stated and proved for constraints defined by polynomial equations that define an algebraic variety with finitely many singular points.

Motivation and methodology

Let $f_1, \ldots, f_s \in \mathbb{Q}[\mathbf{X}]$ and let $V = \mathbb{V}(f_1, \ldots, f_s)$. Given $f \in \mathbb{Q}[\mathbf{X}]$, let $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x)$.

In this chapter, our goal is to provide results to solve problem (A) : Computing certificates for lower bounds on $f^\star$.

As explained in Section 3.2.1, if the existence of certificates of positivity by means of sum of squares on V is proved, then semidefinite programming can be used to compute these lower bounds. Furthermore, we want our results to be as general as possible: we allow to have regularity assumptions on the input that are reasonable in practice and we do not require any assumption on the infimum.

To prove the existence of certificates of positivity, we use Schweighofer's results (see [130] and Theorem 3.16). These results do not assume that $f^\star$ is reached. We use these results on the modified polar varieties, defined in Chapter 5.

Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$ and $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ be the union of the modified polar varieties associated with $V^{\mathbf{A}}$. If $\mathbf{A}$ is generic enough then $f^\star = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$. Hence, the existence of certificates of positivity for f on $V \cap \mathbb{R}^n$ is equivalent to the existence of certificates for $f^{\mathbf{A}}$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$. Furthermore, since $\dim \overline{\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \setminus \mathrm{Crit}\left(f^{\mathbf{A}}, V^{\mathbf{A}}\right)}^{\mathcal{Z}} = 1$, asymptotic phenomena of $f^{\mathbf{A}}$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ are well controlled.

Thus, Schweighofer's results can be used to prove the existence of certificates of positivity by means of sum of squares on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$.

Problem statement

Let $f, f_1, \ldots, f_s \in \mathbb{Q}[\mathbf{X}]$, let $V = \mathbb{V}(f_1, \ldots, f_s)$ and let $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x)$. Let $\mathscr{C}(f, \mathbf{F}) = \mathbb{V}(g_1, \ldots, g_p)$ be the union of the modified polar varieties defined in Chapter 5 and let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski-open set given in Theorem 5.1. Our goal is to prove that for all $\mathbf{A} \in \mathscr{O} \cap \mathrm{GL}_n(\mathbb{Q})$,

- $f^{\mathbf{A}} \geq 0$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ if and only if $f \geq 0$ on $V \cap \mathbb{R}^n$,
- if $f^{\mathbf{A}} \geq 0$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ then for all $\varepsilon > 0$, there exists sums of squares of real polynomials σ_i such that

$$f^{\mathbf{A}} + \varepsilon = \sigma_0 + \sum_{1 \leq i \leq p} \sigma_i g_i^{\mathbf{A}}.$$

Furthermore, our goal is to obtain a result that does not require that $f^\star$ is reached on $V \cap \mathbb{R}^n$.

Prior works

Unconstrained case. This approach has been previously developed in the unconstrained case. In [84], Schmüdgen's Positivstellensatz is used to prove the existence of certificates on a closed ball centered at 0: a polynomial $f > 0$ on $\overline{B}(0, R)$ can be written $f = \sigma + \theta\left(R^2 - \|x\|^2\right)$, where $\sigma, \theta \in \sum \mathbb{R}[\mathbf{X}]^2$. Hence, this provides a local certificate of positivity.

To recover a global certificate from a local one, a method which can be used if $f^\star$ is reached is proposed in [101]. Denote by $\langle \nabla f \rangle$ the ideal $\left\langle \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \right\rangle$. If $\langle \nabla f \rangle$ is radical, then a non-negative polynomial over $V\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right)$ is a sum of squares of polynomials modulo $\langle \nabla f \rangle$. Moreover, if the polynomial is positive, the radical assumption on $\langle \nabla f \rangle$ is not required. Note that if the infimum is reached, it is reached over $V\left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right) \cap \mathbb{R}^n$. Then $f - f^\star$ can be written as a sum of squares on the gradient variety while it is necessarily non-negative outside. Here the local certificate is actually a global certificate of non-negativity. Remark that if $f^\star$ is not reached then $f - f^\star$ can be non-negative on the gradient variety but negative outside. This approach is followed in [2]. A hierarchy of semidefinite relaxations converging to $f^\star$ in a finite number of steps is presented, if $f^\star$ is reached.

When we do not know *a priori* if f attains a minimum, we should take into account asymptotic phenomena. To do so, in [130] the gradient variety is replaced with the gradient tentacle. This is the semi-algebraic set $S(\nabla f) = \left\{x \in \mathbb{R}^n \mid \|\nabla f(x)\|^2 \|x\|^2 \leq 1\right\}$. Over the gradient tentacle, a positive polynomial for which its set of values "at infinity" is a finite subset of $\mathbb{R}_{>0}$ can be written as a sum of squares modulo $\left(1 - \|\nabla f(x)\|^2 \|x\|^2\right)$.

In [54], simpler critical loci of linear projections are considered. They lead to consider only $(n-d+1, n-d+1)$-minors of the Jacobian matrix associated to $f_1, \ldots, f_s, f$.

This leads to simpler algebraic certificates, even if $f^\star$ is not reached, and a better numerical behavior of programs computing numerical approximations of sum of squares decompositions via semidefinite programming.

Constrained case. Let $S = \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\}$, where $f_i \in \mathbb{R}[\mathbf{X}]$. In [39], the gradient variety approach is generalized to obtain certificates of positivity over S. To this end, the gradient ideal is replaced by the Karush-Kuhn-Tucker ideal, its analogous in the constrained case. It is defined by

$$I_{KKT} = \left\langle \frac{\partial f}{\partial X_1} - \sum_{1 \leq j \leq s} \frac{\partial f_j}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} - \sum_{1 \leq j \leq s} \frac{\partial f_j}{\partial X_n}, \lambda_1 f_1, \ldots, \lambda_n f_n \right\rangle,$$

that is a subset of $\mathbb{R}[\mathbf{X}, \lambda_1, \ldots, \lambda_s]$.

Then it is proved that a polynomial is positive over its KKT variety $\mathbb{V}(I_{KKT})$ if and only if it can be written as a sum of squares modulo I_{KKT}. As in the gradient variety approach, if the KKT ideal is radical then a non-negative polynomial over the KKT variety is necessarily a sum of squares modulo KKT ideal. If $f^\star$ is reached, then it is reached at a KKT point. Thus, it is attained on $\mathbb{V}(I_{KKT})$ where the existence of certificates is ensured, so that $f^\star = \inf_{x \in \mathbb{V}(I_{KKT})} f(x)$ can be approximated by a sequence of SDP relaxations. However, $f^\star$ may be a limit that is not reached. In this case, $f^\star \neq \inf_{x \in \mathbb{V}(I_{KKT})} f(x)$, so that the computed approximation may be far away from $f^\star$.

This approach is followed in [1, 99, 100] on a semi-algebraic set. Based on Lasserre's relaxations, these hierarchies of semidefinite relaxations converge to $f^\star$ in a finite number of steps, if $f^\star$ is reached.

In [141], the approach initiated by Schweighofer is followed. The truncated tangency variety is introduced. It is a subset of the region defined by the constraints of smaller dimension and on which the target function f has a finite number of values "at infinity". These truncated tangency varieties are related to critical loci of the square of distance functions to a given point, say $(a_1, \ldots, a_n)$. They are defined by considering $(n - d + 2, n - d + 2)$ minors of the Jacobian matrix associated to $f_1, \ldots, f_s, f$ and $\sum_{i=1}^{n} (X_i - a_i)^2$. Under some assumption of regularity on S, the existence of certificates is proved on the semi-algebraic set S. Then, lower bounds on the infimum of f on the truncated tangency variety can be certificated. However, because many auxiliary constraints are introduced and because they have high degree, the SOS relaxations can be hard to solve. It is then relevant to obtain simpler constraints, without the assumption that $f^\star$ is reached.

Main results

Let $f \in \mathbb{Q}[\mathbf{X}]$ and let $\mathbf{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\mathbf{X}]$ such that the ideal $\langle \mathbf{F} \rangle$ is radical and the variety $V = \mathbb{V}(\mathbf{F})$ is d-equidimensional with finitely many singular points. Let $\mathscr{C}(f, \mathbf{F})$ be the union of the modified polar varieties defined in Chapter 5. We summarize the two

main results in the following theorem. The first item comes from Proposition 7.6 page 114 and the second one from Theorem 7.4 page 112.

Theorem 7.1. *There exists a non-empty Zariski-open set* $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ *such that for all* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$,

- $f^{\mathbf{A}} \geq 0$ *on* $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ *if and only if* $f \geq 0$ *on* $V \cap \mathbb{R}^n$,
- $f^{\mathbf{A}} \geq 0$ *on* $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ *if and only if for all* $\varepsilon > 0$, *there exist a sum of squares of real polynomials* $S^{\mathbf{A}}$ *and* $T^{\mathbf{A}}$ *such that, for any* $B \in f(V \cap \mathbb{R}^n)$,

$$f^{\mathbf{A}} + \varepsilon = S^{\mathbf{A}} + T^{\mathbf{A}}\left(B - f^{\mathbf{A}}\right) \mod \mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right).$$

Then finding a certificate of positivity on $V \cap \mathbb{R}^n$ is equivalent to finding a certificate on $\mathscr{C}(f, \mathbf{F}) \cap \mathbb{R}^n$. Furthermore, the existence of certificates on $\mathscr{C}(f, \mathbf{F}) \cap \mathbb{R}^n$ is ensured for positive polynomials. Hence, for any $\varepsilon > 0$, one can compute successive lower bounds on $f - f^\star + \varepsilon > 0$ using semidefinite programming. Remark that this result works even if $f^\star$ is not assumed to be reached.

Organization of the chapter

We first prove the existence of certificates of positivity on $\mathscr{C}(f, \mathbf{F}) \cap \mathbb{R}^n$ in Section 7.2. In Section 7.3, we briefly recall the connection between sum of squares computation and semidefinite programming. We prove that our result on the existence of certificates leads to a hierarchy of SDP relaxations. It allows to compute numerically an increasing sequence of lower bounds on the number f^{sos}. It is defined as the supremum of the $a \in \mathbb{R}$ such that there exists sums of squares of polynomials $S^{\mathbf{A}}$ and $T^{\mathbf{A}}$ such that $f - a = S^{\mathbf{A}} + T^{\mathbf{A}}\left(B - f^{\mathbf{A}}\right) \mod \mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$. Then we prove that the infimum of f on $V \cap \mathbb{R}^n$ and on $\mathscr{C}(f, \mathbf{F})$ coincide. This means that f^{sos} is actually $f^\star$. Finally in Section 7.4, we consider the computational aspect of this approach. We first present a method to reduce the number of equations defining $\mathscr{C}(f, \mathbf{F})$. Then we give some practical results, that we compare with the previous approaches.

7.2 Existence of Certificates on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$

Let $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ be the algebraic variety defined in Section 5.2. In this section, we prove that for almost all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$, if $f^{\mathbf{A}} \geq 0$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ then $f^{\mathbf{A}} + \varepsilon$ can be written as $f^{\mathbf{A}} + \varepsilon = S^{\mathbf{A}} + T^{\mathbf{A}}\left(B - f^{\mathbf{A}}\right) \mod \mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$, where $B \in f^{\mathbf{A}}\left(V^{\mathbf{A}} \cap \mathbb{R}^n\right)$ and $S^{\mathbf{A}}$ and $T^{\mathbf{A}}$ are sums of squares of polynomials in $\mathbb{R}[\mathbf{X}]$.

Remark that the polynomials depending on $f^{\mathbf{A}}$ that appear in the definition of $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ are actually partial derivatives of $f^{\mathbf{A}}$. Hence, for any $c \in \mathbb{R}$, $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) = \mathscr{C}\left(f^{\mathbf{A}} + c, \mathbf{F}^{\mathbf{A}}\right)$. In particular, if $f^{\mathbf{A}} > 0$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ can be written as a sum of squares then for all $\varepsilon > 0$, so is $f^{\mathbf{A}} - f^\star + \varepsilon$.

Our goal is to use Schweighofer's theorem (coming from [130], see Theorem 3.16 page 46). To this end, we prove that the set

$$R_{\infty}\left(f^{\mathbf{A}},\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\right)=$$
$$\left\{t\in\mathbb{R}\mid\exists\left(x_k\right)_{k\in\mathbb{N}}\subset\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right),\left\|x_k\right\|\underset{k\to+\infty}{\longrightarrow}\infty\text{ and }f^{\mathbf{A}}\left(x_k\right)\underset{k\to+\infty}{\longrightarrow}t\right\}$$

of asymptotic values of the restriction of $f^{\mathbf{A}}$ to $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)$ is finite.

The set of values of $f^{\mathbf{A}}$ over $\mathrm{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$ is finite by Sard's theorem. Hence, proving that there are finitely many asymptotic values on a set S is finite is equivalent to prove that it is finite on $\overline{S\setminus\mathrm{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$. We have seen in Theorem 5.12 page 65 that the components of $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)$ not included in $\mathrm{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$ have dimension 1. We will see that the set of asymptotic values over such a component is finite. Hence, $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\cap\mathbb{R}^n$ is a good candidate to get certificates of positivity.

We first prove an intermediate result, used to prove the finiteness of the set of asymptotic values.

Lemma 7.2. *There exists a non-empty Zariski-open set $\mathscr{O}\subset\mathrm{GL}_n\left(\mathbb{C}\right)$ such that for all $\mathbf{A}\in\mathrm{GL}_n\left(\mathbb{Q}\right)\cap\mathscr{O}$, there exists a non-empty Zariski-open set $\mathcal{Q}^{\mathbf{A}}\subset\mathbb{C}$ such that for all $t\in\mathbb{R}\cap\mathcal{Q}^{\mathbf{A}}$, $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\cap\mathbb{V}\left(f^{\mathbf{A}}-t\right)$ is either empty or 0-dimensional.*

Proof. Let $\mathscr{O}_1\subset\mathrm{GL}_n\left(\mathbb{C}\right)$ be the Zariski-open set given in Theorem 5.9 and $\mathscr{O}_3\subset\mathrm{GL}_n\left(\mathbb{C}\right)$ the Zariski-open set given in Theorem 5.12 (page 65). Let $\mathscr{O}=\mathscr{O}_1\cap\mathscr{O}_3$ and consider $\mathbf{A}\in\mathrm{GL}_n\left(\mathbb{Q}\right)\cap\mathscr{O}$. Denote by $\mathcal{Q}^{\mathbf{A}}\subset\mathbb{C}$ be the Zariski-open set given by Theorem 5.9.

According to Theorem 5.12, $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathrm{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ has dimension at most 1. Recall that by construction, $\mathcal{Q}^{\mathbf{A}}$ does not contain any critical value of $f^{\mathbf{A}}_{|V^{\mathbf{A}}\cap\mathbb{R}^n}$. Hence for all $t\in\mathbb{R}\cap\mathcal{Q}^{\mathbf{A}}$,

$$\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathrm{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}\cap\mathbb{V}\left(f^{\mathbf{A}}-t\right)=\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\cap\mathbb{V}\left(f^{\mathbf{A}}-t\right).$$

Let $Z^{\mathbf{A}}_t$ be an irreducible component of $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\cap\mathbb{V}\left(f^{\mathbf{A}}-t\right)$. There is an irreducible component $Z^{\mathbf{A}}$ of $\overline{\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}},i\right)\setminus\mathrm{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)}^{\mathcal{Z}}$ such that $Z^{\mathbf{A}}_t=Z^{\mathbf{A}}\cap\mathbb{V}\left(f^{\mathbf{A}}-t\right)$. In particular $Z^{\mathbf{A}}$ has dimension at most 1.

Since $Z^{\mathbf{A}}\not\subset\mathrm{Crit}\left(f^{\mathbf{A}},V^{\mathbf{A}}\right)$, the restriction of f to $Z^{\mathbf{A}}$ is not constant. In particular $Z^{\mathbf{A}}$ is not included in $\mathbb{V}\left(f^{\mathbf{A}}-t\right)$.

According to Krull's Principal Ideal Theorem ([79, Corollary 3.2 p. 131]), this means that $Z^{\mathbf{A}}_t=Z^{\mathbf{A}}\cap\mathbb{V}\left(f^{\mathbf{A}}-t\right)$ has dimension $\dim\left(Z^{\mathbf{A}}\right)-1\leq 0$. □

Lemma 7.3. *There exists a non-empty Zariski-open set $\mathscr{O}\subset\mathrm{GL}_n\left(\mathbb{C}\right)$ such that for all $\mathbf{A}\in\mathrm{GL}_n\left(\mathbb{Q}\right)\cap\mathscr{O}$, the set $R_{\infty}\left(f^{\mathbf{A}},\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)\right)$ is finite.*

Proof. Let $\mathscr{O}_1\subset\mathrm{GL}_n\left(\mathbb{C}\right)$ be the Zariski-open set given in Theorem 5.9 and $\mathscr{O}_3\subset\mathrm{GL}_n\left(\mathbb{C}\right)$ the Zariski-open set given in Theorem 5.12 (page 65). Let $\mathscr{O}=\mathscr{O}_1\cap\mathscr{O}_3$ and let $\mathbf{A}\in\mathrm{GL}_n\left(\mathbb{Q}\right)\cap\mathscr{O}$. Let $Z^{\mathbf{A}}$ be an irreducible component of $\mathscr{C}\left(f^{\mathbf{A}},\mathbf{F}^{\mathbf{A}}\right)$ and consider the map $x\in Z^{\mathbf{A}}\to f^{\mathbf{A}}\left(x\right)\in\mathbb{C}$.

Suppose first that $f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ has dimension 0. Then, $R_\infty\left(f^{\mathbf{A}}, Z^{\mathbf{A}}\right) \subset f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ which has dimension 0.

Suppose now that $f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)$ has dimension 1. By the theorem on the dimension of fibers, [134, Theorem 7, Chapter 1, p. 76], there exists a non-empty Zariski-open set $\mathscr{W} \subset \mathbb{C}$ such that for all $t \in \mathscr{W}$, $\dim\left(Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)\right) = \dim\left(Z^{\mathbf{A}}\right) - 1$.

Let $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ be the Zariski-open set given in Theorem 5.9. According to Lemma 7.2, if t lies in $\mathbb{R} \cap \mathcal{Q}^{\mathbf{A}}$ then $Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)$ is either empty or 0-dimensional.

Hence, two situations may occur:

- either $Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)$ is empty and then $\dim\left(Z^{\mathbf{A}}\right) = 0$ which is not possible since, by assumption, $\dim\left(f^{\mathbf{A}}\left(Z^{\mathbf{A}}\right)\right) = 1$;
- or $Z^{\mathbf{A}} \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right)$ has dimension 0 and then $\dim\left(Z^{\mathbf{A}}\right) = 1$. This implies that the set $R_\infty\left(f^{\mathbf{A}}, Z^{\mathbf{A}}\right) \subset \mathbb{C}$ is the set of non-properness of the map $x \in Z^{\mathbf{A}} \longmapsto f^{\mathbf{A}}(x)$. Since $Z^{\mathbf{A}}$ has dimension 1, this set of non-properness has dimension at most 0 by [70, Theorem 3.8].

Since $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)$ has finitely many irreducible components, the lemma is proved. □

Let $B \in \mathbb{R}$ and $\varepsilon \in \mathbb{R}$. For $1 \leq i \leq d$, we will say that property

$$\mathsf{SOS}\left(f^{\mathbf{A}} + \varepsilon, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right), B\right)$$

holds if there exist:

- sums of squares of polynomials $S_i^{\mathbf{A}}$ and $T_i^{\mathbf{A}}$ in $\sum \mathbb{R}[\mathbf{X}]^2$,
- polynomials $C_{i,j}^{\mathbf{A}}$ in the ideal $\mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ and
- polynomials $g_{i,j}^{\mathbf{A}}$ in $\mathbb{R}[\mathbf{X}]$

satisfying

$$f^{\mathbf{A}} + \varepsilon = S_i^{\mathbf{A}} + T_i^{\mathbf{A}}(B - f^{\mathbf{A}}) + \sum_j g_{i,j}^{\mathbf{A}} C_{i,j}^{\mathbf{A}}.$$

We will say that property $\mathsf{SOS}\left(f^{\mathbf{A}} + \varepsilon, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right), B\right)$ holds if for all $1 \leq i \leq d$, properties $\mathsf{SOS}\left(f^{\mathbf{A}} + \varepsilon, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right), B\right)$ hold.

We are now ready to state the main results of this Chapter.

Theorem 7.4. *There exists a non-empty Zariski open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, if $f \geq 0$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ and $B \in f(V \cap \mathbb{R}^n)$, then for all $\varepsilon > 0$, property $\mathsf{SOS}\left(f^{\mathbf{A}} + \varepsilon, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right), B\right)$ holds.*

Proof. Let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski-open set given in Lemma 7.3. Recall that $\mathscr{O} = \mathscr{O}_1 \cap \mathscr{O}_3$, where $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ is the Zariski-open set given in Theorem 5.9 and $\mathscr{O}_3 \subset \mathrm{GL}_n(\mathbb{C})$ the Zariski-open set given in Theorem 5.12 (page 65).

We use Schweighofer's theorem (see Theorem 3.16 page 46). Since f is not necessarily bounded above, we consider the semi-algebraic sets $E_{B,i}^{\mathbf{A}} = \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \cap \left\{x \in \mathbb{R}^n \mid f^{\mathbf{A}}(x) \leq B\right\}$ for $1 \leq i \leq d$. Then for all $\varepsilon > 0$ and all $1 \leq i \leq d$,

1. for all $x \in E_{B,i}^{\mathbf{A}}$, $f^{\mathbf{A}}(x) + \varepsilon > 0$ since $f(x) \geq 0$;
2. $f^{\mathbf{A}}$ is bounded above on $E_{B,i}^{\mathbf{A}}$ by definition of $E_{B,i}^{\mathbf{A}}$;
3. $R_\infty\left(f^{\mathbf{A}} + \varepsilon, E_{B,i}^{\mathbf{A}}\right)$ is finite since $R_\infty\left(f^{\mathbf{A}}, \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right)\right)$ is;
4. $R_\infty\left(f^{\mathbf{A}} + \varepsilon, E_{B,i}^{\mathbf{A}}\right) \subset]0, +\infty[$ since $f + \varepsilon \geq \varepsilon > 0$.

Hence Theorem 3.16 implies that $f^{\mathbf{A}} + \varepsilon$ can be written as

$$f^{\mathbf{A}} + \varepsilon = \sum_{\delta \in \{0,1\}^p} \sigma_\delta e_1^{\delta_1} \ldots e_p^{\delta_p},$$

where $\delta = (\delta_1, \ldots, \delta_p)$ and $\sigma_\delta \in \sum \mathbb{R}[\mathbf{X}]^2$ and the e_j are the polynomials defining the semi-algebraic set $E_{B,i}^{\mathbf{A}}$. An equation $h = 0$ is replaced by the two inequalities $h \geq 0$ and $-h \geq 0$. By definition of $E_{B,i}^{\mathbf{A}}$, the e_j are then either $f^{\mathbf{A}} - B$ or a polynomial in $\mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ or the opposite of a polynomial in $\mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$. Then changing the names and reorganizing, we get

$$f^{\mathbf{A}} + \varepsilon = S_i^{\mathbf{A}} + T_i^{\mathbf{A}}(B - f^{\mathbf{A}}) + \sum_j g_{i,j}^{\mathbf{A}} C_{i,j}^{\mathbf{A}},$$

where $S_i^{\mathbf{A}}, T_i^{\mathbf{A}} \in \sum \mathbb{R}[\mathbf{X}]^2$, for all j, $C_{i,j}^{\mathbf{A}} \in \mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ and $g_{i,j}^{\mathbf{A}} \in \mathbb{R}[\mathbf{X}]$, where $g_{i,j}^{\mathbf{A}}$ is the difference of two sums of squares. □

7.3 Application in Optimization

In this paragraph, consider

- $f, h_1, \ldots, h_p \in \mathbb{Q}[\mathbf{X}]$,
- $S = \{x \in \mathbb{R}^n \mid h_1(x) = \cdots = h_r(x) = 0, h_{r+1}(x) \geq 0, \ldots, h_p(x) \geq 0\}$
- and $f^\star = \inf_{x \in S} f(x)$.

In Section 3.2.1, we have seen that using semidefinite programming, an approximation of a real number defined as

$$f_t^{\mathsf{sos}} = \sup\left\{ a \in \mathbb{R} \mid \exists \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2, f - a = \sigma_0 + \sum_{1 \leq i \leq p} \sigma_i h_i, \deg(\sigma_0), \deg(\sigma_i f_i) \leq 2t \right\},$$

can be computed.

If a belongs to the above set then for all $x \in S$, the inequation $f(x) - a \geq 0$ holds. Then $f(x) \geq a$, so that $f^\star \geq f_t^{\mathsf{sos}}$. This provides a lower bound on the infimum but in general, f_t^{sos} is not equal to $f^\star$.

However, we prove in the sequel that under additional properties, the f_t^{sos} are terms of a sequence converging to $f^\star$.

Proposition 7.5. *Let $h_1, \ldots, h_p \in \mathbb{Q}[\mathbf{X}]$ and $f^\star$ the infimum of f on the semi-algebraic set $\{x \in \mathbb{R}^n \mid h_1(x) = \cdots = h_r(x) = 0, h_{r+1}(x) \geq 0, \ldots, h_p(x) \geq 0\}$. Assume that for all $\varepsilon > 0$, there exists $\sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2$ such that*

$$f - (f^\star - \varepsilon) = \sigma_0 + \sum_{1 \leq i \leq p} \sigma_i h_i.$$

Then the sequence $(f_t^{\mathsf{sos}})_{t \in \mathbb{N}^*}$ converges monotonically increasing to $f^\star$.

Proof. First we show that the sequence $(f_t^{\mathsf{sos}})_{t \in \mathbb{N}^*}$ is monotonically increasing. For $t \in \mathbb{N}^*$, let $\mathbb{R}_{2t}[\mathbf{X}]$ be the set of polynomials in $\mathbb{R}[\mathbf{X}]$ of degree $\leq 2t$. Let $t_1 \leq t_2$. It is clear that $\mathbb{R}_{2t_1}[\mathbf{X}] \subset \mathbb{R}_{2t_2}[\mathbf{X}]$. Thus, $f_{t_1}^{\mathsf{sos}} \leq f_{t_2}^{\mathsf{sos}}$ and the sequence is monotonically increasing.

Furthermore, since $\mathbb{R}[\mathbf{X}] = \bigcup_t \mathbb{R}_{2t}[\mathbf{X}]$, the sequence $(f_t^{\mathsf{sos}})_{t \in \mathbb{N}^*}$ tends to the number

$$f^{\mathsf{sos}} = \sup \left\{ a \in \mathbb{R} \mid \exists \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2, f - a = \sigma_0 + \sum_{1 \leq i \leq p} \sigma_i h_i \right\}.$$

We finish the proof by showing that $f^\star = f^{\mathsf{sos}}$. By assumption, for all $\varepsilon > 0$, $f - (f^\star - \varepsilon)$ can be written

$$f - (f^\star - \varepsilon) = \sigma_0 + \sum_{1 \leq i \leq p} \sigma_i h_i,$$

for some $\sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2$. Then $a = f^\star - \varepsilon$ belongs to the set

$$\left\{ a \in \mathbb{R} \mid \exists \sigma_i \in \sum \mathbb{R}[\mathbf{X}]^2, f - a = \sigma_0 + \sum_{1 \leq i \leq p} \sigma_i h_i \right\}.$$

This means that $f^\star - \varepsilon \leq f^{\mathsf{sos}}$. Since this is true for all $\varepsilon > 0$, this implies that $f^\star \leq f^{\mathsf{sos}}$. Conversely, since $f^\star \geq f_t^{\mathsf{sos}}$ holds for all t, the inequality $f^\star \geq f^{\mathsf{sos}}$ always holds too. □

According to this proposition, if the existence of certificates of positivity on S is ensured then we are able to compute a sequence of lower bounds on $f^\star = \inf_{x \in S} f(x)$ that converges to $f^\star$.

Since we prove the existence of certificates on $E_{B,i}^{\mathbf{A}}$, we are able to compute a sequence converging to $\inf_{x \in E_{B,i}^{\mathbf{A}}} f^{\mathbf{A}}(x) = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i)} f^{\mathbf{A}}(x)$. Then to get a sequence of lower bounds converging to $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x)$, we prove that the infimum on $V \cap \mathbb{R}^n$ and the one on $\bigcup_{1 \leq i \leq d} \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) = \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}})$ are the same.

Proposition 7.6. *Let $\mathscr{O}_1 \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski-open set given in Theorem 5.9 and $f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x)$. Then for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}_1$,*

$$f^\star = \inf_{x \in V \cap \mathbb{R}^n} f(x) = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x).$$

Proof. Note first that if $x \in V \cap \mathbb{R}^n$ then $y = \mathbf{A}^{-1}x$ belongs to $V^{\mathbf{A}} \cap \mathbb{R}^n$ and satisfies $f(x) = f^{\mathbf{A}}(y)$. Then the set of values of f on $V \cap \mathbb{R}^n$ and the one of $f^{\mathbf{A}}$ on $V^{\mathbf{A}} \cap \mathbb{R}^n$ are the same, so that $\inf_{x \in V \cap \mathbb{R}^n} f(x) = \inf_{x \in V^{\mathbf{A}} \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$.

Since by definition, $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n \subset V^{\mathbf{A}}$, the inequality

$$f^\star = \inf_{x \in V^{\mathbf{A}} \cap \mathbb{R}^n} f^{\mathbf{A}}(x) \leq \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$$

holds. In the sequel, we prove that

$$\inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x) \leq \inf_{x \in V^{\mathbf{A}} \cap \mathbb{R}^n} f^{\mathbf{A}}(x) = f^\star.$$

Suppose first that there exists $x \in V^{\mathbf{A}} \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}(x) = f^\star$. Then x is a critical point of $f^{\mathbf{A}}_{|V^{\mathbf{A}} \cap \mathbb{R}^n}$ so that it belongs to $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ (see Remark 5.6 page 63). Since $f^{\mathbf{A}}(x) = f^\star$ is a value of $f^{\mathbf{A}}$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$, it is greater than or equal to the infimum $\inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$. Thus in this case,

$$\inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x) \leq f^\star.$$

Suppose now that for all $x \in V^{\mathbf{A}} \cap \mathbb{R}^n$, $f^{\mathbf{A}}(x) > f^\star$. Since $f^\star = \inf_{x \in V^{\mathbf{A}} \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$, this implies that there exists a real number $c > f^\star$ such that for all $t \in]f^\star, c[$, $V^{\mathbf{A}} \cap V(f^{\mathbf{A}} - t) \cap \mathbb{R}^n$ is not empty.

Let $\mathcal{Q}^{\mathbf{A}} \subset \mathbb{C}$ be the Zariski-open set given by Theorem 5.9. Without loss of generality, one can suppose that c is small enough so that $]f^\star, c[\subset \mathcal{Q}^{\mathbf{A}}$.

Then by Theorem 5.9, this implies that for all $t \in]f^\star, c[$, $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{V}\left(f^{\mathbf{A}} - t\right) \cap \mathbb{R}^n$ is not empty. Thus we can construct by induction a sequence of points (x_k) in $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) \cap \mathbb{R}^n$ such that $f^{\mathbf{A}}(x_k) \underset{k \to +\infty}{\longrightarrow} f^\star$. Since by definition of the infimum, $f^{\mathbf{A}}(x_k) \geq \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$ for all k, we get $f^\star \geq \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$, that ends the proof. □

Using the previous results, we know how to compute a sequence of relaxations that provides certified lower bounds on $f^\star$ that converge to $f^\star$. Practically, it is better to compute the infimum on each $E^{\mathbf{A}}_{B,i}$ instead of the union $\bigcup_{1 \leq i \leq d} E^{\mathbf{A}}_{B,i}$ directly. Indeed, the number of variables involved in the computation over $E^{\mathbf{A}}_{B,i}$ is smaller that in the computation over the union. Then, $f^\star$ is the smaller of previous infima.

More precisely, let B be any value in $f(V \cap \mathbb{R}^n)$. In the sequel, for $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q})$ and $t \in \mathbb{N}^*$, denote by $f^{\mathsf{sos},\mathbf{A}}_{i,t}$ the supremum of the numbers $a \in \mathbb{R}$ such that there exist

- sums of squares of polynomials $S^{\mathbf{A}}_i$ and $T^{\mathbf{A}}_i$ in $\sum \mathbb{R}[\mathbf{X}]^2$,
- polynomials $C^{\mathbf{A}}_{i,j}$ in the ideal $\mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ and

- polynomials $g_{i,j}^{\mathbf{A}}$ in $\mathbb{R}[\mathbf{X}]$

satisfying

$$f^{\mathbf{A}} - a = S_i^{\mathbf{A}} + T_i^{\mathbf{A}}(B - f^{\mathbf{A}}) + \sum_j g_{i,j}^{\mathbf{A}} C_{i,j}^{\mathbf{A}}.$$

Then for $1 \leq i \leq d$, we denote by $f_i^\star = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i) \cap \mathbb{R}^n} f^{\mathbf{A}}(x)$. Since $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}\right) = \bigcup_{1 \leq i \leq d} \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$,

$$\inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x) = \min\left\{f_1^\star, \ldots, f_d^\star\right\}.$$

Theorem 7.7. *There exists a non-empty Zariski-open set $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathscr{O}$, for $1 \leq i \leq d$, each sequence $\left(f_{i,t}^{\mathsf{sos},\mathbf{A}}\right)_{t \in \mathbb{N}^*}$ converges monotonically increasing to $f_i^\star$. Furthermore, $f^\star = \min\{f_1^\star, \ldots, f_d^\star\}$.*

Proof. Let $\mathscr{O} \subset \mathrm{GL}_n(\mathbb{C})$ be the Zariski-open set given in Theorem 7.4. By definition of $f_i^\star$, $f^{\mathbf{A}} \geq f_i^\star$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \cap \mathbb{R}^n$. We apply Theorem 7.4 with the polynomial $f - f_i^\star$ on $\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right) \cap \mathbb{R}^n$. Since for any value $v \in \mathbb{R}$, $\mathscr{C}\left(f^{\mathbf{A}} + v, \mathbf{F}^{\mathbf{A}}, i\right) = \mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)$, Theorem 7.4 implies that for $1 \leq i \leq d$, there exist:

- sums of squares of polynomials $S_i^{\mathbf{A}}$ and $T_i^{\mathbf{A}}$ in $\sum \mathbb{R}[\mathbf{X}]^2$,
- polynomials $C_{i,j}^{\mathbf{A}}$ in the ideal $\mathbb{I}\left(\mathscr{C}\left(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}, i\right)\right)$ and
- polynomials $g_{i,j}^{\mathbf{A}}$ in $\mathbb{R}[\mathbf{X}]$

such that

$$f^{\mathbf{A}} - (f_i^\star - \varepsilon) = S_i^{\mathbf{A}} + T_i^{\mathbf{A}}(B - f^{\mathbf{A}}) + \sum_j g_{i,j}^{\mathbf{A}} C_{i,j}^{\mathbf{A}}.$$

Thus from Proposition 7.5, we deduce that $f_{i,t}^{\mathsf{sos},\mathbf{A}}$ converges monotonically increasing to $f_i^\star$ when t tends to ∞.

Finally, Proposition 7.6 implies that

$$f^\star = \inf_{x \in \mathscr{C}(f^{\mathbf{A}}, \mathbf{F}^{\mathbf{A}}) \cap \mathbb{R}^n} f^{\mathbf{A}}(x),$$

that is necessarily $\min\{f_1^\star, \ldots, f_d^\star\}$. □

7.4 Computational Aspect

7.4.1 Reducing the Number of Equations

Lemma 7.8. *The set* $\mathsf{Minors}\left(\mathsf{Jac}\left(\left[\mathbf{F}^{\mathbf{A}}, f^{\mathbf{A}}\right], i+1\right), n-d+1\right)$ *can be replaced with* $(n-i)(p+1) - (n-d+1)^2 + 1$ *equations.*

Let $N = (N_{ij})$ be an $m \times n$ matrix of indeterminates over $\mathbb{C}$, ΔN its set of minors. Define the determinantal variety

$$D_{t-1}^{m,n} = \left\{ N \in \mathbb{C}^{m \times n} \mid \operatorname{rank} N < t \right\}.$$

For indices $a_1, \ldots, a_t, b_1, \ldots, b_t$ such that $t \leq \min(m, n)$ and

$$1 \leq a_1 < \cdots < a_t \leq m, \quad 1 \leq b_1 < \cdots < b_t \leq n,$$

we define $[a_1, \ldots, a_t | b_1, \ldots, b_t]$ to be the determinant of the submatrix N whose row indices are $a_1, \ldots, a_t$ and column indices are $b_1, \ldots, b_t$. Then

$$D_{t-1}^{m,n} = \left\{ N \in \mathbb{C}^{m \times n} \mid \forall [a_1, \ldots, a_t | b_1, \ldots, b_t] \in \Delta(N),\ [a_1, \ldots, a_t | b_1, \ldots, b_t] = 0 \right\}.$$

We define a partial ordering on $\Delta(N)$ as follows (see also [25, page 46]):

$$\begin{aligned} &[a_1, \ldots, a_u | b_1, \ldots, b_u] \leq [c_1, \ldots, c_v | d_1, \ldots, d_v] \\ &\iff u \geq v,\ a_1 \leq c_1, \ldots, a_v \leq c_v,\ b_1 \leq d_1, \ldots, b_v \leq d_v. \end{aligned}$$

For an arbitrary minor $\xi = [a_1, \ldots, a_u | b_1, \ldots, b_u]$ in $\Delta(N)$, we define its *length* by:

$$\begin{aligned} \operatorname{length} \xi = k \iff &\text{there is a chain } \xi = \xi_k > \xi_{k-1} > \ldots > \xi_1,\ \xi_i \in \Delta N, \\ &\text{and no longer chain starting with } \xi \text{ exits.} \end{aligned}$$

We prefer the notation of the *length* instead of the *rank* defined in [25, page 55].

Let $\Omega(N)$ be the set of all k-minors of N with $k \geq t$. For every $1 \leq l \leq mn - t^2 + 1$, define

$$\theta_l(N) = \sum_{\substack{\xi \in \Omega N \\ \operatorname{length}(\xi) = l}} \xi.$$

Lemma 7.9. *[25, Lemma 5.9] We have that*

$$D_{t-1}^{m,n} = \left\{ N \in \mathbb{C}^{m \times n} :\ \theta_l(N) = 0,\ l = 1, \ldots, mn - t^2 + 1 \right\}.$$

In [24, Theorem 2], they also proved that $mn - t^2 + 1$ is the smallest number of polynomials for defining the determinantal variety $D_{t-1}^{m,n}$.

To find all minors of a given length, it is convenient to generate all chains composed by minors in $\Omega(N)$. The following proposition gives the minor of the maximal length in $\Omega(N)$. Furthermore, we show in its proof how to construct all chains in $\Omega(N)$ starting with this minor.

Proposition 7.10. *The minor of the maximal length in $\Omega(N)$ is $[m - t + 1, \ldots, m | n - t + 1, \ldots, n]$ and its length is $mn - t^2 + 1$.*

Before the proof is given, we illustrate the construction of all chains for a special case where $m = 3, n = 4$ and $t = 2$. First we generate the set of chains consisting of 2-minors. Starting with the minor of the maximal length, if we decrease one of the indices of the previous minor by 1 and keep the indices of the new minor in strictly ascending order, a new minor of smaller length is generated. All chains consisting of 2-minors are shown in Figure 7.1, where the arrows point to minors of higher orderings. Then we collect all 3-minors and add them to the chains we have already constructed. The set of chains consisting of all minors in $\Omega(N)$ for $m = 3, n = 4, t = 2$ is shown in Figure 7.2.

From Figure 7.1 and 7.2, we notice the following two facts:

1. The k-minors in the same column have the same summation of their indices which is one less than that of the previous column.

2. The $(k+1)$-minors that can increase the length of chains consisting of k-minors are the ones with the form $[1, 2, \ldots, k, a|1, 2, \ldots, k, b]$, where $k+1 \leq a \leq m$ and $k+1 \leq b \leq n$.

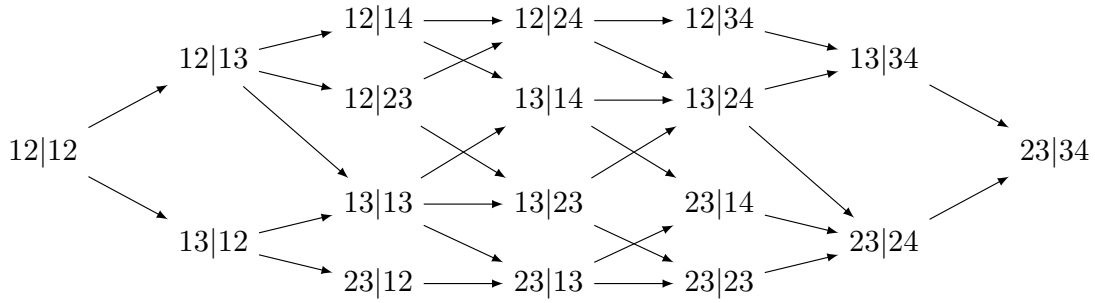


Figure 7.1: All chains consisting only of the 2-minors.

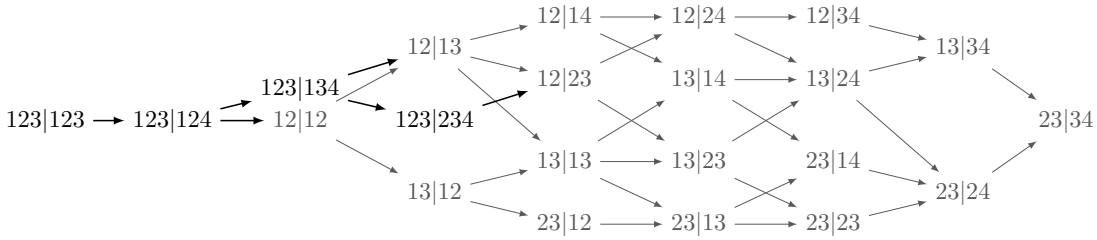


Figure 7.2: All chains consisting of the 2-minors and 3-minors.

Proof of Proposition 7.10. The first part of the statement is obvious. We prove the second part in the following. Without loss of generality, we assume that $m \leq n$.

First, we show how to generate the set of chains consisting of t-minors, denoted by $\mathfrak{C}_t$. Starting with $\xi = [m-t+1, \ldots, m|n-t+1, \ldots, n]$, the t-minor with the maximal length,

we construct new t-minors by decreasing one of the indices in ξ by 1 and keeping the indices of new minors in strictly ascending order. This process continues until we reach the minor $\xi_1 = [1, 2, \ldots, t|1, 2, \ldots, t]$ with the lowest ordering. Based on the observation (1), we can show that the maximal length of the chain χ_t from ξ to ξ_1 is

$$(2m - t + 1)t/2 + (2n - t + 1)t/2 - (1 + t)t + 1 = (m + n)t - 2t^2 + 1.$$

Secondly, we show how to add the $(t+1)$-minors in $\Omega(N)$ to the set of chains $\mathfrak{C}_t$ constructed above. Notice that for every $(t+1)$-minor $\xi = [a_1, \ldots, a_t, a_{t+1}|b_1, \ldots, b_t, b_{t+1}]$, the t-minor $\eta = [a_1, \ldots, a_t|b_1, \ldots, b_t]$ has already appeared in $\mathfrak{C}_t$. Since $\xi < \eta$, we put ξ in the column next (on the left) to the column consisting of η. Therefore, we generate the set of chains consisting of all $t+1$-minors in $\Omega(N)$, denoted by $\mathfrak{C}_{t+1}$. According to (1) and (2), we obtain that the maximal length of the chain χ_{t+1} from $[1, \ldots, t, m|1, \ldots, t, n]$ to $[1, \ldots, t, t+1|1, \ldots, t, t+1]$ is $m+n-2(t+1)+1$. Since all minors in χ_{t+1} are smaller than minors in χ_t, we can add the chain χ_{t+1} to the end of the chain χ_t.

Going through the same process, we can generate the chains $\chi_{t+2}, \ldots, \chi_m$. It is clear that the chain $\chi_m \to \ldots \to \chi_{t+1} \to \chi_t$ consisting in the minors in $\Omega(N)$ from $[1, \ldots, m|1, \ldots, m]$ to ξ and has the largest length

$$(m + n)t - 2t^2 + 1 + \sum_{s=t+1}^{m} (m + n - 2s + 1) = mn - t^2 + 1,$$

which is the length of ξ. □

We are now able to conclude with the proof of Lemma 7.8.

Proof of Lemma 7.8. The size of the Jacobian matrix $\mathsf{Jac}\left([\mathbf{F}^{\mathbf{A}}, f^{\mathbf{A}}], i+1\right)$ is $(p+1) \times (n-i)$. Applying Lemma 7.9 to it for $t = n-d+1$, we can reduce the number of equations in the set $\mathsf{Minors}\left(\mathsf{Jac}\left([\mathbf{F}^{\mathbf{A}}, f^{\mathbf{A}}], i+1\right), n-d+1\right)$ from $\binom{n-i}{n-d+1}\binom{p+1}{n-d+1}$ to $(n-i)(p+1) - (n-d+1)^2 + 1$. □

7.4.2 Numerical Results

In this section, our method is applied to compute certificates for lower bounds on $f^\star$. We set $\mathbf{A}$ to be the identity matrix. Thus we denote by $f_{i,t}^{\mathsf{sos}} = f_{i,t}^{\mathsf{sos},\mathbf{A}}$. We call the command IsRadical in the Maple package Polynomialldeals to test if an ideal I is radical and the command HilbertDimension in the package Groebner to compute the dimension of the variety $\mathbb{V}(I)$. In the following examples, this takes less than 1 second. The Matlab software SOSTOOLS [109] is then used to compute an approximation of $f_{i,t}^{\mathsf{sos}}$.

Optimization with only equality constraints. We consider polynomial optimization with only equality constraints for which we can apply our method directly,

$$\inf_{x \in \mathbb{R}^n} f(x) \tag{7.1}$$

$$\text{s.t. } f_1(x) = \ldots = f_p(x) = 0. \tag{7.2}$$

The main contributions of our approach compared with [84], [39], and [100] are:

- There is no compactness requirement of the feasible set.
- We do not assume that the KKT conditions are satisfied at the minimizer or the minimum $f^\star$ is reached.
- Our regularity assumptions **R** are weaker than the assumptions in [100].

Example 7.11. *[100, Example 5.2] Consider the optimization problem*

$$\begin{aligned}\inf_{x\in\mathbb{R}^3}\ & x_1^6+x_2^6+x_3^6+3x_1^2x_2^2x_3^2-x_1^2(x_2^4+x_3^4)-x_2^2(x_3^4+x_1^4)-x_3^2(x_1^4+x_2^4)\\ s.t.\ & x_1+x_2+x_3-1=0.\end{aligned}$$

The feasible set is non-compact. The objective function is the Robinson polynomial which is non-negative everywhere but not SOS. We have $f^\star=0$. Let $\mathbf{F}=[x_1+x_2+x_3-1]$. Then the dimension of the ideal $\langle\mathbf{F}\rangle$ is 2.

- *To compute f_1^{sos}, we have $\mathscr{C}(f,\mathbf{F},1)=\mathbb{V}(\mathbf{F},h)$ where*

$$\begin{aligned}h=&6x_2^5+6x_1^2x_2x_3^2-4x_1^2x_2^3-2x_2x_3^4-2x_2x_1^4-4x_3^2x_2^3\\&-6x_3^5-6x_1^2x_2^2x_3+4x_1^2x_3^3+4x_2^2x_3^3+2x_3x_1^4+2x_3x_2^4.\end{aligned}$$

  Setting $B=f(1,0,0)=1$, the lower bounds we computed are: $f_{1,3}^{\mathsf{sos}}=-5.8186\times10^{-2}$, $f_{1,4}^{\mathsf{sos}}=-1.6531\times10^{-2}$, $f_{1,5}^{\mathsf{sos}}=-4.1363\times10^{-4}$, $f_{1,6}^{\mathsf{sos}}=4.2929\times10^{-10}$. The sign of the last lower bound is not correct due to the numerical issues.

- *To compute f_2^{sos}, we have $\mathscr{C}(f,\mathbf{F},2)=\mathbb{V}(x_1,g)$. It is equivalent to solving, replacing x_1 with 0,*

$$\begin{aligned}\inf_{(x_2,x_3)\in\mathbb{R}^2}\ & x_2^6+x_3^6-x_2^2x_3^4-x_3^2x_2^4\\ s.t.\ & x_2+x_3-1=0.\end{aligned}$$

  Setting $B=f(1,0)=1$, the lower bounds we obtained are: $f_{2,2}^{\mathsf{sos}}=-8.0658\times10^{-12}$, $f_{2,3}^{\mathsf{sos}}=-9.1665\times10^{-12}$. It is clear that f_2^{sos} is also equal to $f^\star$.

Example 7.12. *Consider the optimization problem*

$$\begin{aligned}\inf_{x\in\mathbb{R}^2}\ & (x_1+1)^2+x_2^2\\ s.t.\ & -x_1^3+x_2^2=0.\end{aligned}$$

*Obviously, we have $x^\star=(0,0)$ and $f^\star=1$. It is easy to check that the feasible set is non-compact and the KKT conditions are not satisfied at the minimizer. The regularity assumption **R** is satisfied and $d=1$. With $\mathscr{C}(f,\mathbf{F},1)=\mathbb{V}\left(-x_1^3+x_2^2\right)$ and $B=f(0,0)=1$, the lower bounds we obtained are: $f_{1,2}^{\mathsf{sos}}=0.99842$, $f_{1,3}^{\mathsf{sos}}=0.9989$, $f_{1,4}^{\mathsf{sos}}=0.99865$, $f_{1,5}^{\mathsf{sos}}=0.99844$. Although there are numerical errors, we do get good approximations of the minimum $f^\star$.*

Example 7.13. *Consider the constrained optimization problem*

$$\begin{aligned} &\inf_{x\in\mathbb{R}^2} \; x_1 \\ &\; s.t. \; x_1x_2^2 - 1 = 0. \end{aligned}$$

The KKT system $\{1-\lambda x_2^2,\ -2x_1x_2\lambda,\ x_1x_2^2-1\}$ *has no solution. Applying our method,* $d = 1$ *and* $\mathscr{C}(f,\mathbf{F},1) = \mathbb{V}\left(x_1^2x_2^2-1\right)$. *With* $B = f(1,1) = 1$, *the lower bounds we obtained are:* $f_{1,3}^{\mathsf{sos}} = 2.5255\times10^{-3}$, $f_{1,4}^{\mathsf{sos}} = 1.902\times10^{-2}$, $f_{1,5}^{\mathsf{sos}} = 8.1335\times10^{-2}$. *Obviously, there are big numerical problems:* $x_2 \to \infty$, *which leads to some elements of the moment matrices used to solve the associated SDP's tending toward infinity. We can employ the sparse support monomials in the computation of* $f_{i,t}^{\mathsf{sos},\mathbf{A}}$ *to fight against this problem. Similar analysis can be found in [54].*

Optimization with inequality constraints. In the following we consider the general optimization problem

$$\begin{aligned} &\inf_{x\in\mathbb{R}^n} \; f(x) \\ &\; s.t. \; f_1(x) = \cdots = f_p(x) = 0, \\ &\qquad g_1(x) \geq 0, \ldots, g_q(x) \geq 0. \end{aligned} \tag{7.3}$$

Although our method applies to the global optimization of polynomials restricted to a smooth variety, it can be used to solve the problem (7.3) if we introduce new variables $t = [t_1, \ldots, t_q]$ and turn inequalities into equality constraints:

$$\begin{aligned} &\inf_{x\in\mathbb{R}^n, t\in\mathbb{R}^q} \; f(x) \\ &\; s.t. \; f_1(x) = \cdots = f_p(x) = 0, \\ &\qquad g_1(x) - t_1^2 = 0, \ldots, g_q(x) - t_q^2 = 0. \end{aligned}$$

However, we notice that related SDP problems may become very ill-conditioned because of these extra variables. Here are some techniques we used to handle numerical difficulties in order to improve the accuracy of a computed solution:

- Scaling the problem to make the magnitudes of all nonzero components of optimal solutions close to 1. Although it is impossible to make an ideal scaling before we know the optimal solutions, sometimes we can still do so by performing a linear transformation of the variables if we know finite lower and upper bounds constraints on them.
- Choosing B as close to the optimum as possible.
- Normalizing the coefficients of the polynomials in (7.3).

For more details about these techniques, see [142].

Example 7.14. *[39, Example 4.3] Consider the optimization problem under constraints*

$$\begin{aligned}&\inf_{x\in\mathbb{R}^2} (-4x_1^2+x_2^2)(3x_1+4x_2-12)\\ &s.t.\ 3x_1-4x_2\le 12,\ 2x_1-x_2\le 0,\ -2x_1-x_2\le 0.\end{aligned}$$

The semi-algebraic set defined by the constraints is non-compact. The global minimum is $f^\star=-\frac{1024}{55}\approx -18.6182$ *and the minimizer is* $x^\star=(24/55,\ 128/55)\approx(-0.4364, 2.3273)$. *Let* $g_1=12-3x_1+4x_2-t_1^2,\ g_2=x_2-2x_1-t_2^2,\ g_3:=x_2+2x_1-t_3^2$, *then the dimension of the ideal* $\langle g_1,g_2,g_3\rangle$ *is 2.*

- *To compute* f_1^{sos}, *we have* $\mathscr{C}(f,\mathbf{F},1)=\mathbb{V}(g_1,g_2,g_3,h)$, *where* $h=(-16x_1^2+6x_2x_1+12x_2^2-24x_2)t_1t_2t_3$. *Setting* $B=f(0,0,0)=0$, *the lower bounds we computed are:* $f_{1,3}^{\mathsf{sos}}=-20.184$, $f_{1,4}^{\mathsf{sos}}=-18.618$.
- *To compute* f_2^{sos}, *we have* $\mathscr{C}(f,\mathbf{F},1)=\mathbb{V}(g_1,g_2,g_3,x_1)$. *It is equivalent to solving*

$$\begin{aligned}&\inf_{x\in\mathbb{R}^4,t\in\mathbb{R}^3} x_2^2(4x_2-12)\\ &\quad s.t.\ -4x_2+t_1^2=12,\ -x_2+t_2^2=0,\ -x_2+t_3^2=0.\end{aligned}$$

  It is easy to see that $f_2^{\mathsf{sos}}=-16$ *which is not equal to* $f^\star$.

Example 7.15. *[39, Example 4.5] Consider the following non-convex quadratic optimization*

$$\begin{aligned}&\inf_{x\in\mathbb{R}^2} x_1^2+x_2^2\\ &s.t.\ x_2^2-1\ge 0,\\ &\quad x_1^2-Nx_1x_2-1\ge 0,\\ &\quad x_1^2+Nx_1x_2-1\ge 0.\end{aligned}$$

It is shown in [39] that the global minimum is $f^\star=\frac{1}{2}\left(N^2+N\sqrt{N^2+4}\right)+2$. *Let*

- $g_1=x_2^2-1-t_1^2$,
- $g_2=x_1^2-Nx_1x_2-1-t_2^2$,
- $g_3=x_1^2+Nx_1x_2-1-t_3^2$.

Then the dimension of the ideal $\langle g_1,g_2,g_3\rangle$ *is 2. It can be checked that* $\mathscr{C}(f,\mathbf{F},2)=\varnothing$. *Hence, in the following we only compute* f_1^{sos} *for some given constants* N. *We have* $\mathscr{C}(f,\mathbf{F},1)=\mathbb{V}(g_1,g_2,g_3,h)$, *where* $h=x_2t_1t_2t_3$.

- $N=2$, *then we have* $f^\star=6.8284$. *For* $B=f(3,1)=10$, *the results are:* $f_{1,2}^{\mathsf{sos}}=4$, $f_{1,3}^{\mathsf{sos}}=6.7692$, $f_{1,4}^{\mathsf{sos}}=6.8284$.

- $N = 3$, *then we have* $f^\star = 11.9083$. *For* $B = f(4,1) = 17$, *the results are:* $f_{1,2}^{\mathsf{SOS}} = 5$, $f_{1,3}^{\mathsf{SOS}} = 11.316$, $f_{1,4}^{\mathsf{SOS}} = 11.908$.
- $N = 4$, *then we have* $f^\star = 18.9443$. *For* $B = f(5,1) = 26$, *the results are:* $f_{1,2}^{\mathsf{SOS}} = 6$, $f_{1,3}^{\mathsf{SOS}} = 17.2$, $f_{1,4}^{\mathsf{SOS}} = 22.168$. *If we set* $B = f(4.3,1) = 19.49$, *the results are:* $f_{1,2}^{\mathsf{SOS}} = 15.333$, $f_{1,3}^{\mathsf{SOS}} = 18.944$.

Index

Index of Notations

Bibliography

[1] M. Abril Bucero and B. Mourrain. Certified relaxation for polynomial optimization on semi-algebraic sets.

[2] M. Abril Bucero, B. Mourrain, and P. Trebuchet. Unconstraint global polynomial optimization via Gradient Ideal.

[3] C. Aholt, S. Agarwal, and R. Thomas. A qcqp approach to triangulation. In *Computer Vision–ECCV 2012*, pages 654–667. Springer, 2012.

[4] C. Aholt, B. Sturmfels, and R. Thomas. A hilbert scheme in computer vision. *arXiv preprint arXiv:1107.2875*, 2011.

[5] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition i: The basic algorithm. *SIAM Journal on Computing*, 13(4):865–877, 1984.

[6] E. Artin. Über die zerlegung definiter funktionen in quadrate. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5:100–115, 1927.

[7] M. Atiyah and I. MacDonald. *Introduction to commutative algebra*. Addison-Wesley, 1969.

[8] B. Balasundaram and S. Butenko. Constructing test functions for global optimization using continuous formulations of graph problems. *Optim. Methods Softw.*, 20(4-5):439–452, 2005.

[9] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop. Polar varieties, real equation solving, and data structures: the hypersurface case. *Journal of complexity*, 13(1):5–27, 1997.

[10] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties, real equation solving, and data structures: the hypersurface case. *Journal of complexity*, 13(1):5–27, 1997.

[11] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop. Polar varieties and efficient real elimination. *Math. Z.*, 238(1):115–144, 2001.

[12] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo. Generalized polar varieties: Geometry and algorithms. *Journal of complexity*, 21(4):377–412, 2005.

[13] B. Bank, M. Giusti, J. Heintz, and M. Safey El Din. Intrinsic complexity estimates in polynomial optimization. *arXiv preprint arXiv:1304.5214*, 2013.

[14] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, 21(1):33–83, 2010.

[15] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, November 1996.

[16] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, second edition, 2006.

[17] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Sci.*, 22(3):317–330, 1983.

[18] R. Berr and T. Wörmann. Positive polynomials and tame preorderings. *Mathematische Zeitschrift*, 236(4):813–840, 2001.

[19] G. Blekherman. There are significantly more nonnegative polynomials than sums of squares. *Israel Journal of Mathematics*, 153:355–380, 2006.

[20] J. Bochnak, M Coste, and M.-F. Roy. *Real Algebraic Geometry*. Springer, 1998.

[21] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[22] C. W. Brown. *Solution formula construction for truth-invariant cads*. PhD thesis, University of Delaware, 1999.

[23] C. W. Brown. Qepcad b: a program for computing with semi-algebraic sets using cads. *ACM SIGSAM Bulletin*, 37(4):97–108, 2003.

[24] W. Bruns and R. Schwänzl. The number of equations defining a determinantal variety. *Bull. London Math. Soc.*, 22(5):439–445, 1990.

[25] W. Bruns and U. Vetter. *Determinantal rings*. Springer, Berlin, 1988.

[26] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 10(3):19–29, August 1976.

[27] G. Cassier. Probléme des moments sur un compact de rn et décomposition de polynomes a plusieurs variables. *Journal of Functional analysis*, 58(3):254–266, 1984.

[28] C. Chen, M. Moreno Maza, B. Xia, and L. Yang. Computing cylindrical algebraic decomposition via triangular decomposition. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, pages 95–102. ACM, 2009.

[29] M. D. Choi, T. Y. Lam, and B. Reznick. Sums of squares of real polynomials. In *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*, volume 58 of *Proc. Sympos. Pure Math.*, pages 103–126. Amer. Math. Soc., Providence, RI, 1995.

[30] T. F. Coleman and A. P. Liao. An efficient trust region method for unconstrained discrete-time optimal control problems. *Comput. Optim. Appl.*, 4(1):47–66, 1995.

[31] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, pages 134–183. Lecture Notes in Comput. Sci., Vol. 33. Springer, Berlin, 1975.

[32] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, pages 134–183. Lecture Notes in Comput. Sci., Vol. 33. Springer, Berlin, 1975.

[33] G. E. Collins and H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. In *Quantifier elimination and cylindrical algebraic decomposition (Linz, 1993)*, Texts Monogr. Symbol. Comput., pages 174–200. Springer, Vienna, 1998.

[34] Clayton W. Commander. Maximum cut problem, max-cut. In *Encyclopedia of Optimization*, pages 1991–1999. Springer, 2009.

[35] M. Coste. *An Introduction to Semialgebraic Geometry.* Dottorato di ricerca in matematica / Università di Pisa, Dipartimento di Matematica. Istituti Editoriali e Poligrafici Internazionali, 2000.

[36] P. Cousot. Proving program invariance and termination by parametric abstraction, lagrangian relaxation and semidefinite programming. In Radhia Cousot, editor, *Verification, Model Checking, and Abstract Interpretation*, volume 3385 of *Lecture Notes in Computer Science*, pages 1–24. Springer Berlin / Heidelberg, 2005.

[37] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms.* Springer, 2006.

[38] E. de Klerk. *Aspects of Semidefinite Programming: interior point algorithms and selected applications.* Kluwer Academic Publishers, 2002.

[39] J. Demmel, J. Nie, and V. Powers. Representations of positive polynomials on noncompact semialgebraic sets via kkt ideals. *Journal of pure and applied algebra*, 209(1):189–200, 2007.

[40] M. M. Deza and M. Laurent. *Geometry of cuts and metrics*, volume 15 of *Algorithms and Combinatorics.* Springer, Heidelberg, 2010. First softcover printing of the 1997 original [MR1460488].

[41] A. Dolzmann and T. Sturm. Redlog: Computer algebra meets computer logic. *Acm Sigsam Bulletin*, 31(2):2–9, 1997.

[42] C. Durvye. *Algorithms for primary decomposition of zero-dimensional polynomial ideals given by an evaluation structure.* PhD thesis, Université de Versailles-Saint-Quentin en Yvelines, 2008.

[43] C. Durvye and G. Lecerf. A concise proof of the kronecker polynomial system solver from scratch. *Expositiones Mathematicae*, 26(2):101–139, 2008.

[44] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry.* Springer-Verlag, 1995.

[45] H. Everett, D. Lazard, S. Lazard, and M. Safey El Din. The Voronoi diagram of three lines. *Discrete Comput. Geom.*, 42(1):94–130, 2009.

[46] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[47] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic), New York, 2002. ACM.

[48] P. Festa, P. M. Pardalos, M. G. C. Resende, and C. C. Ribeiro. Randomized heuristics for the MAX-CUT problem. *Optim. Methods Softw.*, 17(6):1033–1058, 2002.

[49] C. J. Friedrich. *Alfred Weber's theory of location of industries.* University of Chicago Press, 1929.

[50] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.

[51] A. Greuet and M. Safey El Din. Deciding reachability of the infimum of a multivariate polynomial. In *ISSAC*, pages 131–138, 2011.

[52] A. Greuet and M. Safey El Din. Probabilistic and exact algorithm for the global optimization of a polynomial over a real algebraic set. *arXiv:1307.8281*, 2013.

[53] A. Greuet, F. Guo, M. Safey El Din, and L. Zhi. Global optimization of polynomials restricted to a smooth variety using sums of squares. *Journal of Symbolic Computation*, 47(5):503 – 518, 2012.

[54] F. Guo, M. Safey El Din, and L. Zhi. Global optimization of polynomials using generalized critical values and sums of squares. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, 2010.

[55] Q. Guo, M. Safey EI Din, and L. Zhi. Computing rational solutions of linear matrix inequalities. In *Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation*, ISSAC '13, pages 197–204, New York, NY, USA, 2013. ACM.

[56] R. Hartley and A. Zisserman. *Multiple view geometry in computer vision*, volume 2. Cambridge Univ Press, 2000.

[57] J. Heintz and C.-P. Schnorr. Testing polynomials which are easy to compute (extended abstract). In *STOC*, pages 262–272, 1980.

[58] C. Helmberg and F. Oustry. Bundle methods to minimize the maximum eigenvalue function. In *Handbook of Semidefinite Programming*, pages 307–337. Springer, 2000.

[59] C. Helmberg and F. Rendl. A spectral bundle method for semidefinite programming. *SIAM Journal on Optimization*, 10(3):673–696, 2000.

[60] D. Henrion and A. Garulli, editors. *Positive polynomials in control*, volume 312 of *Lecture Notes in Control and Information Sciences*. Springer-Verlag, Berlin, 2005.

[61] D. Henrion and J.-B. Lasserre. GloptiPoly: global optimization over polynomials with Matlab and SeDuMi. *ACM Trans. Math. Software*, 29(2):165–194, 2003.

[62] D. Henrion, M. Šebek, and V. Kučera. Positive polynomials and robust stabilization with fixed-order controllers. *IEEE Trans. Automat. Control*, 48(7):1178–1186, 2003.

[63] D. Hilbert. Über die darstellung definiter formen als summe von formenquadraten. *Mathematische Annalen*, 32(3):342–350, 1888.

[64] C. Hillar. Sums of squares over totally real fields are rational sums of squares. *Proceedings of the American Mathematical Society*, 137(3):921–930, 2009.

[65] J. Hiriart-Urruty and C. Lemarechal. Convex analysis and minimization algorithms ii, 1991.

[66] J.-B. Hiriart-Urruty and C. Lemaréchal. Convex analysis and minimization algorithms i. *Springr-Verlag, Berlin*, 1993.

[67] H. Hong. Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination. In *Papers from the international symposium on Symbolic and algebraic computation*, ISSAC '92, pages 177–188, New York, NY, USA, 1992. ACM.

[68] H. Hong and M. Safey El Din. Variant quantifier elimination. *Journal of Symbolic Computation*, 47(7):883–901, 2012.

[69] T. Jacobi. A representation theorem for certain partially ordered commutative rings. *Mathematische Zeitschrift*, 237(2):259–273, 2001.

[70] Z. Jelonek. Testing sets for properness of polynomial mappings. *Math. Ann.*, 315(1):1–35, 1999.

[71] Z. Jelonek. On the generalized critical values of a polynomial mapping. *manuscripta mathematica*, 110(2):145–157, 2003.

[72] Z. Jelonek and K. Kurdyka. On asymptotic critical values of a complex polynomial. *Journal Fur Die Reine Und Angewandte Mathematik*, 565:1–12, 2003.

[73] G. Jeronimo, D. Perrucci, and E. P. Tsigaridas. On the minimum of a polynomial function on a basic closed semialgebraic set and applications. *SIAM J. on Optimization*, (Accepted):1–17, 2012.

[74] E. Kaltofen. On computing determinants of matrices without divisions. In P. S. Wang, editor, *Proc. 1992 (ISSAC'92)*, pages 342–349, New York, N. Y., 1992. ACM Press.

[75] E. L. Kaltofen, B. Li, Z. Yang, and L. Zhi. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *J. Symbolic Comput.*, 47(1):1–15, 2012.

[76] K. C. Kiwiel. Proximity control in bundle methods for convex nondifferentiable minimization. *Mathematical Programming*, 46(1-3):105–122, 1990.

[77] T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic nullstellensatz. *Duke Mathematical Journal*, 109(3):521–598, 2001.

[78] J.-L. Krivine. Anneaux préordonnés. *J. Analyse Math.*, 12:307–326, 1964.

[79] E. Kunz. *Introduction to commutative algebra and algebraic geometry.* Birkhäuser Boston, 1984.

[80] K. Kurdyka, P. Orro, and S. Simon. Semialgebraic Sard theorem for generalized critical values. *J. Differential Geom.*, 56(1):67–92, 2000.

[81] K. Kurdyka, P. Orro, and S. Simon. Semialgebraic Sard theorem for generalized critical values. *Journal of Differential Geometry*, 56(1):67–92, 2000.

[82] E. Landau. Über die darstellung definiter funktionen durch quadrate. *Mathematische Annalen*, 62(2):272–285, 1906.

[83] S. Lang. *Algebra.* Springer-Verlag New York Inc, revised third edition, 2002.

[84] J.-B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817 (electronic), 2001.

[85] J.-B. Lasserre. A sum of squares approximation of nonnegative polynomials. *SIAM review*, 49(4):651–669, 2007.

[86] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. *Emerging applications of algebraic geometry*, pages 157–270, 2009.

[87] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*, pages 157–270. Springer, 2009.

[88] A. Lax and P. D. Lax. On sums of squares. *Linear Algebra and Appl.*, 20(1):71–75, 1978.

[89] D. Lazard and F. Rouillier. Solving parametric polynomial systems. *J. Symbolic Comput.*, 42(6):636–667, 2007.

[90] G. Lecerf. *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques.* PhD thesis, École polytechnique, France, 2001.

[91] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003.

[92] J. Löfberg. Yalmip: A toolbox for modeling and optimization in matlab. *Proc. IEEE CCA/ISIC/CACSD Conf.*, 2004.

[93] A. Logar. A computational proof of the noether normalization lemma. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 259–273. Springer, 1989.

[94] S. McCallum. An improved projection operation for cylindrical algebraic decomposition. In *Quantifier elimination and cylindrical algebraic decomposition (Linz, 1993)*, Texts Monogr. Symbol. Comput., pages 242–268. Springer, Vienna, 1998.

[95] D. Monniaux. On using sums-of-squares for exact computations without strict feasibility. , 2010.

[96] G. Moroz. Properness defects of projection and minimal discriminant variety. *J. Symbolic Comput.*, 46(10):1139–1157, 2011.

[97] T. S. Motzkin. The arithmetic-geometric inequality. In *Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965)*, pages 205–224. Academic Press, New York, 1967.

[98] Y. Nesterov et al. Squared functional systems and optimization problems. *High performance optimization*, 33:405–440, 2000.

[99] J. Nie. Polynomial optimization with real varieties. *arXiv preprint arXiv:1211.1940*, 2012.

[100] J. Nie. An exact jacobian sdp relaxation for polynomial optimization. *Mathematical Programming*, 137(1-2):225–255, 2013.

[101] J. Nie, J. Demmel, and B. Sturmfels. Minimizing polynomials via sum of squares over the gradient ideal. *Math. Program.*, 106(3, Ser. A):587–606, 2006.

[102] J. Nie and M. Schweighofer. On the complexity of putinar's positivstellensatz. *J. Complex.*, 23(1):135–150, February 2007.

[103] P. A. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization.* Dissertation (Ph.D.), California Institute of Technology, 2000.

[104] P. A. Parrilo and B. Sturmfels. Minimizing polynomial functions. *Algorithmic and quantitative real algebraic geometry, DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 60:83–99, 2003.

[105] H. Peyrl and P. A. Parrilo. Computing sum of squares decompositions with rational coefficients. *Theoretical Computer Science*, 409(2):269 – 281, 2008. Symbolic-Numerical Computations.

[106] Y. Pourchet. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *Acta Arithmetica*, 19(1):89–104, 1971.

[107] V. Powers. Rational certificates of positivity on compact semialgebraic sets. *Pacific J. Math.*, 251(2):385–391, 2011.

[108] V. Powers and T. Wörmann. An algorithm for sums of squares of real polynomials. *Journal of pure and applied algebra*, 127(1):99–104, 1998.

[109] S. Prajna, A. Papachristodoulou, P. Seiler, and P. A. Parrilo. *SOSTOOLS: Sum of squares optimization toolbox for MATLAB*, 2004.

[110] A. Prestel and M. Bradley. Representation of a real polynomial f (x) as a sum of 2m-th powers of rational functions. In *Ordered Algebraic Structures*, pages 197–207. Springer, 1989.

[111] M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana University Mathematics Journal*, 42(3):969–984, 1993.

[112] R. Quarez. Bounding the rational sums of squares over totally real fields. *arXiv preprint arXiv:0907.2336*, 2009.

[113] B. Reznick. Some concrete aspects of Hilbert's 17th Problem. In *Real algebraic geometry and ordered structures (Baton Rouge, LA, 1996)*, volume 253 of *Contemp. Math.*, pages 251–272. Amer. Math. Soc., Providence, RI, 2000.

[114] R. M. Robinson. Some definite polynomials which are not sums of squares of real polynomials. In *Selected questions of algebra and logic (collection dedicated to the memory of A. I. Mal'cev) (Russian)*, pages 264–282. Izdat. "Nauka" Sibirsk. Otdel., Novosibirsk, 1973.

[115] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Appl. Algebra Eng. Commun. Comput.*, 9(5):433–461, 1999.

[116] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *J. Complexity*, 16(4):716–750, 2000.

[117] M. Safey El Din. Testing sign conditions on a multivariate polynomial and applications. *Mathematics in Computer Science*, 1(1):177–207, 2007.

[118] M. Safey El Din. Computing the global optimum of a multivariate polynomial over the reals. In *ISSAC*, pages 71–78, 2008.

[119] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth algebraic set. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 224–231 (electronic), New York, 2003. ACM.

[120] M. Safey El Din and É. Schost. Properness defects of projections and computation of at least one point in each connected component of a real algebraic set. *Discrete Comput. Geom.*, 32(3):417–430, 2004.

[121] M. Safey El Din and E. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *arXiv preprint arXiv:1307.7836*, 2013.

[122] M. Safey El Din and L. Zhi. Computing rational points in convex semialgebraic sets and sum of squares decompositions. *SIAM Journal on Optimization*, 20(6):2876–2889, 2010.

[123] C. Scheiderer. Descending the ground field in sums of squares representations. *arXiv preprint arXiv:1209.2976*, 2012.

[124] J. Schmid. *On the degree complexity of Hilbert's 17th problem and the real nullstellensatz.* Habilitationsschrift, Universitat Dortmund, 1998.

[125] K. Schmüdgen. Thek-moment problem for compact semi-algebraic sets. *Mathematische Annalen*, 289:203–206, 1991.

[126] É. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):349–393, 2003.

[127] H. Schramm and J. Zowe. A version of the bundle idea for minimizing a nonsmooth function: Conceptual idea, convergence analysis, numerical results. *SIAM Journal on Optimization*, 2(1):121–152, 1992.

[128] M. Schweighofer. Algorithmische beweise für nichtnegativ-und positivstellensätze. *Master's thesis, Universität Passau*, 1999.

[129] M. Schweighofer. Iterated rings of bounded elements and generalizations of schmudgen's positivstellensatz. *Journal fur die Reine und Angewandte Mathematik*, pages 19–46, 2003.

[130] M. Schweighofer. Global optimization of polynomials using gradient tentacles and sums of squares. *SIAM Journal on Optimization*, 17(3):920–942 (electronic), 2006.

[131] A. Seidl and T. Sturm. A generic projection operator for partial cylindrical algebraic decomposition. In *Proceedings of the 2003 international symposium on Symbolic and algebraic computation*, pages 240–247. ACM, 2003.

[132] F. Severi. Sulle intersezioni delle varieta algebriche e sopra i loro caratteri e singolarita proiettive. *Mem. Accad. Sci. Torino*, 52(2):61–118, 1902.

[133] F. Severi. La serie canonica e la teoria delle serie principali di gruppi di punti sopra una superficie algebrica. *Commentarii Mathematici Helvetici*, 4(1):268–326, 1932.

[134] I. Shafarevich. *Basic Algebraic Geometry 1*. Springer Verlag, 1977.

[135] N. Z. Shor. An approach to obtaining global extrema in polynomial problems of mathematical programming. *Kibernetika (Kiev)*, pages 102–106, 136, 1987.

[136] G. Stengle. A nullstellensatz and a positivstellensatz in semialgebraic geometry. *Math. Ann.*, 207:87–97, 1974.

[137] A. W. Strzeboński. Cylindrical algebraic decomposition using validated numerics. *Journal of Symbolic Computation*, 41(9):1021–1038, 2006.

[138] A. Tarski. *A decision method for elementary algebra and geometry.* Springer, 1998.

[139] J. A. Todd. The geometrical invariants of algebraic loci. In *Congresso Internationale dei Matematici (Bologna, 1928)*, volume 4, page 93, 1937.

[140] J. A. Todd. The arithmetical invariants of algebraic loci. *Proceedings of the London Mathematical Society*, 2(1):190–225, 1938.

[141] Hà H. V. and Phạm T. S. Global optimization of polynomials using the truncated tangency variety and sums of squares. *SIAM Journal on Optimization*, 19(2):941–951, 2008.

[142] H. Waki, S. Kim, M. Kojima, M. Muramatsu, and H. Sugimoto. Algorithm 883: sparsePOP—a sparse semidefinite programming relaxation of polynomial optimization problems. *ACM Trans. Math. Software*, 35(2):Art. 15, 13, 2009.