Thèse présentée pour obtenir le grade de

DOCTEUR de SORBONNE UNIVERSITÉ

Specialité

Informatique

École Doctorale

Informatique, Télécommunications et Électronique (Paris)

Connexité dans les ensembles algébriques réels

algorithmes et applications

Présentée par

Rémi PRÉBET

Thèse dirigée par

Mohab SAFEY EL DIN

Soutenue le **20 décembre 2023**,
devant un jury composé de :

Laurent BUSÉ, Directeur de Recherche, Inria Sophia Antipolis	*Rapporteur*
Alicia DICKENSTEIN, Professeure, Universidad de Buenos Aires	*Rapporteure*
Peter BÜRGISSER, Professeur, Technical University of Berlin	*Examinateur*
Fatemeh MOHAMMADI, Professeur, Katholieke Universiteit Leuven	*Examinatrice*
Jean PONCE, Professeur des Universités, École Normale Supérieure-PSL/NYU	*Président*
Bernd STURMFELS, Professeur, University of California at Berkeley/MPI Liepzig	*Examinateur*
Emmanuel TRÉLAT, Professeur des Universités, Sorbonne Université	*Examinateur*
Éric SCHOST, Professeur, University of Waterloo	*Invité*
Mohab SAFEY EL DIN, Professeur des Universités, Sorbonne Université	*Directeur de thèse*

Résumé

Titre : *Connexité dans les ensembles algébriques réels : algorithmes et applications*
Mots clés : calcul formel, systèmes polynomiaux, géométrie algébrique réelle, robotique

Résumé : Cette thèse de doctorat porte sur la conception et l'analyse d'algorithmes, relevant du calcul formel, pour la résolution de systèmes polynomiaux. Plus précisément, nous considérons le problème du comptage du nombre de composantes connexes de l'ensemble des solutions réelles de systèmes d'équations polynomiales à variables réelles, ainsi que le problème de décider si deux solutions réelles d'un tel système vivent dans une même composante connexe de son ensemble de solutions réelles. Ces problèmes sont centraux en géométrie algébrique réelle et trouvent des applications en robotique.

Le cadre méthodologique choisi est celui du calcul de *cartes routières*, introduit par Canny en 1988 : il s'agit de calculer une courbe contenue dans l'ensemble des solutions dont l'intersection avec chacune de ses composantes connexes est connexe. Nous décrivons un algorithme calculant de telles cartes routières qui, sous des hypothèses de régularité satisfaites génériquement, a une complexité sous-quadratique en la taille de la sortie, cette dernière étant asymptotiquement quasi optimale. Ceci étend aux cas non compacts les meilleures complexités connues pour ce problème. Nous montrons aussi que le coût du calcul de nombre de composantes connexes d'une courbe algébrique réelle (vivant dans un espace de dimension arbitraire) est similaire au coût du calcul de la topologie de sa projection sur un plan générique. Enfin, nous montrons comment ces avancées, combinées aux algorithmes de la géométrie algébrique réelle permettent de concevoir un algorithme testant la cuspidalité de mécanismes articulés.

Abstract

Title: *Connectivity in real algebraic sets: algorithms and applications*
Keywords: computer algebra, polynomial systems, real algebraic geometry, robotics

Abstract: This PhD thesis focuses on the design and the analysis of computer algebra algorithms for solving polynomial systems. More precisely, we address the problems of counting the number of connected components of sets of real solutions to systems of polynomial equations with real coefficients and of answering connectivity queries over such real solution sets. These problems are central in real algebraic geometry and find applications in robotics.

The chosen framework is the one of *roadmaps*, introduced by Canny in 1988: it consists in computing a curve, included in the solution set under consideration, which has a connected intersection with all its connected components. We design an algorithm which, under some regularity assumptions which are satisfied generically, computes such roadmaps in time subquadratic w.r.t. the output size. This latter quantity is nearly optimal. This extends to non compact situations the best complexity results known for such a computational problem. We also show that the cost to compute the number of connected components of a real algebraic curve (lying in a space of arbitrary dimension) is nearly the same as the one of computing the topology of its projection on a generic plane. Last, by combining these results with algorithms of real algebraic geometry, we design an algorithm to decide the cuspidality of robots.

Remerciements

L'écriture de cette thèse ne fut pas de tout repos, accoucher d'un tel bébé ne se fait pas sans douleur, et celui-ci s'est imposé de lui-même. Il contient ce qu'il devait contenir à mon sens, et de pouvoir maintenant en tirer fierté me donne la satisfaction qui m'était nécessaire. On a finalement peu de telles occasions dans la vie. Bien sûr, l'aboutissement de ce travail n'est individuel qu'en surface, et il me tient à cœur de remercier les personnes qui m'ont construit et qui m'ont permis d'en arriver à écrire ces lignes, après tant de milliers d'autres.

Mes premiers remerciements vont évidemment à Mohab, mon directeur de thèse préféré, sans qui ce document, et le docteur que je suis désormais, n'auraient pas d'existence. Tu m'as permis de m'épanouir scientifiquement mais aussi, personnellement dans une équipe hétéroclite, soudée par d'autres aspects que ceux liés à la recherche. Merci au camarade pour les bières et autres discussions politiques qui m'ont permis d'être moi-même dans mon travail. Merci au Professeur qui m'a poussé jusqu'ici, à l'énergie qu'il m'a accordé, jusqu'à se croiser par mail au milieu de la nuit, et à son dévouement pour combler les dérives du système. Je veux aussi remercier Éric pour sa place non moins importante dans ces quatre dernières années. Merci pour ton accueil !

Je suis aussi reconnaissant aux membres de mon jury de thèse pour leur participation, et en particulier aux rapporteurs pour le temps (que j'imagine conséquent) qu'il et elle ont passé sur mon manuscrit. Aux origines de ma vocation, si elle est, je veux aussi exprimer ma gratitude à ces personnes qui ont posé les jalons de ce parcours. Merci Mme Ducourneau, pour m'avoir encouragé dans mes écrits, merci M. Ibgui de m'avoir donné goût aux maths, et merci M. Cervera pour la rigueur et le goût de la science.

Mes pensées vont aussi à toutes les personnes des équipes PolSys, PEQUAN et MATHEXP que j'ai eu la chance de partager de bons moments à Paris au fil des années : Alin, Andrew, Jérémy, Jocelyn, Hieu, Pierre L., Pierre P., Phuoc, Quentin, Ramtin et Vincent. *I also spent 3 intense months on the other side of the Atlantic, and I am also thinking of Catherine, Josef and Haomin from the Waterloo symbolic computation group, with whom I shared some great discussions and meals. My housemates and friends Subham and Wasim, thank you for those adventurous outings to Niagara Falls and Toronto. Finally, a thought for my climbing (and drinking) mates Arman, Grady, and Roop for those many sessions in Waterloo, and that great trip to boulders at Niagara Falls.*

J'aimerais distinguer certains camarades de thèses avec qui j'ai pu partager des moments particuliers : Dimitri, pour les moments qu'on a passés, d'abord en Master, avant de me rejoindre à PolSys ; Hadrien, pour son accueil chaleureux à l'IHP et nos discussions franches sur le monde de la recherche ; Sriram, pour ce super trip en Norvège, à la lumière continue du jour et des bonbons ; Rafael pour les moult bières et soirées passées ensemble. Finalement, et non des moindres, je veux remercier mes deux comparses, Jorge et Georgy, pour tout ce qu'on a pu vivre ensemble, à Paris comme à Marseille. J'espère que cette amitié restera dans le temps, c'est suffisamment rare à mon sens.

Merci aux camarades de lutte, de Solidaire et d'ailleurs, avec qui on a partagé des moments extraordinaires lors d'action ou d'événements comme ces projections. J'ai nommé Camille, David, Étienne, Lalie, Gomar, Roméo.

Ma vie sans mes amis serait bien tristes et tristement vide, je n'aurais jamais la prétention de pouvoir compter ce que je vous doit, et pour cela merci ! J'espère au moins avoir pu vous en rendre

une partie. Je n'oserai prendre le risque de l'exhaustivité, aussi, je me risquerai simplement à citer celles et ceux qui ont tenu une place importante dans ces quatre années de thèse. Tout d'abord merci à toutes les personnes qui m'ont fait l'insigne honneur d'être présentes à ma soutenance de thèse et/ou aux festivités qui l'ont suivi. Merci pour ces cadeaux et ces attentions qui m'ont profondément marqué. C'est déjà un moment spécial, vous l'avez rendu exceptionnel. Merci à mes ex-collocs de Malakoff Molotov, JB et Johan. Je me souviendrai surtout de ces parties endiablées de Switch et de ces repas de confinement à lutter pour essayer de finir Vikings. Petite pensée pour toi Abou, jumeaux de soutenance, partenaire de soirée. Ces années sont aussi marquées de ces nombreuses séances d'escalade avec toi Justine, entre sport, discussion et bitchage c'est de beaux souvenirs que j'ai là : merci ! Et puisqu'on arrive sur une note plus sportive, je veux dédier ce qu'il se doit à mes partenaires de montagne et autres joyeusetés naturelles : les Strasbourgeois Agathe et Maxime pour leur accueil, et les nombreux périples *eta Eneko euskalduna* pour cette magnifique traversée des Pyrénées (j'aurais aimé que tu sois là pour la finir).

Le tournant de ma vie parisienne a été mon déménagement dans le XVIII^{e} arrondissement et plus précisément à l'artistique 3 rue Lapeyro rempli de voisins incroyables : Estelle, Dominique, Martin, Nathanne et Romain. Une pensée plus émue va aux locataires et locatrices avec qui j'ai pu partager (ou presque) cet appartement : Alix, Louis, Lucie. Merci Alix pour nos discussions, ton expérience et ton soutien jusqu'à la dernière heure où je rédigeais les lignes de ce manuscrit.

Cette thèse sera aussi marquée par des personnes avec qui j'ai partagé de proches moments. Merci Étienne et Thomas, on n'a pas fini d'entendre parler des Petits Pédestre ! Je pense aussi aux voisins du Poteau Chanus et Simon, nos sorties souterraines, les parties endiablées de Codenames. Mais aussi aux ex-Vanvéen·nes Andy et Justine, avec qui j'ai tant partagé surtout pendant les temps troublés du Covid. Cyril, à ces nombreuses bières pour décompresser, souvent pas très bonnes, dans le froid et incontrôlable, mais jamais regrettées. Merci Boudy, pour ces moments, bien trop ponctuels, de fêtes musicales. Je pense aussi à Bertrand, Beberrr comme ils disent, malgré tout, notre amitié et ce qu'on a partagé m'aura construit durablement durant ces dernières années, merci. Finalement, et non des moindres, j'ai nommé Quentin, je pense que tu fais partie des personnes avec qui j'ai le plus partagé, presque toutes catégories confondues. J'attends les prochaines aventures ! C'est inespéré de trouver quelqu'un d'assez bête pour faire ces choses-là avec moi. Par extension, la team du monde à petits pas Johan, Quentin, Sacha : ce qu'on a vécu pendant un an autour du monde nous aura tous et toute forgé·es, et forgé·es ensemble.

Je pense bien sûr aussi à ma famille qui n'a cessé de me m'encourager, la grande famille Vu, mais surtout la petite famille Prébet et son soutien constant, son support dans les moments les plus difficiles, mais aussi dans les meilleurs. Merci Pierre pour ces merveilleux moments en montagne qui m'ont fait respirer et rappelés tout ce qu'elle m'apporte. Merci Papa, merci Maman. Difficile de dire pourquoi tellement la question me paraît ridicule. Cependant, durant ces quatre dernières années, le "retour en arrière" du confinement, les séjours tumultueux à la montagne, les coups de fils épisodiques à rallonge, vous n'avez cessé d'être des fondations solides à ma vie.

Bien sûr, je ne finirai pas sans dédier cette thèse à toi Maëlys qui m'a accompagnée, soutenu, supporté, changé les idées, et fait relativiser les choses aux bons moments. Tu m'as donnée les bouffées d'oxygène qui m'ont permis de respirer ces dernières années, merci mon petit diable de Tasmanie.

Contents

1 Introduction

1.1 Context and motivations

As computer capacities increase, the range of what can be computed progresses everyday further in the realm of mathematics. This paradigm shift has propelled us beyond human limits, as witnessed in the last decade with the computer-aided proofs of the four-hundred-year-old Kepler Conjecture on sphere packing [Lag11, HAB+17] or on Gessel's walks [KKZS09, BK09]. At the intersection of mathematics and computer science, this thesis belongs to the area of *computer algebra*, also known as *symbolic computation*. The methodology adopted in this field can be succinctly summarized as follows:

a) identify the suitable mathematical framework for articulating specific problems arising from practical applications;

b) develop and employ mathematical tools to exhibit the solutions to these problems, with an emphasis on exactness and completeness;

c) combine mathematical insights with techniques from computer science to design algorithms computing well-chosen representations of these solutions;

d) assess the theoretical performances of the algorithms;

e) implement these algorithms within computer algebra systems or using low-level programming languages.

It is important to note that the final step involves the challenge of efficiently representing and computing sophisticated data structures. As a natural extension of this process, researchers in symbolic computation are likely to apply their expertise to address specific instances of the initial problem, coming from diverse application areas.

In contrast with numerical methods, which provide approximate solutions, algorithms in computer algebra are designed to output exact answers, that is satisfying the two distinct requirements:

- *precision*: no loss of information in the computation process;
- *completeness*: a solution is found if and only if it exists.

In particular, it allows to solve decision problems such as deciding the existence of solutions for a problem described by polynomial constraints or the existence of a collision-free trajectory for an object in an ambient space populated with obstacles. Furthermore, these requirements ensure that the algorithms output comprehensive descriptions of the solutions, providing features such as arbitrary precision or convenient manipulation for subsequent computations.

1.1.1 Computational real algebraic geometry

In this thesis, our primary focus is directed towards solving *geometric* problems that are described by *polynomial systems*. These systems arise from various areas of application such as cryptography [KS99, FJ03], signal processing [FdSMR98, GCMT02], etc.. Following the methodology described earlier, the natural mathematical context we explore is *algebraic geometry* whose basic objects are *algebraic sets*, representing solutions in an algebraically closed field $\mathbf{C}$ – such as the complex numbers $\mathbb{C}$ – to systems of polynomial equations of type

$$f_1 = \cdots = f_s = 0,$$

where the f_i's are multivariate polynomials with coefficients in $\mathbf{C}$. Chapter 2 provides an introduction to the main notions of algebraic geometry we will use in this document, to which we refer the reader.

However, our target applications address a more specific problem: the exploration of real solutions within polynomial systems. This problem belongs to the field of mathematics named of *real algebraic geometry* (also known as semi-algebraic geometry), whose basic objects are semi-algebraic sets, that is the solutions within real closed fields $\mathbf{R}$, a generalization of the real numbers $\mathbb{R}$, of finite unions of systems of polynomial equations and inequalities of the type

$$f_1 = \cdots = f_s = 0, \quad g_1 > 0, \ldots, g_r > 0,$$

where the f_i's and the g_j's are multivariate polynomials with coefficients in $\mathbf{R}$. We refer the reader to Chapter 4 for an introduction to real algebraic geometry and the important results associated with semi-algebraic sets and maps between them. Problems involving semi-algebraic sets arise in a wide variety of areas such as robotics [Can88a, CR04, CSS23], biology [FT22, YSCG22], computer vision [FMRS08, GNBS22], stability analysis of differential equations [LS93, WR13, HS12], optimisation [Las01, FRPM06], rigidity [JW18] or program verification [Tiw10, GHMM23]. The strategies developed to solve these applications rely on a combination of fundamental algorithmic problems in real algebraic geometry that stem from the following two important properties that distinguish semi-algebraic sets. Let S be a semi-algebraic set then,

(stability) the projection of S on a coordinate subspace is a semi-algebraic set;

(finiteness) S has finitely many connected components.

Hence, given a semi-algebraic set S, one can naturally ask to:

(A) compute a description of the projection of S on a coordinate subspace;

(B) compute sample points in each connected component of S;

(C) decide if two points lie in the same connected component of S;

(D) count the number of connected component of S.

The analysis of these problems, as well as the design and implementation of algorithms to solve them, constitute the spearhead of *computational real algebraic geometry*.

Remark that given a solution for (B) and (C) one can deduce a solution for (D) as follows: given sample points in each connected component, decide which of these points belong to the same component, and extract a set of unique representatives for these components. The number of these points then equals the number of connected components, an important topological invariant for mathematicians (this is the first Betti number).

When evaluating the performance of the algorithms under investigation, a fundamental measure is their *complexity*, which measures the number of operations with unit cost they perform during their execution. To define asymptotic classes of complexity we use the Big Oh notation as follows. Let f and g be real-valued functions, we say that $f = O(g)$ if the function f/g is defined and bounded for large enough input values. Moreover, as in some situations logarithmic factors can be reasonably ignored, we also use the soft Oh notation: $f = \widetilde{O}(g)$ if $f = O(g \log^a g)$ for some $a > 0$.

A first global approach to solve fundamental problems of computational real algebraic geometry involves the comprehensive computation of the topology inherent to the given input semi-algebraic set, denoted as $S \subset \mathbf{R}^n$, where n assumes a positive integer value. This is tackled by computing a so-called *Cylindrical Algebraic Decomposition* (CAD) adapted to S, using the algorithm introduced by Collins in [Col75]. In essence, a CAD adapted to S is a partition of the ambient space $\mathbf{R}^n$ into finitely many cells, each of which is homeomorphic to an open ball, and such that S is the union of such cells. Nevertheless, on input a semi-algebraic set defined by s polynomials of maximum degree D, the complexity of computing such a decomposition is

$$(sD)^{2^{O(n)}}.$$

This bound is *doubly exponential* in n, the ambient dimension, and polynomial in s and D, which renders this strategy infeasible for applications where the value of n exceeds 4. Moreover, the algorithm of Collins is optimal in the sense that there exists semi-algebraic sets for which any adapted CAD has size doubly exponential in n [DH88, BD07].

Nevertheless, all is not without hope, as the topological complexity of an arbitrary semi-algebraic set cannot exceed $O(snD)^n$ [GV09], that is *singly exponential in* n. This bound, commonly referred to as (Oleinik-Petrovsky-)Thom-Milnor's bound originates from the pioneer respective works [OP49, Ole51, Tho65, Mil64], and is asymptotically tight. Moreover, as mentioned in e.g. [BR18], in computational real algebraic geometry, it is commonly held that computing topological invariants – such as the number of connected components – or deciding topological properties on a semi-algebraic set should be achieved by algorithms with complexity aligned to the mathematical bounds it satisfies.

This motivates the current active research for *dedicated* algorithms addressing *specific* fundamental problems in computational real algebraic geometry with complexity as close as possible to the related mathematical bound. Matching these bounds would then constitute a form of optimum as discussed above, with the first milestone being the *singly exponential* complexity. For instance, the best known algorithm solving the above problem (B) has complexity $s^n D^{O(n)}$, for an input semi-algebraic set defined by s polynomials, in n variables, of maximum degree D. We refer to Chapter 5 for further discussions of these aspects and a historical overview.

In this thesis, we focus on the connectivity queries problem, that is Problem (C). This problem emerged within the context of robotics to address motion planning problems. The pioneering work of addressing this issue was undertaken by Schwartz and Sharir in [SS83c], followed by the influential PhD thesis of Canny [Can88a]. To introduce the aforementioned context, we present in the next subsection the piano mover's problem.

1.1.2 The piano mover's problem

We present here a simplified version of robotics concepts, terminology and notations from [LaV06, Chapter 4], to which we refer for a complete study of the topic – see also [Lat91, Lau98]. We will then see how it boils down to problems in computational real algebraic geometry.

1.1.2.a. The general robotic problem

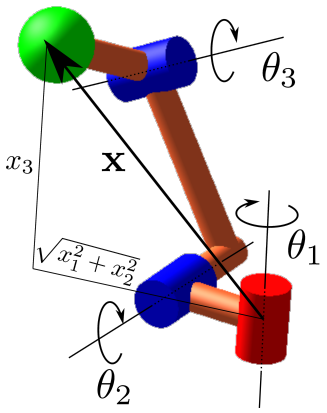
A robot can be modeled as an application $\mathcal{R} : \mathcal{C} \to \mathcal{W}$ that maps a point in the configuration space $\mathcal{C}$ – joint angles, global position and orientation – to a point in the workspace $\mathcal{W}$ – usually the position and orientation of its end-effector. While the workspace is typically $\mathbb{R}^2$ or $\mathbb{R}^3$ and involves a small number of variables, the configuration space can be much more complicated and can involve many more unknowns.

Example 1.1.1.

a) If the robot is reduced to a point in $\mathbb{R}^n$, then $\mathcal{W} = \mathcal{C} = \mathbb{R}^n$ and $\mathcal{R}$ is the identity map as the end-effector is the robot itself.

b) This is not true for a higher dimensional object, as it requires to set its orientation. Considering a three-dimensional object whose end-effector is one of its points, we have $\mathcal{C} = \mathbb{R}^n \times SO(3)$, where $SO(3)$ is the special orthogonal group of 3D rotations, and $\mathcal{W} = \mathbb{R}^3$. Hence, using elementary Euclidean geometry, one can explicitly write $\mathcal{R}$.

c) Similarly, one can consider manipulators, such as the three-revolute joints robotic arms depicted on the opposite figure. Its end-effector is the green ball that is located by its vector of Cartesian coordinates $\boldsymbol{x} = (x_1, x_1, x_3)$. The workspace is then $\mathbb{R}^3$. Its joints are parameterized by the array of the three angles $\boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3)$. Then one can choose for the configuration space either $\mathbb{R}^3$ or the 3-torus $\mathbb{T}^3 = \mathbb{R}^n/(2\pi\mathbb{Z})^n$.
This robot is further studied in Section 9.3 of Chapter 9.



Workspaces are typically populated with obstacles that can either come from the environment – human operator, limited maneuverability, etc. – or the robot itself – joint limits,

self-collision, singular positions, etc.. Then, mechanism designers are willing to identify *collision-free paths* in $\mathcal{C}$ bringing $\mathcal{R}$'s end-effector from one point of $\mathcal{W}$ to a given other.

More precisely, let $\mathcal{O}$ be the closed subset of $\mathcal{W}$ defining the *obstacle region* and let

$$\mathcal{C}_{free} = \{q \in \mathcal{C} \mid \mathcal{R}(q) \notin \mathcal{O}\}$$

be the *free space*. We present below a particular instance of motion planning.

Definition 1.1.2 (Piano Mover's problem)**.** Given $\mathcal{C}, \mathcal{W}, \mathcal{R}, \mathcal{O}$ and $\mathcal{C}_{free}$ as above, on input

1. an initial configuration $q_I \in \mathcal{C}_{free}$;
2. a goal configuration $q_G \in \mathcal{C}_{free}$;

decide the existence of a path $\gamma\colon [0,1] \to \mathcal{C}_{free}$ such that $\gamma(0) = q_I$ and $\gamma(1) = q_G$. Moreover, in case such a path exists, compute it.

As mentioned above, the difficulty of this problem comes from the unbounded dimension of $\mathcal{C}$. An illustration of this problem is given in Figure 1.1.

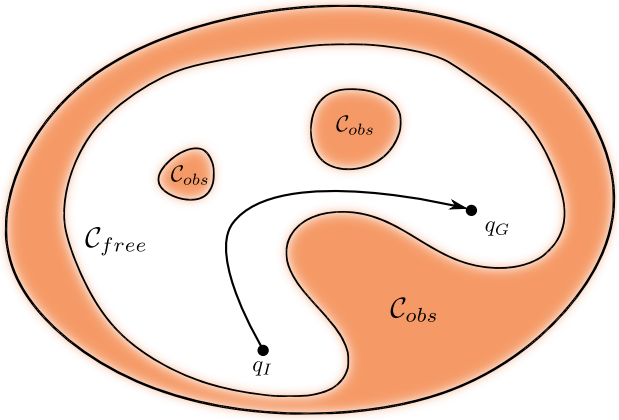


Figure 1.1. An illustration of the piano mover's problem adapted from [LaV06, Fig. 4.11]. Here, $\mathcal{C}_{obs}$ is nothing but the complement of $\mathcal{C}_{free}$ in $\mathcal{C}$, that is $\mathcal{R}^{-1}(\mathcal{O})$, the set of configuration inducing a collision.

According to [LaV06], there are two main methodologies addressing the piano mover's problem: the *sampling based* one and the *combinatorial* one. The first approach avoids the explicit representation of $\mathcal{C}_{free}$ and proceeds by a sampling and interpolation strategy. In essence, it constructs a finite graph of points $\mathcal{C}_{free}$, by iterative local expansion starting, from q_I and q_G [LaV06, §5.4.1]. This reduces the problem of connecting pairs of points in $\mathcal{C}_{free}$, whose relative distance must be smaller than an experimentally chosen parameter Δq [LaV06, §5.3.4]. The choice of the distance in $\mathcal{C}$ is of importance as emphasized in [MPL23] (referring to [LaV06]): "it must capture within the same quantity different degrees of freedom of the system which have different units" (e.g. angles and lengths). For instance, in [MPL23], the authors propose to quantify the distance between two configurations by the minimum volume swept by the robot, over all possible paths between these configurations. Finally, the algorithm makes calls to collision detection subroutines at each point under consideration, to decide which are in $\mathcal{C}_{free}$ – see [LaV06, Section 5.3] for such subroutines.

Although the sampling-based planning methods benefit from *numerical* methods to efficiently provide answers of possibly extreme precision, they cannot achieve the *completeness* criterion that computer algebra algorithms do satisfy. Indeed, for instance, such algorithms cannot certify that no path exists between two configurations, but with limited precision (that still remains to be set). We will see in the next subsection, with the cuspidality decision problem, that this completeness criterion is a requirement that comes for applications as well. Note that weaker versions of completeness can be satisfied by sample-based algorithms, such as the *probabilistic completeness* or the *resolution completeness* [LaV06, p.186].

Hence, to meet the requirements of computer algebra algorithms, we adopt the combinatorial approach, that relies on explicit description of $\mathcal{C}_{free}$ to provide *exact* answers to the piano mover's problem.

1.1.2.b. Real algebraic piano mover's problem

Let $n > 0$ and assume that $\mathcal{C} = \mathbf{R}^n$ for some real closed field $\mathbf{R}$. Then, following the pioneering works of [SS83c] (see also [LaV06, Section 3.1.2]), we assume that the free space $\mathcal{C}_{free}$ can be described using finitely many polynomial equations and inequalities: that is, $\mathcal{C}_{free}$ is a semi-algebraic set of $\mathbf{R}^n$ [1].

We say that two points are semi-algebraically path-connected if they can be connected by a semi-algebraic path, that is a continuous map $\gamma : [0, 1] \to S$ whose graph is a semi-algebraic set of $\mathbb{R}^{n+1}$. We then reformulate the piano mover's problem in real algebraic geometry terms as follows.

Definition 1.1.3 (Connectivity queries in semi-algebraic sets)**.** Let $n \geq 1$, and let S be a semi-algebraic set of $\mathbb{R}^n$. Given two points $\boldsymbol{x}$ and $\boldsymbol{y}$ in S, decide whether $\boldsymbol{x}$ and $\boldsymbol{y}$ can be semi-algebraically path-connected in S and describe such a path when it exists.

While, from the point of view we adopted, this problem clearly finds applications in robotics [Can88a, SS83c, CSS23, Wen07, NS17], it appears also in other areas such as computational geometry [ELLS09] or rigidity problems – see [LSdW20].

Outline of the sequel

We now introduce the thesis' primary *contributions* along two main lines.

The *first section* tackles a challenging robotics problem, relying on efficiently solving the piano mover's problem.

The *second section* offers an overview of the current best known methods for resolving connectivity queries, and introduces our three most significant contributions that extend existing state-of-the-art results

[1] Note that this assumption is not so restrictive since, according to [LaV06, Section 3.1.2]: it is "*sufficient to express any model of interest*". This can be clearly seen considering that most of the robotics problems can be described by Euclidean geometry, and that the cosine and sine of an angle are nothing but the coordinates of a point on a circle.

1.2 An application of computer algebra to robotics

This section relates the contributions developed in Chapter 9. We chose to present this contribution first, as it allows us to introduce, through a *topical application*, the context for the remaining contributions.

We start by introducing the cuspidality decision problem for manipulators, whose resolution constitutes a *first contribution* for this thesis. We show that it boils down to a geometric problem that can be solved using theoretic and algorithmic tools from real algebraic geometry, we introduce succinctly.

1.2.1 Problem statement

Cuspidal robots were discovered at the end of the eighties [PCI88]. A cuspidal robot can move from one of its inverse kinematic solutions to another one without meeting a singular configuration that is, a configuration where it loses degrees of freedom. A major consequence is that determining in which solution the robot operates during motion planning trajectories for cuspidal robots is more challenging than for noncuspidal ones [Wen04]. Knowing whether a robot under design is cuspidal or not is thus of primary importance.

Most existing industrial robots are known to be noncuspidal because they rely on some specific geometric design rules such as their last three joint axes intersecting at a common point [Wen97]. Recently, however, new robots have been proposed that do not follow the aforementioned design rule, which, in turn, could make them cuspidal.[2] Hence, obtaining an algorithm for deciding cuspidality is of first importance in this context of mechanism design.

In the following we employ ourselves to follow the methodology of computer algebra algorithm design we sketched at the very beginning of this document. To emphasize each of these steps we will recall them, where appropriate.

> *"a) identify the suitable mathematical framework for articulating specific problems arising from practical applications;"*

Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ be a sequence of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ and $V = \boldsymbol{V}(\boldsymbol{f}) \subset \mathbb{C}^n$ be the algebraic set it defines (i.e. the set of common complex solutions to the f_i's). We denote by $V_{\mathbb{R}} = V \cap \mathbb{R}^n$ the real trace of V. Let $\mathcal{R} = (r_1, \ldots, r_d)$ be a sequence of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$. By a slight abuse of notation, we still denote by $\mathcal{R}$ the map

$$\mathcal{R} : \boldsymbol{y} \in \mathbb{C}^n \mapsto (r_1(\boldsymbol{y}), \ldots, r_d(\boldsymbol{y})) \in \mathbb{C}^d,$$

and $\mathcal{R}_{|V_{\mathbb{R}}}$ denotes the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. As seen in the previous section, many robots can be represented with such a map $\mathcal{R}$. Indeed, these are polynomial maps that map the configuration of their joints, which are usually lengths and angles, to the position of their end-effector. However, due to the Cartesian parametrization of many problems, robots behave as polynomial maps in the cosines and sines of the angles. Then, replacing the

[2] See e.g. https://achille0.medium.com/why-has-no-one-heard-of-cuspidal-robots-fa2fa60ffe9b

occurrences of $\cos$ and $\sin$ by new variables c and s, and adding $c^2 + s^2 - 1$ to $\boldsymbol{f}$, one gets a formulation as the one previously described.

We denote by $\mathcal{K}(\mathcal{R}, V)$ the union of the set of *critical points* of the restriction of $\mathcal{R}$ to V and the set of *singular points* of V. Roughly speaking, these points are the ones where $\mathcal{R}$ is not locally invertible, that is, the singular configurations of the robot under consideration. We refer to Section 2.5 of Chapter 2 for a precise introduction to these objects.

Following the formalism introduced in [Wen92], we then propose the following formulation of the cuspidality decision problem.

Definition 1.2.1. The map $\mathcal{R}_{|V_{\mathbb{R}}}$ is *cuspidal* if there exist two distinct points $\boldsymbol{y}$ and $\boldsymbol{y}'$ in $V_{\mathbb{R}}$ such that the following holds:

(i) $\mathcal{R}(\boldsymbol{y}) = \mathcal{R}(\boldsymbol{y}')$;

(ii) $\boldsymbol{y}$ and $\boldsymbol{y}'$ are semi-algebraically path connected in $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$.

If two such points $\boldsymbol{y}$ and $\boldsymbol{y}'$ exist, we say that they form a *cuspidal pair* of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. Note that such a pair is not unique in general.

The above definition goes back to some original works in robotics and mechanism design which we present below. The cuspidality decision problem can be then formulated as follows.

Problem I

On input $\boldsymbol{f}$ and $\mathcal{R}$ as above, decide whether $\mathcal{R}_{|V_{\mathbb{R}}}$ is cuspidal.

The formulation of Problem I, shows that cuspidality decision belong naturally to the realm of *computational real algebraic geometry*. Note, in addition, that it can be seen as an infinite version of the piano mover's problem, in the sense that it asks if any pair of distinct points of the infinite set

$$\bigcup_{\boldsymbol{z} \in \mathbb{R}^d} \mathcal{R}^{-1}_{|V_{\mathbb{R}}}(\boldsymbol{z}) \times \mathcal{R}^{-1}_{|V_{\mathbb{R}}}(\boldsymbol{z})$$

are semi-algebraically path-connected in the semi-algebraic set $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ of $\mathbb{R}^n$.

Prior works. Cuspidal robots have been studied mostly for a specific family of robots made with three revolute joints mutually orthogonal [Wen07]. Such robots were shown to be cuspidal if and only if they have at least one cusp point in their workspace [EOW95, SSC+22]. Accordingly, an algorithm can be designed as follows. On input the inverse kinematic polynomial associated with the robot at hand, it counts the number of triple roots of this polynomial. If this number is nonzero, it means that the robot has at least one cusp and is thus cuspidal [Cor05]. We refer to [WC22] for a recent overview of cuspidal robots.

However, for a general robot, no necessary and sufficient condition is known to decide if this robot is cuspidal or not. Thus, no general algorithm has been devised that can decide if a given arbitrary robot is cuspidal or not.

1.2.2 Contribution: a general decision algorithm

We recall first some terminology of commutative algebra and algebraic geometry. In the following, $\boldsymbol{f}$ are polynomials as above and $V = \boldsymbol{V}(\boldsymbol{f}) \subset \mathbf{C}^n$ is the algebraic set defined by $\boldsymbol{f}$. As presented in Section 2.1 of Chapter 2, V can be uniquely decomposed into finitely many *irreducible components*. When all these components have the same dimension d, we say that V is *equidimensional* of dimension d, or d-*equidimensional*. The ideal generated by $\boldsymbol{f}$, denoted $\langle \boldsymbol{f} \rangle$, is said to be radical if, for any $k > 0$, $g^k \in \langle \boldsymbol{f} \rangle$ implies $g \in \langle \boldsymbol{f} \rangle$. Assume now that $\langle \boldsymbol{f} \rangle$ is radical, and $\boldsymbol{V}(\boldsymbol{f})$ is d-equidimensional. The points $\boldsymbol{y} \in V$ at which the Jacobian matrix of $\boldsymbol{f}$ has rank $n - d$ are called *regular* points and the set of those points is denoted by $\mathrm{reg}(V)$. The others are called *singular* points; the set of singular points of V (its singular locus) is denoted by $\mathrm{sing}(V)$ and is an algebraic subset of V. We refer to the Subsection 2.1.5 of Chapter 2 for a more comprehensive introduction to these concepts.

Hence, we say that the assumption $(\mathsf{A}_{\mathrm{cusp}})$ holds, if:

$(\mathsf{A}_{\mathrm{cusp}})$ the ideal $\langle \boldsymbol{f} \rangle$ is radical, $\boldsymbol{V}(\boldsymbol{f})$ is d-equidimensional and $V_{\mathbb{R}} \not\subset \mathrm{sing}(V)$.

The first two parts of this regularity assumption allow one to conveniently describe the critical locus $\mathcal{K}(\mathcal{R}, V)$ by means of minors of the Jacobian matrix $\mathrm{Jac}[\boldsymbol{f}, \mathcal{R}]$. Moreover, the second part ensures that the dimension of the real algebraic set $V_{\mathbb{R}}$ matches the one of V. This can be restated as: the Jacobian matrix $\mathrm{Jac}(\boldsymbol{f})$ has maximal rank $n - d$ in at least one point of $V_{\mathbb{R}}$. Note this assumption can be satisfied using algorithms whose complexities are bounded by the one of our main algorithm – see [Lec03, SYZ21].

Contribution. Together with D. Chablat, M. Safey El Din, D. Salunkhe and P. Wenger, we design in Chapter 9 an algorithm for deciding the cuspidality on input $\boldsymbol{f}$ and $\mathcal{R}$ as above, satisfying the above regularity assumption $(\mathsf{A}_{\mathrm{cusp}})$. Moreover, when the restriction of the map $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal, the algorithm has the ability to output a witness of cuspidality, i.e. a cuspidal pair and an encoding of a semi-algebraic path that connects them in $V_{\mathbb{R}}$ without meeting $\mathcal{K}(\mathcal{R}, V)$.

We also analyze the bit complexity of this algorithm and prove that cuspidality can be decided in time singly exponential in n, polynomial in the maximum degree of the input polynomials, the integer d and quasi-linear in the maximum bit size of the input coefficients. We refer to Section 3.1 of Chapter 3 for definitions and discussions on (bit) complexity and quantitative bounds associated with polynomials. This leads to the following statement.

Contribution to Problem I

Theorem 1.2.2. *Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\mathcal{R} = (r_1, \ldots, r_d)$ be two sequences of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$, let $V = \boldsymbol{V}(\boldsymbol{f})$ and $V_{\mathbb{R}} = V \cap \mathbb{R}^n$. Let D be the maximum degree of these polynomials and let τ be a bound on the bit size of the coefficients of the input polynomials. Then, under assumption $(\mathsf{A}_{\mathrm{cusp}})$, one can decide the cuspidality of the restriction of the map $\mathcal{R}$ to $V_{\mathbb{R}}$ using at most*

$$\widetilde{O}(\tau)\,((s+d)D)^{O(n^2)}$$

bit operations.

In the following, we sketch how such a result has been obtained and refer to Chapter 9 for the full proof and algorithm's description.

1.2.3 Sketch of resolution

We aim to provide in this subsection a pedagogical presentation of the resolution of Problem I. This leads us, along the way, to introduce key results and objects of real algebraic geometry, and its algorithmic counterpart.

According to the "computer algebra procedure" we sketched in the beginning, the next step is to:

> *"b) develop and employ mathematical tools to exhibit the solutions to these problems, with an emphasis on exactness and completeness;"*

To exhibit an algorithmic solution to Problem I, we use a strategy commonly adopted in computational mathematics, that is reducing infinite problems, to finitely many cases. Then, dealing with each of these cases, we deduce a solution for the initial problem. To do so, we apply a semi-algebraic version of Thom's isotopy lemma from [CS92] which allows us to define regions where the fibers of $\mathcal{R}$ are of the same type – more precisely, they are semi-algebraic homeomorphic to each other. We refer to Section 4.4 of Chapter 4 for an introduction to this advanced theorem of real algebraic geometry.

More precisely, let $\mathcal{S}_{\text{val}}(\mathcal{R}, V)$ be the set of *singular values* of the restriction of $\mathcal{R}$ to V, i.e. the image by $\mathcal{R}$ of the set $\mathcal{K}(\mathcal{R}, V)$:

$$\mathcal{S}_{\text{val}}(\mathcal{R}, V) = \mathcal{R}(\mathcal{K}(\mathcal{R}, V)).$$

The restriction of the map $\mathcal{R}$ to V is said to be proper at a point $\boldsymbol{y} \in \mathbb{C}^d$ if there exists a ball $B \subset \mathbb{C}^d$ containing $\boldsymbol{y}$ such that $\mathcal{R}^{-1}(B) \cap V$ is closed and bounded. The restriction of $\mathcal{R}$ to V is said to be proper if it is proper at every point of $\mathbb{C}^d$. We denote by $\mathcal{P}_\infty(\mathcal{R}, V)$ be the set of points of $\mathbb{C}^d$ at which $\mathcal{R}$ is not proper. According to [Jel99, Theorem 3.8] this set is contained in a proper algebraic set of $\mathbb{C}^d$.

Finally, we denote by $\mathcal{A}_{\text{typ}}(\mathcal{R}, V)$ the set of *atypical values* of the restriction of $\mathcal{R}$ to V, that is the union $\mathcal{S}_{\text{val}}(\mathcal{R}, V) \cup \mathcal{P}_\infty(\mathcal{R}, V)$. We also consider $\overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^{Z}$ the Zariski closure in $\mathbb{C}^d$ of $\mathcal{A}_{\text{typ}}(\mathcal{R}, V)$, that is the smallest algebraic set of $\mathbb{C}^d$ containing $\mathcal{A}_{\text{typ}}(\mathcal{R}, V)$.

Then, according to Thom's isotopy Lemma, the following holds. Let C be a connected component of $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^{Z}$, and $\boldsymbol{z}_0 \in C$. Then, there exists a cuspidal pair in

$$\bigcup_{\boldsymbol{z} \in C} \mathcal{R}^{-1}_{|V_{\mathbb{R}}}(\boldsymbol{z}) \times \mathcal{R}^{-1}_{|V_{\mathbb{R}}}(\boldsymbol{z})$$

if and only if there exists one in $\mathcal{R}^{-1}_{|V_{\mathbb{R}}}(\boldsymbol{z}_0) \times \mathcal{R}^{-1}_{|V_{\mathbb{R}}}(\boldsymbol{z}_0)$, which is a finite set by (A_{cusp}). Moreover, as seen above, since $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^{Z}$ is an (open) semi-algebraic set, it has finitely many such connected components C. This leads to the following geometric pseudo-algorithm.

This leads us to the third and fourth steps of the procedure, that is:

> *"c) combine mathematical insights with techniques from computer science to design algorithms computing well-chosen representations of these solutions;"*

Algorithm 1 Cuspidality decision

Input: $\boldsymbol{f}$ and $\mathcal{R}$ as above, satisfying assumption (A_{cusp}).

Output: A decision on the cuspidality of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}} = \boldsymbol{V}(f) \cap \mathbb{R}^n$.

1: compute polynomials $g_1, \ldots, g_p$ whose common zero set is $\overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, \boldsymbol{V}(\boldsymbol{f}))}^{Z}$;

2: compute at least one point $\boldsymbol{z}_i$ in each connected component C_i, of the open semi-algebraic set $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, \boldsymbol{V}(\boldsymbol{f}))}^{Z}$, defined in $\mathbb{R}^d$ by

$$g_1^2 + \cdots + g_p^2 \neq 0.$$

3: **for** $1 \leq i \leq \ell$ **do**

4: **for** $\boldsymbol{y} \neq \boldsymbol{y}' \in \mathcal{R}_{|V_{\mathbb{R}}}^{-1}(\boldsymbol{z}_i)$ **do**

5: **if** $\boldsymbol{y}$ and $\boldsymbol{y}'$ connected in $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, \boldsymbol{V}(\boldsymbol{f}))$ **then**

6: Return `True`

7: Return `False`

and

"d) assess the theoretical performances of the algorithms;".

There are three distinct steps in the above algorithm. In the following, we describe how to perform each of them, using subroutines from computational real algebraic geometry– emphasized in color – and give associated complexity estimates. Recall that, the input consists of polynomials $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\mathcal{R} = (r_1, \ldots, r_d)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ of maximum degree D, and coefficients' bitsize bounded by τ.

The **first step** involves the computation of polynomials defining an algebraic set containing the union of the singular values $\mathcal{S}_{\text{val}}(\mathcal{R}, V)$ and the set of non-properness $\mathcal{P}_{\infty}(\mathcal{R}, V)$. Such computations are tackled by quantifier elimination over the reals, using the algorithm of [BPR06, Theorem 14.22] which we do not detail here, but refer to Section 5.1 of Chapter 5 instead. As there are at most two quantifier alternates, this step can be done using no more than $\tau(sD)^{O(nd)}$ bit operations. The outcome of such step is a sequence of $(sD)^{O(nd)}$ polynomials $\boldsymbol{g} = (g_1, \ldots, g_p) \subset \mathbb{Q}[x_1, \ldots, x_d]$ of degrees bounded by $D^{O(n)}$.

The **second step** involves the computation of sample points in each connected component the semi-algebraic set of $\mathbb{R}^d$ defined by

$$g_1^2 + \cdots + g_p^2 \neq 0.$$

Such a semi-algebraic set is *open* and is often met in the context of robotics, as it represents a set of configurations to avoid, outside which the robot operates. Using the algorithm of best known complexity described in [LS22, Corollary 3], computing these sample points is done using at most $\tau(nd)^{O(nd)}$ bit operations as well. A comprehensive historical overview of algorithms performing such operations can be found in Section 5.2 of Chapter 5.

Finally, the **last step**, consists in considering the finitely many pairs $(\boldsymbol{y}, \boldsymbol{y}')$ of distinct points in $\mathcal{R}_{|V_{\mathbb{R}}}^{-1}(\boldsymbol{z}_i)$ and decide if $\boldsymbol{y}$ and $\boldsymbol{y}'$ are semi-algebraically path-connected in the semi-algebraic set $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$. This clearly belongs to the class of connectivity queries problems, as formulated in Definition 1.1.3. The best known algorithm in this case can be found in [BPR06, Theorem 16.27.c)] and performs at most $\widetilde{O}(\tau)((s+d)D)^{O(n^2)}$ bit operations, which bounds the overall complexity.

We also addressed a proof of concept of the last step of the "computer algebra procedure". More precisely, we set up a prototype implementation of this algorithm in the computer algebra system Maple. We present the results in the last section of Chapter 9.

However, no efficient, ready-to-use, implementation has been written, in particular due to the lack of an efficient and practical algorithm for answering connectivity queries in semi-algebraic sets. Moreover, one sees that in terms of complexity, this step is the bottleneck of the whole algorithm. Hence, the rest of the chapter is devoted to present the contributions made in this thesis to improve the complexity and practicality of connectivity queries algorithm.

1.3 Solving connectivity queries in semi-algebraic sets

In the sequel, for the sake of the generality, we consider a *real field* $\mathbf{Q}$, its *real closure* $\mathbf{R}$ and its algebraic closure $\mathbf{C}$ (one can think of them as $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ without losing much of the intuition). We refer the reader to Section 4.1 of Chapter 4 for an introduction to the theory of real closed fields.

When dealing with semi-algebraic sets, the classic notion of connectedness on $\mathbb{R}^n$ cannot be extended as such for any real closed field $\mathbf{R}^n$. Hence, we say that a semi-algebraic set $S \subset \mathbf{R}^n$ is *semi-algebraically connected* if any two points of S can be connected by a semi-algebraic path lying in S. As mentioned in the beginning, a semi-algebraic set S has finitely many semi-algebraically connected components. These are semi-algebraically connected, both open and closed, semi-algebraic subsets of S, whose disjoint union is S. We refer to Section 4.2 of Chapter 4 for a presentation of these concepts and related results. Note that for $\mathbf{R} = \mathbb{R}$, the notions of classical and semi-algebraic connectedness *coincide* for semi-algebraic sets.

We then reformulate the connectivity queries problem as follows.

Problem II

Let $n \geq 1$, and let S be a semi-algebraic set of $\mathbf{R}^n$ and two points $\boldsymbol{x}$ and $\boldsymbol{y}$ in S.
Decide whether $\boldsymbol{x}$ and $\boldsymbol{y}$ belong to the same semi-algebraically connected component of S.

When its existence is established, the description of a semi-algebraic path connecting the two points will be a consequence of the decision process.

As briefly mentioned in Subsection 1.1.1, Schwartz, Sharir, and others developed in a series of works [SS83a, SS83c, SS83b, SA84, SS84, SSH86] the first exact algorithm for connectivity queries in semi-algebraic sets. This is based on Collins' CAD algorithm [Col75] discussed above, and methods for adjacency determination of cells successively introduced in [ACM84a, ACM84b, ACM85, Arn88]. However, using the CAD algorithm induces the aforementioned prohibitive doubly exponential complexity with respect to the number of variables. This stands in contrast to Thom-Milnor's bound, which calls for *singly exponential* topological complexity. This gap motivated the search for *singly exponential* algorithms. Moreover, as seen in Subsection 1.1.2, for applications in robotics, the dimension of the free

space $\mathcal{C}_{free}$ is much smaller than the one of the ambient space [BPR06, Lat91]. This justifies the motivation to substitute the number of variables with this dimension in the exponents.

To this end, Canny introduced in [Can88a] the concept of *roadmaps* as an alternative to cylindrical algebraic decomposition. Roadmaps are one-dimensional semi-algebraic subsets of a given semi-algebraic set S that are non-empty and semi-algebraically connected within each semi-algebraically connected component of S. This reduces the connectivity problem on semi-algebraic sets of arbitrary dimension to the one of sets of dimension one, which can be solved in polynomial time with respect to the input size – see Subsection 1.3.3.

Then, Canny provided in [Can88a, Can93] the first algorithms for computing roadmaps; we call such algorithms *roadmap algorithms*. Suppose that $S \subset \mathbf{R}^n$ is a semi-algebraic set defined by s polynomials of degree at most D. Canny obtained in [Can88a, Can93] a Monte Carlo roadmap algorithm using $(sD)^{O(n^2)}$ arithmetic operations in $\mathbf{Q}$. A deterministic version is also given, with a runtime $(sD)^{O(n^4)}$. This striking and important result was then reconsidered and improved in [VG90, GR93, HRS94a] (among others) to obtain in [BPR00] a deterministic algorithm using $(sD)^{O(n^2)}$ field operations; this was the state-of-the-art for a decade.

Note that all these algorithms are based on the same following geometric solving pattern. First, a curve, defined as the critical locus of a projection on a plane, is computed; it meets all semi-algebraically connected components of the set under study. Next, connectivity failures are repaired by slicing our set with appropriate hyperplanes and performing recursive calls over these slices.

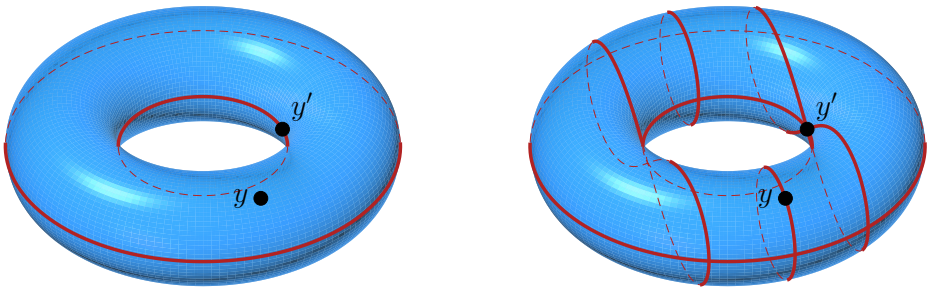


Figure 1.2. Illustration of the two steps of Canny's algorithm on a torus in $\mathbb{R}^3$, with two query points $\boldsymbol{y}$ and $\boldsymbol{y}'$. On the left, the one-dimensional polar variety associated with the projection on the plane below is computed. It intersects the unique connected component, but this intersection is not connected and contains neither $\boldsymbol{y}$ nor $\boldsymbol{y}'$. To repair these failures, we add fibers containing the critical points of a projection on a line and the query points. This gives the figure on the right.

In [SS11], Safey El Din and Schost achieved a significant advancement by generalizing this geometric solving pattern to higher dimensional subsets. They propose subsequently a Monte Carlo roadmap algorithm with complexity exponential in $O(n^{1.5})$, improving upon the initial $O(n^2)$ exponent for the first time. However, this algorithm was designed for *smooth and bounded real algebraic hypersurfaces*. Subsequent work in [BR14, BRSS14] led to further enhancements, ultimately resulting in [SS17] with a Monte Carlo roadmap algorithm for smooth and bounded real algebraic sets. For an input being the real trace of an algebraic

set $V \subset \mathbf{C}^n$, of dimension d, defined by polynomials of maximum degrees D, this algorithm features a complexity of $(nD)^{O(n \log(d))}$.

Problem II.a

The next crucial step in enhancing roadmap algorithms for efficient connectivity queries solving involves relaxing the input assumptions while preserving existing complexity bounds.

Contribution to Problem II.a

Chapters 6 and 7 make partial headway in this regard by eliminating the boundedness assumption. The following two sections delve deeper into these developments.

Remark 1.3.1. Note that relaxing the compactness assumption marks a key milestone in extending roadmap algorithms. Indeed, as seen above, for many applications one needs to deal with semi-algebraic sets defined as the complement of a real hypersurface defined by $f = 0$ where f is a multivariate polynomial. This can be tackled by computing a roadmap for the *unbounded* real algebraic set defined by $tf - 1 = 0$ where t is a new variable.

As we now shift our focus to real algebraic sets, let us introduce a more contemporary definition from [SS11] of roadmaps, which originates from [Can88b, §5].

Definition 1.3.2. Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set and let $\mathcal{P}$ be a *finite* subset of $V \cap \mathbf{R}^n$. For $0 \leq i \leq d$, a *i-roadmap* $\mathscr{R}$ of $(V, \mathcal{P})$ is an *algebraic set* of $\mathbf{C}^n$ having the following properties.

(RM_1) For each semi-algebraically connected component C of $V \cap \mathbf{R}^n$, the set $C \cap \mathscr{R}$ is non-empty and semi-algebraically connected;

(RM_2) $\mathscr{R}$ is contained in V;

(RM_3) $\mathscr{R}$ has dimension at most i;

(RM_4) $\mathscr{R}$ contains $\mathcal{P}$.

The points of $\mathcal{P}$ are called the *query points*. A roadmap is a 1-roadmap.

The connectivity of $V \cap \mathbf{R}^n$ is "captured" by (RM_1) and (RM_2), while property (RM_3) controls the dimension of the roadmap and (RM_4) allows to answer connectivity queries on $\mathcal{P}$. Recent algorithms obtained in [SS11, BR14, BRSS14, SS17] are all based on a connectivity result of [SS11], which makes the boundedness assumption we want to drop. We present it below.

1.3.1 Connectivity results for roadmap algorithms

Let $0 \leq d \leq n$ and $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set and assume that $\mathrm{sing}(V)$ is finite. For $1 \leq i \leq n$, let π_i be the canonical projection,

$$\pi_i \colon (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \longmapsto (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i)$$

For a polynomial map $\varphi\colon \mathbf{C}^n \to \mathbf{C}^m$ a point $\boldsymbol{y} \in V$ is a *critical point* of φ if $\boldsymbol{y} \in \operatorname{reg}(V)$ and the differential of the restriction of φ to V at $\boldsymbol{y}$, denoted by $d_{\boldsymbol{y}}\varphi$, is not surjective, that is

$$d_{\boldsymbol{y}}\varphi(\mathrm{T}_{\boldsymbol{y}}\, V) \subsetneq \mathbf{C}^m,$$

where $\mathrm{T}_{\boldsymbol{y}}\, V$ denotes the tangent space to V at $\boldsymbol{y}$. We will denote by $W^\circ(\varphi, V)$ the set of the critical points of φ on V. A *critical value* is the image of a critical point. We set $K(\varphi, V) = W^\circ(\varphi, V) \cup \operatorname{sing}(V)$. The points of $K(\varphi, V)$ are called the *singular points* of φ on V. We refer to Section 2.5 of Chapter 2 for further details.

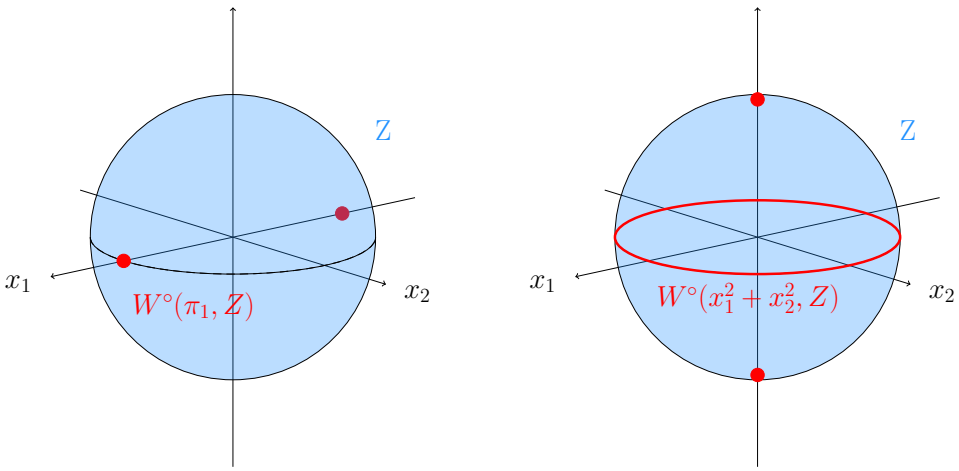


Figure 1.3. Real trace of the critical locus on a sphere Z for: the projection on the first coordinate π_1 (left); the polynomial map φ associated to $x_1^2 + x_2^2 \in \mathbb{R}[x_1, x_2, x_3]$ (right). Let $\boldsymbol{x} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3) \in Z$. The differential of the restriction of π_1 to Z at $\boldsymbol{x}$ is the restriction of π_1 to $\mathrm{T}_{\boldsymbol{x}}\, Z$. The image is not $\mathbf{C}$ if, and only if, $\mathrm{T}_{\boldsymbol{x}}\, Z$ is orthogonal to the x_1-axis, so that critical points of the restriction of π to Z occur at $(\pm 1, 0, 0)$. Besides, the differential of the restriction of φ to Z at $\boldsymbol{x}$ is the restriction of $-2x_3 \cdot \pi_3$ to $\mathrm{T}_{\boldsymbol{x}}\, Z$. Hence, $\boldsymbol{x}$ is a critical point of the restriction of φ to Z if, and only if, either $\boldsymbol{x}_3 = 0$ or $\mathrm{T}_{\boldsymbol{x}}\, Z$ is orthogonal to the x_3-axis.

For $1 \leq i \leq d$, we denote by $W(\pi_i, V)$ the i-th *polar variety* defined as the Zariski closure of the critical locus $W^\circ(\pi_i, V)$ of the restriction of π_i to V. Further, we extend this definition by considering $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n) \subset \mathbf{Q}[x_1, \ldots, x_n]$ and, for $1 \leq i \leq n$, the map

$$\begin{array}{rccc} \boldsymbol{\varphi}_i\colon & \mathbf{C}^n & \longrightarrow & \mathbf{C}^i \\ & \boldsymbol{y} & \mapsto & (\varphi_1(\boldsymbol{y}), \ldots, \varphi_i(\boldsymbol{y})) \end{array}. \tag{1.1}$$

Following [BGHP04, BGHP05, BGH+10] we denote similarly $W(\boldsymbol{\varphi}_i, V)$ the i-th *generalized polar variety* defined as the Zariski closure of the critical locus $W^\circ(\boldsymbol{\varphi}_i, V)$ of the restriction of $\boldsymbol{\varphi}_i$ to V. Polar varieties and their properties are further discussed in Section 2.6 of Chapter 2.

We recall below [SS11, Theorem 14] (see also [BRSS14, Proposition 3.3] for a slight variant of it), making use of polar varieties to establish connectivity statements.

Theorem 1.3.3 ([SS11, Theorem 14]). *For $2 \leq i \leq d$, assume that the following holds:*

- *$V \cap \mathbf{R}^n$ is bounded;*
- *$W(\pi_i, V)$ is either empty or $(i-1)$-equidimensional and smooth outside* $\mathrm{sing}(V)$*;*
- *for any $\boldsymbol{y} \in \mathbf{C}^{i-1}$, $\pi_{i-1}^{-1}(\boldsymbol{y}) \cap V$ is either empty or $(d-i+1)$-equidimensional;*
- *$W(\pi_1, W(\pi_i, V))$ is finite.*

Let $\mathcal{P} \subset V$ be a finite set and

$$K_i = W(\pi_1, W(\pi_i, V)) \cup \mathrm{sing}(V) \cup \mathcal{P} \quad \textit{and} \quad F_i = \pi_{i-1}^{-1}(\pi_{i-1}(K_i)) \cap V.$$

Then, $W(\pi_i, V) \cup F_i$ is a $\widetilde{d}$-roadmap for $(V, \mathcal{P})$, where $\widetilde{d} = \max\{i-1, d-i+1\}$.

For the special case $i = 2$, this result was originally proved by Canny in [Can88a, Can88b]. A variant of it, again assuming $i = 2$, is given for general semi-algebraic sets in [Can93, Can91]. By dropping the restriction $i = 2$, the result in [SS11, Theorem 14] allows more freedom in the choice of i, and then, in the design of roadmap algorithms to obtain a better complexity. The rationale is as follows.

From the above result, one naturally designs a recursive algorithm reducing the problem to algebraic subsets of smaller dimensions, which raises a complexity that is roughly $D^{O(n\rho)}$, where ρ is the depth of recursion and D is the maximum degree of input equations defining V. Restricting to $i = 2$, one expects (up to some linear change of variables or other technical manipulations) a situation where $W(\pi_2, V)$ has dimension at most 1 and F_2 has dimension $d-1$ (see e.g. [SS11, Lemma 31]). Hence, the depth of the recursion is n, which yields a complexity in $(nD)^{O(n^2)}$. In [SS11], using a baby steps/giant steps strategy, it is shown that one can take $i \simeq \sqrt{d}$ and then have a depth of the recursion $\simeq \sqrt{d}$ which results in the complexity bound $(nD)^{O(n\sqrt{n})}$. This algorithm has been generalized in [BRSS14] for general algebraic sets. It has the same complexity but makes use of infinitesimals. Finally, in [SS17], it is shown how to apply [SS11, Theorem 14] with $i \simeq \frac{d}{2}$ so that the depth becomes $\simeq \log_2(d)$ and the complexity $(nD)^{O(n\log_2(d))}$.

Such connectivity results and the algorithms that derive from them are at the foundations of many implementations for answering connectivity queries in real algebraic sets. As far as we know, the first one was reported in [MS06], showing that, at that time, basic computer algebra tools were mature enough to implement rather easily roadmap algorithms. More recently, practical results were reported on applications of roadmap algorithms to kinematic singularity analysis in [CSS20, CSS23], showing the interest in developing roadmap algorithms beyond applications to motion planning. In parallel, the interest in roadmap algorithms keeps growing as they have also been adapted to the numerical side [HMP00, BDRH+13, IC14, BBH+17, CWF20]. This illustrates the interest in improving roadmap algorithms and the connectivity results they rely on.

Dropping the boundedness assumption in this scheme was done in [BR14, BRSS14] using infinitesimal deformation techniques. The algorithms proposed use respectively $(nD)^{O(n\sqrt{n})}$ and $(nD)^{O(n\log^2(n))}$ arithmetic operations in $\mathbf{Q}$. However, the use of infinitesimals induces a growth of intermediate data. The algorithm in [BR14] is not polynomial in its output size, which is $(nD)^{O(n\log(n))}$. In non-bounded cases, one could also study the intersection of V

with either $[-c,c]^n$ or a ball of radius c, for c large enough, but we would then have to deal with semi-algebraic sets instead of real algebraic sets, in which case [SS11, Theorem 14] is still not sufficient.

Problem II.a.(i)

The first step towards an algorithm dealing with unbounded smooth real algebraic sets with a complexity similar to that of [SS17], is to *obtain a new connectivity statement* with no boundedness assumption and the same freedom brought by the one of [SS11].

Contribution: a generalized connectivity result

Together with M. Safey El Din and É. Schost, we answered Problem II.a.(i) by generalizing Theorem 1.3.3 to unbounded cases. Hereafter, we state this result, and we refer to Chapter 6 for the complete proof.

Let $V \subset \mathbf{C}^n$ be an algebraic set defined over $\mathbf{Q}$ and $d > 0$ be an integer. We say that V satisfies assumption (A) when

(A) V is d-equidimensional and its singular locus $\mathrm{sing}(V)$ is finite.

For $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n) \subset \mathbf{Q}[x_1, \ldots, x_n]$, we say that $\boldsymbol{\varphi}$ satisfies assumption (P) when

(P) the restriction of the map $\boldsymbol{\varphi}_1$ to $V \cap \mathbf{R}^n$ is proper and bounded from below.

For instance, choosing arbitrary a point, then the map $\boldsymbol{\varphi}_1$ defined as the squared Euclidean distance to this point, naturally satisfies condition (P).

We denote by $W_i = W(\boldsymbol{\varphi}_i, V)$ the Zariski closure of the set of critical points of the restriction of $\boldsymbol{\varphi}_i$ to V. For $2 \leq i \leq d$ and $\boldsymbol{\varphi}$ as above, we say that $(\boldsymbol{\varphi}, i)$ satisfies assumption (B) when

(B_1) W_i is either empty or $(i-1)$-equidimensional and $\mathrm{sing}(W_i) \subset \mathrm{sing}(V)$;

(B_2) for any $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i) \in \mathbf{C}^i$, $V \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{y})$ is either empty or $(d-i+1)$-equidimensional.

Note that when B_1 holds, $\mathrm{sing}(W_i)$ and the critical loci of polynomial maps restricted to W_i are well-defined. For S_i a finite subset of V, we say that S_i satisfies assumption (C) when

(C_1) S_i is finite;

(C_2) S_i has a non-empty intersection with every semi-algebraically connected component of $W(\boldsymbol{\varphi}_1, W_i) \cap \mathbf{R}^n$.

Finally, similarly to Theorem 1.3.3, for $\mathcal{P} \subset V$ finite, we let

$$K_i = W(\boldsymbol{\varphi}_1, V) \cup S_i \cup \mathrm{sing}(V) \cup \mathcal{P} \qquad \text{and} \qquad F_i = \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(K_i)) \cap V.$$

Contribution to Problem II.a.(i)

Theorem 1.3.4. *Let V, d, i in $\{1, \ldots, d\}$, $\boldsymbol{\varphi}$ and S_i as above, and assume that assumptions (A), (B), (C) and (P) hold.*
Then the algebraic set $W_i \cup F_i$ is a is a $\widetilde{d}$-roadmap for $(V, \mathcal{P})$, where $\widetilde{d} = \max\{i-1, d-i+1\}$.

Comparing with the formulation in Theorem 1.3.3, the above theorem directly generalizes [SS11, Theorem 14] by relaxing the boundedness assumption. Moreover, as in [BRSS14, Proposition 3.3], it does not require $W(\varphi_1, W_i)$ to be finite, but only to have in hand at least one point in each of its semi-algebraically connected components.

1.3.2 Roadmap algorithm

Recall that the best known complexity is reached by the algorithm of [SS17], which runs in time $(nD)^{O(n \log d)}$, where d is the dimension of the input algebraic set, which is assumed to be smooth *and bounded*. Moreover, explicit constants in the big Oh exponent are given, showing that the algorithm runs in time subquadratic in the degree bound of the output. As mentioned earlier, removing these assumptions using techniques from [Can95, BPR00, BR14, BRSS14] would require the introduction of possibly several infinitesimals, resulting in increased intermediate data size and, in particular, the loss of the subquadratic behavior.

For this reason, we have extended the connectivity result underlying the algorithm in [SS17] to generalize it to unbounded cases without any prior infinitesimal deformation.

Problem II.a.(ii)

This now leaves the problem of putting this new connectivity result into practice, and design a roadmap algorithm for smooth real algebraic sets with output size and arithmetic complexity similar to the ones in [SS17], but without using the boundedness assumption.

Contribution: genericity results

Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set, with $\mathrm{sing}(V)$ finite. Our goal is to design an algorithm computing a roadmap for V using the new connectivity result in Theorem 1.3.4. To achieve this, we first need to satisfy the assumptions of this theorem, namely (A), (B), (C), and (P). For simplicity, we will omit discussion of query points in this paragraph.

While (A) holds by assumption, taking, for any $\boldsymbol{\alpha}_1 = (\alpha_{1,1}, \ldots, \alpha_{1,n}) \in \mathbf{R}^n$,

$$\varphi_1(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2 + \alpha_{1,i} x_i \tag{1.2}$$

allows to satisfy (P), as its restriction to $\mathbf{R}^n$ is a proper map, bounded from below by $-\sum_{i=1}^n \alpha_{1,i}^2/4$. Besides, a set S_i satisfying assumption (C) can be computed using sample point algorithms that we presented in Section 1.2 for the resolution of the cuspidality problem, and of which an extensive study can be found in Section 5.2 of Chapter 5.

Finally, (B) is a regularity assumption on the generalized i-th polar variety associated with a polynomial map φ, and its fibers. It corresponds to the generalization of the second and third assumptions of Theorem 1.3.3, which are satisfied in [SS17] using a random linear change of variables on V. This leads to the use of the notion of genericity that we review below.

Genericity. In the following, we use the notion of genericity, that will be a key ingredient for some contributions of this thesis. Roughly speaking, a property that depends on a vector

of values of parameters $\boldsymbol{\lambda} \in \mathbf{C}^m$ for some $m \geq 1$, is said to be *generically true*, if there exists a *non-zero* polynomial $G \in \mathbf{C}[x_1, \ldots, x_m]$ such that if $G(\boldsymbol{\lambda}) \neq 0$, this property holds. The set $\mathbf{C}^m - \boldsymbol{V}(G)$ is called non-empty Zariski open set[3], and the λ's such that $G(\boldsymbol{\lambda}) \neq 0$ are called *generic*. These notions are discussed extensively in Section 2.4 of Chapter 2.

More precisely, in [SS17, Propositions 3.4, 3.5 & 3.7], the authors prove that, by performing a generic linear change of variables on V, the last three assumptions of Theorem 1.3.3 are satisfied. However, as we work with general polynomial maps instead of linear projections, we cannot rely on the genericity results of [SS17]. Moreover, performing such changes of variables would make us lose the structure of $\boldsymbol{\varphi}_1$ chosen in (1.2). Instead, we propose to set $\boldsymbol{\varphi}$ as follows.

Contribution to Problem II.a

For $2 \leq j \leq n$, let $\boldsymbol{\alpha}_j = (\alpha_{j,1}, \ldots, \alpha_{j,n}) \in \mathbf{C}^n$ and

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \sum_{k=1}^{n} x_i^2 + \alpha_{1,k} x_k \quad \text{and} \quad \varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \sum_{k=1}^{n} \alpha_{j,k} x_k, \tag{1.3}$$

and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n)$. Then, we prove in the Sections 7.6 and 7.7 of Chapter 7, for a generic choice of $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n) \in \mathbf{C}^{n^2}$, then for any $1 \leq i \leq d+1$, $(\boldsymbol{\varphi}, i)$ satisfies assumption (B) – that is Propositions 7.2.13 and 7.2.16.

It is worth mentioning, that we also prove in Section 7.5 that for a generic $\boldsymbol{\alpha} \in \mathbf{C}^{n^2}$, the restriction to $W(\boldsymbol{\varphi}_i, V)$ of $\boldsymbol{\varphi}_{i-1}$ is finite – that is Proposition 7.2.3 – generalizing the Noether position obtained in [SS03a, Proposition 2] – see also Theorem 2.6.3. We refer to Subsection 2.3.4 for an introduction to finite maps and Noether position, and to Section 2.6 of Chapter 2 for an extensive overview of generic polar varieties and their properties.

Therefore, selecting a random vector of parameter's values $\boldsymbol{\alpha} \in \mathbf{C}^{n^2}$, and taking $\boldsymbol{\varphi}$ as in (1.3), according to the above discussion, one satisfies the assumptions of Theorem 1.3.4 with high probability – see Subsection 2.4.3 of Chapter 2. This is where the first elements of randomization are needed. A second element comes from the use of a variant of [SS17], which is also a Monte Carlo algorithm.

Contribution: a new roadmap algorithm

Proving and using the aforementioned genericity results, with M. Safey El Din and É. Schost, we made effective the generalized connectivity result presented above by designing a Monte Carlo roadmap algorithm for smooth, potentially unbounded algebraic sets, which exhibits similar performance to that of [SS17]. The full development of these results can be found in Chapter 7.

More precisely, on input a sequence of polynomials of maximum degree D that defines a smooth algebraic set V and query points $\mathcal{P}$ in V, our algorithm computes a roadmap for $(V, \mathcal{P})$. Moreover, the output size and running times of our algorithm are both polynomial in $(nD)^{n \log d}$ where d is the dimension of V. As far as we know, the best previously known

[3]The algebraic sets form the closed set of the so-called Zariski topology, so that $\mathbf{C}^m - \boldsymbol{V}(G)$ is open in this topology.

algorithm dealing with such sets is the one of [BR14], and has an output size and running time polynomial in $(nD)^{n \log^2 n}$.

Let φ be a generic polynomial map as in (1.3). Following the discussion held in the previous subsection, a natural design for our new roadmap algorithm would be to follow the balanced recursive structure adopted in [SS17], computing recursively generalized polar varieties and fibers associated with φ, using Theorem 1.3.4. However, as φ_1 is proper and bounded below on $\mathbf{R}^n$, its fibers are bounded algebraic sets. Our algorithm works as follows:

- compute the second generalized polar variety $W_2 = W(\varphi_2, V)$, which is a curve by (B_1);
- next, use a variant of the algorithm in [SS17], to compute a roadmap $\mathscr{R}_{F_2}$ of the bounded algebraic set
$$F_2 = \bigcup_{i=1}^{\ell} V \cap \varphi_1^{-1}(v_i)$$
for some $v_1, \ldots, v_\ell$ in $\mathbf{R}$, that are the points of $\varphi_1(K_1) \cap \mathbf{R}$, reusing the notations of Theorem 1.3.4. This algebraic set has dimension $\dim(V) - 1$ by assumption (B_2).

This scheme, depicted in Figure 1.4, reduces the problem to the bounded case without introducing any infinitesimals. It involves splitting the roadmap into a one-dimensional unbounded component and a lower-dimensional bounded one.

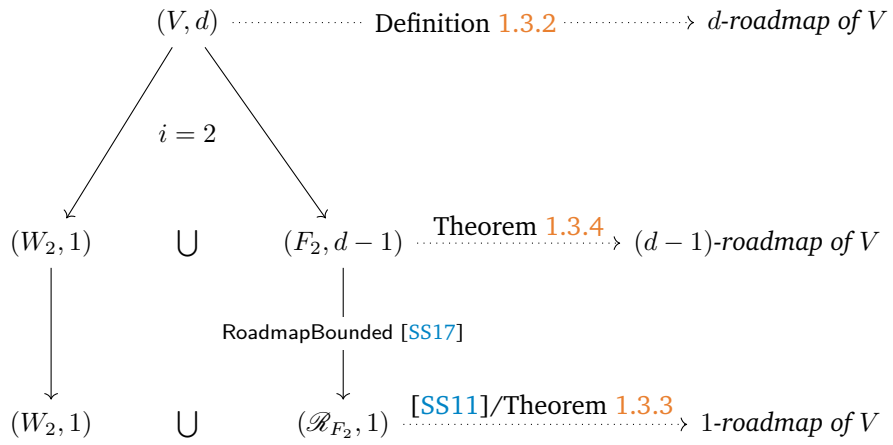


Figure 1.4. Structure diagram of the algorithm presented in Chapter 7, as outlined above, reusing the same notations. The three rows represent the primary steps. On the left, pairs indicate the computed objects at each step along with their associated dimensions. On the right, we give the roadmap definition that is satisfied by the union of the objects on the same row, according to the right connectivity result. Finally, RoadmapBounded refers to the algorithm from [SS17] that computes roadmaps of smooth bounded algebraic sets.

Data structures

Before presenting our main algorithm, we need to introduce the adapted data structures we use to efficiently encode and manipulate the inputs and outputs. For a more detailed introduction and discussions about these structures, we refer to Chapter 3. The natural input of our roadmap algorithm is the data of a *sequence of polynomials* defining a real algebraic set and finitely many *real algebraic query points* in this set. We assume that the input polynomials have coefficients in a computable field $\mathbf{Q}$ of characteristic zero – typically $\mathbf{Q} = \mathbb{Q}$.

Straight-line programs. Polynomials given as input will be represented as *straight-line programs*, which is a flexible way of representing multivariate polynomials as a division and loop-free sequence of operations. Formally, a straight-line program Γ, computing polynomials in $\mathbf{Q}[x_1, \ldots, x_n]$, is a finite sequence $\Gamma = (\gamma_1, \ldots, \gamma_E)$ such that for all $1 \leq i \leq E$, one of the two following statements holds:

- $\gamma_i = \lambda_i$ with $\lambda_i \in \mathbf{Q}$;
- $\gamma_i = (\mathsf{op}_i, a_i, b_i)$ with $\mathsf{op}_i \in \{+, -, \times\}$ and $-n + 1 \leq a_i, b_i < i$.

To Γ we associate polynomials $G_{-n+1}, \ldots, G_E$ such that $G_i = x_{i+n}$ for $-n + 1 \leq i \leq 0$, and for $1 \leq i \leq E$:

- if $\gamma_i = \lambda_i \in \mathbf{Q}$ then $G_i = \lambda_i$;
- if $\gamma_i = (\mathsf{op}_i, a_i, b_i)$ then $G_i = G_{a_i}\ \mathsf{op}_i\ G_{b_i}$.

Then we say that Γ computes some polynomials $f_1, \ldots, f_c$ in $\mathbf{Q}[\boldsymbol{X}]$ if $\{f_1, \ldots, f_c\} \subset \{G_{-n+1}, \ldots, G_E\}$. The integer E is the *length* of the straight-line program Γ. By convention, we note $\Gamma^0 = (0)$ the straight-line program of length 1 that computes the zero polynomial.

Because of the good behavior of such a representation with respect to linear changes of variables, it is used as input in many algorithms for solving polynomial systems [Kri02, GHM+98, GHMP97, GHMP95, GLS01, Lec00]. It is not restrictive since any polynomial of degree D in n variables, can be computed with a straight-line program of length $O(D^n)$ by simply evaluating and summing all its monomials. For more details on straight-line programs and a discussion on the different polynomial representations, see Section 3.2 in Chapter 3.

While the coefficients of the input polynomials can be finitely represented as such, this is not the case for the input query points, that have real algebraic coefficients.

Zero-dimensional parametrizations. To encode finite sets of points with algebraic coordinates over a field $\mathbf{Q}$, we use *zero-dimensional parametrizations*. A zero-dimensional parametrization $\mathscr{P}$ with coefficients in $\mathbf{Q}$ consists of:

- polynomials $(\omega, \rho_1, \ldots, \rho_n)$ in $\mathbf{Q}[u]$ where u is a new variable, ω is a monic square-free polynomial and it holds that $\deg(\rho_i) < \deg(w)$,
- a linear form $\mathfrak{l}$ in variables $x_1, \ldots, x_n$,

such that

$$\mathfrak{l}(\rho_1, \ldots, \rho_n) = u\frac{\partial \omega}{\partial u} \mod \omega.$$

Such a data structure encodes the finite set of points, denoted by $\mathsf{Z}(\mathscr{P})$, defined as follows

$$\mathsf{Z}(\mathscr{P}) = \left\{ \left(\frac{\rho_1}{\partial\omega/\partial u}(\vartheta), \ldots, \frac{\rho_n}{\partial\omega/\partial u}(\vartheta) \right) \in \mathbf{C}^n \mid \omega(\vartheta) = 0 \right\}.$$

According to this definition, the roots of ω are exactly the values taken by $\mathfrak{l}$ on $\mathsf{Z}(\mathscr{P})$. We define the *degree* of such a parametrization $\mathscr{P}$ as the degree of the polynomial ω, which is exactly the cardinality of $\mathsf{Z}(\mathscr{P})$. By convention, we note $\mathscr{P}_\emptyset = (1)$ the zero-dimensional parametrization that encodes the empty set.

As the output of a roadmap algorithm is an algebraic curve, that is an equidimensional algebraic set of dimension 1, we need compact and flexible encoding for such objects.

One-dimensional parametrizations. To encode algebraic curves defined over $\mathbf{Q}$ we use *one-dimensional (rational) parametrizations*. A one-dimensional rational parametrization $\mathscr{R}$ with coefficients in $\mathbf{Q}$ is a pair as follows:

- polynomials $(\omega, \rho_1, \ldots, \rho_n)$ in $\mathbf{Q}[u, v]$ where u and v are new variables, ω is a square-free polynomial, that is monic in u and v, and such that $\deg(\rho_i) < \deg(w)$,

- linear forms $(\mathfrak{l}, \mathfrak{l}')$ in the variables $x_1, \ldots, x_n$,

such that

$$\mathfrak{l}(\rho_1, \ldots, \rho_n) = u\frac{\partial \omega}{\partial u} \mod \omega$$

and

$$\mathfrak{l}'(\rho_1, \ldots, \rho_n) = v\frac{\partial \omega}{\partial u} \mod \omega.$$

Such a data structure encodes the algebraic curve, denoted by $\mathsf{Z}(\mathscr{R})$, defined as the Zariski closure of the following constructible set

$$\left\{ \left(\frac{\rho_1}{\partial\omega/\partial u}(\vartheta, \eta), \ldots, \frac{\rho_n}{\partial\omega/\partial u}(\vartheta, \eta) \right) \in \mathbf{C}^n \mid \omega(\vartheta, \eta) = 0, \frac{\partial\omega}{\partial u}(\vartheta, \eta) \neq 0 \right\}.$$

We define the *degree* of such a parametrization $\mathscr{R}$ as the degree of ω. It is the maximum of the cardinalities of the finite sets obtained by intersecting $\mathsf{Z}(\mathscr{R})$ with a hyperplane, hence the degree of the curve $\mathsf{Z}(\mathscr{R})$. Note that such a parametrization $\mathscr{R}$ of degree δ involves $O(n\delta^2)$ coefficients.

Main result. We say that $(f_1, \ldots, f_c) \subset \mathbf{Q}[\boldsymbol{X}]$ is a *reduced regular sequence* if for every $i \in \{1, \ldots, c\}$, the ideal $\langle f_1, \ldots, f_i \rangle$ is radical and the algebraic set $\boldsymbol{V}(f_1, \ldots, f_i) \subset \mathbf{C}^n$ is either empty or $(n - i)$-equidimensional.

Contribution to Problem II.a.(ii)

Theorem 1.3.5. *Let $\boldsymbol{f} = (f_1, \ldots, f_c)$ be a reduced regular sequence in $\mathbf{Q}[x_1, \ldots, x_n]$, let D be bounding the degrees of the f_i's and suppose that Γ is a straight-line program of length E evaluating $\boldsymbol{f}$. Assume that $\boldsymbol{V}(\boldsymbol{f}) \subset \mathbf{C}^n$ has finitely many singular points.*

Let $\mathscr{P}$ be a zero-dimensional parametrization of degree μ with $\mathsf{Z}(\mathscr{P}) \subset V(\boldsymbol{f})$. There exists a Monte Carlo algorithm which, on input Γ and $\mathscr{P}$ computes a one-dimensional parametrization $\mathscr{R}$ of a roadmap of $(\boldsymbol{V}(\boldsymbol{f}), \mathsf{Z}(\mathscr{P}))$ of degree

$$\mathscr{B} = \mu\, n^{4d\log_2(d)+O(d)}\, D^{2n\log_2(d)+O(n)} = \mu(nD)^{O(n\log_2(d))},$$

where $d = n - c$, using $E\mathscr{B}^3$ arithmetic operations in $\mathbf{Q}$.

Therefore, we dropped the boundedness assumption on $\boldsymbol{V}(\boldsymbol{f}) \cap \mathbf{R}^n$ from [SS17, Theorem 1.1], maintaining a complexity similar to that algorithm. It is worth noting that the above arithmetic complexity is cubic in the *degree* bound $\mathscr{B}$ on the output; the output *size* itself is $O\left(n\mathscr{B}^2\right)$ elements in $\mathbf{Q}$. Hence, as in [SS17], our runtime is subquadratic in the bound on the output size.

In fact, the bound obtained in Theorem 7.1.1 of Chapter 7 is more precise than the one given above, and as in [SS17, Theorem 1], it makes completely explicit the exponent.

The output degree of the above algorithm is bounded by

$$\mathscr{B}' = \widetilde{O}\left(\mu 16^{3d}(n\log_2(n))^{4(d-1+6\log_2(d-1))(\log_2(d-1)+6)} D^{2(n+2)(\log_2(d-1)+4)}\right).$$

and the arithmetic complexity is at most

$$\widetilde{O}\left(\mu^3 16^{9d} E(n\log_2(n))^{12(d+6\log_2(d-1))(\log_2(d-1)+7)} D^{6(n+2)(\log_2(d-1)+5)}\right).$$

Remark that the latter bound can also be written in terms of $\mathscr{B}'$ as:

$$\widetilde{O}\left(E(n\log_2(n))^{12(d+7\log_2(d-1)+1)} D^{6(n+2)} \mathscr{B}'^3\right)$$

We expect that algorithmic progress on the computation of roadmaps for real algebraic and semi-algebraic sets will lead to implementations that will automate the analysis of kinematic singularities e.g. serial and parallel manipulators. In particular, there are many families of robots where these algorithms could be used if they scale enough. This is the case e.g. of 6R manipulators (see e.g. the results on the number of aspects in [Wen07] which need to be extended) in the context of serial manipulators, for the study of self-motion spaces of parallel platforms such as Gough-Stewart ones (the case of such manipulators with 6 lengths still remains open, see e.g. [NS17]) and for the identification of cuspidal manipulators presented above. As mentioned earlier, relaxing the boundedness assumption is a crucial step for these applications. Indeed, many of them involve open semi-algebraic sets, which can be readily reduced to unbounded algebraic sets.

1.3.3 Solving connectivity queries on curves

In the previous subsection, we discussed the reduction of connectivity queries from arbitrary dimensions, to such ones on one-dimensional semi-algebraic sets, in the original space, using roadmaps. This emphasizes the importance of efficiently solving the one-dimensional case. However, there is a lack of algorithms in the literature that are both general and have favorable complexity bounds for this problem. Indeed, the polynomial complexity class, in terms of the input curve's degree, is too coarse for our study as the natural input for these algorithms will be roadmaps with degrees exponential in the number of variables.

Problem II.b

In Chapter 8, we address the problem of designing an algorithm for answering connectivity queries on real algebraic curves in $\mathbb{R}^n$, defined as real traces of algebraic curves of $\mathbb{C}^n$. More precisely, given representations of an algebraic curve $\mathscr{C}$ and a finite set $\mathcal{P}$ of points of $\mathscr{C}$, we want to compute a partition of $\mathcal{P}$, grouping the points lying in the same semi-algebraically connected components of $\mathscr{C} \cap \mathbb{R}^n$, and count the number of such components.

Magnitude. We say that $f \in \mathbb{Z}[x_1, \ldots, x_n]$ has magnitude (δ, τ), if the total degree of f is bounded by δ and all coefficients have absolute values at most 2^τ. This extends to a sequence of polynomials by bounding all entries in the same way. Complexity results are expressed with (δ, τ) bounding the magnitude of the polynomials defining $\mathscr{C}$.

Prior works. The problem of answering connectivity queries on a real algebraic curve has been tackled only through the computation of a piecewise linear approximation sharing the same topology as the curve under study. We succinctly present hereafter the existing approaches and best known results and refer to Subsection 5.3.3 of Chapter 5 for more comprehensive statements.

Computing the topology of plane algebraic curves in $\mathbb{R}^2$ is extensively studied: by subdivision algorithm [BCGY08, LMP08], variants of Cylindrical Algebraic Decomposition methods [BEKS13, CLP+10, DDR+22, Dia09, DRR14, EKW07, GE96, KS15, KS12, MSW15, SW05, DET07, DET09], or also a hybrid approach such as [AMW08]. In particular, [KS15, DDR+22] obtain the best known complexity bound in $\widetilde{O}(\delta^5(\delta+\tau))$, by computing quantitative bounds on (bivariate) real root isolation of the considered polynomials.

The problem in $\mathbb{R}^3$ has been less studied. This is done through various approaches such as computing the topology of the projection on various planes [AS05, GLMT05, CJL13] or lifting the plane projection by algebraic considerations [El 08, DMR08, DMR12]. Yet, few of these papers give a complexity bound for the computation of such topology [CJL13, DMR12], and [JC21] obtains the best known complexity in $\widetilde{O}(\delta^{19}(\delta+\tau))$.

For the general case of real algebraic curves in $\mathbb{R}^n$ the sole known method relies on a variation of the CAD algorithm, drawing from the concepts established in [SS83c]. While the complexity bounds of this algorithm might raise concerns due to their potentially prohibitive nature, in the special case we consider, this approach exhibits a polynomial complexity in the degree δ of the input curve. More comprehensive details on this method can be found in [SS11, p.6], where it is primarily constructed upon the CAD algorithm outlined in [Col75], the adjacency relation methods presented in [SS83c], and Puiseux expansion computations as discussed in works like [Duv89].

However, the aforementioned CAD-based algorithm does not explicitly provide the constant factor in the exponent. And as observed in the cases of $\mathbb{R}^2$ and $\mathbb{R}^3$, this constant could be quite large, which explains the lack of efficient implementation for the general case. However, it is important to note that all the algorithms discussed in this context compute the comprehensive topology of the input curve, requiring the output to be isotopy equivalent to the input. Yet, for connectivity issues, it suffices for the output to share the same connectivity properties. Relaxing the assumptions on the output, we develop in Chapter 8, an algorithm that addresses this problem while maintaining the same complexity bounds as in the planar case. The rest of this section is devoted to presenting this contribution.

Contribution: efficient algorithm for connectivity queries on real algebraic curves

Together with Md N. Islam and A. Poteaux, we designed an algorithm that answers Problem II.b, by counting the number of connected components of the real curve under study, and decides which query point lies in which connected component, in time quasi-linear in N^6, where N is the maximum of the degrees and coefficient bit-sizes of the polynomials given as input. This matches the currently best known bound for computing the topology of real plane curves. The main novelty of this algorithm is the avoidance of the computation of the comprehensive topology of the curve.

Genericity assumptions. This algorithm relies on specific genericity assumptions for the input curve, of which we describe the main ones below.

> These assumptions, along with other technical conditions, are proven to be satisfied through a prior generic change of variables, in Section 8.2 of Chapter 8. This is done by extending well-known results from algebraic geometry on the dimension on secant varieties, to affine singular curves in an ambient space of arbitrary dimension. In particular, generic linear changes of variables in the affine space are translated to the projective setting through projections onto linear spaces within a non-empty Zariski open subset of Grassmanian varieties.

The connectivity analysis of the input curve is greatly simplified thanks to these assumptions. Roughly speaking, they allow to reduce the study to its plane projection along with a finite number of points in this plane called apparent singularities, which need to be identified. These apparent singularities correspond to the points that overlap when projecting on a plane. In particular, the local connectivity "above" the apparent singularities – i.e. in the fiber of their plane projection – will be straightforward.

Sketch of the algorithm. Let $\mathscr{C} \subset \mathbb{C}^n$ be an algebraic curve defined by polynomials in $\mathbb{Q}[\boldsymbol{X}]$ and $\mathcal{P} \subset \mathrm{reg}(\mathscr{C})$ be finite. For all $\boldsymbol{x} \in \mathrm{reg}(\mathscr{C})$, $\mathrm{T}_{\boldsymbol{x}}\mathscr{C}$ is the right-kernel of $\mathrm{Jac}(\boldsymbol{f})$: it is the tangent line of $\mathscr{C}$ at $\boldsymbol{x}$. For $1 \leq i \leq n$ we let $\pi_i : \mathbb{C}^n \to \mathbb{C}^i$ be the canonical projection on the first i variables. *In the following*, we outline our algorithm – that is also depicted in Figure 1.5 – while introducing the key illustrative genericity assumptions (which can be recovered through generic linear changes of coordinates). For a detailed list, we refer to Chapter 8. For the sake of simplicity, we do not consider query points.

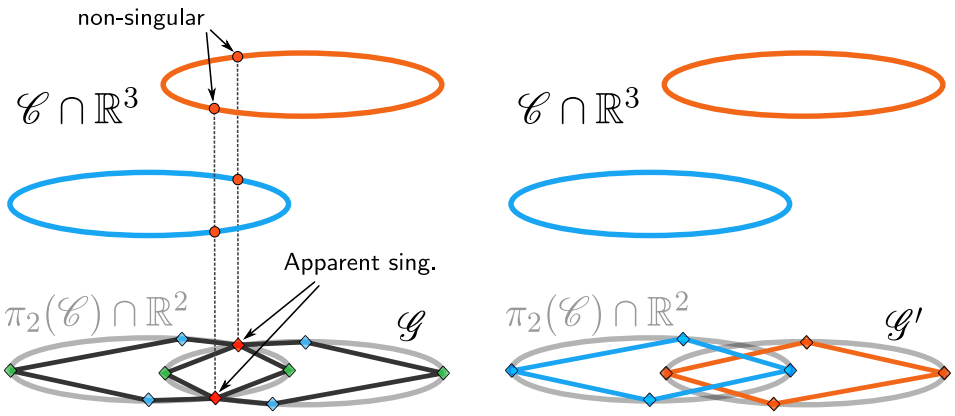


Figure 1.5. Illustration of the algorithm designed in Chapter 8, on input an algebraic curve $\mathscr{C} \subset \mathbb{C}^3$ whose real trace is the union of two disjoint circles, represented in different colors. On the left figure, the algorithm first computes a piecewise linear approximation $\mathscr{G} \subset \mathbb{R}^2$ of the real trace of the plane projection $\pi_2(\mathscr{C})$. Then, it identifies in $\mathscr{G}$ the apparent singularities (in red) introduced by points overlapping through π_2. On the right, the fake self-crossings in $\mathscr{G}$ associated with these apparent singularities are removed by connecting the pairwise opposite neighborhood vertices. This process outputs a combinatorial graph $\mathscr{G}'$ that shares the same connectivity properties as $\mathscr{C}$.

The first step is to reduce the analysis to the projection on the plane defined by the first two coordinates, up to finitely many overlapping points:

(H_1) there is a one-dimensional parametrization $\mathscr{R} = (\Omega, (x_1, x_2))$ encoding $\mathscr{C}$, with $\Omega = (\omega, x_1, x_2, \rho_3, \ldots, \rho_n) \subset \mathbb{Q}[x_1, x_2]$.

As mentioned in Section 3.4 of Chapter 3, such a parametrization exists up to a generic linear change of coordinates affecting the first two coordinates. In particular, the restriction to $\mathscr{C}$ of the projection π_2 is birational onto its image $\mathscr{C}_2 = \pi_2(\mathscr{C})$[4]. In particular, this means that $\mathscr{C}$ and $\mathscr{C}_2$ share the same connectivity properties at all but finitely many points. Moreover, (H_1) says that $\mathscr{C}_2 = \boldsymbol{V}(\omega)$, and that π_2 is invertible outside $\mathrm{sing}(\mathscr{C}_2)$[5].

We now describe the overlapping points. If $\mathscr{C}_2 \subset \mathbb{C}^2$ is the Zariski closure of $\pi_2(\mathscr{C})$, the set of *apparent singularities* of $\mathscr{C}_2$ is defined as $\mathrm{app}(\mathscr{C}_2) = \mathrm{sing}(\mathscr{C}_2) - \pi_2(\mathrm{sing}(\mathscr{C}))$. These are the singularities introduced by π_2. A singular point of $\mathscr{C}_2$ is called a node if it is an ordinary double point that is the intersection of two branches of transversal tangent lines (see [El 08, §3.1]). Then, the following two assumptions say that overlaps involves at most *two regular* points, and their projection is a node of $\mathscr{C}_2$:

(H_2) Let $\boldsymbol{z} \in \mathrm{sing}(\mathscr{C}_2)$, if $\boldsymbol{z} \notin \mathrm{app}(\mathscr{C}_2)$ then $\pi_2^{-1}(\boldsymbol{z}) \cap \mathscr{C}$ has cardinality 1;
if $\boldsymbol{z} \in \mathrm{app}(\mathscr{C}_2)$ then $\boldsymbol{z}$ is a node and $\pi_2^{-1}(\boldsymbol{z}) \cap \mathscr{C}$ has cardinality 2.

In other words, the finitely many overlaps involve exactly two branches, whose projections intersect transversally. According to Figure 1.6 this makes the local topology straightforward as it corresponds to only one of the three cases.

[4] The restriction to an algebraic set V of a polynomial map is birational if it has inverse a rational function on a non-empty Zariski open subset of V.
[5] Indeed, since $\mathscr{C}_2$ is defined by the sole polynomial ω, both its derivatives must vanish at singular points of $\mathscr{C}_2$.

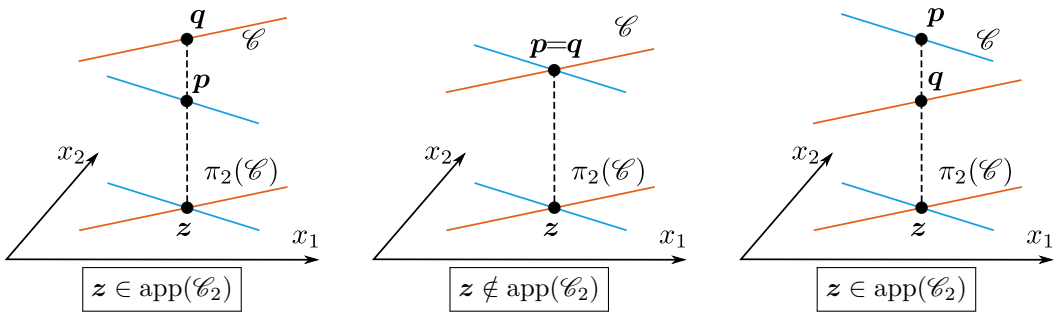


Figure 1.6. A local representation of three different configurations of the curve that projects onto a node. According to (H_2) only these three cases can occur.

But Figure 1.6 tells us more; in terms of local connectivity there are only two cases to consider: whether the two branches intersect each other or not. This leads to the following strategy:

Step 1: compute the topology of $\mathscr{C}_2$;

Step 2: for each node (α, β) of $\mathscr{C}_2$ decide if it is an apparent singularity or not.

Suppose that the input polynomials describing $\mathscr{C}$ have magnitude (δ, τ). Then, **Step 1** can be tackled using any exact algorithm for computing the topology of a planar real algebraic curve. As seen in the presentation of the prior works, this is a very active research topic, and the best known bit-complexity bound is $\widetilde{O}\left(\delta^6 + \delta^5\tau\right)$ in [KS15, DDR+22].

As for **Step 2**, according to (H_2), it is equivalent to decide whether there are at least two points of $\mathscr{C}$, that project on (α, β). According to the following assumption, this can be decided inside $\pi_3(\mathscr{C})$:

(H_3) the restriction of π_3 to $\mathscr{C}$ is injective.

More precisely, we lift the possible solutions in the fiber $\pi_2(\alpha, \beta) \cap \pi_3(\mathscr{C})$ using Puiseux series expansion, which leads to the following criterion, that generalizes the one of [El 08]. Using the parametrization $(\omega, x_1, x_2, \rho_3, \ldots, \rho_n)$ given by (H_1):

Lemma. $z \in \mathrm{app}(\mathscr{C}_2) \iff$ *z is a node of* $\mathscr{C}_2$ *and* $(\partial^2_{x_2}\omega \cdot \partial_{x_1}\rho_3 - \partial^2_{x_1x_2}\omega \cdot \partial_{x_2}\rho_3)(z) \neq 0$

Remark that this criterion involves only derivatives of only two polynomials of the one-dimensional parametrization encoding $\mathscr{C}$. Hence, using resultant and gcd computations, one can compute a zero-dimensional parametrization encoding the nodes of $\mathscr{C}_2$ and extract the apparent singularities using the above criterion. We show in Section 8.5 of Chapter 8 that this process can be done within $\widetilde{O}\left(\delta^6 + \delta^5\tau\right)$ bit operations as well.

Finally, at this stage, we have a topologically correct piecewise linear approximation of $\mathscr{C}_2$, together with an encoding of the apparent singularities. Using the local conic structure of semi-algebraic sets – see Subsection 4.4.2 of Chapter 4 – we show that removing the fake self-crossings associated with the apparent singularities in the piecewise linear approximation, one gets a *combinatorial graph* that shares the *same connectivity properties* than $\mathscr{C}$. This step, depicted in Figure 1.5, comes at a negligible additional computational cost compared to the previous ones.

Main result. To answer Problem II.b, our algorithm must take as input descriptions of an algebraic curve $\mathscr{C} \subset \mathbb{C}^n$ and finitely many points $\mathcal{P}$ in $\mathscr{C} \cap \mathbb{R}^n$. On output, we expect a description of a partition of $\mathcal{P}$, grouping the points lying in the same connected components of $\mathscr{C} \cap \mathbb{R}^n$. Such an algorithm can be directly derived from the one described above: in the planar topology computation, we add the points in $\pi_2(\mathcal{P})$ as vertices of the piecewise linear approximation of $\pi_2(\mathscr{C}) \cap \mathbb{R}^2$. Generically, none of the points in $\pi_2(\mathcal{P})$ are apparent singularities, so these vertices are not removed in the process. Therefore, two vertices are connected in the output combinatorial graph if and only if the associated points in $\pi_2(\mathcal{P})$, and consequently $\mathcal{P}$, lie in $\mathscr{C} \cap \mathbb{R}^n$.

Before stating our main result, that contains both the correction and a complexity bound of the algorithm described above, let us say a few words about inputs and outputs.

`Input`: on input sequences of polynomials defining $\mathscr{C}$ and $\mathcal{P}$, the first step is to perform a generic linear change of variable to meet the genericity assumptions and to compute one-dimensional parametrizations $\mathscr{R}$ and $\mathscr{P}$ encoding $\mathscr{C}$ and $\mathcal{P}$. However, these steps have bit complexity at most cubic in the degree of input algebraic sets, thus fitting within our overall complexity – see [SS17, SS18, GM19]. We will assume that the input has undergone this preprocessing step, as answering connectivity queries on the sheared curve is equivalent to doing so on the original curve.

`Output`: to efficiently describe a partition of $\mathcal{P}$, we avoid computing parametrizations encoding subsets. Instead, we identify the points of $\mathcal{P}$ by their rank when ordered by their first coordinate, which are all distinct by genericity. This identification is computationally achieved using univariate root isolation, which is part of planar topology computation. This approach yields a compact output, requiring at most $\widetilde{O}(|\mathcal{P}|)$ bits.

Following the strategy described above, leads to the following result.

Contribution to Problem II.b

Let $\mathscr{R} \subset \mathbb{Z}[x_1, x_2]$ and $\mathscr{P} \subset \mathbb{Z}[x_1]$ as above of respective magnitudes (δ, τ) and (μ, κ). There exists an algorithm which, on input $\mathscr{R}$ and $\mathscr{P}$, computes a partition of bit size $\widetilde{O}(\mu)$, grouping the points of $\mathcal{P} \cap \mathbb{R}^n$ lying in the same semi-algebraically connected component of $\mathscr{C} \cap \mathbb{R}^n$, using

$$\widetilde{O}(\delta^6 + \mu^6 + \delta^5\tau + \mu^5\kappa)$$

bit operations.

This is to be compared with the best complexity $\widetilde{O}(\delta^{19}(\delta + \tau))$ known to analyze the topology of space curve. Note that the dependency on n in the complexity bound is "hidden" within the potential degrees of the parametrizations and the corresponding algebraic sets. Indeed, according to Bézout's bound, an algebraic set, defined by polynomials, of degree at most D, can have degree at most D^n.

1.4 Conclusion and Perspectives

In this section, we outline the short-term and long-term research prospects related to the contributions presented in this thesis. These prospects primarily revolve around further enhancing the efficiency and generality of our methods, as well as expanding the scope and tackling more challenging applications.

1.4.1 Roadmap algorithms

As seen in the previous sections, roadmap algorithms are the main tool for solving connectivity queries on real algebraic sets and, a fortiori, semi-algebraic sets.

State-of-art. On input a semi-algebraic set S of $\mathbf{R}^n$ defined by s polynomials with coefficients in $\mathbf{Q}$ of maximum degree D, the best known roadmap algorithm is the one of [BPR00]. It performs $(sD)^{O(n^2)}$ arithmetic operations in $\mathbf{Q}$. When S is an arbitrary real algebraic set of dimension d, this bound decreases to $(nD)^{O(n\log^2 d)}$ with the algorithm of [BR14]. Finally, the best-known complexity bound for roadmap algorithms is obtained in Chapter 7, with $(nD)^{O(n\log d)}$ for smooth real algebraic sets. Moreover, the constants in the exponent are made explicit, which gives an output roadmap of degree

$$n^{4d\log_2(d)+O(d)}D^{2n\log_2(d)+O(n)}. \tag{1.4}$$

In the following, we mention different directions to improve these results.

Semi-algebraic sets. The next step is then to extend the applicability of the best roadmap algorithm to semi-algebraic sets, as applications involve such sets as seen for the cuspidality problems. One way is to reformulate the inequalities and inequations as equations, using an extra variable t as follows:

$$g \geq 0 \to g - t^2 = 0, \qquad g > 0 \to g \cdot t^2 - 1 = 0, \qquad g \neq 0 \to g \cdot t - 1 = 0.$$

This allows to apply as such roadmap algorithms for general real algebraic sets, and provided additional regularity assumptions, our algorithm for smooth real algebraic sets. However, these techniques increase the number of variables and the degree in the input systems, making the methods unpractical.

Another approach is to consider the case of closed semi-algebraic sets, that is of the form

$$f_1 = \cdots = f_p = 0, \quad g_1 \geq 0, \ldots g_s \geq 0,$$

where the f_i's and g_i's are polynomials in $\mathbf{Q}[x_1, \ldots, x_n]$. We also make the assumption that $(f_1, \ldots, f_p, g_{i_1}, \ldots, g_{i_\ell})$ is a reduced regular sequence defining a smooth algebraic set for all $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$, which is typically satisfied for the targeted applications.

Thanks to the intermediate results obtained in the proof of the new connectivity result in Chapter 6, we should be able to obtain a new generalization to the semi-algebraic case (but under the regularity assumptions just described). Indeed, we can rely on the extension of the

notion of critical points and values to the semi-algebraic case, which consists in considering the critical points and values of the functions under consideration on the boundaries defined by the reduced regular sequences $(f_1, \ldots, f_p, g_{i_1}, \ldots, g_{i_\ell})$ for $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$. The assumption of regularity ensures good topological properties (namely a Whitney stratification of S) which then allows us to use the semi-algebraic version of Thom's first isotopy lemma of [CS92] to its full potential, and mimic the proof of the connectivity result of Chapter 6.

Here again, the passage from the connectivity result to the algorithm will require new results. Having to consider the edge of S will induce a combinatorial factor in the complexity, which should then be $s^n(nD)^{O(n\log(n))}$. Note this does not require the introduction of any infinitesimal.

General semi-algebraic sets. This leaves the problem to tackle open, possibly singular semi-algebraic sets. The first step would be to generalize the algorithm developed in Chapters 6 and 7 to singular algebraic sets, keeping a similar complexity bound.

A first approach would be to investigate deformation techniques to reduce to the smooth case, but without explicitly manipulating infinitesimals. This has been successfully achieved for the computation of sample points in each semi-algebraically connected component of a semi-algebraic set, which also relies on critical point methods – see Section 5.2 of Chapter 5. This passes by the computation of a basis for an elimination ideal, using Gröbner bases. In particular, this involves saturated ideals, for which a new promising algorithm has been proposed in [BES23] and is under integration in the library msolve[6].

Reduce the size of intermediate data. Let $V \subset \mathbf{C}^n$ be an equidimensional algebraic set such that $V \cap \mathbf{R}^n$ is bounded, and for $1 \leq i \leq n$ the canonical projections π_i on the first i-th variables. Recall that any roadmap algorithm's first steps are to compute the polar variety $W_i = W(\pi_i, V)$, that intersect every connected component, and to repair its connectivity failures in these components, by adjoining fibers $V \cap \pi_{i-1}^{-1}(\pi_{i-1}(\boldsymbol{z}))$, for $\boldsymbol{z}$ ranging in $W(\pi_1, W_i) \cup \mathrm{sing}(V)$, which is assumed to be finite. Indeed, according to the semi-algebraic version of Thom's first isotopy lemma, this is where the topology change of W_i can occur, and then the number of connected components is likely to change.

However, one could expect to reduce the number of fibers by taking them only at the points $\boldsymbol{z} \in W(\pi_1, V) \cup \mathrm{sing}(V)$, which form a subset of $W(\pi_1, W_i) \cup \mathrm{sing}(V)$, which is expected to be of much smaller size. The intuition is that the "relevant" connected components of the polar variety on which it is necessary to consider fibers are those containing at least one point of $W(\pi_1, V) \cup \mathrm{sing}(V)$. For these, taking fibers from $W(\pi_1, V) \cup \mathrm{sing}(V)$ captures the change of the topology of the embedding variety V changes. This can be seen in the example of the torus in Figure 1.7. Therefore, we expect to generalize the connectivity result for roadmap algorithms, to avoid including all the critical points in $W(\pi_1, W_i)$ and reduce both the size of the intermediate data and the computational cost of the computation of such points. Some estimates on these two latter quantities can be found in Subsection 7.3.2 of Chapter 7, which are based on [SS17, Section 6] and [SS18]. Concretely, this would reduce the constants in the exponents in (1.4).

[6] https://msolve.lip6.fr

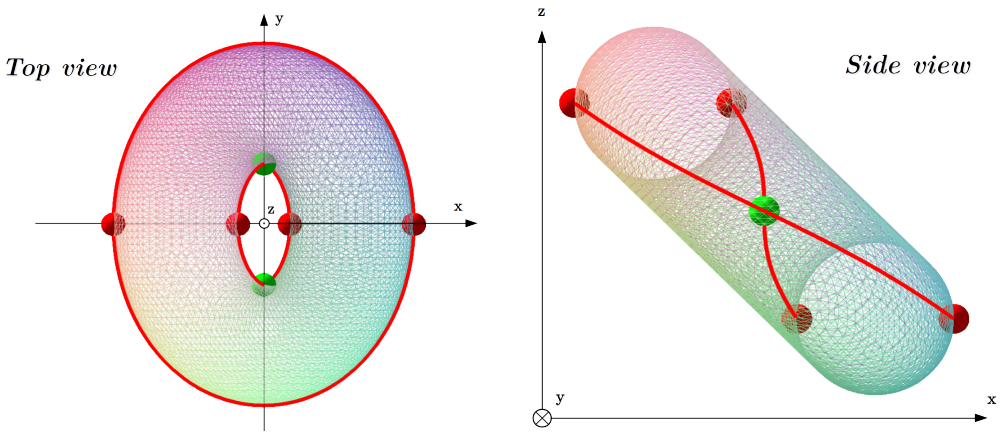


Figure 1.7. Illustration of the critical loci considered for the computation of a roadmap for a three-dimensional torus V. The second polar variety $W_2 = W(\pi_2, V)$ is the red curve. The points of $W(\pi_1, V)$ are the red sphere, while the points of $W(\pi_1, W_i)$ not in $W(\pi_1, V)$ are in green; V is smooth here. You can see that "scanning" the variety along the x-axis, while the type of the fibers might change at the green sphere, the number of connected components of W_2 remain the same between two consecutive red spheres.

Structured systems. Another avenue for improvement would be to take into account the possible structure of the input system for computing roadmaps, following the work initiated in [SS18], which solves efficiently zero-dimensional systems with a multi-homogeneous structure. Of particular interest is the case where the input polynomial system is quadratic as the degree bounds turn out to be much nicer. Indeed, according to [SS18, Corollary 2], the critical points of the restriction of the projection on the first coordinate to a smooth equidimensional algebraic set $V \subset \mathbf{C}^n$ defined by p polynomials of maximum degrees D, has maximum degree

$$\binom{n-1}{p-1} D^p (D-1)^{n-p},$$

that is exponential in n and p. However, when $D = 2$, this bound reduces to $\binom{n-1}{p-1} 2^p$, which is still exponential in p but only *polynomial in n, the number of variables*. Hence, for p fixed we can target, as done in [SS18] for zero-dimensional system, roadmap algorithms whose complexity would be polynomial in $(2n)^{p \log_2(n-p)}$, on input V as above.

This is also to be related with the bound $n^{O(s)}$ proved by Barvinok [Bar97] on the topological complexity of semi-algebraic sets of $\mathbf{R}^n$ defined by s quadratic inequalities – see also [Bas17, §3.6]. Similarly to the Thom-Milnor's bound discussed in Subsection 5.2.1 of Chapter 5, this gives a lower bound of complexity that one can hope to get close to.

Towards optimal roadmap algorithms. As further discussed in Subsection 5.2.1 of Chapter 5, the topological complexity of semi-algebraic sets is upper bounded by Thom-Milnor's bound. This constitutes a lower bound for roadmap algorithms. We hope to achieve it, why? Achieving such a complexity bound for roadmap algorithm would probably require to drop the recursive structure in roadmap algorithms as the complexity of computing critical points matches the complexity class of this lower bound.

Software. We already have a prototype implementation for roadmaps which mimics the approach from [MS06]. This is based a recursive scheme similar to the one introduced by Canny but takes fibers at rational points between critical values instead of manipulating symbolically real algebraic numbers.

This prototype implementation is fast enough to tackle the singularity analysis of a 6 revolute joint PUMA robot. This challenging robotic problem involves dealing with an open semi-algebraic set. The outcome was a roadmap of degree 8000, computed in three hours.

In the coming years, we aim at developing a robust and efficient implementation of asymptotically optimal roadmap algorithms whose practical behaviour does reflect the complexity gains obtained during this PhD and in forthcoming theoretical developments. For algebraic elimination algorithms, we will rely on the msolve[7] library [BES21] which allows to compute efficiently rational parametrizations of algebraic curves.

1.4.2 Connectivity queries on semi-algebraic curves

Dealing efficiently with the connectivity analysis of roadmaps is a key step in connectivity queries decision, as their degree can be very large. Moreover, the best-known algorithms have complexity subquadratic in their output size, so that the analysis of roadmaps, can quickly become the bottleneck of the whole process.

State-of-art. The connectivity analysis of an arbitrary semi-algebraic curve of $\mathbf{R}^n$ defined as the intersection of an algebraic curve of degree at most δ and s inequalities of maximum degrees δ, can be performed in complexity polynomial in $s\delta$. But the degree of the latter complexity has not been bounded yet. We refer to Subsection 5.3.3 of Chapter 5 for more details. For real algebraic curves of $\mathbb{R}^n$, the outcome of Chapter 8, is the first Monte Carlo algorithm with complexity $\widetilde{O}\left(\delta^6\right)$, which matches the best-known bound for curve of $\mathbb{R}^2$. The probabilistic nature of this algorithm is due to a prior random linear change of variable to satisfy genericity assumptions, with high probability.

Deterministic algorithm. A first direction for improvement lies in making our algorithm deterministic. This could involve simplifying or eliminating the genericity assumptions we currently rely on. For instance, we could explore techniques to handle more complex apparent singularities using Puiseux series expansion or leverage the fact that the plane projection need not be in a generic position when using the algorithm of [DDR+22]. Another approach, employed by algorithms like those in [KS15] and [JC21], is to deterministically find a change of variables that places the curve in a generic position.

Union of curves. As the natural output of roadmap algorithms is the union of several curves, adapting the algorithm for such inputs would be of great benefit. Indeed, if $\mathscr{C}_1$ and $\mathscr{C}_2$ are two curves of respective degree δ_1 and δ_2 , then $\mathscr{C}_1 \cup \mathscr{C}_2$ has degree $\delta_1 + \delta_2$. The key idea is that it suffices to decide:

1. decide which query points lie in the same connected component of each curve,

[7] https://msolve.lip6.fr

2. to merge the connected components of the respective curves $\mathscr{C}_1$ and $\mathscr{C}_2$ that contain a point of $\mathscr{C}_1 \cap \mathscr{C}_2$ (which is generically finite).

Semi-algebraic curves. We also aim at generalizing algorithms for answering connectivity to the case of semi-algebraic sets. This involves modifying the algorithm to include inequalities $g_1 > 0, \ldots, g_s > 0$ in the input. The algorithm would use a structure similar to the variant for unions, to obtain a finer partition of query points for each $1 \leq i \leq s$, grouping the points that belong to the same connected component of the algebraic curve and for which the sign of g_i is constant. This would imply a combinatorial factor of $sD\delta$ where D is a bound on the degree of the g_i's, and δ is the degree of the algebraic curve.

Further complexity improvements. The most costly steps of the algorithms for answering connectivity queries on semi-algebraic curves (in the vein of the one developed in this PhD) are the *(a)* the computation of topology of the projection of the set under study on some plane and the *(b)* the identification of apparent singularities.

To improve the first one, an idea would be to avoid the computation of the comprehensive topology of plane curve for connectivity considerations. For instance, this could be done by constructing, on the fly, the partition of the query points, while scanning the plane curve along the x-axis, using e.g. hybrid symbolic-numeric techniques.

To improve the second step, the main direction seems to investigate parametrizations for nodes of smaller size, which are cheaper to compute.

Software. As emphasized above, the step of answering connectivity queries on curves as efficiently as possible is crucial since the input from roadmap algorithms might have a size which is singly exponential w.r.t. the number of variables. Hence, we target to design efficient implementations. This work has already started with an optimized implementation for subresultant and gcd computations involving multi-modular computations, partly using the FLINT[8] library and the real root isolator of the msolve library.

1.4.3 Applications

In this thesis, we successfully designed an algorithm for solving an open problem from robotics, from a general point of view. This employed many high-level routines from the state-of-the-art of computational real algebraic geometry, and advanced results from real algebraic geometry. Moreover, using a prototype implementation, we showed a proof of concept of the practical application of this algorithm.

Extension to semi-algebraic sets. In some situations, kinematic maps modeling robots must be restricted to semi-algebraic algebraic sets e.g. due to constraints on the configuration of the joints. Most of the ingredients used in the proof already apply to the semi-algebraic case: Thom's first isotopy lemma, roadmap algorithm, sample points computation, real quantifier elimination.

[8] https://flintlib.org/

Software. We aim at developing a toolbox, easy to use by researchers in robotics and engineers, which is based on the aforementioned software developments on roadmaps and curves, that will provide specific functionalities which are of interest to analyze the geometry of robots (cuspidality decision, kinematic singularity analysis, etc.). Note that the computation of sample points already benefits from such an efficient implementation in the software RAGlib[9] software written with the computer algebra programming language Maple. Recently, some significant progress has been made on quantifier elimination [LS21]. This makes realistic this ambitious project in the coming years.

New applications Many other problems from applications translate into real algebro-geometric problems. Among them are, we mention quantum computing, rigidity theory [JW18] or program verification [GHMM23, Tiw10].

1.5 Structure of the thesis

This thesis is structured in two parts, which serve different purposes.

In the **first part**, we present notions from the literature that will be used extensively in the second part. This part aims to fix the background and notations, as well as give pedagogic developments, that might not exist in the literature of this thesis's topic. In some chapters, we also provide preliminary results that serve as the basis for our further work. These results are derived from well-established textbook materials.

- In **Chapter 2**: "*Algebraic geometry*", we lay the groundwork by introducing the fundamental tools of complex (as opposed to real) algebraic geometry. Our emphasis here is on the notions of genericity and critical loci of polynomial maps, which are ubiquitous in our contributions. Our main references are [Sha13, Har77, Ful08, Eis95, CLO15].

- In **Chapter 3**: "*Computational algebraic geometry*", we transition to the computational aspects. We describe our computational framework as well as the different representations of polynomials and objects from algebraic geometry introduced in the previous chapter. Moreover, we present two significant computational tools, namely Gröbner bases and geometric resolutions. Our main references are [CLO15, GG13, Eis95]

- In **Chapter 4**: "*Real algebraic geometry*", we shift our focus to the real domain. Here, we explore the theory of real closed fields and their extensions, laying the groundwork for understanding the core concepts of real algebraic geometry. Our main references are [BCR98, BPR06].

- In **Chapter 5**: "*Computational real algebraic geometry*", we provide an extended historical overview of three pivotal challenges in computational real algebraic geometry. These are real quantifier elimination, the computation of sample points in each semi-algebraically connected component of a semi-algebraic set, and solving connectivity queries within such sets. Our main references are [BPR06, Bas17].

[9] RAGlib: https://www-polsys.lip6.fr/~safey/RAGLib/

In the **second part**, we give the comprehensive proofs of the four main contributions we described in this chapter. This includes:

- ⊛ In **Chapter 6**: "*A new connectivity result for unbounded smooth real algebraic sets*", we present the proof of the generalized connectivity we presented in Subsection 1.3.1. This proof has been the main contribution of the paper [PSS24] (with M. Safey El Din and É. Schost), which is published in the *Journal of Symbolic Computation*.

- ⊛ In **Chapter 7**: "*A nearly optimal algorithm for unbounded smooth real algebraic sets*", we detail the generalized roadmap algorithm of Subsection 1.3.2 designed from the connectivity result of the previous chapter. Most of the chapter is devoted to the proof of genericity results, and complexity estimates. The content of this chapter will be very soon submitted as a paper, with M. Safey El Din and É. Schost.

- ⊛ In **Chapter 8**: "*Answering connectivity queries on real algebraic curves*", we present and prove the correction and complexity estimate of the algorithm described in Subsection 1.3.3. We also prove that the assumptions on the input, hold generically. These results are the main contribution of the paper [IPP23] (with N. Islam and A. Poteaux), which has been published in the proceedings of ISSAC 2023 - 48th International Symposium on Symbolic and Algebraic Computation, Jul 2023, Tromsø, Norway.

- ⊛ In **Chapter 9**: "*Real algebraic geometry in action: application to robotics*", we present a detailed version of the resolution of the robotics problem sketched in Section 1.2. This is the content of the paper [CPS+22] (with D. Chablat, M. Safey El Din, D. Salunkhe, P. Wenger), which has been published in the proceedings of ISSAC 2022 - 47th International Symposium on Symbolic and Algebraic Computation, Jul 2022, Lille, France.

Part I

Preliminaries

Algebraic geometry

2

As seen in the previous chapter, we are interested in problems defined by polynomials. These sets are called *algebraic sets* and are the basic objects of *algebraic geometry* of which we aim to provide key aspects in this chapter.

We start by providing in Section 2.1 the first definitions and essential properties of affine algebraic sets before presenting their projective counterparts in Section 2.2. Moving forward, Section 2.3 examines the mappings between algebraic sets and discusses noteworthy classes among them. Building upon the previously introduced Zariski topology, we then review in Section 2.4 the concept of genericity, which is central in this thesis. Finally, in Section 2.5 we explore the notion of critical points before describing in Section 2.6 an important class of critical loci, namely polar varieties, that maintains substantial relevance throughout our study.

In the sequel, we denote by $\mathbf{C}$ an algebraically closed field of characteristic zero. Let $n \geq 1$ and $\boldsymbol{X} = x_1, \ldots, x_n$ be indeterminates. We write $\mathbf{C}[\boldsymbol{X}]$ or $\mathbf{C}[x_1, \ldots, x_n]$ for the ring of polynomials in the indeterminates $x_1, \ldots, x_n$, with coefficients in $\mathbf{C}$. For the results and notions introduced in this chapter we refer, when omitted, to the classic literature in (computational) algebraic geometry such as [Sha13, Har77, Ful08, Eis95, CLO15].

2.1 Definitions and main properties

2.1.1 Affine algebraic sets

Definition 2.1.1. An affine *algebraic set* of $\mathbf{C}^n$ is a subset of $\mathbf{C}^n$ that can be written as

$$\{\boldsymbol{y} \in \mathbf{C}^n \mid f_1(\boldsymbol{y}) = \cdots = f_p(\boldsymbol{y}) = 0\},$$

where $(f_1 \ldots, f_p) \subset \mathbf{C}[x_1, \ldots, x_n]$. For $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbf{C}[x_1, \ldots, x_n]$, we denote by $\boldsymbol{V}(\boldsymbol{f})$ or $\boldsymbol{V}(f_1, \ldots, f_p)$ the algebraic set of $\mathbf{C}^n$ defined by $\boldsymbol{f}$.

Let V be an affine algebraic set of $\mathbf{C}^n$, the affine algebraic *subsets* of V are the algebraic sets of $\mathbf{C}^n$, that are contained in V.

Finally, an affine *hypersurface* is an algebraic set that is the zero-set of a single polynomial.

In the following, when it is clear from the context, affine algebraic sets are simply referred as algebraic sets. The ambiguity could come from the dual notion of projective algebraic sets, that we introduce in Section 2.2.

Let $\boldsymbol{f} = (f_1 \ldots, f_p) \subset \mathbf{C}[x_1, \ldots, x_n]$ be a finite sequence of polynomials. For any $\boldsymbol{y} \in \mathbf{C}^n$, we denote by $\boldsymbol{f}(\boldsymbol{y})$ the point $(f_1(\boldsymbol{y}), \ldots, f_p(\boldsymbol{y})) \in \mathbf{C}^p$, where the f_j's are evaluated at the entries of $\boldsymbol{y}$. Moreover $\boldsymbol{f}(\boldsymbol{y}) = 0$ stands for $f_1(\boldsymbol{y}) = \cdots = f_p(\boldsymbol{y}) = 0$.

Example 2.1.2.

a) The empty set $\emptyset$, $\mathbf{C}^n$ and any finite subset of $\mathbf{C}^n$ are algebraic sets.

b) The proper algebraic sets of $\mathbf{C}$ are exactly the finite subsets of $\mathbf{C}$.

c) The unit circle or the hyperbola are algebraic sets of $\mathbf{C}^2$ defined by the vanishing set of the polynomials $x^2 + y^2 - 1$ and $xy - 1$, respectively. Their projection on any of the two coordinates is respectively $\mathbf{C}$ and $\mathbf{C}^\star$. The latter is not an algebraic set.

d) Let $M(\boldsymbol{X}) \subset \mathbf{C}[\boldsymbol{X}]^{p\times q}$, where p, q are positive integers, be a matrix with polynomial entries. Hence, the locus of $\mathbf{C}^n$ where M has rank at most $r \leq \min(p, q) - 1$ is an algebraic set, defined by the vanishing of all the minors of size $r + 1$ of M.

Remark 2.1.3.

a) The family of algebraic sets is closed under intersection and finite union. However, it is not closed under complementation and then, it is not stable under projections.

b) The family of sets defined by the vanishing of equations and inequations enjoy nicer stability properties. More precisely, the elements of such an obtained family are called the *constructible sets* and, according to [BPR06, Theorem 1.32], this family is stable under the aforementioned operations.

c) Any basic constructible set of $\mathbf{C}^n$ can actually be defined as the projection of an algebraic set of $\mathbf{C}^{n+1}$ as follows. Let $f_1, \ldots, f_p$ in $\mathbf{C}[\boldsymbol{X}]$ and $\boldsymbol{y} \in \mathbf{C}^n$ then

$$f_1(\boldsymbol{y}) \neq 0, \ldots, f_p(\boldsymbol{y}) \neq 0 \;\Leftrightarrow\; (f_1 \cdots f_p)(\boldsymbol{y}) \neq 0 \;\Leftrightarrow\; \exists u \in \mathbf{C},\, u \cdot (f_1 \cdots f_p)(\boldsymbol{y}) = 1.$$

Hence, the constructible set defined by the simultaneous non-vanishing of $f_1, \ldots, f_p$, is the projection of the algebraic set defined by the vanishing of $u \cdot (f_1 \cdots f_p) - 1$.

We will occasionally employ the following refinement.

Definition 2.1.4. Let $\boldsymbol{D}$ be a subring of $\mathbf{C}$. We say that the set $V \subset \mathbf{C}^n$ is a *$\boldsymbol{D}$-algebraic set* of $\mathbf{C}^n$, if it is the zero-set of a finite set of polynomials in $\boldsymbol{D}[x_1, \ldots, x_n]$. Then there exists $\boldsymbol{f} \subset \boldsymbol{D}[x_1, \ldots, x_n]$ such that $V = \boldsymbol{V}(\boldsymbol{f})$.

Let us consider the converse problem: given an arbitrary set, consider the set of polynomials vanishing at each point of this set.

Definition 2.1.5. Let X be a subset of $\mathbf{C}^n$, we denote by

$$\boldsymbol{I}(X) = \{f \in \mathbf{C}[x_1, \ldots, x_n] \;\text{ s.t. }\; \forall \boldsymbol{y} \in X, f(\boldsymbol{y}) = 0\}$$

the set of polynomials vanishing on X. The set $\boldsymbol{I}(X)$ is an ideal of $\mathbf{C}[x_1, \ldots, x_n]$, and is called the *ideal of definition* of X.

The following theorem is fundamental in algebraic geometry as it allows one to characterize the algebraic sets as the common vanishing locus of finitely many polynomials.

Theorem 2.1.6 (Hilbert's basis theorem for field [Eis95, Theorem 1.2])**.**
Let $\mathbf{K}$ *be a field, the ring* $\mathbf{K}[x_1, \ldots, x_n]$ *is Noetherian. In other words, the two following equivalent assertions hold:*

1. *every ideal of* $\mathbf{K}[x_1, \ldots, x_n]$ *is finitely generated;*

2. *there is no infinite strictly increasing chain of ideals of* $\mathbf{K}[x_1, \ldots, x_n]$.

Thus, one can extend the notation $\boldsymbol{V}$ to ideals: given an ideal I of $\mathbf{C}[x_1, \ldots, x_n]$, and let $f_1, \ldots, f_p$ be generators of I given by Theorem 2.1.6, we note $\boldsymbol{V}(I) = \boldsymbol{V}(f_1, \ldots, f_p)$.

We can state now a fundamental result in algebraic geometry that is Hilbert's Nullstellensatz, which requires $\mathbf{C}$ to be algebraically closed. We start with the Weak Nullstellensatz, which is the historic version of the former one.

Theorem 2.1.7 (Weak Nullstellensatz)**.** *[Eis95, Corollary 1.7] Let* I *be an ideal of* $\mathbf{C}[\boldsymbol{X}]$. *Then,* $\boldsymbol{V}(I) = \emptyset$ *if and only if* $1 \in I$.

Example 2.1.8. The above result does not hold anymore when $\mathbf{C}$ is not algebraically closed. For example, the zero-set of $x^2 + 1$ in $\mathbf{R}$ is empty, but $1 \notin (x^2 + 1) \cdot \mathbf{R}[x]$.

Nonetheless, we will investigate in Chapter 4, the situation where the underlying fields are real closed fields. The latter fields are closely connected to algebraically closed fields as adding the square root of -1 raises an algebraically closed field.

Note that the latter condition of Theorem 2.1.7 means that $I = \mathbf{C}[\boldsymbol{X}]$. This theorem gives an effective criterion for deciding the emptiness of an algebraic set. This is a particular case of the ideal membership problem, and we will see in Section 3.3 how it can be solved using Gröbner bases, by computing normal forms.

This result is of importance as it guarantees that the only ideal representing the empty algebraic set is the entire polynomial ring $\mathbf{C}[\boldsymbol{X}]$ (unlike the above example). Pushing forward this identification between ideals and algebraic sets leads to the Strong Nullstellensatz.

Definition 2.1.9. Let I be an ideal of $\mathbf{C}[x_1, \ldots, x_n]$, the radical of I is the set

$$\sqrt{I} = \{f \in \mathbf{C}[x_1, \ldots, x_n] \mid \exists k \geq 1,\ f^k \in I\}.$$

An ideal I is *radical* if $I = \sqrt{I}$. In particular $\sqrt{I}$ is radical.

We can now formulate the Strong Nullstellensatz, which is equivalent to its "Weak" counterpart of Theorem 2.1.7. This constitutes the original Hilbert's Nullstellensatz.

Theorem 2.1.10 (Strong Nullstellensatz)**.** *[Eis95, Theorem 1.6] Let* I *be an ideal of* $\mathbf{C}[\boldsymbol{X}]$, *then* $\boldsymbol{I}(\boldsymbol{V}(I)) = \sqrt{I}$.

Remark that, by definition, for any algebraic set $V \subset \mathbf{C}^n$, $\boldsymbol{V}(\boldsymbol{I}(V)) = V$. As a consequence, $\boldsymbol{V}(I) = \boldsymbol{V}(\sqrt{I})$ and $\boldsymbol{I}(V)$ is a radical ideal. Therefore the above theorem gives a (inclusion-reversing) bijective correspondence between (affine) algebraic sets of $\mathbf{C}^n$ and radical ideals of $\mathbf{C}[\boldsymbol{X}]$ (see e.g. [CLO15, Theorem 7] or [Eis95, Corollary 1.10]).

2.1.2 Zariski topology

Definition 2.1.11. The *Zariski topology* on $\mathbf{C}^n$ is the topology whose closed sets are the algebraic sets of $\mathbf{C}^n$.

The following notions then come naturally with this topology.

Definition 2.1.12. Let X be a subset of $\mathbf{C}^n$.

The *Zariski closure* of X is defined, according to the underlying topology, as the intersection of all the algebraic sets that contain X. It will be denoted by $\overline{X}^Z$.

The set X is said to be *Zariski dense* in $Y \subset \mathbf{C}^n$ if $\overline{X}^Z = Y$.

Note that, by definition, a subset of $\mathbf{C}^n$ is Zariski dense in its Zariski closure. The following proposition gives an effective characterization of the Zariski closure.

Proposition 2.1.13 ([CLO15, Chap. 4, §4, Proposition 1])**.** *The Zariski closure of a set $X \subset \mathbf{C}^n$ is the algebraic set $\boldsymbol{V}(\boldsymbol{I}(X))$.*

We now address a topological notion that is particularly relevant to Zariski topology, as the following Theorem 2.1.19 shows.

Definition 2.1.14. A subset $V \subset \mathbf{C}^n$ is said to be *irreducible* if it cannot be written as $V = V_1 \cup V_2$ for distinct proper algebraic subsets $V_1, V_2 \subsetneq V$. Otherwise, it is said to be *reducible*.

Example 2.1.15.

a) A finite algebraic set is irreducible if and only if it is a singleton.

b) The algebraic set $\boldsymbol{V}(xy) \subset \mathbf{C}^2$ is reducible as $\boldsymbol{V}(xy) = \boldsymbol{V}(x) \cup \boldsymbol{V}(y)$. However the two components $\boldsymbol{V}(x)$ and $\boldsymbol{V}(y)$ are irreducible, and we will see that they are unique, up to ordering.

c) For $f \in \mathbf{C}[\boldsymbol{X}]$, the hypersurface $\boldsymbol{V}(f)$ is irreducible if, and only if, the polynomial f is irreducible.

According to the following proposition, the notion of Zariski irreducibility is mainly relevant for algebraic sets. Hence, in the following, we will simply refer to irreducibility for algebraic sets.

Proposition 2.1.16. *A subset $X \subset \mathbf{C}^n$ is irreducible if and only if its Zariski closure $\overline{X}^Z$ is.*

The following proposition gives an equivalent algebraic criterion for irreducible algebraic sets.

Proposition 2.1.17 ([CLO15, Chap. 4, §5, Proposition 3])**.** *An algebraic set $V \subset \mathbf{C}^n$ is irreducible if and only if its ideal of definition $\boldsymbol{I}(V)$ is a prime ideal.*

Example 2.1.18. The set $\mathbf{C}^n$ is irreducible in the Zariski topology as its ideal of definition $\boldsymbol{I}(\mathbf{C}^n) = \{0\}$ is a prime ideal. However, note that $\mathbf{C}^n$ is reducible in the usual complex topology.

The following theorem is central to the study of algebraic sets. It allows, in particular, to prove properties on irreducible components of a given algebraic set, before extending it to the whole set. Besides, important applications of irreducibility such as dimension (see next subsection), can be extended to general algebraic sets.

Theorem 2.1.19 (Irreducible decomposition [CLO15, Chap. 4, §6, Theorem 4])**.**
Let $V \subset \mathbf{C}^n$ be an algebraic set. There exist $m \geq 1$ and $V_1, \ldots, V_m$, irreducible algebraic subsets of V, such that the following holds:

- $V = V_1 \cup \ldots \cup V_m$;
- *for any* $1 \leq i \neq j \leq m$, $V_i \not\subset V_j$.

The V_i's are called the irreducible components *of V, and are* unique*, up to permutation.*

The computation of the irreducible decomposition of an algebraic set is a challenging problem that is tackled by algorithms from commutative algebra. Indeed, as suggested by Proposition 2.1.17, the irreducible components are obtained by the computation of the so-called primary components. Efficient algorithms can be found in [GTZ88, EHV92] and we refer to [BW93, Chapter 8] and [AL94, §4.4] for an overview.

We now present some interesting properties of Zariski open sets, that will be central in this manuscript. As introduced in Section 2.4 below, this gives an effective geometric characterization for genericity properties.

Let V be an algebraic set, recall that a Zariski open subset of V is a set that can be written as $V - W$, where W is an algebraic set.

Proposition 2.1.20. *Let V be an irreducible algebraic set, then any non-empty Zariski open subset $\mathscr{O}$ of V is Zariski dense in V.*

Moreover, for any other non-empty Zariski open subset $\mathscr{O}'$ of V, $\mathscr{O} \cap \mathscr{O}'$ is a non-empty Zariski open set.

In particular, according to Example 2.1.18, any two non-empty Zariski open subsets of $\mathbf{C}^n$ are Zariski-dense in $\mathbf{C}^n$ and intersect each other.

Besides, a non-empty Zariski open subset of an algebraic set V is Zariski dense in any irreducible component of V it intersects. Similarly, two such non-empty Zariski open subsets of V, intersect in an irreducible component W of V if and only if they both intersect W.

It is worth noting that, when $\mathbf{C} = \mathbb{C}$ the field of complex numbers, these notions match the ones of the more natural analytic topology on $\mathbb{C}^n$. Indeed, a non-empty Zariski open subset of $\mathbb{C}^n$ is dense for the analytic topology, and its complement has measure 0 for the usual Lebesgue measure.

We end this paragraph with an interesting (and quite unusual) property of open cover in the Zariski topology. This is to be connected with the concept of atlases introduced in Chapter 7.

Proposition 2.1.21. *Any algebraic set V of $\mathbf{C}^n$ is compact in the Zariski topology. In particular, any open cover of V (or of any Zariski open subset of V) has a finite subcover.*

2.1.3 Dimension

We can now give a first natural quantitative bound on algebraic sets.

Definition 2.1.22. The *dimension* of an irreducible algebraic set V is the maximal length d of strictly increasing chains $V_0 \subsetneq \ldots \subsetneq V_d$ of non-empty irreducible algebraic subsets of V. We note $\dim(V)$ this dimension.

Remark 2.1.23. The dimension of an irreducible algebraic set always exists and is finite. However, the property of finite dimension is independent of the Noetherian property given by the Hilbert's Theorem 2.1.6, as one might expect at first; see [Eis95, Exercise 9.6].

We can now extend this definition to reducible algebraic sets using their irreducible decomposition.

Definition 2.1.24. The *dimension* of an algebraic set V of $\mathbf{C}^n$, denoted $\dim(V)$, is the maximum of the dimensions of its irreducible components.

The algebraic set V is *equidimensional of dimension* d (or d-equidimensional or of pure dimension d) if all its irreducible components have dimension d.

Example 2.1.25.

a) Finite algebraic sets and $\mathbf{C}^n$ are equidimensional algebraic sets of respective dimensions 0 and n.

b) Equidimensional algebraic sets of dimension 1 and 2 are called respectively algebraic *curves* and *surfaces*.

c) For any non-zero $f \in \mathbf{C}[\boldsymbol{X}]$, the hypersurface $\boldsymbol{V}(f) \subset \mathbf{C}^n$ is an equidimensional algebraic set of dimension $n-1$.

d) The algebraic set $\boldsymbol{V}(xy, xz)$ is not equidimensional as it has two irreducible components $\boldsymbol{V}(x)$ and $\boldsymbol{V}(y, z)$ of respective dimension 2 and 1.

As for the irreducible decomposition, one can be interested in computing an equidimensional decomposition of an algebraic set, that is write it as a a union of equidimensional algebraic sets. Note that, contrary to the irreducible decomposition, such a decomposition is not unique, as one can have many equidimensional components of the same dimension.

We finish by a useful result that will be used for proofs of genericity.

Proposition 2.1.26. *Let V be an irreducible algebraic set, then any proper algebraic subset of V has dimension at most* $\dim(V) - 1$.

2.1.4 Degree

We now deal with another quantitative bound on algebraic sets, that quantifies the complexity of an algebraic set of fixed dimension. We follow a simplification of the original geometric construction from [Hei83].

Consider an algebraic set V, of dimension d. We will see, in Section 2.3, that fixing the image of sufficiently "generic" – this term is precisely defined in Section 2.4 – d linear forms,

one gets finitely many points in V. Hence, the dimension quantifies the number of "degrees of freedom" of a point lying on V.

Besides, one can show – see Theorem 2.3.12 – that there exists a non-empty Zariski open subset $\mathcal{O}$ of $\mathbf{C}^d$ such that the number of points obtained by fixing the image of d generic linear forms at a point of $\mathcal{O}$ is *constant*, and *maximal*. This number is called the degree of an algebraic set.

Definition 2.1.27 ([Hei83, Definition 1])**.** Let $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbf{C}[\boldsymbol{X}]$ defining an *equidimensional* algebraic set $V = \boldsymbol{V}(\boldsymbol{f})$ of dimension d. The *degree* of V, denoted by $\deg(V)$, is defined as the maximum of

$$\operatorname{card}(\boldsymbol{V}(\boldsymbol{f}, \ell_1, \ldots, \ell_d))$$

where $\ell_1, \ldots, \ell_d \in \mathbf{C}[\boldsymbol{X}]$ are affine forms (i.e. polynomials of degree ≤ 1) such that the above cardinality is finite.

The notion of degree can be extended to *general* algebraic sets in two ways:

(weak degree) as the degree of the equidimensional components of maximum dimension;

(strong degree) as the sum of the degrees of its equidimensional components.

In the following, either of the two definitions can be chosen, since the results do not depend on this choice. Moreover, most of the algebraic sets used in this will be equidimensional, for which both definitions agree.

Example 2.1.28.

a) A finite algebraic set has dimension zero, so that its degree equals its cardinality.

b) The degree of a non-empty algebraic set is never zero. Indeed, any point $(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \in V$ is clearly contained in $V \cap \boldsymbol{V}(x_1 - \boldsymbol{y}_1, \ldots, x_d - \boldsymbol{y}_d)$.

c) As $\dim(\mathbf{C}^n) = n$, and as an affine system of equations admits either 1 of infinitely many solutions, then $\mathbf{C}^n$ has degree 1.

d) The degree of a hypersurface is the degree of its defining polynomial i.e. for $f \in \mathbf{C}[\boldsymbol{X}]$, $\deg(\boldsymbol{V}(f)) = \deg(f)$.

It is worth noting that the degree of an algebraic set depends intrinsically of the embedding of the given algebraic set. Hence, unlike the dimension, the degree is not an invariant quantity under isomorphism. For example, the curves defined by $y = x^m$, for $m \geq 2$, are isomorphic to $\mathbf{C}$, but have degree $m > 1$.

Proposition 2.1.29 ([Hei83, Remark 2])**.** *Let V and W be algebraic sets of $\mathbf{C}^n$, then*

$$\deg(V \cup W) \leq \deg(V) + \deg(W).$$

Proposition 2.1.30 ([Hei83, Proposition 2])**.** *If $V \subset \mathbf{C}^n$ and $W \subset \mathbf{C}^m$ are algebraic sets, then*

$$\deg(V \times W) = \deg(V) \cdot \deg(W).$$

The following result is the main result about degrees of algebraic sets.

Theorem 2.1.31 (Heintz-Bezout's bound [Hei83, Theorem 1])**.** *Let V and W be algebraic sets of $\mathbf{C}^n$, then*

$$\deg(V \cap W) \leq \deg(V) \cdot \deg(W).$$

Example 2.1.32. In particular, if $f_1, \ldots, f_p \in \mathbf{C}[\boldsymbol{X}]$ are polynomials of total degree bounded by $D \geq 1$, then $\deg(\boldsymbol{V}(f_1, \ldots, f_p)) \leq D^p$ by Theorem 2.1.31.

An important variant of this result is reported below, in the finite case, where the bound is independent of the number of polynomials. In applications, the latter bound is much better since p is typically large compared to n [Hei83].

Theorem 2.1.33 ([Hei83, Corollary 1])**.** *Let $(f_1, \ldots, f_p) \subset \mathbf{C}[\boldsymbol{X}]$, then any* finite *algebraic set that is defined using the f_i's has cardinality at most $(1+D)^n$, where $D = \sum_{1 \leq i \leq p} \deg(f_i)$.*

Note that, for n fixed, the above bound is asymptotically optimal (take $f_i = x_i^d - 1$ for $1 \leq i \leq n$). Note also that adapted Bézout's bounds exist, for structured cases such as multi-homogeneous polynomials systems [SS18].

Other approaches exist to define the degree of algebraic sets, typically as the degree of their ideal of definition [Har77, Eis95, Ful98, Lan02, HHPS21, Laz21]. These are anterior to the one in consideration here and take into account the multiplicities of points.

2.1.5 Regularity and Jacobian criterion

Definition 2.1.34. Let $\boldsymbol{f} = (f_1, \ldots, f_p)$, where $f_i \in \mathbf{C}[x_1, \ldots, x_n]$ for $1 \leq i \leq p$. The *Jacobian matrix* of $\boldsymbol{f}$ is the matrix of size $p \times n$ with coefficients in $\mathbf{C}[x_1, \ldots, x_n]$ defined as follows:

$$\mathrm{Jac}(\boldsymbol{f}) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial x_1} & \cdots & \frac{\partial f_p}{\partial x_n} \end{bmatrix}.$$

The evaluation of $\mathrm{Jac}(\boldsymbol{f})$ at $\boldsymbol{y} \in \mathbf{C}^n$ is denoted by $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{f})$.

Proposition 2.1.35 ([CLO15, Chap. 9, §6, Proposition 2])**.** *Let $V \subset \mathbf{C}^n$ be an algebraic set and let $\boldsymbol{f} = (f_1, \ldots, f_p)$ be a set of generators of $\boldsymbol{I}(V)$ (given by Theorem 2.1.6).*

Then, for any $\boldsymbol{y} \in V$, the right-kernel of $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{f})$ does not depend on the choice of the generators in $\boldsymbol{f}$. It is called the Zariski tangent space *of V at $\boldsymbol{y}$ and is denoted $\mathrm{T}_{\boldsymbol{y}} V$.*

An important local notion for algebraic sets is the smoothness at a point. We can define regular and singular points by the rise of the dimension of a tangent space at a point, or equivalently, by the drop of its codimension. Recall that the rank of a matrix is the dimension of the vector space spanned by its columns.

Proposition 2.1.36. *Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set and let $\boldsymbol{f} = (f_1, \ldots, f_p)$ be a set of generators of $\boldsymbol{I}(V)$. Then $\operatorname{rank} \mathrm{Jac}_{\boldsymbol{y}} \boldsymbol{f} \leq n - d$ for any $\boldsymbol{y} \in V$ and:*

- *if $\operatorname{rank} \mathrm{Jac}_{\boldsymbol{y}} \boldsymbol{f} = n - d$, then $\boldsymbol{y}$ is called a* regular *point;*

- *if* $\operatorname{rank} \operatorname{Jac}_{\boldsymbol{y}} \boldsymbol{f} < n - d$*, then* $\boldsymbol{y}$ *is called a* singular *point.*

We denote by $\operatorname{reg}(V)$ *(resp.* $\operatorname{sing}(V)$*) the set of all regular (resp. singular) points of* V*. A* smooth *algebraic set is an algebraic set with no singular points.*

Example 2.1.37. Let $f \in \mathbf{C}[\boldsymbol{X}]$ be a non-zero square-free polynomial. We have seen that the hypersurface $\boldsymbol{V}(f)$ is equidimensional of dimension $n-1$ and by Hilbert's Nullstellensatz $\boldsymbol{I}(\boldsymbol{V}(f)) = f$. Hence, the singular points of $\boldsymbol{V}(f)$ are the $\boldsymbol{y} \in \boldsymbol{V}(f)$ where $\operatorname{Jac}_{\boldsymbol{y}}(f)$ has not full rank 1, that is when all the first partial derivatives of f vanish. In other words,

$$\operatorname{sing}(\boldsymbol{V}(f)) = \boldsymbol{V}(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}).$$

Theorem 2.1.38 ([CLO15, Chap. 9, §6, Theorem 8])**.** *Let* V *be a* d*-equidimensional algebraic set, then* $\operatorname{sing}(V)$ *is a proper algebraic subset of* V *of dimension at most* $d-1$*.*

We finish with an important and useful result given by the rank of the Jacobian matrix at a point, namely the *Jacobian criterion*.

Theorem 2.1.39 ([Eis95, Theorem 16.19] and [SS11, Lemma 15])**.** *Let* $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbf{C}[\boldsymbol{X}]$ *and let the constructible set*

$$X = \{\boldsymbol{y} \in \boldsymbol{V}(\boldsymbol{f}) \text{ s.t. } \operatorname{rank} \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{f}) = p\}.$$

Suppose that $\boldsymbol{V}(\boldsymbol{f})$ *is non-empty and* X *is Zariski dense in* $\boldsymbol{V}(\boldsymbol{f})$*. Then the ideal* $\langle \boldsymbol{f} \rangle$*, generated by* $\boldsymbol{f}$*, is radical, and* $\boldsymbol{V}(\boldsymbol{f})$ *is an equidimensional algebraic set of dimension* $n-p$*.*

A direct consequence of the above result is that X is exactly the set of regular points of V, so that if $X = \boldsymbol{V}(\boldsymbol{f})$, then it is smooth.

2.2 Projective algebraic sets

Definition 2.2.1. The *projective space* $\mathbb{P}^n(\mathbf{C})$ of dimension n, over $\mathbf{C}$, is the set of equivalence classes of points in $\mathbf{C}^{n+1} - \{0\}$:

$$[\boldsymbol{y}_0 : \cdots : \boldsymbol{y}_n] = \{(\lambda \boldsymbol{y}_0, \ldots, \lambda \boldsymbol{y}_n),\ \lambda \in \mathbf{C}^\star\}.$$

Here, $[\boldsymbol{y}_0 : \cdots : \boldsymbol{y}_n]$ are the homogeneous coordinates of the associated class in $\mathbb{P}^n(\mathbf{C})$. When there will be no ambiguity from the context, $\mathbb{P}^n(\mathbf{C})$ will be simply denoted by $\mathbb{P}^n$.

The projective space $\mathbb{P}^n$ can be seen as the set of lines of $\mathbf{C}^{n+1}$ that pass through the origin as there is a one-to-one correspondence between these two sets (see [CLO15, Chap. 8, §2, Exercise 1]). The following proposition shows that $\mathbb{P}^n$ is made of $n+1$ copies of $\mathbf{C}^n$, up to some trivial injections.

Proposition 2.2.2 ([CLO15, Chap. 8, §2, Corollary 3])**.** *There exists a decomposition*

$$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i,$$

where, for each $0 \leq i \leq n$

$$U_i = \{[\boldsymbol{y}_0 : \cdots : \boldsymbol{y}_n] \in \mathbb{P}^n \ \ \textit{s.t.} \ \ \boldsymbol{y}_i \neq 0\}.$$

is in one-to-one correspondence with $\mathbf{C}^n$*. The* U_i*'s are then called the* affine charts *of* $\mathbb{P}^n$*.*

By contrast, we introduce the complement of the affine spaces in $\mathbb{P}^n$.

Definition 2.2.3. For each $0 \leq i \leq n$ let

$$\mathcal{H}_i^\infty = \{[\boldsymbol{y}_0 : \cdots : \boldsymbol{y}_n] \in \mathbb{P}^n \ \ \text{s.t.} \ \ \boldsymbol{y}_i = 0\},$$

it is called the *hyperplane at infinity* with respect to the affine chart defined by $\mathbb{P}^n - \mathcal{H}_i^\infty$. Indeed, according to the previous proposition, $\mathbf{C}^n$ and $\mathcal{H}_i^\infty$ are complement to each other in $\mathbb{P}^n$.

Recall that a polynomial $f \in \mathbf{C}[x_0, x_1, \ldots, x_n]$ is homogeneous of degree D if all its monomial terms have the same total degree D. Hence, for any $(\boldsymbol{y}_0, \ldots, \boldsymbol{y}_n) \in \mathbf{C}^{n+1}$ and $\lambda \in \mathbf{C}^\star$, then

$$f(\lambda \boldsymbol{y}_0, \ldots, \lambda \boldsymbol{y}_n) = \lambda^D f(\boldsymbol{y}_0, \ldots, \boldsymbol{y}_n).$$

In particular, if $(\boldsymbol{y}_0, \ldots, \boldsymbol{y}_n)$ is a root of f, then so is every element of $[\boldsymbol{y}_0 : \cdots : \boldsymbol{y}_n]$. Hence, we can extend the notion of root of homogeneous polynomials to elements of the projective space $\mathbb{P}^n$. This leads to the projective counterpart of algebraic sets.

Definition 2.2.4. A *projective algebraic set* V of $\mathbb{P}^n$, is a subset of $\mathbb{P}^n$ that can be written as

$$\{\boldsymbol{y} \in \mathbb{P}^n \ \ \text{s.t.} \ \ f_1(\boldsymbol{y}) = \cdots = f_p(\boldsymbol{y}) = 0\},$$

where $f_1, \ldots, f_p$ are homogeneous polynomials in $\mathbf{C}[x_0, x_1, \ldots, x_n]$. We extend to the projective settings the notations from the affine case, e.g. $\boldsymbol{V}(f_1, \ldots, f_p)$ denotes the projective algebraic set defined by $f_1, \ldots, f_p$.

Proposition 2.2.5 ([CLO15, Chap. 8, §2, Proposition 6])**.** *Let* $\boldsymbol{f} = (f_1, \ldots, f_p)$ *be a sequence of homogeneous polynomials of* $\mathbf{C}[x_0, x_1, \ldots, x_n]$*. Then, using the notation of Proposition 2.2.2, the set* $\boldsymbol{V}(\boldsymbol{f}) \cap U_0$ *can be identified with the affine variety*

$$\boldsymbol{V}(g_1, \ldots, g_p) \subset \mathbf{C}^n,$$

where $g_i(x_1, \ldots, x_n) = f_i(1, x_1, \ldots, x_n)$*, for each* $1 \leq i \leq p$*.*

According to the previous proposition, we can see affine algebraic sets as locally closed sets of $\mathbb{P}^n$. In the following, we will identify the affine algebraic sets of $\mathbf{C}^n$ with their corresponding set in U_0. This leads to the notion of (Zariski) projective closure.

Definition 2.2.6. The *projective closure* $\overline{V} \subset \mathbb{P}^n$ of an affine algebraic set $V \subset \mathbf{C}^n$, is the intersection of all the projective algebraic sets containing V.

The conjunction of Propositions 2.2.2 and 2.2.5 shows that any projective algebraic set can be covered by affine charts, where they can be identified as an affine algebraic set. Hence,

the local notions in affine algebraic sets, introduced in Subsection 2.1.5, can be naturally extended to the projective setting. We do not detail this further, and refer to [Sha13, Chap. 2, §1] instead.

2.3 Mappings on algebraic sets

2.3.1 Polynomial maps

We start by considering the scalar polynomial maps defined on algebraic sets.

Definition 2.3.1. Let V be an algebraic set of $\mathbf{C}^n$, a *polynomial function* on V is a map of the form $\boldsymbol{y} \in V \mapsto f(\boldsymbol{y}) \in \mathbf{C}$, where $f \in \mathbf{C}[\boldsymbol{X}]$. The set of polynomial functions on V, denoted $\mathbf{C}[V]$ is a ring called the *coordinate ring* of V. Moreover,

$$\mathbf{C}[V] \backsimeq \mathbf{C}[\boldsymbol{X}]/\boldsymbol{I}(V),$$

where $\backsimeq$ denotes the existence of an isomorphism.

The bijective correspondence given by Theorem 2.1.10 raises, through quotient, a bijective correspondence between the algebraic sets V and their associated coordinate ring $\mathbf{C}[\boldsymbol{X}]/\boldsymbol{I}(V)$. Since $\boldsymbol{I}(V)$ can range over all possible radical ideals, the coordinate rings are exactly the $\mathbf{C}$-algebras that are reduced and finitely generated, also called affine algebras for this reason (see e.g. [Eis95, Corollary 1.8]). Therefore, we have a bijective correspondence between the affine algebraic sets of $\mathbf{C}^n$ and the affine $\mathbf{C}$-algebra

A first illustration of this correspondence is the following.

Proposition 2.3.2. *Let V be an algebraic set of $\mathbf{C}^n$, then*

(i) V is irreducible if and only if $\mathbf{C}[V]$ is an integral domain;

(ii) the Krull dimension of the ring $\mathbf{C}[V]$ is exactly the dimension of V.

We now naturally extend the notion of polynomial functions, to the one of polynomial maps.

Definition 2.3.3. Let $V \subset \mathbf{C}^n$ and $W \subset \mathbf{C}^m$ be two algebraic sets. A *polynomial* map between V and W is a map that can be written as

$$\begin{array}{rccc} \boldsymbol{\varphi}: & V & \to & W \\ & \boldsymbol{y} & \mapsto & (\varphi_1(\boldsymbol{y}), \ldots, \varphi_m(\boldsymbol{y})) \end{array},$$

where $(\varphi_1, \ldots, \varphi_m) \subset \mathbf{C}[\boldsymbol{X}]$.

To a polynomial map, we can associate its dual, associated to the coordinate rings of the starting and ending algebraic sets of this map.

Definition 2.3.4 (Pullback [Sha13, Chap. 1, §2.3, p.30])**.** Reusing the notation of Definition 2.3.3, the *pullback* φ^* of φ is the $\mathbf{C}$-algebra homomorphism

$$\begin{array}{rccc} \varphi^*\colon & \mathbf{C}[W] & \longrightarrow & \mathbf{C}[V] \\ & f & \longmapsto & f \circ \varphi \end{array}.$$

Conversely, for every $\mathbf{C}$-algebra homomorphism $\psi : \mathbf{C}[W] \to \mathbf{C}[V]$, there exists a unique polynomial map $\varphi : V \to W$ such that $\psi = \varphi^*$.

Hence, the correspondence between algebraic sets and their coordinate rings can be extended to the polynomial maps between algebraic sets and their pullbacks. This describes an equivalence between the category of the affine algebraic sets, and the category of the affine $\mathbf{C}$-algebras, reversing the arrows of the morphisms (see e.g. [Eis95, Corollary 1.10]). This translates into a perfect correspondence between the two categories of objects and the morphisms between them, as many results in the following will illustrate.

In the rest of this section, and without further precision, we refer to V, W and φ as in the above definition.

2.3.2 Isomorphisms

Definition 2.3.5. Let $V \subset \mathbf{C}^n$ and $W \subset \mathbf{C}^m$ be two algebraic sets. We say that a polynomial map $\varphi : V \to W$ is an *isomorphism*, if it bijective and φ^{-1} is polynomial as well. In this case, we say that V and W are isomorphic algebraic sets.

Recall that a polynomial map is said to be Zariski *continuous* if the inverse image of any algebraic set, is an algebraic set. It is a Zariski *homeomorphism* if, in addition, it is bijective and has a continuous inverse.

Lemma 2.3.6. *A polynomial map is a continuous map for the Zariski topology. Hence an isomorphism is a Zariski* homeomorphism*.*

Proof. Let $V \subset \mathbf{C}^n$ and $W \subset \mathbf{C}^m$ be algebraic sets and let $\varphi\colon V \to W$ be a polynomial map. Since W is an algebraic set, there exist $h_1, \ldots, h_p$ in $\mathbf{C}[x_1, \ldots, x_m]$ such that $W = \boldsymbol{V}(h_1, \ldots, h_p)$. Let Z be a Zariski closed subset of W, then there exist $h_{p+1}, \ldots, h_s$, in $\mathbf{C}[x_1, \ldots x_m]$, with $s \geq p+1$, and such that

$$Z = \boldsymbol{V}(h_{p+1}, \ldots, h_s) \cap W = \boldsymbol{V}(h_1, \ldots h_s).$$

Since φ is polynomial there exists $(\varphi_1, \ldots, \varphi_m) \subset \mathbf{C}[x_1, \ldots, x_n]$ such that

$$\varphi^{-1}(Z) = \{\boldsymbol{y} \in \mathbf{C}^n \mid \forall\, 1 \leq i \leq s,\, h_i(\varphi_1(\boldsymbol{y}), \ldots, \varphi_m(\boldsymbol{y})) = 0\} \cap X.$$

For all $1 \leq i \leq s$, let $g_i = h_i(\varphi_1, \ldots, \varphi_m) \in \mathbf{C}[x_1, \ldots, x_n]$. Note that

$$\varphi^{-1}(Z) = \boldsymbol{V}(g_1, \ldots, g_s) \cap X,$$

which is a Zariski closed subset of X. In conclusion, since the inverse image of every Zariski closed set of W is a Zariski closed set of X, then $\varphi\colon V \to W$ is a Zariski continuous map.

If φ is an isomorphism, then φ^{-1} is polynomial, so it is Zariski continuous by the first item. Hence, φ is a homeomorphism for the Zariski topology. □

Remark 2.3.7. Note that the converse of the above proposition is not true. Indeed, consider the map φ from $\mathbf{C}$ to itself, exchanging 0 and 1, and being the identity elsewhere. Then, φ is a Zariski homeomorphism, but not an isomorphism.

The following result shows that equidimensionality (and thus dimension) is invariant through isomorphisms.

Lemma 2.3.8. *Assume that $\varphi : V \to W$ is an isomorphism, then the following hold:*

1. *the irreducible components of V and W are in one-to-one correspondence through φ;*
2. *the algebraic set V is d-equidimensional if and only if W is.*

Proof. Let V' be an irreducible component of V, then $\varphi(V')$ is Zariski closed as φ is a Zariski homeomorphism by Lemma 2.3.6. Suppose that

$$\varphi(V') = W_1 \cup W_2,$$

where W_1 and W_2 are two Zariski closed sets of W. Then $V' = \varphi^{-1}(W_1) \cup \varphi^{-1}(W_2)$ and by Lemma 2.3.6, $\varphi^{-1}(W_i)$ is a Zariski closed subset of W for $i = 1, 2$. Then, as V' is irreducible, it is either equal to $\varphi^{-1}(W_1)$ or $\varphi^{-1}(W_2)$. Equivalently, $\varphi(V')$ is either equal to W_1 or W_2. Thus $\varphi(V')$ is an irreducible component of W. One proves the converse by replacing V and φ by W and φ^{-1} respectively. To conclude, we have proved that φ is a correspondence between the irreducible components of V and W. Since φ is bijective, this correspondence is one-to-one.

Let us tackle the second statement. Let V' be an irreducible component of V. According to the first item, there exists a unique irreducible component W' of W such that V' and W' are isomorphic through φ. Assuming that V' has dimension d, there exists by [Sha13, Corollary 1.5] a strictly increasing chain $V'_0 \subsetneq \ldots \subsetneq V'_d$ of non-empty irreducible algebraic subsets of V'. Thus,

$$\varphi(V'_0) \subsetneq \ldots \subsetneq \varphi(V'_d)$$

is a strictly increasing chain of irreducible algebraic subset of W' (by the first item) so that $\dim W' \geq \dim V'$ holds. The same argument for φ^{-1} leads to $\dim W' \leq \dim V'$. All in all, one finally gets $\dim W' = \dim V'$. To conclude, if V is d-equidimensional, all its irreducible components have dimension d. Then, according to the previous paragraph, all the irreducible components of W have dimension d and W is d-equidimensional as well. The converse is proved identically. □

We also have the following dual criterion, using the equivalence described above.

Proposition 2.3.9. *The polynomial map φ is an isomorphism of algebraic sets if and only if its pullback φ^* is an isomorphism of rings. In consequence, V and W are isomorphic if and only if $\mathbf{C}[V]$ and $\mathbf{C}[W]$ are (as ring).*

2.3.3 Dominant maps

Definition 2.3.10 (Dominant morphism)**.** We say that $\varphi : V \to W$ is dominant if the image of every irreducible component V' of V, is Zariski dense in W, that is $\overline{\varphi(V')}^{Z} = W$.

The following proposition characterizes algebraically the dominant morphisms.

Proposition 2.3.11. *The polynomial map $\varphi : V \to W$ dominant if and only if $\varphi^* : \mathbf{C}[W] \to \mathbf{C}[V]$ is injective. In particular, φ^* defines an isomorphic inclusion $\mathbf{C}[W] \hookrightarrow \mathbf{C}[V]$ in this case.*

The above algebraic property of dominant maps allows to prove powerful results on these maps as the following one, which will be extensively used in this document.

Proposition 2.3.12 (Theorem on the dimension of the fiber [Sha13, Theorem 1.25])**.** *Let $\varphi : V \to W$ be a dominant map, then $\dim W \leq \dim V$, and*

(i) for any $z \in W$, $\dim \varphi^{-1}(z) \geq \dim V - \dim W$;

(ii) there exists a non-empty Zariski open subset $\mathcal{O}$ of W, such that $\dim \varphi^{-1}(z) = \dim V - \dim W$ for every $z \in \mathcal{O}$.

Example 2.3.13. Let $\mathscr{H}$ be the algebraic set of $\mathbf{C}^2$ defined by $xy - 1 = 0$, then the projection $\pi : (x, y) \in \mathscr{H} \mapsto x \in \mathbf{C}$ is a dominant, but not surjective, map. Indeed, $\mathbf{C}[x]$ clearly injects into

$$\mathbf{C}[\mathscr{H}] \simeq \{f(x) + g(y), f, g \in \mathbf{C}[t]\}.$$

One checks that for $z \in \mathbf{C}^\star$, $\pi^{-1}(0)$ is zero-dimensional, but $\pi^{-1}(0)$ is empty.

2.3.4 Finite maps

We recall that, given two rings R and R' and an injective homomorphism $R \hookrightarrow R'$, we say that R' is an extension of R. We also say that $R \hookrightarrow R'$ is a ring extension.

Definition 2.3.14 (Integral extension)**.** Let $R \hookrightarrow R'$ be a ring extension, we say that an element $a \in R'$ is *integral over* R if there exists a monic polynomial $f \in R[t]$ such that $f(a) = 0$.

The extension $R \hookrightarrow R'$ is *integral*, if every element of R' is integral over R.

Remark that, if R and R' are fields, then the notion of integral extension corresponds to the one of the algebraic extension.

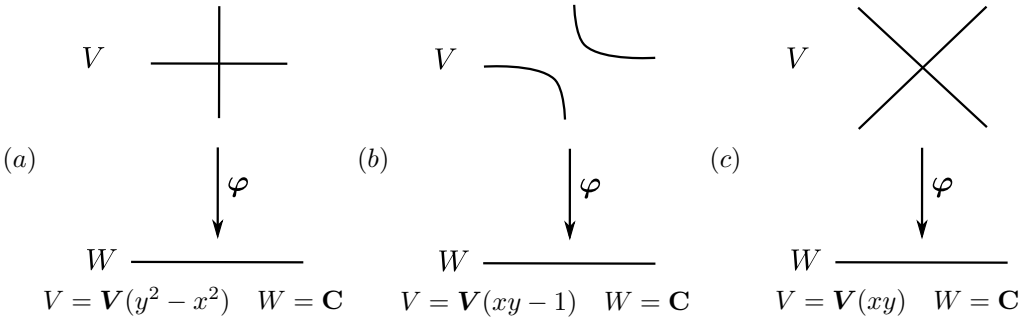
Proposition 2.3.15. *A ring extension $R \hookrightarrow R'$ is integral if and only if $R' \simeq R[a_1, \ldots, a_n]$, for integral elements $a_1, \ldots, a_n \in R'$.*

Definition 2.3.16. A polynomial map $\varphi : V \to W$ is a *finite map* if

1. φ is dominant;
2. the extension $\mathfrak{K}[Y] \hookrightarrow \mathfrak{K}[X]$ induced by the pullback φ^* of φ, is integral.

Proposition 2.3.17 ([Sha13, Chap. 1, §5.3, p.61])**.** *A finite map has finite fibers.*

Example 2.3.18. Below are three examples (in $\mathbb{R}^2$) of dominant maps, where φ is the restriction of the projection on the first variable, restricted to different algebraic sets of $\mathbb{C}^2$.



$V = \boldsymbol{V}(y^2 - x^2) \quad W = \mathbf{C}$ $V = \boldsymbol{V}(xy - 1) \quad W = \mathbf{C}$ $V = \boldsymbol{V}(xy) \quad W = \mathbf{C}$

a) Here, the map is not finite as $\varphi^{-1}(0) \cap \boldsymbol{V}(y^2 - x^2)$ is infinite. Hence, according to the contrapositive of Proposition 2.3.17, φ cannot be finite.

b) The restriction of φ has, this time, finite fibers, but is not finite, as the class of y in $\mathbf{C}[x, y]/\langle xy - 1\rangle$ is not integral over $\mathbf{C}[x]$. In particular, this proves that Proposition 2.3.17 admits no converse. One also sees that this map is not proper at 0, the notion of finite and proper maps are closely related (see e.g. the remark after [Sha13, Theorem 1.11]).

c) Finally, in this case, the restriction of φ is a finite map, as the defining equation $y^2 - x^2 = 0$ gives directly a monic annihilator, with coefficient in $\mathbf{C}[x]$ of the class of y in $\mathbf{C}[x, y]/\langle x^2 - y^2\rangle$.

Theorem 2.3.19 ([Sha13, Theorem 1.12])**.** *A finite map is surjective and Zariski closed i.e. it maps algebraic sets, to algebraic sets.*

In particular, according to Theorem 2.3.12, if $\varphi : V \to W$ is finite, then V and W have same dimension. Another consequence of the above theorem is the following one. It can be seen as a converse of Proposition 2.1.20.

Theorem 2.3.20 ([Sha13, Theorem 1.14])**.** *If $\varphi : V \to W$ is a dominant map, then $\varphi(V)$ contains a non-empty Zariski open subset of Y.*

We end this subsection with a fundamental result on the existence of finite maps.

Theorem 2.3.21 (Noether normalization [Sha13, Theorem 1.18])**.** *Let V be an algebraic set of dimension d. Then, there exist linear forms $\ell_1, \ldots, \ell_d \in \mathbf{C}[V]$ such that the map*

$$\begin{array}{rccc} \mathfrak{l}: & V & \longrightarrow & \mathbf{C}^d \\ & \boldsymbol{y} & \mapsto & (\ell_1(\boldsymbol{y}), \ldots, \ell_d(\boldsymbol{y})) \end{array}$$

is a finite map. Moreover, the coefficients of such $\ell_1, \ldots, \ell_d$ can be chosen in a non-empty Zariski open subset of $\mathbf{C}^{dn}$.

2.3.5 Rational maps

In this subsection, V is supposed to be *irreducible*.

Definition 2.3.22. The field of fraction of the coordinate ring $\mathbf{C}[V]$ is called the *field of (rational) functions* of V, and is denoted $\mathbf{C}(V)$.

Note that $\mathbf{C}(V)$ can be defined as follows. Let $\mathcal{O}_V$ (resp. M_V) be the set of $f/g \in \mathbf{C}(x_1, \ldots, x_n)$, where $g \notin \boldsymbol{I}(V)$ (resp. $f \in \boldsymbol{I}(V)$). Then

$$\mathbf{C}(V) = \mathcal{O}_V / M_V.$$

As V is irreducible, we have seen that $\mathbf{C}[V]$ is an integral domain, and then can be embedded into its field of fraction. In other words, polynomial functions are rational.

Definition 2.3.23. A rational function $\varphi \in \mathbf{C}(V)$ is *regular* at a point $\boldsymbol{y} \in V$, if there exists $f, g \in \mathbf{C}[V]$ such that $\varphi = f/g$ and $g(\boldsymbol{y}) \neq 0$. In this case, we note $\varphi(\boldsymbol{y}) = f(\boldsymbol{y})/g(\boldsymbol{y})$ the value of φ at $\boldsymbol{y}$.

Theorem 2.3.24 ([Sha13, Theorem 1.7])**.** *Let $\varphi \in \mathbf{C}(V)$. The set of points at which φ is regular is a non-empty Zariski open subset of $\boldsymbol{V}$. Moreover, if φ is regular on all V, then $\varphi \in \mathbf{C}[V]$ i.e φ is a polynomial function.*

Definition 2.3.25. A *rational map* $\boldsymbol{\varphi} : V \to W \subset \mathbf{C}^m$, is a sequence of rational functions $(\varphi_1, \ldots, \varphi_m) \subset \mathbf{C}(V)$ such that

$$\boldsymbol{\varphi}(\boldsymbol{y}) = (\varphi_1(\boldsymbol{y}), \ldots, \varphi_m(\boldsymbol{y})) \in W,$$

for all $\boldsymbol{y} \in V$ where all the φ_i's are regular. We naturally extend the notion of value and regularity of rational functions to rational maps.

The image of V under $\boldsymbol{\varphi}$ is the set

$$\boldsymbol{\varphi}(V) = \left\{ \boldsymbol{\varphi}(\boldsymbol{y}) \text{ s.t. } \boldsymbol{y} \in V \text{ and } \boldsymbol{\varphi} \text{ is regular at } \boldsymbol{y} \right\}$$

Definition 2.3.26. A rational map $\boldsymbol{\varphi} : V \to W$ is *birational* if it has an inverse rational map $\boldsymbol{\psi} : W \to V$, that is $\boldsymbol{\varphi}(V)$ and $\boldsymbol{\psi}(W)$ are Zariski dense in W and V respectively, and $\boldsymbol{\psi} \circ \boldsymbol{\varphi}$ and $\boldsymbol{\varphi} \circ \boldsymbol{\psi}$ are the identity maps, on their respective sets of regularity. In this case, we say that V and W are *birational* or *birationally equivalent*.

Proposition 2.3.27 ([Sha13, Chap. 1, §3.3, p.38])**.** *The algebraic sets V and W are birational if and only if the fields $\mathbf{C}(V)$ and $\mathbf{C}(W)$ are isomorphic over $\mathbf{C}$.*

We conclude this subsection with a general result that illustrates the nature of birational equivalence.

Theorem 2.3.28 ([Sha13, Theorem 1.8 and Remark 1.2])**.** *Let V be an irreducible algebraic set of dimension d. Then, there exist linear forms $\ell_1, \ldots, \ell_{d+1} \in \mathbf{C}[V]$ and a polynomial $f \in \mathbf{C}[z_1, \ldots z_{d+1}]$ such that the polynomial map*

$$\begin{array}{rccc} \mathfrak{l}: & V & \longrightarrow & \boldsymbol{V}(f) \subset \mathbf{C}^{d+1} \\ & \boldsymbol{y} & \mapsto & (\ell_1(\boldsymbol{y}), \ldots, \ell_{d+1}(\boldsymbol{y})) \end{array}$$

is birational. Moreover, the coefficients of such $\ell_1, \ldots, \ell_{d+1}$ can be chosen in a non-empty Zariski open subset of $\mathbf{C}^{(d+1)n}$.

This result is to be compared with Theorem 2.3.21. Theorem 2.3.28 shows that adding one more dimension, one can represent a non-empty Zariski open subset of the algebraic set as a hypersurface.

2.4 Genericity properties

This section is devoted to the notion of genericity, which will be a powerful concept for proving assumptions that will hold "most of the time", that is for "most of" the instances of a class of objects.

In this work, we will use extensively the notion of genericity and generic objects. Note that in algebraic geometry, the term "general" is sometimes preferred. However, according to [Har77, p.54]:

> *'using "generic" and "general" interchangeably is one of the more venial sins associated with the use of the word(s)'.*

In this section, we address to make precise the use of this notion and its variations.

2.4.1 Definition and examples

Definition 2.4.1 ([Har77, p.53])**.** Let $\{X_p\}_{p\in V}$ be a family of objects (sets, maps, etc.) indexed by the points of an irreducible algebraic set V of $\mathbf{C}^n$.

Hence, we say that a *generic object* $X \in \{X_p\}_{p\in V}$ satisfies a property $\mathcal{P}$, if there exists a non-empty Zariski open subset $\mathcal{O}$ of V, such that for all $p \in \mathcal{O}$, X_p satisfies $\mathcal{P}$.

In this case, we also say that an object of $\{X_p\}_{p\in V}$ *generically* satisfies $\mathcal{P}$ or, that for a *generic choice* of $p \in V$, $\mathcal{P}$ holds (for X_p).

Similarly, we will say that $\mathcal{P}$ *generically holds* on $\{X_p\}_{p\in V}$ or, when it is clear from the context, that $\mathcal{P}$ is a *genericity property*.

Note that, as seen in Proposition 2.1.20, if $\mathbf{C} = \mathbb{C}$ the field of complex numbers, then the complement of $\mathcal{O}$ has zero measure for the usual Lebesgue measure on $\mathbf{C}^m$. Moreover, Proposition 2.1.20 also says that the conjunction of finitely many genericity properties is still a genericity property.

Example 2.4.2. Let V be an algebraic set of $\mathbf{C}^n$ of dimension d, we can reformulate the previously seen theorems as follows:

a) *Theorem 2.1.38*: a generic point of V is smooth;

b) *Theorem 2.3.24*: a rational map $\varphi \in \mathbf{C}(V)$ is regular at a generic point of V;

c) *Theorem 2.3.21*: linear forms $(\ell_1, \ldots, \ell_d)$ generically form a finite map on V;

d) *Theorem 2.3.28*: linear forms $(\ell_1, \ldots, \ell_{d+1})$ generically form a birational map on V;

e) *Theorem 2.3.12*: if W is an algebraic set of dimension m and V is equidimensional, a generic fiber of a regular map $\varphi : V \to W$ has dimension $n - m$.

2.4.2 Changes of variables

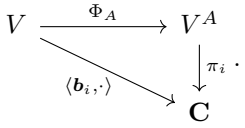
Many of the genericity results we will see in this work are about properties of canonical projections, which will be satisfied through some generic linear changes of coordinates. More precisely, let $\mathrm{GL}_n(\mathbf{C})$ be the group of invertible matrices of size n, with coefficients in $\mathbf{C}$ then we use the following notations.

Definition 2.4.3 (Change of variables)**.** Let $A \in \mathrm{GL}_n(\mathbf{C})$. For $f \in \mathbf{C}[\boldsymbol{X}]$, we note f^A the polynomial $f(AX)$, that is the resulting polynomial after the change of variables $X \mapsto AX$. Besides, we denote by V^A the image of V by the map $\Phi_A : \boldsymbol{y} \mapsto A^{-1}\boldsymbol{y}$.

The above notations are coherent since, for $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbf{C}[\boldsymbol{X}]$ and $A \in \mathrm{GL}_n(\mathbf{C})$,

$$\boldsymbol{V}(\boldsymbol{f}^A) = \Phi_A\left(\boldsymbol{V}(\boldsymbol{f})\right) = \boldsymbol{V}(\boldsymbol{f})^A.$$

Moreover, if $\pi_i : \mathbf{C}^n \to \mathbf{C}$ is the projection on the i-th coordinate, and $\boldsymbol{b}_i$ is the i-th row of A^{-1}, then the following diagram commutes:



Therefore, for a generic choice of A, the restriction $\widetilde{\pi}_i : V^A \to \mathbf{C}^n$ is a generic linear form in the variables $x_1, \ldots, x_n$. In this case, we say that the new variable $y_i = \langle \boldsymbol{b}_i, \boldsymbol{X} \rangle$ is in *generic position* with respect to V.

Note that linear changes of variables correspond to the action of the group $\mathrm{GL}_n(\mathbf{C})$ on the algebraic sets V of $\mathbf{C}^n$, and the dual action on their coordinate ring $\mathbf{C}[V]$ (see [CLO15, Chap. 7]).

We can hence reformulate the above Theorems 2.3.21 and 2.3.28, replacing the generic linear forms by a generic linear change of variable.

Corollary 2.4.4. *Let V be an equidimensional algebraic set of dimension d. Then, there exists a non-empty Zariski open subset $\mathscr{A}$ of $\mathbf{C}^{n^2}$ such that for any every $A \in \mathscr{A} \cap \mathrm{GL}_n(\mathbf{C})$ the following holds:*

1. (Theorem 2.3.21) *the restriction to V^A, of the canonical projection on $x_1, \ldots, x_d$, is a finite map;*

2. (Theorem 2.3.28) *the restriction to V^A, of the canonical projection on $x_1, \ldots, x_{d+1}$, realizes a birational map on some hypersurface of $\mathbf{C}^{d+1}$.*

In other words, if the variables $x_1, \ldots, x_d$ (resp. $x_1, \ldots, x_{d+1}$) are in generic position with respect to V^A, then the respective above statements hold on V^A. In particular, when the first statement holds, we say that $x_1, \ldots, x_d$ are in *Noether position* with respect to V^A.

2.4.3 Probabilistic and algorithmic aspects

Schwartz-Zippel's Lemma gives a way to estimate the probability for a generic property to hold, for a random selection of parameters. In other words, the probability that a randomly selected element is generic.

This justifies quantitatively the intuition that a generic property holds "most of the time".

Proposition 2.4.5 (Schwartz-Zippel lemma [DL78],[Zip79, Theorem 1] and [Sch80, Lemma 1]). *Let $\mathbf{K}$ be a field and $f \in \mathbf{K}[x_1, \ldots, x_n]$ be a non-zero polynomial of total degree at most $D \geq 0$.*

Then, for a finite $S \subset \mathbf{K}$, the number of zeros of f in S^n is at most $D \cdot (\operatorname{card} S)^{n-1}$.

Hence, for any $q \geq 1$, selecting a point $\boldsymbol{y} \in \mathbf{K}^n$, whose entries are chosen independently and uniformly in a subset of cardinality at least $2^q D$, it annihilates f with probability at most 2^{-q}. This also gives a probabilistic method for testing if a polynomial is zero with probability $1 - 2^{-q}$, using at most q evaluations.

The previous result gives then a strategy for ensuring that some genericity property $\mathcal{P}$ holds, with some prescribed success probability. Indeed, by definition, and without loss of generality, there exists some polynomial $f \in \mathbf{C}[\boldsymbol{X}]$ such that, if $f(\boldsymbol{y}) \neq 0$, then $\mathcal{P}$ holds. While computing such a polynomial f can be challenging and computationally expensive, bounding its degree can be usually done using variants of Bézout's bound (e.g. [Hei83, SS18]) or quantitative versions of transversality theorems of Subsection 2.5.2 (see e.g. [EGS23]).

Hence, given some positive integer D, according to Proposition 2.4.5, for a point $\boldsymbol{y}$ whose entries are taken randomly from a set of cardinality at least $2^q D$, property $\mathcal{P}$ holds with probability at least $1 - 2^q$. This leads to the design of randomized algorithms.

Definition 2.4.6 ([MR95, p.3]). A *randomized algorithm* is an algorithm that makes random choices during execution.

Most of the algorithms designed in this work will be randomized algorithms as their successes will rely on the successive random selection of generic parameters $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots$ in affine spaces $\mathbf{C}^{a_1}, \mathbf{C}^{a_2}, \ldots$. These represent a particular class of randomized algorithms, namely the *Monte Carlo* algorithms.

Definition 2.4.7 ([MR95, p.9]). A *Monte Carlo* algorithm is a randomized algorithm whose output can be incorrect, with bounded (typically small) probability.

Most of our algorithms will be of Monte Carlo type. Indeed, while we can make the probability of success arbitrarily close to 1, we cannot always completely guarantee the correctness of the output with reasonable complexity. Nevertheless, in cases when we can detect failure, our procedures will output fail (though not returning fail does not guarantee correctness).

2.5 Critical points

2.5.1 Definition and characterization

In this subsection, we let V be a d-equidimensional algebraic set and $\varphi : \mathbf{C}^n \to \mathbf{C}^m$ be a polynomial map.

Definition 2.5.1. Let $\boldsymbol{y} \in V$. The *differential map* (sometimes called linear part) $\mathrm{d}_{\boldsymbol{y}}\varphi$ of the restriction of φ to V at $\boldsymbol{y}$, is defined as the linear map

$$\begin{array}{rccc} \mathrm{d}_{\boldsymbol{y}}\varphi : & \mathrm{T}_{\boldsymbol{y}} V & \longrightarrow & \mathbf{C}^m \\ & \boldsymbol{u} & \mapsto & \mathrm{Jac}_{\boldsymbol{y}}(\varphi) \cdot \boldsymbol{u} \end{array}.$$

Definition 2.5.2. A point $\boldsymbol{y} \in V$ is a *critical point* of the restriction of φ to V if $\boldsymbol{y} \in \mathrm{reg}(V)$ (see Proposition 2.1.36) and $\mathrm{d}_{\boldsymbol{y}}\varphi$, is not surjective, that is

$$\mathrm{d}_{\boldsymbol{y}}\varphi(\mathrm{T}_{\boldsymbol{y}} V) \neq \mathbf{C}^m.$$

We will denote by $W^\circ(\varphi, V)$ the set of the critical points of φ on V. A point in $\mathbf{C}^m$ that is the image of a critical point is called a *critical value*, otherwise it is called a *regular value*.

Let $K(\varphi, V) = W^\circ(\varphi, V) \cup \mathrm{sing}(V)$, it is called the set of *singular points* of φ on V.

Example 2.5.3. In Figure 2.1, the real trace of the critical locus on a sphere Z is depicted for: the projection on the first coordinate π_1 (left); the polynomial map φ associated to $x_1^2 + x_2^2 \in \mathbb{R}[x_1, x_2, x_3]$ (right). Let $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_3) \in Z$. The differential of the restriction of π_1 to Z at $\boldsymbol{y}$ is the restriction of π_1 to $\mathrm{T}_{\boldsymbol{y}} Z$. The image is not $\mathbf{C}$ if and only if $\mathrm{T}_{\boldsymbol{y}} Z$ is orthogonal to the x_1-axis, so that critical points of the restriction of π to Z occur at $(\pm 1, 0, 0)$. Besides, the differential of the restriction of φ to Z at $\boldsymbol{y}$ is the restriction of $-2x_3 \cdot \pi_3$ to $\mathrm{T}_{\boldsymbol{y}} Z$. Hence, $\boldsymbol{y}$ is a critical point of the restriction of φ to Z if and only if either $\boldsymbol{y}_3 = 0$ or $\mathrm{T}_{\boldsymbol{y}} Z$ is orthogonal the x_3-axis.

The following criterion provides an algebraic characterization of critical points.

Proposition 2.5.4 (Jacobian criterion [SS17, Lemma A.2])**.** *Let $\boldsymbol{g} = (g_1, \ldots, g_p)$ be generators of $\boldsymbol{I}(V)$, then*

$$W^\circ(\varphi, V) = \left\{ \boldsymbol{y} \in V \mid \begin{array}{l} \mathrm{rank}\, \mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{g}) = n - d \\ \textit{and} \quad \mathrm{rank}\, \mathrm{Jac}_{\boldsymbol{y}}([\boldsymbol{g}, \varphi]) < n - d + m \end{array} \right\};$$

$$K(\varphi, V) = \{\boldsymbol{y} \in V \mid \mathrm{rank}\, \mathrm{Jac}_{\boldsymbol{y}}([\boldsymbol{g}, \varphi]) < n - d + m\}.$$

Let us present a direct consequence of this result, which gives a more effective criterion for the singular points of a polynomial map.

Proposition 2.5.5. *Let R be a ring, $n, m \geq 1$ be integers, and $M \in \mathcal{M}_{m,n}(R)$ an $m \times n$ matrix with coefficients in R. For any integer p such that $1 \leq p \leq \min(m, n)$, a* minor of order p *or a p-minor of M is the determinant of a $p \times p$ submatrix of M.*

Then, the matrix M has a rank less than p if and only if all its p-minors are zeros.

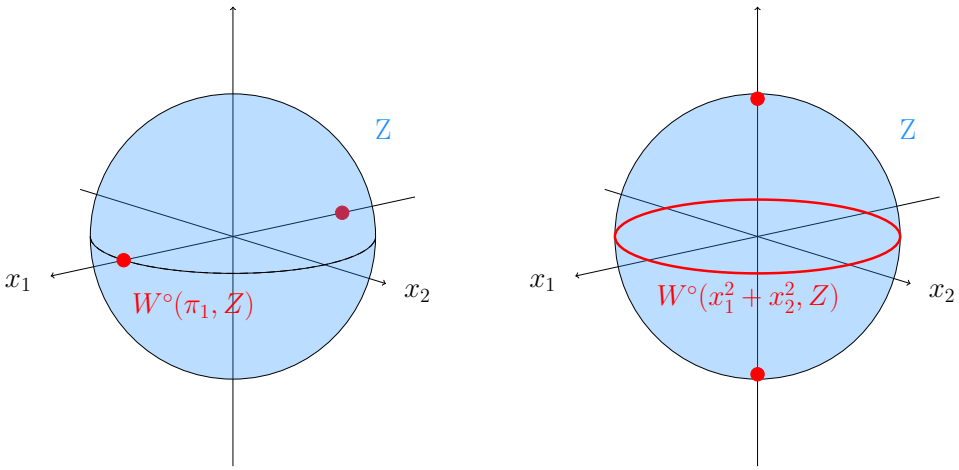


Figure 2.1. Two examples of critical loci on the sphere described in the Example 2.5.3.

Corollary 2.5.6. *The set $K(\varphi, V)$ is the algebraic subset of V defined by the vanishing of g and the $(n-d+m)$-minors of $\mathrm{Jac}([g, \varphi])$.*

Proof. One directly deduces from Proposition 2.5.4 that $K(\varphi, V)$ is exactly the intersection of V, the zero-set of g, with the set of points $y \in \mathbf{C}^n$ where $\operatorname{rank} \mathrm{Jac}_y([g, \varphi]) < n - d + m$. The latter set is the zero-set of the $(n-d+m)$-minors of $\mathrm{Jac}([g, \varphi])$. □

Example 2.5.7. If one considers $\varphi = (x_1, \ldots, x_m)$, then φ is associated to the projection π_m on the m first coordinates. Then, by Corollary 2.5.6, we have the following characterization [SS17, Lemma A.3]. The algebraic set $K(\pi_m, V)$ is the subset of V defined by the vanishing of f and the p-minors of $\mathrm{Jac}(f, m)$; where $\mathrm{Jac}(f, m)$ is the Jacobian matrix of f with respect to $(x_{m+1}, \ldots, x_n)$.

2.5.2 Transversality theorems

The notion of transversality aims at describing intersections with linear spaces. These notions are then applied to differentiable manifolds and their maps to give important results that come from these situations; we refer to [Dem00] for a complete introduction.

These concepts translate well to algebraic sets, as well as the associated theorems, which give important tools to study critical values and points. Indeed a map is not transverse to a point in its image if and only if this point is a critical value.

We start with an algebraic version of Sard's Lemma, which states that a map is transverse to most of the points in its image. An original formulation can be found in [Dem00, Theorem 3.6.7].

Theorem 2.5.8 (Algebraic Sard's Lemma [SS17, Proposition B.2.])**.** *Let V be an equidimensional algebraic set of $\mathbf{C}^n$, and let $\varphi : V \to \mathbf{C}^m$ be a polynomial map. Then the set singular values of φ is contained in a hypersurface of $\mathbf{C}^m$.*

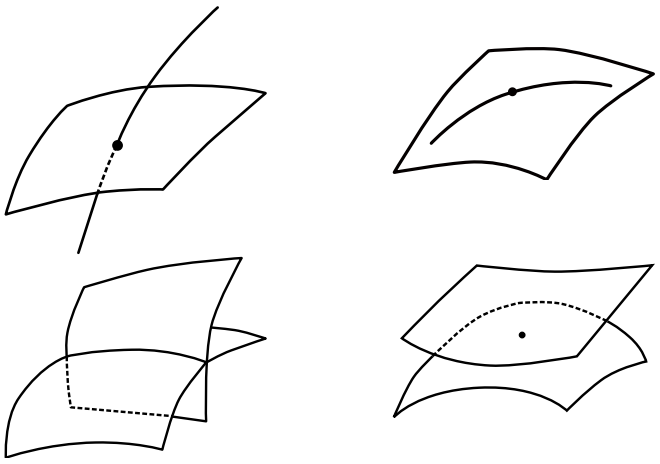


Figure 2.2. Transverse (left) and non-transverse (right) intersections of surfaces and lines in the three-dimensional space.

In other words, the complement of $\varphi(W^\circ(\varphi, V))$ is contained in a non-empty Zariski open of $\mathbf{C}^m$.

According to the previous section, another formulation of the above result is that a generic point of $\mathbf{C}^m$ is a regular value of φ.

Note that this theorem is a slight extension in affine cases of results from the more classic literature of algebraic geometry. Namely, [Mum95, Proposition 3.7], where V is supposed to be irreducible and φ dominant, and [Sha13, Theorem 2.27] where V is supposed smooth. In the latter version, it is called Second Bertini's Theorem. The first Bertini's theorem giving a criterion for the irreducibility of generic fibers of a polynomial map.

We end this paragraph with an algebraic version of Thom's weak transversality theorem, in the particular case of the transversality to a point. The original formulation, in the setting of differential manifolds, can be found in [Dem00, Theorem 3.7.4].

Theorem 2.5.9 (Algebraic Thom's weak transversality [SS17, Proposition B.3.])**.** *Let $\Phi : \mathbf{C}^n \times \mathbf{C}^d \to \mathbf{C}^m$ be a polynomial map. Assume that there exists a Zariski open subset $\mathcal{O}$ of $\mathbf{C}^n$ such that 0 is a regular value of the restriction of Φ to $\mathcal{O} \times \mathbf{C}^d$. Then, there exists a non-empty Zariski open subset $\mathcal{U}$ of $\mathbf{C}^d$ such that for all $\vartheta \in \mathcal{U}$, 0 is a regular value of $\Phi(\cdot, \vartheta)$ on $\mathcal{O}$.*

These two theorems are fundamental for proving genericity assumptions on algebraic sets. In particular, many of the genericity results of the next subsection can be proved using transversality considerations.

2.6 Polar varieties

We have defined and characterized in the previous section the set of critical points of polynomials maps. As in the theory of differential manifolds, these critical loci are of importance in algebraic geometry and their real counterpart that we will study in Chapter 4. Indeed the data of well-chosen critical loci allows one to characterize and describe the underlying (real) algebraic set. This motivated the introduction of *polar varieties*.

Polar varieties are critical loci of the canonical projections $\pi_i : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i)$, for $1 \leq i \leq n$. The general study of polar loci goes back to Severi [Sev02, Sev32], whose ideas were taken up by [Tod38] to define characteristic classes, and later developed by [Por71, Poh65, Tei82, BGHP04, BGHP05, BGH$^+$10, SS03a, BGHM01, SS17], among others. See [Pie78, Tei88, Bra00, BGH$^+$10] for a more extensive history of polar varieties.

2.6.1 Definition and first properties

In this work, we consider slightly more general objects that are critical loci of arbitrary graded polynomial maps. Following the terminology introduced in [BGHP04, BGHP05, BGH$^+$10], we call them *generalized polar varieties*.

In the following, let V be a d-equidimensional algebraic set of $\mathbf{C}^n$ and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n) \subset \mathbf{C}[\boldsymbol{X}]$. For $1 \leq i \leq n$, we define the map

$$\begin{array}{rccc} \boldsymbol{\varphi}_i : & \mathbf{C}^n & \longrightarrow & \mathbf{C}^i \\ & \boldsymbol{y} & \mapsto & (\varphi_1(\boldsymbol{y}), \ldots, \varphi_i(\boldsymbol{y})) \end{array} \tag{2.1}$$

Following the ideas of [BGHP04, BGHP05, BGH$^+$10] we denote by similarly $W(\boldsymbol{\varphi}_i, V)$ the i-th *generalized polar variety* defined as the Zariski closure of the critical locus $W^\circ(\boldsymbol{\varphi}_i, V)$ of the restriction of $\boldsymbol{\varphi}_i$ to V.

Definition 2.6.1 (Generalized polar variety)**.** Let $1 \leq i \leq n$, we denote by $W(\boldsymbol{\varphi}_i, V)$ the *i-th generalized polar variety* defined as the Zariski closure of the critical locus $W^\circ(\boldsymbol{\varphi}_i, V)$ (then called the *open polar variety*) of the restriction of $\boldsymbol{\varphi}_i$ to V. In particular, $W(\pi_i, V)$ is the (classic) i-th polar variety.

Remark that by minimality of the Zariski closure,

$$W^\circ(\boldsymbol{\varphi}_i, V) \subset W(\boldsymbol{\varphi}_i, V) \subset K(\boldsymbol{\varphi}_i, V) \subset V.$$

Hence $K(\boldsymbol{\varphi}_i, V) = W(\boldsymbol{\varphi}_i, V) \cup \mathrm{sing}(V)$ but the union is not necessarily disjoint.

The proposition is a direct generalization of [SS17, Lemma A.4-5], using Corollary 2.5.6.

Proposition 2.6.2. *Let $1 \leq j \leq i \leq n$, then*

(i) $W^\circ(\boldsymbol{\varphi}_j, V) \subset W^\circ(\boldsymbol{\varphi}_i, V)$;

(ii) $W^\circ(\boldsymbol{\varphi}_j, V) \subset W(\boldsymbol{\varphi}_j, V) \subset K(\boldsymbol{\varphi}_j, W(\boldsymbol{\varphi}_i, V))$, *if $W(\boldsymbol{\varphi}_i, V)$ is equidimensional.*

2.6.2 Properties of generic classic polar varieties

As mentioned in Subsection 2.4.2, polar loci of generic linear forms can be equivalently considered as classic polar varieties on algebraic sets, on which a generic linear change of variables has been performed. The latter are called *generic polar varieties*. In the following, we give some important properties, from the literature, that generic (classic) polar varieties satisfy.

In the following, we consider a d-equidimensional algebraic set $V \subset \mathbf{C}^n$ with *finitely many* singular points i.e. such that $\mathrm{sing}(V)$ is finite. We first present a generalization of the Noether normalization for polar varieties.

Theorem 2.6.3 (Noether position for polar varieties [SS03a, Proposition 2]). *For each $1 \leq i \leq d$, there exists a non-empty Zariski open subset $\mathscr{A}_i$ of $\mathbf{C}^{n^2}$, such that for every $A \in \mathscr{A} \cap \mathrm{GL}_n(\mathbf{C})$, the following holds. The algebraic set $W(\pi_i, V^A)$ has dimension at most $i-1$, and the restriction of π_{i-1} to $W(\pi_i, V^A)$ is finite. In other words, the variables $x_1, \ldots, x_{i-1}$ are in Noether position with respect to $W(\pi_i, V^A)$.*

The following theorem outlines the expected regularity properties of generic polar varieties.

Theorem 2.6.4 (Regularity of generic polar varieties [SS17, Proposition 3.4]). *For each $1 \leq i \leq d$, there exists a non-empty Zariski open subset $\mathscr{A}_i$ of $\mathbf{C}^{n^2}$, such that for every $A \in \mathscr{A} \cap \mathrm{GL}_n(\mathbf{C})$, the following holds. Let $W_i = W(\pi_i, V^A)$, either it is empty or*

(i) W_i is equidimensional of dimension $i-1$ and,

(ii) if $i \leq (d+3)/2$, then $\mathrm{sing}(W_i) \subset \mathrm{sing}(V^A)$.

Remark that the condition $i \leq (d+3)/2$ is a necessary one, as in [BGH+10, Section 3], the authors exhibit a general method to construct singular higher dimensional polar varieties from smooth algebraic sets. However, this condition can be relaxed in the particular case of hypersurfaces.

Proposition 2.6.5. *Let $f \in \mathbf{C}[\boldsymbol{X}]$ be a non-constant square-free polynomial, then there exists a non-empty Zariski open subset $\mathscr{A}_i$ of $\mathbf{C}^{n^2}$, such that for every $A \in \mathscr{A} \cap \mathrm{GL}_n(\mathbf{C})$,*

$$\mathrm{sing}(W(\pi_i, \boldsymbol{V}(f^A))) \subset \mathrm{sing}(\boldsymbol{V}(f^A)).$$

We end this paragraph by considering critical loci on polar varieties.

Theorem 2.6.6 (Critical points on generic polar varieties [SS17, Proposition 3.5]). *For each $1 \leq i \leq (d+3)/2$, there exists a non-empty Zariski open subset $\mathscr{A}_i$ of $\mathbf{C}^{n^2}$, such that for every $A \in \mathscr{A} \cap \mathrm{GL}_n(\mathbf{C})$, the following holds. Let $W_i = W(\pi_i, V^A)$, it is either empty or equidimensional of dimension $i-1$ and $K(\pi_1, W_i)$ is finite.*

In Chapter 7, we prove that the same results hold for generic generalized polar varieties, in the sense that one can add a generic linear form to the given polynomial map. Namely, the generalizations of Theorems 2.6.3, 2.6.4 and 2.6.5 correspond to respectively Propositions 7.2.3,7.2.13 and 7.2.14. These properties allow us to adapt the proofs and algorithms of [SS11, SS17] to a more general setting.

3 Computational algebraic geometry

In this chapter, we address the problem of computing objects of algebraic geometry that we introduced in the previous chapter. As shown, geometric computations can be reduced to algebraic manipulations on polynomials and ideals they generate. Hence, our focus shifts toward algorithmic procedures for handling these objects, including the exploration of approaches for their efficient representation.

More precisely, Section 3.1 addresses computational complexity, providing the framework for evaluating algorithmic performance and comparing different strategies. Furthermore, Section 3.2 delves into various methodologies and associated properties related to polynomial representation. With these polynomial representations established, the exploration extends to suitable representations for algebraic sets. A first approach is presented in Section 3.3, introducing Gröbner bases to provide a convenient representation of the defining ideals of algebraic sets. We also discuss relevant algorithmic techniques. Finally, Section 3.4 adopts a geometric perspective to introduce rational parametrizations. In this section, we survey different definitions and computational approaches related to this concept.

3.1 Computational complexity

We start with considerations on the ground settings of our study, defining the elementary operations and addressing computational cost quantification.

Computable field. In the following, we consider a *computable* field $\mathbf{Q}$ that is an algebraic structure where one can represent elements and has algorithms for computing and operating tests on them. Therefore, in this work, we will not go further into the details of the manipulation of the elements of $\mathbf{Q}$. As we will mainly work in characteristic 0, the field of rational numbers $\mathbb{Q}$ will be the main example for such a field $\mathbf{Q}$. However, for other applications or efficient computations over $\mathbb{Q}$ through the Chinese Remainder theorem, finite fields $\mathbb{F}_q$ are widely used.

Complexity. The computational cost of the algorithms is measured through the notion of complexity. Fixing a computational model in $\mathbf{Q}$, the available operations and their unit cost we define

- the *time complexity* measuring the sum of the unit costs of the elementary operations performed by the algorithm;

- the *space complexity* measuring the amount of memory used during the execution of the algorithm.

For the sake of completeness, we mention that the *Random Access Machine* computational model will be the one considered in this work. We refer to [AH74] for further details on these aspects. Further, we will not deal with space complexity and mainly focus on making algorithms terminate in a tractable amount of time. This point of view deserves to be discussed since algebraic computations on multivariate polynomials can require a significant amount of RAM. However, this falls behind the scope of this work.

Instead, we will distinguish the two following types of time complexities in this document.

- The *arithmetic complexity* which is the total number of arithmetic operations in $\mathbf{Q}$. This complexity is relevant when the cost of the arithmetic operations is preponderant and each of them is essentially constant. Hence, the parameters of such complexities will be the size of the input objects (degree, dimension, etc.), but we will ignore the one of the elements of the base field. This complexity suits well to finite fields, but not always for rationals as the cost of arithmetic operations grows with the size of the numbers.

  However, arithmetic complexity bounds can give bounds on the degree and the height[1] of the polynomials involved in the computation as shown in e.g. [SS18]. Hence, these bounds give first estimates on the expected bit complexity that we introduce below.

- The *bit complexity* (or Boolean complexity), is designed for computations involving integers (and then rationals) as it measures the number of bit operations performed by the algorithm. More precisely, arithmetic operations on $\mathbb{Z}$ are decomposed into modular computations on B-words integers, that are represented in B-bit chunks. Hence, the bitsize $\log_2(a)$ of the input integers a will influence the total cost according to this complexity.

Usually, arithmetic complexity will be the first goal of any complexity estimate of computer algebra algorithms as it is easier to conduct. Moreover, as we mentioned, many implementations of procedures rely on modular computation which makes the arithmetic complexity relevant in some sense. For an overview of this theory see [BCS97]. As we meet most of the time situations where polynomials have integer coefficients (up to multiply by some constant integer), we eventually target the bit-complexity, which reflects better the real performances.

Also, we will always consider the *worst-case* complexity, that is the maximum of the complexity of the executions of an algorithm for all possible inputs of a fixed size.

Asymptotic complexity. Recall that a partial function is a function that does not have to be defined for every value. We refer to [GG13, §25.7] for this paragraph, and [GKP94] for a complete discussion of these notions.

[1] The height of a non-zero polynomial f is the maximum of the bitsizes of v and the coefficients of vf, where $v \in \mathbb{N}$ is the minimal common denominator non-zero coefficients of f.

Definition 3.1.1 (Big Oh)**.** Let $p \geq 1$ and $g : \mathbb{N}^p \to \mathbb{R}$ be a partial function. We denote by $O(g)$ the set of all partial function $f : \mathbb{N}^p \to \mathbb{R}$ for which there exist $N, C \in \mathbb{N}$ such that for all $k_1, \ldots, k_p \geq N$, both f and g are defined at $(k_1, \ldots, k_p)$ and

$$|f(k_1, \ldots, k_p)| \leq C\,|g(k_1, \ldots, k_p)|\,.$$

We will use the following common abuse of notation. For any $h : \mathbb{N} \times \mathbb{R} \to \mathbf{R}$, $f(n) = h(n, O(g(n)))$ will stand for $f = h(n, k(n))$, with $k \in O(g)$.

The Big-Oh notation allows to describe the asymptotic behavior of quantities, up to some bounded variations. It will be extensively used for describing the asymptotic complexity of algorithms, when the size of the inputs become "large".

Example 3.1.2. According to the algorithm of Schönhage & Strassen [GG13, Theorem 8.24], two integers of maximum bit size τ can be multiplied in bit complexity $O(\tau \log \tau \log\log \tau)$.

Remark 3.1.3. In this thesis, we will often meet complexities with big Oh in exponents, as most of the complexities in real algebraic geometry are at least exponential in the number of variables (see Chapter 5). Precautions have to be taken with exponentiation of O, indeed

$$e^{2n} = e^{O(n)} \qquad \text{but} \qquad e^{2n} = (e^n)^2 \neq O(e^n).$$

The constant hidden in the O influence strongly the rate of growth when being in the exponent. In Chapter 7 we will see a situation when having an explicit constant is crucial.

In some situations, we might want to describe an even more big picture of the asymptotic behavior of algorithms. For instance, the algorithm of Example 3.1.2 has complexity essentially linear. The soft Oh notation, introduced by [BLS88], aims to make the previous sentence precise.

Definition 3.1.4 (Soft Oh)**.** Let $p \geq 1$ and $g : \mathbb{N}^p \to \mathbb{R}$ be a partial function. We denote by $\widetilde{O}(g)$ the set

$$O\left(g(n) \cdot (\log_2(3 + g(n))^{O(1)})\right).$$

Hence the soft Oh characterizes the class of functions that shares the same asymptotic behavior, up to some multiplicative power of logarithms. Note that the constant 3 is only here to make the logarithm greater than 1.

Definition 3.1.5 (Orders of growth)**.** Given a univariate polynomial $f \in \mathbf{R}[x]$, the rate of growths can be classified as shown in the table below. In the row labeled "Time", to provide intuitive context, we present an order of magnitude estimation for the time that an algorithm within this category would require for an input size of $n = 20$, with unit operations taking approximately 10^{-8} seconds.

Growth	constant	logarithmic	linear	soft linear	polynomial	singly expo.	doubly expo.
Complexity	$O(1)$	$\widetilde{O}(1)$	$O(n)$	$\widetilde{O}(n)$	$O(n^{f(n)})$	$O(2^{f(n)})$	$O(2^{2^{f(n)}})$
Time ($n = 20$)	10^{-8} s	10^{-8} s	10^{-7} s	10^{-7} s	10^{-4} s	10^{-2} s	$> 10^{10^6}$ s
Example	Memory access	Binary search	Mod add.	Fast mult.	Mat mult.	SAT solving	Quantifier elim.

We end by defining two categories of algorithms, that can be considered as the ones of (nearly)-optimal complexity.

Definition 3.1.6 (Optimal algorithms)**.** If N is the sum of the size of the input and the output, an algorithm will be called *optimal* – resp. *nearly-optimal* – when its complexity is bounded by $O(N)$ – resp. $\widetilde{O}((N))$.

3.2 Polynomial representations

In order to manipulate multivariate polynomials, one needs to be able to represent them efficiently. Hence, appropriate *data structures* need to be defined, depending on the context.

3.2.1 Dense representation

Let $f \in \mathbf{Q}[x_1, \ldots, x_n]$ be a multivariate polynomial with coefficients in $\mathbf{Q}$, of total degree D. By definition f can be written as a sum of monomials as follows

$$f = \sum_{\substack{i_1,\ldots,i_n \geq 0 \\ i_1+\cdots+i_n \leq D}} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

where $a_{i_1,\ldots,i_n} \neq 0$ for at least one of the $(i_1, \ldots, i_n)$ such that $i_1 + \ldots + i_n = D$, provided that $f \neq 0$. Representing f as the complete array of the $a_{i_1,\ldots,i_n}$'s and the associated multi-indices $(i_1, \ldots, i_n)$, is called the *dense representation*. It is the most direct way to represent polynomials in a computer and it is optimal for generic polynomials. The *length* of such representation is the number of coefficients in the array.

Proposition 3.2.1. *The dense representation of a polynomial $f \in \mathbf{Q}[x_1, \ldots, x_n]$ of total degree $D \geq 0$ has length*

$$\binom{n+D}{D}.$$

Factorization and Gcd computations of multivariate polynomials can be done in random polynomial time in the length of their dense representations. However, according to the above proposition, this length grows *exponentially* in the number of variables, and more importantly in the degree of the polynomial.

Example 3.2.2 ([GG13, §16.6])**.** Let the Fermat polynomial $x_1^3 + x_2^3 - x_3^3 \in \mathbf{Q}[x_1, x_2, x_3]$, it has total degree 3, and its dense representation reads

$$\begin{aligned} f = {} & 1 \cdot x_1^3 + 0 \cdot x_1^2 x_2 + 0 \cdot x_1^2 x_3 + 0 \cdot x_1^2 + 0 \cdot x_1 x_2^2 + 0 \cdot x_1 x_2 x_3 + 0 \cdot x_1 x_3^2 \\ & + 0 \cdot x_1 x_2 + 0 \cdot x_1 x_3 + 0 \cdot x_1 + 1 \cdot x_2^3 + 0 \cdot x_2^2 x_3 + 0 \cdot x_2^2 \\ & + 0 \cdot x_2 x_3^2 + 0 \cdot x_2 x_3 + 0 \cdot x_2 + (-1) \cdot x_3^3 + 0 \cdot x_3^2 + 0 \cdot x_3 + 0 \cdot 1. \end{aligned}$$

As seen in the above example, even if polynomials have generically as many non-zero coefficients as the length of their dense representation (they are called *dense polynomials*), this is not the case for some of the ones we can meet.

3.2.2 Sparse representation

As seen in the previous subsection, one can also represent a polynomial by the list of its *non-zero* coefficients, together with the associated monomial. More precisely, given a polynomial $f \in \mathbf{Q}[x_1, \ldots, x_n]$ of total degree D, its support $\mathrm{supp}(f)$ is the finite subset of the $(i_1, \ldots, i_n) \in \mathbb{N}^n$ for which the coefficient of f associated to $x^{i_1} \cdots x^{i_n}$ is non-zero. Hence, the sparse representation of f consists in the data of $\mathrm{supp}(f)$ and the array of the $a_{i_1,\ldots,i_n}$'s for each $(i_1, \ldots, i_n) \in \mathrm{supp}(f)$, so that

$$f = \sum_{(i_1,\ldots,i_n)\in \mathrm{supp}(f)} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

The advantage of such a representation is that it optimizes the stored data with respect to the polynomial sparsity. As seen in Example 3.2.2, sparse representation is the natural mathematical notation and many natural problems coming from applications tend to be sparse (see e.g. [GG13, §24.4] or [CPS+22, §5]).

However, no known algorithms can factor sparse polynomials in a time polynomial in the length of the representation (that is the number of non-zero terms). Moreover, the output size of such algorithms tends to uncontrollably grow, sometimes more than polynomial in the input size (addition and multiplication might have output size which is respectively double and quadratic in the input size). We refer to [Roc18] for an overview of what is possible or not with sparse polynomials.

3.2.3 Straight-line programs

In the previous subsection, we have seen that when trying to reduce the input size using sparse representations, one loses efficiency (complexity and output size) of the algorithm in the length of the description. According to [GG13, p. 464]:

> "The key to get over this hurdle is to consider even more concise representations".

The idea is to represent polynomials as *arithmetic circuits* computing a polynomial $f \in \mathbf{Q}[x_1, \ldots, x_n]$ from the variables $x_1, \ldots, x_n$ and the constants of $\mathbf{Q}$, using only the arithmetic operations $+, \times$ and $-$. More precisely, these circuits are directed acyclic graphs, whose input are the variables and the constants of $\mathbf{Q}$, the outputs are the polynomials computed and the internal nodes represent arithmetic operations (except division) of their parent nodes. The value of a polynomial can be computed by evaluating its arithmetic circuit, on input the values of the variables.

Arithmetic circuits can also be represented as *straight-line programs*. Formally, a straight-line program Γ, computing polynomials in $\mathbf{Q}[x_1, \ldots, x_n]$, is a finite sequence $\Gamma = (\gamma_1, \ldots, \gamma_E)$ such that for all $1 \leq i \leq E$, one of the two following holds:

- $\gamma_i = \lambda_i$ with $\lambda_i \in \mathbf{Q}$;
- $\gamma_i = (\mathsf{op}_i, a_i, b_i)$ with $\mathsf{op}_i \in \{+, -, \times\}$ and $-n + 1 \leq a_i, b_i < i$.

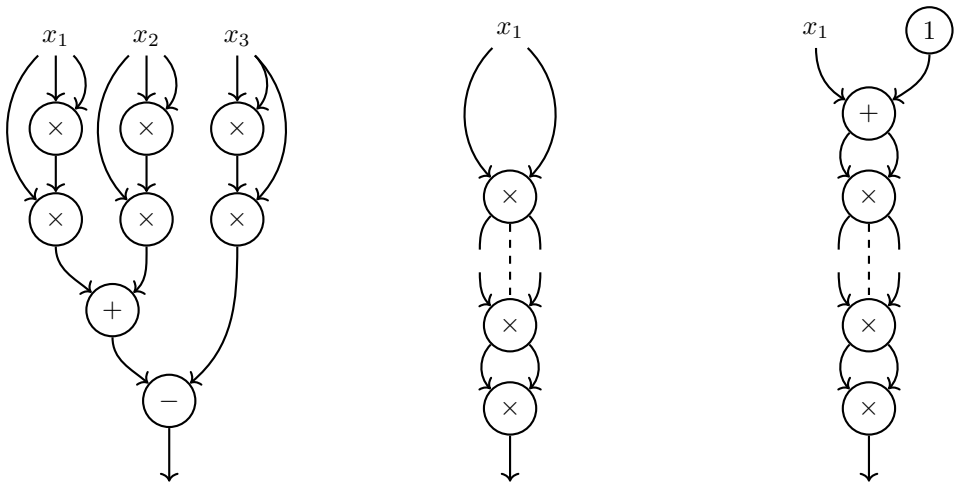


Figure 3.1. Arithmetic circuits computing in $\mathbf{Q}[x_1, x_2, x_3]$ the polynomials, from left to right: $x_1^3 + x_2^3 - x_3^3$, $x_1^{2^m}$ and $(x_1 + 1)^{2^m}$.

To Γ we associate polynomials $G_{-n+1}, \ldots, G_E$ such that $G_i = x_{i+n}$ for $-n + 1 \leq i \leq 0$, and for $1 \leq i \leq E$:

- if $\gamma_i = \lambda_i \in \mathbf{Q}$ then $G_i = \lambda_i$;
- if $\gamma_i = (\mathsf{op}_i, a_i, b_i)$ then $G_i = G_{a_i}\ \mathsf{op}_i\ G_{b_i}$.

Then we say that Γ computes some polynomials $f_1, \ldots, f_c \in \mathbf{Q}[\boldsymbol{X}]$ if $\{f_1, \ldots, f_c\} \subset \{G_{-n+1}, \ldots, G_E\}$. The integer E is the *length* of the straight-line program Γ. By convention, we note $\Gamma^0 = (0)$ the straight-line program of length 1 that computes the zero polynomial.

Example 3.2.3. We give an illustrating example presented in [Kri02, Section 1.1]. For $m \in \mathbb{N}^*$, a straight-line program computing x^{2^m} in $\mathbf{Q}[x]$ is given by taking

$$\begin{cases} \gamma_1 &= (\times, 1, 1) \\ \gamma_2 &= (\times, 1, 1) \\ &\vdots \\ \gamma_m &= (\times, m, m) \end{cases}$$

where we associate $G_1 = x^2$ to γ_1, $G_2 = G_1^2 = x^4$ to γ_2 and so on with $G_m = G_{m-1}^2 = x^{2^m}$ which is associated to γ_m. Such a program has length m, while the dense and sparse representations of x^{2^m} have respective length $2^m + 1$ and 1. But remark that a straight-line program computing $(x + 1)^{2^m}$ can be obtained by inserting at the beginning of the straight-line program $(1, (+, 1, 0))$, which computes $x + 1$. The latter modification increments the length by two, while both dense and sparse representations have now maximal length 2^m.

As seen in Figure 3.1 and Example 3.2.3, straight-line programs allow good input size for various polynomials, while both dense and sparse representations fail to have a compact

expression. Moreover, contrary to sparse representations, there exist algorithm computing factorizations [Kal85, Kal89] and gcd's [Kal88] in random polynomial-time in the length of the input straight-line programs. In addition, their nice behavior with respect to linear changes of variables, make it used as input in many algorithms for solving polynomial systems [Kri02, GHM+98, GHMP97, GHMP95, GLS01, Lec00, SS17].

It is worth noting that computing with such representations is not restrictive since any polynomial of degree D in n variables, can be computed with a straight-line program of length $O(D^n)$ by simply evaluating and summing all its monomials.

3.3 Gröbner bases

Now we have different representations for polynomials defining the algebraic sets, we need to compute efficient and powerful representations of their ideals of definition. To this end, we introduce in this section Gröbner bases, their properties and discuss their computation. We will denote by $\mathbf{Q}$ a field and by $\mathbf{C}$ its algebraic closure.

3.3.1 Monomial orders

Definition 3.3.1. A *monomial* is a polynomial of the form $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. We note $|\alpha| = \alpha_1 + \cdots + \alpha_n$ the *total degree* of x^α.

Definition 3.3.2. A *monomial order* on $\mathbf{Q}[\boldsymbol{X}]$, is an order $\succ$ on the monomial $x^\alpha \in \mathbf{Q}[\boldsymbol{X}]$ which satisfies the following assumptions:

(i) $\succ$ is a total order i.e. $x^\beta \succ x^\alpha$ or $x^\alpha \succ x^\beta$ for any $\alpha, \beta \in \mathbb{N}^n$;

(ii) $\succ$ is compatible with multiplication: if $x^\beta \succ x^\alpha$ then $x^{\beta+\gamma} \succ x^{\alpha+\gamma}$, for any $\alpha, \beta, \gamma \in \mathbb{N}^n$;

(iii) $x^\alpha \succ x^0$ for all $\alpha \in \mathbb{N}^n - \{0, \ldots, 0\}$.

Such an order does not depend on the base field $\mathbf{Q}$ as it is induced by an order on the multi-exponents in $\mathbb{N}^n$.

In the following, and without further precision, we denote by $\succ$ any monomial order on $\mathbf{Q}[\boldsymbol{X}]$. The three above assumptions imply in particular that $\succ$ is a well-order, that is every non-empty subset of monomials of $\mathbf{Q}[\boldsymbol{X}]$ has a smallest element (see [Eis95, Lemma 15.2] or [CLO15, Chap. 2, §2,Lemma 2]. Hence, given a polynomial $f \in \mathbf{Q}[\boldsymbol{X}]$, $\succ$ orders its finitely many monomials in such a way that there is a smallest and a largest term in f.

Definition 3.3.3. Let $a_\alpha x^\alpha$ be the largest term of $f \in \mathbf{Q}[\boldsymbol{X}]$, then $a_\alpha x^\alpha$ is called the *leading term* of f and is denoted by $\mathrm{lt}_\succ(f)$. Moreover a_α and x^α will be called the *leading coefficient* $\mathrm{lc}_\succ(f)$ and the *leading monomial* $\mathrm{lm}_\succ(f)$.

Example 3.3.4. Let $\alpha, \beta \in \mathbb{N}^n$. We list below the most frequently monomial orders encountered in the literature. We will discuss their interest in later in this section.

a) *(Lexicographic order)*: $x^\alpha \succ_{lex} x^\beta$ if if the *leftmost* nonzero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n$ is *positive*;

b) *(Graded Lex Order)*: $x^\alpha \succ_{grlex} x^\beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $x^\alpha \succ_{lex} x^\beta$

c) *(Graded Reverse Lex Order)*: $x^\alpha \succ_{grevlex} x^\beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the *rightmost* nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is *negative*;

The following theorem is a generalization of the Euclidean division in the multivariate setting. The price of such a generalization is the loss of uniqueness.

Theorem 3.3.5 (Polynomial division [CLO15, Chap. 2, §3, Theorem 3])**.** *Let $(f_1, \dots, f_p)$ be an ordered sequence of non-zero polynomials in $\mathbf{Q}[\boldsymbol{X}]$. For all $f \in \mathbf{Q}[\boldsymbol{X}]$, there exists polynomials $(q_1, \dots, q_p, r)$ in $\mathbf{Q}[\boldsymbol{X}]$ such that*

$$f = q_1 f_1 + \cdots + q_p f_p + r,$$

and such that the following holds:

1. *for all $1 \leq i \leq r$, either $q_i f_i = 0$ or $\mathrm{lt}_\succ(f) \succeq \mathrm{lt}_\succ(q_i f_i)$;*
2. *either $r = 0$ or r is a $\mathbf{Q}$-linear combination of monomials, none of which is divisible by any of $\mathrm{lt}_\succ(f_1), \dots, \mathrm{lt}_\succ(f_p)$.*

Note that the proof of such a result (e.g. in [CLO15]) relies on an explicit algorithm for computing such q_i's and r, known as polynomial division algorithm. According to the following example, the output polynomials $(q_1, \dots, q_p, r)$ depend strongly on the order of the polynomials in $(f_1, \dots, f_p)$.

Example 3.3.6. Let $f = x_1x_2^2 - x_1$, $f_1 = x_1x_2 - 1$ and $f_2 = x_2^2 - 1$, we consider the lexicographic order $x_1 \succ_{lex} x_2$. Then the divisions of f by (f_1, f_2) and by (f_2, f_1) give respectively

$$\begin{aligned} & x_1x_2^2 - x_1 = x_2 \cdot (x_1x_2 - 1) + 0 \cdot (x_2^2 - 1) + (-x_1 + x_2) \\ \text{and} \quad & x_1x_2^2 - x_1 = x_1 \cdot (x_2^2 - 1) + 0 \cdot (x_1x_2 - 1) + 0. \end{aligned}$$

In particular, one sees from the second division, that $f \in \langle f_1, f_2 \rangle$, while it is not clear from the first one.

According to Example 3.3.6, one cannot decide the membership of a polynomial to an ideal from the division by any set of generators of this ideal. Gröbner bases have been introduced to solve this problem.

3.3.2 Gröbner bases: definition and properties

Definition 3.3.7 (Gröbner basis [CLO15, Chap. 2, §5, Definition 5 and §7, Definition 4])**.** A finite subset $G = \{g_1, \dots, g_p\}$ of an ideal $\{0\} \neq I \subset \mathbf{Q}[\boldsymbol{X}]$, is said to be a *$\succ$-Gröbner basis* (or *$\succ$-standard basis*) if

$$\langle \mathrm{lt}_\succ(g_1), \dots, \mathrm{lt}_\succ(g_p) \rangle = \langle \mathrm{lt}_\succ(I) \rangle ,$$

where $\mathrm{lt}_\succ(I) = \{\mathrm{lt}_\succ(f), f \in I\}$. Moreover, we set $\emptyset$ to be the Gröbner basis of $\{0\}$, using the convention $\langle\emptyset\rangle = \{0\}$.

Moreover, G is called a *reduced $\succ$-Gröbner basis* if it satisfies the following:

(i) $\mathrm{lc}_\succ(g) = 1$ for all $g \in G$;

(ii) for all $g \in G$, no monomial of g lies in $\langle \mathrm{lt}_\succ(G - \{g\})\rangle$.

When it is clear from the context, we will omit the mention of the monomial order in consideration. The following theorem ensures the non-vacuity of this definition as well as the uniqueness of reduced Gröbner bases.

Theorem 3.3.8 (Existence and uniqueness [CLO15, Chap. 2, §7, Theorem 5])**.** *Every non-zero ideal $I \subset \mathbf{Q}[\boldsymbol{X}]$ has a* unique *reduced Gröbner basis.*

Even if the uniqueness is not preserved, the existence of not necessarily reduced Gröbner bases is of course guaranteed as well. Not that Theorem 3.3.8 reduce the problem of deciding the equality of ideals to the one of computing two reduced Gröbner bases.

We can now start to give the properties of such bases, the first proposition justifying the generating aspect behind the "basis" denomination.

Proposition 3.3.9 ([CLO15, Chap. 2, §5, Corollary 6])**.** *A Gröbner basis of an ideal constitutes a generating set.*

We now state the exceptional properties of these sets of generators, regarding the polynomial division. This justifies the uniqueness aspect associated to the "basis" denomination. In particular, it answers the problem emphasized in Example 3.3.6 and the following remarks.

Proposition 3.3.10 ([CLO15, Chap. 2, §6, Proposition 1])**.** *Let G be a Gröbner basis of an ideal $I \subset \mathbf{Q}[\boldsymbol{X}]$. Then, the remainder of the polynomial division (from Theorem 3.3.5) of any $f \in \mathbf{Q}[\boldsymbol{X}]$ by the elements of G (regardless of their order) is unique. It is called the* normal form *of f with respect to G and is denoted by $\mathrm{NF}_G(f)$.*

In particular, it solves the ideal membership problem mentioned above, as follows.

Corollary 3.3.11 ([CLO15, Chap. 2, §6, Corollary 2])**.** *Let G be a Gröbner basis of an ideal $I \subset \mathbf{Q}[\boldsymbol{X}]$ and $f \in \mathbf{Q}[\boldsymbol{X}]$. Then, $f \in I$ if and only if $\mathrm{NF}_G(f) = 0$.*

3.3.3 Application to geometric computations

We now describe the geometric operations that can be performed using Gröbner bases for the ideal of definition of the algebraic sets in consideration. According to the correspondence emphasized in Chapter 2, the ideal theoretic operations that can be performed using Gröbner bases have a geometric counterpart for algebraic sets.

A fundamental property of Gröbner is their notably nice behavior with elimination, which corresponds to projection of algebraic sets as shown by the following theorem. Computing the projection of algebraic sets is an important problem in algebraic geometry e.g. for computing critical values of polynomial maps as we will see in Chapter 5.

Theorem 3.3.12 ([CLO15, Chap. 3, §2, Theorem 2]). *Let $V \subset \mathbf{C}^n$ be an algebraic set and $\pi_i : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i)$ be the canonical projection on the first i variables. Then*

$$\boldsymbol{I}\Big(\pi_i(V)\Big) = \boldsymbol{I}(V) \cap \mathbf{C}[x_1, \ldots, x_i].$$

It is worth noting that, such results for projection can be extended to any polynomial maps. Indeed, for any polynomial $\varphi \in \mathbf{C}[\boldsymbol{X}]$, one can consider the algebraic set Z of $\mathbf{C}^{n+1}$ made of the points $(\boldsymbol{y}, t)$ such that $\boldsymbol{y} \in V$ and $t = \varphi(\boldsymbol{y})$. Hence, the following diagram commutes:

$$\begin{array}{ccc} V & \longrightarrow & Z \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \pi_1} \\ & & \mathbf{C} \end{array}.$$

We have seen that computing projection boils down to compute elimination ideals, let us see now how to do so using Gröbner bases. We first need the notion of elimination orders.

Definition 3.3.13 (Elimination order). Let $\boldsymbol{X}' \subset \boldsymbol{X}$ be a subset of variables, a monomial order $\succ_{\boldsymbol{X}'}$ is said to be a *$\boldsymbol{X}'$-elimination order* provided that any $x_i \in \boldsymbol{X}'$ is larger than all monomial of $\mathbf{Q}[\boldsymbol{X} - \boldsymbol{X}']$.

Example 3.3.14 ([CLO15, Chap. 3, §1, Exercise 6]).

a) The lexicographic order is an $\{x_1, \ldots, x_\ell\}$-elimination order for any $1 \leq \ell \leq n$.

b) Let $I \subset \{1, \ldots, n\}$. Define the following order: let $\alpha, \beta \in \mathbb{N}^n$, then $x^\alpha \succ x^\beta$ if

$$\sum_{i \in I} \alpha_i > \sum_{i \in I} \beta_i \quad \text{or} \quad \sum_{i \in I} \alpha_i = \sum_{i \in I} \beta_i \text{ and } x^\alpha \succ_{\text{grevlex}} x^\beta.$$

Then, if $\boldsymbol{X}' = \{x_i, i \in I\}$, this order is an $\boldsymbol{X}'$-elimination order due to Bayer and Stillman [BS87]. This is a particular case of *weighted order* – see e.g. [Rob86].

c) Similarly, for a partition $\boldsymbol{X} = \boldsymbol{X}' \cup \boldsymbol{X}''$, and $\alpha, \beta \in \mathbb{N}^n$, decompose $\alpha = (\alpha', \alpha'')$ and $\beta = (\beta', \beta'')$ according to this partition. Then define the order: $\alpha \succ \beta$ if

$$x^{\alpha'} \succ_{grevlex} x^{\beta'} \quad \text{or} \quad x^{\alpha'} = x^{\beta'} \text{ and } x^{\alpha''} \succ_{grevlex} x^{\beta''}.$$

This is a $\boldsymbol{X}'$-elimination order, which is a particular case of a *product order*, as it mixes two orders on disjoint sets of variables.

Hence, given an elimination order, the following theorem reduces the computation of an elimination ideal, to the computation of a Gröbner basis for this order.

Theorem 3.3.15 (Elimination theorem [CLO15, Chap. 3, §1, Theorem 2. and Exercise 5]). *Let $\boldsymbol{X} = \boldsymbol{X}' \cup \boldsymbol{X}''$ be a partition of $\boldsymbol{X}$ and let I be an ideal of $\mathbf{Q}[\boldsymbol{X}]$. If $\succ_{\boldsymbol{X}'}$ is an elimination order and G a $\succ_{\boldsymbol{X}'}$-Gröbner basis of I, then $G \cap \mathbf{Q}[\boldsymbol{X}'']$ is a Gröbner basis of $I \cap \mathbf{Q}[\boldsymbol{X}'']$ for the order induced by $\succ_{\boldsymbol{X}'}$ on $\mathbf{Q}[\boldsymbol{X}'']$.*

Example 3.3.16.

a) Using the last two elimination orders of Example 3.3.14, one sees that it obtains a $\succ_{grevlex}$-Gröbner basis in $\mathbf{Q}[\boldsymbol{X}'']$. This is of importance for computations as we will see in the next subsection.

b) As we will see in Chapter 5, computing the critical values of projections is a crucial step for computing the topology of the real trace of an algebraic set. This can be done using the previous theorem as follows.

   Let $V = \boldsymbol{V}(x_1^2 + x_2^2 + x_3^2 - 1) \subset \mathbf{C}^2$ be the complex sphere. Since V is smooth, according to Corollary 2.5.6, the critical points of the projection π_1 on x_1 are the points of V satisfying $x_2 = x_3 = 0$. Hence, the ideal of definition of $K(\pi_1, V)$ is $\langle x_1^2 + x_2^2 - 1, x_2, x_3\rangle$, and its reduced Gröbner basis with respect to $x_3 \succ_{lex} x_2 \succ_{lex} x_1$ is

$$\{x_1^2 - 1, x_2, x_3\}.$$

   Therefore, according to Theorem 3.3.15, $\{x_1^2 - 1\}$ generates the ideal of definition of the Zariski closure of $\pi_1(K(\pi_1, V))$. As this set is finite, the latter closure is the set itself.

We end this subsection with two applications of this result.

Proposition 3.3.17 ([CLO15, Chap 4., §3, Theorem 11])**.** *Let I, J be ideals of $\mathbf{Q}[\boldsymbol{X}]$, y an indeterminate and $\succ$ an $\{y\}$-elimination order on $\mathbf{Q}[\boldsymbol{X}, y]$. Then, if G is a $\succ$-Gröbner of the ideal*

$$(yI + (1 - y)J) \subset \mathbf{Q}[\boldsymbol{X}, y],$$

then $G \cap \mathbf{Q}[\boldsymbol{X}]$ is a Gröbner basis of $I \cap J$.

Hence, as $\boldsymbol{V}(I \cap J) = \boldsymbol{V}(I) \cup \boldsymbol{V}(J)$, this gives an algorithm for computing an algebraic representation of the union of algebraic sets.

The following trick is due to Rabinowitsch, who used it in [Rab30] to prove the equivalence between the so-called "weak" and "strong" Nullstellensatz. Recall that, given two ideal $I, J \subset \mathbf{Q}[\boldsymbol{X}]$, the saturation of I by J is the set

$$I : J^\infty = \{f \in \mathbf{C}[\boldsymbol{X}] \text{ s.t. } \exists k \in \mathbb{Z}, fJ^k \subset I\},$$

where J^k is the ideal product of J with itself, k times.

Proposition 3.3.18 (Rabinowitsch trick [CLO15, Chap. 4, §4, Theorem 14])**.** *Let $I \subset \mathbf{Q}[\boldsymbol{X}]$ be an ideal, $g \in \mathbf{Q}[\boldsymbol{X}]$ a polynomial, y a new variable and $\succ$ an $\{y\}$-elimination order on $\mathbf{Q}[\boldsymbol{X}, y]$. Then if G is a $\succ$-Gröbner of the ideal*

$$(I + \langle 1 - yg\rangle) \subset \mathbf{Q}[\boldsymbol{X}, y],$$

then $G \cap \mathbf{Q}[\boldsymbol{X}]$ is a Gröbner basis of $I : \langle g\rangle^\infty$.

Geometrically speaking, according to [CLO15, Chap. 4, §4, Theorem 10],

$$\boldsymbol{V}(I : J^\infty) = \overline{\boldsymbol{V}(I) - \boldsymbol{V}(J)}^Z.$$

Moreover, if $J = \langle g_1, \ldots, g_q \rangle$, then $\boldsymbol{V}(I) - \boldsymbol{V}(J) = \boldsymbol{V}(I) - \boldsymbol{V}(g_1 \cdots g_q)$. Hence, the above trick allows us to compute the Zariski closure of the difference of algebraic sets as in the following example.

Example 3.3.19. Recall that, in Section 2.6, given a polynomial map $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n)$ we defined the i- th generalized polar variety of an algebraic set $V \subset \mathbf{C}^n$ as the Zariski closure of

$$W^\circ(\boldsymbol{\varphi}_i, V) = K(\boldsymbol{\varphi}_i, V) - \mathrm{sing}(V).$$

Since generators of the ideals of definition of $K(\boldsymbol{\varphi}_i, V)$ and $\mathrm{sing}(V)$ are given by Corollary 2.5.6, one can compute generators of the ideal of definition of the i-th generalized polar variety, using the above trick.

3.3.4 Computing Gröbner bases

We have seen that Gröbner bases constitute a set of generators enjoying many interesting properties. Moreover, the data of such a basis allows one to perform many computations in algebraic geometry.

In this subsection, we address the problem of computing such bases and give a rough historical overview of the related works.

3.3.4.a. Buchberger's algorithm

After introducing and laying the theoretical foundations of Gröbner bases, Bruno Buchberger proposed the first algorithm to compute them in successively [Buc65, Buc70, Buc76].

Description. This algorithm starts from a set of generators $\{f_1, \ldots, f_p\}$ of the input ideal I and computes new generators with new leading terms using the so-called S-polynomials defined below. This way, it increases the size of the ideal generated by the leading term, until it covers all $\langle \mathrm{lt}_\succ(I) \rangle$ (which always happens in finite time by Hilbert's basis Theorem 2.1.6).

Definition 3.3.20 ([CLO15, Chap. 2, §6, Definition 4])**.** Let f, g in $\mathbf{Q}[\boldsymbol{X}]$ be non-zero polynomials, and let x^γ be the *least common multiple* $\mathrm{lcm}(\mathrm{lm}_\succ(f), \mathrm{lm}_\succ(g))$. The *$S$-polynomial* of f and g is

$$S_\succ(f, g) = \frac{x^\gamma}{\mathrm{lt}_\succ(f)} \cdot f - \frac{x^\gamma}{\mathrm{lt}_\succ(g)} \cdot g \ \in \ \mathbf{Q}[\boldsymbol{X}].$$

One sees that the S-polynomials have been constructed on purpose to annihilate the leading term of f, with the one of g, creating a possibly new one.

Then, Buchberger's algorithm consists in performing iteratively the two following steps. Suppose that we have a generating ordered set $H = (f_1, \ldots, f_p)$:

Step 1: *choose a pair (f_i, f_j) from H, and compute their S-polynomial $S_\succ(f_i, f_j)$;*

Step 2: *reduce $S_\succ(f_i, f_j)$ w.r.t H i.e. compute the remainder of the division of $S_\succ(f_i, f_j)$ by H.*

As said above, these two steps increase the size of the ideal generated by the leading monomials, with polynomials lying in the ideal. And according to Hilbert's basis Theorem 2.1.6 this latter sequence of ideals must stabilize to its maximum $\mathrm{lt}_\succ(I)$ at some point.

The following result gives an effective criterion for deciding if a generating set is a Gröbner basis, using S-polynomials. In particular, this constitutes a stopping criterion for Buchberger's algorithm.

Theorem 3.3.21 (Buchberger's criterion [CLO15, Chap. 2, §6, Theorem 6]). *Let $I \subset \mathbf{Q}[\boldsymbol{X}]$ be an ideal and $G = \{g_1, \ldots, g_p\}$ be a generating set. Then, G is a $\succ$ −Gröbner basis of I if and only if for all $1 \leq i \neq j \leq p$, the remainder of the division of $S_\succ(g_i, g_j)$ by G (ordered in some way) is zero.*

Finally, given a Gröbner basis output by Buchberger's algorithm, one can deduce a *reduced* one according to [CLO15, Lemma 3]. This is done by removing the elements whose leading term reduces to zero w.r.t. the leading terms of the other elements, and making monic the remaining ones. One can also modify the algorithm to compute directly, "on the fly", a reduced Gröbner basis (see [Buc85]).

3.3.4.b. Drawbacks and solutions

Each of the above two steps reveals an intrinsic weakness of this algorithm. Indeed, in the first step, the pairs are *chosen freely* among the current generating set, and this choice has an impact on the performance. Indeed, in the second step, it is observed that most of the S-polynomials either reduce to 0 w.r.t H or do not play any further role in the computation and are not part of the reduced Gröbner basis. Hence, computing and reducing these S-polynomials constitute useless operations to compute a Gröbner basis, and can amount to most of the computing time.

Several strategies have been developed to overcome these two weaknesses and then improve Buchberger's algorithm. A partial overview can be found in [Buc01].

Pairs selection. Several strategies have been proposed for efficiently selecting the pairs with which to calculate S-polynomials [Buc85, GM88, GMN+91, BW93].

Later, Faugère proposes to avoid this selection in his F4 algorithm, presented in [Fau99], which relies on fast linear algebra methods. This algorithm first computes a so-called *Macaulay matrix*, that is a matrix indexed by monomials, from the current generating set. Then, it carries out many S-polynomial computations and reductions at a time by computing an echelon form of the aforementioned matrix. This strategy is very efficient in practice and it (and its variants) represents the state-of-the art algorithms for computing Gröner bases. It is implemented in many computer algebra systems such as Magma[2], Maple[3] or libraries such as FGb[4] [Fau10] and msolve[5] [BES21].

Avoid zero reductions. To avoid computing useless S-polynomials, that is the one that will reduce to 0 in the final Gröbner basis one approach is to refine Buchberger's criterion of Theorem 3.3.21; see e.g. [Buc79, KB78] and [CLO15, Chap. 2 §9]. As an illustration, the following result allows to detect such zero reduction using an inexpensive criterion.

[2] https://magma.maths.usyd.edu.au/magma/handbook/groebner_bases
[3] https://fr.maplesoft.com/support/help/Maple/view.aspx?path=Groebner
[4] https://www-polsys.lip6.fr/~jcf/FGb/index.html
[5] https://msolve.lip6.fr

Proposition 3.3.22 ([CLO15, Chap. 2, §10, Proposition 1]). *Let $G \subset \mathbf{Q}[\boldsymbol{X}]$ be a finite set and let $f, g \in G$. If*

$$\operatorname{lcm}(\operatorname{lm}_{\succ}(f), \operatorname{lm}_{\succ}(g)) = \operatorname{lm}_{\succ}(f) \cdot \operatorname{lm}_{\succ}(g),$$

then $S(f, g)$ will reduce to zero in any Gröbner basis computed from G.

More recently in [Fau02], Faugère proposed to keep track of the previous computations that lead to zero reductions using signatures of polynomials. He then proposed a signature-based algorithm, F5, which avoids many reductions to zero, with a small additional cost. Moreover, for generic input systems (namely regular sequences), this algorithm avoids *all* reductions to zero. Many other signature-based algorithms have been subsequently proposed and a comprehensive survey can be found in [EF17]. It is worth noting that many of the encountered systems from *real algebraic geometry* come from determinantal systems, which are not generic. However, very recent work focuses on adapting F5 for these systems and already allows one to avoid all reductions to zero in some cases [GNS23].

This new algorithm already showed practical efficiency in solving challenging problems in cryptography that were previously intractable (by e.g. F4) [FJ03]. However, few implementations of F5 algorithm are available as understanding and implementing signature-based algorithms seems challenging as the size of the signatures can grow very rapidly. We mention below a non-exhaustive list of implementations of variants of F5:

- a C++ source code of implementations presented in [RS12] [6];
- a high-level implementation in SINGULAR of the variant G2V, presented in [GGV10] [7];
- a Julia implementation is part of the AlgebraicSolving.jl package [8].

3.3.4.c. Change of monomial order

According to their definition, Gröbner bases are associated with a monomial order. Hence, depending on this choice, the cost of Gröbner bases computations can vary considerably and changes of variables or order often can reduce this cost.

For instance, in [BS87], Bayer and Stillman showed that most of the times, Gröbner bases with respect to the grevlex order should have minimal degree; in the zero-dimensional case [CGH88, CGH91] gives an exponential bound on the degree, while [Laz83] proves asymptotic optimal bounds under some conditions. On the other hand, lexicographic order is better suited for computations as the associated bases convey more geometric information (elimination, triangular systems, etc.); see e.g. [Tri78, GM89, Laz92] in the zero-dimensional case. However, lexicographic Gröbner bases often come with higher degrees and terms [Laz83].

A fruitful approach for overcoming this obstacle is to compute a Gröbner basis with respect to a more appropriate order and subsequently convert the result into the desired order, typically lexicographic or elimination order. This concept traces its origins back to

[6] http://www.broune.com/papers/issac2012.html
[7] http://www.math.clemson.edu/~sgao/code/g2v.sing
[8] https://algebraic-solving.github.io/

Buchberger's work in [Buc70], while a historical account of the evolution of this idea can be found in [CKM97].

In the zero-dimensional case, this is efficiently tackled by the so-called FGLM algorithm, named after Faugère, Gianni, Lazard and Mora [FGLM93]. This algorithm exploits the fact that the coordinate ring $\mathbf{C}[\boldsymbol{X}]/I$ of a zero-dimensional ideal has the structure of a *finite dimensional* $\mathbf{C}$-vector space, of which a basis can be easily derived from a Gröbner basis of $\boldsymbol{I}(V)$. In particular, they showed that for the computation of a lexicographic basis from a grevlex basis, this strategy is usually much faster than a direct application of Gröbner basis algorithms.

Note that variants of this algorithm have been developed recently such as the typically much faster Sparse-FGLM [FM17] that exploits the typical sparsity of the matrices in consideration. Additionally, a parametric version of the FGLM algorithm has also been presented in [DH17], and a version tailored for colon ideals has been introduced very recently in [BES23]. It is also noteworthy to mention that in [BES23], the authors present a variant of the F4 algorithm designed for computing saturated ideals, effectively bypassing the need to compute a Gröbner basis with respect to an elimination order as seen in Subsection 3.3.3.

We end this Subsection by mentioning the positive dimensional case where FGLM-like algorithms fail. To our knowledge, only two approaches exist for the general case: the Hilbert function approach of Traverso [Tra96] and the Gröbner walks introduced by Collart, Kalkbrener, and Mall [CKM97]. The latter relies on the theory of Gröbner fan introduced by Mora and Robbiano in [MR88] and is interesting as it is independent of the dimension of the ideal. Roughly speaking, the algorithm takes as input two monomial orders $\succ$ and $\succ'$, and a $\succ$-Gröbner basis G of an ideal $I \subset \mathbf{C}[\boldsymbol{X}]$. Then, it constructs a finite "path" of monomial orders $\succ = \succ_0, \ldots, \succ_m = \succ'$ and bases $G_0, \ldots, G_m$ such that G_i is a $\succ_i$-Gröbner basis. Due to the "proximity" of G_{i+1} to G_i, where the corresponding cones of the Gröbner Fan of I are adjacent, the computation of G_{i+1} from G_i becomes relatively straightforward.

In [AGK97], the authors showed good practical performance for this method, even compared to FGLM, in the zero-dimensional case, at that time. Relatively recent progress has also been made to make this algorithm more practical, mainly by improving the choice of the path of monomial orders [Tra00, FJLT07].

3.4 Rational parametrizations

In this section, we present another type of representation for algebraic sets: rational parametrization. Although they enjoy less algebraic properties than Gröbner bases, they allow better degree bounds and interesting complexities for elementary manipulations, especially in low dimensions (see [SS17, Section J]).

In fact, in generic coordinates, a rational parametrization of an algebraic set V is very similar to a lexicographic Gröbner basis of its associated ideal $\boldsymbol{I}(V)$. The latter has the so-called "shape lemma form", where the first coordinates are the zeros of a polynomial and the others are polynomial functions of the former. However, the coefficients of the latter

polynomials tend to be very large – see [ABRW96, Section 6]– and this is what rational parametrizations try to avoid.

Intuitively, rational parametrizations can be seen as an effective application of a slight generalization of Theorem 2.3.28. The latter says that every equidimensional algebraic set V of dimension d is birational to a hypersurface $\mathcal{H}$ of $\mathbf{C}^{d+1}$. In other words, a non-empty Zariski open subset of V, can be *parameterized* by *rational* functions in $d+1$ variables lying on a *hypersurface* $\mathcal{H}$ of $\mathbf{C}^{d+1}$.

Remark 3.4.1. Note that the rational parametrizations presented here need not be confused with parametrizations of rational algebraic sets by $\mathbf{C}^d$. While the former has its parameters lying in some hypersurface defined implicitly as a projection of the algebraic set, the latter has parameters varying freely in $\mathbf{C}^d$. Hence, the parametrizations we deal with here always exist and do not assume more assumptions than the equidimensionality one.

This idea goes back to the works of Kronecker and König, [Kro82, Kön03] and is also referred to as *Kronecker parametrization*. For a d-equidimensional algebraic set of $\mathbf{C}^n$, it has the form

$$\begin{cases} x_1 = \dfrac{w_1}{\partial_{x_{d+1}} q}\Big(\ell_1(\boldsymbol{X}), \ldots, \ell_{d+1}(\boldsymbol{X})\Big) \\ \vdots \qquad\qquad\qquad\qquad\qquad\qquad \text{and} \quad q(\ell_1(\boldsymbol{X}), \ldots, \ell_{d+1}(\boldsymbol{X})) = 0 \\ x_n = \dfrac{w_n}{\partial_{x_{d+1}} q}\Big(\ell_1(\boldsymbol{X}), \ldots, \ell_{d+1}(\boldsymbol{X})\Big) \end{cases}$$

where

- $q, v_1, \ldots, v_n$ are polynomials in $x_1, \ldots, x_{d+1}$, with q *square-free* and monic as a univariate polynomial in x_i, for $1 \leq i \leq d+1$;
- $\ell_1, \ldots, \ell_{d+1}$ are *generic* linear forms in $x_1, \ldots, x_n$.

These notions were also later reconsidered by Macaulay in [Mac16], where he provides a good summary of the previous works.

These parametrizations have been rediscovered in [GHMP95, Par95] for dealing with the zero-dimensional case. It has subsequently been used in a broad range of applications, to efficiently solve polynomial systems with finitely many solutions [GM89, Can88a, HRS90, Laz92, LL91, Lec00, GLS01, ABRW96, GHMP97, GHM+98, Rou99]. We refer to [CPHM01, Section 2.2] for a historical overview. We give hereafter a precise definition of the rational parametrization in this case, that will be called a *zero-dimensional parametrization*.

Definition 3.4.2 (Zero-dimensional parametrizations [SS17, §1.2])**.** A zero-dimensional parametrization $\mathscr{P}$ with coefficients in $\mathbf{Q}$ is the data of:

- polynomials $(\omega, \rho_1, \ldots, \rho_n)$ in $\mathbf{Q}[u]$ where u is an indeterminate, ω is a monic square-free polynomial and it holds that $\deg(\rho_i) < \deg(w)$,
- a $\mathbf{Q}$-linear form $\mathfrak{l}$ in the indeterminates $x_1, \ldots, x_n$,

such that

$$\mathfrak{l}(\rho_1, \ldots, \rho_n) = u\frac{\partial \omega}{\partial u} \mod \omega.$$

Such a data structure encodes the finite algebraic sets of $\mathbf{C}^n$, denoted by $\mathsf{Z}(\mathscr{P})$ defined as follows:

$$\mathsf{Z}(\mathscr{P}) = \left\{ \left(\frac{\rho_1}{\partial_u \omega}(\vartheta), \ldots, \frac{\rho_n}{\partial_u \omega}(\vartheta) \right) \in \mathbf{C}^n \ \text{ s.t. } \ \omega(\vartheta) = 0 \right\}.$$

The *degree* of $\mathscr{P}$ is the one of ω, which is exactly the one of $\mathsf{Z}(\mathscr{P})$ (i.e. its cardinality). By convention, we note $\mathscr{P}_\emptyset = (1)$ the zero-dimensional parametrization that encodes the empty set.

In particular, given such a parametrization, one can compute isolating disks (or intervals for the real roots) of the solutions as follows. First isolate the roots of the eliminating polynomial ω using tailor-made algorithms such as [RZ04, SM16, KRS16, MSW15, KS15, Mor22]. Then use interval arithmetic to derive isolating areas of the coordinates of the solution that is the image of the roots of ω by the rational functions $\rho_1/\partial_u\omega, \ldots, \rho_n/\partial_u\omega$.

Such parametrizations can be computed using different approaches. The first one, introduced first in [ABRW96] and later developed by Rouiller in [Rou99], consists in computing the so-called *Rational Univariate Representation* (RUR) of an ideal using Gröbner bases computations. Note that this representation might need some straightforward post-treatment to be a zero-dimensional parametrization, as the input ideals of the algorithm need not be radical. In particular, the RUR captures the root multiplicities of the input system. An implementation of this algorithm has been integrated into the computer algebra system Maple.[9]

Besides, another approach to compute such parametrization consists in computing the so-called *geometric resolutions* introduced in [GLS01]. In [GLS01], the authors propose a probabilistic algorithm relying on incremental lifting and intersecting of curves and using extensively straight-line programs. See [DL08] for a simplified and pedagogical presentation of this algorithm. The complexity of this strategy is polynomial in the degrees of the intermediate algebraic sets computed, which is bounded by the degree of the input by Bézout bound (see Theorem 2.1.31). Two implementations are available in respectively the Kronecker [Lec02] and the Geomsolvex [Lec12] libraries of the computer algebra systems Magma[10] and Mathemagix[11], respectively.

We mention also a parametric version of geometric resolution introduced in [Sch03]. Consider a polynomial system $\boldsymbol{f}(z_1, \ldots, z_r, \boldsymbol{X})$ with coefficients in $\mathbf{Q}$, in the indeterminates $x_1, \ldots, x_n$ and with parameters $z_1, \ldots, z_r$. Suppose that the parameters are in Noether position with respect to the algebraic set of $\mathbf{C}^{r+n}$ defined by $\boldsymbol{f}$, in particular for a generic $\eta \in \mathbf{C}^r$, $\boldsymbol{f}(\eta, \boldsymbol{X})$ defines a zero-dimensional algebraic set. Hence, a *parametric geometric resolution* of $\boldsymbol{f}$, is a zero-dimensional parametrization $\mathscr{P}$ with coefficients in $\mathbf{Q}(z_1, \ldots, z_r)$, together with a polynomial $h \in \mathbf{Q}[z_1, \ldots, z_r]$, such that if $h(\eta) \neq 0$ then the specialization of $\mathscr{P}$ at η is a zero-dimensional parametrization of $\boldsymbol{V}(\boldsymbol{f}(\eta, \boldsymbol{X})) \subset \mathbf{C}^n$. In other words, parametric geometric resolutions describe the solutions in an algebraically closed field of a parametric system, as the parameters range in a non-empty Zariski open set. However, when considering the solutions in a non-algebraically closed field it is not sufficient. The case of "real solutions" is much harder and is extensively studied in [Le21, LS22].

[9] https://fr.maplesoft.com/support/help/maple/view.aspx?path=Groebner/RationalUnivariateRepresentation

[10] http://magma.maths.usyd.edu.au/magma/

[11] http://www.mathemagix.org

We end this section by dealing with the one-dimensional case. As it will be ubiquitous in this thesis, we also give a precise definition.

Definition 3.4.3 (One-dimensional parametrizations [SS17, §1.2])**.** A *one-dimensional rational parametrization* $\mathscr{R}$ with coefficients in $\mathbf{Q}$ is the data of:

- polynomials $(\omega, \rho_1, \ldots, \rho_n)$ in $\mathbf{Q}[u, v]$ where u and v are indeterminates, ω is a monic square-free polynomial and with $\deg(\rho_i) < \deg(w)$,
- linear forms $(\mathfrak{l}, \mathfrak{l}')$ in the indeterminates $x_1, \ldots, x_n$,

such that

$$\mathfrak{l}(\rho_1, \ldots, \rho_n) = u\frac{\partial \omega}{\partial u} \mod \omega \quad \text{and} \quad \mathfrak{l}'(\rho_1, \ldots, \rho_n) = v\frac{\partial \omega}{\partial u} \mod \omega.$$

Such a data structure encodes the algebraic curve, denoted by $\mathsf{Z}(\mathscr{R})$, defined as the Zariski closure of the following constructible set

$$\left\{ \left(\frac{\rho_1}{\partial_u \omega}(\vartheta, \eta), \ldots, \frac{\rho_n}{\partial_u \omega}(\vartheta, \eta) \right) \in \mathbf{C}^n \text{ s.t. } \omega(\vartheta, \eta) = 0, \quad \frac{\partial \omega}{\partial u}(\vartheta, \eta) \neq 0 \right\}.$$

The *degree* of $\mathscr{R}$ is the defined as the one of ω, which is actually the degree of $\mathsf{Z}(\mathscr{R})$ as an algebraic set. Note that such a parametrization $\mathscr{R}$ of degree δ involves $O(n\delta^2)$ coefficients.

Such parametrizations for algebraic curves always exist by [Sch03], and efficient algorithms for computing them can be found in [Lec00, GM19] and [SS17, Appendix J, §5], all based on geometric resolution algorithm from [GLS01].

We will extensively use rational parametrization for encoding algebraic (finitely many) points (query points, critical points, etc.) and curves (mainly roadmaps). In particular, as straight-line programs, they will often constitute the standard input/output of our algorithms. The reasons, briefly mentioned at the beginning of this section, are twofold.

- First, they allow compact representations. Indeed, the classic Kronecker representation does not require the denominator to be the derivative of the eliminating polynomial. Even more, in the zero-dimensional case, one can even avoid denominators. However, this constraint on the denominator allows to control both the degree (bounded by the one of the algebraic set) and the bitsize of the coefficients; see [ABRW96, Rou99, GLS01, DS04].
- Secondly, rational parametrizations allow to perform basic operations such as unions, intersections, (inverse) projections or changes of variables, with complexity polynomial in the degree of the parametrizations (that is of the algebraic sets in consideration).

Finally, we mention the algorithms of [Lec00, GM19] that compute Kronecker representations of equidimensional algebraic sets of positive dimension. In particular, in the recent [GM19], the authors give a randomized algorithm tackling locally closed sets defined by polynomials with integer coefficients and provide a bound on its bit complexity. This bound is roughly quadratic in the Bézout bound of the system, and linear in its bitsize.

4 Real algebraic geometry

In this chapter, we study the properties of algebraic sets defined on fields that are generalizations of the field of real numbers, and in particular, not algebraically closed. As the foundational Hilbert's Nullstellensatz does not hold anymore, the theory of algebraic geometry elaborated in Chapter 2 is not valid anymore. However, we will see that, considering a wider class of sets, namely the semi-algebraic sets, one can get powerful results that have many connections with differential analysis on $\mathbb{R}$.

In Section 4.1 we first introduce the theory of real closed fields and their extensions, highlighting the significant example of algebraic Puiseux series as a tool for investigating infinitesimals. Moving forward, Section 4.2 provides an introduction to semi-algebraic sets and semi-algebraic maps defined over real fields. Emphasis is placed on discussing the topology of these constructs and their behavior concerning real closed extensions. Additionally, Section 4.3 explores an alternative geometric characterization of algebraic Puiseux series, namely semi-algebraic germs. This approach yields valuable insights into local properties. Lastly, Section 4.4 investigates aspects of semi-algebraic differential geometry, enabling us to establish the influential Implicit Function and Thom's first isotopy theorems.

4.1 Real fields and their extensions

4.1.1 The theory of real closed fields

Real closed fields are fields that share many important properties with $\mathbb{R}$ the field of real numbers, and where important results from the standard analysis on $\mathbb{R}$ still hold. However, by contrast with the set of real numbers, general real closed fields can contain infinitesimal (or equivalently unbounded) elements, and then not being Archimedean. When omitted, we refer to [BCR98] and to [BPR06] for most of the definitions and results introduced here.

Definition 4.1.1. An *ordered set* $(A, \preceq)$ is a set A, together with a binary relation $\preceq$, that satisfies the following assertions:

- $\preceq$ is reflexive: $a \preceq a$;
- $\preceq$ is transitive: if $a \preceq b$ and $b \preceq c$ then $a \preceq c$;
- $\preceq$ is anti-symmetric: $a \preceq b$ and $b \preceq a$ if and only if $a = b$.

We say that $(A, \preceq)$ is *totally ordered* if, in addition, $\preceq$ is total that is for every $a, b \in A$, $a \preceq b$ or $b \preceq a$ does hold. If so, $a \prec b$ will stand for $a \preceq b$ together with $a \neq b$. We define $\succeq$ and $\succ$ in a symmetric way.

Example 4.1.2.

a) The set $\mathcal{P}(X)$ of the subsets of a set X, together with $\subset$, the inclusion of sets, is an ordered set

b) The set of integers $\mathbb{Z}$, together with the divisibility relation $|$, is an ordered set.

c) The nonnegative integers $\mathbb{N}$, together with its natural order $\leq$, is a totally ordered set.

Definition 4.1.3. An *ordered ring* $(R, \preceq)$ is a ring R, together with a total order $\preceq$ such that $(R, \preceq)$ is an ordered set and $\preceq$ is compatible with the ring structure of R that is:

- if $a \preceq b$ then $a + c \preceq b + c$ for any a, b, c in R;
- if $0 \preceq a$ and $0 \preceq b$ then $0 \preceq ab$ for any a, b in R.

If, in addition, R is a field, then $(R, \preceq)$ is an *ordered field*.

Example 4.1.4.

a) The ring $\mathbb{Z}$, together with its natural order $\leq$, is an ordered ring.

b) The fields $\mathbb{Q}$ and $\mathbb{R}$, together with their natural order $\leq$, are ordered fields.

c) The complex field $\mathbb{C}$, together with the lexicographic order $\preceq_{\text{lex}}$:

$$a + ib \preceq_{\text{lex}} c + id \iff a < c \quad \text{or} \quad a = c \text{ and } b \leq d,$$

is a totally ordered set. It is not an ordered field though, as $\preceq_{\text{lex}}$ is not compatible with the ring structure of $(\mathbb{C}, +, \times)$.

Besides, the order on real parts $\preceq_{\text{rea}}$ of complex numbers:

$$a + ib \preceq_{\text{rea}} c + id \iff a \leq c,$$

is compatible with the ring structure of $(\mathbb{C}, +, \times)$, but is not total.

Actually, the following result implies that $\mathbb{C}$ cannot be ordered as a field.

We now consider a particular class of ordered fields, whose order relations gives particular

Theorem 4.1.5 ([BCR98, Theorem 1.1.8])**.** *Let* $\mathbf{Q}$ *be a field, the following statements are equivalent:*

1. $\mathbf{Q}$ *can be ordered;*
2. -1 *is not a sum of squares in* $\mathbf{Q}$*.*
3. *for every* $a_1, \ldots, a_n$ *in* $\mathbf{Q}$*, if* $\sum_{i=1}^{n} a_i^2 = 0$*, then* $a_1 = \cdots = a_n = 0$*.*

Definition 4.1.6 ([BCR98, Definition 1.1.9])**.** A field $\mathbf{Q}$, satisfying the equivalent properties of Theorem 4.1.5, is called a *real field*.

Example 4.1.7.

a) The fields $\mathbb{Q}$ and $\mathbb{R}$ are real fields.

b) Back to Example 4.1.4.c), as $-1 = i^2$, the field $\mathbb{C}$ is not a real field. Hence, it cannot be ordered as a field i.e. there is no total order $\preceq$ such that $(\mathbb{C}, \preceq)$ is an ordered field.

c) If $\mathbf{Q}$ is a real field, then there exists an order on $\mathbf{Q}(x)$, the field of rational fractions with coefficients in $\mathbf{Q}$. This order is such that x is infinitesimal over $\mathbf{Q}$ (see Subsection 4.1.2). Hence $\mathbf{Q}(x)$ is a real field.

d) Every field of non-zero characteristic is not a real field, as it cannot be ordered.

Let us recall some classic notions of field theory.

Proposition-definition 4.1.8. *Let $\mathbf{C}$ and $\mathbf{K}$ be two fields such that $\mathbf{C} \subset \mathbf{K}$ up to an injective morphism of fields. Then, the following holds:*

1. *$\mathbf{K}$ is a $\mathbf{C}$-vector space and is called an* extension *of $\mathbf{C}$, denoted by $\mathbf{K}/\mathbf{C}$;*
2. *$\mathbf{K}/\mathbf{C}$ is algebraic if every element of $\mathbf{K}$ is a root of a nonzero polynomial with coefficients in $\mathbf{C}$;*
3. *$\mathbf{C}$ is algebraically closed if every non-constant polynomial in $\mathbf{C}[x]$ has a root in $\mathbf{C}$. Then, if $\mathbf{K}/\mathbf{C}$ is algebraic, the extension is trivial i.e. $\mathbf{K} = \mathbf{C}$.*

Definition 4.1.9 ([BCR98, Definition 1.2.1])**.** A field $\mathbf{R}$ is a *real closed field* if it is a real field that has no non-trivial real algebraic extension.

Since $\mathbb{R}$ can be seen as a model of a real closed field, it is important to ensure that fundamental properties of differentiable functions over $\mathbb{R}$ still hold over real closed fields.

Definition 4.1.10 ([BPR06, p.45])**.** A field $\mathbf{R}$ has the *intermediate value property* if $\mathbf{R}$ is an ordered field such that: for any polynomial $f \in \mathbf{R}[x]$ such that $f(a)f(b) < 0$, where $a < b$ in $\mathbf{R}$, there exists $c \in (a, b)$ such that $f(c) = 0$.

The following fundamental theorem gives equivalent characterizations of real closed fields. It shows, in particular, that the *intermediate value property* is a precise requirement for a real field to be closed.

Theorem 4.1.11 ([BPR06, Theorem 2.17])**.** *Let $\mathbf{R}$ be a field, the following statements are equivalent:*

1. *$\mathbf{R}$ is real closed;*
2. *$\mathbf{R}$ has the intermediate value property;*
3. *there is a unique ordering of $\mathbf{R}$ such that any nonnegative element of $\mathbf{R}$ has a square root in $\mathbf{R}$ and every polynomial in $\mathbf{R}[x]$ with odd degree, has a root in $\mathbf{R}$;*
4. *$\mathbf{R}[i] = \mathbf{R}[x]/(x^2 + 1)$ is an algebraically closed field.*

Example 4.1.12. The real field $\mathbb{R}$ is real closed, as $\mathbb{R}[i] = \mathbb{C}$, but $\mathbb{Q}$ is not, as $\sqrt{2} \notin \mathbb{Q}$.

A real closed field also satisfies many important theorems and properties that hold in $\mathbb{R}$, such as polynomial versions of Mean Value or Rolle's theorem (see [BCR98, Proposition 1.2.6 and Corollaries 1.2.7 and 1.2.8]). The following theorem forms a converse to the last statement of Theorem 4.1.11.

Theorem 4.1.13 ([BPR06, Theorem 2.42]). *Let* $\mathbf{C}$ *be an algebraically closed field of characteristic zero. Then there exists a real closed field* $\mathbf{R} \subset \mathbf{C}$ *such that* $\mathbf{R}[i] = \mathbf{C}$*, where* $i \in \mathbf{C}$*.*

We conclude this section, with the natural notion of real closure, which intuitively follows the algebraically closed one.

Definition 4.1.14 ([BCR98, Definition 1.3.1]). An algebraic extension $\mathbf{R}$ of an ordered field $\mathbf{K}$, is called a *real closure* of $\mathbf{K}$ if $\mathbf{R}$ is real closed and if its unique ordering extends the ordering of $\mathbf{K}$.

As for algebraic closure, the existence of such real closure is always guaranteed and has some uniqueness properties. However, it is worth noting that the uniqueness of real closure is, in some sense, stronger than the one of algebraic closure (see [BCR98, Remark 1.3.5]).

Theorem 4.1.15 ((Artin-Schreier) [BCR98, Theorem 1.3.2]). *The real closure of* $\mathbf{K}$ *exists and is unique, up to a* $\mathbf{K}$*-isomorphism.*

We end this paragraph with a useful criterion to construct the real closure of a real field, from any of its real closed extensions.

Proposition 4.1.16 ([BPR06, Exercise 2.40]). *Let* $\mathbf{R}$ *be a real closed field extending* $\mathbf{K}$*. Then the real closure of* $\mathbf{K}$ *is exactly the subfield of elements of* $\mathbf{R}$ *that are algebraic over* $\mathbf{K}$*.*

Example 4.1.17.

a) Let $\mathbb{R}_{\text{alg}}$ be the field of real algebraic numbers over $\mathbb{Q}$. Since $\mathbb{Q} \subset \mathbb{R}$ and $\mathbb{R}$ is real closed, $\mathbb{R}_{\text{alg}}$ is the real closure of $\mathbb{Q}$. In particular, this proves that $\mathbb{R}_{\text{alg}}$ is real closed. Of course, the latter can also be proved more directly using one of the last two characterizations of Theorem 4.1.11.

b) The following subsection details the construction of a noticeable example of real closure: the field of algebraic Puiseux series. This is the smallest real closed extension $\mathbf{R}'$ of a real closed field, containing elements that are infinitesimal over $\mathbf{R}$.

4.1.2 Algebraic Puiseux series: seeking infinitesimals

Given any ordered field $\mathbf{K}$, we denote by $|a|$ the *absolute value* of an element $a \in \mathbf{K}$ that is the maximum of a and $-a$.

Definition 4.1.18. Let $\mathbf{K} \subset \mathbf{K}'$ be two ordered fields such that the inclusion is order preserving. We say that an element of $\mathbf{K}'$ is:

1. *infinitesimal* over $\mathbf{K}$ if its absolute value is positive and smaller than any positive element of $\mathbf{K}$;
2. *unbounded* over $\mathbf{K}$ if its absolute value is positive and greater than any element of $\mathbf{K}$.

Remark 4.1.19. Given the same notations, if $\varepsilon \in \mathbf{K}'$ is infinitesimal over $\mathbf{K}$, then, as it is nonzero, $\varepsilon^{-1} \in \mathbf{K}'$ is unbounded over $\mathbf{K}$. Moreover, if such ε exists, then $\mathbf{K}'$ is *non-Archimedean* since $|\varepsilon|$ is smaller than $1/n \in \mathbf{K}$ for any positive integer n.

In the following, we fix an arbitrary closed field $\mathbf{R}$, and we construct, step by step, a real closed extension $\mathbf{R}'$, of $\mathbf{R}$, that contains infinitesimals over $\mathbf{R}$. Then, using Proposition 4.1.16, we directly get, from $\mathbf{R}'$, the real closure of $\mathbf{R}$.

Definition 4.1.20 ([BCR98, Example 1.1.2])**.** Let $\mathbf{R}(\varepsilon)$ be the field of rational fractions with coefficients in $\mathbf{R}$ and for $0 \leq m \leq n$, let

$$f(\varepsilon) = a_m\varepsilon^m + a_{m+1}\varepsilon^{m+1} + \cdots + a_n\varepsilon^n$$

be a nonzero polynomial in $\mathbf{R}[\varepsilon]$ such that $a_m \neq 0$. Let $g \in \mathbf{R}[\varepsilon]\backslash\{0\}$, we say that:

1. f is positive (or $0 < f$) if and only if $0 < a_m$;
2. $f/g \in \mathbf{R}(\varepsilon)$ is positive (or $0 < f/g$) if and only if fg is.

Hence, for any F, G in $\mathbf{R}(\varepsilon)$, we say that $F \leq G$ if and only if $F = G$ or $0 < G - F$.

Proposition 4.1.21 ([BPR06, Exercise 2.9])**.** *Given the order defined in Definition 4.1.20, the following holds:*

1. $(\mathbf{R}(\varepsilon), \leq)$ *is an ordered field;*
2. *the inclusion* $\mathbf{R} \subset \mathbf{R}(\varepsilon)$ *is order preserving;*
3. ε *is an infinitesimal element of* $\mathbf{R}(\varepsilon)$ *over* $\mathbf{R}$*.*

The above proposition claims that $\mathbf{R}(\varepsilon)$ is a real extension of $\mathbf{R}$ containing infinitesimals over $\mathbf{R}$ as requested. But $\mathbf{R}(\varepsilon)$ is not real closed as the following proposition illustrates.

Proposition 4.1.22. *The field* $\mathbf{R}(\varepsilon)$ *equipped with the order of Definition 4.1.20 is not real closed.*

Proof. Let $\mathbf{R}[[\varepsilon]]$ denote the ring of formal power series in ε with coefficients in $\mathbf{R}$. Let $\mathbf{R}(\!(\varepsilon)\!)$ be the field of Laurent series in ε with coefficients in $\mathbf{R}$, that is the quotient field of $\mathbf{R}[[\varepsilon]]$.

Remark that $\mathbf{R}(\!(\varepsilon)\!)$ contains $\mathbf{R}(\varepsilon)$ and algebraic elements over $\mathbf{R}(\varepsilon)$ that are not in $\mathbf{R}(\varepsilon)$ as well. Hence, the subfield of $\mathbf{R}(\!(\varepsilon)\!)$ of algebraic elements over $\mathbf{R}(\varepsilon)$ is a non-trivial real algebraic extension of $\mathbf{R}(\varepsilon)$, that is $\mathbf{R}(\varepsilon)$ is not real closed, by Definition 4.1.9. □

However recalling Theorem 4.1.15, to find the real closure of $\mathbf{R}(\varepsilon)$, one just needs to find any real closed extension of $\mathbf{R}(\varepsilon)$. However, the field $\mathbf{R}(\!(\varepsilon)\!)$ seen above is not real closed as well, as it does not contain square roots of ε, which is a positive element. Fixing this failure, we define the so-called set of Puiseux series.

Definition 4.1.23 (Puiseux Series)**.** The set $\mathbf{R}\langle\langle\varepsilon\rangle\rangle$ of Puiseux Series with coefficients in $\mathbf{R}$ is the set of formal series defined as follows:

$$\mathbf{R}\langle\langle\varepsilon\rangle\rangle = \left\{ \overline{a} = \sum_{i \geq k} a_i\varepsilon^{i/q} \mid a_i \in \mathbf{R},\ k \in \mathbb{Z},\ q \in \mathbb{N}^\star \right\}.$$

By this means, we add the roots of the polynomials of the form $X^q - \varepsilon^i$ with $i \in \mathbb{Z}$ and $q > 0$. Indeed, as a positive element, one requires that ε has square roots in the real closure containing it.

Finally, our goal is achieved according to the following theorem.

Theorem 4.1.24 ([BPR06, Theorem 2.113])**.** *The set $\mathbf{R}\langle\langle\varepsilon\rangle\rangle$ of Puiseux series is a real closed field.*

Remark 4.1.25. The order on $\mathbf{R}\langle\langle\varepsilon\rangle\rangle$ is the unique order that satisfies: given $\overline{a} = a_1\varepsilon_1^r + a_2\varepsilon_2^r + \cdots \in \mathbf{R}\langle\langle\varepsilon\rangle\rangle$ with $a_1 \neq 0$, then $\overline{a}$ is nonnegative if and only if a_1 is.

Corollary 4.1.26. *Let $\mathbf{R}\langle\varepsilon\rangle$ be the subfield of elements of $\mathbf{R}\langle\langle\varepsilon\rangle\rangle$ that are algebraic over $\mathbf{R}(\varepsilon)$. Then $\mathbf{R}\langle\varepsilon\rangle$ is the real closure of $\mathbf{R}(\varepsilon)$, equipped with the order of Definition 4.1.20, and is called the* field of algebraic Puiseux series.

We conclude by considering the limit morphism that connects some elements in $\mathbf{R}\langle\varepsilon\rangle$ to ones in $\mathbf{R}$. This constitutes the main motivation for the introduction of infinitesimals in this thesis. This will allow us, in the next subsection, to use infinitesimal calculus in an algebraic framework.

Recall that a discrete valuation ring A is a principal ring, which is local, that is A has a unique maximal ideal $\mathfrak{m}$. Hence, $A/\mathfrak{m}$ is the *residual field* of A. Let t be a generator of $\mathfrak{m}$, it is called a *uniformizer*, and satisfies $\mathfrak{m} = (t)$ as A is principal. For any $a \in A$, there exists a unique $i \geq 0$ such that $(a) = (t^i)$; such an integer i is called the valuation of a in A.

Proposition 4.1.27 ([BPR06, Proposition 2.121])**.** *Let $\mathbf{R}\langle\varepsilon\rangle_b$ be the set of algebraic Puiseux series bounded over $\mathbf{R}$ i.e. the elements of $\mathbf{R}\langle\varepsilon\rangle$ with an absolute value less than a positive element of $\mathbf{R}$. Then,*

$$\mathbf{R}\langle\varepsilon\rangle_b = \left\{ \overline{a} = \sum_{i\geq 0} a_i\varepsilon^{i/q} \mid \overline{a} \in \mathbf{R}\langle\varepsilon\rangle,\ q \in \mathbb{N}^\star,\ a_i \in \mathbf{R} \right\},$$

and $\mathbf{R}\langle\varepsilon\rangle_b$ is a discrete valuation ring *of valuation $v(\overline{a}) = \inf_{a_i\neq 0} i$, of uniformizer ε and residual field is $\mathbf{R}$.*

Definition 4.1.28. The limit morphism is the canonical projection from $\mathbf{R}\langle\varepsilon\rangle_b$ to its residual field:

$$\lim_\varepsilon : \mathbf{R}\langle\varepsilon\rangle_b \to \mathbf{R}.$$

This morphism maps any $\sum_{i\geq 0} a_i\varepsilon^{i/q} \in \mathbf{R}\langle\varepsilon\rangle_b$ to its first coefficient a_0.

Puiseux series can be defined over arbitrary fields, of any characteristic. As shown in this subsection, they can inherit important properties from their base field. In particular the Newton-Puiseux theorem [Eis95, Corollary 13.15] claims that, if $\mathbf{K}$ is an algebraically closed field of characteristic zero, then $\mathbf{K}\langle\langle\varepsilon\rangle\rangle$ is the algebraic closure of the field of Laurent series $\mathbf{K}(\!(\varepsilon)\!)$. Remark that it is also a consequence of Theorems 4.1.24 and 4.1.11 and 4.1.13 since $\mathbf{R}\langle\langle\varepsilon\rangle\rangle[i] = \mathbf{R}[i]\langle\langle\varepsilon\rangle\rangle$. The Newton-Puiseux theorem has an important historic application, which motivated the introduction of Puiseux series, for the study of plane algebraic curves (see [Eis95, Corollary 13.16]).

4.2 Semi-algebraic sets and maps

We recall here some basic ingredients of semi-algebraic geometry. In the following, let $n > 0$, and $\boldsymbol{X} = x_1, \ldots, x_n$ be indeterminates. We also fix a real closed field $\mathbf{R}$, and let $\mathbf{C}$ be its algebraic closure. When omitted, we refer to [BCR98] and [BPR06] for the definitions and results introduced here.

4.2.1 Semi-algebraic sets

Following the algebro-geometric spirit of Chapter 2, in real algebraic geometry we first consider the real counterpart of algebraic sets.

Definition 4.2.1. A *real algebraic set* of $\mathbf{R}^n$ is a subset of $\mathbf{R}^n$ that can be written as

$$\{\boldsymbol{y} \in \mathbf{R}^n \mid f_1(\boldsymbol{y}) = 0, \ldots, \ f_p(\boldsymbol{y}) = 0\},$$

where $f_1, \ldots, f_p \in \mathbf{R}[x_1, \ldots, x_n]$.

The following proposition shows the first difference with algebraic sets. It can be easily proved that any real algebraic set can be defined by a single equation, by considering the sum of the squares of the polynomials defining the real algebraic set.

Proposition 4.2.2. *Any real algebraic set of $\mathbf{R}^n$ can be written as the zero-set of a single $f \in \mathbf{R}[\boldsymbol{X}]$.*

Example 4.2.3. Let $E = \{\boldsymbol{x} \in \mathbf{R}^n \mid \boldsymbol{f}(\boldsymbol{x}) = 0\}$ where $\boldsymbol{f} \subset \mathbf{R}[x_1, \ldots, x_n]$, be a real algebraic set of $\mathbf{R}^n$. Then $V = \{\boldsymbol{x} \in \mathbf{C}^n \mid \boldsymbol{f}(\boldsymbol{x}) = 0\}$ is an algebraic set of $\mathbf{C}^n$ and $E = V \cap \mathbf{R}^n$.

This is an example of importance as in the second part of this thesis we will extensively study real algebraic sets through the algebraic set defined by some defining polynomials. This allows one to use the powerful machinery of algebraic geometry from the previous chapters. Finally, one ultimately considers the real trace of the objects in consideration.

However, we need to consider a more general family of sets defined over $\mathbf{R}^n$ for stability reasons.

Definition 4.2.4. A *semi-algebraic set* of $\mathbf{R}^n$ is a subset of $\mathbf{R}^n$ that can be written as a finite union of basic semi-algebraic sets of the form:

$$\{\boldsymbol{y} \in \mathbf{R}^n \mid f_1(\boldsymbol{y}) = \cdots = f_p(\boldsymbol{y}) = 0, \ g_1(\boldsymbol{y}) > 0, \ldots, \ g_q(\boldsymbol{y}) > 0\},$$

where $f_1, \ldots, f_p, g_1, \ldots g_q \in \mathbf{R}[x_1, \ldots, x_n]$.

Example 4.2.5.

a) Every real algebraic set of $\mathbf{R}^n$ is a semi-algebraic set.

b) Every interior of a polygon (resp. polyhedra) is a semi-algebraic set of $\mathbb{R}^2$ (resp. of $\mathbb{R}^3$).

c) The following sets are *not* semi-algebraic sets: $\mathbb{Z}^n$, $\{(x,y) \in \mathbb{R}^2 \mid y = \cos(x)\}$ and the infinite "zigzag" $\{(x,y) \in \mathbb{R}^2 \mid y = d(x,\mathbb{Z}) = |x - \lfloor x + 1/2 \rfloor|\}$.

d) The semi-algebraic sets of $\mathbf{R}$ are exactly the finite unions of points and open intervals.

The following proposition ensures that the family of semi-algebraic sets is stable under finitely many elementary set operations.

Proposition 4.2.6. *Let $A \subset \mathbf{R}^n$ and $B \subset \mathbf{R}^n$, for $m > 0$, be semi-algebraic sets. Then,*

1. *$\mathbf{R}^n - A$ is a semi-algebraic set of $\mathbf{R}^n$;*
2. *if $m = n$, $A \cup B$ and $A \cap B$ are semi-algebraic sets of $\mathbf{R}^n$;*
3. *$A \times B$ is a semi-algebraic set of $\mathbf{R}^{n+m}$.*

The following striking theorem is fundamental in computational semi-algebraic geometry. Together with the above proposition, it shows that the family of semi-algebraic sets enjoy strong stability properties. The first proof has been given by Tarski [Tar51], and made completely effective in a following paper of Seidenberg [Sei54].

Theorem 4.2.7 (Tarski-Seidenberg Theorem [BPR06, Theorem 2.92])**.** *Let $S \subset \mathbf{R}^{n+1}$ and $\pi : \mathbf{R}^{n+1} \to \mathbf{R}^n$ be the projection on the first n coordinates. Then, $\pi(S)$ is a semi-algebraic set of $\mathbf{R}^n$.*

However, the projection of a real algebraic set is, in general, not a real algebraic set, but it is a semi-algebraic set. Conversely, Motzkin [Mot70] proved that every semi-algebraic set of $\mathbf{R}^n$ is actually the projection of a real algebraic set of $\mathbf{R}^{n+1}$. An important application of the two previous stability results is the following reformulation. This illustrates the ubiquity of semi-algebraic sets in real algebraic geometry.

Definition 4.2.8 ([BCR98, Definition 2.2.3])**.** A first-order formula in the language of the ordered fields, with parameters in $\mathbf{R}$, is a formula written as finite conjunctions, disjunctions, negations, and universal or existential quantifiers in $\mathbf{R}$ on variables $y_1, \ldots, y_m$, starting from atomic formulas which are of the type $f(y_1, \ldots, y_m) = 0$ of $g(y_1, \ldots, y_m) > 0$, where $f, g \in \mathbf{R}[y_1, \ldots, y_m]$.

The free variables $x_1, \ldots, x_n$ of a formula Φ are the ones appearing in the formula, which are not quantified. In this case, we note $\Phi(x_1, \ldots, x_n)$. The realization of Φ, is the set of $\boldsymbol{x} \in \mathbf{R}^n$ such that $\Phi(\boldsymbol{x})$ is true. Finally, a quantifier-free formula is a formula involving no quantifiers or, equivalently, involving only free variables.

Looking at the above definitions, semi-algebraic sets can be naturally written as the realization of quantifier-free formulas and conversely. The conjunction of Proposition 4.2.6 and Theorem 4.2.7 gives way more. Indeed, the realization of existential (and universal by negation) quantifiers can be seen as projections of realizations of formulas with fewer (one-block) quantifiers.

Theorem 4.2.9 ([BCR98, Theorem 2.2.4])**.** *Let $\Psi(x_1, \ldots, x_n)$ be a first-order formula in the language of the ordered fields, with coefficients in $\mathbf{R}$. Then the realization of Φ is a semi-algebraic set.*

Example 4.2.10.

a) Let $\Phi(x, y)$ be the formula "$\exists z \in \mathbf{R}$ s.t. $x^2 + y^2 + z^2 = 1$". According to the above theorem, the realization of Φ is a semi-algebraic set. In this case, it is the unit disk $\{(x, y) \in \mathbf{R}^2 \text{ s.t. } x^2 + y^2 \leq 1\}$. Remark that the realization of $\Phi(x, y)$ can also be seen as the projection of the 2-sphere $S = \{(x, y, z) \in \mathbf{R}^3 \text{ s.t. } x^2 + y^2 + z^2 = 1\}$ on the first two coordinates. Hence, Theorem 4.2.7, gives the same conclusion.

b) ([BPR06, Remark 3.2]) Let $S = \{(x, y) \in \mathbf{R}^2 \text{ s.t. } x^3 - x^2 - y^2 > 0\}$, and

$$\overline{S} = \{(x, y) \in \mathbf{R}^2 \text{ s.t. } \forall r > 0, \exists (x', y') \in S, \ (x - x')^2 + (y - y')^2 < r^2\}.$$

Then, by Theorem 4.2.9, $\overline{S}$ is a semi-algebraic set. Such a set will be called the Euclidean closure of S in the next subsection. It is worth noting that $\overline{S} = \{(x, y) \in \mathbf{R}^2 \text{ s.t. } x^3 - x^2 - y^2 \geq 0 \quad \text{and} \quad x \geq 1\}$ and not $\{(x, y) \in \mathbf{R}^2 \text{ s.t. } x^3 - x^2 - y^2 \geq 0\}$ as one could expect.

c) ([BCR98, Example 2.1.5.e]) The realization of the formula $\Phi(x, y)$: "$\exists n \in \mathbb{N}$ s.t. $y = nx''$ is not a semi-algebraic set. Indeed, as Φ is a first-order formula, in the language of the ordered fields, its parameter n does not range over a real closed field.

A reformulation of Theorem 4.2.9 is that the realization of any such formula can be written as the realization of a quantifier-free formula. A direct consequence is the decidability of the first-order theory of real closed fields (that is involving only first-order formulas). Although the original proof of Theorem 4.2.7 was constructive, its complexity cannot be bounded by any finite tower of exponents, which makes it impractical for actual computations. We will discuss more in detail the algorithmic aspects of quantifier elimination later in Chapter 5.

4.2.2 Topology of semi-algebraic sets

In order to work with semi-algebraic sets, we introduce in this section the Euclidean topology on $\mathbf{R}^n$, that derives from the classical one on $\mathbb{R}^n$. For that, we use the ordering structure on $\mathbf{R}$ to define the following basic objects.

Definition 4.2.11. Let $\boldsymbol{y} \in (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \in \mathbf{R}^n$, $r \in \mathbf{R}$ and $r > 0$. We denote by:

- $||\boldsymbol{y}||$ the unique positive square root of $\boldsymbol{y}_1^2 + \cdots + \boldsymbol{y}_n^2$;
- $B_n(\boldsymbol{y}, r) = \{\boldsymbol{z} \in \mathbf{R}^n \text{ s.t. } ||\boldsymbol{y} - \boldsymbol{z}|| < r\}$ the *open* ball of radius r, centered at $\boldsymbol{y}$;
- $\overline{B_n}(\boldsymbol{y}, r) = \{\boldsymbol{z} \in \mathbf{R}^n \text{ s.t. } ||\boldsymbol{y} - \boldsymbol{z}|| \leq r\}$ the *closed* ball of radius r, centered at $\boldsymbol{y}$;
- $S^{n-1}(\boldsymbol{y}, r) = \{\boldsymbol{z} \in \mathbf{R}^n \text{ s.t. } ||\boldsymbol{y} - \boldsymbol{z}|| = r\}$ the $(n-1)$-*sphere* of radius r, centered at $\boldsymbol{y}$.

The *euclidean topology* on $\mathbf{R}^n$ is the one whose open sets are the unions of open balls. Recall that the closed sets are then, the complements of the open sets. Moreover, for a set $S \subset \mathbf{R}^n$, we note $\overline{S}$ the (Euclidean) *closure* of S, that is the intersection of all closed sets containing S (for the Euclidean topology).

Remark 4.2.12. Note that, $B_n(\boldsymbol{y}, r)$, $\overline{B_n}(\boldsymbol{y}, r)$ and $S^{n-1}(\boldsymbol{y}, r)$ are semi-algebraic sets. Moreover, according to Theorem 4.2.9, the closure of a semi-algebraic set is a semi-algebraic set. Hence, semi-algebraic sets behave well with the Euclidean topology on $\mathbf{R}^n$.

We now focus on the notion of connectivity for semi-algebraic sets. This notion will be central to this thesis.

Definition 4.2.13 ([BCR98, Definition 2.4.2])**.** A semi-algebraic set S of $\mathbf{R}^n$ is *semi-algebraically connected* if S is not the disjoint union of two non-empty semi-algebraic sets that are both closed in S.

The following example, from [BPR06, Section 3.2], illustrates why a semi-algebraic definition of connectedness is required when dealing with arbitrary closed fields.

Example 4.2.14. Consider $\mathbf{R}$ to be $\mathbb{R}_{\text{alg}}$, the field of real algebraic numbers. Then, we have the following disjoint union:

$$\mathbb{R}_{\text{alg}} \;=\; \mathbb{R}_{\text{alg}} \cap (-\infty, \pi) \quad \bigcup \quad \mathbb{R}_{\text{alg}} \cap (\pi, +\infty)$$

The sets are both closed in $\mathbb{R}_{\text{alg}}$, as each one is the complement of the other, and is open in $\mathbb{R}_{\text{alg}}$. However, neither $\mathbb{R}_{\text{alg}} \cap (-\infty, \pi)$ nor $\mathbb{R}_{\text{alg}} \cap (\pi, +\infty)$ are semi-algebraic sets of $\mathbb{R}_{\text{alg}}$, as these are finite unions of points and open interval, and $\pi \notin \mathbb{R}_{\text{alg}}$. Thus $\mathbb{R}_{\text{alg}}$ is disconnected. However, $\mathbb{R}_{\text{alg}}$ is not semi-algebraically disconnected.

The following proposition ensures that the notion of semi-algebraic connectedness behaves well with elementary semi-algebraic sets.

Proposition 4.2.15 ([BPR06, Propositions 3.9, 3.11])**.** *The field $\mathbf{R}$, its intervals, and the open cubes $(0, 1)^n$ are semi-algebraically connected.*

We end this subsection with the fundamental theorem about semi-algebraically connected sets.

Theorem 4.2.16 ([BCR98, Theorem 2.4.4])**.** *Every semi-algebraic set $S \subset \mathbf{R}^n$ is a disjoint union of a finite number of non-empty semi-algebraically connected semi-algebraic sets $C_1, \ldots, C_N$ which are both open and closed in S. The sets $C_1, \ldots, C_N$ are called the* semi-algebraically connected components *of S.*

The following direct consequence will be useful when characterizing the semi-algebraically connected components of a semi-algebraic set.

Proposition 4.2.17. *Using the same notations as in the above theorem, let $\boldsymbol{x} \in S$. Then, there is a unique $1 \leq i \leq N$, such that C_i contains $\boldsymbol{x}$ and C_i is the union of all the semi-algebraically connected sets containing $\boldsymbol{x}$.*

In particular, any semi-algebraically connected semi-algebraic subset of S containing C_i equals C_i.

It is worth noting that, the fact that semi-algebraic sets have finitely many semi-algebraically connected component leads to natural algorithmic questions. In particular, this allows to compute finite representations of these components and to bound the complexity of these procedures. Together with Theorem 4.2.7, these results constitute the theoretic foundations of computational real algebraic geometry as we will discuss in Chapter 5.

4.2.3 Semi-algebraic maps

We now consider, together with the notion of semi-algebraic sets, the family of maps that preserve this structure. In this subsection, we consider two semi-algebraic sets $A \subset \mathbf{R}^n$ and $B \subset \mathbf{R}^m$.

Definition 4.2.18. A map $f\colon A \to B$ is *semi-algebraic* if its graph

$$\text{Graph}(f) = \{(\boldsymbol{x}, f(\boldsymbol{x})) \text{ for } \boldsymbol{x} \in A\},$$

is a semi-algebraic set of $\mathbf{R}^{n+m}$.

Proposition 4.2.19. *Let $f : A \to B$ be a semi-algebraic map then:*

1. *the composition $g \circ f$ is a semi-algebraic map, for any semi-algebraic set C and semi-algebraic map $g : B \to C$;*
2. *for any semi-algebraic sets $A' \subset A$ and $B' \subset B$, the sets $f(B')$ and $f^{-1}(B')$ are semi-algebraic sets of $\mathbf{R}^n$ and $\mathbf{R}^m$ respectively.*

As we defined a topology for the semi-algebraic sets, an important family of semi-algebraic maps are the ones preserving the open sets.

Definition 4.2.20. We say that $f : A \to B$ is a semi-algebraic *continuous* map if, for every semi-algebraic *open* subset $B' \subset B$, $f^{-1}(B')$ is open.

As for semi-algebraic maps, the family of semi-algebraic continuous maps is stable under composition and arithmetic operations.

Example 4.2.21.

a) Any (restriction to a semi-algebraic set of a) polynomial map, with coefficients in $\mathbf{R}$, is a semi-algebraic continuous map.

b) The function $x \in [-1, 1] \mapsto \sqrt{1 - x^2} \in [1, 1]$ whose graph is the upper-half unit circle is semi-algebraic.

c) Any rational fraction f/g, where $f, g \in \mathbf{R}[x]$, restricts to a semi-algebraic map on the semi-algebraic set $\{x \in \mathbf{R} \text{ s.t. } g(x) \neq 0\}$ (and any semi-algebraic subsets of it). In particular, any birational map (see Definition 2.3.26) h restricts to a bijective map on a non-empty semi-algebraic set, such that, both h and h^{-1}, are semi-algebraic and continuous maps.

The last above example revealed an important subfamily of semi-algebraic continuous maps that preserve the topological properties of semi-algebraic sets.

Definition 4.2.22. We say that $f : A \to B$ is a semi-algebraic *homeomorphism* if f is a bijection such that both f and f^{-1} are semi-algebraic continuous maps.

We end this subsection by giving a direct, but important result on the stability of semi-algebraic connectedness with respect to semi-algebraic homeomorphisms.

Proposition 4.2.23 ([BPR06, Exercise 3.8])**.** *Let $f\colon A \to B$ be a semi-algebraic homeomorphism. Then, the semi-algebraically connected subsets of A and B are in correspondence through f. In particular, the semi-algebraically connected components of A and B are in* one-to-one *correspondence through f.*

A noticeable application of the above result in this thesis will be when f is the restriction of an isomorphism of algebraic sets, to their real traces.

Another important example of semi-algebraic continuous maps in this work will be the following one.

Definition 4.2.24. Let $\boldsymbol{y}, \boldsymbol{y}' \in A$. A *semi-algebraic path connecting $\boldsymbol{y}$ to $\boldsymbol{y}'$ in A,* is a semi-algebraic continuous map $\gamma : [0,1] \to A$ such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(1) = \boldsymbol{y}'$.

These semi-algebraic paths are ubiquitous when studying the semi-algebraic connectedness of semi-algebraic sets. Indeed, unlike the Euclidean topology, the notions of connectedness and path-connectedness coincide for semi-algebraic sets.

Theorem 4.2.25 ([BPR06, Theorem 5.23])**.** *A semi-algebraic set S is semi-algebraically connected if and only if for every pair $(\boldsymbol{y}, \boldsymbol{y}') \in S^2$, there exists a semi-algebraic path connecting $\boldsymbol{y}$ to $\boldsymbol{y}'$ in S (that is S is semi-algebraically path connected).*

Note that in classical geometry, a set can be connected while not being path-connected. A counter-example is the topological closure of the graph of the function $f\colon x \in]0,1] \mapsto \sin(\frac{1}{x}) \in \mathbb{R}$. However, the latter set is not semi-algebraic. In fact, according to [BPR06, Theorem 5.22], a semi-algebraic set of $\mathbb{R}^n$ is semi-algebraically connected if, and only if, it is connected (in the usual sense).

4.2.4 Extension of semi-algebraic sets and functions

In this subsection, we consider an arbitrary closed field $\mathbf{R}$ and a real closed extension $\mathbf{R}'$, whose unique order extends the one of $\mathbf{R}$ (e.g. $\mathbf{R}' = \mathbf{R}\langle\varepsilon\rangle$).

We start by the Transfer Principle on real closed fields, that allow us to extend first-order formulas to real closed extensions.

Theorem 4.2.26 ([BPR06, Theorem 2.98])**.** *Let $\mathbf{R}'$ be a real closed extension of $\mathbf{R}$ and Φ be a first-order formula in the language of the ordered fields, with parameters in $\mathbf{R}$. Then Φ is true in $\mathbf{R}$ if and only if it is true in $\mathbf{R}'$.*

Hence, according to the Tarski-Seindenberg theorem, this leads to the following definition for extension of semi-algebraic sets.

Definition 4.2.27. Let S be a semi-algebraic set of $\mathbf{R}^n$, and $\Phi(\boldsymbol{X})$ be a quantifier-free formula, whose realization in $\mathbf{R}^n$ is S. Then, the *extension of S to $\mathbf{R}'$,* is defined as the realization of $\Phi(\boldsymbol{X})$ in $(\mathbf{R}')^n$, that is the set of points $\boldsymbol{y} \in (\mathbf{R}')^n$ such that $\Phi(\boldsymbol{y})$ is true. We denote this extension by $\mathrm{ext}(S, \mathbf{R}')$ and it does not depend of Φ.

A direct consequence of this definition is the following one.

Proposition 4.2.28 ([BPR06, Proposition 2.105]). *The inclusion mapping $S \subset \mathbf{R}^n \mapsto \operatorname{ext}(S, \mathbf{R}') \subset (\mathbf{R}')^n$ preserves the Boolean operations (finite intersection, finite union, and complementation) and the inclusion.*

Example 4.2.29. Let S be the semi-algebraic set $(2,3) \cap \mathbb{R}_{\text{alg}}$ of $\mathbb{R}_{\text{alg}}$. Then, the Euler number $e \notin S$ but $e \in \operatorname{ext}(S, \mathbb{R})$.

The extension operation also preserve semi-algebraic connectedness as the following proposition shows.

Proposition 4.2.30 ([BPR06, Proposition 5.24]). *Let S be a semi-algebraic set of $\mathbf{R}^n$, and $C_1, \ldots, C_\ell$ be its semi-algebraically connected components. Then $\operatorname{ext}(C_1, \mathbf{R}'), \ldots, \operatorname{ext}(C_\ell, \mathbf{R}')$ are the semi-algebraically connected components of $\operatorname{ext}(S, \mathbf{R}')$.*

In particular, S is semi-algebraically connected component if and only if $\operatorname{ext}(S, \mathbf{R}')$ is.

As semi-algebraic sets, semi-algebraic maps can be extended to larger real closed fields.

Definition 4.2.31. Let $f\colon S \to T$ be a semi-algebraic map. Then, $\operatorname{ext}(\operatorname{Graph}(f), \mathbf{R}')$ is the graph of a semi-algebraic map

$$\operatorname{ext}(f, \mathbf{R}')\colon \operatorname{ext}(S, \mathbf{R}') \to \operatorname{ext}(T, \mathbf{R}'),$$

that is called the extension of f to $\mathbf{R}'$.

Proposition 4.2.32. *With the notation of the above definition, for any semi-algebraic subsets $A \subset S$ and $B \subset T$, the following holds:*

$$\operatorname{ext}(f(A), \mathbf{R}') = \operatorname{ext}(f, \mathbf{R}')\Big(\operatorname{ext}(A, \mathbf{R}')\Big);$$
$$\operatorname{ext}(f^{-1}(B), \mathbf{R}') = \operatorname{ext}(f, \mathbf{R}')^{-1}\Big(\operatorname{ext}(B, \mathbf{R}')\Big).$$

In particular, the extension of a semi-algebraic homeomorphism is still a semi-algebraic homeomorphism.

The case where $\mathbf{R}' = \mathbf{R}\langle\varepsilon\rangle$ is of particular interest, as it allows one to work with semi-algebraic sets and maps at some infinitesimal neighborhood, considering their extension to $\mathbf{R}\langle\varepsilon\rangle$. This brings methods from analysis to the current algebraic settings. The following result is an illustration of this use.

Proposition 4.2.33 ([BPR06, Proposition 3.6]). *Let S be a semi-algebraic set and f be a semi-algebraic map defined on S. Then, f is continuous in $\boldsymbol{x} \in S$ if and only if for all $\boldsymbol{y} \in \operatorname{ext}(S, \mathbf{R}\langle\varepsilon\rangle)$*

$$\lim_\varepsilon \operatorname{ext}(f, \mathbf{R}\langle\varepsilon\rangle)(\boldsymbol{y}) = f(\boldsymbol{x}).$$

This characterization of continuity gives the intuition of the algebraic Puiseux series to behave as semi-algebraic paths, of infinitesimal length, lying in the prescribed semi-algebraic set. The next section aims to precise this intuition using the notion of semi-algebraic germs.

4.3 Semi-algebraic germs

Let us now examine an alternative geometric description of algebraic Puiseux series. We follow here the approach presented in [BPR06, Section 3.3].

Definition 4.3.1. The set of *germs of semi-algebraic continuous functions at the right of the origin* is the set of the equivalence classes of semi-algebraic continuous functions $f\colon (0,t) \to \mathbf{R}$, for $t > 0$, with respect to the equivalent relation:

$$f \sim g \text{ if and only if there exists } t_0 > 0 \text{ such that } f(t) = g(t) \text{ for every } t \in (0, t_0).$$

This set can be equipped with a ring structure that naturally derive from the one of the ring of semi-algebraic functions. In particular, the 0 (respectively 1) of this new ring is the germ associated with the constant 0 (respectively 1) function. Moreover, as the semi-algebraic sets of $\mathbf{R}$ are finite union of points and open intervals, for any representative f of a germ φ, there exists $t_0 > 0$ such that f does not vanish on $(0, t_0)$. Hence, the inverse of $\varphi \neq 0$ can be defined, along with its sign, which matches that of f on the interval $(0, t_0)$. One checks that the algebraic structure and order thus defined make the set of germs of semi-algebraic continuous functions an *ordered field*.

The following theorem states that this structure constitutes a real closed field. Moreover, by [BPR06, Proposition 2.104], it is an algebraic extension of $\mathbf{R}(\varepsilon)$, which gives the second part of statement of the theorem.

Theorem 4.3.2 ([BPR06, Theorem 3.13, 3.16 & 3.17])**.** *The set of germs of semi-algebraic continuous functions at the right of the origin is a real closed field.*

Moreover, it is the real closure of $\mathbf{R}(\varepsilon)$ equipped with the order defined in Proposition 4.1.21. Hence it is isomorphic to the field of algebraic Puiseux series $\mathbf{R}\langle\varepsilon\rangle$.

Remark 4.3.3. The isomorphic equivalence between these two fields can be understood as follows. Let $\varepsilon > 0$ and $f : (0, \varepsilon) \to \mathbf{R}$ be a continuous semi-algebraic function. According to [BPR06, Proposition 2.104], the graph of f is a branch of a real algebraic plane curve, that is, there exists a non-zero polynomial $P \in \mathbf{R}[t, s]$ such that $P(t, f(t)) = 0$ for every $t \in (0, \varepsilon)$. Besides, according to the Newton-Puiseux theorem [Wal78, Theorem 3.1], the latter branch can be parameterized by a Puiseux series, that is, there exists $\sigma \in \mathbf{R}\langle\langle t \rangle\rangle$ such that

$$f(t) = \sigma(t) \quad \text{for all} \quad t \in (0, \varepsilon).$$

Since by definition $P(t, \sigma) = 0$, then σ is algebraic over $\mathbf{R}$ i.e. $\sigma \in \mathbf{R}\langle t \rangle$.

Remark 4.3.4. According to the proof of the above theorem – see e.g. [BPR06, p.102] –, $1 \in \mathbf{R}(\varepsilon)$ is sent to the class of the constant function $t \in (0, 1) \mapsto 1 \in \mathbf{R}$ and $\varepsilon \in \mathbf{R}(\varepsilon)$ is sent to the class of the identity map $t \in (0, 1) \mapsto t \in \mathbf{R}$.

We end this section with important results that derive from this alternative representation.

Proposition 4.3.5 ([BPR06, Proposition 3.19])**.** *Let S be a semi-algebraic subset of $\mathbf{R}^n$ and*

$$\varphi = (\varphi_1, \ldots, \varphi_n) \in \mathbf{R}\langle\varepsilon\rangle^n.$$

Let $f_1, \dots, f_n$ be representatives of $\varphi_1, \dots, \varphi_n$, on a common segment $(0, t_0)$, where $t_0 > 0$. We note $\boldsymbol{f} = (f_1, \dots, f_n)$. Then, the following holds:

$$\varphi \in \operatorname{ext}(S, \mathbf{R}\langle\varepsilon\rangle) \iff \exists\, t_0' \in (0, t_0),\ \forall\, t \in (0, t_0'),\ \boldsymbol{f}(t) \in S.$$

Another important property of $\mathbf{R}\langle\varepsilon\rangle$ is that, sentences that are true on $\mathbf{R}[\varepsilon]$, are also true on a sufficiently small interval $(0, r) \subset \mathbf{R}$.

Proposition 4.3.6 ([BPR06, Proposition 3.20])**.** *Let Φ be a first-order formula in the language of ordered fields, with coefficients in $\mathbf{R}[\varepsilon]$ and for $t \in \mathbf{R}$, let $\Phi'(t)$ be the sentence obtained by replacing ε with t in Φ.*

Then, Φ is true if and only if there exists $t_0 \in \mathbf{R}$ such that $\Phi'(t)$ is true for every $t \in (0, t_0)$.

Example 4.3.7. Let S be a semi-algebraic set of $\mathbf{R}^n$ and let $\boldsymbol{x}$ be a point in the closure of S. Then,

$$\forall\, t > 0,\ B(\boldsymbol{x}, t) \cap S \neq \emptyset.$$

The sentences defining S and $B(0, t)$ are in the language of ordered fields with coefficients in $\mathbf{R}[t]$. Hence by Proposition 4.3.6,

$$B(\boldsymbol{x}, \varepsilon) \cap \operatorname{ext}(S, \mathbf{R}') \neq \emptyset.$$

This is actually the core of Theorem 4.3.9.

The following proposition comes directly from [BPR06, Proposition 3.21]. We propose here a more detailed statement, that will be useful in some proofs of Chapter 6. As it requires some precautions, we propose an extended version of the proof proposed in [BPR06, Proposition 3.21].

Proposition 4.3.8 ([BPR06, Proposition 3.21])**.** *Let a be a positive element of $\mathbf{R}$ and let $f\colon (0, a) \to \mathbf{R}$ be a continuous, bounded, semi-algebraic function. Then there exists a continuous, bounded, semi-algebraic function $\overline{f}\colon [0, a) \to \mathbf{R}$ that extends f and such that:*

$$\overline{f}(0) = \lim_{\varepsilon} \varphi,$$

where φ is the semi-algebraic germ of f at the right of the origin.

Proof. Let φ be the germ of f at the right of the origin. Since f is bounded on $(0, a)$, then φ is bounded by an element of $\mathbf{R}$ by Proposition 4.3.5. Hence, $\varphi \in \mathbf{R}\langle\varepsilon\rangle_b$ and $\ell = \lim_{\varepsilon} \varphi$ is defined. Let $\overline{f}\colon [0, a) \to \mathbf{R}$ be such that

$$\overline{f}(t) = \begin{cases} \ell & \text{if } t = 0; \\ f(t) & \text{else.} \end{cases}$$

The graph of $\overline{f}$ is the union of the graph of f with the point $\{(0, \ell)\}$, then $\overline{f}$ is semi-algebraic and bounded. Let $\eta > 0$ and $X = \{t \in \mathbf{R} \mid |f(t) - \ell| < \eta\}$. Since $\lim_{\varepsilon}(f(\varepsilon) - \ell) = 0$, then

$f(\varepsilon) - \ell$ is an infinitesimal over $\mathbf{R}$ and $\varepsilon \in \mathrm{ext}(X, \mathbf{R}\langle\varepsilon\rangle)$. Then, by Proposition 4.3.5, there exists $t_0 \in \mathbf{R}$ such that,

$$\forall t \in (0, a), |t| < t_0 \Longrightarrow |f(t) - \ell| < \eta,$$

as ε is associated with the germ of the identity map. Hence $\overline{f}$ is continuous in 0. Finally, as f is continuous on $(0, a)$, the bounded semi-algebraic function $\overline{f}$ is continuous on $[0, a)$. □

An important consequence is the following one.

Theorem 4.3.9 (Curve selection lemma [BPR06, Theorem 3.22])**.** *Let S be a semi-algebraic set of $\mathbf{R}^n$ and let $\boldsymbol{x}$ be in its closure $\overline{S}$. Then there exists a semi-algebraic path $\gamma\colon [0, 1) \to \overline{S}$ such that*

$$\gamma(0) = \boldsymbol{x} \quad \textit{and} \quad \gamma((0, 1)) \subset S.$$

This theorem concretely illustrates the isomorphic correspondence between the algebraic Puiseux series and the germs of semi-algebraic functions at the right of the origins. Indeed, from this result, one can associate the infinitesimally close points from an algebraic set S – that is in $\overline{S}$ – to semi-algebraic paths lying in S at the right of the origin, ending in $\overline{S}$.

As for the notion of connectedness, the compact sets[1] do not behave as well in the Euclidean topology on $\mathbf{R}^n$, than in the one on $\mathbb{R}^n$. For instance, closed intervals such as $[0, 1]$ in $\mathbb{R}_{\mathrm{alg}}$ of $\mathbf{R}\langle\varepsilon\rangle$ are not compact, neither the images of such sets through continuous functions [BPR06, §3.4]. However, closed semi-algebraic sets (such as $[0, 1]$) enjoy some of the properties sought for compact ones, as the following important one.

Proposition 4.3.10 ([BPR06, Theorem 3.23])**.** *Let S be a closed, bounded semi-algebraic set and let f be a semi-algebraic continuous function defined on S. Then $f(S)$ is a closed and bounded semi-algebraic set.*

4.4 Real algebraic differential geometry

In the previous sections, we introduced the foundational notions of real algebraic geometry through the introduction of semi-algebraic sets and maps on real closed fields (and their extension), followed by various properties. We end this chapter by listing some fundamental results from this theory. Many of these results find their origin from classic theorems of the theory of differentiable manifolds on $\mathbb{R}$. We do not intend to provide an exhaustive overview of the topic; instead, we refer the reader to the classic literature [BCR98, BPR06], from which this content is primarily sourced. Note that many results presented here can be generalized to o-minimal structures that include for instance classes of sets definable with the exponential functions (see [Dri98]).

[1] Recall that a compact set is a set for which every open covering has a finite subcovering.

4.4.1 Implicit Function Theorem

Definition 4.4.1. Let $f : (a, b) \to \mathbf{R}$ be a semi-algebraic function, we say that f is *differentiable* at $x \in (a, b)$, with derivative $f'(x)$ if

$$\forall\, r > 0,\ \exists\, \delta > 0,\ \forall h, \quad |h| < \delta \Longrightarrow \left| \frac{f(x+h) - f(x)}{h} - f'(x) \right| < r;$$

we also say that $\lim_{h \to 0} (f(x+h) - f(x))/h = f'(x)$.

We say that f is differentiable on an open semi-algebraic subset $U \subset (a, b)$ if it is differentiable at every $x \in U$. In this case,

$$\begin{array}{rccc} f' : & U & \longrightarrow & \mathbf{R} \\ & x & \longmapsto & f'(x) \end{array}$$

is the *derivative* of f on U.

From the above definition of the derivative, it is defined by a first-order formula in the language of the ordered fields, with parameters in $\mathbf{R}$. Hence, the following proposition is a direct consequence of Theorem 4.2.9.

Proposition 4.4.2. *[BCR98, Proposition 2.9.1] Let $f : (a, b) \to \mathbf{R}$ be a semi-algebraic function, differentiable on some open semi-algebraic subset $U \subset (a, b)$, then f is continuous and its derivative f' is a semi-algebraic function.*

We classically extend these definitions to semi-algebraic maps as follows.

Definition 4.4.3. Let $f : U \subset \mathbf{R}^n \to \mathbf{R}$ be a multivariate semi-algebraic function. Let $1 \leq i \leq n$, we say that f admits a *partial derivative* $\frac{\partial f}{\partial x_i}$ at $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \in U$, with respect to the variable x_i, if

$$\lim_{h \to 0} \frac{f(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{i-1}, \boldsymbol{y}_i + h, \boldsymbol{y}_{i+1}, \ldots, \boldsymbol{y}_n) - f(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n)}{h} = \frac{\partial f}{\partial x_i}(\boldsymbol{y}).$$

If $f = (f_1, \ldots, f_k) : U \to \mathbf{R}^k$ is a semi-algebraic map, then the *Jacobian matrix* of f at $\boldsymbol{y} \in U$, is the matrix

$$\mathrm{Jac}_{\boldsymbol{y}}(f) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1}(\boldsymbol{y}) & \cdots & \frac{\partial f_1}{\partial x_n}(\boldsymbol{y}) \\ \vdots & & \vdots \\ \frac{\partial f_k}{\partial x_1}(\boldsymbol{y}) & \cdots & \frac{\partial f_k}{\partial x_n}(\boldsymbol{y}) \end{bmatrix},$$

whose determinant is called the *Jacobian* of f at $\boldsymbol{y}$. Finally the derivative $\mathrm{d}_{\boldsymbol{y}} f$ of f at $\boldsymbol{y}$ is the linear map from $\mathbf{R}^n$ to $\mathbf{R}^k$ whose matrix is $\mathrm{Jac}_{\boldsymbol{y}}(f)$.

It is clear from the definition that partial derivatives are semi-algebraic functions by Proposition 4.4.2. Since we defined properly the derivation of semi-algebraic maps of $\mathbf{R}^k$, one can naturally consider higher-order derivatives. Similarly to the class of $\mathscr{C}^k$ map, we define the so-called ring of Nash functions.

Definition 4.4.4. Let $U \subset \mathbf{R}^n$ and $V \subset \mathbf{R}^k$ be semi-algebraic sets with U open. The set of semi-algebraic maps from U to V which admit *continuous partial derivatives* up to order $\ell \geq 0$ is denoted by $\mathcal{S}^\ell(U, V)$.

The set $\mathcal{S}^\infty(U, V)$ is the intersection of all the sets $\mathcal{S}^\ell(U, V)$ for $\ell \geq 0$ and the ring $\mathcal{S}^\infty(U, \mathbf{R})$, abbreviated $\mathcal{S}^\infty(U)$, is called the ring of *Nash functions* from U to $\mathbf{R}$.

Example 4.4.5. The following functions are of Nash type: polynomials maps on $\mathbf{R}$, rational functions on their domain of definition, $x \mapsto \sqrt{1 - x^2}$ on $(-1, 1)$.

In the following, $\mathcal{S}^\ell$ for $1 \leq \ell \leq \infty$, will denote either any $\mathcal{S}^\ell$ for $\ell \geq 1$, or $\mathcal{S}^\infty$. We extend the notion of semi-algebraic homeomorphisms to this class of sets.

Definition 4.4.6 ([BCR98, Definition 2.9.2-3])**.** Let $\ell \geq 1$, and let $U \subset \mathbf{R}^n$ and $V \subset \mathbf{R}^k$ be semi-algebraic open sets. A *$\mathcal{S}^\ell$-diffeomorphism* f from U to V is a semi-algebraic bijection from U to V such that $f \in \mathcal{S}^\ell(U, V)$ and $f^{-1} \in \mathcal{S}^\ell(V, U)$. When $l = \infty$, f is called a *Nash diffeomorphism*.

Recall that a semi-algebraic open neighborhood of a point $\boldsymbol{y}_0 \in \mathbf{R}^n$ is a semi-algebraic open set containing $\boldsymbol{y}_0$.

Theorem 4.4.7 (Semi-algebraic Inverse Function Theorem [BCR98, Proposition 2.9.7])**.** *Let U_0 be a semi-algebraic open neighborhood of $0 \in \mathbf{R}^k$ and let $f \in \mathcal{S}^\ell(U_0, \mathbf{R}^k)$ where $1 \leq \ell \leq \infty$, such that $f(0) = 0$ and $\mathrm{Jac}_{\boldsymbol{y}}(f)$ is invertible.*

Then there exist semi-algebraic open neighborhoods U, V of $0 \in \mathbf{R}^k$, with $U \subset U_0$, such that f restricts to a $\mathcal{S}^\ell$-diffeomorphism from U to V.

Theorem 4.4.8 (Semi-algebraic Implicit Function Theorem [BCR98, Corollary 2.9.8])**.** *Let W be a semi-algebraic open neighborhood of a point $(\boldsymbol{x}^0, \boldsymbol{y}^0) \in \mathbf{R}^{n+k}$. Let $1 \leq \ell \leq \infty$ and $\boldsymbol{g} \in \mathcal{S}^\ell(W, \mathbf{R}^k)$ be a semi-algebraic map such that $\boldsymbol{g}(\boldsymbol{x}^0, \boldsymbol{y}^0) = 0$ and $\mathrm{Jac}_{(\boldsymbol{x}^0, \boldsymbol{y}^0)}(\boldsymbol{g}(\boldsymbol{x}_0, \cdot))$ is invertible.*

Then, there exist semi-algebraic open neighborhoods U and V of $\boldsymbol{x}^0$ and $\boldsymbol{y}^0$, respectively, and a semi-algebraic map $\boldsymbol{f} \in \mathcal{S}^\ell(U, V)$ such that $\boldsymbol{f}(\boldsymbol{x}^0) = \boldsymbol{y}^0$ and for all $(\boldsymbol{x}, \boldsymbol{y}) \in U \times V$, the following holds:

$$\boldsymbol{g}(\boldsymbol{x}, \boldsymbol{y}) = 0 \iff \boldsymbol{y} = \boldsymbol{f}(\boldsymbol{x})$$

4.4.2 Trivializations

In semi-algebraic geometry, we are interested in describing and classifying the topology of slices of the studied varieties. This is done through homeomorphisms that we call trivializations.

Definition 4.4.9 (Trivialization [CS95])**.** Let X, Y and Y' be semi-algebraic sets such that $Y' \subset Y$, and let $f \colon X \to Y$ be a continuous semi-algebraic map. A semi-algebraic *trivializa-*

tion of f over Y' with fiber F is a semi-algebraic homeomorphism $\Psi = (\Psi^0, f)\colon f^{-1}(Y') \to F \times Y'$ such that the following diagrams commutes:

$$\begin{array}{ccc} f^{-1}(Y') & \xrightarrow{\Psi} & F \times Y' \\ & \searrow^{f} & \downarrow{\scriptstyle \pi_{Y'}} \\ & & Y' \end{array}$$

where $\pi_{Y'}$ is the projection onto Y'. We say that Ψ is *compatible* with $X' \subset X$ if there is $F' \subset F$ such that $\Psi^{-1}(F' \times Y') = X' \cap f^{-1}(Y')$.

The following theorem, originally proved in a slightly weaker form by Hardt in [Har80], shows that any semi-algebraic map is trivial over finitely many regions. In other words, its fibers can be classified in finitely many types.

Theorem 4.4.10 (Semi-algebraic Hardt's triviality [BPR06, Theorem 5.46]). *Let $S \subset \mathbf{R}^n$ and $T \subset \mathbf{R}^k$ be semi-algebraic sets. Given a continuous semi-algebraic function $f : S \to T$, there exists a finite partition*

$$T = \bigcup_{i=1}^{n} T_i$$

into semi-algebraic sets, such that for each $i = 1, \ldots, n$ and any $\boldsymbol{x}_i \in T_i$ there exists a semi-algebraic trivialization $\Psi_i = (\Psi_i^0, f) : f^{-1}(T_i) \to T_i \times f^{-1}(\boldsymbol{x}_i)$ of f over T_i with fiber $f^{-1}(\boldsymbol{x}_i)$ such that $\Psi_i^0(\boldsymbol{y}) = (\boldsymbol{y})$ for all $\boldsymbol{y} \in f^{-1}(\boldsymbol{x}_i)$.

Moreover, if $S_1, \ldots, S_q$ are semi-algebraic subsets of S, then we can ask each Ψ_i to be compatible with every B_j, for $1 \leq j \leq q$.

An important application of the above theorem is the following one. It roughly says that semi-algebraic sets are locally homeomorphic to cones at non-isolated points. Recall that $S_{n-1}(\boldsymbol{x}, r)$ and $\overline{B}_n(\boldsymbol{x}, r)$ denote respectively the sphere and the closed ball of $\mathbf{R}^n$, centered at $\boldsymbol{x} \in \mathbf{R}^n$, with radius $r > 0$.

Theorem 4.4.11 (Local conic structure [BCR98, Theorem 9.3.6]). *Let S be a semi-algebraic subset of $\mathbf{R}^n$, and $\boldsymbol{x}$ a* non-isolated *point of S. Then there exist $r \in \mathbf{R}$, $r > 0$, and for every r', $0 < r' \leq r$, a semi-algebraic homeomorphism $\Psi : \overline{B}_n(x, r') \to \overline{B}_n(x, r')$ such that:*

- *$||\Psi(\boldsymbol{y}) - \boldsymbol{x}|| = ||\boldsymbol{y} - \boldsymbol{x}||$ for every $\boldsymbol{y} \in \overline{B}_n(\boldsymbol{x}, r')$;*
- *the restriction of Ψ to $S_{n-1}(\boldsymbol{x}, r')$ is the identity mapping;*
- *$\Psi\left(S \cap \overline{B}_n(\boldsymbol{x}, r')\right)$ is a cone with vertex $\boldsymbol{x}$ and base $S \cap S_{n-1}(\boldsymbol{x}, r')$.*

This will be particularly useful in Chapter 8 when studying plane curves locally at singularities, identifying the incoming/outgoing branches with their intersection to a sufficiently small circle. It is worth noting that a similar result exists for a retraction "at infinity": for a sufficiently large $r > 0$, a semi-algebraic set can be continuously retracted to its intersection with $\overline{B}_n(0, r)$; see [BCR98, Corollary 9.3.7] or [BPR06, Proposition 5.49].

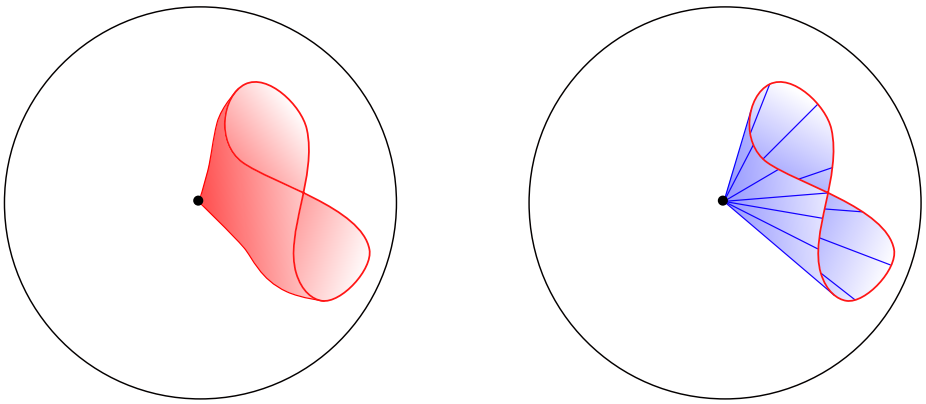


Figure 4.1. Illustration of the local conic structure at a point of a semi-algebraic set whose intersection with a ball is depicted in red on the left. Theorem 4.4.11 says that this intersection is homeomorphic with the cone generated by the intersection with the sphere. In other words, topologically speaking, "nothing happens" inside the ball.

The above Hardt's triviality gives the existence of a partition where a map can be trivialized, but does not provide any description of it. In particular, one can be interested in constructing (sub)-cells of this partition, or even deciding if a subset satisfies this. This is the purpose of Thom's isotopy lemma whose introduction (and its variants) will provide the rest of this section.

We first extend the classic notion of differentiable submanifolds to the Nash settings.

Definition 4.4.12 (Nash manifold [BCR98, Definition 2.9.9])**.** A semi-algebraic subset $M \subset \mathbf{R}^n$ is a *Nash submanifold* of $\mathbf{R}^n$ of *dimension* d if for every $\boldsymbol{y} \in M$, there exist

- open semi-algebraic neighborhoods Ω_0 and $\Omega_{\boldsymbol{y}}$ in $\mathbf{R}^n$ of respectively 0 and $\boldsymbol{y}$,
- a Nash diffeomorphism $\Psi : \Omega_0 \to \Omega_{\boldsymbol{y}}$, such that

$$\Psi(0) = \boldsymbol{y} \quad \text{and} \quad \Psi\Big((\mathbf{R}^d \times \{0\}) \cap \Omega_0)\Big) = M \cap \Omega_{\boldsymbol{y}}.$$

Moreover, we define the *tangent space* to M at $\boldsymbol{y}$ as the affine space:

$$\mathrm{T}_{\boldsymbol{y}}\, M = \boldsymbol{y} + \mathrm{d}_{\boldsymbol{y}}\varphi\left(\mathbf{R}^d \times \{0\}\right).$$

In other words, a Nash submanifold M of $\mathbf{R}^n$ of dimension d is at every point locally diffeomorphic (in terms of Nash functions) to some Euclidean space $\mathbf{R}^d$, so that it can be locally differentially parameterized by d variables. Moreover, according to [BPR06, Proposition 3.32], for any $\boldsymbol{y} \in M$, and any $\mathcal{S}^\infty$ curve $\gamma : [-1, 1] \to \mathbf{R}^n$, contained in M, such that $\gamma(0) = \boldsymbol{y}$, $\boldsymbol{y} + \gamma'(0) \in \mathrm{T}_{\boldsymbol{y}}\, M$, as expected. Hence, this matches the definition from the theory of $\mathscr{C}^\infty$ manifolds.

Definition 4.4.13 (Nash maps [BCR98, Definition 2.9.9] and [BPR06, page 111])**.** Let M be a Nash manifold of $\mathbf{R}^n$, and $f : M \to \mathbf{R}^k$ a semi-algebraic map. We say that f is a *Nash map* if for every $\boldsymbol{y} \in M$, and Ω_0 and Ψ as in Definition 4.4.12, the restriction

$$f \circ \Psi \in \mathcal{S}^\infty\Big((\mathbf{R}^d \times \{0\}) \cap \Omega_0,\ \mathbf{R}^k\Big).$$

In this case, the linear map $\mathrm{d}f(x) : \mathrm{T}_{\boldsymbol{y}}\, M \to \mathbf{R}^k$, defined by

$$\mathrm{d}f(\boldsymbol{y})(v) = f(\boldsymbol{y}) + \mathrm{d}(f \circ \varphi)(0)\Big(\mathrm{d}\varphi^{-1}(\boldsymbol{y})(v - \boldsymbol{y})\Big),$$

is called the *derivative* of f at $\boldsymbol{y}$.

Definition 4.4.14 (Submersion)**.** Let M be Nash manifold of $\mathbf{R}^n$, we say that a map $f : M \to \mathbf{R}^k$ is a *Nash submersion* at $\boldsymbol{y} \in M$ if it is a Nash map such that the linear map $\mathrm{d}_{\boldsymbol{y}} f\colon\ \mathrm{T}_{\boldsymbol{y}}\, M \to \mathbf{R}^k$ is surjective.

Example 4.4.15. Let $\varphi, f_1, \ldots f_p \in \mathbf{R}[\boldsymbol{X}]$ be polynomials with real coefficients and suppose that $V = \boldsymbol{V}(f_1, \ldots, f_p) \subset \mathbf{C}^n$ is equidimensional. Then, for all $\boldsymbol{y} \in V \cap \mathbf{R}^n$, the restriction of φ to $M = V \cap \mathbf{R}^n - \mathrm{sing}(V)$ is a submersion if and only if $\varphi(\boldsymbol{y})$ is a regular value. Indeed, as a smooth algebraic set, $M = V \cap \mathbf{R}^n - \mathrm{sing}(V)$ is a Nash manifold and φ is a Nash map. Moreover, since $\boldsymbol{y}$ is non-singular, then by locality

$$\mathrm{T}_{\boldsymbol{y}}\, M = \mathrm{T}_{\boldsymbol{y}}(V \cap \mathbf{R}^n) = \mathrm{T}_{\boldsymbol{y}}\, V \cap \mathbf{R}^n$$

by [BCR98, Proposition 3.3.11]. Hence, $\mathrm{d}\varphi(\mathrm{T}_{\boldsymbol{y}}\, M) = \mathbf{R}^n$ as $\mathrm{d}\varphi(\mathrm{T}_{\boldsymbol{y}}\, V) = \mathbf{C}$ by definition of the critical points.

Finally, as mentioned at the end of the previous section, the notion of compactness is not well-behaved in general real closed fields. Hence, as suggested by Proposition 4.3.10, we use instead the notion of closed bounded semi-algebraic sets.

Definition 4.4.16 (Proper map [Esc01])**.** A semi-algebraic map $f : A \subset \mathbf{R}^n \to B \subset \mathbf{R}^k$ between semi-algebraic subsets A and B is said to be *proper* if $f^{-1}(K)$ is closed and bounded for any closed and bounded semi-algebraic subset $K \subset B$.

Thom's first isotopy lemma is a classical result of differential geometry that allows one to construct diffeomorphisms between submanifolds [GWDPL76]. In the context of real algebraic geometry, given semi-algebraic data, a semi-algebraic version of this theorem has been obtained in [CS95, Theorem 1]. This is done by replacing the integration of some vector fields with the trivialization of some proper surjective submersions using a result previously obtained in [CS92, Theorem 2.4].

Theorem 4.4.17 (Semi-algebraic Thom's first isotopy lemma [CS95, Theorem 1])**.**
Let M be a Nash submanifold of $\mathbf{R}^n$ of dimension $d \geq 1$ and let $f\colon M \to \mathbf{R}^k$ be a Nash map. Then, for any semi-algebraic open subset $N \subset \mathbf{R}^k$ such that the restriction of f to $f^{-1}(N)$ is a proper Nash submersion*, the following holds. Let $\eta \in N$, there exists a semi-algebraic trivialization of f over N with fiber $f^{-1}(\eta)$, that is a semi-algebraic homeomorphism:*

$$\Psi = \big(\Psi^0, f_{|f^{-1}(N)}\big) : f^{-1}(N) \longrightarrow f^{-1}(\eta) \times N,$$

such that $\Psi^0(\boldsymbol{y}) = \boldsymbol{y}$ for all $\boldsymbol{y} \in f^{-1}(\eta)$.

Note that the above formulation of the more general [CS95, Theorem 1], is in the particular case where the locally closed semi-algebraic set M is reduced to one stratum

(or union of strata) of dimension d. A semi-algebraic version of the second Thom's isotopy lemma, dealing with families of semi-algebraic maps, can be found in [Esc01].

We conclude this section by noting that there are extensions to Thom's isotopy lemma for non-proper maps. These are obtained by considering the set of generalized critical values introduced by Rabier in [Rab97], which has been later shown to be of zero-measure by Kurdyka, Orro and Simon in [KOS00]. These results have been further developed, in particular towards effective construction of the generalized critical values. For an overview and recent contributions on these aspects, we refer to [Fer22] and references therein.

5 Computational real algebraic geometry

In the previous chapter, we introduced the theoretical foundations of real algebraic geometry, as well as many important results in this area. In particular, Tarski-Seidenberg theorem showed that problems arising from the first-order theory on a real closed field $\mathbf{R}$ are always decidable, by the mean of a *quantifier-free formula* arising from this theory. Making this result effective at first sight purely theoretical, brings the following algorithmic problem:

(A) on input a first-order formula in the language of the ordered fields, with parameters in $\mathbf{R}$, compute a quantifier-free equivalent formula.

Besides, as seen in Chapter 4, semi-algebraic sets have finitely many semi-algebraically connected components so that one can be interested in computing a finite set of (not necessarily unique) *representative points* of these components. In particular, this allows one to decide the emptiness of given semi-algebraic sets. This raises the second problem we address here:

(B) given a semi-algebraic set S, compute a finite sample subset of S meeting every semi-algebraically connected components of S.

Finally, once a set of representatives of the semi-algebraically connected component of a semi-algebraic set is computed, one can ask to identify which of them lie in the same component and eventually, extract a subset of unique representatives. This allows, in particular, to count the number of these components. This problem, related to *motion planning* problems can be stated as follows:

(C) decide if two points lie in the same semi-algebraically connected component of a given semi-algebraic set.

In the following, we deal with the problems (A), (B) and (C) in respectively Sections 5.1, 5.2 and 5.3. We target, in each section, to give a rough historic overview of the approaches developed to solve them, as well as the best-known complexity results. As these problems constitute the main framework of the contributions of this thesis, this chapter intersects – though being distinct to – Chapter 1, to which we refer for some more technical insights.

5.1 Real quantifier elimination

According to Tarski-Seidenberg's theorem [Tar51, Sei54], problems that can be expressed in the first-order logic are decidable. Recall that this theorem states that any first-order formula

expressed in the language of the ordered fields, with parameters in $\mathbf{R}$, is equivalent to a quantifier-free such formula. Hence, the first step towards the aforementioned computational problems is the computation of quantifier-free equivalent formula; this is called *real quantifier elimination*.

In the following, we roughly describe two algorithmic approaches, in chronological order, to solve this problem. We refer to [Bas17] for a complete survey on this topic.

5.1.1 Tarski-Seidenberg elimination

The proof given by Tarski and Seidenberg in respectively [Tar51] and [Sei54] is effective and hence gives a first algorithm for performing quantifier elimination. This method relies on Sturm's theorem on real root counting, utilizing a methodology that eliminates variables recursively. This approach involves a parametric variant of the Euclidean remainder sequence, as detailed in [BPR06, §2.4].

However, the utilization of the Euclidean remainder sequence leads to rapid growth in the number and degrees of the polynomials in the remaining variables, and introduce denominators increasing the number of branches in the computation. Consequently, the complexity of this method defies bounding by any tower of exponents with a fixed height, rendering it non-elementary recursive – that is that cannot be described using only elementary recursive functions.

Note that in the case of a formula with no free variable, an elementary recursive algorithm can be found in [Mon75]. This particular instance of quantifier elimination is called *The General Decision Problem*.

5.1.2 Cylindrical algebraic decomposition

In order to overcome the unpractical complexity of Tarski-Seidenberg's method, Collins introduced in [Col75] the so-called *Cylindrical Algebraic Decomposition (CAD)*. The ideas behind this decomposition can be found before in the literature, and were used e.g. in [Loj64] for describing the triangulation of semi-analytic sets.

5.1.2.a. Definition

We start with the definition of the cylindrical algebraic decomposition of the ambient space.

Definition 5.1.1 (Cylindrical Algebraic Decomposition [BPR06, Definition 5.1])**.** A cylindrical algebraic decomposition of $\mathbf{R}^n$ is a sequence $\mathcal{S}_1, \dots, \mathcal{S}_n$ where, for each $1 \leq i \leq n$, $\mathcal{S}_i$ is a finite partition of $\mathbf{R}^i$ into semi-algebraic subsets, called the *cells of level* i, which satisfy the following properties:

- Each cell $S \in \mathcal{S}_1$ is either a point or an open interval.
- For every $1 \leq i < n$ and every $S \in \mathcal{S}_i$, there are finitely many continuous semi-algebraic functions $\xi_{S,1} < \ldots < \xi_{S,\ell_S} : S \to \mathbf{R}$ such that the cylinder $S \times \mathbf{R} \subset \mathbf{R}^{i+1}$ is the disjoint union of cells of $\mathcal{S}_{i+1}$ each of which is:

– either the graph of one of the functions $\xi_{S,j}$, for $j = 1, \ldots, \ell_S$:

$$\{(\boldsymbol{y}', y_{j+1}) \in S \times \mathbf{R} \mid y_{j+1} = \xi_{S,j}(\boldsymbol{y})\},$$

– or a band of the cylinder bounded from below and from above by the graphs of the functions $\xi_{S,j}$ and $\xi_{S,j+1}$, for $j = 0, \ldots, \ell_S$, where we take $\xi_{S,0} = -\infty$ and $\xi_{S,\ell_{S+1}} = +\infty$:

$$\{(\boldsymbol{y}', y_{j+1}) \in S \times \mathbf{R} \mid \xi_{S,j}(\boldsymbol{y}') < y_{j+1} < \xi_{S,j+1}(\boldsymbol{y}')\}.$$

A Cylindrical Algebraic Decomposition of the space $\mathbf{R}^n$, consists, as the name suggests, of a recursive partition of the subspaces $\mathbf{R}^i$, for $2 \leq i \leq n$, into cylinders with lower-dimensional cells as base, which are sliced by semi-algebraic functions defined on these lower-dimensional cells.

Example 5.1.2. A trivial CAD of $\mathbf{R}^n$ is obtained by taking the trivial partition $\mathcal{S}_i = \{(-\infty, +\infty)^i\}$ for all $1 \leq i \leq n$. Indeed, $(-\infty, +\infty)$ is an open interval, and for each $1 \leq i < n$, the cylinder $\mathcal{S}_i \times \mathbf{R}$ is exactly $\mathbf{R}^{i+1} = (-\infty, +\infty)^{i+1} \in \mathcal{S}_{i+1}$. This CAD contains a unique cell at each level.

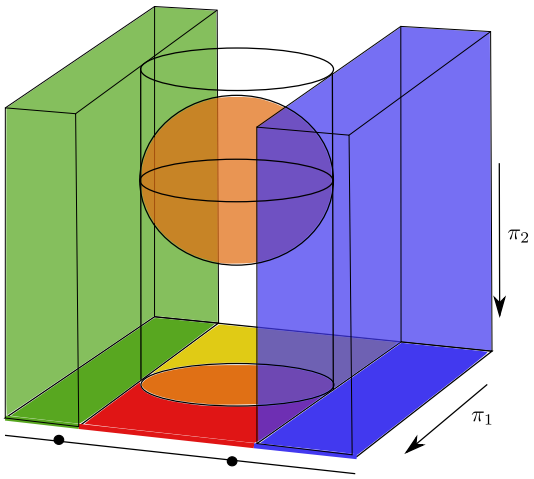
In fact, up to some homeomorphism, the geometry of cells is not more complicated that in the above example, according to the following proposition.

Proposition 5.1.3 ([BPR06, Proposition 5.3])**.** *Every cell of a cylindrical algebraic decomposition is semi-algebraically homeomorphic to an open i-hypercube $(0,1)^i$ – with $(0,1)^0$ being a point by convention. In particular, they are semi-algebraically connected.*

As seen in Example 5.1.2, computing a CAD of $\mathbf{R}^n$ can be done straightforwardly and the definition does not allow more information about a specific semi-algebraic set of $\mathbf{R}^n$. Indeed, as the definition of the CAD describes the rules for slicing the ambient space – that is in cylinder and following semi-algebraic paths – given a semi-algebraic set S, we need to describe how to perform these slices w.r.t. the boundaries of S.

Definition 5.1.4. Given a semi-algebraic set $S \subset \mathbf{R}^n$, we say that a cylindrical algebraic decomposition of $\mathbf{R}^n$ *is adapted to* S if S is a union of cells. More precisely, if $\mathcal{S}_1, \ldots, \mathcal{S}_n$ is a CAD adapted to S, then for every cell $C \in \mathcal{S}_n$, either $C \subset S$ or $C \cap S = \emptyset$.

Example 5.1.5 ([BPR06, Example 5.4])**.** In the figure below is depicted a CAD adapted to the sphere $\mathscr{S}^2$ of $\mathbb{R}^3$. One sees that this decomposition can be constructed incrementally, from $\mathbb{R}$ to $\mathbb{R}^3$, adapting to the respective projections of $\mathscr{S}^2$.



We consider the successive projection of $\mathscr{S}^2$ through π_2 and π_1. The latter is $[-1,1]$, hence we partition $\mathbb{R}$ into the three intervals: $(-\infty,-1)$, $(-1,1)$ and $(1,+\infty)$; together with the two endpoints -1 and 1. This constitutes a CAD $\mathcal{S}_1$ of $\mathbb{R}$ adapted to $[-1,1]$.

Next, this decomposition is lifted into a CAD $\mathcal{S}_1,\mathcal{S}_2$ of $\mathbb{R}^2$ adapted to the unit disk $\mathscr{D}$. We slice the cylinders above each of the intervals and points of $\mathcal{S}_1$, along the boundaries of $\mathscr{D}$, which are semi-algebraic by [BPR06, Proposition 3.1]. This defines the cells of level 2 of $\mathcal{S}_2$.

Finally, the lifting step is repeated above each of the cells of $\mathcal{S}_2$, slicing the cylinder along the boundaries of $\mathscr{S}^2$. This raises $\mathcal{S}_3$. We refer to [BPR06, Example 5.4] for the complete semi-algebraic formulas defining the cells described here.

5.1.2.b. Computational aspects

Following the ideas of the above example, we get the following important result due to Collins [Col75] and Wüthrich [Wüt76]. Note that a more recent description can be found in [BPR06, Chapter 11].

Theorem 5.1.6. *Let S be a semi-algebraic set of $\mathbf{R}^n$ defined by s polynomials of maximum degree D. Then there exists a cylindrical algebraic decomposition of $\mathbf{R}^n$ adapted to S, and it can be computed in time $(sD)^{2^{O(n)}}$.*

Algorithms that, on input polynomials defining a semi-algebraic set, compute a CAD adapted to this set are called CAD algorithms. They are mainly based on two steps, that have been sketched in Example 5.1.5.

1. The first step consists of recursive projections of the input semi-algebraic set. This step relies on subresultant computations, which is a variant of Euclidean remainder sequence avoiding denominators in the coefficients and controlling their growth rate (compared to Euclidean remainders) – see e.g. [GG13, §6.10].

2. The second step consists of incrementally lifting an explicit representation of cylindrical algebraic decompositions adapted to the previously computed projections.

At each recursive projection step in the first step, the degree of the involved polynomials is squared, and since the depth is the number of variables, this leads to the doubly exponential bound given above.

Provided a CAD adapted to a semi-algebraic set, one solves the real quantifier elimination problem within the same complexity bounds – see [Bro99] and [BPR06, §11.3]). Moreover, many other problems can be tackled such as described in [BPR06, Remark 11.46] and [SS83c]. In particular, one can compute a triangulation of a semi-algebraic set from a CAD, and then extract the topological invariants.

Hence, the CAD algorithm given by Collins in [Col75] is the first algorithm performing real quantifier elimination within an elementary recursive complexity method. It is worth emphasizing that the main reason is the use of subresultant sequences instead of Euclidean remainder sequences. Indeed, this allows, in particular, better control of the number of branches in the computation.

Note that several improvements have been subsequently proposed to Collins' algorithm, in e.g. [CH91, Hon92, Bro99, Bro01, Laz94, McC88, BM20]. See [Nai21] for an overview.

On the implementation side, CAD and then CAD-based quantifier elimination is available in different software, namely:

- the interactive command-line program QEPCAD[1] [CH91, Bro03];
- the software system Mathematica[2] [Str06];
- the SyNRAC[3] [IYA14, YA07b, YA07a, AY03] and RegularChains[4] [CM16, CM14] packages of the computer algebra system (CAS) Maple;
- the REDLOG[5] package [SS03b, DS97] of the CAS REDUCE.

5.1.2.c. Discussion

Although the elementary recursive complexity of Collins' CAD algorithm is a striking improvement for eliminating quantifiers, the doubly exponential complexity bound is prohibitive for problems involving more than 4 variables.

Moreover, this bound lies in the optimal complexity class for this problem. Indeed, real quantifier elimination has a doubly exponential lower bound (even with only one free variable). In [DH88] Davenport and Heintz constructed formulas such that any equivalent quantifier-free formula is doubly exponentially larger than the original one. More recently, in [BD07], Brown and Davenport proved that this doubly exponential lower bound on size occurs even with a single free variable and all quantified input polynomials being linear. In the same paper, they also show that there are classes of semi-algebraic sets for which the CAD algorithm outputs doubly exponentially many cells, regardless of the chosen order of the variables.

However, the examples constructed in [DH88] have a large number of quantifier alternation. Hence, by fixing the number of quantifier alternates, one can construct algorithms with complexity singly exponential in the number of variables.

[1] QEPCAD: https://www.usna.edu/CS/qepcadweb/B/QEPCAD.html
[2] Mathematica: http://www.wolfram.com/mathematica/
[3] SyNRAC: http://www.fujitsu.com/jp/group/labs/en/resources/tech/announced-tools/synrac/
[4] RegularChains: https://www.regularchains.org/
[5] REDLOG: http://www.redlog.eu/

These are based on the critical point method pioneered by Grigoriev and Vorobjov [GV88, GV92] and Renegar [Ren92] that we discuss in the next section. The idea is to reduce the elimination of one block of quantifiers to the computation of parameter-dependent sample points in each semi-algebraically connected component of a compact and closed semi-algebraic set. This, in particular, involves infinitesimal deformations that give interesting complexity bounds but are not suited for practical implementations. Then, the first step outputs a tree of realizable sign conditions for the input polynomials which can be used to perform real quantifier elimination using *Sign Determination Algorithms* [BOKR84, RS90, Per11]. We refer to [BPR96a] and [BPR06, Section 14] for a complete presentation of this method.

5.2 Sample points algorithms

As mentioned in the introduction, the problem of computing at least one point on each semi-algebraically connected component of a given semi-algebraic set is a problem of importance in semi-algebraic geometry, and often constitutes a basic subroutine of many algorithms that handle semi-algebraic sets.

In the sequel, let $\boldsymbol{f} = (f_1, \ldots, f_p)$ and $\boldsymbol{g} = (g_1, \ldots, g_s)$ be sequences in $\mathbf{Q}[x_1, \ldots, x_n]$ of maximum degree $D \geq 0$. We denote by $\mathscr{S}(\boldsymbol{f}, \boldsymbol{g})$ the basic semi-algebraic set of $\mathbf{R}^n$ defined by

$$f_1 = \cdots = f_p = 0, \quad g_1 > 0, \ldots, g_s > 0.$$

5.2.1 General approach and lower complexity bound

A first approach would be to compute a cylindrical algebraic decomposition adapted to $\mathscr{S}(\boldsymbol{f}, \boldsymbol{g})$ using the algorithm seen in the previous section, but the prohibitive *doubly exponential* complexity $((p+s)D)^{2^{O(n)}}$ leads us to look for more specialized, but less computationally expensive methods. Indeed, an adapted CAD allows an exhaustive description of $\mathscr{S}(\boldsymbol{f}, \boldsymbol{g})$ while we target here a particular instance in the wide range of problems that CAD can solve.

Moreover, the cost of computing sample points in each semi-algebraically connected component of $\mathscr{S}(\boldsymbol{f}, \boldsymbol{g})$ cannot be lower than the number of these components. This latter number is not larger than the (Oleinik-Petrovsky-)Thom-Milnor's bound: $O((p+s)nD)^n$ – this reduces to $O((p+s)D)^n$ for the subclass of closed semi-algebraic sets. Note that this bound originates from the independent works of [OP49, Ole51],[Tho65] and [Mil64, Theorem 2] on real algebraic sets, later extended to semi-algebraic sets and improved in [BPR96b, Bas99a, Bas03, GV05, GV09] – see [BPR05] for a survey. Note, in addition, that this bound is sharp as a semi-algebraic set defined by the non-vanishing of s products of D generic affine forms, have at least $(CsD)^n$ semi-algebraically connected components, for some constant $C > 0$ [Bas17, Remark 3.3]. Hence, any optimal algorithm computing sample points on the semi-algebraically connected components of $\mathscr{S}(\boldsymbol{f}, \boldsymbol{g})$, must have complexity *singly exponential* in the number of variables n.

5.2.2 Deterministic algorithms: towards optimal complexity

5.2.2.a. The critical point method

The data of such lower bounds motivated the pioneer work of Grigoriev and Vorobjov [GV88] and its improvements [Can88c, HSR89, GV92, Ren92, HRS93, Can93, Can95, HRS94b] which gave rise to a new family of algorithms based on the so-called *critical point method*. This method relies on the fact that any proper non-negative polynomial map reaches its extrema on any real algebraic set, so that the critical locus of its restriction to $\mathscr{S}(\boldsymbol{f},\boldsymbol{g})$ meets every semi-algebraically connected components of $\mathscr{S}(\boldsymbol{f},\boldsymbol{g})$. Provided a good choice of such a polynomial map, one gets either no (in case $\mathscr{S}(\boldsymbol{f},\boldsymbol{g})$ is empty) or finitely many such critical points, that can be computed using Gröbner bases or Geometric Resolution Techniques as seen in Chapter 3. However according to the Heintz-Bézout bound, the number of critical points cannot exceed $D^{O(n)}$. Hence, [GV88] gives the first singly exponential algorithm for computing sample points in every semi-algebraically connected component of a real algebraic set, and the bound $D^{O(n)}$ is reached for the first time in [Can88c, Ren92] on real algebraic sets.

5.2.2.b. Distinguishing combinatorial and algebraic complexity

Later, in [BPR96a, BPR97, BPR98] Basu, Pollack and Roy extended these techniques to semi-algebraic sets reducing the general case to several smooth and bounded real algebraic sets as follows. First, it considers the hypersurface defined by $f = 0$ where $f = f_1^2 + \cdots + f_p^2$ to handle a unique equation. Next, it introduces an infinitesimal ε to reduce the original problem to the one of computing sample points in each connected component of the real algebraic set defined by

$$f = 0, \qquad g_{i_1} = \varepsilon, \ldots, g_{i_m} = \varepsilon,$$

where $\{i_1, \ldots, i_m\} \subset \{1, \ldots, s\}$. The latter is done through [BPR06, Proposition 13.2] which allows one to reduce the original problem to one of computing sample points in real algebraic sets. Hence, by introducing another infinitesimal, one can reduce the latter problem to the case of smooth bounded hypersurfaces.

The resulting algorithm has complexity bounded by $s^n D^{O(n)}$, separating the combinatorial (polynomial) component s^n, the number of real algebraic boundaries of $\mathscr{S}(\boldsymbol{f},\boldsymbol{g})$, from the geometric component $D^{O(n)}$, the degrees of the (complex) algebraic sets associated with these boundaries. Note that the exponent of s can be taken as the (typically much smaller) dimension of $\mathscr{S}(\boldsymbol{f},\boldsymbol{g})$ in the sense of [BPR06, Section 5.3]. We refer to [BPR06, Section 12.6 and 13.3] for a more recent description of these algorithms. We give below a formulation of this result in the context of this manuscript, where the output is encoded by zero-dimensional parametrizations.

Theorem 5.2.1 ([BPR06, Theorem 13.24]). *There exists a* deterministic *algorithm which on input $\boldsymbol{f}$ and $\boldsymbol{g}$, with D the maximum degree of the f_i's and the g_i's, computes at least one point per semi-algebraically connected component of $\mathscr{S}(\boldsymbol{f},\boldsymbol{g})$ by means of zero-dimensional parametrizations of degree bounded by $D^{O(n)}$ using at most*

$$s^n D^{O(n)}$$

arithmetic operations in $\mathbf{Q}$. *Moreover, if the polynomials in* $\boldsymbol{g}$ *and* $\boldsymbol{h}$ *have coefficients in* $\mathbb{Q}$, *of maximum bit size* τ, *then the bit-complexity is at most* $\tau s^n D^{O(n)}$.

5.2.2.c. Drawbacks

The primary drawback of the approach described in the last paragraph lies in its practical computational cost. Indeed, manipulating even a small number of infinitesimals is expensive, although this aspect does not impact the asymptotic complexity bounds when using the big Oh in the exponent. Moreover, the constant in the exponent is not made explicit, but this constant has a big impact on the performance as mentioned in Remark 3.1.3. Making this constant explicit is even the main motivation of the works conducted in Chapters 6 and 7.

These observations are emphasized in [ARS02, Saf01], and Hong shows in [Hon91] that the methods of Grigorév and Vorobjov [GV88] and Renegar [Ren92] are not usable in practice before concluding that:

> "*theoretical analyses based on the big O notation are too coarse for comparing decision algorithms over the reals*".

This assertion finds support through experiments conducted in [RRS00] on the algorithms of [HRS93, BPR96a, Roy96]. Nonetheless, this perturbation method stands out as the current sole approach offering deterministic algorithms with the most favorable worst-case complexity bound.

5.2.3 Randomized algorithms: towards practical efficiency

In order to fill the gap between theoretical complexity and practical efficiency a new family of algorithms appeared subsequently, still based on the critical point method. These algorithms are randomized (or probabilistic) as they rely on a prior generic change of variables (except for [SS04]); see Section 2.4 for an introduction to genericity aspects.

Another aspect of these algorithms is that they target complexity bounds that depend on intrinsic quantitative data such as the *dimension* and the *degree* of the algebraic sets in $\mathbf{C}^n$ associated to the input semi-algebraic given as input or sometimes the *length* of the representation (usually straight-line programs) of the input polynomials – see Section 3.2. This is to be compared to extrinsic data that depends on the way the input system of dense polynomials is given. These are the number of variables, the number of polynomials, their maximum degrees and bitsize coefficients – see [Bas17, §2.6].

In the following, for the sake of comparison, we keep providing the complexity bounds according to the extrinsic data, by the mean of Heintz-Bezout's bound. Recall that the works presented in the previous section provide algorithms with a complexity *polynomial* in the Heintz-Bezout's bound, manipulating several infinitesimals. In this section, the algorithms target to improve practical efficiency by:

1. avoiding working directly with more than one infinitesimal (most of the time such infinitesimals are avoided);
2. making explicit the degree of this polynomial dependence (the best ones being essentially cubic).

5.2.3.a. Algebraic sets

The particular case of real algebraic sets has known several striking improvements during the decade 2000's. In the following approaches, the real algebraic set $V_{\mathbb{R}} = \mathscr{S}(\boldsymbol{f}, 0) \subset \mathbf{R}^n$ is considered as the *real trace* of the complex algebraic set $\boldsymbol{V}(\boldsymbol{f}) \subset \mathbf{C}^n$. This allows one to use the whole toolbox of algebraically closed algebraic geometry we presented in Chapter 2. This is also the approach developed in our contributions.

A first approach was adopted by Bank, Giusti, Heintz and Mbakop in a series of works [BGHM97, BGHM01] for respectively smooth compact hypersurfaces and smooth compact complete intersections. They prove that the critical points of the projection on a *generic* line can be described as *generic* polar varieties that we discussed in Section 2.6. Using geometric resolution algorithms – see Section 3.4 – they obtain a complexity bound cubic in the degree of V. This work is then extended to non-compact cases, with the same cubic bound, in another series of work [BGHP04, BGHP05, BGH$^+$10] by the mean of *generic* generalized polar varieties, that are nothing but critical loci of quadratic forms – see Section 2.6.

At the same time, Safey El Din developed in his PhD thesis [Saf01] another family of algorithms, presented in [RRS00, ARS02], dealing with general algebraic sets by considering the critical points of the square of a distance function to a *generic* point. To handle positive dimensional singularities [RRS00] uses a single infinitesimal deformation in some specific cases, while [ARS02] recursively studies the real points of the singular locus. While the reduction to the compact case is also achieved by considering critical points of a quadratic form, the algorithms in this paragraph differ from those of the previous paragraph as they rely on Gröbner basis computations to eventually compute Rational Univariate Representations – see Sections 3.3 and 3.4 respectively. While no explicit complexity bound is provided, these algorithms, and in particular the one of [ARS02], showed practical efficiency to solve challenging problems.

As summarized in [SS04], at this point, a severe dilemma was posed. On the one hand, the distance-based approaches allow to tackle non-compact situations, but involve higher output degrees which limit their performances. On the other hand, despite the efficiency of projection-based methods, they are limited to compact situations where it is expensive to reduce to (infinitesimal deformations).

This dilemma was eventually resolved by Safey El Din and Schost in [SS03a] who proposed an algorithm for smooth unbounded algebraic sets based on critical loci of *generic* projections. The algorithm proceeds by computing sections of some generic polar varieties that are zero-dimensional thanks to Noether position properties – See Theorem 2.6.3 – and whose union intersects all the targeted components. Using the geometric resolution algorithm, they obtain a complexity *cubic* in the Heintz-Bezout's bound. This algorithm is somehow extended in [SS04] to general real algebraic sets, by replacing the generic properness assumptions, by the computation of the properness defect of projections. This makes, in particular, this algorithm *deterministic*. However, the complexity is not estimated and suspected not to be polynomial in the Heintz-Bézout's bound. It is worth noting that it still has shown good practical behavior, especially for low-dimensional problems. Finally, in [Saf05], Safey El Din proposes an adapted version of [SS03a] to singular real hypersurfaces, keeping the cubic

complexity. The key idea is to avoid the explicit manipulation of infinitesimals by computing a basis of some elimination ideal.

We end this paragraph by mentioning that the bit-complexity and error probability of the algorithm of [SS03a] has very recently been studied in [EGS23], from which the following theorem is adapted.

Theorem 5.2.2 ([SS03a, Theorem 3] & [EGS23, Theorem 1.1]). *There exists a* probabilistic *algorithm which on input $\boldsymbol{f} = (f_1, \ldots, f_p)$, of degrees bounded by D, computes at least one point per semi-algebraically connected component of $\boldsymbol{V}(\boldsymbol{f}) \cap \mathbf{R}^n$ by means of zero-dimensional parametrizations of degree bounded by D^{n+p} using at most*

$$\widetilde{O}\left(D^{3n+2p+1}\right)$$

arithmetic operations in $\mathbf{Q}$. Moreover, if the polynomials in $\boldsymbol{f}$ have coefficients in $\mathbb{Q}$, of maximum bit sizes τ, then the bit-complexity is at most $\widetilde{O}\left(\tau D^{3n+2p+1}\right)$.

5.2.3.b. Semi-algebraic sets

We end this section by mentioning the extension of the algorithm from the previous paragraph to semi-algebraic sets. In the case of semi-algebraic sets defined by non-strict inequalities, [BPR06, Proposition 13.1] allows the authors of [LRS04] to reduced to several algebraic sets, on which they apply the algorithm of [SS03a]. They then obtain a complexity bound cubic in the degree of each of these algebraic sets, allowing them to solve a challenging pattern-matching problem.

The case of strict inequalities cannot be tackled similarly as [BPR06, Proposition 13.2] requires the introduction of infinitesimals, which would make complexity bounds fall into the ones of the previous subsection. The literature does, however, include efficient algorithms for open semi-algebraic sets, that are defined by only strict inequalities.

In [SED07], computing the generalized critical values of a polynomial function, Safey El Din obtains a *quadratic* algorithm for semi-algebraic sets defined by a *single* strict inequality $f > 0$. Later, in the context of the resolution of a camera positioning problem, the authors describe in [FMRS08] an algorithm for *bounded* semi-algebraic sets defined by inequations and strict inequalities. It uses the ideas introduced in [Saf05] (later generalized in [HS12, Lemma 10 and 11]) to avoid explicitly introducing infinitesimals. However, no complexity bound is given. This algorithm is then extended to non-bounded situations in [LS22] (see also [Le21]) in the case of semi-algebraic sets defined by *inequations*, with a complexity bound that is essentially cubic in the Heintz-Bézout's bound. This is obtained by combining the results of [FMRS08], properness results of [SS03a], together with multi-homogeneous bounds proved in [Sch03, SS18]. Following [BPR06, Theorem 13.18] they also provide a corollary routine that computes sample points with rational coefficients. We provide an adapted version of the latter below.

Theorem 5.2.3 ([LS22, Corollary 3]). *There exists an algorithm which on input $\boldsymbol{h} = (h_1, \ldots, h_t)$ in $\mathbf{Q}[x_1, \ldots, x_n]$, of maximum degrees D, computes a set of points $\mathcal{Q}$ in $\mathbf{Q}^n$ of car-*

dinality at most $(2tD)^n$ *and such that* $\mathcal{Q}$ *meets every semi-algebraically connected components of* $\mathbf{R}^n - \cup_{i=1}^t \boldsymbol{V}(h_i)$ *using*

$$\widetilde{O}\left(\binom{D+n}{n} t^{n+1}\, 2^{3n}\, D^{2n+1}\right)$$

arithmetic operations in $\mathbf{Q}$. *Moreover, if the polynomials in* $\boldsymbol{h}$ *have coefficients in* $\mathbb{Q}$, *of maximum bit sizes* τ, *then the bit-complexity is at most* $\tau(tD)^{O(n)}$ *bit operations.*

The large increase in the bit complexity bound is due to the worst-case possibly large bitsize of the small value in $\mathbb{Q}$ chosen to relax the strict inequalities – see [LS22, Remark 2]. However, this worst-case bound does not occur in practice.

We end this subsection by mentioning that many of the algorithms presented here (and still unpublished others) are available in the RAGlib[6] software written with the computer algebra programming language Maple.

5.3 Connectivity queries

The problem of solving connectivity queries in semi-algebraic sets has been first considered by Schwartz and Sharir in [SS83c] in order to solve motion planning problems coming from robotics. We refer to Chapter 1 for a presentation of this problem and discussion on the choice of the framework of algebraic methods developed here to solve it. Another motivation has a more topological flavor. Given a set of representatives of the semi-algebraically connected components of a given semi-algebraic set, deciding which ones lie in the same component allows one to extract a set of *unique* representative. In particular, this gives the number of these components. We recall first the problem we address here.

Definition 5.3.1 (Connectivity queries in semi-algebraic sets)**.** Let $n \geq 1$, and $S \subset \mathbf{R}^n$ be a semi-algebraic set defined by s polynomials of degrees bounded by D.

Given $\boldsymbol{y}, \boldsymbol{y}' \in S$, decide whether $\boldsymbol{y}$ and $\boldsymbol{y}'$ belong to the same semi-algebraically connected component of S.

5.3.1 A first CAD-based approach

Remark that this problem is equivalent to deciding the truth of the following formula:

$$\exists \gamma : [0,1] \to S, \quad \gamma(0) = \boldsymbol{y},\ \gamma(1) = \boldsymbol{y}' \quad \text{and} \quad \gamma \in \mathcal{S}^0\left((0,1), S\right).$$

However, the formulation of this problem does not belong to the first-order theory, since a function appears in the quantifiers. In fact, it is proved in [Bas99b] (see also [BDLW98] in a more general context) that semi-algebraic connectivity problems are not expressible by a first-order formula. Hence, an algorithm for deciding this problem does not follow directly from Tarski-Seidenberg theorem and the methods considered in the previous sections.

However, as mentioned in the first section, one can derive from a CAD adapted to S, a triangulation. Hence this allows to solve topological problems of any type. Following this

[6] RAGlib: https://www-polsys.lip6.fr/~safey/RAGLib/

idea, and the approach outlined in [Rei79], Schwartz, Sharir and collaborators developed in a series of works [SS83a, SS83c, SS83b, SA84, SS84, SSH86] the first exact algorithm solving connectivity queries into semi-algebraic sets. This is based on Collins' CAD algorithm discussed above, to compute a decomposition of S in finitely many semi-algebraically connected cells. Hence, computing points in each of these cells, the algorithm connects the ones lying in adjacency cells using methods introduced in successively [ACM84a, ACM84b, ACM85, Arn88]. However, as their method is based on the computation of a CAD, it has complexity at least doubly exponential in the number of variables. This complexity is prohibitive for any interesting application e.g. in robotics where the number of variables of the configuration space can be quite large.

As discussed at the beginning of the previous section, this doubly exponential complexity is all the more unsatisfactory in that topological complexity (and in particular the number of semi-algebraically connected component) is at most singly exponential in the number of variables, according to the Thom-Milnor's sharp bound. Moreover, the fact that optimal algorithms (that is with complexity polynomial in this latter bound) have been obtained for the computation of sample points in every semi-algebraically connected component enforced the idea that one can hope to target singly exponential bounds.

Finally, in applications such as robotics the dimension of the algebraic set in consideration (that embeds the collision-free space) is significantly smaller than the one of the ambient space [BPR06, Lat91]. Hence, this also justifies the effort to replace the number of variables with this dimension in the exponents.

5.3.2 Roadmap algorithms

5.3.2.a. Definition

In [Can88a], Canny introduced the concept of roadmaps to circumvent the need for computing a cylindrical algebraic decomposition (CAD). Essentially, a roadmap is a one-dimensional semi-algebraic subset of a given semi-algebraic set that is non-empty and semi-algebraically connected within each semi-algebraically connected component of the set. Hence, this approach reduces the connectivity problem from an arbitrary dimension to dimension one. As we will see in the next section, the latter can be solved in a time polynomial in the degree of the input curve. In regards to the complexity bounds of roadmap algorithms, this does not change the overall cost.

For the sake of simplicity, we consider as in the previous section, basic semi-algebraic sets $\mathscr{S}(\boldsymbol{g}, \boldsymbol{h})$ defined by

$$g_1 = \cdots = g_p = 0, \quad h_1 > 0, \ldots, h_t > 0.$$

where $\boldsymbol{g} = (g_1, \ldots, g_p)$ and $\boldsymbol{h} = (h_1, \ldots, h_t)$ are sequences of polynomials in $\mathbf{Q}[x_1, \ldots, x_n]$. Moreover, we consider a finite set of points $\mathcal{P} \subset \mathscr{S}(\boldsymbol{g}, \boldsymbol{h})$ on which connectivity queries are addressed: these are called *query points*.

We give below a modern definition of roadmaps, following the works of [SS11].

Definition 5.3.2. A *roadmap* $\mathcal{R}$ for $(\mathscr{S}(\boldsymbol{g}, \boldsymbol{h}), \mathcal{P})$, is a real algebraic curve, such that:

- $\mathcal{P}$ is contained in $\mathcal{R}$;

- the intersection $\mathcal{R}$ with the semi-algebraic set defined by $h_1 > 0, \ldots, h_t > 0$ is contained in $\mathscr{S}(\boldsymbol{g}, \boldsymbol{h})$ and has a non-empty and semi-algebraically connected intersection with all its semi-algebraically connected components.

From this definition, a *roadmap* captures the connectivity of $\mathscr{S}(\boldsymbol{g}, \boldsymbol{h})$ as well as the relative positions of the query points $\mathcal{P}$. Hence connectivity queries on $\mathscr{S}(\boldsymbol{g}, \boldsymbol{h})$ are reduced to connectivity queries on the curve defined by the roadmap.

5.3.2.b. First algorithms

Canny proposed the first Monte-Carlo algorithm in [Can88a, Can88b], with subsequent modifications in [Can91, Can93], that constructs roadmaps – a.k.a. *roadmap algorithms* for general semi-algebraic sets with complexity bounded by $s^n \log(s) D^{O(n^2)}$.

Canny's approach is based on more advanced critical point methods, inspired by Morse Theory. Roughly speaking, the algorithm starts by computing the critical locus of a generic plane projection $\pi_2 = (\pi_{2,1}, \pi_{2,2}) : \mathbf{R}^n \to \mathbf{R}^2$, that forms a *silhouette curve* of the semi-algebraically connected components. This curve intersects each semi-algebraically connected component of the input semi-algebraic set, but this curve might not be connected inside these components, and then not preserve the original connectivity. According to Morse Theory, the topology changes occur at the critical values of $\pi_{2,1}$. Hence, to repair the connectivity failures of the silhouette, the algorithm computes $(n-1)$-dimensional slices of the input semi-algebraic set at these critical values. Computing recursively a roadmap of this $(n-1)$-dimensional slice, until it outputs only curves, this yields a roadmap, in the sense of the above definition. Figure 5.1 depicts this two-step computation.

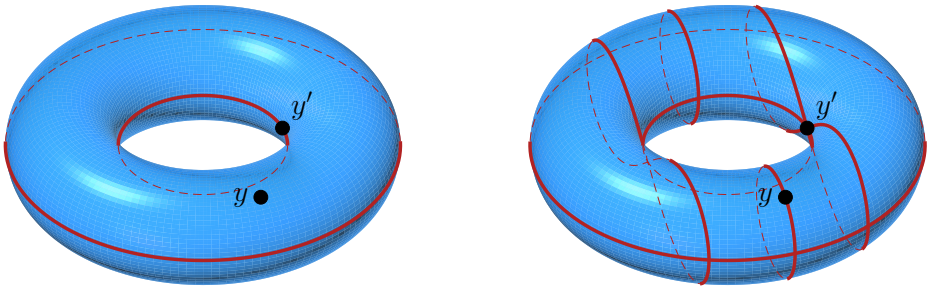


Figure 5.1. Illustration of the two steps of Canny's algorithm on a torus in $\mathbb{R}^3$, with two query points $\boldsymbol{y}$ and $\boldsymbol{y}'$. On the left, the one-dimensional polar variety associated with the projection on the plane below is computed. It intersects the unique connected component, but this intersection is not connected, and does not contain neither $\boldsymbol{y}$ nor $\boldsymbol{y}'$. To repair these failures, we add fibers containing the critical points of a projection on a line and the query points. This gives the right figure.

For a more detailed description of this algorithm and the underlying topological results, we refer to Subsection 1.3.2.

The algorithm of Canny is probabilistic in the sense that it performs a generic linear change of variables on the input to satisfy stratification assumptions – of Whitney's type – in order to apply a semi-algebraic version of Thom's first isotopy lemma – see Section 4.4 – to each stratum. A deterministic version is also given by Canny in [Can91, Can93], which relies on deformation techniques, requiring computations in extensions of the base field of quite large

degree – about $O(s+n^2)$. Even though this gives the worse complexity $s^n \log(s) D^{O(n^4)}$, this is the first deterministic algorithm solving the general problem with singly exponential complexity bound. Moreover, both complexity bounds split the combinatorial part (which is nearly optimal) from the algebraic one (see the previous section).

An alternative direction, taken by [GV92, HRS90, HRS94a, GR93], offers deterministic roadmap algorithms for general semi-algebraic sets. Although their complexities are bound by the coarse bound $(sD)^{n^{O(1)}}$ – in particular we loose the combinatorial/algebraic separation – they avoid stratification and strong position assumptions.

This change led Basu, Pollack, and Roy to develop in [BPR00] – further detailed in [BPR06] – a deterministic roadmap algorithm for general semi-algebraic sets, with complexity in $s^{d+1} D^{O(n^2)}$, where d is the dimension of a real algebraic set containing S. To achieve this complexity, the algorithm reduces to bounded smooth algebraic sets using a constant number of infinitesimals, which limits the algebraic complexity to $D^{O(n^2)}$. Moreover, we recover the separated combinatorial part, whose degree is the (possibly much lower) dimension of the input problem. We report, hereafter a formal version of this result, adapted to our case.

Theorem 5.3.3 ([BPR00] [BPR06, Algorithm 16.26])**.** *Let $\boldsymbol{g}$, $\boldsymbol{h}$ as above and $\mathscr{P}$ be a zero-dimensional parametrization encoding the set $\mathcal{P}$. Assume that the entries of $\boldsymbol{g}$ and $\boldsymbol{h}$ have degree bounded by D and let δ be the degree of $\mathscr{P}$. There exists an algorithm* RoadMap *which computes a one-dimensional rational parametrization encoding a* roadmap *for $(\mathscr{S}(\boldsymbol{g},\boldsymbol{h}),\mathcal{P})$ using $t^{n+1} D^{O(n^2)}$ arithmetic operations in $\mathbf{Q}$. Besides, the degree of the output rational parametrization is polynomial in $t^{n+1}\delta D^{n^2}$. Moreover, if the polynomials in $\boldsymbol{f},\boldsymbol{g}$ and $\mathscr{P}$ have coefficients in $\mathbb{Q}$, of maximum bit sizes τ, then the bit-complexity is at most*

$$\widetilde{O}(\tau)\, t^{O(n)} \delta D^{O(n^2)}$$

bit operations.

However, no practical improvement followed the complexity breakthrough of the above algorithm. In order to obtain efficient implementation, Mezzarobba and Safey El Din presented a practical version of Canny's algorithm for smooth compact algebraic sets in [MS06], with roughly the same complexity. Instead of repairing the connectivity failures of the polar variety by fibers at critical values – which are typically real algebraic numbers – they take fibers at rational numbers separating these values. Hence, this replaces computations in towers of algebraic extensions, by specialization of coordinates at rational numbers. Additionally, the authors detailed the constant in the exponent and showed that this version runs in time cubic in its output size. This is the first complexity result of this kind.

5.3.2.c. Modern algorithms

The exponent in $O(n^2)$ remained the state-of-the-art for a decade until Safey El din and Schost proposed in [SS11] a new recursive approach resulting in a Monte-Carlo roadmap algorithm for smooth bounded real hypersurfaces, with complexity $D^{O(n^{1.5})}$. The key idea was to see in Canny's strategy as a recursive scheme, reducing the problem to algebraic subsets of smaller dimensions. One can show that the complexity of such a strategy is roughly $D^{O(n\rho)}$, where ρ is the depth of recursion. For an input dimension d, the strict

subsets are polar varieties, which are already one-dimensional, and fibers of dimension $d-1$. Hence, the depth of recursion is at most d, which brings the $O(n^2)$ bound. Hence, considering higher dimensional varieties, one can better balance the dimension reduction between polar varieties and fibers, and then reduce the depth. This requires, in particular, to extend the connectivity result of Canny to handle higher dimensional polar varieties [SS11, Theorem 14]. Then, adopting a baby-step/giant-step scheme, the authors give a roadmap algorithm whose depth of recursion is $\sqrt{n}$, which gives the claimed complexity bound. This algorithm is later extended to a deterministic version in [BRSS14], handling arbitrary real algebraic sets, for the same complexity bound. This is done by introducing a constant number of infinitesimal deformations.

The natural next step is the divide and conquer strategy, which provides the optimal recursive depth. This is accomplished by Basu and Roy in [BR14], providing a deterministic roadmap algorithm for general real algebraic sets, with complexity $(n^{\log(n)}D)^{O(n\log^2(n))}$. However, this algorithm is not polynomial in its output size as it introduces $O(\log(n))$ infinitesimals. In particular, this makes the algorithm of theoretic flavor only.

Finally, Safey El Din and Schost proposed in [SS17] a nearly optimal Monte-Carlo algorithm, based on a divide and conquer strategy as well, and with the better complexity bound $(nD)^{O(n\log(d))}$. By making explicit the constants in the exponent, they proved that this algorithm achieves *sub-quadratic complexity in the output size*. This algorithm makes no use of infinitesimals but only tackles smooth bounded algebraic sets. However, even under these assumptions, it outperforms all previous methods. Relaxing the last assumptions on the input while keeping the same complexity bounds is the next step for roadmap algorithms. In particular in Chapters 6 and 7 we solve partly this problem, by removing the compactness assumption.

5.3.2.d. Related problems and applications

Note also that contributions have also been made on numeric [HMP00, IC14, BDRH+13, BBH+17, CWF20] or hybrid symbolic/numeric [HRSS20, Hon10] roadmap algorithms, based on Canny's approach. On another aspect, a more extensive concern revolves around the computation of semi-algebraic formulas describing the semi-algebraically connected components. Notably, [CGV92, HRS94a] tackled this problem, achieving an algorithmic complexity of $(sD)^{n^{O(1)}}$. Later, in [BPR06, Chapter 16], using a parametric version of the roadmap algorithm introduced in [BPR00], Basu, Pollack and Roy are able to compute a description of the semi-algebraically connected component using quantifier-free formulas, with complexity $s^{n+1}D^{O(n^4)}$.

The important development of roadmap algorithms allowed to solve various challenging applications such as in computational geometry, for Voronoi diagrams [ELLS07, ELLS09], or in robotics [CSS20, CSS23]. We refer to [CLH+05, Lat91] for an overview of the use of roadmap algorithms in the context of robotics.

5.3.3 Solving connectivity queries on semi-algebraic curves

We saw in the previous subsection, that, using roadmaps, one can reduce connectivity queries problems in arbitrary dimensions, to the case of connectivity queries problems for semi-algebraic sets of dimension one, lying in the original ambient space. Finding efficient methods to tackle the one-dimensional problem is then a crucial and challenging step for solving the general one. Indeed, as roadmaps have typically exponential degree, algorithms that are polynomial in the degree of the input curve, end up with complexity exponential in the number of variables in the roadmap setting.

Recall that an isotopy of $\mathbf{R}^n$ is an application $\mathcal{H}\colon \mathbf{R}^n \times [0,1] \to \mathbf{R}^n$ such that $\boldsymbol{y} \in \mathbf{R}^n \mapsto \mathcal{H}(\boldsymbol{y},0)$ is the identity map of $\mathbf{R}^n$ and for all $t \in [0,1]$, the map $\boldsymbol{y} \in \mathbf{R}^n \mapsto \mathcal{H}(\boldsymbol{y},t)$ is a homeomorphism. Then we say that two subsets Y and Z of $\mathbf{R}^n$ are isotopy equivalent if there exists an isotopy $\mathcal{H}$ of $\mathbf{R}^n$ such that $\mathcal{H}(Y,1) = Z$. In particular, any path in Y continuously deforms in a path in Z through $\mathcal{H}$.

Consider polynomials $\boldsymbol{h} = (h_1,\ldots,h_s) \in \mathbf{Q}[\boldsymbol{X}]$ and the semi-algebraic curve $\mathscr{D} \subset \mathbf{R}^n$ defined as the intersection of an algebraic curve $\mathscr{C} \subset \mathbf{C}^n$ with the open semi-algebraic set $\mathscr{S}(0,\boldsymbol{h})$ defined by

$$h_1 > 0, \ldots, h_t > 0.$$

The main result of this subsection is that on input a description of $\mathscr{D}$, answering connectivity queries on $\mathscr{D}$ can be done in time which is *linear in the number of inequalities* t and *polynomial in the degree* δ of $\mathscr{C}$. This is done by running algorithms that compute a piecewise linear curve that is *isotopy equivalent* to the input curve, and which can be considered as a graph. Then, deciding connectivity queries on this curve is reduced to deciding connectivity queries on a graph, which is a classically solved algorithmic problem (see for e.g. [CLRS09, Section 22.2]).

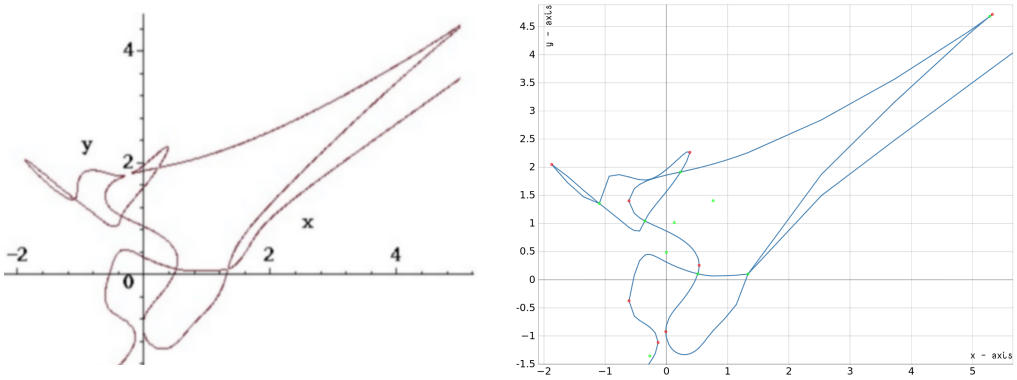


Figure 5.2. On the left, a plot in Maple of a plane real algebraic curve of degree 25, defined as the plane projection of the intersection of two generic surfaces of $\mathbb{R}^3$ of degree 5. On the right, the plot outputted by the software ISOTOP[7], that represent a piecewise-linear curve, that is *isotopy equivalent* to the first curve.

First remark that one can first reduce to the case of real algebraic curves. Indeed, computing the arrangements between $\mathscr{C} \cap \mathbb{R}^n$ and each of the curves $\boldsymbol{V}(h_i) \cap \mathbf{R}^n$, for $i = 1 \ldots t$, one can compute the intersection $\mathscr{C}$ with $\mathscr{S}(0,\boldsymbol{h})$. This eventually leads to an

additional combinatorial factor of $tD\delta$, where δ is the degree of $\mathscr{C}$ and D is a bound on the degrees of the h_i's.

The case of plane algebraic curves in $\mathbb{R}^2$ has been extensively is extensively studied: by subdivision algorithm [BCGY08, LMP08], variants of Cylindrical Algebraic Decomposition methods [BEKS13, CLP+10, DDR+22, Dia09, DRR14, EKW07, GE96, KS15, KS12, MSW15, SW05, DET07, DET09], as well as hybrid approach such as [AMW08]. In particular, [KS15, DDR+22] obtain the best-known complexity bound in $\widetilde{O}(\delta^5(\delta+\tau))$, where δ is the degree of the algebraic curve in $\mathbf{C}^2$ defined by the input polynomials. This is done by computing quantitative bounds on (bivariate) real root isolation of the considered polynomials. An implementation of the algorithm based on [CLP+10], written in the computer algebra programming language Maple, is available in the software ISOTOP[7]

The problem of algebraic curves $\mathbb{R}^3$ has been less studied. This is done through various approaches such as computing the topology of the projection on various planes [AS05, GLMT05, CJL13] or lifting the plane projection by algebraic considerations [El 08, DMR08, DMR12]. Yet, few of these papers give a complexity bound for the computation of such a topology [CJL13, DMR12], and [JC21] obtains the best-known complexity in $\widetilde{O}(\delta^{19}(\delta+\tau))$.

For the general case of real algebraic curves in $\mathbf{R}^n$ (and even $\mathbb{R}^n$), the only known method is based on a variant of the CAD algorithm, drawing upon the concepts established in [SS83c]. While the aforementioned algorithm's complexity bounds may raise concerns due to their potentially prohibitive nature, it is noteworthy that this approach is polynomial in the degree δ of the input curves when dealing with curves. Detailed insights into this method can be found in [SS11, p.6], where it is primarily built upon the CAD algorithm outlined in [Col75], the adjacency relation methods presented in [SS83c], and Puiseux expansions computations as discussed in works like [Duv89]. We summarized the above discussion in the form of the following statement.

Theorem 5.3.4 ([SS11, BPR06]). *Let $\mathscr{R}$ be a one-dimensional rational parametrization, $\boldsymbol{h} = (h_1, \ldots, h_t)$ be polynomials and $\mathscr{P}$ be a zero-dimensional parametrization such that $\mathsf{Z}(\mathscr{P}) \subset \mathsf{Z}(\mathscr{R})$, all of them with coefficients in $\mathbf{Q}$. Let $\delta_{\mathscr{P}}$ and $\delta_{\mathscr{R}}$ be the respective degrees of $\mathscr{P}$ and $\mathscr{R}$ and D be the maximum of $\delta_{\mathscr{R}}$ and the degrees of the polynomials in $\boldsymbol{h}$.*

There exists an algorithm GRAPHISOTOP *which, on input $\mathscr{R}, \boldsymbol{h}$ and $\mathscr{P}$ computes a graph $\mathscr{G} = (\mathcal{V}, \mathcal{E})$, with $\mathcal{V} \subset \mathbf{R}^n$ such that:*

- *the piecewise linear curve $\mathscr{C}_{\mathscr{G}}$ associated to $\mathscr{G}$, is isotopy equivalent to $\mathsf{Z}(\mathscr{R}) \cap \mathscr{S}(0, \boldsymbol{h})$;*
- *the points of $\mathcal{V}$ and $\mathsf{Z}(\mathscr{P}) \cap \mathscr{S}(0, \boldsymbol{h})$ are in one-to-one correspondence through the isotopy.*

Moreover the algorithm outputs a procedure $\text{VERT}_{\mathscr{G}}$*, that on input a zero-dimensional parametrization $\mathscr{Q}$ such that $\mathsf{Z}(\mathscr{Q}) \subset \mathsf{Z}(\mathscr{P})$, computes, using a number of arithmetic operations in $\mathbf{Q}$ which is linear in t and polynomial in $\delta_{\mathscr{P}}$, the subset $\mathcal{V}_{\mathscr{Q}}$ of vertices of $\mathcal{V}$ that are associated to*

$$\mathsf{Z}(\mathscr{Q}) \cap \mathscr{S}(0, \boldsymbol{h}).$$

[7] ISOTOP:https://isotop.gamble.loria.fr/

This is done using at most $t(\delta_{\mathscr{P}} D)^{O(1)}$ *arithmetic operations in* $\mathbf{Q}$. *Moreover, if the input polynomials have coefficients in* $\mathbb{Q}$, *of maximum bit sizes* τ, *then the bit-complexity of* VERT$_{\mathscr{G}}$ *and* GRAPHISOTOP *is at most respectively*

$$\tau t(\delta_{\mathscr{P}})^{O(1)} \quad \text{and} \quad \widetilde{O}(\tau)\, t(\delta_{\mathscr{P}} D)^{O(1)}$$

bit operations.

Hence, given a graph $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ computed by GRAPHISOTOP the following characterization occurs: two points of $\mathsf{Z}(\mathscr{P}) \cap \mathscr{S}(0, \boldsymbol{h})$ are connected in $\mathsf{Z}(\mathscr{R}) \cap \mathscr{S}(0, \boldsymbol{h})$ if and only if the vertices in $\mathcal{V}$, associated with these points, are connected in $\mathscr{G}$.

Concluding this section, it is worth mentioning that the aforementioned algorithm does not explicitly provide the constant factor in the exponent. As observed in the cases of $\mathbb{R}^2$ and $\mathbb{R}^3$, this constant could be quite large. However, it's important to note that all the algorithms discussed in this context compute the complete topology of the input curve, requiring the output to be isotopy equivalent to the input. Yet, for connectivity issues, it suffices for the output to be *semi-algebraic homeomorphic*. With this in mind, in Chapter 8, we relax the isotopy equivalence assumption and develop an algorithm that addresses this problem while maintaining the same complexity bounds as in the planar case.

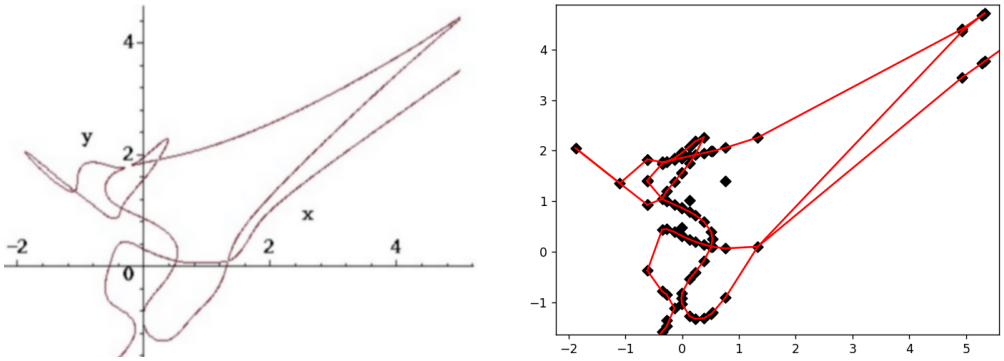


Figure 5.3. On the left, a plot in Maple of a plane real algebraic curve of degree 25, defined as the plane projection of the intersection of two generic surfaces of $\mathbb{R}^3$ of degree 5. On the right, the plot in Matplotlib a piecewise-linear curve, that is *semi-algebraic homeomorphic* to the first curve. The latter has been obtained with a prototype implementation in Sagemath.

Part II

Contributions

6 A new connectivity result for unbounded smooth real algebraic sets

Abstract. As introduced in Section 1.3 of Chapter 1, the problem of answering connectivity queries in real algebraic sets is tackled through the computation of so-called *roadmaps* which are real algebraic subsets of the set V under study, of dimension at most one, and which have a connected intersection with all semi-algebraically connected components of V. Current algorithms for computing roadmaps rely on statements establishing connectivity properties of some well-chosen subsets of V, assuming that V is bounded.

In this chapter, we tackle the first step towards the extension of the new generation of roadmap algorithms to more general inputs. More precisely, we extend connectivity statements, on which roadmap algorithms rely, by dropping the boundedness assumption on the algebraic sets under study. This exploits properties of so-called *generalized polar varieties*, which are critical loci of the considered variety, for some well-chosen polynomial maps. This will allows us, in the next chapter, to extend to unbounded cases the state-of-the-art algorithms

This is joint work with M. Safey El Din and É. Schost.

6.1 Introduction

Let $\mathbf{Q}$ be a real field of real closure $\mathbf{R}$ and let $\mathbf{C}$ be its algebraic closure (one can think about $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ without losing much) and let $n \geq 0$ be an integer. Let $V \subset \mathbf{C}^n$ be an algebraic set defined over $\mathbf{Q}$, that is defined by polynomials with coefficients in $\mathbf{Q}$. As seen in Subsection 1.3, the problem of solving connectivity queries on some finitely many query points $\mathcal{P} \subset V \cap \mathbf{R}^n$, in the real algebraic set $V \cap \mathbf{R}^n$, can be reduced to the computation of a roadmap of $(V, \mathcal{P})$ – see also Subsection 5.3. We have also seen in Subsection 1.3.1 that the effective construction of roadmaps, given a defining system for V, relies on the connectivity statement we recall below, which makes the assumption that V has finitely many singular points and $V \cap \mathbf{R}^n$ is bounded.

Let $0 \leq d \leq n$ and $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set and assume that $\mathrm{sing}(V)$ is finite. For $1 \leq i \leq n$, let π_i be the canonical projection,

$$\pi_i \colon (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n) \longmapsto (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i)$$

For $1 \leq i \leq d$, we denote by $W(\pi_i, V)$ the i-th *polar variety* defined as the Zariski closure of the critical locus $W^\circ(\pi_i, V)$ of the restriction of π_i to V. We recall below [SS11, Theorem 14]

(see also [BRSS14, Proposition 3.3] for a slight variant of it), making use of polar varieties to establish connectivity statements.

Theorem ([SS11, Theorem 14]). *For $2 \leq i \leq d$, assume that the following holds:*

- *$V \cap \mathbf{R}^n$ is bounded;*
- *$W(\pi_i, V)$ is either empty or $(i-1)$-equidimensional and smooth outside $\mathrm{sing}(V)$;*
- *for any $\boldsymbol{y} \in \mathbf{C}^{i-1}$, $\pi_{i-1}^{-1}(\boldsymbol{y}) \cap V$ is either empty or $(d-i+1)$-equidimensional;*
- *$W(\pi_1, W(\pi_i, V))$ is finite.*

Let $\mathcal{P} \subset V$ be a finite set and

$$K_i = W(\pi_1, W(\pi_i, V)) \cup \mathrm{sing}(V) \cup \mathcal{P} \quad \text{and} \quad F_i = \pi_{i-1}^{-1}(\pi_{i-1}(K_i)) \cap V.$$

Then, the real trace of $W(\pi_i, V) \cup F_i$ has a non-empty and semi-algebraically connected intersection with each semi-algebraically connected component of $V \cap \mathbf{R}^n$.

From the above result, one naturally designs a recursive algorithm reducing the problem to algebraic subsets of smaller dimensions, which raises a complexity that is roughly $D^{O(n\rho)}$, where ρ is the depth of recursion and D is the maximum degree of input equations defining V. Using this strategy, the algorithm with the best-known complexity bound $(nD)^{O(n \log_2(d))}$ has been obtained in [SS17], using a divide and conquer strategy. This algorithm assumes, in particular, that the input defines a smooth and bounded algebraic set.

Dropping the boundedness assumption in this scheme was done in [BR14, BRSS14] using infinitesimal deformation techniques. The proposed algorithms use respectively $(nD)^{O(n\sqrt{n})}$ and $(nD)^{O(n \log^2(n))}$ arithmetic operations in $\mathbf{Q}$. However, the use of infinitesimals induces a growth of intermediate data. The algorithm in [BR14] is not polynomial in its output size, which is $(nD)^{O(n \log(n))}$. In non-bounded cases, one could also study the intersection of V with either $[-c, c]^n$ or a ball of radius c, for c large enough, but we would then have to deal with semi-algebraic sets instead of real algebraic sets, in which case [SS11, Theorem 14] is still not sufficient.

Open problem for Chapter 6

The first step towards an algorithm dealing with unbounded smooth real algebraic sets with a complexity similar to that of [SS17], is to *obtain a new connectivity statement* with no boundedness assumption and the same freedom brought by the one of [SS11].

In this chapter, we focus on the proof of such a new connectivity statement which generalizes the one of [SS11] to the unbounded case and will be used in the next chapter to obtain asymptotically faster algorithms for computing roadmaps without assuming the real algebraic set defined by the input is bounded.

Hereafter, the following notation will be used. Let $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n) \subset \mathbf{Q}[x_1, \ldots, x_n]$ then, for $1 \leq i \leq n$, we denote by $\boldsymbol{\varphi}_i$ the polynomial map defined by

$$\begin{array}{rccc} \boldsymbol{\varphi}_i \colon & \mathbf{C}^n & \longrightarrow & \mathbf{C}^i \\ & \boldsymbol{y} & \mapsto & (\varphi_1(\boldsymbol{y}), \ldots, \varphi_i(\boldsymbol{y})) \end{array}. \tag{6.1}$$

Further, we extend this definition by considering $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n) \subset \mathbf{Q}[x_1, \ldots, x_n]$ and, for $1 \leq i \leq n$, the map

$$\begin{array}{rccc} \boldsymbol{\varphi}_i\colon & \mathbf{C}^n & \longrightarrow & \mathbf{C}^i \\ & \boldsymbol{y} & \mapsto & (\varphi_1(\boldsymbol{y}), \ldots, \varphi_i(\boldsymbol{y})) \end{array}. \tag{6.2}$$

Following [BGHP04, BGHP05, BGH+10] we denote similarly $W(\boldsymbol{\varphi}_i, V)$ the i-th *generalized polar variety* defined as the Zariski closure of the critical locus $W^\circ(\boldsymbol{\varphi}_i, V)$ of the restriction of $\boldsymbol{\varphi}_i$ to V. Polar varieties and their properties are discussed in Section 2.6 of Chapter 2

Main result. Let $V \subset \mathbf{C}^n$ be an algebraic set defined over $\mathbf{Q}$ and $d > 0$ be an integer. We say that V satisfies assumption (A) when

(A) V is d-equidimensional and its singular locus $\mathrm{sing}(V)$ is finite.

For $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n) \subset \mathbf{Q}[x_1, \ldots, x_n]$, we say that $\boldsymbol{\varphi}$ satisfies assumption (P) when

(P) the restriction of the map $\boldsymbol{\varphi}_1$ to $V \cap \mathbf{R}^n$ is proper and bounded from below.

We denote by $W_i = W(\boldsymbol{\varphi}_i, V)$ the Zariski closure of the set of critical points of the restriction of $\boldsymbol{\varphi}_i$ to V. For $2 \leq i \leq d$ and $\boldsymbol{\varphi}$ as above, we say that $(\boldsymbol{\varphi}, i)$ satisfies assumption (B) when

(B_1) W_i is either empty or $(i-1)$-equidimensional and smooth outside $\mathrm{sing}(V)$;

(B_2) for any $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i) \in \mathbf{C}^i$, $V \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{y})$ is either empty or $(d-i+1)$-equidimensional.

Note that when B_1 holds, $\mathrm{sing}(W_i)$ and critical loci of polynomial maps restricted to W_i are well-defined. For S_i a finite subset of V, we say that S_i satisfies assumption (C) when

(C_1) S_i is finite;

(C_2) S_i has a non-empty intersection with every semi-algebraically connected component of $W(\boldsymbol{\varphi}_1, W_i) \cap \mathbf{R}^n$.

Finally, using a construction similar to the one used in [SS11, Theorem 14], we let

$$K_i = W(\boldsymbol{\varphi}_1, V) \cup S_i \cup \mathrm{sing}(V) \qquad \text{and} \qquad F_i = \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(K_i)) \cap V.$$

Contribution to the open problem

Theorem 6.1.1. *For V, d, i in $\{1, \ldots, d\}$, $\boldsymbol{\varphi}$ and S_i as above, and under assumptions (A), (B), (C) and (P), the subset $W_i \cup F_i$ has a non-empty and semi-algebraically connected intersection with each semi-algebraically connected component of $V \cap \mathbf{R}^n$.*

The proof structure of the above result follows a pattern similar to the one of [SS11]. Its foundations rely on the following basic idea, sweeping the ambient space with level sets of $\boldsymbol{\varphi}_1$, having a look at the connectivity of $V \cap {\boldsymbol{\varphi}_1}^{-1}(]-\infty, a])$ and $(W_i \cup F_i) \cap {\boldsymbol{\varphi}_1}^{-1}(]-\infty, a])$. The bulk of the proof consists in showing that these two slices share the same connectivity properties. When one does not assume that $i = 2$ but does assume boundedness, one can

take for φ_1 a linear projection, so that its level sets are hyperplanes. In this context, the proof in [SS11] also uses ingredients such as Thom's isotopy lemma, which can be used thanks to the boundedness assumption. Dropping the boundedness assumption makes these steps more difficult and requires us to use a higher degree polynomial for φ_1 (e.g. a quadratic form) to ensure assumption (P). This in turn makes the geometric analysis more involved since now, the level sets of φ_1 are not hyperplanes anymore.

Structure of the chapter. Section 6.2 proves two auxiliary results which analyze the connectivity of fibers of some polynomial maps. These are used in the proof of Theorem 6.1.1, which is given in Section 6.3.

6.2 Connectivity and critical values

In this section we consider for $n \geq 1$ an equidimensional algebraic set $Z \subset \mathbf{C}^n$ of dimension $d > 0$. We are going to prove two main connectivity results on the semi-algebraically connected components of $Z \cap \mathbf{R}^n$ through some polynomial map. These results, along with ingredients of Morse theory such as critical loci and critical values of polynomial maps, will be essential in the proof of Theorem 6.1.1. Most of the results presented here are generalizations of those given in [SS11, Section 3] in the unbounded case, replacing projections by suitable polynomial maps.

6.2.1 Connectivity changes at critical values

The main result of this subsection is to prove the following proposition, which deals with the connectivity changes of semi-algebraically connected components in the neighbourhood of singular values of a polynomial map.

Let X be a subset of $\mathbf{C}^n$, $U \subset \mathbf{R}$ and $f \in \mathbf{R}[x_1, \ldots, x_n]$. With a slight abuse of notation, we still denote by f the polynomial map $\boldsymbol{y} \in \mathbf{C}^n \mapsto f(\boldsymbol{y}) \in \mathbf{C}$, and we write $X_{|f \in U} = X \cap f^{-1}(U) \cap \mathbf{R}^n$. In particular if $u \in \mathbf{R}$ we note

$$X_{|f<u} = X_{|f \in]-\infty,u[}, \quad X_{|f \leq u} = X_{|f \in]-\infty,u]} \quad \text{and} \quad X_{|f=u} = X_{|f \in \{u\}}.$$

Proposition 6.2.1. *Let $\varphi\colon \mathbf{C}^n \to \mathbf{C}$ be a regular map defined over $\mathbf{R}$. Let $A \subset \mathbf{R}^k$ be a semi-algebraically connected semi-algebraic set, and $u \in \mathbf{R}$ and*

$$\gamma\colon A \to Z_{|\varphi \leq u} - \left(Z_{|\varphi=u} \cap K(\varphi, Z)\right)$$

be a continuous semi-algebraic map. Then there exists a unique semi-algebraically connected component B of $Z_{|\varphi<u}$ such that $\gamma(A) \subset \overline{B}$.

Notation 6.2.2. In this subsection we fix a regular (polynomial) map $\varphi\colon \mathbf{C}^n \to \mathbf{C}$ defined over $\mathbf{R}$. With a slight abuse of notation, the underlying polynomial in $\mathbf{R}[x_1, \ldots, x_n]$ will be denoted in the same manner.

We start by proving an extended version of [SS11, Lemma 6]. This can be seen as the founding stone of all the connectivity results presented in this paper. For any $\boldsymbol{y} \in Z \cap \mathbf{R}^n - K(\boldsymbol{\varphi}, Z)$, it shows the existence of a regular map $\boldsymbol{\alpha} : Z \to \mathbf{C}^{n+1}$ such that Z and $\boldsymbol{\alpha}(Z)$ are isomorphic, with $\pi_1 \circ \boldsymbol{\alpha} = \boldsymbol{\varphi}$ on $\boldsymbol{\alpha}(Z)$ and that there is an open Euclidean neighborhood N of $\boldsymbol{\alpha}(\boldsymbol{y})$ such that the implicit function theorem applies to $\boldsymbol{\alpha}(Z) \cap N$. (Recall that an open Euclidean neighborhood of a point $\boldsymbol{y} \in \mathbf{R}^n$ is any subset of $\mathbf{R}^n$ that contains $\boldsymbol{y}$ and is open for the Euclidean topology on $\mathbf{R}^n$.)

Lemma 6.2.3. *Let $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n)$ be in $Z \cap \mathbf{R}^n - K(\boldsymbol{\varphi}, Z)$. Then, there exists a regular map $\boldsymbol{\alpha} \colon Z \to \mathbf{C}^{n+1}$ such that the following holds :*

a) there exist open Euclidean neighborhoods $N' \subset \mathbf{R}^d$ of $\pi_d(\alpha(\boldsymbol{y}))$ and $N \subset \mathbf{R}^{n+1}$ of $\boldsymbol{\alpha}(\boldsymbol{y})$, and a continuous semi-algebraic map $\boldsymbol{f} \colon N' \to \mathbf{R}^{n+1-d}$ such that:

$$\boldsymbol{\alpha}(Z) \cap N = \big\{(\boldsymbol{z}', \boldsymbol{f}(\boldsymbol{z}')) \mid \boldsymbol{z}' \in N'\big\};$$

b) $\boldsymbol{\alpha} \colon Z \to \boldsymbol{\alpha}(Z)$ is an isomorphism of algebraic sets defined over $\mathbf{R}$;

c) $\boldsymbol{\varphi} \circ \boldsymbol{\alpha}^{-1} = \pi_1$ on $\boldsymbol{\alpha}(Z)$.

Proof. Let $\mathcal{O}_{\boldsymbol{y}} \subset \mathbf{R}^n$ be an open Euclidean neighborhood of $\boldsymbol{y}$ and let $\boldsymbol{g} = (g_1, \ldots, g_{n-d})$ be an $(n-d)$-tuple of polynomials in $\mathbf{C}[x_1, \ldots, x_n]$, such that $Z \cap \mathcal{O}_{\boldsymbol{y}} = \boldsymbol{V}(\boldsymbol{g}) \cap \mathcal{O}_{\boldsymbol{y}}$ and $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{g})$ has full rank $n-d$. Such a $\mathcal{O}_{\boldsymbol{y}}$ and $\boldsymbol{g}$ are given by [BCR98, Proposition 3.3.10] since $\boldsymbol{y}$ is in $\mathrm{reg}(Z)$. Also, since $\boldsymbol{y} \notin W(\boldsymbol{\varphi}, Z)$, there exists a non-zero $(n-d+1)$-minor of $\mathrm{Jac}_{\boldsymbol{y}}([\boldsymbol{g}, \boldsymbol{\varphi}])$ by Corollary 2.5.6. Therefore, there exists a permutation σ of $\{1, \ldots, n\}$ such that the matrix

$$\begin{bmatrix} \frac{\partial \boldsymbol{g}}{\partial x_{\sigma(i)}}(\boldsymbol{y}) \\ \frac{\partial \boldsymbol{\varphi}}{\partial x_{\sigma(i)}}(\boldsymbol{y}) \end{bmatrix}_{d \le j \le n}$$

is invertible. Let x_0 be a new variable and define $\boldsymbol{h}$ as the following finite subset of polynomials of $\mathbf{R}[x_0, x_1, \ldots, x_n]$,

$$\boldsymbol{h} = (\widetilde{\boldsymbol{g}}, \widetilde{\boldsymbol{\varphi}}) = \big(\boldsymbol{g}(\sigma^{-1} \cdot (x_1, \ldots, x_n)), \boldsymbol{\varphi}(\sigma^{-1} \cdot (x_1, \ldots, x_n)) - x_0\big)$$

where $\tau \cdot (x_1, \ldots, x_n) = (x_{\tau(1)}, \ldots, x_{\tau(n)})$ for any permutation τ of $\{1, \ldots, n\}$. Hence,

$$\boldsymbol{V}(\boldsymbol{h}) \cap (\mathbf{R} \times \mathcal{O}_{\boldsymbol{y}}) = \big\{(\boldsymbol{\varphi}(\boldsymbol{z}), \sigma \cdot \boldsymbol{z}) \mid \boldsymbol{z} \in Z \cap \mathcal{O}_{\boldsymbol{y}}\big\} \subset \mathbf{R}^{n+1}.$$

By the chain rule, for any $1 \le j \le n$ and $\boldsymbol{z} \in \mathbf{R}^n$,

$$\frac{\partial \widetilde{\boldsymbol{g}}}{\partial x_j}(\boldsymbol{\varphi}(\boldsymbol{z}), \boldsymbol{z}) = \frac{\partial \boldsymbol{g}}{\partial x_{\sigma(j)}}(\sigma^{-1} \cdot \boldsymbol{z}) \quad \text{and} \quad \frac{\partial \widetilde{\boldsymbol{\varphi}}}{\partial x_j}(\boldsymbol{\varphi}(\boldsymbol{z}), \boldsymbol{z}) = \frac{\partial \boldsymbol{\varphi}}{\partial x_{\sigma(j)}}(\sigma^{-1} \cdot \boldsymbol{z}).$$

Hence, for $\mathrm{Jac}(\boldsymbol{f}, i)$ the Jacobian matrix of $\boldsymbol{f}$ with respect to $(x_{i+1}, \ldots, x_n)$, and $\widetilde{\boldsymbol{y}} = (\boldsymbol{\varphi}(\boldsymbol{y}), \sigma \cdot \boldsymbol{y})$,

$$\mathrm{Jac}_{\widetilde{\boldsymbol{y}}}(\boldsymbol{h}, d-1) = \begin{bmatrix} \mathrm{Jac}_{\widetilde{\boldsymbol{y}}}(\widetilde{\boldsymbol{g}}, d-1) \\ \mathrm{Jac}_{\widetilde{\boldsymbol{y}}}(\widetilde{\boldsymbol{\varphi}}, d-1) \end{bmatrix} = \begin{bmatrix} \frac{\partial \boldsymbol{g}}{\partial x_{\sigma(i)}}(\boldsymbol{y}) \\ \frac{\partial \boldsymbol{\varphi}}{\partial x_{\sigma(i)}}(\boldsymbol{y}) \end{bmatrix}_{d \leq j \leq n},$$

which is invertible by assumption on σ.

Therefore, applying the semi-algebraic implicit function theorem [BPR06, Th 3.30] to $\boldsymbol{h}$, there is an open Euclidean neighborhoods $N' \subset \mathbf{R}^d$ of $(\boldsymbol{\varphi}(\boldsymbol{y}), \boldsymbol{y}')$ where $\boldsymbol{y}' = (\boldsymbol{y}_{\sigma(\ell)}, 1 \leq \ell \leq d-1)$, an open Euclidean neighborhood $N'' \subset \mathbf{R}^{n-d+1}$ of $\boldsymbol{y}'' = (\boldsymbol{y}_{\sigma(\ell)}, d \leq \ell \leq n)$ and a map $\boldsymbol{f} = (f_1, \ldots, f_{n-d+1}) \in \mathcal{S}^\infty(N', N'')$ (since $\boldsymbol{\varphi}$ and the g_i's are polynomials) such that:

$$\forall\, \boldsymbol{z} = (\boldsymbol{z}', \boldsymbol{z}'') \in N' \times N'',\ \left[\boldsymbol{h}(\boldsymbol{z}) = 0 \iff \boldsymbol{z}'' = \boldsymbol{f}(\boldsymbol{z}')\right]$$

Then, let $N = (N' \times N'') \cap (\mathbf{R} \times \sigma \cdot \mathcal{O}_{\boldsymbol{y}}) \subset \mathbf{R}^{n+1}$, the previous assertion becomes:

$$\left\{(\boldsymbol{\varphi}(\boldsymbol{z}), \sigma \cdot \boldsymbol{z}) \mid \boldsymbol{z} \in Z\right\} \cap N = \left\{ (\boldsymbol{z}', \boldsymbol{f}(\boldsymbol{z}')) \mid \boldsymbol{z}' \in N' \right\} \tag{6.3}$$

Finally, we claim that taking $\boldsymbol{\alpha} \colon \boldsymbol{z} \in Z \mapsto (\boldsymbol{\varphi}(\boldsymbol{z}), \sigma \cdot \boldsymbol{z})$ ends the proof. Indeed, by equation (6.3), assertion $a)$ immediately holds since N' and N are Euclidean open neighborhood of $\pi_d(\boldsymbol{\alpha}(\boldsymbol{y}))$ and $\boldsymbol{\alpha}(\boldsymbol{y})$ respectively. Further, one checks that $\boldsymbol{\alpha}$ is a Zariski isomorphism, of inverse σ^{-1} after projecting on the last n coordinates, which proves $b)$. Finally, one sees that $\pi_1 \circ \boldsymbol{\alpha} = \boldsymbol{\varphi}$ so that $c)$ holds as well. □

Remark 6.2.4. The previous lemma shows in particular that $Z \cap \mathbf{R}^n - K(\boldsymbol{\varphi}, Z)$ is a Nash manifold (see [BPR06, Section 3.4]) of dimension d, i.e. locally $\mathcal{S}^\infty$-diffeomorphic to $\mathbf{R}^d$.

Lemma 6.2.5. *Let $\boldsymbol{y}$ be in $Z \cap \mathbf{R}^n - K(\boldsymbol{\varphi}, Z)$ and $u = \boldsymbol{\varphi}(\boldsymbol{y})$. Then there exists an open Euclidean neighborhood $N(\boldsymbol{y})$ of $\boldsymbol{y}$ such that the following holds:*

a) $N(\boldsymbol{y})$ is semi-algebraically connected;

b) $(Z \cap N(\boldsymbol{y}))_{|\boldsymbol{\varphi} < u}$ is non-empty and semi-algebraically connected;

c) $(Z \cap N(\boldsymbol{y}))_{|\boldsymbol{\varphi} = u}$ is contained in $\overline{(Z \cap N(\boldsymbol{y}))_{|\boldsymbol{\varphi} < u}}$.

This result is illustrated by Figure 6.1.

Proof. Let $\boldsymbol{\alpha}, N', N$ and $\boldsymbol{f}$ be obtained by applying Lemma 6.2.3. Let $\boldsymbol{F} \colon \boldsymbol{z}' \in N' \mapsto (\boldsymbol{z}', \boldsymbol{f}(\boldsymbol{z}')) \in N$. Let $\varepsilon > 0$ be such that

$$\mathcal{B} = \mathcal{B}\left(\pi_d(\alpha(\boldsymbol{y})), \varepsilon\right) \subset N' \subset \mathbf{R}^d$$

where $\mathcal{B}\left(\pi_d(\alpha(\boldsymbol{y})), \varepsilon\right)$ is the open ball of $\mathbf{R}^d$ with radius ε and center $\pi_d(\alpha(\boldsymbol{y}))$. We claim that taking $N(\boldsymbol{y}) = \boldsymbol{\alpha}^{-1}(\boldsymbol{F}(\mathcal{B}))$ is enough to prove the result.

First, $\boldsymbol{F}(\mathcal{B})$ is open, semi-algebraic and semi-algebraically connected, since $\boldsymbol{F}$ is an open continuous map on $\mathcal{B}$. Then, by assumptions on $\boldsymbol{\alpha}$, together with Proposition 4.2.23,

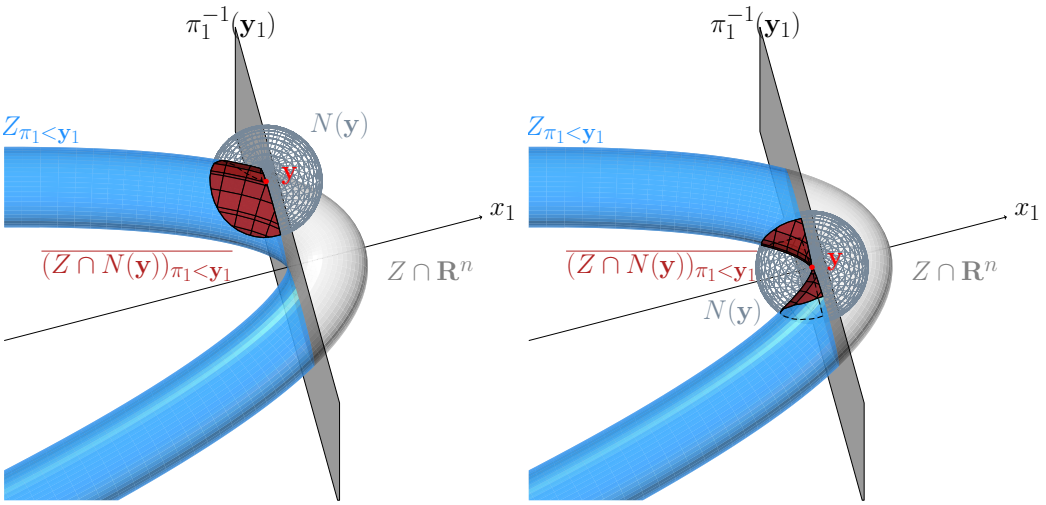


Figure 6.1. Illustration of Lemma 6.2.5 where $\boldsymbol{\varphi}=\pi_1$, $u=\boldsymbol{y}_1$ and Z is isomorphic to $\boldsymbol{V}(x_1^2+x_2^2-1)\times\boldsymbol{V}(x_1+x_2^2)$. On the left, $\boldsymbol{y}$ is not critical and one sees that it satisfies all the statements. On the right $\boldsymbol{y}$ is critical, and $(Z\cap N(\boldsymbol{y}))_{|\pi_1<\boldsymbol{y}_1}$ is disconnected. Note that in both cases, $\boldsymbol{y}_1$ is a critical *value*.

$\boldsymbol{\alpha}^{-1}(\boldsymbol{F}(\mathcal{B}))$ is a semi-algebraically connected open neighborhood of $\boldsymbol{y}$. Hence $N(\boldsymbol{y})$ satisfies statement a).

Besides, remark that $\boldsymbol{F}(\mathcal{B})\subset\boldsymbol{\alpha}(Z)$, so that

$$(\boldsymbol{\alpha}(Z)\cap\boldsymbol{F}(\mathcal{B}))_{|\pi_1<u}=\boldsymbol{F}(\mathcal{B})_{|\pi_1<u}=\boldsymbol{F}(\mathcal{B}_{|\pi_1<u})$$

as $\pi_1(\boldsymbol{F}(\boldsymbol{z}'))=\pi_1(\boldsymbol{z}')$ for $\boldsymbol{z}'\in N'$. Since $\pi_1(\alpha(\boldsymbol{y}))=\boldsymbol{\varphi}(\boldsymbol{y})=u$, the semi-algebraic set $\mathcal{B}_{|\pi_1<u}$ is non-empty and semi-algebraically connected (since $\mathcal{B}$ is convex), and so is its image through $\boldsymbol{F}$ by [BPR06, Section 3.2]. But remark that for all $X\subset\mathbf{R}$,

$$(Z\cap N(\boldsymbol{y}))_{|\boldsymbol{\varphi}\in X}=\boldsymbol{\alpha}^{-1}\left((\boldsymbol{\alpha}(Z)\cap\boldsymbol{F}(\mathcal{B}))_{|\pi_1\in X}\right)=\alpha^{-1}\circ\boldsymbol{F}(\mathcal{B}_{|\pi_1\in X}),\tag{6.4}$$

since $\boldsymbol{\varphi}\circ\boldsymbol{\alpha}^{-1}=\pi_1$. Therefore, by Proposition 4.2.23, $(Z\cap N(\boldsymbol{y}))_{|\boldsymbol{\varphi}<u}$ is non-empty and semi-algebraically connected, as claimed in statement b).

To prove assertion c), remark that $\mathcal{B}_{|\pi_1=u}$ is contained in $\overline{\mathcal{B}_{|\pi_1<u}}$, so that $\alpha^{-1}\circ\boldsymbol{F}(\mathcal{B}_{|\pi_1=u})$ is contained in $\alpha^{-1}\circ\boldsymbol{F}(\overline{\mathcal{B}_{|\pi_1<u}})$. Since $\boldsymbol{F}$ and α^{-1} are continuous,

$$\alpha^{-1}\circ\boldsymbol{F}\left(\overline{\mathcal{B}_{|\pi_1<u}}\right)\subset\overline{\alpha^{-1}\circ\boldsymbol{F}\left(\mathcal{B}_{|\pi_1<u}\right)}.$$

Finally, by (6.4), we get

$$(Z\cap N(\boldsymbol{y}))_{|\boldsymbol{\varphi}=u}\subset\overline{(Z\cap N(\boldsymbol{y})_{|\boldsymbol{\varphi}<u}}.$$

□

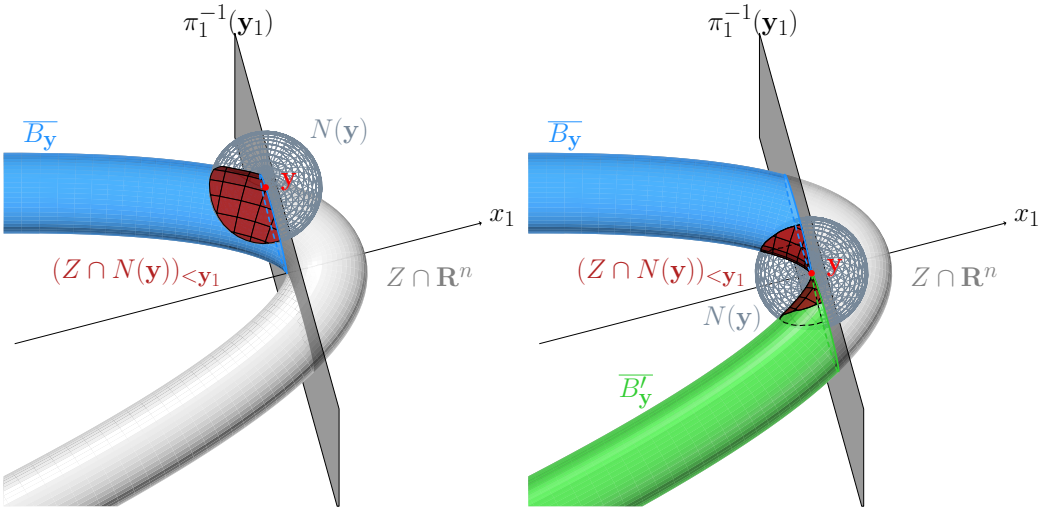


Figure 6.2. Illustration of Lemma 6.2.6 where $\varphi = \pi_1$, $u = \boldsymbol{y}_1$ and Z is isomorphic to $\boldsymbol{V}(x_1^2 + x_2^2 - 1) \times \boldsymbol{V}(x_1 + x_2^2)$. On the left $\boldsymbol{y}$ is not critical and one sees that $\boldsymbol{y} \in \overline{B_{\boldsymbol{y}}}$ and $(Z \cap N(\boldsymbol{y}))_{|\pi_1 < \boldsymbol{y}_1} \subset B_{\boldsymbol{y}}$. However on the right, $\boldsymbol{y}$ is critical, and one observes that $\boldsymbol{y}$ belongs to both $\overline{B_{\boldsymbol{y}}}$ and $\overline{B'_{\boldsymbol{y}}}$, and, in addition, that $(Z \cap N(\boldsymbol{y}))_{|\pi_1 < \boldsymbol{y}_1}$ is not contained in any of these components. Note that in both cases, $\boldsymbol{y}_1$ is a critical *value*.

Lemma 6.2.6. *Let $\boldsymbol{y}$ be in $Z \cap \mathbf{R}^n - K(\varphi, Z)$, let $u = \varphi(\boldsymbol{y})$ and let $N(\boldsymbol{y})$ as in Lemma 6.2.5. Then, there exists a* unique *semi-algebraically connected component $B_{\boldsymbol{y}}$ of $Z_{|\varphi<u}$ such that $\boldsymbol{y} \in \overline{B_{\boldsymbol{y}}}$. Moreover,*

$$(Z \cap N(\boldsymbol{y}))_{|\varphi<u} \subset B_{\boldsymbol{y}}.$$

This lemma is illustrated in Figure 6.2.

Proof. By the second item of Lemma 6.2.5, $(Z \cap N(\boldsymbol{y}))_{|\varphi<u}$ is non-empty and semi-algebraically connected. Thus, it is contained in a semi-algebraically connected component $B_{\boldsymbol{y}}$ of $Z_{|\varphi<u}$. Since the semi-algebraically connected components of $Z_{|\varphi<u}$ are pairwise disjoint, $B_{\boldsymbol{y}}$ is well defined and unique. Moreover by Lemma 6.2.5,

$$\boldsymbol{y} \in \overline{(Z \cap N(\boldsymbol{y}))_{|\varphi<u}} \subset \overline{B_{\boldsymbol{y}}}.$$

Finally, suppose that there exists another connected component B' of $Z_{|\varphi<u}$ such that $\boldsymbol{y} \in \overline{B'}$. Then $\boldsymbol{y}$ belongs to the closure of B', so that $N(\boldsymbol{y}) \cap B' \neq \emptyset$, since $N(\boldsymbol{y})$ is a neighborhood of $\boldsymbol{y}$. Thus $B' \cap B_{\boldsymbol{y}}$ is not empty, and since they are both semi-algebraically connected components of the same set, $B' = B_{\boldsymbol{y}}$. □

Let us see a geometric consequence of this result. The following lemma shows that if u is the least element of $\mathbf{R}$ such that the hypersurface $\varphi^{-1}(\{u\})$ intersects a semi-algebraically connected component C of $Z \cap \mathbf{R}^n$, then this intersection consists entirely of singular points of φ on Z. It is illustrated by Figure 6.3.

Lemma 6.2.7. *Let $\boldsymbol{y} \in Z \cap \mathbf{R}^n$ with $u = \varphi(\boldsymbol{y})$ and let C be the semi-algebraically connected component of $Z_{|\varphi \leq u}$ containing $\boldsymbol{y}$. If $C_{|\varphi<u} = \emptyset$ then $C = C_{|\varphi=u} \subset K(\varphi, Z)$. In particular, $\boldsymbol{y} \in K(\varphi, Z)$.*

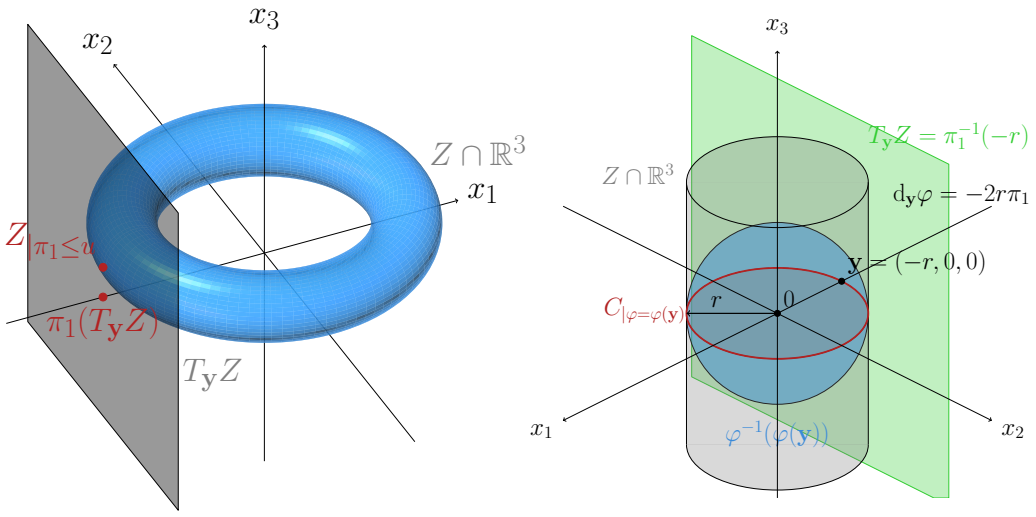


Figure 6.3. Illustration of Lemma 6.2.7 in two cases. On the left, $\varphi = \pi_1$ and $Z \cap \mathbb{R}^3$ is a torus. The plane $\{x_1 = u\}$ indicated satisfies $C_{|\varphi<u} = \emptyset$. One sees that $C_{|\varphi=u} \subset K(\varphi, Z)$, and indeed $C_{|\varphi=u} = \{\boldsymbol{y}\}$. On the right, φ is the square of the Euclidean norm, and Z is a cylinder of radius r. Remark first that $C_{|\varphi<r} = \emptyset$. Moreover, for $\boldsymbol{x} = (\boldsymbol{x}_1, \boldsymbol{x}_2, 0) \in Z$, the differential at $\boldsymbol{x}$ of restriction of φ to Z is the restriction of the projection on the (x_1, x_2)-plane to $\mathrm{T}_{\boldsymbol{x}} Z$. Since these two latter planes are orthogonal, $\boldsymbol{x}$ is indeed a critical point.

Proof. If $C_{|\varphi<u} = \emptyset$, since $C \subset Z_{|\varphi \leq u}$ then $C = C_{|\varphi=u}$ holds. Let us prove the contrapositive of the rest of the lemma. Suppose that $C_{|\varphi=u} \not\subset K(\varphi, Z)$, and let

$$\boldsymbol{z} \in C_{|\varphi=u} - K(\varphi, Z).$$

Let $B_{\boldsymbol{z}}$ be the semi-algebraically connected component of $Z_{|\varphi<u}$ obtained by applying Lemma 6.2.6. Since $\overline{B_{\boldsymbol{z}}}$ contains $\boldsymbol{z}$ and is a semi-algebraically connected set of $Z_{|\varphi \leq u}$, $\overline{B_{\boldsymbol{z}}} \subset C$. Hence $C_{|\varphi<u}$ contains $(\overline{B_{\boldsymbol{z}}})_{|\varphi<u} = B_{\boldsymbol{z}}$, which is then not empty. □

We prove now an important consequence of the previous lemma. It is a fundamental property of generalized polar varieties and motivates their introduction among the ingredients of a roadmap.

Proposition 6.2.8. *Let $u \in \mathbf{R}$ and let B be a* bounded *semi-algebraically connected component of $Z_{|\varphi<u}$. Then $B \cap K(\varphi, Z) \neq \emptyset$.*

Proof. Since φ is a semi-algebraic continuous map and B is semi-algebraic, then $\varphi(\overline{B})$ is a closed and bounded semi-algebraic set by [BPR06, Theorem 3.23]. In particular, φ reaches its minimum $\varphi(\boldsymbol{z})$ on $\overline{B}$ and since $\emptyset \neq B \subset Z_{|\varphi<u}$,then $\varphi(\boldsymbol{z}) < u$. But B is a semi-algebraically connected component of $Z_{|\varphi<u}$, so in particular it is closed in $Z_{|\varphi<u}$, so that

$$\overline{B} - B \subset Z_{|\varphi=u}.$$

Therefore $\boldsymbol{z} \in B$ and as $B_{|\varphi<\varphi(\boldsymbol{z})}$ is empty ($\boldsymbol{z}$ is a minimizer), $B_{|\varphi=\varphi(\boldsymbol{z})}$ and $\boldsymbol{z}$ is in $K(\varphi, Z)$ by Lemma 6.2.7. Finally $\boldsymbol{z} \in B \cap K(\varphi, Z)$, and the latter is non-empty. □

We are now able to prove a weaker version of Proposition 6.2.1, which is illustrated in Figure 6.4. It deals with the particular case when the map has values in some fiber $Z_{|\varphi=u}$, where $u \in \mathbf{R}$.

Lemma 6.2.9. *Let $u \in \mathbf{R}$ and $A \subset \mathbf{R}^k$ be a semi-algebraically connected set. Let*

$$\gamma \colon A \longrightarrow Z_{|\varphi=u} - K(\varphi, Z)$$

be a continuous semi-algebraic map. Then there exists a unique *semi-algebraically connected component B of $Z_{|\varphi<u}$ such that $\gamma(A) \subset \overline{B}$.*

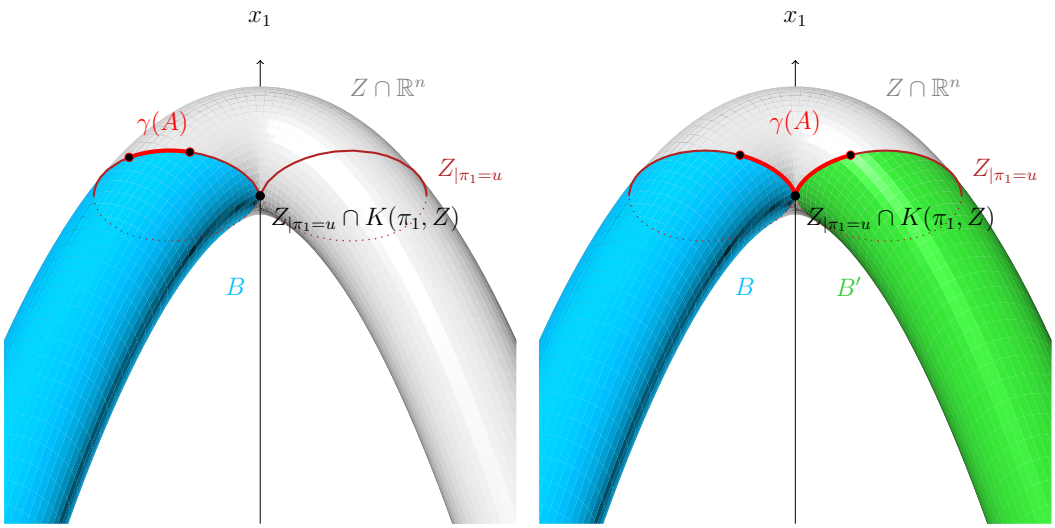


Figure 6.4. Illustration of the proof of Proposition 6.2.1 where $\varphi = \pi_1$ and Z is isomorphic to $\boldsymbol{V}(x_1^2+x_2^2-1) \times \boldsymbol{V}(x_1+x_2^2)$ in two cases. On the left the $\gamma(A) \cap (Z_{|\pi_1=u} \cap K(\pi_1, Z)) = \emptyset$ and on the right, this intersection is non-empty.

Proof. Let $\boldsymbol{a}_0 \in A$ and $\boldsymbol{y} = \gamma(\boldsymbol{a}_0)$, by assumption, $\boldsymbol{y} \in Z_{|\varphi=u} - K(\varphi, Z)$. Then by Lemmas 6.2.5 and 6.2.6, there exist an open neighborhood $N(\boldsymbol{y})$ of $\boldsymbol{y}$ and a semi-algebraically connected component $B_{\boldsymbol{y}}$ of $Z_{|\varphi<u}$ such that

$$(Z \cap N(\boldsymbol{y}))_{|\varphi=u} \subset \overline{(Z \cap N(\boldsymbol{y}))_{|\varphi<u}} \subset \overline{B_{\boldsymbol{y}}}.$$

Hence for every $\boldsymbol{z} \in (Z \cap N(\boldsymbol{y}))_{|\varphi=u} - K(\varphi, Z)$, $\boldsymbol{z} \in \overline{B_{\boldsymbol{y}}}$ so that $B_{\boldsymbol{z}} = B_{\boldsymbol{y}}$ by application of Lemma 6.2.6. Since γ is a continuous semi-algebraic map, there exists an open semi-algebraic neighborhood $N'(\boldsymbol{a}_0)$ of $\boldsymbol{a}_0$ such that

$$\gamma(N'(\boldsymbol{a}_0)) \subset (Z \cap N(\boldsymbol{y}))_{|\varphi=u} - K(\varphi, Z).$$

Hence the map $\boldsymbol{a} \mapsto B_{\gamma(\boldsymbol{a})}$ is constant on $N(\boldsymbol{a}_0)$. Let

$$\mathfrak{B} : \boldsymbol{a} \in A \mapsto B_{\gamma(\boldsymbol{a})} \in \mathcal{P}(Z_{|\varphi<u})$$

be the map given by Lemma 6.2.6, where $\mathcal{P}(Z_{|\varphi<u})$ denote the power set of $Z_{|\varphi<u}$. We proved that $\mathfrak{B}$ is locally constant on A and then, equivalently, continuous for the discrete topology on $\mathcal{P}(Z_{|\varphi<u})$. But since A is semi-algebraically connected, $\mathfrak{B}(A)$ is connected for the discrete topology, that is $\mathfrak{B}$ is constant A.

Let then B be the constant value that $\mathfrak{B}$ takes on A. By Lemma 6.2.6, for all $\boldsymbol{a} \in A$, $\gamma(\boldsymbol{a}) \in \overline{B_{\gamma(\boldsymbol{a})}} = \overline{B}$, that is $\gamma(A) \subset \overline{B}$. Besides, if B' is another semi-algebraically connected component of $Z_{|\varphi<u}$ such that $\gamma(A) \subset \overline{B'}$, then for all $\boldsymbol{a} \in A$,

$$\gamma(\boldsymbol{a}) \in \overline{B} \cap \overline{B'} \cap Z_{|\varphi=u} - K(\varphi, Z),$$

so that $B = B'$ by uniqueness in Lemma 6.2.6. □

We can now prove the main proposition by sticking together all the pieces. The points of the map that belong to the fiber $Z_{|\varphi=u}$ are managed by Lemma 6.2.9, while the remaining ones, in $Z_{|\varphi<u}$, are more convenient to deal with. This proof is illustrated by Figure 6.5.

Proof of Proposition 6.2.1. Since γ is semi-algebraic and continuous, $\gamma(A)$ is semi-algebraically connected. Hence, if $\gamma(A) \subset Z_{|\varphi<u}$, it is contained in a unique semi-algebraically connected component B of $Z_{|\varphi<u}$ and we are done.

We assume now that $\gamma(A) \not\subset Z_{|\varphi<u}$. Let $G = \gamma^{-1}(Z_{|\varphi=u})$. It is a closed subset of A since $Z_{|\varphi=u}$ is closed in $Z_{|\varphi\leq u}$ and γ is continuous. Then, let $G_1, \dots, G_N$ be the semi-algebraically connected components of G; they are closed in A since they are closed in G, which is closed in A. Besides, let $H_1, \dots, H_M$ be the semi-algebraically connected components of $A - G$. They are open in A since they are open in $A - G$, which is open in A.

We define a map $\mathfrak{B}\colon A \to \mathcal{P}(Z_{|\varphi<u})$, where $\mathcal{P}(Z_{|\varphi<u})$ is the power set of $Z_{|\varphi<u}$. The family formed by both $G_1, \dots, G_N$ and $H_1, \dots H_M$ is a partition of A; hence, we can define $\mathfrak{B}$ by defining it on this partition.

$\boldsymbol{H_i}$: Since $H_i \subset A - G$, $\gamma(H_i) \subset Z_{|\varphi<u}$ and $\gamma(H_i)$ is semi-algebraically connected as γ is continuous. Then, there exists a unique semi-algebraically connected component B_i of $Z_{|\varphi<u}$ such that $\gamma(H_i) \subset B_i \subset \overline{B_i}$.

$\boldsymbol{G_i}$: Since G_i is semi-algebraically connected and $\gamma(G_i) \subset Z_{|\varphi=u} - K(\varphi, Z)$, Lemma 6.2.9 with $A = G_i$ states that there is a unique semi-algebraically connected component B_i' of $Z_{|\varphi<u}$ such that $\gamma(G_i) \subset \overline{B_i'}$.

Therefore, for all $\boldsymbol{a} \in A$, let $\mathfrak{B}$ such that

$$\mathfrak{B}(\boldsymbol{a}) = \begin{cases} B_i & \text{if } \boldsymbol{a} \in H_i \\ B_i' & \text{if } \boldsymbol{a} \in G_i \end{cases} \quad \text{so that } \gamma(\boldsymbol{a}) \in \overline{\mathfrak{B}(\boldsymbol{a})}.$$

Let us show that $\mathfrak{B}$ is locally constant, that is, for every $\boldsymbol{a} \in A$, there exists an open Euclidean neighborhood $N(\boldsymbol{a}) \subset A$ of $\boldsymbol{a}$, such that for all $\boldsymbol{a}' \in N(\boldsymbol{a})$, $\mathfrak{B}(\boldsymbol{a}') = \mathfrak{B}(\boldsymbol{a})$. Then, we will conclude by connectedness as above. Let $\boldsymbol{a} \in A$ and $1 \leq i \leq \max(M, N)$.

- If $\boldsymbol{a} \in H_i$, since H_i is open in A, there exists an open Euclidean neighborhood $N(\boldsymbol{a})$ of $\boldsymbol{a}$ contained in H_i. By construction, for all $\boldsymbol{a}' \in N(\boldsymbol{a})$, $\mathfrak{B}(\boldsymbol{a}') = \mathfrak{B}(\boldsymbol{a})$. Moreover, since

H_i is semi-algebraically connected, this also proves that $\mathfrak{B}$ is actually constant on H_i, and we let $\mathfrak{B}(H_i)$ be the unique value it assumes on H_i.

- Else $\boldsymbol{a} \in G_i$, since the G_j's are closed in A, then $\boldsymbol{a}$ does not belong to the closure of any other G_j, $j \neq i$. However, the set

$$J = \left\{1 \leq j \leq M \mid \boldsymbol{a} \in \overline{H_j}\right\}$$

is not empty. By construction, $\gamma(\boldsymbol{a}) \in \overline{\mathfrak{B}(\boldsymbol{a})}$ and by definition of J, for every $j \in J$, $\gamma(\boldsymbol{a}) \in \overline{\mathfrak{B}(H_j)}$. But, by Lemma 6.2.6 applied with $\boldsymbol{y} = \gamma(\boldsymbol{a})$, such a semi-algebraically connected component is unique. Hence for all $j \in J$, $\mathfrak{B}(H_j) = \mathfrak{B}(\boldsymbol{a})$. One can then take $N(\boldsymbol{a}) = \mathcal{B}(\boldsymbol{a}, r)$ with $r > 0$ such that this open ball intersects either the H_j's for $j \in J$ or G_i, and only them.

Finally, we proved that $\mathfrak{B}$ is locally constant and then, equivalently, continuous for the discrete topology on $\mathcal{P}(Z_{|\boldsymbol{\varphi}<u})$. Since A is semi-algebraically connected, $\mathfrak{B}(A)$ is connected for the discrete topology and $\mathfrak{B}$ is constant on A. Denoting by $B \subset Z_{|\boldsymbol{\varphi}<u}$ the unique value it assumes, we have $\gamma(A) \subset \overline{B}$ as claimed. Besides if B' is another semi-algebraically connected component of $Z_{|\boldsymbol{\varphi}<u}$ such that $\gamma(A) \subset \overline{B'}$, then in particular $\overline{B} \cap \overline{B'}$ contains $\gamma(G_1) \subset Z_{|\boldsymbol{\varphi}=u} - K(\boldsymbol{\varphi}, Z)$, so that $B = B'$ by Lemma 6.2.9. □

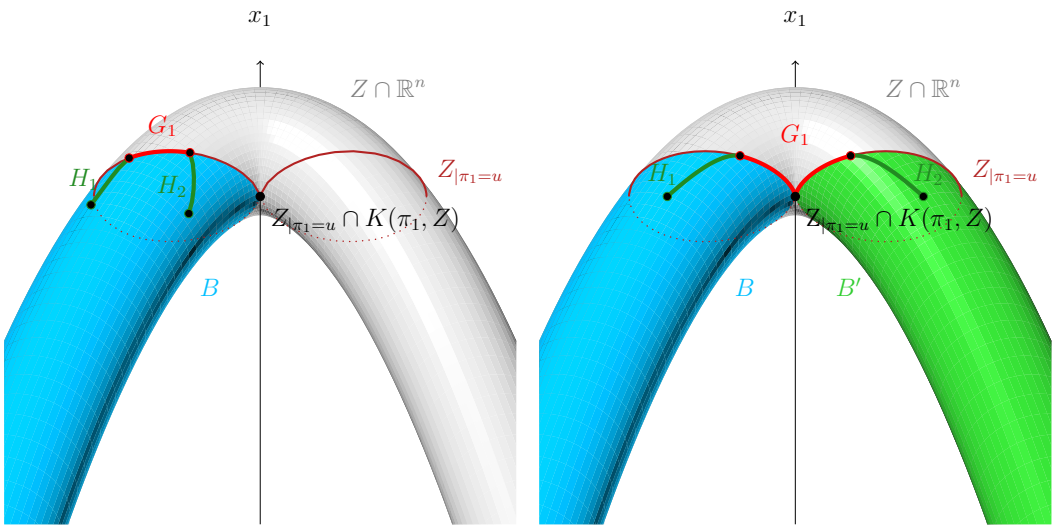


Figure 6.5. Illustration of the proof of Proposition 6.2.1 with $\boldsymbol{\varphi} = \pi_1$ and Z is isomorphic to $\boldsymbol{V}(x_1^2 + x_2^2 - 1) \times \boldsymbol{V}(x_1 + x_2^2)$ in two cases. The intersection $\gamma(A) \cap (Z_{|\pi_1=u} \cap K(\pi_1, Z))$ is empty on the left while, on the right, it is not.

We then deduce the following consequence on the semi-algebraically connected components of Z with respect to $\boldsymbol{\varphi}$. This result is illustrated in Figure 6.6.

Corollary 6.2.10. *Let $\boldsymbol{\varphi}\colon \mathbf{C}^n \to \mathbf{C}$ be a regular map defined over $\mathbf{R}$ and $Z \subset \mathbf{C}^n$ be an equidimensional algebraic set of positive dimension. Let $u \in \mathbf{R}$ such that $Z_{|\boldsymbol{\varphi}=u} \cap K(\boldsymbol{\varphi}, Z) = \emptyset$ and let C be a semi-algebraically connected component of $Z_{|\boldsymbol{\varphi}\leq u}$. Then, $C_{|\boldsymbol{\varphi}<u}$ is a semi-algebraically connected component of $Z_{|\boldsymbol{\varphi}<u}$.*

Proof. Let γ be the inclusion map $\gamma\colon C \hookrightarrow Z_{|\varphi\leq u}$. Since $Z_{|\varphi=u} \cap K(\varphi, Z) = \emptyset$, γ satisfies the assumptions of Proposition 6.2.1 with $A = C$. Then there exists a unique semi-algebraically connected component B of $Z_{|\varphi<u}$ such that $C \subset \overline{B}$, so that $C_{|\varphi<u} \subset \overline{B}_{|\varphi<u} = B$.

First, since $Z_{|\varphi=u} \cap K(\varphi, Z) = \emptyset$ by assumption, then in particular $C_{|\varphi=u} \not\subset K(\varphi, Z)$. By the contrapositive of Lemma 6.2.7, $C_{|\varphi<u}$ is not empty. Hence, since B is a semi-algebraically connected set of $Z_{|\varphi\leq u}$, containing $C_{|\varphi<u}$, B is contained in the semi-algebraically connected component C of $Z_{|\varphi\leq u}$. Finally $B \subset Z_{|\varphi<u} \cap C = C_{|\varphi<u}$ and $C_{|\varphi<u} = B$, which is a semi-algebraically connected component of $Z_{|\varphi<u}$. □

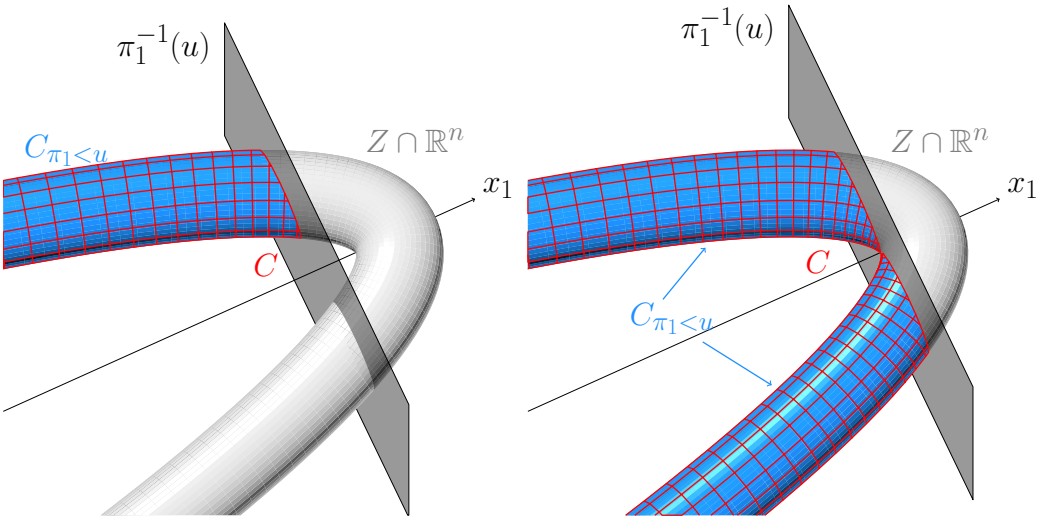


Figure 6.6. Illustration of Corollary 6.2.10 where $\varphi = \pi_1$ and Z is isomorphic to $\boldsymbol{V}(x_1^2 + x_2^2 - 1) \times \boldsymbol{V}(x_1 + x_2^2)$. On the left $Z_{|\pi_1=u} \cap K(\pi_1, Z) = \emptyset$ and one sees that $C_{|\pi_1<u}$ is still a semi-algebraically connected component of $Z_{|\pi_1<u}$. On the right $Z_{|\pi_1=u} \cap K(\pi_1, Z) \neq \emptyset$ and one sees that $C_{|\pi_1<u}$ is disconnected.

6.2.2 Fibration and critical values

As in [SS11, Section 3.2] we are going to use a Nash version of Thom's isotopy lemma, stated in [CS95, Theorem 1], which, again, is an ingredient of Morse theory. We refer to Section 4.4 for the definitions of Nash diffeomorphisms, manifolds and submersions together with their properties.

Proposition 6.2.11. *Let $\varphi\colon \mathbf{C}^n \to \mathbf{C}$ be a regular map defined over $\mathbf{R}$ and $A \subset \varphi^{-1}((-\infty, w)) \cap \mathbf{R}^n$ be a semi-algebraically connected semi-algebraic set. Let $v < w$ such that $A_{|\varphi\in(v,w)}$ is a non-empty Nash manifold, bounded, closed in $\varphi^{-1}((v, w)) \cap \mathbf{R}^n$ and such that φ is a submersion on $A_{|\varphi\in(v,w)}$. Then for all $u \in [v, w)$, $A_{|\varphi\leq u}$ is non-empty and semi-algebraically connected.*

Proof. We first prove that $\varphi\colon A_{|\varphi\in(v,w)} \to (v, w)$ is a proper surjective submersion. Since $A_{|\varphi\in(v,w)}$ is bounded and φ is semi-algebraic and continuous, $\varphi\colon A_{|\varphi\in(v,w)} \to (v, w)$ is a proper map. Let us prove that φ is also surjective on $A_{|\varphi\in(v,w)}$ that is

$$\varphi(A_{|\varphi\in(v,w)}) = (v, w).$$

By assumption, $\boldsymbol{\varphi}$ is a submersion from $A_{|\boldsymbol{\varphi}\in(v,w)}$ to (v,w). Then by the semi-algebraic inverse function theorem [BPR06, Proposition 3.29], $\boldsymbol{\varphi}$ is an open map. Besides, as $A_{|\boldsymbol{\varphi}\in(v,w)}$ is closed and bounded, there exists a closed and bounded semi-algebraic set $X \subset \mathbf{R}^n$ such that $A_{|\boldsymbol{\varphi}\in(v,w)} = X \cap \boldsymbol{\varphi}^{-1}((v,w)) = X_{|\boldsymbol{\varphi}\in(v,w)}$. Then

$$\boldsymbol{\varphi}(A_{|\boldsymbol{\varphi}\in(v,w)}) = \boldsymbol{\varphi}(X_{|\boldsymbol{\varphi}\in(v,w)}) = \boldsymbol{\varphi}(X) \cap (v,w).$$

Since X is bounded and closed, $\boldsymbol{\varphi}(X)$ is closed and bounded by [BPR06, Theorem 3.23]. Hence, $\boldsymbol{\varphi}(A_{|\boldsymbol{\varphi}\in(v,w)})$ is both open and closed in (v,w). Since (v,w) is semi-algebraically connected, $\boldsymbol{\varphi}(A_{|\boldsymbol{\varphi}\in(v,w)}) = (v,w)$.

By the Nash version of Thom's isotopy lemma [CS95, Theorem 1], since the map $\boldsymbol{\varphi}\colon A_{|\boldsymbol{\varphi}\in(v,w)} \to (v,w)$ is a proper surjective submersion, it is a globally trivial fibration. Hence, for $\zeta \in (v,w)$, there exists a Nash diffeomorphism Ψ of the form

$$\begin{array}{rccc} \Psi\colon & A_{|\boldsymbol{\varphi}\in(v,w)} & \longrightarrow & (v,w) \times A_{|\boldsymbol{\varphi}=\zeta} \\ & \boldsymbol{y} & \longmapsto & (\ \boldsymbol{\varphi}(\boldsymbol{y})\ ,\ \psi(\boldsymbol{y})\ ). \end{array}$$

We now proceed to prove the main statement of the proposition. There are, at first sight, two different situations to consider: whether $u > v$ or $u = v$ (see Figure 6.7). Using Puiseux series, we actually prove them simultaneously.

Take $u \in [v,w)$; we prove that $A_{|\boldsymbol{\varphi}\leq u}$ is non-empty and semi-algebraically connected. To prove that $A_{|\boldsymbol{\varphi}=u}$ is non-empty, we consider $\boldsymbol{z} \in A_{|\boldsymbol{\varphi}=\zeta}$ and the map

$$\begin{array}{rccc} \gamma\colon & [0,1) & \longrightarrow & A_{|\boldsymbol{\varphi}\in(v,w)} \\ & t & \longmapsto & \Psi^{-1}(tu + (1-t)\zeta, \boldsymbol{z}). \end{array}$$

This map is well defined and continuous, since Ψ is a Nash diffeomorphism from $A_{|\boldsymbol{\varphi}\in(v,w)}$ to $(v,w) \times A_{|\boldsymbol{\varphi}=\zeta}$, and satisfies $\boldsymbol{\varphi}(\gamma(t)) = tu + (1-t)\zeta$ for every $t \in [0,1)$. Moreover γ is a bounded map as $A_{|\boldsymbol{\varphi}\in(v,w)}$ is bounded by assumption. Then, by [BPR06, Proposition 3.21], γ can be continuously extended to $[0,1]$, with $\boldsymbol{\varphi}(\gamma(t)) = tu + (1-t)\zeta$ continuous on $[0,1]$, and $\boldsymbol{\varphi}(\gamma(1)) = u$. Finally $\gamma(1) \in A_{|\boldsymbol{\varphi}\leq u}$ and $A_{|\boldsymbol{\varphi}\leq u}$ is not empty.

We prove now that $A_{|\boldsymbol{\varphi}\leq u}$ is semi-algebraically connected. Consider two points $\boldsymbol{y}$ and $\boldsymbol{y}'$ in $A_{|\boldsymbol{\varphi}\leq u}$. Since A is semi-algebraically connected by assumption, there exists a continuous path $\gamma\colon [0,1] \to A$ such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(1) = \boldsymbol{y}'$. Let us construct, from γ, another path that lies in $A_{|\boldsymbol{\varphi}\leq u}$.

Let ε be an infinitesimal, and let $\mathbf{R}' = \mathbf{R}\langle\varepsilon\rangle$ be the field of algebraic Puiseux series in ε (see [BPR06, Section 2.6]). We denote by $A', (v,w)', \Psi', \psi', \boldsymbol{\varphi}'$ and γ' the extensions of respectively $A, (v,w), \Psi, \psi, \boldsymbol{\varphi}$ and γ to $\mathbf{R}'$ in the sense of [BPR06, Proposition 2.108]. According to [BPR06, Exercise 2.110], $\Psi'\colon A'_{|\boldsymbol{\varphi}\in(v,w)'} \to (v,w)' \times A'_{|\boldsymbol{\varphi}=\zeta}$ is a bijective map. Then let $g'\colon [0,1]' \subset \mathbf{R}' \to A'$ be such that

$$\begin{array}{lll} g'(t) = \gamma'(t) & \text{if} & \boldsymbol{\varphi}'(\gamma'(t)) \leq u + \varepsilon, \\ g'(t) = \Psi'^{-1}(u + \varepsilon, \psi'(\gamma'(t))) & \text{if} & u + \varepsilon \leq \boldsymbol{\varphi}'(\gamma'(t)) < w. \end{array}$$

This map is well defined since $u+\varepsilon \in (v,w)$ and if $\varphi'(\gamma'(t)) = u+\varepsilon$, then $\Psi'^{-1}(u+\varepsilon, \psi'(\gamma'(t))) = \gamma'(t)$. Moreover g' is a continuous semi-algebraic map since by [BPR06, Exercise 3.4], Ψ'^{-1}, ψ' and γ' are continuous semi-algebraic maps.

Finally one observes that g' is bounded over $\mathbf{R}$. Indeed if $\varphi'(\gamma'(t)) \leq u+\varepsilon$, then $g'(t) = \gamma(t)$, which is continuous on $[0,1]'$ and then bounded over $\mathbf{R}$. Else $\varphi'(\gamma'(t)) \in (v,w)$ and $g'(t) \in A'_{|\varphi\in(v,w)'}$, which is bounded over $\mathbf{R}$ by [BPR06, Proposition 3.19] since $A_{|\varphi\in(v,w)}$ is. Hence, its image $G' = g'([0,1]')$ is a semi-algebraically connected semi-algebraic set, bounded over $\mathbf{R}$ and contained in $A'_{|\varphi\leq u+\varepsilon}$.

Let $G = \lim_\varepsilon G'$. By [BPR06, Proposition 12.49], G is a closed and bounded semi-algebraic set. Then, since φ is a continuous semi-algebraic map defined over G, by [BPR06, Lemma 3.24] for all $z' \in G'$,

$$\varphi(\lim_\varepsilon z') = \lim_\varepsilon \varphi(z') \leq \lim_\varepsilon (u+\varepsilon) = u$$

So that G is contained in $A_{|\varphi\leq u}$. In addition, since G' is semi-algebraically connected and bounded over $\mathbf{R}$, then by [BPR06, Proposition 12.49], G is semi-algebraically connected and contains $y = \lim_\varepsilon g(0)$ and $y' = \lim_\varepsilon g(1)$. We deduce that there exists, inside G, a semi-algebraic path connecting y to y' in $A_{|\varphi\leq u}$, which ends the proof. □

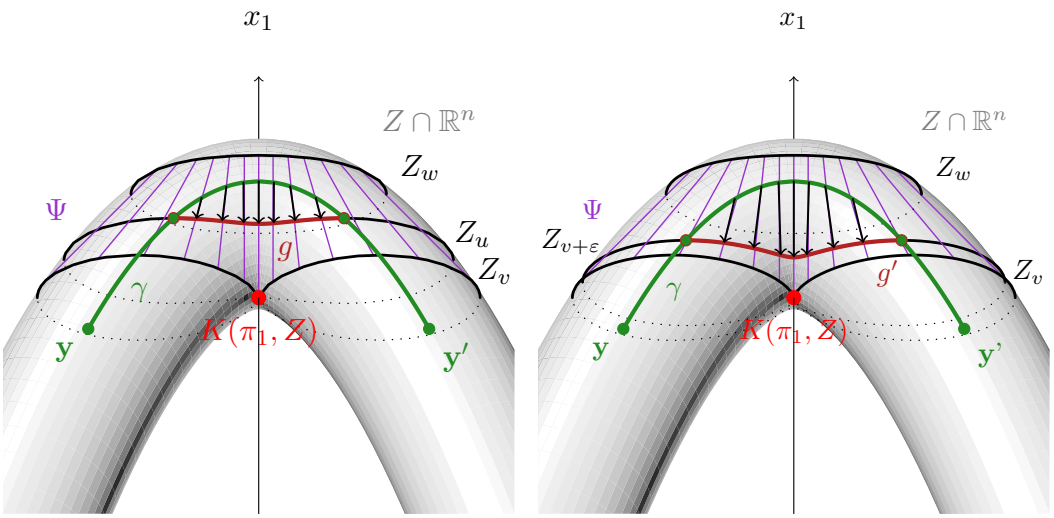


Figure 6.7. Illustration of the two cases covered by the proof of Proposition 6.2.11 where $\varphi = \pi_1$ and $A = Z_{|\pi_1<w}$, where Z is isomorphic to $\boldsymbol{V}(x_1^2+x_2^2-1) \times \boldsymbol{V}(x_1+x_2^2)$. The two cases are quite similar; we consider here the one where v is a critical value. One sees that Ψ connects all the slices $A_{|\pi_1=u}$ for $u \in (v,w)'$. This diffeomorphism allows to transform the problematic parts (not in $A_{|\pi_1\leq u}$) of the initial path γ (in green), into another path g (in red), that lies in $A_{|\pi_1=u} \subset A_{|\pi_1\leq u}$.

The following result is a consequence of Proposition 6.2.11 as it deals with a particular case. An illustration of this statement can be found in Figure 6.8.

Corollary 6.2.12. *Let $Z \subset \mathbf{C}^n$ be an equidimensional algebraic set of positive dimension and let $\varphi\colon \mathbf{C}^n \to \mathbf{C}$ be a regular map defined over $\mathbf{R}$ and proper on $Z \cap \mathbf{R}^n$. Let $v < w$ be in $\mathbf{R}$*

such that $Z_{|\varphi\in(v,w]} \cap K(\varphi, Z) = \emptyset$, and let C be a semi-algebraically connected component of $Z_{|\varphi\leq w}$. Then, $C_{|\varphi\leq v}$ is a semi-algebraically connected component of $Z_{|\varphi\leq v}$.

Proof. As $C_{|\varphi<w} = C \cap \varphi^{-1}((-\infty, w)) \cap \mathbf{R}^n$, we are going to use Proposition 6.2.1 with $A = C_{|\varphi<w}$.

First we need to prove that $C_{|\varphi<w}$ is a non-empty semi-algebraically connected semi-algebraic set. Since $Z_{|\varphi=w} \cap K(\varphi, Z) = \emptyset$, by Corollary 6.2.10 $C_{|\varphi<w}$ is a semi-algebraically connected component of $Z_{|\varphi<w}$. Hence it is non-empty and semi-algebraically connected.

Then, we need to prove that $C_{|\varphi\in(v,w)}$ is a non-empty Nash manifold, bounded and closed in $\varphi^{-1}((v, w)) \cap \mathbf{R}^n$. Suppose first that $C_{|\varphi\in(v,w)} = \emptyset$. Then

$$C_{|\varphi\leq v} \cup C_{|\varphi=w} = C \quad \text{and} \quad C_{|\varphi\leq v} \cap C_{|\varphi=w} = \emptyset.$$

Since C is semi-algebraically connected, either $C_{|\varphi\leq v}$ or $C_{|\varphi=w}$ is empty (as they are both closed in C). In both cases our conclusion follows. It remains to tackle the case where $C_{|\varphi\in(v,w)}$ is not empty, which we assume to hold from now on.

We prove that $C_{|\varphi\in(v,w)}$ is bounded. Observe that $C_{|\varphi\in(v,w)} \subset C_{|\varphi\in[v,w]} = C \cap \mathbf{R}^n \cap \varphi^{-1}([v, w])$. Recall that φ is proper on $Z \cap \mathbf{R}^n$ by assumption, and thus on $C \cap \mathbf{R}^n$. Hence, $C_{|\varphi\in[v,w]}$ is bounded. Besides $C_{|\varphi\in(v,w)}$ is closed in $\varphi^{-1}((v, w)) \cap \mathbf{R}^n$ as

$$C_{|\varphi\in(v,w)} = C \cap \varphi^{-1}((v, w)) \cap \mathbf{R}^n,$$

and C is closed in $\mathbf{R}^n$ as it is closed in the closed set $Z_{|\varphi\leq w}$. Since $C_{|\varphi\in(v,w)} \cap K(\varphi, Z) = \emptyset$ then by [BCR98, Proposition 3.3.11], $C_{|\varphi\in(v,w)}$ is a Nash manifold of dimension $\dim(Z)$.

To apply Proposition 6.2.1, it remains to prove that φ is a Nash submersion on $C_{|\varphi\in(v,w)}$. Let $\boldsymbol{y} \in C_{|\varphi\in(v,w)}$. Since $\boldsymbol{y} \notin \operatorname{sing}(Z)$, then $\mathrm{T}_{\boldsymbol{y}} C_{|\varphi\in(v,w)} = \mathrm{T}_{\boldsymbol{y}} Z \cap \mathbf{R}^n$ according to [BCR98, Proposition 3.3.11]. Since $C_{|\varphi\in(v,w)} \cap K(\varphi, Z) = \emptyset$, $\mathrm{d}_{\boldsymbol{y}}\varphi$ is onto on $\mathrm{T}_{\boldsymbol{y}} Z$ and since $\dim Z > 0$, the image $\mathrm{d}_{\boldsymbol{y}}\varphi(\mathrm{T}_{\boldsymbol{y}} Z)$ is $\mathbf{C}$. Hence

$$\mathrm{d}_{\boldsymbol{y}}\varphi(\mathrm{T}_{\boldsymbol{y}} C_{|\varphi\in(v,w)}) = \mathbf{R}.$$

We just established that all the assumptions of Proposition 6.2.11 are satisfied. One can then apply it to $C_{|\varphi<w}$ and conclude that $C_{|\varphi\leq v}$ is non-empty and semi-algebraically connected. Finally, since C is a semi-algebraically connected component of $Z_{|\varphi\leq w}$, any semi-algebraically connected component of $Z_{|\varphi\leq v}$ contained in C is contained in $C_{|\varphi\leq v}$. Thus $C_{|\varphi\leq v}$ is a semi-algebraically connected component of $Z_{|\varphi\leq v}$. □

6.3 Proof of the main connectivity result

Recall that $\varphi = (\varphi_1, \ldots, \varphi_n) \subset \mathbf{R}[x_1, \ldots, x_n]$ and for $1 \leq i \leq n$, $\varphi_i \colon \boldsymbol{y} \mapsto (\varphi_1(\boldsymbol{y}), \ldots, \varphi_i(\boldsymbol{y}))$. We denote by $W_i = W(\varphi_i, V)$ the Zariski closure of the set of critical points of the restriction of φ_i to V and recall that

$$K_i = W(\varphi_1, V) \cup S_i \cup \operatorname{sing}(V) \qquad \text{and} \qquad F_i = \varphi_{i-1}^{-1}(\varphi_{i-1}(K_i)) \cap V,$$

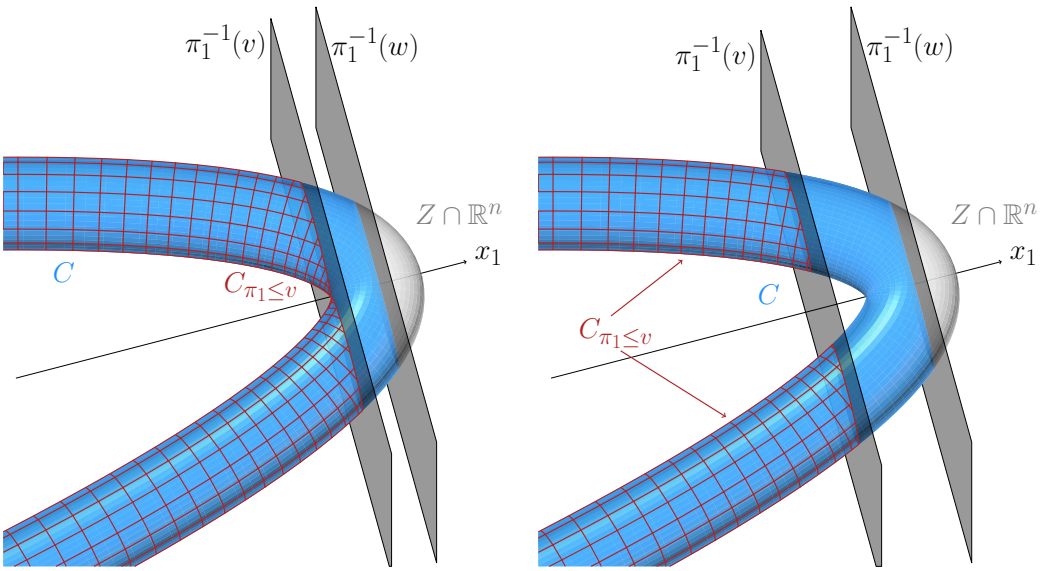


Figure 6.8. Illustration of Corollary 6.2.12 where $\varphi = \pi_1$ and Z is isomorphic to $\boldsymbol{V}(x_1^2 + x_2^2 - 1) \times \boldsymbol{V}(x_1 + x_2^2)$ in two cases. On the left $Z_{|\pi_1 \in (v,w)} \cap K(\pi_1, Z) = \emptyset$ and we see that $C_{|\pi_1 \leq v}$ is still a semi-algebraically connected component of $Z_{|\pi_1 \leq v}$. On the right $Z_{|\pi_1 \in (v,w)} \cap K(\pi_1, Z)$ contains a point and we see that $C_{|\pi_1 \leq v}$ is semi-algebraically disconnected.

where S_i is a given subset of V. We suppose that the following assumptions hold:

(A) V is d-equidimensional and its singular locus $\mathrm{sing}(V)$ is finite;

(P) the restriction of the map φ_1 to $V \cap \mathbf{R}^n$ is proper and bounded from below;

(B_1) W_i is either empty or $(i-1)$-equidimensional and smooth outside $\mathrm{sing}(V)$;

(B_2) for any $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i) \in \mathbf{C}^i$, $V \cap \varphi_{i-1}^{-1}(\boldsymbol{y})$ is either empty or $(d-i+1)$-equidimensional;

(C_1) S_i is finite;

(C_2) S_i has a non-empty intersection with every semi-algebraically connected component of $W(\varphi_1, W_i) \cap \mathbf{R}^n$.

Then the goal of this section is to prove that $W_i \cup F_i$ intersects each semi-algebraically connected component of $V \cap \mathbf{R}^n$ and that their intersection is semi-algebraically connected.

Let $\mathcal{R} = F_i \cup W_i$. We prove that the following so-called roadmap property holds:

RM: *"For any semi-algebraically connected component C of $V \cap \mathbf{R}^n$, the set $C \cap \mathcal{R}$ is non-empty and semi-algebraically connected",*

by proving a truncated version of RM and show that it is enough. For $u \in \mathbf{R}$ let

RM(u): *"For any semi-algebraically connected component C of $V_{|\varphi_1 \leq}u$, the set $C \cap \mathcal{R}$ is non-empty and semi-algebraically connected".*

Lemma 6.3.1. *If* RM(u) *holds for all* $u \in \mathbf{R}$*, then* RM *holds.*

Proof. Let C be a semi-algebraically connected component of $V \cap \mathbf{R}^n$. Since C is non-empty and semi-algebraically connected, there exist $\boldsymbol{y}$ and $\boldsymbol{y}'$ in C, and a semi-algebraic path $\gamma\colon [0,1] \to C$ connecting them. Let

$$u = \max\{\boldsymbol{\varphi}_1(\gamma(t)), t \in [0,1]\} \in \mathbf{R}.$$

Such a maximum u exists by continuity of γ and $\boldsymbol{\varphi}_1$, since $[0,1]$ is closed and bounded, and it follows that $\gamma([0,1]) \subset V_{|\boldsymbol{\varphi}_{1\leq}} u$. Since $\gamma([0,1])$ is semi-algebraically connected, there exists a (unique) semi-algebraically connected component B of $V_{|\boldsymbol{\varphi}_{1\leq}} u$ containing $\gamma([0,1])$. In particular, B contains $\boldsymbol{y}$ and $\boldsymbol{y}'$. Since $\mathrm{RM}(u)$ holds by assumption, then $B \cap \mathcal{R}$ is non-empty. But as $\boldsymbol{y} \in B \cap C$ and B is semi-algebraically connected, C contains B. Finally, $C \cap \mathcal{R}$ contains $B \cap \mathcal{R}$ and the former is non-empty.

We can suppose now, in addition, that $\boldsymbol{y}$ and $\boldsymbol{y}'$ are in $C \cap \mathcal{R}$, and let B be defined as above. Then, $\boldsymbol{y}$ and $\boldsymbol{y}'$ are in $B \cap \mathcal{R}$, which is semi-algebraically connected by $\mathrm{RM}(u)$. Therefore $\boldsymbol{y}$ and $\boldsymbol{y}'$ are connected by a semi-algebraic path in $B \cap \mathcal{R}$. Since $B \subset C$, $\boldsymbol{y}$ and $\boldsymbol{y}'$ are semi-algebraically connected in $C \cap \mathcal{R}$. In conclusion, $C \cap \mathcal{R}$ is semi-algebraically connected and RM holds. □

Remark 6.3.2. The previous lemma trivially holds in the case of [SS11, Theorem 14], since $V \cap \mathbf{R}^n$ is assumed to be bounded. Indeed, in this case, considering $u = \max_{\boldsymbol{y} \in V \cap \mathbf{R}^n} \boldsymbol{\varphi}_1(\boldsymbol{y})$, one has $V_{|\boldsymbol{\varphi}_{1\leq}} u = V \cap \mathbf{R}^n$.

6.3.1 Restoring connectivity

Before proving $\mathrm{RM}(u)$ for all $u \in \mathbf{R}$, we need to prove the following result, which constitutes the core of the proof of Theorem 6.1.1. This proposition shows that the connectivity property of our roadmap candidate is satisfied when u is increasing towards singular points of $\boldsymbol{\varphi}_1$ on V. This is ensured by the addition of the fibers F_i.

Proposition 6.3.3. *Let $u \in \mathbf{R}$ and C be a semi-algebraically connected component of $V_{|\boldsymbol{\varphi}_{1\leq}} u$ such that $C_{|\boldsymbol{\varphi}_{1<}} u$ is non-empty. Let B be a semi-algebraically connected component of $C_{|\boldsymbol{\varphi}_{1<}} u$, then:*

1. *$\overline{B} \cap (F_i \cup W_i)$ is non-empty;*
2. *Any point $\boldsymbol{y} \in \overline{B} \cap (F_i \cup W_i)$ can be connected to a point $\boldsymbol{z} \in B \cap (F_i \cup W_i)$ by a semi-algebraic path in $\overline{B} \cap (F_i \cup W_i)$.*

Let us begin with a technical lemma:

Lemma 6.3.4. *Let $\mathbf{K}$ be a real closed field containing $\mathbf{R}$ and $\overline{\mathbf{K}}$ be its algebraic closure. Let $Z \subset \overline{\mathbf{K}}^n$ be a d-equidimensional algebraic set, where $d > 0$. Assume that for any $\boldsymbol{z} \in \overline{\mathbf{K}}^{i-1}$,*

$$Z \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{z}) \text{ is either empty or } (d-i+1)\text{-equidimensional.}$$

Let B be a bounded *semi-algebraically connected component of $Z \cap \mathbf{K}^n$ and let $\boldsymbol{y} \in B$. Let H be the semi-algebraically connected component of $B \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\boldsymbol{y}))$ containing $\boldsymbol{y}$. Then, the intersection $H \cap K(\boldsymbol{\varphi}_i, Z)$ is not empty.*

Proof. Let $Y = Z \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\boldsymbol{y}))$. By assumption, Y is an equidimensional algebraic set of dimension $d-i+1$. Besides, H is a bounded semi-algebraically connected component of $Y \cap \mathbf{K}^n$, since B is a bounded semi-algebraically connected component of $Z \cap \mathbf{K}^n$.

Recall that $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n)$. Then $\varphi_i(H) \subset \mathbf{R}$ is a closed and bounded semi-algebraic set by [BPR06, Theorem 3.23]. In particular, φ_i reaches its minimum on H. Let $\boldsymbol{z} \in H$ be such that $\varphi_i(\boldsymbol{z}) = \min \varphi_i(H)$, so that $H_{|\varphi_i < \varphi_i(\boldsymbol{z})}$ is empty. Then, by Lemma 6.2.7,

$$\boldsymbol{z} \in H \cap K(\varphi_i, Y).$$

Let $\boldsymbol{g} \subset \mathbf{K}[x_1, \ldots, x_n]$ be a finite sequence of generators of $\boldsymbol{I}(Z)$, so that $Y = \boldsymbol{V}(\boldsymbol{g}, \boldsymbol{\varphi}_{i-1} - \boldsymbol{\varphi}_{i-1}(\boldsymbol{y}))$. Since Y is $(d-i+1)$-equidimensional, Proposition 2.5.4 establishes that $\boldsymbol{z}$ is such that

$$\operatorname{rank} \begin{bmatrix} \operatorname{Jac}_{\boldsymbol{z}}(\boldsymbol{g}) \\ \operatorname{Jac}_{\boldsymbol{z}}(\boldsymbol{\varphi}_{i-1}) \\ \operatorname{Jac}_{\boldsymbol{z}}(\varphi_i) \end{bmatrix} < n - (d - (i-1)) + 1.$$

Since $\boldsymbol{\varphi}_i = (\boldsymbol{\varphi}_{i-1}, \varphi_i)$, one deduces that

$$\operatorname{rank} \begin{bmatrix} \operatorname{Jac}_{\boldsymbol{z}}(\boldsymbol{g}) \\ \operatorname{Jac}_{\boldsymbol{z}}(\boldsymbol{\varphi}_i) \end{bmatrix} < n - d + i,$$

which means that $\boldsymbol{z} \in H \cap K(\boldsymbol{\varphi}_i, Z)$. Finally, the latter set is non-empty and the statement is proved. □

Notation 6.3.5. For the rest of the subsection let u, C and B as defined in Proposition 6.3.3.

Let us deal with one particular case of the second item of Proposition 6.3.3.

Lemma 6.3.6. *Let $\boldsymbol{y}$ be in $\overline{B} \cap F_i$. Then, there exists a point $\boldsymbol{z} \in B \cap (F_i \cup W_i)$ and a semi-algebraic path in $\overline{B} \cap (F_i \cup W_i)$ connecting $\boldsymbol{y}$ to $\boldsymbol{z}$.*

Proof. Let $\boldsymbol{y}$ be in $\in \overline{B} \cap F_i$. We assume that $\boldsymbol{y} \notin B$ so that $\boldsymbol{\varphi}_1(\boldsymbol{y}) = u$, otherwise taking $\boldsymbol{z} = \boldsymbol{y}$ would end the proof. Since $\boldsymbol{y} \in \overline{B}$, by the curve selection lemma [BPR06, Th. 3.22], there exists a semi-algebraic path $\gamma\colon [0,1] \to \mathbf{R}^n$ such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(t) \in B$ for all $t \in (0,1]$. Let ε be an infinitesimal, $\mathbf{R}' = \mathbf{R}\langle\varepsilon\rangle$ be the field of algebraic Puiseux series and $\psi = (\psi_1, \ldots, \psi_n)$ be the semi-algebraic germ of γ at the right of the origin (see [BPR06, Section 3.3]). According to [BPR06, Theorem 3.17], we can identify ψ with an element of $(\mathbf{R}')^n$ (by a slight abuse of notation, we will denote them in the same manner). Hence by [BPR06, Proposition 3.21], $\lim_\varepsilon \psi = \boldsymbol{y}$. Let finally

$$H = \operatorname{ext}(B, \mathbf{R}') \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\psi)) \subset (\mathbf{R}')^n$$

where $\operatorname{ext}(B, \mathbf{R}')$ is the extension of B to $\mathbf{R}'$ and $\boldsymbol{\varphi}\varphi j$ for $1 \leq j \leq n$, with some notation abuse, still denote the extension of $\boldsymbol{\varphi}\varphi j$ to $\mathbf{R}'$.

Since $\gamma((0,1)) \subset B$, by [BPR06, Proposition 3.19], ψ is in $\operatorname{ext}(B, \mathbf{R}')$. Hence, ψ in H and H is non-empty. Moreover B is bounded since $\boldsymbol{\varphi}_1 : V \cap \mathbf{R}^n \to \mathbf{R}$ is a proper map bounded

below by assumption (P). Then [BPR06, Proposition 3.19] states that $\mathrm{ext}(B, \mathbf{R}')$ and then H are bounded over $\mathbf{R}$. Hence the map $\lim_\varepsilon$ is well defined on H and

$$\boldsymbol{y} \in \lim_\varepsilon H = \{\lim_\varepsilon \boldsymbol{y}',\ \boldsymbol{y}' \in H\} \subset \mathbf{R}^n.$$

Finally, as $\boldsymbol{\varphi}_{i-1}$ is semi-algebraic and continuous, $\lim_\varepsilon H$ is contained in $\overline{B} \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\boldsymbol{y}))$ by [BPR06, Lemma 3.24]. But $\boldsymbol{y} \in F_i$, so that

$$\boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\boldsymbol{y})) \subset \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(K_i)),$$

and finally $\lim_\varepsilon H$ is actually in $\overline{B} \cap F_i$.

Let H_1 be the semi-algebraically connected component of H containing ψ. By [BPR06, Proposition 5.24], $\lim_\varepsilon H_1$ is the semi-algebraically connected component of $\lim_\varepsilon H$ containing $\boldsymbol{y}$. Actually, we just proved that every $\boldsymbol{w}$ in $\lim_\varepsilon H_1$ can be semi-algebraically connected to $\boldsymbol{y}$ into $\overline{B} \cap F_i$. We find now some $\boldsymbol{w} \in \lim_\varepsilon H_1$ that can be connected to a point $\boldsymbol{z} \in B \cap (F_i \cup W_i)$ to end the proof. Such a $\boldsymbol{w}$ must be the origin of a germ of semi-algebraic functions that lies in $B \cap (W_i \cup F_i)$.

By assumption (A), V is d-equidimensional. By assumption (B_2), for all $\boldsymbol{z} \in V$, the algebraic set $V \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\boldsymbol{z}))$ is $(d-i+1)$-equidimensional. Then, if we denote by $\mathbf{C}'$ the algebraic closure of $\mathbf{R}'$, it is an algebraic closed extension of $\mathbf{C}$, so that the algebraic sets of $(\mathbf{C}')^n$

$$Z = \left\{\boldsymbol{z} \in (\mathbf{C}')^n \mid \forall h \in \boldsymbol{I}(V), h(\boldsymbol{z}) = 0\right\} \quad \text{and} \quad Z \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\psi)))$$

are equidimensional of dimension respectively d and $(d-i+1)$. Since B is a semi-algebraically connected component of $V_{|\boldsymbol{\varphi}_{1<}} u$, then, by [BPR06, Proposition 5.24], $\mathrm{ext}(B, \mathbf{R}')$ is a semi-algebraically connected component of

$$\mathrm{ext}(V_{|\boldsymbol{\varphi}_{1<}} u, \mathbf{R}') = \mathrm{ext}(V \cap \mathbf{R}^n, \mathbf{R}')_{|\boldsymbol{\varphi}_{1<}} u = Z_{|\boldsymbol{\varphi}_1 < u},$$

by [BPR06, Transfer Principle, Th. 2.98]. Then, since H_1 is a semi-algebraically connected component of $H = \mathrm{ext}(B, \mathbf{R}') \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{\varphi}_{i-1}(\psi))$, one can apply Lemma 6.3.4 on Z with $\mathbf{K} = \mathbf{R}'$. Hence

$$H_1 \cap K(\boldsymbol{\varphi}_i, Z) \neq \emptyset.$$

By Corollary 2.5.6, $K(\boldsymbol{\varphi}_i, Z)$ is defined over $\mathbf{R}$ as V and $\boldsymbol{\varphi}_i$ are. Then, by [BPR06, Transfer Principle, Th. 2.98],

$$K(\boldsymbol{\varphi}_i, Z) \cap (\mathbf{R}')^n = \mathrm{ext}(K(\boldsymbol{\varphi}_i, V) \cap \mathbf{R}^n, \mathbf{R}'),$$

so that

$$\emptyset \quad \subsetneq \quad H_1 \cap \mathrm{ext}(K(\boldsymbol{\varphi}_i, V) \cap \mathbf{R}^n, \mathbf{R}') \quad \subset \quad \mathrm{ext}(B \cap K(\boldsymbol{\varphi}_i, V), \mathbf{R}').$$

Therefore let $\zeta \in \mathrm{ext}(B \cap K(\boldsymbol{\varphi}_i, V), \mathbf{R}')$, let $\boldsymbol{w} = \lim_\varepsilon \zeta$ and τ be a representative of ζ on $(0, t_0)$, where $t_0 > 0$. By [BPR06, Proposition 3.21], we can continuously extend τ to 0 such that $\tau(0) = \boldsymbol{w}$. Besides for all $t \in (0, t_0)$,

$$\tau(t) \in B \cap K(\boldsymbol{\varphi}_i, V) \subset B \cap (W_i \cup F_i).$$

Then $\tau([0, t_0)) \subset \overline{B} \cap (F_i \cup W_i)$ so that

$$\boldsymbol{w} \in \overline{B} \cap (F_i \cup W_i) \quad \text{and} \quad \boldsymbol{z} = \tau(t_0/2) \in B \cap (F_i \cup W_i).$$

Besides, since $\boldsymbol{w} \in \lim_\varepsilon H_1$ we have seen that it can be connected to $\boldsymbol{y}$ a semi-algebraic path in $\overline{B} \cap (F_i \cup W_i)$. In the end, there exist two consecutive paths into $\overline{B} \cap (F_i \cup W_i)$, connecting $\boldsymbol{y}$ to $\boldsymbol{w}$, and $\boldsymbol{w}$ to $\boldsymbol{z} \in B \cap \mathcal{R}$ (namely τ). □

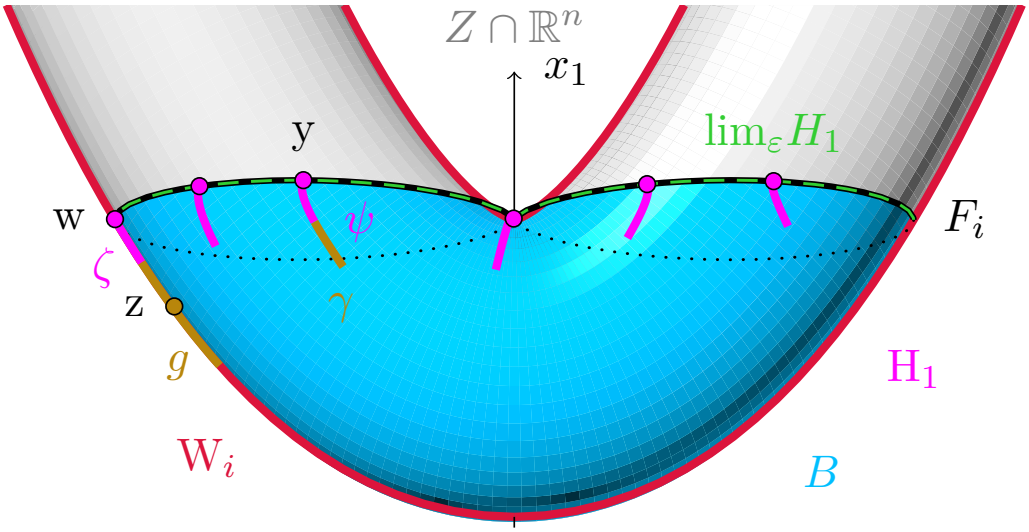


Figure 6.9. Illustration of proof of Lemma 6.3.6 with $\boldsymbol{\varphi}_1 = \pi_1$ and V is isomorphic to $\boldsymbol{V}(x_1^2 + x_2^2 - 1) \times \boldsymbol{V}(x_1 - x_2^2)$. Elements of H_1 can be seen as curves of infinitesimal lengths, starting from a point of $\lim_\varepsilon H_1$, and lying in B. Here, $\lim_\varepsilon H_1$ is the set of points that share the same first coordinate than $\boldsymbol{y}$. Hence, the above proof consisted in choosing a ζ in H_1, that lives "inside" $W_i \cup \mathrm{sing}(V)$ (actually in $\mathrm{ext}(W_i \cup \mathrm{sing}(V), \mathbf{R}\langle\varepsilon\rangle)$).

We can now prove Proposition 6.3.3. This proof is illustrated by Figure 6.9.

Proof of Proposition 6.3.3. Let B be a semi-algebraically connected component of $C_{|\boldsymbol{\varphi}_{1<}} u$. Since $\boldsymbol{\varphi}_1$ is a proper map bounded from below on $V \cap \mathbf{R}^n$ by assumption P, $C_{|\boldsymbol{\varphi}_{1<}} u$, and then B, are bounded. Then applying Proposition 6.2.8 shows that:

$$\emptyset \subsetneq B \cap K(\boldsymbol{\varphi}_1, V) \subset B \cap F_i \subset B \cap (F_i \cup W_i).$$

The first item is then proved. Let $\boldsymbol{y} \in \overline{B} \cap (F_i \cup W_i)$. To prove the second item, one only needs to consider the case where $\boldsymbol{y} \in \overline{B} \cap (W_i - F_i)$ according to Lemma 6.3.6. Moreover one can assume that $\boldsymbol{y} \notin B$ and then $\boldsymbol{\varphi}_1(\boldsymbol{y}) = u$, otherwise, taking $\boldsymbol{z} = \boldsymbol{y}$, would end the proof.

Let D be the semi-algebraically connected component of $(W_i)_{|\varphi_1\leq}u$ containing $\boldsymbol{y}$. We consider two disjoint cases.

1. *If $D \not\subset \overline{B}$,* there exists $\boldsymbol{y}' \in D$ such that $\boldsymbol{y}' \notin \overline{B}$. Then let $\gamma\colon [0,1] \to D$ such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(1) = \boldsymbol{y}'$. Hence, if

$$t_1 = \max\{t \in [0,1) \mid \gamma(t) \in \overline{B}\},$$

then $\gamma(t_1) \in K(\varphi_1, V)$ by the contrapositive of statement $c)$ of Lemma 6.2.5. Since $K(\varphi_1, V) \subset F_i$, we can apply Lemma 6.3.6 to $\gamma(t_1)$ and find $\boldsymbol{z} \in B \cap (F_i \cup W_i)$ that is connected to $\gamma(t_1)$ and then to $\boldsymbol{y}$ by a semi-algebraic path in $\overline{B} \cap (F_i \cup W_i)$.

2. *If $D \subset \overline{B}$,* we claim that there exists some $\boldsymbol{z} \in D \cap F_i$. Indeed since D is a semi-algebraically connected component of $(W_i)_{|\varphi_1 \leq u}$ and φ_1 is a proper map, D is bounded. Then by Proposition 6.2.8 there exists $\boldsymbol{y}' \in D \cap K(\varphi_1, W_i)$. If $\boldsymbol{y}' \in \operatorname{sing}(W_i)$ then $\boldsymbol{y}' \in \operatorname{sing}(V)$ by assumption B_1 and taking $\boldsymbol{z} = \boldsymbol{y}' \in F_i$ one concludes as in the first item.

   Else $\boldsymbol{y}'$ is in $W(\varphi_1, W_i)$, and we let E be the semi-algebraically connected component of $W(\varphi_1, W_i)$ containing $\boldsymbol{y}'$. Since $\varphi_1(W(\varphi_1, W_i))$ is finite by Sard's lemma, $\varphi_1(E) = \{\varphi_1(\boldsymbol{y}')\}$, so that $E \subset (W_i)_{|\varphi_1 \leq u}$. Hence, since E is semi-algebraically connected, $E \subset D$. By assumption C_2, there exists $\boldsymbol{z} \in E \cap S_i$, so that $\boldsymbol{z} \in D \cap S_i \subset D \cap F_i$ and we are done.

   Then we can connect $\boldsymbol{y}$ to $\boldsymbol{z}$ inside $D \subset \overline{B} \cap W_i$ and since $\boldsymbol{z}$ is in $D \cap F_i$, which is contained in $\overline{B} \cap F_i$, we can connect similarly $\boldsymbol{z}$ to some $\boldsymbol{z}' \in B \cap (F_i \cup W_i)$ inside $\overline{B} \cap F_i$ by Lemma 6.3.6. Putting things together, $\boldsymbol{y}$ is connected to some $\boldsymbol{z}' \in B \cap (F_i \cup W_i)$ by a semi-algebraic path in $\overline{B} \cap F_i$.

□

Corollary 6.3.7. *Let $u \in \mathbf{R}$ such that for all $u' < u$, $\mathrm{RM}(u')$ holds. Let C be a semi-algebraically connected component of $V_{|\varphi_1 \leq}u$ such that $C_{|\varphi_1 <}u$ is non-empty. If B is a semi-algebraically connected component of $C_{|\varphi_1 <}u$, then $\overline{B} \cap \mathcal{R}$ is non-empty and semi-algebraically connected.*

Proof. Let $\boldsymbol{y}$ and $\boldsymbol{y}'$ be in $\overline{B} \cap \mathcal{R}$. According to Proposition 6.3.3, they can respectively be connected to some $\boldsymbol{z}$ and $\boldsymbol{z}'$ in $B \cap \mathcal{R}$, by a semi-algebraic path in $\overline{B} \cap \mathcal{R}$. As B is semi-algebraically connected, there exists a semi-algebraic path $\gamma\colon [0,1] \to B$ connecting $\boldsymbol{z}$ to $\boldsymbol{z}'$. Let

$$u' = \max\left\{\varphi_1(\gamma(t)) \mid t \in [0,1]\right\},$$

so that $\gamma([0,1]) \subset V_{|\varphi_1 \leq}u'$. Such a u' exists by continuity of γ, and satisfies $u' < u$, as $[0,1]$ is closed and bounded.

Let B' be the semi-algebraically connected component of $B_{|\varphi_1 \leq}u'$ that contains $\gamma([0,1])$. Since B' is also a semi-algebraically connected component of $V_{|\varphi_1 \leq}u'$, property $\mathrm{RM}(u')$ states that $B' \cap \mathcal{R}$ is non-empty and semi-algebraically connected. Then, as $\boldsymbol{z}$ and $\boldsymbol{z}'$ are in $B' \cap \mathcal{R}$, they can be connected by a semi-algebraic path in $B' \cap \mathcal{R}$, and then, in $B \cap \mathcal{R}$. Thus $\boldsymbol{y}$ and $\boldsymbol{y}'$ are connected by a semi-algebraic path in $\overline{B} \cap \mathcal{R}$ and we are done. □

6.3.2 Recursive proof of the truncated roadmap property

In order to prove that $\mathrm{RM}(u)$ holds for all $u \in \mathbf{R}$, one can consider two disjoint cases: whether u is a real singular value of φ_1, that is $u \in \varphi_1(K_i)$, or not. The following lemma allows us to proceed by induction.

Lemma 6.3.8. *The set $\varphi_1(K_i)$ is non-empty and finite.*

Proof. By the algebraic version of Sard's theorem [SS17, Proposition B.2], the set of critical values of φ_1 on V is an algebraic set of $\mathbf{C}$ of dimension 0. Then, it is either empty or non-empty but finite. Hence, $\varphi_1(K_i)$ is either empty or non-empty but finite, as S_i and $\mathrm{sing}(V)$ are, by assumption. Moreover since φ_1 is a proper map bounded from below on $V \cap \mathbf{R}^n$ by assumption (P), for any $u \in \mathbf{R}$, $Z_{|\varphi<u}$ is bounded. Then, since V is not empty, by Proposition 6.2.8 the sets $K(\varphi_1, V)$ and then $\varphi_1(K_i)$ are not empty. □

We denote by $v_1 < \ldots < v_\ell$ the points of $\varphi_1(K_i \cap \mathbf{R}^n)$ and, in addition, let $v_{\ell+1} = +\infty$. We proceed by proving the two following steps.

Step 1: Let $u \in \mathbf{R}$, if $\mathrm{RM}(u')$ holds for all $u' < u$, then $\mathrm{RM}(u)$ holds.

Step 2: Let $j \in \{1, \ldots, \ell\}$, if $\mathrm{RM}(v_j)$ holds, then for all $u \in (v_j, v_{j+1})$, $\mathrm{RM}(u)$ holds.

Remark that, by Lemma 6.2.7, $v_1 = \min_{V \cap \mathbf{R}^n} \varphi_1$, since $V \cap \mathbf{R}^n$ is closed. Then for $u' < v_1$, $V_{|\varphi \leq u'} = \emptyset$ and $\mathrm{RM}(u')$ trivially holds. Hence, proving these two steps is enough to prove $\mathrm{RM}(u)$ for all u in $\mathbf{R}$, by an immediate induction.

Proposition 6.3.9 (Step 1). *Let $u \in \mathbf{R}$. Assume that for all $u' < u$, $\mathrm{RM}(u')$ holds. Then $\mathrm{RM}(u)$ holds.*

The proof of this proposition is illustrated by Figure 6.10.

Proof. Let $u \in \mathbf{R}$ be such that for all $u' < u$, $\mathrm{RM}(u')$ holds and let C be a semi-algebraically connected component of $V_{|\varphi_1 \leq} u$. We have to prove that $C \cap \mathcal{R}$ is non-empty and semi-algebraically connected.

If $C_{|\varphi_{1<}} u$ is empty, then, by Lemma 6.2.7, $C \subset K(\varphi_1, V)$. But the points of $K(\varphi_1, V)$ are either in W_i or in $\mathrm{sing}(V) \subset F_i$. Hence $K(\varphi_1, V) \subset \mathcal{R}$ and $C \cap \mathcal{R} = C$, which is non-empty and semi-algebraically connected by definition.

From now on, $C_{|\varphi_{1<}} u$ is supposed to be non-empty and let $B_1, \ldots, B_r$ be its semi-algebraically connected components. According to Corollary 6.3.7, for all $1 \leq j \leq r$, $\overline{B_j} \cap \mathcal{R}$ is non-empty and semi-algebraically connected. Then, as $\overline{B_j} \subset C$,

$$\overline{B_j} \cap \mathcal{R} \subset C \cap \mathcal{R}$$

for every $1 \leq j \leq r$, and $C \cap \mathcal{R}$ is non-empty.

Let us now prove that $C \cap \mathcal{R}$ is semi-algebraically connected. Let $\boldsymbol{y}$ and $\boldsymbol{y}'$ in $C \cap \mathcal{R}$. As C is semi-algebraically connected, there exists a semi-algebraically continuous map $\gamma \colon [0,1] \to C$ such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(1) = \boldsymbol{y}'$. Now let

$$G = \gamma^{-1}(C_{|\varphi_{1=}} u \cap K(\varphi_1, V)) \quad \text{and} \quad H = [0,1] - G.$$

We denote by $G_1, \ldots, G_N$ the connected components of G and $H_1, \ldots, H_M$ those of H. The sets H_j for $1 \leq j \leq M$ are open intervals of $[0,1]$, and we note $\ell_j = \inf(H_j)$ and $r_j = \sup(H_j)$. Since $\gamma(G)$ already lies in $C \cap \mathcal{R}$, let us establish that for every $1 \leq j \leq M$, $\gamma(\ell_j)$ and $\gamma(r_j)$ can be connected by another semi-algebraic path τ_j in $C \cap \mathcal{R}$.

Let $1 \leq j \leq M$, then $\gamma(H_j) \cap (C_{|\boldsymbol{\varphi}_{1=}} u \cap K(\boldsymbol{\varphi}_1, V)) = \emptyset$ by definition. Moreover, $\gamma(H_j) \subset C$ so that

$$\gamma(H_j) \cap (V_{|\boldsymbol{\varphi}_{1=}} u \cap K(\boldsymbol{\varphi}_1, V)) = \emptyset.$$

Hence, since H_j is connected, there exists (by Proposition 6.2.1) a unique semi-algebraically connected component B of $V_{|\boldsymbol{\varphi}_{1<}} u$ such that $\gamma(H_j) \subset \overline{B}$. But $\gamma(H_j) \subset C$, so that $\overline{B}$ and thus B are actually contained in C. Therefore, B is actually a semi-algebraically connected component of $C_{|\boldsymbol{\varphi}_{1<}} u$ and there exists $1 \leq k \leq r$ such that $B = B_k$. At this step $\gamma(H_j) \subset \overline{B_k}$, so that

$$\gamma([\ell_j, r_j]) = \gamma(\overline{H_j}) \subset \overline{\gamma(H_j)} \subset \overline{B_k},$$

and both $\gamma(\ell_j)$ and $\gamma(r_j)$ are in $\overline{B_k}$. Remark that both ℓ_j and r_j are in G, so that both $\gamma(\ell_j)$ and $\gamma(r_j)$ are in $K(\boldsymbol{\varphi}_1, V) \subset F_i \subset \mathcal{R}$. Thus, both $\gamma(\ell_j)$ and $\gamma(r_j)$ are in $\overline{B_k} \cap \mathcal{R}$. According to Corollary 6.3.7, they can be connected by a semi-algebraic path $\tau_j \colon [0,1] \to \overline{B_k} \cap \mathcal{R} \subset C \cap \mathcal{R}$.

In conclusion, we have proved that for $1 \leq j \leq M$, $\gamma(\ell_j)$ and $\gamma(r_j)$ can be connected by a semi-algebraic path τ_j in $C \cap \mathcal{R}$. Therefore the semi-algebraic sub-paths $\gamma_{|H_j}$ can be replaced by the τ_j's, which lie in $C \cap \mathcal{R}$. Moreover, for all $1 \leq j \leq N$

$$\gamma(G_j) \subset C \cap \mathcal{R}.$$

Since the H_j's and G_j's form a partition of $[0,1]$, by putting together alternatively the τ_j's and the $\gamma_{|G_j}$'s, one obtains a semi-algebraic path in $C \cap \mathcal{R}$ connecting $\boldsymbol{y} = \gamma(0)$ to $\boldsymbol{y}' = \gamma(1)$. And we are done. □

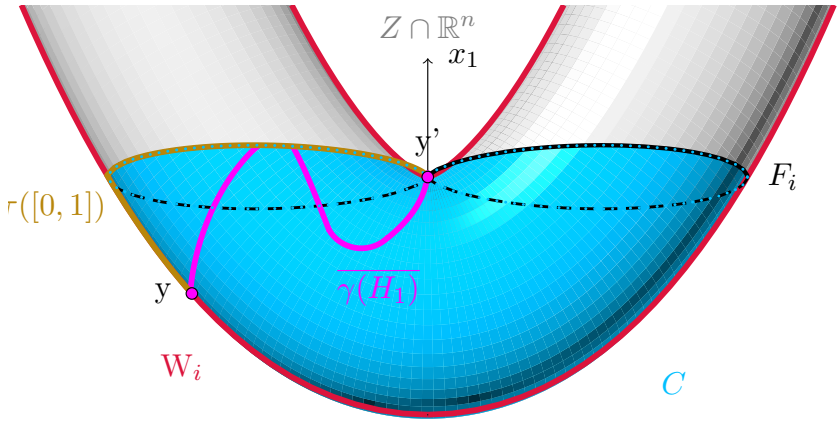


Figure 6.10. Illustration of proof of Proposition 6.3.9 with $\boldsymbol{\varphi}_1 = \pi_1$ and V is isomorphic to $\boldsymbol{V}(x_1^2 + x_2^2 - 1) \times \boldsymbol{V}(x_1 - x_2^2)$. Here, only $\boldsymbol{y}'$ belongs to $C_{|\pi_1 = u} \cap K(\pi_1, V)$. Then we replace the path $\gamma = \gamma_{|H_1}$ by a path τ_1 that lies in the intersection of the roadmap and the semi-algebraically connected component C.

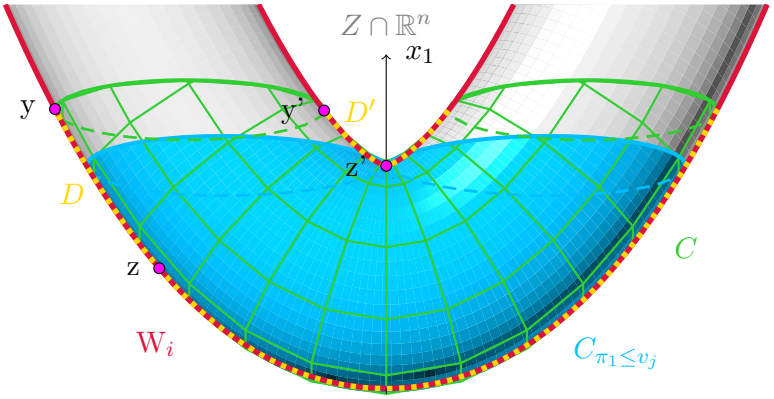


Figure 6.11. Illustration of proof of Proposition 6.3.10 with $\varphi_1 = \pi_1$ and V is isomorphic to $\boldsymbol{V}(x_1^2 + x_2^2 - 1) \times \boldsymbol{V}(x_1 - x_2^2)$. We connect the points $\boldsymbol{y}$ and $\boldsymbol{y}'$ in $C \cap W_i$ to respectively $\boldsymbol{z}$ and $\boldsymbol{z}'$ in $C_{|\pi_1 \leq v_j}$. Then we are reduced to the case of Step 1.

Proposition 6.3.10 (Step 2). *Let $j \in \{1, \ldots, \ell\}$, if $\mathrm{RM}(v_j)$ holds, then for all $u \in (v_j, v_{j+1})$, $\mathrm{RM}(u)$ holds.*

The proof of this proposition is illustrated by Figure 6.11 above.

Proof. Let $j \in \{0, \ldots, \ell\}$ and $u \in (v_j, v_{j+1})$. Let C be a semi-algebraically connected component of $V_{|\varphi_{1\leq}} u$; we have to prove that $C \cap \mathcal{R}$ is non-empty and semi-algebraically connected.

Let us first prove that $C_{|\varphi_{1\leq}} v_j \cap \mathcal{R}$ is non-empty and semi-algebraically connected. By assumption (A), V is an equidimensional algebraic set of positive dimension, and by assumption (P), the restriction of φ_1 to $V \cap \mathbf{R}^n$ is a proper map bounded below. Moreover, as $\varphi_1\left(K(\varphi_1, V) \cap \mathbf{R}^n\right) \subset \{v_1, \ldots, v_\ell\}$, then

$$V_{|\varphi_{1\in}}(v_j, u] \cap K(\varphi_1, V) = \emptyset.$$

Then using Corollary 6.2.12, one deduces that $C_{|\varphi_{1\leq}} v_j$ is a semi-algebraically connected component of $V_{|\varphi_{1\leq}} v_j$. Hence, by property $\mathrm{RM}(v_j)$, the set $C_{|\varphi_{1\leq}} v_j \cap \mathcal{R}$ is non-empty and semi-algebraically connected. In particular, $C \cap \mathcal{R}$ is non-empty.

Let us now prove that $C \cap \mathcal{R}$ is semi-algebraically connected. Let $\boldsymbol{y}$ be in $C \cap \mathcal{R}$. According to the previous paragraph, one just need to be able to connect $\boldsymbol{y}$ to a point $\boldsymbol{z}$ of $C_{|\varphi_{1\leq}} v_j \cap \mathcal{R}$ by a semi-algebraic path in $C \cap \mathcal{R}$ and then apply $\mathrm{RM}(v_j)$. First, if $\boldsymbol{y} \in C_{|\varphi_{1\leq}} v_j \cap \mathcal{R}$, there is nothing to do. Suppose now that $\boldsymbol{y} \in C_{|\varphi_{1\in}}(v_j, u] \cap \mathcal{R}$. We claim that actually

$$\boldsymbol{y} \in C \cap W_i.$$

Indeed, if $\boldsymbol{y} \in C \cap F_i$, then $\varphi_{i-1}(\boldsymbol{y}) \in \varphi_{i-1}(K_i)$ and $\varphi_1(\boldsymbol{y})$ would be one of the $v_1, \ldots, v_\ell$.

Let D be the semi-algebraically connected component of $(C \cap W_i)_{|\varphi_{1\leq u}}$ containing $\boldsymbol{y}$. Remark that D is a semi-algebraically connected component of $(W_i)_{|\varphi_{1\leq u}}$, as it contains $\boldsymbol{y}$ and is contained in C. Since $\varphi_1(W(\varphi_1, W_i))$ is finite by Sard's lemma, we get that $\varphi_1(W(\varphi_1, W_i)) \subset \varphi_1(S_i)$, by assumption (C_2), so that

$$(v_j, u) \cap \varphi_1(W(\varphi_1, W_i)) = \emptyset.$$

Since W_i is equidimensional and smooth outside $\mathrm{sing}(V)$, then by Corollary 6.2.12, $D_{|\varphi_1 \leq v_j}$ is a semi-algebraically connected component of $(W_i)_{|\varphi_1 \leq v_j}$. Therefore, let $z \in D_{|\varphi_1 \leq} v_j$. Since D is semi-algebraically connected, there exists a semi-algebraic path, connecting $y \in D \subset C \cap \mathcal{R}$ to

$$z \in D_{|\varphi_1 \leq} v_j \subset C_{|\varphi_1 \leq} v_j \cap \mathcal{R}$$

in $D \subset C \cap \mathcal{R}$. We are done. □

Conclusion

In this chapter, we proved a new connectivity result for constructing roadmaps for smooth unbounded algebraic sets. This has been done by adapting the proofs and constructions designed in [SS11] for linear projections to general polynomial maps.

This provides the theoretical tools for a new class of roadmap algorithms dealing with unbounded real algebraic sets, without prior infinitesimal deformation to satisfy the original connectivity result.

Hence, adapting the construction of [SS17], one can hope to emulate the same structure of their algorithm, relying this time on the new connectivity result. This would allow to get similar complexity performances while relaxing the boundedness assumption on the input. This is the purpose of the next chapter.

7 A nearly optimal algorithm for unbounded smooth real algebraic sets

Abstract. In this chapter, we make effective the new connectivity result proved in the previous chapter to design a Monte Carlo algorithm which, on input a finite sequence of polynomials with coefficients in a real field $\mathbf{Q}$, defining an algebraic set $V \subset \mathbf{C}^n$, with $\mathbf{C}$ the algebraic closure of $\mathbf{Q}$, satisfying regularity assumptions and an algebraic representation of finitely many sample points $\mathcal{P}$ in V, computes a roadmap for $(V, \mathcal{P})$. This algorithm generalizes the state-of-the-art algorithm designed in [SS17] by dropping a boundedness assumption on the real trace of V.

The output size and running times of our algorithm are both polynomial in $(nD)^{n \log d}$ where D is the maximal degree of the input equations and d is the dimension of V. As far as we know, the best previously known algorithm dealing with such sets has an output size and running time polynomial in $(nD)^{n \log^2 n}$. Moreover, the constants in the exponent of this complexity bound are made explicit, as in [SS17].

This is joint work with M. Safey El Din and É. Schost.

7.1 Introduction

Let $\mathbf{Q}$ be a real field and let $\mathbf{R}$ (resp. $\mathbf{C}$) be a real (resp. algebraic) closure of $\mathbf{Q}$. Further, $n \geq 0$ is an integer. Let $V \subset \mathbf{C}^n$ be an algebraic set defined over $\mathbf{Q}$, that is defined by polynomials with coefficients in $\mathbf{Q}$. As seen in Section 1.3, the problem of solving connectivity queries on some finitely many query points $\mathcal{P} \subset V \cap \mathbf{R}^n$, in the real algebraic set $V \cap \mathbf{R}^n$, can be reduced to the computation of a roadmap of $(V, \mathcal{P})$ – see also Section 5.3. The algorithm with the best known complexity can be found in [SS17]. This algorithm runs in time $(nD)^{O(n \log d)}$, where d is the dimension of the input algebraic set, which is assumed to be smooth and bounded. Moreover, explicit constants in the big Oh exponent are given, showing that the algorithm runs in time subquadratic in the degree bound of the output. As mentioned earlier, removing these assumptions using techniques from [Can95, BPR00, BR14, BRSS14] would require the introduction of possibly several infinitesimals, resulting in increased intermediate data size and, in particular, the loss of the subquadratic behavior.

For this reason, in the previous chapter we have extended the connectivity result underlying the algorithm in [SS17] to generalize it to unbounded cases without any prior infinitesimal deformation.

Open problem for Chapter 7

This now leaves the problem of putting this new connectivity result into practice, and design a roadmap algorithm for smooth real algebraic sets with output size and arithmetic complexity similar to the ones in [SS17], but without using the boundedness assumption.

In this chapter, we design a Monte Carlo algorithm for computing roadmaps based on this latter result, assuming regularity assumptions on the system defining V. Under those assumptions, this improves the state of the art complexity. We illustrate now how Theorem 6.1.1 is used in this chapter to generalize the algorithms of [SS17] to the case of unbounded smooth real algebraic sets.

Let $V \subset \mathbf{C}^n$ be an equidimensional algebraic set of dimension d given as the solutions of some polynomials $f_1, \ldots, f_c$ in $\mathbf{Q}[x_1, \ldots, x_n]$. Assume that $\mathrm{sing}(V)$ is finite. Take

$$\varphi_1 = \sum_{k=1}^{n} x_k^2 - \boldsymbol{a}_k x_k \quad \text{and for } 2 \leq j \leq n \quad \varphi_j = \sum_{k=1}^{n} \boldsymbol{b}_{j,k} x_k,$$

where $\boldsymbol{a} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \in \mathbf{Q}^n$ and, for $2 \leq j \leq n$, $\boldsymbol{b}_j = (\boldsymbol{b}_{j,1}, \ldots, \boldsymbol{b}_{j,n}) \in \mathbf{Q}^n$. Then, the assumption (P) holds, that is:

(P) the restriction of the map $\boldsymbol{\varphi}_1$ to $V \cap \mathbf{R}^n$ is proper and bounded from below.

Now for some chosen $2 \leq i \leq d$, let W_i and F_i be respectively the polar variety and set of fibers as defined in the statement of Theorem 6.1.1. Then, following the preliminary results of [BGHP05, BGH+10], we prove that for a generic choice of $\boldsymbol{a}$ and $\boldsymbol{b}$, assumption (B) do hold:

(B_1) W_i is either empty or $(i-1)$-equidimensional and smooth outside $\mathrm{sing}(V)$;

(B_2) for any $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_i) \in \mathbf{C}^i$, $V \cap \boldsymbol{\varphi}_{i-1}^{-1}(\boldsymbol{y})$ is either empty or $(d-i+1)$-equidimensional.

Finally, one can compute a set $S \subset W(\varphi_1, W_i) \subset V$ by using any algorithm such as [BPR06, Chap. 13] or [SS03a], returning sample points in all connected components of real algebraic sets. Then, such a set S satisfies the last assumption (C) of Theorem 6.1.1:

(C_1) S_i is finite;

(C_2) S_i has a non-empty intersection with every semi-algebraically connected component of $W(\boldsymbol{\varphi}_1, W_i) \cap \mathbf{R}^n$.

Therefore, one can apply Theorem 6.1.1 to V, $\boldsymbol{\varphi}$ and i. We deduce that $W_i \cup F_i$ has a non-empty and connected intersection with all connected components of $V \cap \mathbf{R}^n$, but it is in general an object of dimension greater than 1, so more work is needed.

The design our new algorithm takes $i = 2$. Then, W_2 is expected to have dimension 1 (or be empty), so no further computation is needed. On the other hand, F_2 still has dimension $d-1$, but a key observation is that F_2 is now *bounded*. Then, one can directly apply a slight variant of the algorithm in [SS17] taking F_2 as input: that algorithm already keeps the depth of recursion bounded by $\log_2(n)$, but we should now handle the fact that we work in a hypersurface defined as some level sets of $\boldsymbol{\varphi}_1$. Again, all of this is under the assumption that one can make F_2 satisfy the assumptions of Theorem 6.1.1.

The purpose of this chapter is to conduct this approach. First, by ensuring that the assumptions of Theorem 6.1.1 hold for a "generic" choice of φ (and precise the way this choice is made). Then, by describing precisely the algorithmic steps, taking close attention to the size of the manipulated objects, and the complexities of these manipulations.

Open subproblems for Chapter 7

More precisely, the steps to obtain nearly optimal algorithms for computing roadmaps of smooth real algebraic sets, without boundedness assumptions, are:

- to study how the constructions of generalized Lagrange systems introduced in [SS17] for encoding polar varieties associated to linear projections can be reused in our context; this is covered by Section 7.4;
- to prove that assumption (B) holds for some generic choice of $\boldsymbol{a}$ and $\boldsymbol{b}$ for our polar varieties, which by contrast to those used in [SS17] are no more associated to linear projections; this is the purpose of Sections 7.5, 7.6 and 7.7;
- to prove that the variant of the algorithm designed in [SS17] discussed above still has a complexity similar to the one obtained in [SS17]; this is tackled by Subsection 7.4.5.

Main result. Answering all these problems and putting together the solutions, we get the following result. Recall that $(f_1, \ldots, f_c) \subset \mathbf{Q}[\boldsymbol{X}]$ is said to be a *reduced regular sequence* if for every $i \in \{1, \ldots, c\}$, the ideal $\langle f_1, \ldots, f_i \rangle$ is radical and the algebraic set $\boldsymbol{V}(f_1, \ldots, f_i) \subset \mathbf{C}^n$ is either empty or $(n-i)$-equidimensional.

Contribution to the open problem

Theorem 7.1.1. *Let $\boldsymbol{f} = (f_1, \ldots, f_c)$ be a reduced regular sequence in $\mathbf{Q}[\boldsymbol{X}]$, with $\boldsymbol{X} = x_1, \ldots, x_n$, let D be the maximal degree of the f_i's and suppose that Γ is a straight-line program of length E evaluating $\boldsymbol{f}$. Suppose additionally that $\boldsymbol{V}(\boldsymbol{f}) \subset \mathbf{C}^n$ has finitely many singular points.*
Let $\mathscr{P}$ be a zero-dimensional parametrization of degree μ with $\mathsf{Z}(\mathscr{P}) \subset V(\boldsymbol{f})$. There exists a Monte Carlo algorithm which, on input Γ and $\mathscr{P}$ computes a one-dimensional parametrization $\mathscr{R}$ of a roadmap of $(\boldsymbol{V}(\boldsymbol{f}), \mathsf{Z}(\mathscr{P}))$ of degree

$$\widetilde{O}\left(\mu 16^{3d} (n \log_2(n))^{2(2d-2+12\log_2(d-1))(\log_2(d-1)+6)} D^{(2n+4)(\log_2(d-1)+4)}\right),$$

that is in $\mu(nD)^{O(n \log_2(d))}$, using

$$\widetilde{O}\left(\mu^3 16^{9d} E (n \log_2(n))^{6(2d+12\log_2(d-1))(\log_2(d-1)+7)} D^{3(2n+4)(\log_2(d-1)+5)}\right),$$

that is in $\mu E(nD)^{O(n \log_2(d))}$, arithmetic operations in $\mathbf{Q}$, with $d = n - c$.

Hence, we dropped the boundedness assumption on $\boldsymbol{V}(\boldsymbol{f}) \cap \mathbf{R}^n$ made in [SS17, Theorem 1.1], still keeping a complexity similar to the algorithm presented in [SS17]. Note that the arithmetic complexity statement above is cubic in the *degree* bound $\mathscr{B}$ on the output;

the output *size* itself is $O\left(n\mathscr{B}^2\right)$ elements in $\mathbf{Q}$. Hence, as in [SS17], our runtime is subquadratic in the bound on the output size. The example below illustrates an application of this algorithm on a simple example.

Example 7.1.2. Let $V = \boldsymbol{V}(g) \subset \mathbb{C}^3$ be the hypersurface defined by the vanishing set of the polynomial $g = x_1^3 + x_2^3 + x_3^3 - x_1 - x_2 - x_3 - 1 \in \mathbb{Q}[x_1, x_2, x_3]$. As a hypersurface, V is 2-equidimensional and since $\operatorname{sing}(V) = \emptyset$, V satisfies (A).

Let $\boldsymbol{\varphi} = ((x_1 - 1)^2 + x_2^2 + x_3^2,\ x_1,\ x_2) \subset \mathbb{Q}[x_1, x_2, x_3]$. As the restriction of $\boldsymbol{\varphi}_1$ to $\mathbb{R}^n$ is the square of the Euclidean distance to $(1, 0, 0)$, (P) is satisfied. Since $2 \leq i \leq d$, we must take $i = 2$. Then we see that one can write

$$W_2 = \boldsymbol{V}(f, (3x_1x_3 + 1)(x_1 - x_3) + 3x_3^2 - 1).$$

One checks that W_2 is 1-equidimensional and has no singular point as well, so that $(\boldsymbol{\varphi}, 2)$ satisfies (B_1). Let $K_2 = W^\circ(\boldsymbol{\varphi}_1, W_2)$, which is a finite set of cardinality 45 (of which 5 are real). Besides, for any $\alpha \in \mathbb{C}$,

$$V \cap \boldsymbol{\varphi}_1^{-1}(\alpha) = \boldsymbol{V}(f, (x_1 - 1)^2 + x_2^2 + x_3^2 - \alpha)$$

is either empty or an equidimensional algebraic set of dimension 1. Therefore, $(\boldsymbol{\varphi}, 2)$ satisfies (B). Finally, since $W^\circ(\boldsymbol{\varphi}_1, W_2) \cap \mathbb{R}^3$ is a finite set, assumption (C) holds vacuously. Recall that, by definition, $F_2 = {\boldsymbol{\varphi}_1}^{-1}(\boldsymbol{\varphi}_1(K_2)) \cap V$. In conclusion, by Theorem 6.1.1, $W_2 \cup F_2$ is a 1-roadmap of $(V, \emptyset)$. Figure 7.1 illustrates this example.

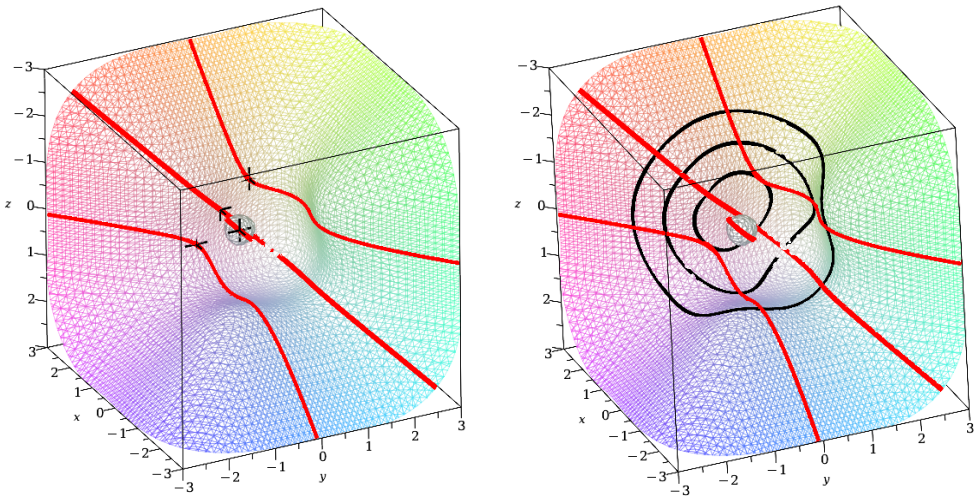


Figure 7.1. An illustration of Example 7.1.2. The real trace $V \cap \mathbb{R}^3$ is plotted twice as a grid. On the left, $W_2 \cap \mathbb{R}^3$ is represented as red lines, and the crosses represent all the real points of K_2. Then, on the right, we replaced the points of K_2 by the fibers of $F_2 \cap \mathbb{R}^3$ (black lines), to repair the connectivity failures of $W_2 \cap \mathbb{R}^3$. In particular, $F_2 \cap \mathbb{R}^3$ connects the semi-algebraically connected components of $W_2 \cap \mathbb{R}^3$ that lie in the same semi-algebraically connected component of $V \cap \mathbb{R}^3$.

7.2 Preliminaries

7.2.1 Minors, rank and submatrices

We present here some technical results on the minors and the rank of a certain class of matrices that will occur in this chapter, when dealing with particular cases and incidence varieties in Section 7.4.

Lemma 7.2.1. *Let $q \geq 1$ and $1 \leq c \leq p$ be integers. Let A, B, C be respectively $c \times p$, $c \times q$ and $i \times p$ matrices with coefficients in a commutative ring R such that M_1 and M_2 are the following $(c+q) \times (q+p)$ matrices:*

$$M_1 = \begin{bmatrix} B & A \\ I_q & \boldsymbol{O} \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} \boldsymbol{O} & A \\ I_q & C \end{bmatrix},$$

where I_q is the identity matrix of size q. Let $m \in R$ and $0 \leq e \leq c$, then for $k = 1, 2$ the following conditions are equivalent:

1. *m is the determinant of a $(q+e)$-submatrix of M_k that contains I_q;*
2. *$(-1)^{qe}m$ is an e-minor of A.*

In this case, if $1 \leq i_1 \leq \cdots \leq i_e \leq c$ and $1 \leq j_1, \ldots, j_e \leq p$ are the indices of respectively the rows and the columns of A selected in item 2, then the corresponding rows and columns in M_k are of respective indices

$$1 \leq i_1 \leq \cdots \leq i_e \leq c+1 \leq \cdots \leq c+q \quad \text{and} \quad 1 \leq \cdots \leq q \leq q+j_1 \leq \cdots \leq q+j_e.$$

Proof. The determinant of any submatrix of M_i containing I_q can be reduced, up to the sign $(-1)^{qe}$, to a minor of A by using the cofactor expansion with respect to the last q rows of M_1 (resp. the first q columns of M_2). Conversely, any e-minor of A is a $(q+e)$-minor of M_k, by extending the associated submatrix of A to a submatrix of M_k containing I_q. The correspondence between indices stated above is then straightforward. □

Lemma 7.2.2. *With the notation of Lemma 7.2.1, if R is a field, then $\operatorname{rank}(M_k) = \operatorname{rank}(A) + q \geq q$ for $k = 1, 2$.*

Proof. For $k = 1$, performing row operations allows us to replace B by the zero matrix, after which the claim becomes evident. For $k = 2$, use column operations. □

7.2.2 Polynomial maps, generalized polar varieties and fibers

Let $Z \subset \mathbf{C}^n$ be an equidimensional algebraic set and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_m)$ be a finite set of polynomials of $\mathbf{C}[\boldsymbol{X}]$; we still denote by $\boldsymbol{\varphi}\colon Z \to \mathbf{C}^m$ the restriction of the polynomial map induced by $\boldsymbol{\varphi}$ to Z.

Let $K(\boldsymbol{\varphi}, Z) = W^\circ(\boldsymbol{\varphi}, Z) \bigcup \operatorname{sing}(Z)$ be the set of *singular points* of $\boldsymbol{\varphi}$ on Z – see Section 2.5 of Chapter 2. Recall that, when Z is defined by a reduced regular sequence $\boldsymbol{f} = (f_1, \ldots, f_c)$,

$K(\varphi, Z)$ is the defined as the intersection of Z with the set of points of $\mathbf{C}^n$ where the Jacobian matrix of $(\boldsymbol{f}, \varphi)$ has rank at most $c+m-1$ (see [SS17, Lemma A.2]).

For $1 \leq i \leq m$, we set

$$\begin{array}{rccc} \varphi_i\colon & \mathbf{C}^n & \to & \mathbf{C}^i \\ & \boldsymbol{y} & \mapsto & (\varphi_1(\boldsymbol{y}), \ldots, \varphi_i(\boldsymbol{y})). \end{array}$$

Given the maps $(\varphi_i)_{1\leq i\leq m}$, we denote $W^\circ(\varphi_i, Z)$, $W(\varphi_i, Z)$ and $K(\varphi_i, Z)$ by respectively $W^\circ_\varphi(i, Z)$, $W_\varphi(i, Z)$ and $K_\varphi(i, Z)$. For $i = 0$, we let $\mathbf{C}^0$ be a singleton of the form $\mathbf{C}^0 = \{\bullet\}$, and $\varphi_0\colon \boldsymbol{y} \in \mathbf{C}^n \to \bullet \in \mathbf{C}^0$ be the unique possible map. Then for all $\boldsymbol{y} \in \mathbf{C}^0$, $\varphi_0^{-1}(\boldsymbol{y}) = \mathbf{C}^n$; we set $W^\circ_\varphi(0, Z) = W_\varphi(0, Z) = \emptyset$. For $0 \leq i \leq m$, the set $W_\varphi(i, Z)$ is called the *i-th generalized polar variety associated to φ on Z*. We refer to Section 2.6 of Chapter 2 for an extended discussion on polar varieties.

The main result we state in this subsection is the following (the somewhat lengthy proof is in Section 7.5). It establishes some genericity properties of generalized polar varieties associated to a class of polynomial maps. It is a generalization of [SS03a, Theorem 1], which only deals with projections.

Proposition 7.2.3. *Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set with finitely many singular points and θ be in $\mathbf{C}[\boldsymbol{X}]$. Let $2 \leq \mathfrak{r} \leq d+1$. For $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_\mathfrak{r})$ in $\mathbf{C}^{\mathfrak{r}n}$, we define $\varphi = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1), \ldots, \varphi_\mathfrak{r}(\boldsymbol{X}, \boldsymbol{\alpha}_\mathfrak{r}))$, where for $2 \leq j \leq m$*

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^n \alpha_{1,k} x_k \quad \text{and} \quad \varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \sum_{k=1}^n \alpha_{j,k} x_k.$$

Then, there exists a non-empty Zariski open subset $\Omega_\mathsf{I}(V, \theta) \subset \mathbf{C}^{\mathfrak{r}n}$ such that for every $\boldsymbol{\alpha} \in \Omega_\mathsf{I}(V, \theta)$ and $i \in \{1, \ldots, \mathfrak{r}\}$, the following holds:

1. *either $W_\varphi(i, V)$ is empty or $(i-1)$-equidimensional;*
2. *the restriction of φ_{i-1} to $W_\varphi(i, V)$ is a Zariski-closed map;*
3. *for any $\boldsymbol{z} \in \mathbf{C}^{i-1}$, the fiber $K_\varphi(i, V) \cap \varphi_{i-1}^{-1}(\boldsymbol{z})$ is finite.*

The connectivity result Theorem 6.1.1 of the previous chapter involve of generalized polar varieties satisfying these properties, but also of fibers of polynomial maps. This pushes us to fix some notations below.

Remark 7.2.4. Let $\varphi = (\varphi_1, \ldots, \varphi_\mathfrak{r})$ be polynomials in $\mathbf{C}[\boldsymbol{X}]$ and an integer $1 \leq e \leq \mathfrak{r}$. Given an algebraic set $V \subset \mathbf{C}^n$ and a set $Q \subset \mathbf{C}^e$, the *fiber of V over Q with respect to φ* is the set $V_{|\varphi_e \in Q} = V \cap \varphi_e^{-1}(Q)$. We say that V *lies over Q with respect to φ* if $\varphi_e(V) \subset Q$. Finally, for $\boldsymbol{z} \in \mathbf{C}^e$, the set $V_{|\varphi_e \in \{\boldsymbol{z}\}}$ will be denoted by $V_{|\varphi_e = \boldsymbol{z}}$.

7.2.3 Charts and atlases of algebraic sets

We say that an algebraic set is *complete intersection* if it can be defined by a number of equations equal to its codimension. Not all algebraic sets are complete intersections; for

instance determinantal varieties and, consequently, a whole class of generalized polar varieties, are a prototype of non-complete intersections. This creates complications to control the complexity of algorithms manipulating generalized polar varieties recursively.

However, we may use local representations which describe Zariski open subsets of an algebraic set with a number of equations equal to its codimension.

Such local representations are obtained by considering *locally closed sets*. We say that a subset V° of $\mathbf{C}^n$ is locally closed if there exist an open $\mathcal{O}$ and a closed Zariski subset Z of $\mathbf{C}^n$ such that $V^\circ = Z \cap \mathcal{O}$. In that case, the dimension of V° is the dimension of its Zariski closure V, and V° is said to be equidimensional if V is. In this situation, we define $\mathrm{reg}(V^\circ) = \mathrm{reg}(V) \cap V^\circ$ and $\mathrm{sing}(V^\circ) = \mathrm{sing}(V) \cap V^\circ$, and V° is said to be non-singular if $\mathrm{reg}(V^\circ) = V^\circ$. For $\boldsymbol{f} = (f_1, \ldots, f_c) \subset \mathbf{C}[\boldsymbol{X}]$ with $c \leq n$, we define the locally closed set $\boldsymbol{V}^\circ_{\mathrm{reg}}(\boldsymbol{f})$ as the set of all $\boldsymbol{y}$ where the Jacobian matrix $\mathrm{Jac}(\boldsymbol{f})$ of $\boldsymbol{f}$ has full rank c. We will denote by $\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{f})$ the Zariski closure of $\boldsymbol{V}^\circ_{\mathrm{reg}}(\boldsymbol{f})$.

A *chart* associated to an algebraic set $V \subset \mathbf{C}^n$ can be seen as a local representation of V by another locally closed subset of V that is smooth and in complete intersection. We recall hereafter the definitions introduced in [SS17, Section 2.5], which we slightly generalize. Below, for a polynomial m in $\mathbf{C}[\boldsymbol{X}]$, recall that we write $\mathcal{O}(m) = \mathbf{C}^n - \boldsymbol{V}(m)$.

Definition 7.2.5 (Charts of algebraic sets)**.** Let $1 \leq e \leq \mathfrak{r} \leq n+1$ be integers and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_{\mathfrak{r}}) \subset \mathbf{C}[\boldsymbol{X}]$. Let $Q \subset \mathbf{C}^e$ be a *finite* set and $V, S \subset \mathbf{C}^n$ be algebraic sets lying over Q with respect to $\boldsymbol{\varphi}$. We say that a pair of the form $\chi = (m, \boldsymbol{h})$ with m and $\boldsymbol{h} = (h_1 \ldots, h_c)$ in $\mathbf{C}[\boldsymbol{X}]$ is a *chart* of $(V, Q, S, \boldsymbol{\varphi})$ if the following holds:

(C_1) $\mathcal{O}(m) \cap V - S$ is non-empty;

(C_2) $\mathcal{O}(m) \cap V - S = \mathcal{O}(m) \cap \boldsymbol{V}(\boldsymbol{h})_{|\boldsymbol{\varphi}_e \in Q} - S$;

(C_3) $e + c \leq n$;

(C_4) for all $\boldsymbol{y} \in \mathcal{O}(m) \cap V - S$, $\mathrm{Jac}_{\boldsymbol{y}}([\boldsymbol{h}, \boldsymbol{\varphi}_e])$ has full rank $c + e$.

When $\boldsymbol{\varphi} = (x_1, \ldots, x_n)$ defines the canonical projection, one will simply refer to χ as a chart of (V, Q, S), and if $e = 0$ as a chart of (V, S) (no matter what $\boldsymbol{\varphi}$ is).

The first condition C_1 ensures that χ is not trivial, and the following ones ensure that χ is a smooth representation of $V - S$ in complete intersection (typically, for V equidimensional, S contains the singular points of V). This is a generalization of [SS17, Definition 2.2] in the sense that, if $\boldsymbol{\varphi} = (x_1, \ldots, x_n)$, one recovers the same definition.

Lemma 7.2.6. *Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional. Let $\chi = (m, \boldsymbol{h})$, with $\boldsymbol{h} = (h_1, \ldots, h_c)$, be a chart of (V, S) and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_{n+1}) \subset \mathbf{C}[\boldsymbol{X}]$. Then, for $1 \leq i \leq d+1$ and $\boldsymbol{y} \in \mathcal{O}(m) \cap V - S$, $\boldsymbol{y}$ lies in $W_{\boldsymbol{\varphi}}(i, V)$ if and only if $\mathrm{Jac}_{\boldsymbol{y}}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ does not have full rank $c + i$.*

Proof. Let $\boldsymbol{y} \in \mathcal{O}(m) \cap V - S$. By [SS17, Lemma A.8], $\boldsymbol{y} \in \mathrm{reg}(V)$, so that $\boldsymbol{y}$ lies in $W_{\boldsymbol{\varphi}}(i, V)$ if and only if it lies in $W^\circ_{\boldsymbol{\varphi}}(i, V)$. Besides, by [SS17, Lemma A.7], $\mathrm{T}_{\boldsymbol{y}} V$ coincide with $\ker \mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})$. Hence, by definition $\boldsymbol{y}$ lies in $W_{\boldsymbol{\varphi}}(i, V)$ if and only if $\mathrm{d}_{\boldsymbol{y}} \boldsymbol{\varphi}_i(\ker \mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})) \neq \mathbf{C}^i$. But the latter, is equivalent to saying that the matrix $\mathrm{Jac}_{\boldsymbol{y}}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ does not have full rank $c + i$. □

A straightforward rewriting of Lemma 7.2.6 is the following which provides a local description of polar variety by means of a critical locus on a variety defined by a complete intersection.

Lemma 7.2.7. *Reusing the notation of Lemma 7.2.6, the sets* $W_{\boldsymbol{\varphi}}(i, V)$ *and* $W^{\circ}_{\boldsymbol{\varphi}}(i, \boldsymbol{V}_{reg}(\boldsymbol{h}))$ *coincide in* $\mathcal{O}(m) - S$.

Together with the notion of charts, we define atlases as a collection of charts that cover the whole algebraic set we consider.

Definition 7.2.8 (Atlases of algebraic sets)**.** Let $1 \leq e \leq n$ be integers and the sequence $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_{n+1}) \subset \mathbf{C}[\boldsymbol{X}]$. Let $Q \subset \mathbf{C}^e$ be a *finite* set and $V, S \subset \mathbf{C}^n$ be algebraic sets lying over Q with respect to $\boldsymbol{\varphi}$. Let $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ with $\chi_j = (m_j, \boldsymbol{h}_j)$ for all j, and $m \in \mathbf{C}[\boldsymbol{X}]$ and $\boldsymbol{h} = (h_1 \ldots, h_c) \subset \mathbf{C}[\boldsymbol{X}]$. We say that $\boldsymbol{\chi}$ is an *atlas* of $(V, Q, S, \boldsymbol{\varphi})$ if the following holds:

(A_1) $s \geq 1$;

(A_2) for each $1 \leq j \leq s$, χ_i is a chart of $(V, Q, S, \boldsymbol{\varphi})$;

(A_3) $V - S \subset \bigcup_{1 \leq j \leq s} \mathcal{O}(m_j)$.

When $\boldsymbol{\varphi} = (x_1, \ldots, x_n)$ is defines the canonical projection, one simply refers to $\boldsymbol{\chi}$ as an atlas of (V, Q, S), and if $e = 0$ as an atlas of (V, S).

Here the definition is the same as [SS17, Definition 2.3]. Note that, according to [SS17, Lemma A.13], there exists an atlas of $(V, \mathrm{sing}(V))$ for any equidimensional algebraic set V. This allows us to construct atlases of objects of V through regular representations.

7.2.4 Charts and atlases for generalized polar varieties

We deal now with the geometry of generalized polar varieties (under genericity assumptions) and show how to define charts and atlases for them. In the following, if no mention is made, we let $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_{n+1}) \subset \mathbf{C}[\boldsymbol{X}]$; for $1 \leq i \leq n$, we denote by $\boldsymbol{\varphi}_i$ the sequence $(\varphi_1, \ldots, \varphi_i)$ and, by a slight abuse of notation, the polynomial map it defines.

Definition 7.2.9. Let $\boldsymbol{h} = (h_1, \ldots, h_c) \subset \mathbf{C}[\boldsymbol{X}]$ with $1 \leq c \leq n$ and let $i \in \{1, \ldots, n - c\}$. Let m'' be a $(c + i - 1)$-minor of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ containing the rows of $\mathrm{Jac}(\boldsymbol{\varphi}_i)$. We denote by $\mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')$ the sequence of $(c + i)$-minors of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ obtained by successively adding the missing row and a missing column of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ to m''. This sequence has length $n - c - i + 1$.

Then, given a chart $\chi = (m, \boldsymbol{h})$ of some algebraic set V, we can define a candidate for being a chart of generalized polar varieties associated to $\boldsymbol{\varphi}_i$ and $V(\boldsymbol{h}) \cap \mathcal{O}(m)$.

Definition 7.2.10. Let $V, S \subset \mathbf{C}^n$ be two algebraic sets, $\chi = (m, \boldsymbol{h})$ be a chart of (V, S), with $\boldsymbol{h}$ of length c and $i \in \{1, \ldots, n - c\}$. For every c-minor m' of $\mathrm{Jac}(\boldsymbol{h})$ and every $(c + i - 1)$-minor m'' of $\mathrm{Jac}(\boldsymbol{h}, \boldsymbol{\varphi}_i)$ containing the rows of $\mathrm{Jac}(\boldsymbol{\varphi}_i)$, we define $W_{\mathrm{chart}}(\chi, m', m'', \boldsymbol{\varphi}_i)$ as the pair:

$$W_{\mathrm{chart}}(\chi, m', m'', \boldsymbol{\varphi}_i) = \Big(mm'm'', \ (\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')) \Big)$$

Then, the definition of the associated atlas comes naturally. Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional, $\boldsymbol{\chi} = (\chi_j)_{1\leq j\leq s}$ be an atlas of (V, S) (with $\chi_j = (m_j, \boldsymbol{h}_j)$) and $i \in \{1, \dots, d\}$. Since V is d-equidimensional, by [SS17, Lemma A.12], all the sequences of polynomials $\boldsymbol{h}_j$ have same cardinality $c = n - d$.

Definition 7.2.11. We let $W_{\text{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, i)$ be the sequence of all $W_{\text{chart}}(\chi_j, m', m'', \boldsymbol{\varphi}_i)$ for every $j \in \{1, \dots, s\}$, every c-minor m' of $\operatorname{Jac}(\boldsymbol{h}_j)$ and every $(c + i - 1)$-minor m'' of $\operatorname{Jac}(\boldsymbol{h}_j, \boldsymbol{\varphi}_i)$ containing the rows of $\operatorname{Jac}(\boldsymbol{\varphi}_i)$, for which $\mathcal{O}(m_j m' m'') \cap W_{\boldsymbol{\varphi}}(i, V) - S$ is not empty.

These constructions generalize the ones introduced in [SS17, Section 3.1] in the following sense: for $\boldsymbol{\varphi} = (x_1, \dots, x_n)$, except for some trivial cases, the objects we just defined match the ones in [SS17, Definition 3.1 to 3.3], possibly up to signs (which are inconsequential). The next lemma makes this more precise; in this lemma, we write $\boldsymbol{\pi} = (x_1, \dots, x_n)$ and $\boldsymbol{\pi}_i = (x_1, \dots, x_i)$.

Lemma 7.2.12. *Let V, S be algebraic sets and $\boldsymbol{h} = (h_1, \dots, h_c) \subset \mathbf{C}[\boldsymbol{X}]$. Let $1 \leq i \leq n - c$ and m'' be a $(c + i - 1)$-minor of $\operatorname{Jac}(\boldsymbol{h}, \boldsymbol{\pi}_i)$, containing the rows of $\operatorname{Jac}(\boldsymbol{\pi}_i)$. Then either $m'' = 0$ or*

1. *$\mu'' = (-1)^{i(c-1)} m''$ is a $(c - 1)$-minor of $\operatorname{Jac}(\boldsymbol{h}, i)$;*
2. *$\mathcal{H}_{\boldsymbol{\pi}}(\boldsymbol{h}, i, m'') = (-1)^{ic} H$, where H is the $(n - c - i + 1)$-sequence of c-minors of $\operatorname{Jac}(\boldsymbol{h}, i)$ obtained by successively adding the missing row and the missing columns of $\operatorname{Jac}(\boldsymbol{h}, i)$ to μ'';*
3. *if $\chi = (\boldsymbol{h}, m)$ is a chart of (V, S), then for every c-minor m' of $\operatorname{Jac}(\boldsymbol{h})$,*

$$W_{\text{chart}}(\chi, m', m'') = W_{\text{chart}}(\chi, m', (-1)^{i(c-1)}\mu'') = \left(mm'm'', (\boldsymbol{h}, (-1)^{ic} H)\right),$$

with H as above.

Assume, in addition, that V is d-equidimensional, with $d = n - c$. Let $\boldsymbol{\chi} = (\chi_j)_{1\leq j\leq s}$ be an atlas of (V, S), with $\chi_j = (\boldsymbol{h}_j, m_j)$, and let c be the common cardinality of the $\boldsymbol{h}_j$'s. Then

4. *$W_{\text{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\pi}, i)$ is the sequence of all those $W_{\text{chart}}(\chi_j, m', (-1)^{i(c-1)}\mu'')$, for $j \in \{1, \dots, s\}$ and for m', μ'' respectively a c-minor of $\operatorname{Jac}(\boldsymbol{h}_j)$ and a $(c - 1)$-minor of $\operatorname{Jac}(\boldsymbol{h}_j, i)$ for which $\mathcal{O}(m_j m' \mu'') \cap W(\boldsymbol{\pi}_i, V) - S$ is not empty.*

Proof. According to Lemma 7.2.1, up to the sign $(-1)^{i(c-1)}$, the $(c - 1)$-minors of $\operatorname{Jac}(\boldsymbol{h}, i)$ are exactly the $(i + c - 1)$-minors of $\operatorname{Jac}(\boldsymbol{h}, \boldsymbol{\pi}_i)$ containing the identity matrix $I_i = \operatorname{Jac}(\boldsymbol{\pi}_i)$, since

$$\operatorname{Jac}_{x_1,\dots,x_n}(\boldsymbol{h}, \boldsymbol{\pi}_i) = \begin{bmatrix} \operatorname{Jac}_{x_1,\dots,x_i}(\boldsymbol{h}) & \operatorname{Jac}_{x_{i+1},\dots,x_n}(\boldsymbol{h}) \\ I_i & \boldsymbol{O} \end{bmatrix}.$$

Since m'' contains the rows of $\operatorname{Jac}(\boldsymbol{\pi}_i) = [I_i \ \ \boldsymbol{O}]$, either it actually contains I_i or it is zero, as a zero row appears. We assume the first case; then, by the discussion above, $\mu'' = (-1)^{i(c-1)} m''$ is the determinant of a $(c - 1)$-submatrix M of $\operatorname{Jac}(\boldsymbol{h}, i) = \operatorname{Jac}_{x_{i+1},\dots,x_n}(\boldsymbol{h})$.

The row and columns of $\mathrm{Jac}(\boldsymbol{h}, i)$ that are not in M have respective indices $1 \leq k \leq c$ and $1 \leq \ell_1 \leq \ldots \leq \ell_{n-i-c+1} \leq n$. Since m'' contains I_i, the rows and columns of $\mathrm{Jac}(\boldsymbol{h}, \boldsymbol{\pi}_i)$ that are not in m'' have respective indices $1 \leq k' \leq c$ and $i+1 \leq \ell'_1 \leq \ldots \leq \ell'_{n-c-i+1} \leq n$. Then, according to Lemma 7.2.1, for all $1 \leq j \leq n-c-i+1$,

$$k = k' \quad \text{and} \quad \ell_j = \ell'_j - i.$$

Hence, by Lemma 7.2.1, the $(c+i)$-minors obtained by adding the missing row and the missing columns of $\mathrm{Jac}(\boldsymbol{h}, \boldsymbol{\pi}_i)$ to the submatrix used to define m'' are exactly the c-minors of $\mathrm{Jac}(\boldsymbol{h}, i)$ obtained by adding the missing row and the missing columns of $\mathrm{Jac}(\boldsymbol{h}, i)$ to μ'', up to a factor $(-1)^{ic}$. This gives the second statement. The third statement is then nothing but the definition of $W_{\mathrm{chart}}(\chi, m, m'')$.

of

Finally, consider an atlas $\boldsymbol{\chi}$ of (V, S). By Lemma 7.2.1, for $j \in \{1, \ldots, s\}$, all $(c-1)$-minors μ'' of $\mathrm{Jac}(\boldsymbol{h}_j, i)$ are, up to sign, $(c+i-1)$-minors of $\mathrm{Jac}(\boldsymbol{h}_j, \boldsymbol{\pi}_i)$ built with the rows of $\mathrm{Jac}(\boldsymbol{\pi}_i)$. Conversely, let $j \in \{1, \ldots, s\}$, m' be a c-minor of $\mathrm{Jac}(\boldsymbol{h}_j)$ and let m'' be a $(c+i-1)$-minor of $\mathrm{Jac}(\boldsymbol{h}_j, \boldsymbol{\pi}_i)$ containing the rows of $\mathrm{Jac}(\boldsymbol{\pi}_i)$. Then either $m'' = 0$, so that $\mathcal{O}(m'')$ and then $\mathcal{O}(m_j m' m'') \cap W(\boldsymbol{\pi}_i, V) - S$ is empty, or $\mu'' = (-1)^{i(c-1)} m''$ is a $(c-1)$-minor of $\mathrm{Jac}(\boldsymbol{h}_j, i)$. Hence, according to the third item, for $j \in \{1, \ldots, s\}$ and any c-minor m' of $\mathrm{Jac}(\boldsymbol{h}_j)$, the sequences of

- all those $W_{\mathrm{chart}}(\chi_j, m', m'')$ for every $(c+i-1)$-minor m'' of $\mathrm{Jac}(\boldsymbol{h}, \boldsymbol{\pi}_i)$ containing the rows of $\mathrm{Jac}(\boldsymbol{\pi}_i)$, for which $\mathcal{O}(m_j m' m'') \cap W(\boldsymbol{\pi}_i, V) - S$ is not empty, and
- all those $W_{\mathrm{chart}}(\chi_j, m', (-1)^{i(c-1)} m'')$ for every $(c-1)$-minor μ' of $\mathrm{Jac}(\boldsymbol{h}_j, i)$ for which $\mathcal{O}(m_j m' m'') \cap W(\boldsymbol{\pi}_i, V) - S$ is not empty,

are equal to $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\pi}, i)$. □

We can now state the main result of this subsection, which we prove in Section 7.6. This is a generalization of [SS17, Proposition 3.4] which only deals with the case of projections.

Proposition 7.2.13. *Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional and S finite and $\boldsymbol{\chi}$ be an atlas of (V, S). Let $2 \leq \mathfrak{r} \leq d+1$ and $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_{\mathfrak{r}})$ and $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_{\mathfrak{r}})$, and for $1 \leq j \leq \mathfrak{r}$, let $\boldsymbol{\alpha}_j = (\alpha_{j,1}, \ldots, \alpha_{j,n}) \in \mathbf{C}^n$ and*

$$\varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \theta_j(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{j,k} x_k + \xi_j(\boldsymbol{\alpha}_j) \in \mathbf{C}[\boldsymbol{X}].$$

where $\theta_j \in \mathbf{C}[\boldsymbol{X}]$ and $\xi_j \colon \mathbf{C}^n \to \mathbf{C}$ is a polynomial map, with coefficients in $\mathbf{C}$.

There exists a non-empty Zariski open subset $\Omega_{\mathrm{W}}(\boldsymbol{\chi}, V, S, \boldsymbol{\theta}, \boldsymbol{\xi}) \subset \mathbf{C}^{\mathfrak{r}n}$ such that for every $\boldsymbol{\alpha} \in \Omega_{\mathrm{W}}(\boldsymbol{\chi}, V, S, \boldsymbol{\theta}, \boldsymbol{\xi})$, writing $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}), \ldots, \varphi_{\mathfrak{r}}(\boldsymbol{X}, \boldsymbol{\alpha}))$, the following holds. For i in $\{1, \ldots, \mathfrak{r}\}$, either $W_{\boldsymbol{\varphi}}(i, V)$ is empty or

1. *$W_{\boldsymbol{\varphi}}(i, V)$ is an equidimensional algebraic set of dimension $i-1$;*
2. *if $2 \leq i \leq (d+3)/2$, then $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, i)$ is an atlas of $(W_{\boldsymbol{\varphi}}(i, V), S)$ and $\mathrm{sing}(W_{\boldsymbol{\varphi}}(i, V)) \subset S$.*

We end this subsection with a statement we use further for the proof of our main algorithm.

Proposition 7.2.14. *Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set with $d \geq 1$ and $\mathrm{sing}(V)$ finite. Let $\theta \in \mathbf{C}[\boldsymbol{X}]$, and for $i = 1, 2$, let $\boldsymbol{\alpha}_i = (\alpha_{i,1}, \ldots, \alpha_{i,n})$ in $\mathbf{C}^n$ and*

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{1,k} x_k \quad \text{and} \quad \varphi_2(\boldsymbol{X}, \boldsymbol{\alpha}_2) = \sum_{k=1}^{n} \alpha_{2,k} x_k.$$

Then there exists a non-empty Zariski open subset $\Omega_{\mathsf{K}}(V, \theta) \subset \mathbf{C}^{2n}$ such that for every $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2) \in \Omega_{\mathsf{K}}(V, \theta)$, and $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1), \varphi_2(\boldsymbol{X}, \boldsymbol{\alpha}_2))$, the following holds. Either $W_{\boldsymbol{\varphi}}(2, V)$ is empty or

1. *$W_{\boldsymbol{\varphi}}(2, V)$ is 1-equidimensional;*
2. *the sets $W^{\circ}_{\boldsymbol{\varphi}}(1, W_{\boldsymbol{\varphi}}(2, V))$, $W_{\boldsymbol{\varphi}}(1, W_{\boldsymbol{\varphi}}(2, V))$ and $K_{\boldsymbol{\varphi}}(1, W_{\boldsymbol{\varphi}}(2, V))$ are finite.*

Proof. Let $\boldsymbol{\chi}$ be an atlas of $(V, \mathrm{sing}(V))$, as obtained by applying [SS17, Lemma A.13]. Let $\Omega_{\mathsf{K}}(V, \boldsymbol{\theta})$ be the intersection of the non-empty Zariski open subsets $\Omega_{\mathsf{I}}(V, \theta)$ and

$$\Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), (\theta, 0), 0)$$

of $\mathbf{C}^{2n}$, obtained by applying respectively Propositions 7.2.3 and 7.2.13 with $\mathfrak{r} = 2$ (recall that we assume $d \geq 1$). From now on, choose $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2) \in \Omega_{\mathsf{K}}(V, \theta)$ and let $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1), \varphi_2(\boldsymbol{X}, \boldsymbol{\alpha}_2))$. In the following, we denote $W_{\boldsymbol{\varphi}}(2, V)$ by W_2. Suppose W_2 is non-empty, otherwise the result trivially holds.

Since $\boldsymbol{\alpha} \in \Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \boldsymbol{\theta}, 0)$ and $2 \leq (d+3)/2$ for $d \geq 1$, then, by Proposition 7.2.13, W_2 is equidimensional of dimension 1 and $\mathrm{sing}(W_2) \subset \mathrm{sing}(V)$ is finite. Hence $K_W = W_{\boldsymbol{\varphi}}(1, W_2)$ is well defined and the following inclusion holds

$$K_W \subset \bigcup_{z \in \boldsymbol{\varphi}_1(K_W)} W_2 \cap \boldsymbol{\varphi}_1^{-1}(z)$$

By the algebraic version of Sard's lemma from [SS17, Proposition B.2], $\boldsymbol{\varphi}_1(W_{\boldsymbol{\varphi}}(1, W_2))$ is finite. Besides, since $\boldsymbol{\alpha} \in \Omega_{\mathsf{I}}(V, \theta)$, then by Proposition 7.2.3, $\boldsymbol{\varphi}_1^{-1}(z) \cap W_2$ is finite for any $z \in \mathbf{C}$.

Hence, as a set contained in a finite union of finite sets, K_W is finite, and so are $W^{\circ}_{\boldsymbol{\varphi}}(1, W_2)$ and $K_{\boldsymbol{\varphi}}(1, W_2) = K_W \cup \mathrm{sing}(W_2)$. □

7.2.5 Charts and atlases for fibers of polynomial maps

We now study the regularity and dimensions of fibers of some generic polynomial maps over algebraic sets. The construction we introduce below is quite similar to the one in [SS17], but a bit more general.

Definition 7.2.15. Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional, $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ be an atlas of (V, S). Let $1 \leq e \leq \mathfrak{r} \leq n+1$ be integers and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_{\mathfrak{r}}) \subset$

$\mathbf{C}[\boldsymbol{X}]$. For $Q \subset \mathbf{C}^e$ we define $F_{\text{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$ as the sequence of all $\chi_j = (m_j, \boldsymbol{h}_j)$ such that $\mathcal{O}(m_j) \cap F_Q - S_Q$ is not empty, where

$$F_Q = V_{|\boldsymbol{\varphi}_e \in Q} \quad \text{and} \quad S_Q = \big(S \cup W_{\boldsymbol{\varphi}}(e, V)\big)_{|\boldsymbol{\varphi}_e \in Q}.$$

The above definition, is a direct generalization of [SS17, Definition 3.6], where $\boldsymbol{\varphi} = (x_1, \ldots, x_n)$. The main result of this subsection is the following proposition, which we prove in Section 7.7.

Proposition 7.2.16. *Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional and S finite. Let $\boldsymbol{\chi}$ be an atlas of (V, S). Let $2 \leq \mathfrak{r} \leq d+1$ and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_{\mathfrak{r}}) \subset \mathbf{C}[\boldsymbol{X}]$. For $2 \leq j \leq d$, let $\boldsymbol{\alpha}_j = (\alpha_{j,1}, \ldots, \alpha_{j,n}) \in \mathbf{C}^n$ and*

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{1,k} x_k \quad \text{and} \quad \varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \sum_{k=1}^{n} \alpha_{j,k} x_k$$

where $\theta \in \mathbf{C}[\boldsymbol{X}]$.

There exists a non-empty Zariski open subset $\Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, S, \theta) \subset \mathbf{C}^{\mathfrak{r}n}$ such that for every $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{\mathfrak{r}}) \in \Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, S, \theta)$ and writing $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1), \ldots, \varphi_{\mathfrak{r}}(\boldsymbol{X}, \boldsymbol{\alpha}_{\mathfrak{r}}))$, the following holds. Let $0 \leq e \leq d$, $Q \in \mathbf{C}^e$ a finite subset and F_Q and S_Q be as in Definition 7.2.15. Then either F_Q is empty or

1. *S_Q is finite;*
2. *V_Q is an equidimensional algebraic set of dimension $d - e$;*
3. *$F_{\text{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$ is an atlas of (F_Q, S_Q) and $\text{sing}(F_Q) \subset S_Q$.*

7.3 The algorithm

7.3.1 Overall description

Recall that $\boldsymbol{X}$ denotes a sequence of n indeterminates $x_1, \ldots, x_n$. In this chapter, we also consider a family $\boldsymbol{A} = (a_{i,j})_{1 \leq i,j \leq n}$ of n^2 new indeterminates, which stand for generic parameters. For $1 \leq i, j \leq n$, we note $a_i = (a_{i,1}, \ldots, a_{i,n})$, so that $\boldsymbol{A}_{\leq i}$ represents the subfamily $(a_1, \ldots, a_i)$. An element $\boldsymbol{\alpha} \in \mathbf{C}^{in}$ will often be represented as a vector of length i of the form $(\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_i)$, with all $\boldsymbol{\alpha}_j = (\alpha_{j,1}, \ldots, \alpha_{j,n}) \in \mathbf{C}^n$.

Then, as suggested by Propositions 7.2.3, 7.2.13, 7.2.14 and 7.2.16, we will consider polynomials of the form:

$$\phi_i(\boldsymbol{X}, a_i) = \theta_i(\boldsymbol{X}) + \sum_{j=1}^{n} a_{i,j} x_j + \xi_i(a_i) \in \mathbf{R}[\boldsymbol{X}, \boldsymbol{A}]. \tag{7.1}$$

where $1 \leq i \leq n$, $\theta_i \in \mathbf{R}[\boldsymbol{X}]$ and $\xi_i \in \mathbf{R}[\boldsymbol{A}]$. We can choose θ_i so that the polynomial map ϕ_i inherits some useful properties. For instance, taking $\theta_i = x_1^2 + \cdots + x_n^2$, for any $\boldsymbol{\alpha}_i$ in $\mathbf{R}^n$, the polynomial map associated to $\phi_i(\boldsymbol{X}, \boldsymbol{\alpha}_i)$ is proper and bounded from below on $\mathbf{R}^n$.

Hereafter, we describe, on an example, the core idea of the the strategy that guided the design of our algorithm and the choice of data structures.

Example 7.3.1. Consider the algebraic set $V = \boldsymbol{V}(f) \subset \mathbb{C}^4$ defined as the vanishing locus of the polynomial

$$f = \sum_{i=1}^{4} (x_i^3 - x_i) - 1 \in \mathbb{Q}[x_1, x_2, x_3, x_4].$$

We want to compute a roadmap of $(V, \emptyset)$ (or simply V). Following the strategy we designed in the introduction, V must satisfies some regularity properties, that is

(H_1) V is d-equidimensional, $d \geq 2$, and $\mathrm{sing}(V)$ is finite.

The first part of the assumption can be satisfied by computing an equidimensional decomposition of V that is done within the complexity bounds considered in this work (see e.g. [Lec03] for the best-known complexity bound for a probabilistic algorithm. Besides, the condition $d \geq 2$ is not restrictive as the case $d = 1$ is trivial for roadmap computations. The smoothness assumption is more restrictive. Indeed, it can be satisfied using deformation techniques, such as done in [BR14, BRSS14], but these steps would not fit, as such, in our complexity bounds.

Let us check that, in our example, V satisfies H_1. We will describe further a subroutine SingularPoints, to compute $\mathrm{sing}(V)$ as long as this holds.

Checking (H_1). As an hypersurface, V is irreducible, and then equidimensional, of dimension 3. The partial derivatives of f, $\frac{\partial f}{\partial x_i} = 3x_i^2 - 1$, for $1 \leq i \leq 4$, do not simultaneously vanish on V. Hence, $\mathrm{sing}(V) = \emptyset$, and V satisfies assumption (H_1).

We want to choose a sequence of polynomial $\boldsymbol{\varphi} = (\boldsymbol{\varphi}_1, \ldots, \boldsymbol{\varphi}_n)$ in $\mathbf{Q}[\boldsymbol{X}]$ such that the following holds:

(H_2) the restriction of $\boldsymbol{\varphi}_1$ to $V \cap \mathbb{R}^n$ is proper and bounded from below;

(H_3) $W_2 = W_{\boldsymbol{\varphi}}(2, V)$ is 1 equidimensional, and smooth outside $\mathrm{sing}(V)$;

(H_4) for any $z \in \mathbf{C}$, $V_{|\boldsymbol{\varphi}_1 = z}$ is $(d-1)$-equidimensional;

(H_5) $K_{\boldsymbol{\varphi}}(1, W_2)$ is finite.

In addition, let $K = K_{\boldsymbol{\varphi}}(1, W_2) \cup \mathrm{sing}(V)$ and $F = V \cap \boldsymbol{\varphi}_1^{-1}(\boldsymbol{\varphi}_1(K))$. We require that

(H_6) $\mathcal{P}_W = F \cap W_2$ is finite.

Then, under the above assumptions if $\mathcal{R}_F$ is a roadmap of $(F, \mathcal{P}_W)$, then $W_2 \cup \mathcal{R}_F$ is a roadmap of V. This statement, is a consequence of both [SS11, Proposition 2] and Theorem 6.1.1, and will be properly stated and proved in Proposition 7.3.10. This splits the problem of computing a roadmap of V into the computation of representations of W_2, F and $\mathcal{P}_W$, and a roadmap of $(F, \mathcal{P}_W)$. Since $F \cap \mathbb{R}^n$ is bounded, by assumption (H_2), the latter computation can be done using the algorithm of [SS17].

We describe this process more precisely with our example. Each step consisting in checking the assumptions, and computing the associated objects.

Checking $(\mathsf{H}_{2/3})$. Set first $\varphi = \left(\sum_{i=1}^4 x_i^2,\ x_2,\ x_3,\ x_4\right)$. The restriction of φ_1 to $V \cap \mathbf{R}^4$ is proper and non-negative. We can then compute a representation of $W_2 = W_\varphi(2, V)$, before computing one for its singular locus $\mathrm{sing}(W_2)$. However, the latter singular set is not empty, while $\mathrm{sing}(V)$ is. This contradicts the assumptions needed in Theorem 6.1.1 and the strategy for computing a roadmap of V designed in the introduction might fail.

Following Propositions 7.2.3, 7.2.13, 7.2.14 and 7.2.16 from the preliminaries, we propose the following. To prevent these regularity failures, and to satisfy all assumptions of Theorem 6.1.1, while keeping the properties of φ, we add to φ_1 a generic linear form, e.g. $x_1 - x_4$.

Hence, consider now the finite sequence φ of polynomials maps

$$\varphi = \left(\sum_{i=1}^4 x_i^2 + x_1 - x_4,\ x_2,\ x_3,\ x_4\right),$$

whose restriction to $\mathbf{R}^4$ is still a proper and bounded below map, by construction. If the linear form we added has been sufficiently randomly chosen, Proposition 7.2.13 claims that W_2 satisfies assumption (H_3).

Using Gröbner basis computations on a determinantal ideal defining W_2, we computes a representation of W_2, and next $\mathrm{sing}(W_2)$, that turns out to be empty, as requested. More generally, computing the two previous sets efficiently is the purpose of the algorithm SolvePolar, presented in Lemma 7.3.5.

Checking (H_4). By Proposition 7.2.16, this assumption holds if we have added to φ a linear form that is generic enough. Using the Jacobian criterion, we can check that in our case, for any $z \in \mathbb{C}$, the fiber $F_z = V \cap \varphi_1^{-1}(z)$ is an equidimensional algebraic set of dimension 2 (if it is not empty). Moreover the singular locus of F_z is contained in the finite set $W_\varphi(1, V)$. Computing the latter set is tackled by the subroutine Crit, presented in Lemma 7.3.4.

Checking (H_5). We also need to check the finiteness and compute the set $K_\varphi(1, W_2)$. If φ is generic enough, the finiteness is ensured by Proposition 7.2.14; computing this set is the purpose of the algorithm CritPolar, presented in Lemma 7.3.7. In our case, there are finitely many (more precisely 129) such points, and 23 of them are real.

Checking (H_6). We need to compute the set $K = K_\varphi(1, W_2) \cup \mathrm{sing}(V)$. As the two members of the unions have been computed by the algorithms CritPolar and SingularPoints, respectively, one can compute this union using the procedure Union from [SS17, Lemma J.3] (also presented in the next subsection).

Then, for φ generic enough, Proposition 7.2.3 ensures that the last assumption holds. The computation of $\mathcal{P}_W$ boils down to computing finitely many fibers on the restriction of φ_1 to W_2. This is the purpose of the algorithm FiberPolar, presented in Lemma 7.3.7.

At this point, we have computed representations of W_2 and $\mathcal{P}_W$, and ensured that all assumptions of Theorem 6.1.1 are satisfied. Hence, one only need to compute a roadmap

of $(F, \mathcal{P}_W)$. This is the purpose of the algorithm RoadmapBounded, presented in Proposition 7.3.8.

7.3.2 Subroutines

Our algorithm (Algorithm 2) makes use of several subroutines which allow us to manipulate zero-dimensional and one-dimensional parametrizations, polar varieties and fibers of polynomial maps in order to make effective Theorem 6.1.1.

As a reminder, in this chapter, we manipulate subroutines that involve selecting suitable parameters in $\mathbf{Q}^i$, for some $i \geq 1$. These algorithms are probabilistic, which means that there exists a non-zero polynomial Δ, such that for a randomly chosen parameter $\boldsymbol{\lambda} \in \mathbf{Q}^i$, success is achieved if $\Delta(\boldsymbol{\lambda}) \neq 0$. However, it is important to note that these algorithms are considered Monte Carlo, as their output's correctness cannot be guaranteed within a reasonable complexity. In certain cases, where we can identify errors, we require our procedures to output fail. However, the absence of this output does not guarantee correctness.

Let $1 \leq c \leq n$, and $\boldsymbol{f} = (f_1, \ldots, f_c)$ be a sequence of polynomials in $\mathbf{R}[\boldsymbol{X}]$. We say that $\boldsymbol{f}$ satisfies assumption (A) if

(A) : $\boldsymbol{f}$ is a reduced regular sequence, with $d = n - c \geq 2$, and $\mathrm{sing}(\boldsymbol{V}(\boldsymbol{f}))$ is finite.

In particular, the zero-set of $\boldsymbol{f}$ is then either empty or d-equidimensional.

7.3.2.a. Basic subroutines

The first two subroutines we use are described in [SS17] and are used to compute $\mathrm{sing}(V(\boldsymbol{f}))$ (on input a straight-line program evaluating $\boldsymbol{f}$) and to compute a rational parametrization encoding the union of zero-dimensional sets or the union of algebraic curves. They are both Monte Carlo algorithms, in the sense described above, and can output fail in case errors have been detected during the execution. However, in case of success, the following holds.

- SingularPoints, described in [SS17, Section J.5.4], takes as input a straight-line program Γ that evaluates polynomials $\boldsymbol{f} \in \mathbf{C}[\boldsymbol{X}]$ satisfying assumption (A) and outputs a zero-dimensional parametrization describing $\mathrm{sing}(\boldsymbol{V}(\boldsymbol{f}))$.
- Union, described in [SS17, Lemma J.3] (resp. [SS17, Lemma J.8]), takes as input two zero-dimensional (resp. one-dimensional) parametrizations $\mathscr{P}_1$ and $\mathscr{P}_2$ and outputs a zero-dimensional (resp. one-dimensional) parametrization encoding $\mathsf{Z}(\mathscr{P}_1) \cup \mathsf{Z}(\mathscr{P}_2)$.

We now describe basic subroutines performing elementary operations on straight-line program and zero-dimensional parametrizations. The first one allows to generate a generic polynomial with a prescribed structure.

Lemma 7.3.2. *Let $1 \leq i \leq n$ and $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_i) \in \mathbf{C}^{in}$. Then there exists an algorithm PhiGen which takes as input $\boldsymbol{\alpha}$ and returns a straight-line program Γ^{φ} of length $2(i+1)n - i$ computing in $\mathbf{Q}[\boldsymbol{X}]$:*

$$\varphi_1 = \sum_{k=1}^{n} x_k^2 + \alpha_{1,k} x_k \quad \text{and} \quad \varphi_j = \sum_{k=1}^{n} \alpha_{j,k} x_k \quad \text{for } 2 \leq j \leq i.$$

Proof. For $1 \leq j \leq i$, the straight-line program

$$\Gamma_j = \Big((\times, \alpha_{j,1}, -n+1), \ldots, (\times, \alpha_{j,n}, 0), (+, n, 1), \ldots, (+, 2n-1, n-1)\Big)$$

has length $2n-1$ and computes $\sum_{k=1}^{n} \alpha_{j,k} x_k$ in $\mathbf{Q}[\boldsymbol{X}]$. Similarly, the straight-line program

$$\Gamma = \Big((\times -n+1, -n+1), \ldots, (\times, 0, 0), (+, n, 1), \ldots, (+, 2n-1, n-1)\Big),$$

has length $2n-1$, and computes $\sum_{k=1}^{n} x_k^2$ in $\mathbf{Q}[\boldsymbol{X}]$. Hence, there exists a straight-line program Γ'_1, of length $4n-1$, computing φ_1 as defined in the statement. Then, up to translation of indices, the straight-line program $\Gamma^{\boldsymbol{\varphi}} = (\Gamma'_1, \Gamma_2, \ldots, \Gamma_i)$, has length $2(i+1)n - i$, that computes $\varphi_1, \ldots, \varphi_i$, as defined in the statement, in $\mathbf{Q}[\boldsymbol{X}]$. □

Hereafter, we present a procedure computing the image of a zero-dimensional parametrization by a polynomial map, given as a straight-line program, generalizing the subroutine Projection from [SS17, Lemma J.5]. The proof of the next lemma is given in Subsection 7.4.1.

Lemma 7.3.3. *Let $\mathscr{P}$ be a zero-dimensional parametrization of degree κ such that $\mathsf{Z}(\mathscr{P}) \subset \mathbf{C}^n$ and let $\Gamma^{\boldsymbol{\varphi}}$ be a straight-line program of length E' computing polynomials $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_i)$. There exists a Monte Carlo algorithm Image which, on input $\Gamma^{\boldsymbol{\varphi}}$, $\mathscr{P}$ and $j \in \{1, \ldots, i\}$, outputs either fail or a zero-dimensional parametrization $\mathscr{Q}$, of degree at most κ, using*

$$\widetilde{O}\left((n^2\kappa + E')\kappa\right)$$

operations in $\mathbf{Q}$. In case of success, $\mathsf{Z}(\mathscr{Q}) = \boldsymbol{\varphi}_j(\mathsf{Z}(\mathscr{P}))$.

7.3.2.b. Subroutines for polar varieties

The next subroutines are used to compute generalized polar varieties and quantities related to them. The proof of all statements below can be found in Subsection 7.4.4. In this subsection, we fix $1 \leq c \leq n-1$ and we refer to the following objects:

- sequences of polynomials $\boldsymbol{g} = (g_1, \ldots, g_c)$ and $\boldsymbol{\varphi} = (\varphi_1, \varphi_2)$ in $\mathbf{Q}[x_1, \ldots, x_n]$, of degrees bounded by D, such that $\boldsymbol{g}$ satisfies assumption (A); we note $d = n - c$;
- straight-line programs Γ and $\Gamma^{\boldsymbol{\varphi}}$, of respective lengths E and E', computing respectively $\boldsymbol{g}$ and $\boldsymbol{\varphi}$;
- zero-dimensional parametrizations $\mathscr{S}$ and $\mathscr{Q}''$, of respective degrees σ and κ'', describing finite sets $S \subset \mathbf{C}^n$ and $Q'' \subset \mathbf{C}$, such that $\mathrm{sing}(\boldsymbol{V}(\boldsymbol{g})) \subset S$;
- an atlas $\boldsymbol{\chi}$ of $(\boldsymbol{V}(\boldsymbol{g}), S)$, given by [SS17, Lemma A.13], as S is finite and contains $\mathrm{sing}(\boldsymbol{V}(\boldsymbol{g}))$.

We start with the subroutine Crit, which is used for computing critical and singular points of some polynomial map, again under some regularity assumption. These critical points are nothing but zero-dimensional polar varieties.

Lemma 7.3.4. *Assume that $K_{\boldsymbol{\varphi}}(1, \boldsymbol{V}(\boldsymbol{g}))$ is finite. There exists a Monte Carlo algorithm Crit which takes as input Γ, $\Gamma^{\boldsymbol{\varphi}}$ and $\mathscr{S}$ and which outputs either fail or a zero-dimensional parametrization $\mathscr{S}_F$, with coefficients in $\mathbf{Q}$, of degree at most*

$$\binom{n+1}{d} D^{c+2}(D-1)^d + \sigma$$

such that, in case of success, $\mathsf{Z}(\mathscr{S}_F) = K_{\boldsymbol{\varphi}}(1, \boldsymbol{V}(\boldsymbol{g})) \cup S$, and using at most

$$\widetilde{O}\left(E''(n+2)^{4d+8} D^{2n+3}(D-1)^{2d} + n\sigma^2\right)$$

operations in $\mathbf{Q}$, where $E'' = E + E'$.

We now tackle higher dimensional cases, with the subroutine SolvePolar which, under some assumptions, computes one-dimensional parametrization encoding one-dimensional generalized polar varieties.

Lemma 7.3.5. *Let $W = W_{\boldsymbol{\varphi}}(2, \boldsymbol{V}(\boldsymbol{g}))$ and assume that one of the following holds*

- *W is empty or*
- *W is 1-equidimensional, with $\mathrm{sing}(W) \subset S$, and $W_{\mathrm{atlas}}(\boldsymbol{\chi}, \boldsymbol{V}(\boldsymbol{g}), S, \boldsymbol{\varphi}, 2)$ is an atlas of (W, S)*

Then, there exists a Monte Carlo probabilistic algorithm SolvePolar which takes as input Γ, $\Gamma^{\boldsymbol{\varphi}}$ and $\mathscr{S}$ and which outputs either fail or a one-dimensional parametrization $\mathscr{W}_2$, with coefficients in $\mathbf{Q}$, of degree at most

$$\delta = (n+c+4) D^{c+2}(D-1)^d (c+2)^d.$$

such that, in case of success, $\mathsf{Z}(\mathscr{W}_2) = W$. It uses at most

$$\widetilde{O}\left((n+c)^3(E'' + (n+c)^3) D\delta^3 + (n+c)\delta\sigma^2\right)$$

operations in $\mathbf{Q}$, where $E'' = E + E'$.

The subroutine CritPolar is devoted to compute critical points of the restriction of some polynomial map to a generalized polar variety of dimension at most one. It generalizes the subroutine W_1 from [SS17, Proposition 6.4].

Lemma 7.3.6. *Let $W = W_{\boldsymbol{\varphi}}(2, \boldsymbol{V}(\boldsymbol{g}))$ and assume that either W is empty, or*

- *W is 1-equidimensional, with $\mathrm{sing}(W) \subset S$, and $W_{\mathrm{atlas}}(\boldsymbol{\chi}, \boldsymbol{V}(\boldsymbol{g}), S, \boldsymbol{\varphi}, 2)$ is an atlas of (W, S),*
- *and $W_{\boldsymbol{\varphi}}(1, W)$ is finite.*

There exists a Monte Carlo algorithm CritPolar which takes as input Γ, $\Gamma^{\boldsymbol{\varphi}}$ and $\mathscr{S}$ and which outputs either fail or a zero-dimensional parametrization $\mathscr{K}$, with coefficients in $\mathbf{Q}$, such that $\mathsf{Z}(\mathscr{K}) = W_{\boldsymbol{\varphi}}(1, W) \cup S$ using at most

$$\widetilde{O}\left((n+c)^{12} E'' D^3 \delta^2 + (n+c)\sigma^2\right)$$

operations in $\mathbf{Q}$*, where* $E'' = E + E'$*, and* $\delta = (n+c+4)D^{c+2}(D-1)^d(c+2)^d$*. Moreover* $\mathscr{K}$ *has degree at most* $\delta(n+c+4)D + \sigma$*.*

Finally, we consider the subroutine FiberPolar which, given polynomials defining a generalized polar variety of dimension at most one, a polynomial map and some real algebraic numbers, computes the fibers of the polynomial map over the polar variety.

Lemma 7.3.7. *Let* $W = W_{\boldsymbol{\varphi}}(2, \boldsymbol{V}(\boldsymbol{g}))$ *and assume that either* W *is empty, or*

- W *is 1-equidimensional, with* $\mathrm{sing}(W) \subset S$*, and* $W_{\mathrm{atlas}}(\boldsymbol{\chi}, \boldsymbol{V}(\boldsymbol{g}), S, \boldsymbol{\varphi}, 2)$ *is an atlas of* (W, S)*;*
- $W \cap \boldsymbol{\varphi}_1^{-1}(Q'')$ *is finite;*

There exists a Monte Carlo algorithm FiberPolar which takes as input Γ*,* $\Gamma^{\boldsymbol{\varphi}}$*,* $\mathscr{S}$ *and* $\mathscr{Q}''$ *and which outputs either fail or a zero-dimensional parametrization* $\mathscr{Q}$*, with coefficients in* $\mathbf{Q}$*, such that* $\mathsf{Z}(\mathscr{Q}) = \big(W \cap \boldsymbol{\varphi}_1^{-1}(Q'')\big) \cup S$*, using at most*

$$\widetilde{O}\left((n+c)^4\big(E'' + (n+c)^2\big)D\kappa''^2\delta^2 + (n+c)\sigma^2\right)$$

operations in $\mathbf{Q}$*, where* $E'' = E + E'$*, and* $\delta = (n+c+4)D^{c+2}(D-1)^d(c+2)^d$*. Moreover,* $\mathscr{Q}$ *has degree at most* $\kappa''\delta + \sigma$*.*

7.3.2.c. Subroutines for computing roadmaps in the bounded case

As seen above, in Example 7.3.1, we are ultimately led to compute a roadmap for a bounded real algebraic set. Moreover this set is given as fibers over finitely many algebraic points of the restriction of a polynomial map to an bigger algebraic set. To do so, we come back to the case of projections, where $\boldsymbol{\varphi} = \boldsymbol{\pi}$, before calling the algorithm RoadmapRecLagrange from [SS17]. The description and the complexity analysis of this procedure are given in Subsection 7.4.5. The subtlety comes from the fact that, in [SS17], the correction and complexity estimate of RoadmapRecLagrange are only given in the particular case when the input describes an algebraic set that is not fiber of any polynomial. More precisely, we prove in Subsection 7.4.5 the following result.

Proposition 7.3.8. *Let* Γ *and* $\Gamma^{\boldsymbol{\varphi}}$ *be straight-line programs, of respective length* E *and* E'*, computing respectively polynomials* $\boldsymbol{g} = (g_1, \ldots, g_c)$ *and* $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n)$ *in* $\mathbf{Q}[x_1, \ldots, x_n]$*, of degrees bounded by* D*. Assume that* $\boldsymbol{g}$ *satisfies* (A)*. Let* $\mathscr{Q}$ *and* $\mathscr{S}_Q$ *be zero-dimensional parametrizations of respective degrees* κ *and* σ *that encode finite sets* $Q \subset \mathbf{C}^e$ *(for some* $0 < e \leq n$*) and* $S_Q \subset \mathbf{C}^n$*, respectively. Let* $V = \boldsymbol{V}(\boldsymbol{g})$ *and* $F_Q = V_{|\boldsymbol{\varphi}_e \in Q}$*, and assume that*

- F_Q *is equidimensional of dimension* $d - e$*, where* $d = n - c$*;*
- $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, \boldsymbol{\varphi})$ *is an atlas of* (F_Q, S_Q)*, and* $\mathrm{sing}(F_Q) \subset S_Q$*;*
- *the real algebraic set* $F_Q \cap \mathbf{R}^n$ *is bounded.*

Consider additionally a zero-dimensional parametrization $\mathscr{P}$ *of degree* μ *encoding a finite subset* $\mathcal{P}$ *of* F_Q*, which contains* S_Q*. Assume that* $\sigma \leq ((n+e)D)^{n+e}$*.*

There exists a probabilistic algorithm RoadmapBounded which takes as input the pair $((\Gamma, \Gamma^{\varphi}, \mathscr{Q}, \mathscr{S}), \mathscr{P})$ *and which, in case of success, outputs a roadmap of* $(F_Q, \mathcal{P})$*, of degree*

$$\widetilde{O}\left((\mu+\kappa)16^{3d_F}(n_F\log_2(n_F))^{2(2d_F+12\log_2(d_F))(\log_2(d_F)+5)}D^{(2n_F+1)(\log_2(d_F)+3)}\right),$$

where $n_F = n + e$ *and* $d_F = d - e$*, and using*
$\widetilde{O}\left((\mu+\kappa)^3 16^{9d_F}(E+E'+e)(n_F\log_2(n_F))^{6(2d_F+12\log_2(d_F))(\log_2(d_F)+6)}D^{3(2n_F+1)(\log_2(d_F)+4)}\right)$
arithmetic operations in $\mathbf{Q}$*.*

7.3.3 Description of the main algorithm

Now, we describe hereafter the main algorithm that is expected to compute roadmaps of smooth unbounded real algebraic sets. In addition to the subroutines mentioned above, we define Random as a procedure that takes as input a set X and returns a random element in X. Together with PhiGen, it allows to generate "generic enough" polynomial maps so that the results of the previous section do apply (Propositions 7.2.3, 7.2.13, 7.2.14 and 7.2.16).

Algorithm 2 Roadmap algorithm for smooth unbounded real algebraic sets.

Input: ▷ a straight-line program Γ that evaluates polynomials $\boldsymbol{f} = (f_1, \ldots, f_c) \subset \mathbf{Q}[\boldsymbol{X}]$, satisfying assumption (A); we note $V = \boldsymbol{V}(\boldsymbol{f})$;
▷ a zero-dimensional parametrization $\mathscr{P}_0$ encoding a finite set $\mathcal{P}_0 \subset V$.

Output: a one-dimensional parametrization $\mathscr{R}$ encoding a roadmap of $(V, \mathcal{P}_0)$.

1: $\mathscr{S} \leftarrow \mathsf{SingularPoints}(\Gamma)$; // $\mathsf{Z}(\mathscr{S}) = \mathrm{sing}(V)$;
2: $\mathscr{P} \leftarrow \mathsf{Union}(\mathscr{P}_0, \mathscr{S})$; // $\mathcal{P} := \mathsf{Z}(\mathscr{P}) = \mathcal{P}_0 \cup \mathrm{sing}(V)$
3: $\boldsymbol{\alpha} \leftarrow \mathsf{Random}(\mathbf{Q}^{2n})$;
4: $\Gamma^{\varphi} \leftarrow \mathsf{PhiGen}(\boldsymbol{\alpha})$; // Γ^{φ} computes $\varphi = \left(||\boldsymbol{X}||^2 + \langle\boldsymbol{\alpha}_1, \boldsymbol{X}\rangle, \langle\boldsymbol{\alpha}_2, \boldsymbol{X}\rangle\right)$
5: $\mathscr{W}_2 \leftarrow \mathsf{SolvePolar}(\Gamma, \Gamma^{\varphi}, \mathscr{S})$; // $W_2 := \mathsf{Z}(\mathscr{W}_2) = W_{\varphi}(2, V)$;
6: $\mathscr{K} \leftarrow \mathsf{CritPolar}(\Gamma, \Gamma^{\varphi}, \mathscr{P})$; // $K := \mathsf{Z}(\mathscr{K}) = W_{\varphi}(1, W_2) \cup \mathcal{P}_0 \cup \mathrm{sing}(V)$;
7: $\mathscr{Q} \leftarrow \mathsf{Image}(\Gamma^{\varphi}, 1, \mathscr{K})$; // $Q := \mathsf{Z}(\mathscr{Q}) = \varphi_1(K)$;
8: $\mathscr{P}_F \leftarrow \mathsf{FiberPolar}(\Gamma, \Gamma^{\varphi}, \mathscr{Q}, \mathscr{P})$; // $\mathsf{Z}(\mathscr{P}_F) = [W_2 \cup \mathcal{P}_0 \cup \mathrm{sing}(V)] \cap \varphi_1^{-1}(Q)$;
9: $\mathscr{S}_F \leftarrow \mathsf{Crit}(\Gamma, \Gamma^{\varphi}, \mathscr{S})$ // $\mathsf{Z}(\mathscr{S}_F) = K_{\varphi}(1, V)$;
10: $\mathscr{R}_F \leftarrow \mathsf{RoadmapBounded}\left((\Gamma, \Gamma^{\varphi}, \mathscr{Q}, \mathscr{S}_F), \mathscr{P}_F\right)$ // $\mathsf{Z}(\mathscr{R}_F)$ is a roadmap of $\left(V \cap \varphi_1^{-1}(Q), \mathsf{Z}(\mathscr{P}_F)\right)$;
11: return $\mathsf{Union}(\mathscr{W}_2, \mathscr{R}_F)$ // $W_2 \cup \mathsf{Z}(\mathscr{R}_F)$ is a roadmap of $(V, \mathcal{P}_0)$.

7.3.4 Correctness

This subsection is devoted to the proof of the following theorem, which directly implies Theorem 7.1.1.

Theorem 7.3.9. *Let* Γ *be a straight-line program of length* E *evaluating polynomials* $\boldsymbol{f} = (f_1, \ldots, f_c)$ *of degrees bounded by* D*, satisfying* (A)*. Let* $\mathscr{P}_0$ *be a zero-dimensional parametrization of degree* μ *encoding a finite subset of* $\boldsymbol{V}(\boldsymbol{f}) \subset \mathbf{C}^n$*. Then there exists a non-empty Zariski open* $\Omega \subset \mathbf{C}^{2n}$ *such that the following holds.*

Let $\boldsymbol{\alpha} \in \mathbf{Q}^{2n}$ the vector randomly chosen in the execution of Algorithm 2, then if $\boldsymbol{\alpha} \in \Omega$, and if the calls to the subroutines

SingularPoints, Union, SolvePolar, CritPolar, Image, FiberPolar, Crit and RoadmapBounded

are successful then, on inputs $\Gamma, \Gamma^{\boldsymbol{\alpha}}$ and $\mathscr{P}_0$, Algorithm 2 either returns a one-dimensional parametrization of degree

$$\widetilde{O}\left(\mu 16^{3d}(n\log_2(n))^{2(2d-2+12\log_2(d-1))(\log_2(d-1)+6)}D^{(2n+4)(\log_2(d-1)+4)}\right)$$

using

$$\widetilde{O}\left(\mu^3 16^{9d}E(n\log_2(n))^{6(2d+12\log_2(d-1))(\log_2(d-1)+7)}D^{3(2n+4)(\log_2(d-1)+5)}\right)$$

arithmetic operations in $\mathbf{Q}$, with $d = n - c$.

In case of success, the output of Algorithm 2 describes a roadmap of $(\boldsymbol{V}(\boldsymbol{f}), \mathsf{Z}(\mathscr{P}_0))$.

The correctness of Algorithm 2 relies mainly on the conjunction of Theorem 6.1.1 and [SS11, Proposition 2], that form the following statement, with slightly stronger assumptions, which hold in our context.

Proposition 7.3.10. *Let $V \subset \mathbf{C}^n$ be a $\mathbf{Q}$-algebraic set of dimension d and let $\mathcal{P}_0$ be a finite subset of V. Let $\varphi = (\varphi_1, \varphi_2) \subset \mathbf{R}[\boldsymbol{X}]$ and $W = W_{\boldsymbol{\varphi}}(2, V)$. Suppose that the following holds:*

(H_1) *V is equidimensional and $\mathrm{sing}(V)$ is finite;*

(H_2) *the restriction of $\boldsymbol{\varphi}_1$ to $\boldsymbol{V} \cap \mathbf{R}^n$ is a proper map bounded from below;*

(H_3) *W is either empty or 1-equidimensional and smooth outside $\mathrm{sing}(V)$;*

(H_4) *for any $\boldsymbol{y} \in \mathbf{C}^2$, the set $V \cap \boldsymbol{\varphi}_1^{-1}(\boldsymbol{y})$ is either empty or $(d-1)$-equidimensional;*

(H_5) *$K_{\boldsymbol{\varphi}}(1, W)$ is finite.*

Let further $K = K_{\boldsymbol{\varphi}}(1, W) \cup \mathcal{P}_0 \cup \mathrm{sing}(V)$ and $F = V \cap \boldsymbol{\varphi}_1^{-1}(\boldsymbol{\varphi}_1(K))$. Assume in addition that

(H_6) *$\mathcal{P}_W = F \cap W$ is finite.*

If $\mathcal{R}_F$ is a roadmap of $(F, \mathcal{P}_0 \cup \mathcal{P}_W)$, then $W \cup \mathcal{R}_F$ is a roadmap of $(V, \mathcal{P}_0)$.

Proof. Remark first that the so-called assumptions A, P and B from the connectivity result from of Theorem 6.1.1 are direct consequences of assumptions H_1 to H_4. Besides, $W_{\boldsymbol{\varphi}}(1, V) \subset K_{\boldsymbol{\varphi}}(1, W)$ and $\mathrm{sing}(W) \subset \mathrm{sing}(V)$, by [SS17, Lemma A.5.] together with assumption H_3. Hence, one can write

$$K = W_{\boldsymbol{\varphi}}(1, V) \cup S \cup \mathrm{sing}(V).$$

where $S = W_{\boldsymbol{\varphi}}(1, W) \cup \mathcal{P}_0$. By H_5, S is a finite subset of V, that intersects every semi-algebraically connected component of $W_{\boldsymbol{\varphi}}(1, W) \cap \mathbf{R}^n$ by definition. Hence, S satisfies assumption C of of Theorem 6.1.1. By application of this latter result, $W \cup F$ has then a non-empty and semi-algebraically connected intersection with every semi-algebraically connected component of $V \cap \mathbf{R}^n$ and it contains $\mathcal{P}_0$ by construction.

Moreover, by H_6, $F \cap W$ is finite, so that by [SS11, Proposition 2], the following holds. If $\mathcal{R}_W$ and $\mathcal{R}_F$ are roadmaps of respectively $(W, \mathcal{P}_0 \cup \mathcal{P}_W)$ and $(F, \mathcal{P}_0 \cup \mathcal{P}_W)$, then $\mathcal{R}_W \cup \mathcal{R}_F$ is a roadmap of $(V, \mathcal{P}_0)$. But remark that W is a roadmap of $(W, \mathcal{P}_W)$ since W has dimension one. Besides, [SS11, Proposition 2] can be slightly generalized as only one of $\mathcal{R}_W$ or $\mathcal{R}_F$ must contain $\mathcal{P}_0$. Hence taking $\mathcal{R}_W = W$, allows to conclude. □

Proof of Theorem 7.3.9. Let Γ and $\mathscr{P}_0$ be the inputs of the Algorithm 2 and assume that Γ evaluates polynomials $\boldsymbol{f} = (f_1, \ldots, f_c)$ satisfying assumption A. Let $V = \boldsymbol{V}(\boldsymbol{f})$ and $\mathcal{P}_0 = \mathsf{Z}(\mathscr{P}_0)$.

Recall that we assume all calls to the subroutines SingularPoints, Union, SolvePolar, CritPolar, Image, FiberPolar, Crit and RoadmapBounded do succeed.

Steps 1-2. According to [SS17, Proposition J.35], the procedure SingularPoints outputs a zero-dimensional parametrization $\mathscr{S}$ describing $\mathrm{sing}(V)$ using $\widetilde{O}(ED^{4n+1})$ operations in $\mathbf{Q}$. By [SS17, Proposition I.1] (or [SS18, Proposition 3]) $\mathscr{S}$ has degree at most

$$\sigma_{\mathscr{S}} = \binom{n-1}{c-1} D^c (D-1)^d = \binom{n-1}{d} D^c (D-1)^d \in O(n^d D^n)$$

Then, according to [SS17, Lemma J.3] and our assumptions, the procedure Union outputs a zero-dimensional parametrization $\mathscr{P}$ of degree at most

$$\delta_{\mathscr{P}} = \mu + \sigma_{\mathscr{S}} \;=\; O(\mu + n^d D^n), \quad \text{using} \quad \widetilde{O}(n(\mu^2 + n^{2d} D^{2n})) \text{ operations in } \mathbf{Q}$$

which describes $\mathcal{P} := \mathcal{P}_0 \cup \mathrm{sing}(V)$.

Besides, since V is equidimensional, there exists, by [SS17, Lemma A.13], an atlas $\boldsymbol{\chi}$ of $(V, \mathrm{sing}(V))$. According to Definition 7.2.8, $\boldsymbol{\chi}$ is an atlas of $(V, \mathcal{P})$ as well.

Steps 3-4. By definition of the procedure Random, $\boldsymbol{\alpha}$ is an arbitrary element of $\mathbf{Q}^{2n}$, and according to Lemma 7.3.2, Γ^{φ} is a straight-line program of length $E' = 6n - 2 \;=\; O(n)$, which evaluates $\varphi = (\theta(\boldsymbol{X}) + \langle \boldsymbol{\alpha}_1, \boldsymbol{X} \rangle, \langle \boldsymbol{\alpha}_2, \boldsymbol{X} \rangle)$, where $\theta = x_1^2 + \cdots + x_n^2$. In particular, $E'' := E + E' \;=\; O(E + n)$.

Let Ω be the intersection of the following four non-empty Zariski open subsets of $\mathbf{C}^{2n}$:

$$\Omega_{\mathsf{I}}(V, \theta), \quad \Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \theta, 0), \quad \Omega_{\mathsf{K}}(V, \theta) \quad \text{and} \quad \Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \theta),$$

defined respectively by Propositions 7.2.3, 7.2.13, 7.2.14 and 7.2.16 applied to V, $\boldsymbol{\varphi}$ and possibly $\boldsymbol{\chi}$. The set Ω is a non-empty Zariski open subset of $\mathbf{C}^{2n}$ as well, and from now on, we suppose that $\boldsymbol{\alpha} \in \Omega$.

Step 5. Let $W = W_{\boldsymbol{\varphi}}(2, V)$. Since $\boldsymbol{\alpha} \in \Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \theta, 0)$, by Proposition 7.2.13, either W is empty or it is equidimensional of dimension 1, with $\mathrm{sing}(W) \subset \mathrm{sing}(V)$. Moreover, in the latter case, since $(d+3)/2 \geq 2$ by assumption, $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \varphi, 2)$ is an atlas of $(W, \mathrm{sing}(V))$.

Hence, by Lemma 7.3.5 and our assumptions, SolvePolar returns a one-dimensional parametrization $\mathscr{W}_2$, of degree at most

$$\delta = (n+c+4)D^{c+2}(D-1)^d(c+2)^d \;=\; O(n^{d+1}D^{n+2}),$$

such that $\mathsf{Z}(\mathscr{W}_2) = W$, using at most

$$\widetilde{O}\left((n+c)^3(E+(n+c)^3)D\delta^3 + (n+c)\delta\sigma_{\mathscr{S}}^2\right) \;=\; \widetilde{O}\left(n^{3d+4}(E+n^3)D^{3n+7}\right)$$

operations in $\mathbf{Q}$.

Steps 6-7. Since we assume $\boldsymbol{\alpha} \in \Omega_{\mathsf{K}}(V,\theta)$, Proposition 7.2.14 states that either W is empty or it is equidimensional of dimension 1, and $W_{\boldsymbol{\varphi}}(1,W)$ is finite. Moreover, since $\boldsymbol{\alpha} \in \Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \theta, 0)$, we deduce by Proposition 7.2.13 that $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, \mathcal{P}, \varphi, 2)$ is an atlas of $(W,\mathcal{P})$, as W is 1-equidimensional or empty and $\mathcal{P}_0$ is finite.

Let $K = W_{\boldsymbol{\varphi}}(1,W) \cup \mathcal{P}$. By Lemma 7.3.6, CritPolar returns either fail or a zero-dimensional parametrization $\mathscr{K}$, of degree at most

$$\delta_{\mathscr{K}} = \delta(n+c+4)D + \delta_{\mathscr{P}} \;=\; O\left(n^{d+2}D^{n+3} + \mu\right),$$

using at most

$$\widetilde{O}\left((n+c)^{12}(E+n)D^3\delta^2 + (n+c)\delta_{\mathscr{P}}^2\right) \;=\; \widetilde{O}\left(n^{2d+14}(E+n)D^{2n+7} + n\mu^2\right)$$

operations in $\mathbf{Q}$. Moreover, by assumption, $\mathscr{K}$ describes K. Finally, let $Q = \boldsymbol{\varphi}_1(K)$ then, by Lemma 7.3.3 and our assumptions, there exists a procedure Image that, on input $\Gamma^{\boldsymbol{\varphi}}$,$\mathscr{K}$ and $j = 1$, outputs a zero-dimensional parametrization $\mathscr{Q}$, of degree less than $\delta_{\mathscr{K}}$, such that, in case of success, $\mathsf{Z}(\mathscr{Q}) = Q$. Moreover, since by Lemma 7.3.2, $\Gamma^{\boldsymbol{\varphi}}$ has length in $O(n)$, then the execution of Image uses at most

$$\widetilde{O}\left((n^2\delta_{\mathscr{K}} + n)\delta_{\mathscr{K}}\right) \;=\; \widetilde{O}\left(n^{2d+6}D^{2n+6}\right)$$

operations in $\mathbf{Q}$.

Step 8. Since $\boldsymbol{\alpha} \in \Omega_{\mathsf{I}}(V,\theta)$, by Proposition 7.2.3, $W \cap \boldsymbol{\varphi}_1^{-1}(z)$ is finite for any $z \in \mathbf{C}$. In particular, $W \cap \boldsymbol{\varphi}_1^{-1}(Q)$ is finite, since $Q = \mathsf{Z}(\mathscr{Q})$ is. Besides, as seen above, $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, \mathcal{P}, \varphi, 2)$ is an atlas of $(W,\mathcal{P})$ since $\boldsymbol{\alpha} \in \Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \theta, 0)$.

Let $\mathcal{P}_F = [W \cap \boldsymbol{\varphi}_1^{-1}(Q)] \cup \mathcal{P}$. By Lemma 7.3.7 and our assumptions, FiberPolar outputs a zero-dimensional parametrization $\mathscr{P}_F$, of degree bounded by

$$\mu_{\mathscr{P}_F} = \delta_{\mathscr{K}}\delta + \delta_{\mathscr{P}} \;=\; O(n^{2d+3}D^{2n+5} + \mu),$$

using at most

$$\widetilde{O}\left((n+c)^4(E+(n+c)^2)D\delta_{\mathscr{K}}^2\delta^2 + (n+c)\delta_{\mathscr{P}}^2\right) \;=\; \widetilde{O}\left(n^{4d+10}(E+n^2)D^{4n+10} + n\mu^2\right)$$

operations in $\mathbf{Q}$ and such that $\mathscr{P}_F$ describes $\mathcal{P}_F$. Besides, remark that by definition $\varphi(\mathcal{P}) \subset \varphi(Q)$ so that $\mathcal{P}_F = [W \cup \mathcal{P}] \cap \boldsymbol{\varphi}_1^{-1}(Q)$.

Step 9. Since $\boldsymbol{\alpha} \in \Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \theta, 0)$, by Proposition 7.2.13 $W_{\boldsymbol{\varphi}}(1, V)$ is finite. Besides, under assumption (A), V is equidimensional with finitely many singular points. Let $\mathcal{S}_F = K_{\boldsymbol{\varphi}}(1, V)$. By Lemma 7.3.4 and our assumptions, Crit outputs a zero-dimensional parametrization $\mathscr{S}_F$, which describes $\mathcal{S}_F$, of degree bounded by

$$\sigma_{\mathscr{S}_F} = \binom{n+1}{d} D^{c+2}(D-1)^d \;=\; O(n^d D^{n+2})$$

using at most

$$\widetilde{O}\left((n+2)^{4d+8}(E+n)D^{2n+3}(D-1)^{2d} + n\sigma_{\mathscr{S}}^2\right) \;=\; \widetilde{O}\left(n^{4d+8}(E+n)D^{4n+3}\right)$$

operations in $\mathbf{Q}$.

Step 10. Since $\boldsymbol{f}$ satisfies assumption (A), the ideal $\langle \boldsymbol{f} \rangle$ generated by the polynomials in $\boldsymbol{f}$ is radical. Besides, the restriction of $\boldsymbol{\varphi}_1$ to $\boldsymbol{V}(\boldsymbol{f}) \cap \mathbf{R}^n$ is naturally proper and bounded from below by $-\sum_{i=1}^n \alpha_{1,i}^2/4$. Hence, as $Q = \mathsf{Z}(\mathscr{Q})$ is finite, then $Q \cap \mathbf{R}$ is bounded and so is

$$V \cap \mathbf{R}^n \cap \boldsymbol{\varphi}_1^{-1}(Q \cap \mathbf{R}^2) = V \cap \boldsymbol{\varphi}_1^{-1}(Q) \cap \mathbf{R}^n,$$

as $\boldsymbol{\varphi} \subset \mathbf{Q}[\boldsymbol{X}]$, since $\boldsymbol{\alpha} \in \mathbf{Q}^{2n}$ by above.

Let $F_Q = V \cap \boldsymbol{\varphi}_1^{-1}(Q)$. Since $\boldsymbol{\alpha} \in \Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, \mathrm{sing}(V), \theta)$, by Proposition 7.2.16 F_Q is either empty or equidimensional of dimension $d-1$, with $\mathrm{sing}(F_Q) \subset S_Q$, where

$$S_Q := \mathrm{sing}(V) \cup [W_{\boldsymbol{\varphi}}(1, V) \cap \boldsymbol{\varphi}_1^{-1}(Q)] = K_{\boldsymbol{\varphi}}(1, V),$$

since $\boldsymbol{\varphi}_1(K_{\boldsymbol{\varphi}}(1, V)) \subset \boldsymbol{\varphi}_1(Q)$. Moreover, in the latter case, $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, \mathrm{sing}(V), \boldsymbol{\varphi})$ is an atlas of (F_Q, S_Q). Finally, by above, the zero-dimensional parametrizations $\mathscr{P}_F$ and $\mathscr{S}_F$ describe respectively finite sets $\mathcal{P}_F$ and $\mathcal{S}_F$ such that

$$S_Q = \mathcal{S}_F \subset \mathcal{P}_F \subset F_Q,$$

and $\mathscr{S}_F$ has degree $\sigma_{\mathscr{S}_F} \leq (nD)^{n+2}$. Finally, recall that $\mathscr{Q}$ and $\mathscr{P}_F$ both have degree bounded by $\widetilde{O}\left(\mu + n^{2d+3}D^{2n+5}\right)$. Hence, according to Proposition 7.3.8, and after a few straightforward simplifications, we deduce that RoadmapBounded either outputs fail or a one-dimensional parametrization $\mathscr{R}_F$ of degree at most

$$\mathscr{B}_{\mathscr{R}_F} = \widetilde{O}\left(\mu 16^{3d}(n\log_2(n))^{2(2d-2+12\log_2(d-1))(\log_2(d-1)+6)} D^{(2n+4)(\log_2(d-1)+4)}\right),$$

using

$$\widetilde{O}\left(\mu^3 16^{9d} E(n\log_2(n))^{6(2d+12\log_2(d-1))(\log_2(d-1)+7)} D^{3(2n+4)(\log_2(d-1)+5)}\right)$$

operations in $\mathbf{Q}$. Moreover, in case of success, $\mathscr{R}_F$ describes a roadmap of $(F_Q, \mathcal{P}_F)$.

Step 11. Remark that, $\mathscr{W}_2$ and $\mathscr{R}_F$ both have degree at most $\mathscr{B}_{\mathscr{R}_F}$. Hence, by [SS17, Lemma J.8], on input $\mathscr{W}_2$ and $\mathscr{R}_F$, Union either outputs fail or a one-dimensional parametrization of degree at most $\widetilde{O}(\mathscr{B}_{\mathscr{R}_F})$ using $\widetilde{O}(n\mathscr{B}^3_{\mathscr{R}_F})$ operations in $\mathbf{Q}$. Therefore, the complexity of this step is bounded by the one of previous step. Moreover, in case of success, the output describes $W \cup F_Q$.

By above, under assumption (A), all assumptions from Proposition 7.3.10 are satisfied. Hence, since $\mathsf{Z}(\mathscr{R}_F)$ is a roadmap of $(F_Q, \mathcal{P}_F)$ and $\mathcal{P}_F = \mathcal{P} \cup (F_Q \cap W)$, by Proposition 7.3.10, Algorithm 2 returns a roadmap of $(V, \mathcal{P})$. Since $\mathcal{P}$ contains $\mathcal{P}_0$, the output is a roadmap of $(V, \mathcal{P}_0)$ as well.

In conclusion, if $\boldsymbol{\alpha} \in \Omega$ and all calls to the subroutines are successful then, on input Γ, Γ^{α} and $\mathscr{P}_0$ such that assumption (A) is satisfied, Algorithm 2 outputs a one-dimensional parametrization encoding a roadmap of $(V, \mathcal{P}_0)$. Moreover this parametrization is bounded by $\mathscr{B}_{\mathscr{R}_F}$ and all steps have complexity bounded by the one of Step 10. Since these bounds match the ones given in the statement of Theorem 7.3.9, we are done. □

Our main result, namely Theorem 7.1.1, is a direct consequence of Theorem 7.3.9 since, if $n - c < 2$ then $\boldsymbol{V}(\boldsymbol{f})$ is a roadmap of $(\boldsymbol{V}(\boldsymbol{f}), \mathsf{Z}(\mathscr{P}))$.

Remark 7.3.11. Remark that, as long as the restriction of $\boldsymbol{\varphi}_1$ to $\boldsymbol{V}(\boldsymbol{f}) \cap \mathbf{R}^n$ is proper and bounded below, the above proof still holds. This could allow one, a more *ad-hoc* choice for $\boldsymbol{\varphi}$.

7.4 Subroutines

7.4.1 Proof of Lemma 7.3.3

Lemma 7.4.1. *Let Γ and $\Gamma^{\boldsymbol{\varphi}}$ be straight-line programs of respective lengths E and E' computing sequences of polynomials respectively $\boldsymbol{f}$ and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_i)$ in $\mathbf{Q}[x_1, \ldots, x_n]$. Then there exists an algorithm IncSLP which takes as input Γ, $\Gamma^{\boldsymbol{\varphi}}$ and returns a straight-line program $\widetilde{\Gamma}$ of length*

$$E + E' + i,$$

that evaluates $\boldsymbol{f}^{\boldsymbol{\varphi}} = (\boldsymbol{f}, \varphi_1 - e_1, \ldots, \varphi_i - e_i)$ in $\mathbf{Q}[\boldsymbol{E}, \boldsymbol{X}]$, where $\boldsymbol{E} = (e_1, \ldots, e_i)$ are new variables.

Proof. Up to reordering, we can suppose that the polynomials $\varphi_1, \ldots, \varphi_i$ correspond to the respective indices $E' - i + 1, \ldots, E'$ in $\Gamma^{\boldsymbol{\varphi}}$. Let $1 \leq j \leq N$, then the straight-line program

$$\Gamma^{\boldsymbol{\varphi} - \boldsymbol{E}} = \Big(\Gamma^{\boldsymbol{\varphi}},\ (+,\ E' - i + 1,\ -n - i + 1), \ldots, (+,\ E',\ -n)\Big)$$

has length $E' + i$ and computes $(\varphi_1 - e_1, \ldots, \varphi_i - e_i)$ in $\mathbf{Q}[e_1, \ldots, e_i, x_1, \ldots, x_n]$. Finally let

$$\Gamma' = (\Gamma, \Gamma^{\boldsymbol{\varphi} - \boldsymbol{E}}),$$

then Γ' is a straight-line program of length $E + E' + i$, that computes $\boldsymbol{f}^{\boldsymbol{\varphi}} = (\boldsymbol{f}, \varphi_1 - e_1, \ldots, \varphi_i - e_i)$ in $\mathbf{Q}[e_1, \ldots, e_i, x_1, \ldots, x_n]$. □

Let $1 \leq i \leq n$ be integers and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_i) \subset \mathbf{C}[\boldsymbol{X}]$ and

$$\begin{array}{rccc} \Psi_{\boldsymbol{\varphi}}\colon & \mathbf{C}^n & \to & \mathbf{C}^{i+n} \\ & \boldsymbol{y} & \mapsto & (\boldsymbol{\varphi}(\boldsymbol{y}), \boldsymbol{y}) \end{array}.$$

Then $\Psi_{\boldsymbol{\varphi}}$ is an isomorphic embedding of algebraic sets, with inverse the projection on the last n coordinates. We call $\Psi_{\boldsymbol{\varphi}}$ the *incidence isomorphism associated to* $\boldsymbol{\varphi}$.

Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set with $1 \leq d \leq n$. Then $V^{\boldsymbol{\varphi}} = \Psi_{\boldsymbol{\varphi}}(V) \subset \mathbf{C}^{i+n}$ is called the *incidence variety associated to* V *with respect to* $\boldsymbol{\varphi}$, or in short, the incidence variety of $(V, \boldsymbol{\varphi})$.

Finally, we note $\boldsymbol{\pi} = (e_1, \ldots, e_i)$ so that for $0 \leq j \leq i$, $\boldsymbol{\pi}_j$ is the canonical projection on the first j coordinates in $\mathbf{C}^{i+n}$. The following lemma is immediate, and illustrates the main feature that motivates the introduction of incidence varieties.

Lemma 7.4.2. *For any $0 \leq j \leq i$, the following diagram commutes*

$$\begin{array}{ccc} V & \xrightarrow{\Psi_{\boldsymbol{\varphi}}} & V^{\boldsymbol{\varphi}} \\ & \searrow^{\boldsymbol{\varphi}_j} & \downarrow \boldsymbol{\pi}_j \\ & & \mathbf{C}^j \end{array}.$$

Lemma 7.4.3. *Let $\mathscr{Q}$ be a zero-dimensional parametrization of degree κ such that $\mathsf{Z}(\mathscr{Q}) \subset \mathbf{C}^n$ and let $\Gamma^{\boldsymbol{\varphi}}$ be a straight-line program of length E' which evaluates polynomials $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_i)$. There exists an algorithm IncParam which takes as input $\mathscr{Q}$, $\Gamma^{\boldsymbol{\varphi}}$ and returns a zero-dimensional parametrization $\widetilde{\mathscr{Q}}$ of degree κ and encoding $\Psi_{\boldsymbol{\varphi}}(\mathsf{Z}(\mathscr{Q})) \subset \mathbf{C}^{i+n}$, where $\Psi_{\boldsymbol{\varphi}}$ is the incidence isomorphism associated to $\boldsymbol{\varphi}$, using*

$$\widetilde{O}\left(E'\kappa\right)$$

operations in $\mathbf{Q}$.

Proof. Write $\mathscr{Q} = ((q, v_1, \ldots, v_n), \mathfrak{l})$ following the definition of zero-dimensional parametrizations given in the introduction. Since

$$\mathsf{Z}(\mathscr{Q}) = \{(v_1(\boldsymbol{t}), \ldots, v_n(\boldsymbol{t})) \mid q(\boldsymbol{t}) = 0\}$$

then

$$\Psi_{\boldsymbol{\varphi}}(\mathsf{Z}(\mathscr{Q})) = \left\{ \left(\varphi_1\big(v_1(\boldsymbol{t}), \ldots, v_n(\boldsymbol{t})\big), \ldots, \varphi_i\big(v_1(\boldsymbol{t}), \ldots, v_n(\boldsymbol{t})\big), v_1(\boldsymbol{t}), \ldots, v_n(\boldsymbol{t}) \right) \mid q(\boldsymbol{t}) = 0 \right\}.$$

Let $e_1, \ldots, e_i$ be new indeterminates and $\mathfrak{l}'(e_1, \ldots, e_i, x_1, \ldots, x_n) = \mathfrak{l}(x_1, \ldots, x_n)$ and for all $1 \leq j \leq i$, let $w_j = \varphi_j(v_1, \ldots, v_n) \mod q \in \mathbf{Q}[t]$. Hence, we claim that taking $\widetilde{\mathscr{Q}} = ((q, w_1, \ldots, w_i, v_1, \ldots, v_n), \mathfrak{l})$ one gets a zero-dimensional parametrization of $\Psi_{\boldsymbol{\varphi}}(\mathsf{Z}(\mathscr{Q}))$. Indeed, $\deg(w_j) < \deg(q)$, for all $1 \leq j \leq i$, and

$$\mathfrak{l}'\big(w_1, \ldots, w_i, v_1, \ldots, v_n\big) = \mathfrak{l}\big(v_1, \ldots, v_n\big) = t.$$

Besides, computing $\widetilde{\mathscr{Q}}$ is done by evaluating $\Gamma^{\boldsymbol{\varphi}}$ at $v_1, \ldots, v_n$ doing all operations modulo q; this can be done using $\widetilde{O}(E'\kappa)$ operations in $\mathbf{Q}$. □

We can now prove Lemma 7.3.3.

Proof of Lemma 7.3.3. Let $\Psi_{\boldsymbol{\varphi}}$ be the incidence isomorphism associated to $\boldsymbol{\varphi}$. According to Lemma 7.4.2, the image of $\mathsf{Z}(\mathscr{P})$ by $\boldsymbol{\varphi}_j$, can be obtained by projecting the incidence variety $\Psi_{\boldsymbol{\varphi}}(\mathsf{Z}(\mathscr{P}))$ on the first j coordinates.

Hence the algorithm Image can be performed as follows. First, according to Lemma 7.4.3, there exists an algorithm IncParam which, on input $\mathscr{P}$ and $\Gamma^{\boldsymbol{\varphi}}$, computes a zero-dimensional parametrization $\widetilde{\mathscr{P}}$ of degree κ, encoding $\Psi_{\boldsymbol{\varphi}}(\mathsf{Z}(\mathscr{P})) \subset \mathbf{C}^{j+n}$, and using $\widetilde{O}(E'\kappa)$ operations in $\mathbf{Q}$. Secondly, according to [SS17, Lemma J.5.], there exists an algorithm Projection which, on input $\widetilde{\mathscr{P}}$ and $j \in \{1, \ldots, i\}$, computes a zero-dimensional parametrization $\mathscr{Q}$ encoding

$$\boldsymbol{\pi}_j(\widetilde{\mathscr{P}}) = \boldsymbol{\pi}_j\left(\Psi_{\boldsymbol{\varphi}}(\mathsf{Z}(\mathscr{P}))\right) = \boldsymbol{\varphi}_j(\mathsf{Z}(\mathscr{P})),$$

using $\widetilde{O}\left(n^2\kappa^2\right)$ operations in $\mathbf{Q}$. □

7.4.2 Auxiliary results for generalized polar varieties

We reuse the notation introduced in the previous subsection. Let $\boldsymbol{E} = (e_1 \ldots, e_i)$ be new indeterminates. Recall that $V \subset \mathbf{C}^n$ is a d-equidimensional algebraic set.

Lemma 7.4.4. *Let $\boldsymbol{h} \subset \mathbf{C}[\boldsymbol{X}]$ be a set of generators of $\boldsymbol{I}(V)$. Then*

$$\boldsymbol{h}^{\boldsymbol{\varphi}} = (\boldsymbol{h}, \varphi_1 - e_1, \ldots, \varphi_i - e_1) \subset \mathbf{C}[\boldsymbol{E}, \boldsymbol{X}]$$

is a set of generator of $\boldsymbol{I}(V^{\boldsymbol{\varphi}}) \subset \mathbf{C}[\boldsymbol{E}, \boldsymbol{X}]$, which is equidimensional of dimension d.

Proof. Remark that by Lemma 7.2.2, for any $(\boldsymbol{t}, \boldsymbol{y}) \in V^{\boldsymbol{\varphi}}$,

$$\operatorname{rank} \operatorname{Jac}_{\boldsymbol{t},\boldsymbol{y}}(\boldsymbol{h}^{\boldsymbol{\varphi}}) = \operatorname{rank} \begin{bmatrix} \boldsymbol{O} & \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{h}) \\ -I_i & \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{\varphi}) \end{bmatrix} = \operatorname{rank} \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{h}) + i,$$

so that for all $\boldsymbol{y} \in \operatorname{reg}(V)$, since $\operatorname{Jac}(\boldsymbol{h})$ has rank $n - d$ at $\boldsymbol{y}$, then $\operatorname{Jac}(\boldsymbol{h}^{\boldsymbol{\varphi}})$ has rank $n - d + i$ at $\Psi_{\boldsymbol{\varphi}}(\boldsymbol{y})$. Hence, since $\operatorname{reg}(V)$ is Zariski dense in V, by [SS11, Lemma 15] $\langle \boldsymbol{h}^{\boldsymbol{\varphi}} \rangle$ is an equidimensional radical ideal of dimension d.

Besides, let $(\boldsymbol{t}, \boldsymbol{y}) \in \mathbf{C}^n$, then $\boldsymbol{h}^{\boldsymbol{\varphi}}(\boldsymbol{t}, \boldsymbol{y}) = 0$ if and only if $\boldsymbol{h}(\boldsymbol{y}) = 0$ and $\boldsymbol{\varphi}(\boldsymbol{y}) = \boldsymbol{t}$ that is $(\boldsymbol{t}, \boldsymbol{y}) \in V^{\boldsymbol{\varphi}}$ since $\boldsymbol{h}$ generates $\boldsymbol{I}(V)$. Hence $\boldsymbol{V}(\langle \boldsymbol{h}^{\boldsymbol{\varphi}} \rangle) = V^{\boldsymbol{\varphi}}$ so that by the Hilbert's Nullstellensatz [Eis95, Theorem 1.6],

$$\boldsymbol{I}(V^{\boldsymbol{\varphi}}) = \sqrt{\langle \boldsymbol{h}^{\boldsymbol{\varphi}} \rangle} = \langle \boldsymbol{h}^{\boldsymbol{\varphi}} \rangle .$$

□

The following lemma shows an important consequence of Lemma 7.4.2 for polar varieties.

Lemma 7.4.5. *For $0 \leq j \leq i$, the restriction of $\Psi_{\boldsymbol{\varphi}}$ induces an isomorphism between $W_{\boldsymbol{\varphi}}(j, V)$ (resp. $K_{\boldsymbol{\varphi}}(j, V)$) and $W(\boldsymbol{\pi}_j, V^{\boldsymbol{\varphi}})$ (resp. $K(\boldsymbol{\pi}_j, V^{\boldsymbol{\varphi}})$).*

Proof. Let $\boldsymbol{h}$ be generators of $\boldsymbol{I}(V)$. By Lemma 7.4.4, $\boldsymbol{h}^{\boldsymbol{\varphi}}$ are generators of $\boldsymbol{I}(V)$. Let $\boldsymbol{y} \in V$, $\boldsymbol{y}^{\boldsymbol{\varphi}} = \Psi_{\boldsymbol{\varphi}}(\boldsymbol{y}) \in V^{\boldsymbol{\varphi}}$ and $0 \leq j \leq i$. Then by Lemma 7.2.2,

$$\operatorname{rank} \operatorname{Jac}_{\boldsymbol{y}^{\boldsymbol{\varphi}}}([\boldsymbol{h}^{\boldsymbol{\varphi}}, \boldsymbol{\pi}_j]) = \operatorname{rank} \begin{bmatrix} \boldsymbol{O} & \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{h}) \\ -I_i & \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{\varphi}) \\ I_j \ \boldsymbol{O} & \boldsymbol{O} \end{bmatrix} = \operatorname{rank} \operatorname{Jac}_{\boldsymbol{y}}([\boldsymbol{h}, \boldsymbol{\varphi}_j]) + i, \tag{7.2}$$

where I_ℓ denotes the $\ell \times \ell$ identity matrix. Since both V and $V^{\boldsymbol{\varphi}}$ are d-equidimensional, then by [SS17, Lemma A.2.], $K_{\boldsymbol{\varphi}}(j, V)$ and $K(\boldsymbol{\pi}_j, V^{\boldsymbol{\varphi}})$ are the sets of points $\boldsymbol{y} \in V$ and $\boldsymbol{y}^{\boldsymbol{\varphi}} \in V^{\boldsymbol{\varphi}}$ where respectively

$$\operatorname{Jac}_{\boldsymbol{y}}([\boldsymbol{h}, \boldsymbol{\varphi}_j]) < n - d + j \quad \text{and} \quad \operatorname{Jac}_{\boldsymbol{y}^{\boldsymbol{\varphi}}}([\boldsymbol{h}^{\boldsymbol{\varphi}}, \boldsymbol{\pi}_j]) < n + i - d + j.$$

Hence by (7.2), the two conditions are equivalent so that $\Psi_{\boldsymbol{\varphi}}(K_{\boldsymbol{\varphi}}(j, V)) = K(\boldsymbol{\pi}_j, V^{\boldsymbol{\varphi}})$ for all $0 \leq j \leq i$. In particular, for $j = 0$, $\Psi_{\boldsymbol{\varphi}}(\operatorname{sing}(V)) = \operatorname{sing}(V^{\boldsymbol{\varphi}})$, so that for all $0 \leq j \leq i$,

$$\Psi_{\boldsymbol{\varphi}}(W^{\circ}_{\boldsymbol{\varphi}}(j, V)) = W^{\circ}(\boldsymbol{\pi}_j, V^{\boldsymbol{\varphi}}).$$

Since $\Psi_{\boldsymbol{\varphi}}$ is an isomorphism of algebraic sets, it is a homeomorphism for the Zariski topology, so that it maps the Zariski closure of sets to the Zariski closure of their image. Hence, we can conclude that $\Psi_{\boldsymbol{\varphi}}(W_{\boldsymbol{\varphi}}(j, V)) = W(\boldsymbol{\pi}_j, V^{\boldsymbol{\varphi}})$ for all $0 \leq j \leq i$. □

Lemma 7.4.6 (Chart and atlases)**.** *Let $1 \leq e \leq n$, $Q \subset \mathbf{C}^e$ be a finite set and S be an algebraic set such that V and S lie over Q with respect to $\boldsymbol{\varphi}$. By a slight abuse of notation, we denote equally $m \in \mathbf{C}[\boldsymbol{X}]$ when seen in $\mathbf{C}[\boldsymbol{E}, \boldsymbol{X}]$. Then, the following holds.*

1. *Let $\chi = (m, \boldsymbol{h}) \subset \mathbf{C}[\boldsymbol{X}]$ be a chart of $(V, Q, S, \boldsymbol{\varphi})$, then $\chi^{\boldsymbol{\varphi}} = (m, \boldsymbol{h}^{\boldsymbol{\varphi}}) \subset \mathbf{C}[\boldsymbol{E}, \boldsymbol{X}]$ is a chart of $(V^{\boldsymbol{\varphi}}, Q, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi})$, where $S^{\boldsymbol{\varphi}} = \Psi_{\boldsymbol{\varphi}}(S)$.*
2. *Let $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ be an atlas of $(V, Q, S, \boldsymbol{\varphi})$, then if $\boldsymbol{\chi}^{\boldsymbol{\varphi}} = (\chi_j^{\boldsymbol{\varphi}})_{1 \leq j \leq s}$ as defined in the previous item, $\boldsymbol{\chi}^{\boldsymbol{\varphi}}$ is an atlas of $(V^{\boldsymbol{\varphi}}, Q, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi})$.*

Proof. We start with the first statement, let Q, S and $\chi = (m, \boldsymbol{h})$ be as in the statement. It holds that:

C_1 : Let $\boldsymbol{y} \in \mathcal{O}(m) \cap V - S$, which is non-empty by property C_1 of χ. Then by definition $\Psi_{\boldsymbol{\varphi}}(\boldsymbol{y}) \in V^{\boldsymbol{\varphi}}$, and since $\Psi_{\boldsymbol{\varphi}}$ is an isomorphism on $V^{\boldsymbol{\varphi}}$, $\Psi_{\boldsymbol{\varphi}}(\boldsymbol{y}) \notin S^{\boldsymbol{\varphi}}$. Finally since $m \in \mathbf{C}[\boldsymbol{X}]$, then $m(\Psi_{\boldsymbol{\varphi}}(\boldsymbol{y})) = m(\boldsymbol{y}) \neq 0$ so that $\mathcal{O}(m) \cap V^{\boldsymbol{\varphi}} - S^{\boldsymbol{\varphi}}$ is not empty.

C_2 : Note that since $m \in \mathbf{C}[\boldsymbol{X}]$, $\Psi_{\boldsymbol{\varphi}}(\mathcal{O}(m))$ is defined by $m \neq 0$. By a slight abuse of notation, we still denote this Zariski open set $\mathcal{O}(m)$. Hence, it follows from the definition of $\Psi_{\boldsymbol{\varphi}}$ that $\Psi_{\boldsymbol{\varphi}}(\mathcal{O}(m) \cap V - S) = \mathcal{O}(m) \cap V^{\boldsymbol{\varphi}} - S^{\boldsymbol{\varphi}}$. Besides, by Lemma 7.4.2, $\boldsymbol{\pi}_e \circ \Psi_{\boldsymbol{\varphi}}$ and $\boldsymbol{\varphi}_e$ coincide on V. Then

$$Z_{|\boldsymbol{\varphi}_e \in Q} = \Psi_{\boldsymbol{\varphi}}(Z)_{|\boldsymbol{\pi}_e \in Q} \text{ for any } Z \subset V.$$

Finally, as seen in the proof of Lemma 7.4.4, $\Psi_{\boldsymbol{\varphi}}(\boldsymbol{V}(\boldsymbol{h})) = \boldsymbol{V}(\boldsymbol{h}^{\boldsymbol{\varphi}})$. Hence by property C_2 of χ,

$$\mathcal{O}(m) \cap V^{\boldsymbol{\varphi}} - S^{\boldsymbol{\varphi}} = \Psi_{\boldsymbol{\varphi}}(\mathcal{O}(m) \cap \boldsymbol{V}(\boldsymbol{h})_{|\boldsymbol{\varphi}_e \in Q} - S) = \mathcal{O}(m) \cap \boldsymbol{V}(\boldsymbol{h}^{\boldsymbol{\varphi}})_{|\boldsymbol{\pi}_e \in Q} - S^{\boldsymbol{\varphi}},$$

since $\mathcal{O}(m) \cap \boldsymbol{V}(\boldsymbol{h})_{|\boldsymbol{\varphi}_e \in Q} - S$ is a subset of V.

C_3 : Let c be the cardinality of $\boldsymbol{h}$, then $\boldsymbol{h}^{\boldsymbol{\varphi}}$ has cardinality $c+i$. Hence by property C_3 of χ, $e+c+i \leq i+n$ as required.

C_4 : Finally let $\boldsymbol{y}^{\boldsymbol{\varphi}} = (\boldsymbol{t}, \boldsymbol{y}) \in \mathcal{O}(m) \cap V^{\boldsymbol{\varphi}} - S^{\boldsymbol{\varphi}}$, we know from above that $\boldsymbol{y} \in \mathcal{O}(m) \cap V - S$, so that by property C_4 of χ, $\mathrm{Jac}_{\boldsymbol{y}}[\boldsymbol{h}, \boldsymbol{\varphi}_e]$ has full rank $c+e$. But by the equality (7.2) in the proof of Lemma 7.4.5, this means that $\mathrm{Jac}_{\boldsymbol{y}^{\boldsymbol{\varphi}}}([\boldsymbol{h}^{\boldsymbol{\varphi}}, \boldsymbol{\pi}_e])$ has full rank $c+i+e$ as required.

Now we have shown that charts can be transferred to incidence varieties, let us prove that this naturally gives rise to atlases. Consider an atlas $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ of $(V, Q, S, \boldsymbol{\varphi})$, and let $\boldsymbol{\chi}^{\boldsymbol{\varphi}} = (\chi_j^{\boldsymbol{\varphi}})_{1 \leq j \leq s}$, where for all $1 \leq j \leq s$, $\chi_j^{\boldsymbol{\varphi}}$ is defined from χ_j as above. We proved that $\boldsymbol{\chi}^{\boldsymbol{\varphi}}$ is an atlas of $(V^{\boldsymbol{\varphi}}, Q, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi})$.

Property A_1 is straightforward, and A_2 is given by the first statement of this lemma which we just proved. Finally, since $\Psi_{\boldsymbol{\varphi}}(V - S) = V^{\boldsymbol{\varphi}} - S^{\boldsymbol{\varphi}}$, then for any $\boldsymbol{y}^{\boldsymbol{\varphi}} = (\boldsymbol{t}, \boldsymbol{y}) \in V^{\boldsymbol{\varphi}} - S^{\boldsymbol{\varphi}}$, by property A_3 of $\boldsymbol{\chi}$, there exists $1 \leq j \leq s$ such that $m_j(\boldsymbol{y}^{\boldsymbol{\varphi}}) = m_j(\boldsymbol{y}) \neq 0$. Then $\boldsymbol{\chi}^{\boldsymbol{\varphi}}$ satisfies property A_3 of atlases. □

We deduce the following results for two important particular cases.

Lemma 7.4.7. *Let $S \subset \mathbf{C}^n$ be an algebraic set, $\chi = (m, \boldsymbol{h})$ and $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ be respectively a chart and an atlas of (V, S), and let $\chi^{\boldsymbol{\varphi}}$ and $\boldsymbol{\chi}^{\boldsymbol{\varphi}}$ the chart and atlas constructed from respectively χ and $\boldsymbol{\chi}^{\boldsymbol{\varphi}}$ as in Lemma 7.4.6. The following holds.*

1. *If $\boldsymbol{h}$ has cardinality c, then for any c-minor m' of $\mathrm{Jac}(\boldsymbol{h})$ and any $(c+i-1)$-minor m'' of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$, containing the rows of $\mathrm{Jac}(\boldsymbol{\varphi}_i)$, the following holds. If $W_{\mathrm{chart}}(\chi, m', m'')$ is a chart of $\mathscr{W} = (W_{\boldsymbol{\varphi}}(i, V), S)$, then $W_{\mathrm{chart}}(\chi^{\boldsymbol{\varphi}}, m', m'')$ is a chart of $\mathscr{W}^{\boldsymbol{\varphi}} = (W(\boldsymbol{\pi}_i, V^{\boldsymbol{\varphi}}), S^{\boldsymbol{\varphi}})$.*
2. *If $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, i)$ is an atlas of $\mathscr{W}$ then, $W_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, V^{\boldsymbol{\varphi}}, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi}, i)$ is an atlas of $\mathscr{W}^{\boldsymbol{\varphi}}$.*

Proof. Let m' and m'' be respectively a c-minor of $\mathrm{Jac}(\boldsymbol{h})$ and a $(c+i-1)$-minor of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$, containing the rows of $\mathrm{Jac}(\boldsymbol{\varphi}_i)$. Assume that

$$W_{\mathrm{chart}}(\chi, m', m'', \boldsymbol{\varphi}) = \left(mm'm'',\ (\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')) \right)$$

is a chart of $\mathscr{W}$. By C_1, $\mathcal{O}(mm'm'') \cap W_{\boldsymbol{\varphi}}(i, V) - S$ is not empty, so that m' and m'' are not identically zero. Since

$$\mathrm{Jac}(\boldsymbol{h}^{\boldsymbol{\varphi}}) = \begin{pmatrix} \boldsymbol{O} & \mathrm{Jac}(\boldsymbol{h}) \\ -I_i & \mathrm{Jac}(\boldsymbol{\varphi}_i) \end{pmatrix},$$

Lemma 7.2.1 shows that m' is a $(c+i)$-minor of $\mathrm{Jac}(\boldsymbol{h}^{\boldsymbol{\varphi}})$ and m'' is a $(c+i+i-1)$-minor of $\mathrm{Jac}(\boldsymbol{h}^{\boldsymbol{\varphi}}, \boldsymbol{\pi}_i)$ containing $I_i = \mathrm{Jac}(\boldsymbol{\pi}_i)$. Hence, according to Definition 7.2.10,

$$W_{\mathrm{chart}}(\chi^{\boldsymbol{\varphi}}, m', m'') = \left(mm'm'', (\boldsymbol{h}^{\boldsymbol{\varphi}}, \mathcal{H}_{\boldsymbol{\pi}}(\boldsymbol{h}^{\boldsymbol{\varphi}}, i, m'')) \right),$$

where, by definition, $\mathcal{H}_{\boldsymbol{\pi}}(\boldsymbol{h}^{\boldsymbol{\varphi}}, i, m'')$ is the sequence of $(c+i+i)$-minors of $\mathrm{Jac}([\boldsymbol{h}^{\boldsymbol{\varphi}}, \boldsymbol{\pi}_i])$ obtained by successively adding the missing row and the missing columns of $\mathrm{Jac}([\boldsymbol{h}^{\boldsymbol{\varphi}}, \boldsymbol{\pi}_i])$ to m''.

But, since $m'' \neq 0$, Lemma 7.2.12 implies that $\mathcal{H}_{proj}(\boldsymbol{h}^{\boldsymbol{\varphi}}, i, m'')$ is, as well, the sequence of $(c+i)$-minors obtained by successively adding the missing row and the missing columns of $\mathrm{Jac}(\boldsymbol{h}^{\boldsymbol{\varphi}}, i) = \mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i)$ to m''. We deduce that

$$\mathcal{H}_{\boldsymbol{\pi}}(\boldsymbol{h}^{\boldsymbol{\varphi}}, i, m'') = \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''),$$

so that if $\boldsymbol{g} = (\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''))$, then $\boldsymbol{g}^{\boldsymbol{\varphi}} = (\boldsymbol{h}^{\boldsymbol{\varphi}}, \mathcal{H}_{\boldsymbol{\pi}}(\boldsymbol{h}^{\boldsymbol{\varphi}}, i, m''))$. Hence $W_{\mathrm{chart}}(\chi^{\boldsymbol{\varphi}}, m', m'')$ is exactly the chart constructed from $W_{\mathrm{chart}}(\chi, m', m'', \boldsymbol{\varphi})$ in Lemma 7.4.6, and since, by Lemma 7.4.5, $\Psi_{\boldsymbol{\varphi}}(W_{\boldsymbol{\varphi}}(i, V)) = W(\boldsymbol{\pi}_i, V^{\boldsymbol{\varphi}})$, the first statement of Lemma 7.4.6 implies that $W_{\mathrm{chart}}(\chi^{\boldsymbol{\varphi}}, m', m'')$ is a chart of $\mathscr{W}^{\boldsymbol{\varphi}}$.

To prove the second assertion, remark that by the third assertion of Lemma 7.2.12, $W_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, V^{\boldsymbol{\varphi}}, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi}, i)$ is the sequence of all those $W_{\mathrm{chart}}(\chi_j^{\boldsymbol{\varphi}}, m', m'')$, for $j \in \{1, \ldots, s\}$ and for m', m'' respectively a $c+i$-minor of $\mathrm{Jac}(\boldsymbol{h}_j^{\boldsymbol{\varphi}})$ and a $(c+i-1)$-minor of $\mathrm{Jac}(\boldsymbol{h}_j^{\boldsymbol{\varphi}}, i)$ for which $\mathcal{O}(m_j m' m'') \cap W(\boldsymbol{\pi}_i, V^{\boldsymbol{\varphi}}) - S$ is not empty.

As seen above, the polynomials m' and m'' are actually c-minors of $\mathrm{Jac}(\boldsymbol{h}_j)$ and $(c+i-1)$-minors of $\mathrm{Jac}([\boldsymbol{h}_j^{\boldsymbol{\varphi}}, \boldsymbol{\varphi}_i])$, and in the first point, we prove that $W_{\mathrm{chart}}(\chi_j^{\boldsymbol{\varphi}}, m', m'')$ is the chart constructed in the first point of Lemma 7.4.6 from $W_{\mathrm{chart}}(\chi_j, m', m'')$. Hence $W_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, V^{\boldsymbol{\varphi}}, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi}, i)$ is exactly the atlas constructed from $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, i)$ in the second item of Lemma 7.4.6. In conclusion, by Lemma 7.4.6, if $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, i)$ is an atlas of $\mathscr{W}$, then $W_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, V^{\boldsymbol{\varphi}}, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi}, i)$ is an atlas of $\mathscr{W}^{\boldsymbol{\varphi}}$. □

Lemma 7.4.8. *Let $1 \leq e \leq n$, $Q \subset \mathbf{C}^e$ be a finite set and S be an algebraic set such that V and S lie over Q with respect to $\boldsymbol{\varphi}$. Let further*

$$\mathscr{F} = \left(V_{|\boldsymbol{\varphi}_e \in Q},\ (S \cup W_{\boldsymbol{\varphi}}(e, V))_{|\boldsymbol{\varphi}_e \in Q}\right) \quad \text{and} \quad \mathscr{F}^{\boldsymbol{\varphi}} = \left(V^{\boldsymbol{\varphi}}_{|\boldsymbol{\pi}_e \in Q},\ (S^{\boldsymbol{\varphi}} \cup W(\boldsymbol{\pi}_e, V^{\boldsymbol{\varphi}}))_{|\boldsymbol{\pi}_e \in Q}\right).$$

Let $\chi = (m, \boldsymbol{h})$ and $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ be respectively a chart and an atlas of $(V, Q, S, \boldsymbol{\varphi})$ and let $\chi^{\boldsymbol{\varphi}}$ and $\boldsymbol{\chi}^{\boldsymbol{\varphi}}$ the chart and atlas constructed from respectively χ and $\boldsymbol{\chi}^{\boldsymbol{\varphi}}$ as in Lemma 7.4.6.

If $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$ is an atlas of $\mathscr{F}$ then $F_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, V^{\boldsymbol{\varphi}}, Q, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi})$ is an atlas of $\mathscr{F}^{\boldsymbol{\varphi}}$.

Proof. Without loss of generality one can assume that $S \subset V$. Since by Lemma 7.4.2, $\boldsymbol{\pi}_e \circ \Psi_{\boldsymbol{\varphi}}$ and $\boldsymbol{\varphi}_e$ coincide on V, then

$$\Psi_{\boldsymbol{\varphi}}\left((S \cup W_{\boldsymbol{\varphi}}(e, V))_{|\boldsymbol{\varphi}_e \in Q}\right) = (S^{\boldsymbol{\varphi}} \cup W(\boldsymbol{\pi}_e, V^{\boldsymbol{\varphi}}))_{|\boldsymbol{\pi}_e \in Q}.$$

Hence, for any $1 \leq j \leq s$,

$$\mathcal{O}(m_j) \cap V^{\boldsymbol{\varphi}}_{|\boldsymbol{\pi}_e \in Q} - (S^{\boldsymbol{\varphi}} \cup W(\boldsymbol{\pi}_e, V^{\boldsymbol{\varphi}}))_{|\boldsymbol{\pi}_e \in Q} \ = \ \Psi_{\boldsymbol{\varphi}}\left(\mathcal{O}(m_j) \cap V_{|\boldsymbol{\varphi}_e \in Q} - (S \cup W_{\boldsymbol{\varphi}}(e, V))_{|\boldsymbol{\varphi}_e \in Q}\right),$$

so that these sets are not-empty for the same j's in $\{1, \ldots, s\}$. Hence $F_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, V^{\boldsymbol{\varphi}}, Q, S^{\boldsymbol{\varphi}}, \boldsymbol{\pi})$ is exactly the atlas constructed from $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\pi})$ in Lemma 7.4.6.

In conclusion, by the second assertion of Lemma 7.4.6, if $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\pi})$ is an atlas of $\mathscr{F}$ then $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\pi})$ is an atlas of $\mathscr{F}^{\boldsymbol{\varphi}}$. □

7.4.3 Lagrange systems

We present here a simplified version of generalized Lagrange systems defined in [SS17, Section 5.2] to encode polar varieties and provide equivalent results adapted to our case. As we only use a simplified version (involving a single block of Lagrange multipliers), we call them simply Lagrange systems.

7.4.3.a. Definitions

The following is nothing but a simplified version of [SS17, Definition 5.3].

Definition 7.4.9. A *Lagrange system* is a triple $L = (\Gamma, \mathscr{Q}, \mathscr{S})$ where

- Γ is a straight-line program evaluating a sequence $\boldsymbol{F} = (\boldsymbol{f}, \boldsymbol{g}) \subset \mathbf{Q}[\boldsymbol{X}, \boldsymbol{L}]$, where
  - $\boldsymbol{X} = (X_1, \ldots, X_n)$ and $\boldsymbol{L} = (L_1, \ldots, L_m)$;
  - $\boldsymbol{f} = (f_1, \ldots, f_p) \subset \mathbf{Q}[\boldsymbol{X}]$ and $\boldsymbol{g} = (g_1, \ldots, g_q) \subset \mathbf{Q}[\boldsymbol{X}, \boldsymbol{L}]$ with $\deg_{\boldsymbol{L}} \boldsymbol{g} \leq 1$;
- $\mathscr{Q}$ is a zero-dimensional parametrization with coefficients in $\mathbf{Q}$, with $Q = \mathsf{Z}(\mathscr{Q}) \subset \mathbf{C}^e$;
- $\mathscr{S}$ is a zero-dimensional parametrization with coefficients in $\mathbf{Q}$, with $S = \mathsf{Z}(\mathscr{S}) \subset \mathbf{C}^n$ lying over Q;
- $(n+m) - (p+q) \geq e$.

We also define N and P as respectively the number of variables and equations, so that

$$N = n + m, \quad P = p + q \quad \text{and} \quad d = N - e - P \geq 0.$$

One checks that such a Lagrange system is also a generalized Lagrange system in the sense of [SS17, Definition 5.3]. We can then define the same objects associated to such systems as follows. We denote by $\pi_{\boldsymbol{X}} \colon \mathbf{C}^N \to \mathbf{C}^n$ the projection on the variables associated to $\boldsymbol{X}$ in any set of $\mathbf{C}^N$ defined by equations in $\mathbf{C}[\boldsymbol{X}, \boldsymbol{L}]$.

Definition 7.4.10. Let $L = (\Gamma, \mathscr{Q}, \mathscr{S})$ be a Lagrange system and all associated data defined in Definition 7.4.9. We define the following objects:

- the *type of* L is the triplet $T = (\boldsymbol{n}, \boldsymbol{p}, e)$ where $\boldsymbol{n} = (n, m)$ and $\boldsymbol{p} = (p, q)$;
- $\mathscr{U}(L) = \pi_{\boldsymbol{X}}\left(\boldsymbol{V}(\boldsymbol{F})_{|\boldsymbol{\pi}_e \in Q} - \pi_{\boldsymbol{X}}^{-1}(S)\right) \subset \mathbf{C}^n$
- $\overline{\mathscr{U}(L)}^Z \subset \mathbf{C}^n$ the Zariski closure of $\mathscr{U}(L)$.

Then we say that L defines $\overline{\mathscr{U}(L)}^Z$.

We see here that Lagrange systems are nothing but generalized Lagrange systems of type $(1, \boldsymbol{n}, \boldsymbol{p}, e)$. We now define local and global normal forms, that can be seen as equivalent to charts and atlases for Lagrange systems where replacing the notion of complete intersection by the one of normal form presented below.

For any non-zero polynomial M of a polynomial ring $\mathbf{C}[\boldsymbol{Y}]$ we denote by $\mathbf{C}[\boldsymbol{Y}]_M$ the localization of $\mathbf{C}[\boldsymbol{Y}]$ at M, that is the of all g/M^j where $\boldsymbol{g} \in \mathbf{C}[\boldsymbol{Y}]$ and $j \in \mathbb{N}$.

Definition 7.4.11. For a non-zero $M \in \mathbf{Q}[\boldsymbol{X}]$ and polynomials $\boldsymbol{H} \subset \mathbf{Q}[\boldsymbol{X}, \boldsymbol{L}]_M$, we say that $\boldsymbol{H}$ *is in normal form in* $\mathbf{Q}[\boldsymbol{X}, \boldsymbol{L}]$ if these polynomials have the form

$$\boldsymbol{H} = (h_1, \ldots, h_c, L_1 - \rho_1, \ldots, L_m - \rho_m),$$

where the h_j's are in $\mathbf{Q}[\boldsymbol{X}]$ and the ρ_j's are in $\mathbf{Q}[\boldsymbol{X}]_M$. We call $\boldsymbol{h} = (h_1, \ldots, h_c)$ and $\boldsymbol{\rho} = (L_j - \rho_j)_{1 \leq j \leq m}$ respectively the $\boldsymbol{X}$ and $\boldsymbol{L}$ components of $\boldsymbol{H}$.

Definition 7.4.12. A *local normal form* of a Lagrange system $L = (\Gamma, \mathscr{Q}, \mathscr{S})$ is the data of $\psi = (\mathfrak{m}, \mathfrak{d}, \boldsymbol{h}, \boldsymbol{H})$ that satisfies the following conditions:

- L_1 $\mathfrak{m}, \mathfrak{d} \in \mathbf{Q}[\boldsymbol{X}] - \{0\}$ and $\boldsymbol{H}$ is in normal form in $\mathbf{Q}[\boldsymbol{X}, \boldsymbol{L}]_{\mathfrak{m}\mathfrak{d}}$ with $\boldsymbol{X}$-component $\boldsymbol{h} = (h_1, \ldots, h_c)$;
- L_2 $\boldsymbol{H}$ and $\boldsymbol{F}$ have the same cardinality $n - c = N - P$;
- L_3 $\langle \boldsymbol{F}, \boldsymbol{I}(Q) \rangle = \langle \boldsymbol{H}, \boldsymbol{I}(Q) \rangle$ in $\mathbf{Q}[\boldsymbol{X}, \boldsymbol{L}]_{\mathfrak{m},\mathfrak{d}}$;
- L_4 $(\mathfrak{m}, \boldsymbol{h})$ is a chart of (V, Q, S);
- L_5 $\mathfrak{d}$ does not vanish on $\mathcal{O}(\mathfrak{m}) \cap \mathscr{U}(L)$.

Given such a local normal form ψ we will note $\chi = (\mathfrak{m}, \boldsymbol{h})$ the associated chart.

As for atlases and charts, we define now global normal forms using local normal forms.

Definition 7.4.13. A *global normal form* of a Lagrange system $L = (\Gamma, \mathscr{Q}, \mathscr{S})$ is the data of $\boldsymbol{\psi} = (\psi_j)_{1 \leq j \leq s}$ such that:

- G_1 each $\psi_j = (\mathfrak{m}_j, \mathfrak{d}_j, \boldsymbol{h}_j, \boldsymbol{H}_j)$ is a local normal form;
- G_2 $\boldsymbol{\chi} = ((\mathfrak{m}_j, \boldsymbol{h}_j))_{1 \leq j \leq s}$ is an atlas of (V, Q, S).

Let further $\mathscr{Y} = (Y_1, \ldots, Y_r)$ be algebraic subsets of $\mathbf{C}^n$. A global normal form of $(L; \mathscr{Y})$ is the data of a global normal form $\boldsymbol{\psi} = (\psi_j)_{1 \leq j \leq s}$ of L such that for all $1 \leq j \leq s$ and $1 \leq k \leq r$:

- G_3 for any irreducible component Y of Y_k contained in V and such that $\mathcal{O}(\mathfrak{m}_j) \cap Y - S$ is not empty, $\mathcal{O}(\mathfrak{m}_j \mathfrak{d}_j) \cap Y - S$ is not empty.

We say that L (resp. $(L; \mathscr{Y})$) has the *global normal form property* if there exists a global normal form $\boldsymbol{\psi}$ of L (resp. $(L; \mathscr{Y})$) and we will note $\boldsymbol{\chi}$ the associated atlas.

7.4.3.b. Lagrange system for polar varieties

We give here a slightly different version of results presented in [SS17, Section 5.5]. We first recall the construction of [SS17, Definition 5.11] adapted to our more elementary case.

Definition 7.4.14. Let $L = (\Gamma, (1), \mathscr{S})$ be a Lagrange system of type $((n, 0), (p, 0), 0)$, let $\boldsymbol{f} \subset \mathbf{C}[\boldsymbol{X}]$ be the polynomials which are evaluated by Γ and let $i \in \{1, \ldots, n - p\}$.
Let $\boldsymbol{L} = (L_1, \ldots, L_p)$ be new indeterminates, for $\boldsymbol{u} = (u_1, \ldots, u_p) \in \mathbf{Q}^p$, define

$$\boldsymbol{F_u} = \Big(\boldsymbol{f},\ \mathsf{Lagrange}(\boldsymbol{f}, i, \boldsymbol{L}),\ u_1 L_1 + \cdots + u_p L_p - 1\Big),$$

where $\mathsf{Lagrange}(\boldsymbol{f}, i, \boldsymbol{L})$ denotes the entries of

$$\begin{bmatrix} L_1 & \cdots & L_p \end{bmatrix} \cdot \mathrm{Jac}(\boldsymbol{f}, i).$$

We define $W_{\mathrm{lag}}(L, \boldsymbol{u}, i)$ as the triplet $(\Gamma_{\boldsymbol{u}}, \mathscr{Q}, \mathscr{S})$, where $\Gamma_{\boldsymbol{u}}$ is a straight-line program that evaluates $\boldsymbol{F}_{\boldsymbol{u}}$, it is a Lagrange system of type $((n,p),(p,n-i+1),0)$.

We can now prove an analog of [SS17, Proposition 5.13].

Proposition 7.4.15. *Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional and S finite. Let $\boldsymbol{\chi}$ be an atlas of (V,S) and let $i \in \{2,\ldots,(d+3)/2\}$. Write $W = W(\boldsymbol{\pi}_i, V)$ and assume that the following holds. Either W is empty or it is equidimensional of dimension $i-1$, with $\mathrm{sing}(W) \subset S$, and $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\pi}, i)$ is an atlas of (W,S).*

Let $L = (\Gamma, (1), \mathscr{S})$ be a Lagrange system such that $V = \overline{\mathscr{U}(L)}$ and $S = \mathsf{Z}(\mathscr{S})$. Let $\mathscr{Y} = (Y_1, \ldots, Y_r)$ be algebraic sets in $\mathbf{C}^n$ and let finally $\boldsymbol{\psi}$ be a global normal form for $(L; (W, \mathscr{Y}))$ such that $\boldsymbol{\chi}$ is the associated atlas of (V,S). There exists a non-empty Zariski open subset $\mathscr{I}(L, \boldsymbol{\psi}, \mathscr{Y})$ of $\mathbf{C}^p$ such that for all $\boldsymbol{u} \in \mathscr{I}(L, \boldsymbol{\psi}, \mathscr{Y}) \cap \mathbf{Q}^p$, the following holds:

- *$W_{\mathrm{lag}}(L, \boldsymbol{u}, i)$ is a Lagrange system that defines W;*
- *if $W \neq \emptyset$, then $(W_{\mathrm{lag}}(L, \boldsymbol{u}, i); \mathscr{Y})$ has a global normal form with atlas $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\pi}, i)$.*

Proof. The statement of this proposition is identical as [SS17, Proposition 5.13] except that, in [SS17, Proposition 5.13], our assumptions on W are replaced by a generic linear change of variables on V. [SS17, Proposition 5.13] claims the same statements on $V^{\boldsymbol{A}}$ where $\boldsymbol{A}$ is assumed to lie in a non-empty Zariski open set $\mathscr{G}_1(\boldsymbol{\chi}, V, \emptyset, S, i)$ defined in [SS17, Proposition 3.4].

In the proof of [SS17, Proposition 5.13], the fact that $\boldsymbol{A} \in \mathscr{G}_1(\boldsymbol{\chi}, V, \emptyset, S, i)$ allows to assume that the statements of [SS17, Proposition 3.4] but also [SS17, Lemma B.12] hold. In our proposition stated above, according to Lemma 7.2.12, the assumptions on W are exactly the statement of [SS17, Proposition 3.4], while [SS17, Lemma B.12] is nothing but a consequence of these facts. Therefore, under these assumptions, the proof of [SS17, Proposition 5.13] can be replicated, *mutatis mutandis*, for V instead of $V^{\boldsymbol{A}}$, and constitutes a valid proof for the above statement. □

7.4.3.c. Lagrange system for fibers

Definition 7.4.16. Let $L = (\Gamma, (1), \mathscr{S})$ be a Lagrange system of type $((n,0),(p,0),0)$ and let $e \in \{1,\ldots,n-p\}$. Let $\mathscr{Q}''$ be a zero-dimensional parametrization that encodes a finite set $Q'' \subset \mathbf{C}^e$ and let $\mathscr{S}''$ be a zero-dimensional parametrization that encodes a finite set $S'' \subset \mathbf{C}^n$ lying over Q''. We define $F_{\mathrm{lag}}(L, \mathscr{Q}'', \mathscr{S}'')$ as the triplet $(\Gamma, \mathscr{Q}'', \mathscr{S}'')$, it is a Lagrange system of type $((n,0),(p,0),e)$.

As in the previous paragraph, we state an analog of [SS17, Proposition 5.16] where we replaced the assumption of a generic linear change of variables, by the assumptions that such a change of variables allows to satisfy. In addition, we handle here the more general situation where, using the notation below, $W = W(\boldsymbol{\pi}_e, V^{\boldsymbol{\varphi}})$, as the case $W = W(\boldsymbol{\pi}_{e+1}, V^{\boldsymbol{\varphi}})$ considered in [SS17] can be deduced from the former.

Proposition 7.4.17. *Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional and S finite. Let $\boldsymbol{\chi}$ be an atlas of (V, S) and let $e \in \{2, \ldots, (d+3)/2\}$. Define $W = W(\boldsymbol{\pi}_e, V^{\boldsymbol{\varphi}})$ and let $\mathscr{Q}''$ and $\mathscr{S}''$ be zero-dimensional parametrizations with coefficients in $\mathbf{Q}$ that respectively encode a finite set $Q'' \subset \mathbf{C}^e$ and $S'' = S \cup W_{|\boldsymbol{\pi}_e \in Q''}$ and let $V'' = V_{|\boldsymbol{\pi}_e \in Q''}$. Assume that S'' is finite and, either V'' is empty or its is equidimensional of dimension $d - e$, with $\mathrm{sing}(V'')$ contained in S'', and $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \mathscr{Q}'', \boldsymbol{\pi})$ is an atlas of (V'', Q'', S'').*

Let $L = (\Gamma, (1), \mathscr{S})$ be a Lagrange system such that $V = \overline{\mathscr{W}(L)}$ and $S = \mathsf{Z}(\mathscr{S})$. Let $\mathscr{Y} = (Y_1, \ldots, Y_r)$ be algebraic sets in $\mathbf{C}^n$ and let finally $\boldsymbol{\psi}$ be a global normal form for $(L; (V'', \mathscr{Y}))$ such that $\boldsymbol{\chi}$ is the associated atlas of (V, S). Then the following holds:

- *$F_{\mathrm{lag}}(L, \mathscr{Q}'', \mathscr{S}'')$ is a Lagrange system that defines V'';*
- *if $V'' \neq \emptyset$, then the pair $(F_{\mathrm{lag}}(L, \mathscr{Q}'', \mathscr{S}''); \mathscr{Y})$ has a global normal form whose atlas is $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q'', S, \boldsymbol{\pi})$.*

Proof. As above the statement of this proposition is identical to the one in [SS17, Proposition 5.16] except that the assumptions on S'' and V'' are replaced by a generic change of variables on V. Indeed, [SS17, Proposition 5.16] claims the same statements, as we do, on $V^{\boldsymbol{A}}$ where $\boldsymbol{A}$ is assumed to lie in a non-empty Zariski open set $\mathscr{G}_3(\boldsymbol{\chi}, V, \emptyset, S, e)$ defined in [SS17, Proposition 3.7].

In the proof of [SS17, Proposition 5.17], the fact that $\boldsymbol{A} \in \mathscr{G}_3(\boldsymbol{\chi}, V, \emptyset, S, e)$ allows to assume that the statements of [SS17, Proposition 3.7] but also [SS17, Lemma C.1] hold. In the case of the proposition stated above, the assumptions on S'' and V'' are exactly the statement of [SS17, Proposition 3.7], while [SS17, Lemma C.1] is nothing but a consequence of these facts. Therefore, under these assumptions, the proof of [SS17, Proposition 5.17] can be replicated, *mutatis mutandis*, for V instead of $V^{\boldsymbol{A}}$, and constitutes a valid proof for the above statement. □

7.4.4 Proofs of Lemmas 7.3.4, 7.3.5, 7.3.6 and 7.3.7

As done in the paragraph 7.3.2.b, we fix $1 \leq c \leq n-1$ and we refer to the following objects:

- sequences of polynomials $\boldsymbol{g} = (g_1, \ldots, g_c)$ and $\boldsymbol{\varphi} = (\varphi_1, \varphi_2)$ in $\mathbf{Q}[\boldsymbol{X}]$, of maximal degrees D, such that $\boldsymbol{g}$ satisfies assumption A that is: $\boldsymbol{g}$ is a reduced regular sequence and $\mathrm{sing}(\boldsymbol{V}(\boldsymbol{g}))$ is finite;
- straight-line programs Γ and $\Gamma^{\boldsymbol{\varphi}}$, of respective lengths E and E', computing respectively $\boldsymbol{g}$ and $\boldsymbol{\varphi}$;
- the equidimensional algebraic set $V = \boldsymbol{V}(\boldsymbol{g})$, of dimension $d = n - c$, defined by $\boldsymbol{g}$;
- zero-dimensional parametrizations $\mathscr{S}$ and $\mathscr{Q}''$, of respective degrees σ and κ'', describing finite sets $S \subset \mathbf{C}^n$ and $Q'' \subset \mathbf{C}$, such that $\mathrm{sing}(V) \subset S$;
- an atlas $\boldsymbol{\chi}$ of (V, S), given by [SS17, Lemma A.13], as S is finite and contains $\mathrm{sing}(V)$.

Let $\Psi_{\boldsymbol{\varphi}}$ be the incidence isomorphism associated to $\boldsymbol{\varphi}$ and let $\boldsymbol{g}^{\boldsymbol{\varphi}}$ as defined in Lemma 7.4.4, so that $\widetilde{V} := \boldsymbol{V}(\boldsymbol{g}^{\boldsymbol{\varphi}}) = \Psi_{\boldsymbol{\varphi}}(V)$. According to Lemmas 7.4.4 and 7.4.5, $\widetilde{V} \subset \mathbf{C}^{2+n}$ is equidimensional with finitely many singular points.

Lemma 7.4.18. *Let $\mathscr{Y} = (Y_1, \ldots, Y_r)$ be algebraic sets in $\mathbf{C}^n$. There exists an algorithm such that, on input $\Gamma, \mathscr{S}$ and $\Gamma^{\boldsymbol{\varphi}}$, runs using at most $\widetilde{O}(E'\sigma)$ operations in $\mathbf{Q}$, and outputs*

- *$\widetilde{\Gamma}$, a straight-line program of length $E + E' + 2$, computing $\boldsymbol{g}^{\boldsymbol{\varphi}}$,*
- *$\widetilde{\mathscr{S}}$, a zero-dimensional parametrization of degree σ, encoding $\widetilde{S} = \Psi_{\boldsymbol{\varphi}}(S)$,*

such that the following holds. The Lagrange system $\widetilde{L} = (\widetilde{\Gamma}, (1), \widetilde{\mathscr{S}})$ of type $((2+n, 0), (2+c, 0), 0)$ defines $\widetilde{V}$, and $(\widetilde{L}, \mathscr{Y})$ has a global normal form.

Proof. By Lemmas 7.4.1 and 7.4.3, there exist algorithms IncSLP and IncParam respectively, which, on input $\Gamma, \mathscr{S}$ and $\Gamma^{\boldsymbol{\varphi}}$, output $\widetilde{\Gamma}$ and $\widetilde{\mathscr{S}}$ as described in the statement, using at most $\widetilde{O}(E'\sigma)$ operations in $\mathbf{Q}$. Let $\widetilde{L} = (\widetilde{\Gamma}, (1), \widetilde{\mathscr{S}})$. By Lemma 7.4.4, $\boldsymbol{g}^{\boldsymbol{\varphi}}$ is a reduced regular sequence as $\boldsymbol{g}$ is. Then, according to [SS17, Proposition 5.10], $\widetilde{L}$ defines a Lagrange system that defines $\widetilde{V}$ and $\boldsymbol{\psi} = ((1, 1, \boldsymbol{g}^{\boldsymbol{\varphi}}, \boldsymbol{g}^{\boldsymbol{\varphi}}))$ is a global normal form of $(\widetilde{L}, \mathscr{Y})$. □

We deduce an algorithm for computing critical points on V.

Proof of Lemma 7.3.4. By Lemmas 7.4.4, 7.4.2 and 7.4.5, $W_{\boldsymbol{\varphi}}(1, V)$ can be obtained by projecting the incidence polar variety $W(\boldsymbol{\pi}_1, \widetilde{V})$ on the last n coordinates. Computing a parametrization of the latter set can then be done using the algorithm W_1 of [SS17, Proposition 6.3] on the Lagrange system given by [SS17, Proposition 5.10].

According to Lemma 7.4.18, we can compute a Lagrange system $\widetilde{L}$ of type $((2+n, 0), (2+c, 0), 0)$, with the global normal form property, that defines $\widetilde{V}$. Hence, by [SS17, Proposition 6.4], there exists a Monte Carlo algorithm W_1 which, on input $\widetilde{L}$, either fails or returns a zero-dimensional parametrization $\widetilde{\mathscr{W}_1}$ which described it using at most

$$\widetilde{O}\left((E+E')(n+2)^{4d+8} D^{2n+3} (D-1)^{2d} + n\sigma^2\right)$$

operations in $\mathbf{Q}$. Moreover, in case of success, $\widetilde{\mathscr{W}_1}$ describes $W(\boldsymbol{\pi}_1, \widetilde{V}) - \widetilde{S}$, with the notation of Lemma 7.4.18. Besides, by [SS17, Proposition I.1] (or [SS18, Proposition 3]) the degree of $K(\boldsymbol{\pi}_1, \widetilde{V})$ is upper bounded by

$$\tbinom{n+1}{c+1} D^{c+2} (D-1)^d = \tbinom{n+1}{d} D^{c+2} (D-1)^d.$$

Finally, by Lemma 7.4.5, $W_{\boldsymbol{\varphi}}(1, V)$ can be obtained by projecting $W(\boldsymbol{\pi}_1, \widetilde{V})$ on the last n coordinates and taking the union with S. This is done by performing the subroutines Projection and Union [SS17, Lemma J.3 and J.5] which uses at most

$$\widetilde{O}\left(n^2 \tbinom{n+1}{c+1}^2 D^{2c+4} (D-1)^{2d} + n\sigma^2\right)$$

operations in $\mathbf{Q}$. □

In the following, we consider the polar varieties $W = W_{\boldsymbol{\varphi}}(2, V)$ and $\widetilde{W} = W(\boldsymbol{\pi}_2, \widetilde{V})$ so that, by Lemma 7.4.5, $\widetilde{W} = \Psi_{\boldsymbol{\varphi}}(W)$.

Lemma 7.4.19. *Let $\mathscr{Y} = (Y_1, \ldots, Y_r)$ be algebraic sets in $\mathbf{C}^n$. There exists a Monte Carlo algorithm which, on input $\Gamma, \mathscr{S}$ and $\Gamma^{\boldsymbol{\varphi}}$, runs using at most $\widetilde{O}\left(E'\sigma + n(E+E')\right)$ operations in $\mathbf{Q}$, and outputs a Lagrange system $\widetilde{L_W}$ of type*

$$\big((2+n,\ 2+c),\ (2+c,\ n+1),\ 0\big).$$

Either W is empty or assume that W is 1-equidimensional, with $\mathrm{sing}(W) \subset S$, and in addition that $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, 2)$ is an atlas of (W, S). Then, in case of success, $\widetilde{L_W}$ defines $W(\boldsymbol{\pi}_2, \widetilde{V})$ and $(\widetilde{L_W}, \mathscr{Y})$ has a global normal form.

Proof. According to Lemma 7.4.18, one can compute, using $\widetilde{O}\left(E'\sigma\right)$ operations in $\mathbf{Q}$, a Lagrange system $\widetilde{L}$ of type $((2+n, 0), (2+c, 0), 0)$, defining $\widetilde{V}$, and such that $(\widetilde{L}, (\widetilde{W}, \mathscr{Y}))$ has a global normal form $\boldsymbol{\psi}$.

Let $\boldsymbol{u}$ be an arbitrary element of $\mathbf{Q}^{c+2}$, such an element can be provided by the procedure Random we mentioned in Subsection 7.3.3. Let $\widetilde{L_W} = W_{\text{Lagrange}}(\widetilde{L}, \boldsymbol{u}, 2)$, according to Definition 7.4.14, $\widetilde{L_W}$ is a Lagrange system of type

$$\big((2+n,\ 2+c),\ (2+c,\ n+1),\ 0\big).$$

Computing $\widetilde{L_W}$ boils down to apply Baur-Strassen's algorithm [BS83] to obtain a straight-line program evaluating the Jacobian matrix associated to $\boldsymbol{g}, \boldsymbol{\varphi}$ as in the proof of [SS17, Lemma O.1].

By assumption, either W is empty, and so is $\widetilde{W}$, or W is equidimensional of dimension 1, with $\mathrm{sing}(W) \subset S$. Then, by Lemma 7.4.5, $\widetilde{W}$ is equidimensional of dimension 1, with $\mathrm{sing}(\widetilde{W}) \subset \Psi_{\boldsymbol{\varphi}}(S) = \widetilde{S}$. Moreover, as $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, 2)$ is an atlas of (W, S) then, by Lemma 7.4.7, $W_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, \widetilde{V}, \widetilde{S}, \boldsymbol{\pi}, 2)$ is an atlas of $(\widetilde{W}, \widetilde{S})$.

Therefore, by Proposition 7.4.15, there exists a non-empty Zariski open subset $\mathscr{I}(\widetilde{L}, \boldsymbol{\psi}, \mathscr{Y})$ of $\mathbf{C}^p$ such that, if $\boldsymbol{u} \in \mathscr{I}(\widetilde{L}, \boldsymbol{\psi}, \mathscr{Y})$ then, either $\widetilde{W} \neq \emptyset$ or $(\widetilde{L_W}, \mathscr{Y})$ admits a global normal form. In both cases, $\widetilde{L_W}$ is a Lagrange system that defines $\widetilde{W}$. □

Proof of Lemma 7.3.5. According to Lemmas 7.4.4, 7.4.2 and 7.4.5, $W_{\boldsymbol{\varphi}}(2, V)$ can be obtained by projecting the incidence polar variety $W(\boldsymbol{\pi}_2, \widetilde{V})$ on the last n coordinates. Computing a parametrization of the latter set can then be done using the algorithm SolveLagrange of [SS17, Proposition 6.3] on the Lagrange system given by Proposition 7.4.15.

By Lemma 7.4.19, we can compute a Lagrange system $\widetilde{L_W}$ defining $W(\boldsymbol{\pi}_2, \widetilde{V})$, that admits a global normal form. Then, by [SS17, Proposition 6.3], there exists a Monte Carlo algorithm SolveLagrange which, on input $\widetilde{L_W}$, either fails or returns a one-dimensional parametrization $\widetilde{\mathscr{W}}$ of degree at most

$$\delta = (n+c+4)D^{c+2}(D-1)^d(c+2)^d,$$

describing $\overline{\mathscr{U}(\widetilde{L_W})}$, which is exactly $\widetilde{W}$ by Proposition 7.4.15. Moreover, by [SS17, Proposition 6.3], the execution of SolveLagrange uses at most

$$\widetilde{O}\left((n+c)^3(E+E'+(n+c)^3)D\delta^3 + (n+c)\delta\sigma^2\right)$$

operations in $\mathbf{Q}$. Finally, by Lemma 7.4.5, W can be obtained by projecting $\widetilde{W}$ on the last n coordinates. Hence, running Projection, with input $\widetilde{\mathscr{W}}$ and n, we get a one-dimensional parametrization $\mathscr{W}$, of degree at most δ, encoding W. According to [SS17, Lemma J.9.], the latter operation costs at most $\widetilde{O}\left(n^2\delta^3\right)$ operations in $\mathbf{Q}$. □

Proof of Lemma 7.3.6. By Lemma 7.4.19, we can compute a Lagrange system $\widetilde{L_W}$ defining $W(\boldsymbol{\pi}_2, \widetilde{V})$, such that $(\widetilde{L_W}; W(\boldsymbol{\pi}_1, \widetilde{W}))$ has the global normal form property. Hence, by [SS17, Proposition 6.4], there exists a Monte Carlo algorithm W_1 which, on input $\widetilde{L_W}$, either fails or returns a zero-dimensional parametrization $\widetilde{\mathscr{K}}$ of degree at most $\delta(n+c)D$, where

$$\delta = (n+c+4)D^{c+2}(D-1)^d(c+2)^d,$$

describing $W(\boldsymbol{\pi}_1, \overline{\widetilde{\mathscr{U}}(\widetilde{L_W})}) - \widetilde{S}$, which is exactly $W(\boldsymbol{\pi}_1, \widetilde{W}) - \widetilde{S}$ by Proposition 7.4.15. Moreover, by [SS17, Proposition 6.3], the execution of W_1 uses at most

$$\widetilde{O}\left((n+c)^{12}(E+E')D^3\delta^2 + (n+c)\sigma^2\right)$$

operations in $\mathbf{Q}$. Finally, by Lemma 7.4.5, $W_{\boldsymbol{\varphi}}(1, W)$ can be obtained by projecting $W(\boldsymbol{\pi}_1, \widetilde{W})$ on the last n coordinates and taking the union with S. This is done, using the subroutines Projection and Union which, according to [SS17, Lemma J.3 and J.5], use at most $\widetilde{O}\left((n+c)^4D^2\delta^2 + n\sigma^2\right)$ operations in $\mathbf{Q}$. □

Proof of Lemma 7.3.7. By Lemma 7.4.19, we can compute a Lagrange system $\widetilde{L_W}$ defining $W(\boldsymbol{\pi}_2, \widetilde{V})$, such that $(\widetilde{L_W}; \widetilde{W} \cap \boldsymbol{\pi}_1^{-1}(\widetilde{Q''}))$ has the global normal form property. Hence, by [SS17, Proposition 6.5], there exists a Monte Carlo algorithm Fiber which, on input $\widetilde{L_W}$, either fails or returns a zero-dimensional parametrization $\widetilde{\mathscr{F}}$ of degree at most $\kappa''\delta$ where

$$\delta = (n+c+4)D^{c+2}(D-1)^d(c+2)^d,$$

describing $[\overline{\widetilde{\mathscr{U}}(\widetilde{L_W})} \cap \boldsymbol{\pi}_1^{-1}(\widetilde{Q''})] - \widetilde{S}$, which is exactly $[\widetilde{W} \cap \boldsymbol{\pi}_1^{-1}(\widetilde{Q''})] - \widetilde{S}$ by Proposition 7.4.15. Moreover, by [SS17, Proposition 6.3], the execution of FiberPolar uses at most

$$\widetilde{O}\left((n+c)^4\left[E+E'+(n+c)^2\right]D(\kappa'')^2\delta^2 + (n+c)\sigma^2\right)$$

operations in $\mathbf{Q}$,according to [SS17, Definition 6.1]. Finally, by Lemma 7.4.5, $W \cap \boldsymbol{\varphi}_1^{-1}(Q'')$ can be obtained by projecting $\widetilde{W} \cap \boldsymbol{\pi}_1^{-1}(\widetilde{Q''})$ on the last n coordinates and taking the union with S.. This is done, using the subroutines Projection and Union which, according to [SS17, Lemma J.3 and J.5], use at most $\widetilde{O}\left((n+c)^2(\kappa'')^2\delta^2 + n\sigma^2\right)$ operations. □

7.4.5 Proof of Proposition 7.3.8

This paragraph is devoted to prove Proposition 7.3.8. We recall its statement below.

Proposition (7.3.8)**.** *Let Γ and $\Gamma^{\boldsymbol{\varphi}}$ be straight-line programs, of respective length E and E', computing respectively polynomials $\boldsymbol{g} = (g_1, \ldots, g_p)$ and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n)$ in $\mathbf{Q}[x_1, \ldots, x_n]$,*

of degrees bounded by D. Assume that $\boldsymbol{g}$ satisfies (A). *Let $\mathscr{Q}$ and $\mathscr{S}_Q$ be zero-dimensional parametrizations of respective degrees κ and σ that encode finite sets $Q \subset \mathbf{C}^e$ (for some $0 < e \leq n$) and $S_Q \subset \mathbf{C}^n$, respectively. Let $V = \boldsymbol{V}(\boldsymbol{g})$ and $F_Q = V_{|\boldsymbol{\varphi}_e \in Q}$, and assume that*

- *F_Q is equidimensional of dimension $d - e$, where $d = n - p$;*
- *$F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, \boldsymbol{\varphi})$ is an atlas of (F_Q, S_Q), and $\mathrm{sing}(F_Q) \subset S_Q$;*
- *the real algebraic set $F_Q \cap \mathbf{R}^n$ is bounded.*

Consider additionally a zero-dimensional parametrization $\mathscr{P}$ of degree μ encoding a finite subset $\mathcal{P}$ of F_Q, which contains S_Q. Assume that $\sigma \leq ((n+e)D)^{n+e}$.

There exists a probabilistic algorithm RoadmapBounded which takes as input the pair $((\Gamma, \Gamma^{\boldsymbol{\varphi}}, \mathscr{Q}, \mathscr{S}), \mathscr{P})$ and which, in case of success, outputs a roadmap of $(F_Q, \mathcal{P})$, of degree

$$\widetilde{O}\left((\mu+\kappa)16^{3d_F}(n_F \log_2(n_F))^{2(2d_F+12\log_2(d_F))(\log_2(d_F)+5)} D^{(2n_F+1)(\log_2(d_F)+3)}\right),$$

where $n_F = n + e$ and $d_F = d - e$, and using

$$\widetilde{O}\left((\mu+\kappa)^3 16^{9d_F}(E+E'+e)(n_F \log_2(n_F))^{6(2d_F+12\log_2(d_F))(\log_2(d_F)+6)} D^{3(2n_F+1)(\log_2(d_F)+4)}\right)$$

arithmetic operations in $\mathbf{Q}$.

We start by proving a variant of this result for when $\boldsymbol{\varphi}$ encodes projections. Then, using incidence varieties and the associated subroutines, we will generalize it to arbitrary polynomial maps.

7.4.5.a. The particular case of projections

We study here, the call to the algorithm RoadmapRecLagrange from [SS17, Sec. 7.1]. It takes as input a Lagrange system $L_\rho = (\Gamma_\rho, \mathscr{Q}_\rho, \mathscr{S}_\rho)$ having the global normal form property, and where $\mathsf{Z}(\mathscr{Q})$ is not empty. The following proposition ensures the correction of such a call and describes the related complexity, with respect to [SS17]. Let $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$, where $m \geq 0$, be new indeterminates.

Proposition 7.4.20. *Let $\boldsymbol{f} = (f_1, \ldots, f_{p_\rho}) \subset \mathbf{Q}[\mathfrak{x}_1, \ldots, \mathfrak{x}_m]$ be given by a straight-line program Γ_ρ of length E_ρ with $\deg(f_i) \leq D$ for $1 \leq i \leq p_\rho$, let $\mathscr{Q}_\rho$ and $\mathscr{S}_\rho$ be zero-dimensional parametrizations which have respective degrees κ_ρ and σ_ρ and encode finitely many points in respectively $\mathbf{C}^{e_\rho}$ (for some $e_\rho > 0$) and in $\mathbf{C}^m$. Assume that the Lagrange system $L_\rho = (\Gamma_\rho, \mathscr{Q}_\rho, \mathscr{S}_\rho)$ has the global normal form property. Let $d_\rho = m - p_\rho - e_\rho$, hence the dimension of $V(\Gamma_\rho)_{|\boldsymbol{\pi}_{e_\rho} \in \mathsf{Z}(\mathscr{Q}_\rho)}$.*

Consider a zero-dimensional parametrization $\mathscr{P}_\rho$ of degree μ_ρ such that $\mathsf{Z}(\mathscr{P}_\rho)$ is a finite subset of $V(\Gamma_\rho)_{|\boldsymbol{\pi}_{e_\rho} \in \mathsf{Z}(\mathscr{Q}_\rho)}$ which contains $\mathsf{Z}(\mathscr{S}_\rho)$. Assume that $\sigma_\rho \leq (mD)^m$.

There exists a Monte Carlo algorithm RoadmapBounded which takes as input the pair $((\Gamma_\rho, \mathscr{Q}_\rho, \mathscr{S}_\rho), \mathscr{P}_\rho)$ and which, in case of success, outputs a roadmap for $(V(\Gamma_\rho)_{|\boldsymbol{\pi}_{e_\rho} \in \mathsf{Z}(\mathscr{Q}_\rho)}, \mathscr{P}_\rho)$ of degree

$$\widetilde{O}\left((\mu_\rho+\kappa_\rho)16^{3d_\rho}(m\log_2(m))^{2(2d+12\log_2(d_\rho))(\log_2(d_\rho)+5)} D^{(2m+1)(\log_2(d_\rho)+3)}\right)$$

using

$$O^{\sim}\Big((\mu_\rho+\kappa_\rho)^3 16^{9d_\rho} E_\rho (m\log_2(m))^{6(2d+12\log_2(d_\rho))(\log_2(d_\rho)+6)} D^{3(2m+1)(\log_2(d_\rho)+4)}\Big)$$

arithmetic operations in $\mathbf{Q}$.

Proof. Since, by assumption, L_ρ has the global normal form property, one can call the algorithm RoadmapRecLagrange from [SS17, Sec. 7.1] on input $L_\rho = (\Gamma_\rho, \mathscr{Q}_\rho, \mathscr{S}_\rho)$ and $\mathscr{P}_\rho$. This algorithm computes data-structures, which are called generalized Lagrange systems, that encode:

- a polar variety in $V(\Gamma_\rho)_{|\boldsymbol{\pi}_{e_\rho}\in \mathsf{Z}(\mathscr{Q}_\rho)}$ of dimension $\widetilde{d}-1 \simeq d_\rho/2$ for $\widetilde{d} = \lfloor \frac{d_\rho+3}{2} \rfloor$;
- appropriate fibers in $V(\Gamma_\rho)_{|\boldsymbol{\pi}_{e_\rho}\in \mathsf{Z}(\mathscr{Q}_\rho)}$ of dimension $d_\rho - (\widetilde{d}-1) \simeq d_\rho/2$.

A generalized Lagrange system (see [SS17, Def. 5.3]) is encoded by a triplet $L = (\Gamma, \mathscr{Q}, \mathscr{S})$ such that Γ is a straight-line program that evaluates some polynomials $\boldsymbol{F} = (\boldsymbol{f}, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_s)$ where

- $\boldsymbol{f}$ lies in $\mathbf{Q}[\mathfrak{X}]$, with $\mathfrak{X} = (\mathfrak{x}_1, \ldots, \mathfrak{x}_m)$;
- $\boldsymbol{f}_i$ lies in $\mathbf{Q}[\mathfrak{X}, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_i]$ and has length p_i, where the $\boldsymbol{L}_j$'s are sequences of extra variables of length m_j (these are called blocks of Lagrange multipliers);
- for any $f_{i,j}$ in $\boldsymbol{f}_i$, the degree of $f_{i,j}$ in $\boldsymbol{L}_j$ is at most 1 for $1 \le i \le p_i$ and $1 \le j \le i$.

Also, $\mathscr{Q}$ (resp. $\mathscr{S}$) is a zero-dimensional parametrization encoding points in $\mathbf{C}^e$ (resp. $\mathbf{C}^m$).

The algebraic set of $\mathbf{C}^m$ defined by $L = (\Gamma, \mathscr{Q}, \mathscr{S})$ is the Zariski closure of the projection on the $\mathfrak{X}$-space of $V(\boldsymbol{F})_{|\boldsymbol{\pi}_{\mathfrak{X},e}\in \mathsf{Z}(\mathscr{Q})} \setminus \pi_{\mathfrak{X}}^{-1}(\mathsf{Z}(\mathscr{S}))$.

Short description of RoadmapRecLagrange. From a generalized Lagrange system L satisfying the global normal form property and encoding some algebraic set X, one can build a generalized Lagrange system encoding a polar variety W over X using [SS17, Def 5.11 and Prop. 5.13], which satisfies the global normal form property, up to some generic enough linear change of coordinates and some restriction on the dimension of W. Additionally, given finitely many base points $Q' \subset \mathbf{C}^{e'}$ encoded by a zero-dimensional parametrization $\mathscr{Q}'$, [SS17, Def. 5.14 and Prop. 5.16] show how to deduce from L and $\mathscr{Q}'$ a generalized Lagrange system for $X_{|\boldsymbol{\pi}_{e'}\in Q'}$ satisfying the global normal form property, again assuming the coordinate system is generic enough.

Maintaining the global normal form property allows us to call recursively the procedure RoadmapRecLagrange. All in all, these computations are organised in a binary tree $\mathcal{T}$, whose root is denoted by ρ. Each child node τ encodes computations performed by a recursive call with input some generalized Lagrange system $L_\tau = (\Gamma_\tau, \mathscr{Q}_\tau, \mathscr{S}_\tau)$ and some zero-dimensional parametrization $\mathscr{P}_\tau$ encoding some control points. Both L_τ and $\mathscr{P}_\tau$ have been computed by the parent node. Correctness is proved in [SS17, Sec. N.3]. Further, we denote by κ_τ, σ_τ and μ_τ the respective degrees of $\mathscr{Q}_\tau$, $\mathscr{S}_\tau$ and $\mathscr{P}_\tau$.

The dimension of $\mathcal{V}(L_\tau)$ is denoted by d_τ. Calling RoadmapRecLagrange, with input L_τ sets $\widetilde{d}_\tau = \lfloor \frac{d_\tau+3}{2} \rfloor$ and computes

(a) a generalized Lagrange system L'_τ encoding the polar variety $W = W(e_\tau, d'_\tau, \mathcal{V}(L_\tau)^{\boldsymbol{A}})$, where $\boldsymbol{A}$ is randomly chosen;

(b) a zero-dimensional parametrization $\mathscr{B}_\tau$ which encodes the union of $W(e_\tau, 1, W)$ with $\mathsf{Z}(\mathscr{P})^{\boldsymbol{A}}$; we denote its degree by β_τ; note that by construction (see [SS17,], $\mathsf{Z}(\mathscr{B}_\tau)$ contains $\mathsf{Z}(\mathscr{S}_\tau)$);

(c) a zero-dimensional parametrization $\mathscr{Q}''_\tau$ which encodes the projection of $\mathscr{B}_\tau$ on the e''_τ first coordinates (with $e''_\tau = e_\tau + \widetilde{d}_\tau - 1$); we denote its degree by κ''_τ;

(d) a zero-dimensional parametrization $\mathscr{P}'_\tau$ encoding $\mathsf{Z}(\mathscr{P}_\tau)^{\boldsymbol{A}} \cup Y_\tau$ with

$$Y_\tau = V(\mathcal{V}(L'_\tau))_{|\boldsymbol{\pi}_{e''_\tau} \in \mathsf{Z}(\mathscr{Q}''_\tau)}$$

and a zero-dimensional parametrization and $\mathscr{P}''_\tau$ which encodes those points of $\mathsf{Z}(\mathscr{P}'_\tau)$ which project on $\mathsf{Z}(\mathscr{Q}''_\tau)$; further we denote their degrees by μ'_τ and μ''_τ, the degree of Y_τ will be denoted by γ_τ;

(e) zero-dimensional parametrizations $\mathscr{S}'_\tau$ and $\mathscr{S}''_\tau$ of respective degrees σ'_τ and σ''_τ which do encode $\mathsf{Z}(\mathscr{S}_\tau)^{\boldsymbol{A}} \cup Y_\tau$ and those points of $\mathsf{Z}(\mathscr{S}''_\tau)$ which project on $\mathsf{Z}(\mathscr{Q}''_\tau)$; note that by construction, $\mathsf{Z}(\mathscr{S}'_\tau)$ and $\mathsf{Z}(\mathscr{S}''_\tau)$ are contained in $\mathsf{Z}(\mathscr{P}'_\tau)$ and $\mathsf{Z}(\mathscr{P}''_\tau)$ respectively;

(f) and, finally, a generalized Lagrange system L''_τ which encodes $\mathcal{V}(L_\tau)_{|\boldsymbol{\pi}_{e''_\tau} \in \mathsf{Z}(\mathscr{Q}''_\tau)}$.

The recursive calls of RoadmapRecLagrange are then performed on $(L'_\tau, \mathscr{P}'_\tau)$ and $(L''_\tau, \mathscr{P}''_\tau)$.

For a given generalized Lagrange system L_τ corresponding to some node τ, the number of blocks of Lagrange multipliers is denoted by k_τ. The total number of variables (resp. polynomials) lying in $\mathbf{Q}[\mathfrak{X}, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_i]$ for $i \leq k_\tau$ is denoted by $M_{i,\tau}$ (resp. $P_{i,\tau}$). By construction, for $i = 0$, we have $P_{0,\tau} = p_\rho$. For $i = k_\tau$, we denote $M_{k_\tau,\tau}$ (resp. $P_{k_\tau,\tau}$) by M_τ (resp. P_τ).

As in [SS17, Sec. 6.1], we attach to each such generalized Lagrange system the quantity

$$\delta_\tau = (P_\tau + 1)^{k_\tau} D^p (D-1)^{m - e_\tau - p_\rho} \prod_{i=0}^{k_\tau - 1} M_{i+1,\tau}^{M_{i,\tau} - e_\tau - P_{i,\tau}}.$$

We establish below that the degree of $\mathcal{V}(L_\tau)$ is bounded by $\kappa_\tau \delta_\tau$.

Complexity analysis. The complexity of RoadmapRecLagrange is analysed in [SS17, Sec. O], assuming that $e_\rho = 0$ (see [SS17, Prop. O.7]). This is done by proceeding in two steps:

- *Step (i)* proves some elementary bounds on the number of variables and polynomials (the m_i's and the p_i's) involved in the data-structures encoding these polar varieties and fibers in the recursive calls (see [SS17, Sec. O.1]);
- *Step (ii)* proves uniform degree bounds for the parametrizations $\mathscr{P}'_\tau, \mathscr{P}''_\tau, \mathscr{B}_\tau, \mathscr{Q}'_\tau, \mathscr{Q}''_\tau$, as well as $\mathscr{S}'_\tau, \mathscr{S}''_\tau$ where τ ranges over all nodes of the binary tree $\mathcal{T}$. Uniform degree bounds are also given for all $\mathcal{V}(L_\tau)$.

These degree bounds are used in combination with the complexity estimates of [SS17, Sec. 6.2] for solving generalized Lagrange systems and [SS17, Sec. J.1 and J.2] which do depend polynomially on these bounds and the ones established in *(i)*.

Since the total number of nodes is $O(m)$, it suffices to take m times the sum of all costs established by *(ii)*. Hereafter, we slightly extend this analysis when $e_\rho > 0$, following the same reasoning, which we recall step by step by highlighting the main (and tiny) differences.

Step (i). We start with step *(i)*. Both [SS17, Lemma O.1] and [SS17, Lemma O.2] control the lengths of the straight-line programs, the numbers of blocks of Lagrange multipliers and their lengths, as well as the numbers of polynomials and total number of variables remain valid, assuming $e_\rho = 0$. Their proofs are based on how these quantity evolve when building generalized Lagrange systems encoding polar varieties and fibers (see [SS17, Lemmas 5.12 and 5.15]). This is not changed in our context where the initial call to RoadmapRecLagrange is done with some base points $\mathsf{Z}(\mathscr{Q}_\rho)$ with $e_\rho > 0$ because for each note τ, we take $\widetilde{d}_\tau = \lfloor \frac{d_\tau+3}{2} \rfloor$ as in [SS17]. This implies that the conclusions of [SS17, Lemma O.1] and [SS17, Lemma O.2] still hold when taking $d_\rho = m - p_\rho - e_\rho$.

All in all, we deduce that:

- the maximum number of blocks of Lagrange multipliers and the depth of $\mathcal{T}$ are bounded by $\lceil \log_2(d_\rho) \rceil$
- All straight-line programs have length bounded by $4m^{4+2\log_2(d_\rho)}(E_\rho + m^4)$
- the total number of variables for the generalized Lagrange system L_τ is bounded by $(m^2)^{\frac{d_\rho}{h_\tau}+1}$ where h_τ is the height of the node τ.

Step (ii). We can now investigate Step *(ii)*. The two main quantities to consider are

$$\boldsymbol{\delta} = 16^{d_\rho+2} m^{2d_\rho+12\log_2(d_\rho)} D^m$$

and

$$\boldsymbol{\zeta} = (\mu_\rho + \kappa_\rho) 16^{2(d_\rho+3)} (m\log_2(m))^{2(2d_\rho+12\log_2(d_\rho))} D^{(2m+1)(\log_2(d_\rho+2))}.$$

The first step is to prove that for any node τ, the degree of $\mathcal{V}(L_\tau)$ is dominated by $\kappa_\tau \boldsymbol{\delta}$. Using the global normal form property, [SS17, Prop. 5.13 and 6.2] prove that the degree of $\mathcal{V}(L_\tau)$ is upper bounded by $\kappa_\tau \delta_\tau$. Recall that, by definition,

$$\delta_\tau = (P_\tau + 1)^{k_\tau} D^p (D-1)^{m-e_\tau-p_\rho} \prod_{i=0}^{k_\tau-1} M_{i+1,\tau}^{M_{i,\tau}-e_\tau-P_{i,\tau}}.$$

[SS17, Lemma O.4] shows that the above left-hand side quantity is dominated by $\boldsymbol{\delta}$, using the results of Step *(i)* which we proved to still hold. We then deduce that the degree of $\mathcal{V}(L_\tau)$ is upper bounded by $\kappa_\tau \boldsymbol{\delta}$.

[SS17, Lemma O.5] establishes recurrence formulas for the quantities β_τ, γ_τ, $\mu_\tau + \kappa_\tau$ and σ_τ when τ ranges in the set of nodes of the binary tree $\mathcal{T}$. It states that, letting τ' and τ'' be the two children of τ, β_τ, γ_τ, $\mu_{\tau'} + \kappa_{\tau'}$, $\mu_{\tau''} + \kappa_{\tau''}$, $\sigma_{\tau'}$ and $\sigma_{\tau''}$ are bounded above by $2\boldsymbol{\delta}^2 \zeta_\tau (\mu_\tau + \kappa_\tau)$ where $\zeta_\tau = \left(m^2 \log_2(m) D\right)^{\frac{d_\rho}{2^{h_\tau}}+1}$ (here h_τ is the height of τ) in the context

of [SS17] with $e_\rho = 0$ and assuming that $\mathsf{Z}(\mathscr{S}_\tau)$ is contained in $\mathsf{Z}(\mathscr{P}_\tau)$ for any node τ of $\mathcal{T}$ (this is used to prove the statements on $\sigma_\tau, \sigma_{\tau'}$ and $\sigma_{\tau''}$). In the context of [SS17], we have $\mathsf{Z}(\mathscr{S}_\rho) = \emptyset$. In our context, we still take $\widetilde{d}_\tau = \lfloor \frac{d_\tau+3}{2} \rfloor$ as in [SS17], hence the structure of our binary tree $\mathcal{T}$ is the same as the one in [SS17]. Also we assume that $\mathsf{Z}(\mathscr{S}_\rho)$ is contained in $\mathsf{Z}(\mathscr{P}_\tau)$ and that its degree is bounded by $(mD)^m$. This is enough to transpose the recursion performed in the proof of [SS17, Lemma O.5 and Prop.O.3] and deduce that μ_τ, κ_τ and σ_τ are bounded by ζ when τ ranges over the set of nodes of $\mathcal{T}$.

The runtime estimates in [SS17, Sec. O.3] to compute the parametrizations and generalized Lagrange systems in steps (a) to (f) above are then the same (they depend on δ, ζ and the above bounds on deduced at Step *(i)*). The statements of [SS17, Lemmas O.8, O.9, O.10 and O.11] can then be applied here *mutatis mutandis* which, as in [SS17, Sec. O.3], allow us to deduce the same statement as [SS17, Prop. O.7], i.e. that the total runtime lies in

$$\mathcal{O}\Big((\mu_\rho + \kappa_\rho)^3 16^{9d_\rho} E_\rho (m \log_2(m))^{6(2d+12\log_2(d_\rho))(\log_2(d_\rho)+6)} D^{3(2m+1)(\log_2(d_\rho)+4)}\Big)$$

and outputs a roadmap of degree in

$$\mathcal{O}\Big((\mu_\rho + \kappa_\rho) 16^{3d_\rho} (m \log_2(m))^{2(2d+12\log_2(d_\rho))(\log_2(d_\rho)+5)} D^{(2m+1)(\log_2(d_\rho)+3)}\Big).$$

□

7.4.5.b. Proof of Proposition 7.3.8

To prove Proposition 7.3.8, we now show how to return to the case of projections from the general one, before calling the procedure RoadmapRecLagrange, whose complexity is analysed in Proposition 7.4.20.

Consider the notations introduced in the statement of the proposition. In the following let $\Psi_{\boldsymbol{\varphi}_e}$ be the incidence isomorphism associated to $\boldsymbol{\varphi}_e$ and let $\boldsymbol{g}^{\boldsymbol{\varphi}_e}$ as defined in Lemma 7.4.4, so that $\widetilde{V} := \boldsymbol{V}(\boldsymbol{g}^{\boldsymbol{\varphi}_e}) = \Psi_{\boldsymbol{\varphi}_e}(V)$. According to Lemma 7.4.4 and 7.4.5, $\widetilde{V} \subset \mathbf{C}^{e+n}$ is equidimensional with finitely many singular points. Additionally, let $\widetilde{F_Q} = \Psi_{\boldsymbol{\varphi}_e}(F_Q)$ and $\widetilde{S_Q} = \Psi_{\boldsymbol{\varphi}_e}(S_Q)$, so that $\widetilde{F_Q} = \widetilde{V}_{|\boldsymbol{\pi}_e \in Q}$, according to Lemma 7.4.2

Lemma 7.4.21. *There exists an algorithm such that, on input Γ, $\Gamma^{\boldsymbol{\varphi}}$, $\mathscr{Q}$ and $\mathscr{S}$ as above, runs using at most $\widetilde{O}(E'\sigma)$ operations in $\mathbf{Q}$, and outputs a Lagrange system $\widetilde{L_F}$ of type*

$$\big((e+n,0),\ (e+c,0),\ e\big).$$

Under the assumptions of Proposition 7.3.8, $\widetilde{L_F}$ has a global normal form, and defines $\widetilde{F_Q}$.

Proof. According to Lemma 7.4.18, we can compute a Lagrange system $\widetilde{L}$ of type $((e+n,0),(e+c,0),0)$, with the global normal form property, that defines $\widetilde{V}$. Let $\widetilde{L_F} = F_{\mathrm{lag}}(\widetilde{L}, \mathscr{Q}, \mathscr{S})$, as defined in Definition 7.4.16, it is a Lagrange system of type

$$\big((\,(e+n,0),\ (e+c,0),\ e\,).$$

By assumptions of Proposition 7.3.8, either F_Q is empty, and so is $\widetilde{F_Q}$, or F_Q is equidimensional of dimension $d-e$, with $\mathrm{sing}(F_Q) \subset S_Q$. Then, by Lemma 7.4.5, $\widetilde{F_Q}$ is

equidimensional of dimension $d-e$, with $\operatorname{sing}(\widetilde{F_Q}) \subset \Psi_{\boldsymbol{\varphi}}(S_Q) = \widetilde{S_Q}$. Moreover, as $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S_Q, \boldsymbol{\varphi})$ is an atlas of (F_Q, S_Q) then, by Lemma 7.4.8, $F_{\mathrm{atlas}}(\boldsymbol{\chi}^{\boldsymbol{\varphi}}, \widetilde{V}, \widetilde{S_Q}, \boldsymbol{\pi})$ is an atlas of $(\widetilde{F_Q}, \widetilde{S_Q})$.

Hence, by Proposition 7.4.17, either $\widetilde{F_Q} = \emptyset$ or $\widetilde{L_F}$ admits a global normal form. □

Suppose now that the Lagrange system $\widetilde{L_F}$, given by Lemma 7.4.21 has been computed. According to Lemma 7.4.3, one can compute a zero-dimensional parametrization $\widetilde{\mathscr{P}}$, encoding $\widetilde{\mathcal{P}} = \Psi_{\boldsymbol{\varphi}_e}(\mathcal{P})$, within the same complexity bound. One checks, by assumption, that $\widetilde{S_Q} \subset \widetilde{\mathcal{P}} \subset \widetilde{F_Q}$ and that $\widetilde{S_Q}$ has degree bounded by $((n+e)D)^{n+e}$.

Therefore, according to Proposition 7.4.20, there exists a Monte Carlo algorithm RoadmapRecLagrange which, on input $\widetilde{L_F}$ and $\widetilde{\mathscr{P}}$, outputs, in case of success, a roadmap $\widetilde{\mathscr{R}_{F_Q}}$ of $(\widetilde{F_Q}, \widetilde{\mathcal{P}})$ of degree

$$\widetilde{O}\left((\mu+\kappa)16^{3d_F}(n_F\log_2(n_F))^{2(2d_F+12\log_2(d_F))(\log_2(d_F)+5)}D^{(2n_F+1)(\log_2(d_F)+3)}\right),$$

where $n_F = n+e$ and $d_F = d-e$, and using

$$\widetilde{O}\left((\mu+\kappa)^3 16^{9d_F}(E+E'+e)(n_F\log_2(n_F))^{6(2d_F+12\log_2(d_F))(\log_2(d_F)+6)}D^{3(2n_F+1)(\log_2(d_F)+4)}\right)$$

arithmetic operations in $\mathbf{Q}$.

Finally, let $\mathscr{B}_{\mathrm{RM}}$ be the degree bound, given above, on the roadmap $\widetilde{\mathscr{R}_{F_Q}}$ of $(\widetilde{F_Q}, \widetilde{Q})$ output by RoadmapRecLagrange. Then, by [SS17, Lemma J.9], one can compute the projection $\mathscr{R}_{F_Q}$, of $\widetilde{\mathscr{R}_{F_Q}}$, on the last n variables. The complexity of such step is bounded by $\widetilde{O}\left(n_F^2\mathscr{B}_{\mathrm{RM}}^3\right)$, that is bounded by

$$\widetilde{O}\left((\mu+\kappa)^3 16^{9d_F}(n_F\log_2(n_F))^{6(2d_F+12\log_2(d_F))(\log_2(d_F)+6)}D^{3(2n_F+1)(\log_2(d_F)+3)}\right),$$

operations in $\mathbf{Q}$. Finally, since $\Psi_{\boldsymbol{\varphi}_e}$ is an isomorphism of algebraic sets, it induces a one-to-one homeomorphic correspondence between the semi-algebraically connected components of $\widetilde{F_Q} \cap \mathbf{R}^{n_F}$ and $F_Q \cap \mathbf{R}^n$ by Proposition 4.2.23. Therefore, $\mathscr{R}_{F_Q}$ is a roadmap of $(F_Q, \mathcal{P})$.

7.5 Proof of Proposition 7.2.3: finiteness of fibers

We recall the statement of the proposition we adress to prove.

Proposition (7.2.3). *Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set with finitely many singular points and θ be in $\mathbf{C}[\boldsymbol{X}]$. Let $2 \leq \mathfrak{r} \leq d+1$. For $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{\mathfrak{r}})$ in $\mathbf{C}^{\mathfrak{r}n}$, we define $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1), \ldots, \varphi_{\mathfrak{r}}(\boldsymbol{X}, \boldsymbol{\alpha}_{\mathfrak{r}}))$, where for $2 \leq j \leq \mathfrak{r}$*

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{1,k}x_k \quad \text{and} \quad \varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \sum_{k=1}^{n} \alpha_{j,k}x_k.$$

Then, there exists a non-empty Zariski open subset $\Omega_{\mathsf{l}}(V, \theta, \mathfrak{r}) \subset \mathbf{C}^{\mathfrak{r}n}$ such that for every $\boldsymbol{\alpha} \in \Omega_{\mathsf{l}}(V, \theta, \mathfrak{r})$ and $i \in \{1, \ldots, \mathfrak{r}\}$, the following holds:

1. *either $W_{\boldsymbol{\varphi}}(i, V)$ is empty or $(i-1)$-equidimensional;*

2. *the restriction of φ_{i-1} to $W_{\varphi}(i,V)$ is a Zariski-closed map;*

3. *for any $z \in \mathbf{C}^{i-1}$, the fiber $K_{\varphi}(i,V) \cap \varphi_{i-1}^{-1}(z)$ is finite.*

The rest of this section is devoted to the proof of this result. We first establish a general lower bound on the dimension of the non-empty generalized polar varieties. This is a direct generalization of [SS17, Lemma B.5. & B.13.].

Lemma 7.5.1. *Let $\mathfrak{K}$ be an algebraically closed field, and let $V \subset \mathfrak{K}^n$ be a d-equidimensional algebraic set. Then, for any $\varphi = (\phi_1, \ldots, \phi_{d+1}) \subset \mathfrak{K}[\boldsymbol{X}]$, and any $1 \leq i \leq d+1$, all irreducible components of $W_{\varphi}(i,V)$ have dimension at least $i-1$.*

Proof. Since V is d-equidimensional, the case $i = d+1$ is immediate; assume now that $i \leq d$. According to [SS17, Lemma A.13], there exists an atlas $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ of $(V, \mathrm{sing}(V))$. For $1 \leq j \leq s$, let $\chi_j = (m_j, \boldsymbol{h}_j)$. By [SS17, Lemma A.12], $\boldsymbol{h}_j$ has cardinality $c = n - d$. According to Lemma 7.2.6, fix $j \in \{1, \ldots, s\}$, the following holds in $\mathcal{O}(m_j) - \mathrm{sing}(V)$,

$$W_{\varphi}(i,V) \;=\; \{\boldsymbol{y} \in \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h}_j) \mid \mathrm{rank}(\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h}_j, \varphi_i) < c+i\} = W^{\circ}_{\varphi}(i, \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h}_j)). \tag{7.3}$$

Let $\boldsymbol{y} \in W^{\circ}_{\varphi}(i,V) = W_{\varphi}(i,V) - \mathrm{sing}(V)$. Since $\boldsymbol{y} \in V$, there exists $j \in \{1, \ldots, s\}$ such that $\boldsymbol{y} \in \mathcal{O}(m_j)$. Hence, by (7.3), in $\mathcal{O}(m_j) - \mathrm{sing}(V)$, the irreducible component of $W_{\varphi}(i,V)$ containing $\boldsymbol{y}$ is the same as the irreducible component of the Zariski closure of $W^{\circ}_{\varphi}(i, \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h}_j))$ containing $\boldsymbol{y}$. Since these irreducible components are equal over a non-empty Zariski open set, they have same dimension by [Sha13, Theorem 1.19]. Hence, proving that this common dimension is at least $i-1$ allows us to conclude.

Let $\mathfrak{m} \subset \mathfrak{K}[\boldsymbol{X}]$ be the ideal generated by the $(c+i)$-minors of $\mathrm{Jac}[\boldsymbol{h}_j, \varphi_i]$. Then,

$$W^{\circ}_{\varphi}(i, \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h}_j)) = \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h}_j) \cap \boldsymbol{V}(\mathfrak{m})$$

which is contained in the algebraic set $\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j) \cap \boldsymbol{V}(\mathfrak{m})$. We assume that $\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j) \cap \boldsymbol{V}(\mathfrak{m})$ is not empty otherwise the statement of the proposition trivially holds.

Note that any irreducible component Z of $\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j) \cap \boldsymbol{V}(\mathfrak{m})$, has an ideal of definition $\mathfrak{p}$ in $\mathfrak{K}[\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j)]$ that is an isolated prime component of the determinantal ideal $\mathfrak{m} \cdot \mathfrak{K}[\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j)]$. Then by [EN62, Theorem 3.], $\mathfrak{p}$ has height at most $n - c - (i-1)$ so that the codimension of Z in $\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j)$ is at most $n - c - (i-1)$. Since $\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j)$ has dimension $n-c$, the dimension of Z is then at most $i-1$.

One concludes by observing that, any irreducible component of the Zariski closure of $W^{\circ}_{\varphi}(i, \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h}_j))$ is the union of irreducible components of $\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j) \cap \boldsymbol{V}(\mathfrak{m})$. □

7.5.1 An adapted Noether normalization lemma

Consider an algebraically closed field $\mathfrak{K}$, let $\boldsymbol{f} = (f_1, \ldots, f_m) \colon \mathfrak{K}^n \to \mathfrak{K}^m$ be a polynomial map and $V \subset \mathfrak{K}^n$ and let $Y \subset \mathfrak{K}^m$ be algebraic sets such that $\boldsymbol{f}(V) \subset Y$. Finally, consider the restriction $\widetilde{\boldsymbol{f}} : V \to Y$ of $\boldsymbol{f}$, and recall that the pullback $\widetilde{\boldsymbol{f}}^*$ of $\widetilde{\boldsymbol{f}}$ is defined by

$$\begin{array}{rccc} \widetilde{\boldsymbol{f}}^* \colon & \mathfrak{K}[Y] = \mathfrak{K}[y_1, \ldots, y_m]/\boldsymbol{I}(Y) & \longrightarrow & \mathfrak{K}[V] = \mathfrak{K}[x_1, \ldots, x_n]/\boldsymbol{I}(V) \\ & g & \longmapsto & g \circ \boldsymbol{f} \end{array}.$$

Definition 7.5.2 ([Sha13, Section 5.3])**.** We say that the restriction $\widetilde{\boldsymbol{f}}$ of $\boldsymbol{f}$ is a *finite map* if

1. $\boldsymbol{f}(V)$ is dense in Y, which is equivalent to $\widetilde{\boldsymbol{f}}^*$ being injective;
2. the extension $\mathfrak{K}[Y] \hookrightarrow \mathfrak{K}[V]$ induced by $\widetilde{\boldsymbol{f}}^*$ is integral.

The following lemma shows that to verify such conditions, we may not have to work over an algebraically closed field: if V and Y are defined over a subfield $\mathbf{K}$ of $\mathfrak{K}$, finiteness of $\widetilde{\boldsymbol{f}}$ is equivalent to the pullback $\mathbf{K}[\boldsymbol{Y}]/\boldsymbol{I}(Y) \to \mathbf{K}[\boldsymbol{X}]/\boldsymbol{I}(V)$ being injective and integral.

Lemma 7.5.3. *Let $\mathbf{K} \subset \boldsymbol{L}$ be two fields, let I, J be ideals in respectively $\mathbf{K}[\boldsymbol{Y}] = \mathbf{K}[y_1, \ldots, y_m]$ and $\mathbf{K}[\boldsymbol{X}] = \mathbf{K}[x_1, \ldots, x_n]$ and let I', J' be their extensions in respectively $\boldsymbol{L}[\boldsymbol{Y}]$ and $\boldsymbol{L}[\boldsymbol{X}]$. Let finally $\boldsymbol{f} = (f_1, \ldots, f_m)$ be in $\mathbf{K}[\boldsymbol{X}]$, such that for g in I, $g \circ \boldsymbol{f}$ is in J.*

Consider the ring homomorphisms $\zeta_{\mathbf{K}} : \mathbf{K}[\boldsymbol{Y}]/I \to \mathbf{K}[\boldsymbol{X}]/J$ and $\zeta_{\boldsymbol{L}} : \boldsymbol{L}[\boldsymbol{Y}]/I' \to \boldsymbol{L}[\boldsymbol{X}]/J'$, that both map y_j to f_j, for all j. Then, $\zeta_{\mathbf{K}}$ is injective, resp. integral, if and only if $\zeta_{\boldsymbol{L}}$ is.

Proof. Injectivity of $\zeta_{\mathbf{K}}$ is equivalent to the equality between ideals $I = (J\mathbf{K}[\boldsymbol{Y}, \boldsymbol{X}] + \langle y_1 - f_1, \ldots, y_m - f_m \rangle) \cap \mathbf{K}[\boldsymbol{Y}]$; similarly, injectivity of $\zeta_{\boldsymbol{L}}$ is equivalent to $I' = (J'\boldsymbol{L}[\boldsymbol{Y}, \boldsymbol{X}] + \langle y_1 - f_1, \ldots, y_m - f_m \rangle) \cap \boldsymbol{L}[\boldsymbol{Y}]$. These properties can be determined by Gröbner basis calculations; since the generators of I, J are the same as those of I', J', they are thus equivalent.

Next, integrality of $\zeta_{\mathbf{K}}$ directly implies that of $\zeta_{\boldsymbol{L}}$. Conversely, integrality of $\zeta_{\boldsymbol{L}}$ is equivalent to the existence of polynomials $G_1, \ldots, G_n$ in $\boldsymbol{L}[y_1, \ldots, y_m, s]$, all monic in s, such that $G_j(f_1, \ldots, f_m, x_j)$ is in J' for all j. If we assume that such polynomials exist, we can then linearize these membership equalities, reducing such properties to the existence of a solution to certain linear system with entries in $\mathbf{K}$. Since we know that a solution exists with entries in $\boldsymbol{L}$, one must also exist with entries in $\mathbf{K}$. This then yields integrality of $\zeta_{\mathbf{K}}$. □

The Noether normalization lemma says that for V r-dimensional and $Y = \mathfrak{K}^r$, the restriction of a generic linear mapping $\mathfrak{K}^n \to \mathfrak{K}^m$ to V is finite. We give here a proof of this lemma adapted to our setting, where the shape of the projections we perform is made explicit. We start with a statement for ideals rather than algebraic sets.

Proposition 7.5.4 (Noether normalization)**.** *Let $\mathbf{K}$ be a field, let J be an ideal in $\mathbf{K}[\boldsymbol{X}]$ and let r be the dimension of its zero-set over an algebraic closure of $\mathbf{K}$. Let further $\boldsymbol{a}$ be $r(n-r)$ new indeterminates. Then the $\mathbf{K}(\boldsymbol{a})$-algebra homomorphism*

$$\begin{array}{rccc} \zeta_{\boldsymbol{a}} \colon & \mathbf{K}(\boldsymbol{a})[z_1, \ldots, z_r] & \longrightarrow & \mathbf{K}(\boldsymbol{a})[\boldsymbol{X}]/J\mathbf{K}(\boldsymbol{a})[\boldsymbol{X}] \\ & z_j & \longmapsto & x_j + \displaystyle\sum_{k=1}^{n-r} a_{j,k}\, x_{r+k} \mod J \end{array}$$

is injective and makes $\mathbf{K}(\boldsymbol{a})[\boldsymbol{X}]/J\mathbf{K}(\boldsymbol{a})[\boldsymbol{X}]$ *integral over* $\mathbf{K}(\boldsymbol{a})[z_1,\dots,z_r]$.

Proof. We proceed by induction on the number n of variables. The case $n=0$ is straightforward. Assume now that $n>0$ and that the statement holds for $k<n$ variables. Remark that if $J=\{0\}$, we have $r=n$, $\zeta_{\boldsymbol{a}}$ is the isomorphism $\mathbf{K}[z_1\dots,z_n]\to\mathbf{K}[\boldsymbol{X}]$ mapping z_i to x_i for all i (which is then integral); in this case, we are done.

Assume now that $J\neq\{0\}$, and let f be non-zero in J. Let δ be the total degree of f and let $\boldsymbol{\ell}=(\ell_1,\dots,\ell_{n-1})$ be new indeterminates. Writing $f=\sum_{i_1,\dots,i_n}c_{i_1,\dots,i_n}x_1^{i_1}\cdots x_n^{i_n}$, the leading coefficient of $f(x_1+\ell_1x_n,\dots,x_{n-1}+\ell_{n-1}x_n,x_n)$ in x_n is

$$\sum_{i_1+\cdots+i_n=\delta}c_{i_1,\dots,i_n}\ell_1^{i_1}\cdots\ell_{n-1}^{i_{n-1}}=f_\delta(\ell_1,\dots,\ell_{n-1},1)$$

where f_δ is the homogeneous degree-δ component of f. Therefore, if $F=f_\delta(\ell_1,\dots,\ell_{n-1},1)$, then F is not the zero polynomial and the polynomial

$$\frac{1}{F}f(x_1+\ell_1x_n,\dots,x_{n-1}+\ell_{n-1}x_n,x_n)\in\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{X}]$$

is monic in x_n. Let further J' be the extension of J to $\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{X}]$, let $\boldsymbol{Y}=(y_1,\dots,y_{n-1})$ be new indeterminates and consider the $\mathbf{K}(\boldsymbol{\ell})$-algebra homomorphism

$$\begin{array}{rccc}\tau\colon & \mathbf{K}(\boldsymbol{\ell})[\boldsymbol{Y}] & \longrightarrow & \mathbf{K}(\boldsymbol{\ell})[\boldsymbol{X}]\\ & y_j & \longmapsto & x_j-\ell_jx_n\end{array};$$

the contraction $J'^c=\tau^{-1}(J')$ is an ideal in $\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{Y}]$. For $1\leq j\leq n-1$, let $[y_j]=y_j \mod J'^c$ and for $1\leq k\leq n$ let $[x_j]=x_j \mod J'$. Then let

$$\begin{array}{rccc}[\tau]\colon & \mathbf{K}(\boldsymbol{\ell})[\boldsymbol{Y}]/J'^c & \longrightarrow & \mathbf{K}(\boldsymbol{\ell})[\boldsymbol{X}]/J'\\ & [y_j] & \longmapsto & [x_j]-\ell_j[x_n]\end{array}$$

and

$$g(s)=\frac{1}{F}f\big([y_1]+\ell_1s,\dots,[y_{n-1}]+\ell_{n-1}s,s\big)\in\Big(\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{Y}]/J'^c\Big)[s];$$

this is a monic polynomial in s.

If we extend $[\tau]$ to a $\mathbf{K}(\boldsymbol{\ell})$-algebra homomorphism $\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{Y}]/J'^c[s]\to\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{X}]/J'[s]$, g satisfies

$$[\tau](g)\big([x_n]\big)=\frac{1}{F}f([x_1],\dots,[x_n])=0,$$

since $f\in J$ by assumption. Since $[\tau]$ is by construction injective, it makes $\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{X}]/J'$ an integral extension of $\mathbf{K}(\boldsymbol{\ell})[\boldsymbol{Y}]/J'^c$ (the integral dependence relation for $[x_j]$, for $j<n$, is obtained by replacing s by $(s-[y_j])/\ell_j$ in g and clearing denominators).

In particular, these two rings have the same Krull dimension [Kun85, Corollary 2.13]. This latter dimension is the same as that of $\mathbf{K}[\boldsymbol{X}]/J$ (because it can be read off a Gröbner basis of J, and such Gröbner bases are also Gröbner bases of J'), that is, r. In other words, the zero-set of J'^c over an algebraic closure of $\mathbf{K}(\boldsymbol{\ell})$ has dimension r.

Then we can apply the induction hypothesis to $J'^c \subset \mathbf{K}(\boldsymbol{\ell})[\boldsymbol{Y}]$. If we consider $r(n-1-r)$ new indeterminates $\boldsymbol{b} = (b_{i,j})_{1\le i\le r, 1\le j\le n-1-r}$, and introduce $\boldsymbol{Z} = (z_1, \ldots, z_r)$, the $\mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})$-algebra homomorphism

$$\begin{array}{rccl} \eta_{\boldsymbol{b}}\colon & \mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{Z}] & \longrightarrow & \mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{Y}]/J'^c\mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{Y}] \\ & z_j & \longmapsto & [y_j] + \displaystyle\sum_{k=1}^{n-1-r} b_{j,k}\,[y_{r+k}] \end{array}$$

is thus injective and realizes an integral extension of the polynomial ring $\mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{Z}]$. On the other hand, by Lemma 7.5.3, the extended map

$$[\tau]^e : \mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{Y}]/J'^c\mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{Y}] \longrightarrow \mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{X}]/J'\mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{X}]$$

remains injective and integral. By transitivity, it follows that the $\mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})$-algebra homomorphism

$$\begin{array}{rccl} [\tau]^e \circ \eta_{\boldsymbol{b}}\colon & \mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{Z}] & \longrightarrow & \mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{X}]/J'\mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})[\boldsymbol{X}] \\ & z_j & \longmapsto & [x_j] + \displaystyle\sum_{k=1}^{n-r} m_{j,k}\,[x_{r+k}] \end{array},$$

where for all $1 \le j \le r$,

$$\boldsymbol{m}_j = \left(b_{j,1}, \ldots, b_{j,n-1-r},\ -\ell_j - \sum_{k=1}^{n-1-r} b_{j,k}\,\ell_{r+k}\right),$$

is injective and integral as well. In particular, the restriction of $[\tau]^e \circ \eta_{\boldsymbol{b}}$ to a mapping $\mathbf{K}(\boldsymbol{m})[\boldsymbol{Z}] \to \mathbf{K}(\boldsymbol{m})[\boldsymbol{X}]/J\mathbf{K}(\boldsymbol{m})[\boldsymbol{X}]$ is still injective and integral, by Lemma 7.5.3 (here, we write $\mathbf{K}(\boldsymbol{m}) = \mathbf{K}(m_{1,1}, \ldots, m_{r(n-r)})$).

Letting $\boldsymbol{a}$ be $r(n-r)$ new indeterminates, we observe that $\iota : a_{i,j} \mapsto m_{i,j}$ defines a $\mathbf{K}$-isomorphism $\mathbf{K}(\boldsymbol{a}) \to \mathbf{K}(\boldsymbol{m}) \subset \mathbf{K}(\boldsymbol{\ell}, \boldsymbol{b})$, since the entries of $\boldsymbol{m}$ are $\mathbf{K}$-algebraically independent. The conclusion follows. □

Corollary 7.5.5. *Let $V \subset \mathbf{C}^n$ be an r-dimensional algebraic set. Let $\boldsymbol{a} = (a_{i,j})_{1\le i\le r, 1\le j\le n-r}$ be $r(n-r)$ new indeterminates and let $V_{\mathfrak{K}} \subset \mathfrak{K}^n$ be the extension of V to the algebraic closure $\mathfrak{K}$ of $\mathbf{K} = \mathbf{C}(\boldsymbol{a})$. Then the restriction $\widetilde{\boldsymbol{f}} : V_{\mathfrak{K}} \to \mathfrak{K}^r$ of the polynomial map $\boldsymbol{f} = (f_1, \ldots, f_r)$ given by*

$$f_j = x_j + \sum_{k=1}^{n-r} a_{j,k}\,x_{r+k}, \quad 1 \le j \le r$$

is finite.

Proof. Let J be the defining ideal of V in $\mathbf{C}[\boldsymbol{X}]$. Letting $\boldsymbol{Z} = z_1, \ldots, z_r$ be r new indeterminates, the previous proposition shows that $\widetilde{\boldsymbol{f}}^* : \mathbf{C}(\boldsymbol{a})[\boldsymbol{Z}] \to \mathbf{C}(\boldsymbol{a})[\boldsymbol{X}]/J\mathbf{C}(\boldsymbol{a})[\boldsymbol{X}]$ is injective and integral. By Lemma 7.5.3, we further deduce that it is also the case for the extension of $\boldsymbol{f}^* : \mathfrak{K}[\boldsymbol{Z}] \to \mathfrak{K}[\boldsymbol{X}]/J\mathfrak{K}[\boldsymbol{X}]$.

Because $\mathbf{C}$ is algebraically closed, J remains radical in $\mathfrak{K}[\boldsymbol{X}]$, so that $J\mathfrak{K}[\boldsymbol{X}]$ is the defining ideal of $V_{\mathfrak{K}}$, and we are done. □

7.5.2 Finiteness on polar varieties

In this section, we prove the core of the Proposition 7.2.3, by proving finiteness properties on the restriction of the considered morphisms to their associated polar varieties.

Proposition 7.5.6. *Let $V \subset \mathbf{C}^n$ be a d-equidimensional algebraic set with finitely many singular points and let $\theta \in \mathbf{C}[\boldsymbol{X}]$. For $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{d+1})$ in $\mathbf{C}^{(d+1)n}$, and for $2 \leq j \leq d+1$, let*

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{1,k} x_k \quad \text{and} \quad \varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \sum_{k=1}^{n} \alpha_{j,k} x_k.$$

Then for any $1 \leq i \leq d+1$, there exists a non-empty Zariski open set $\Omega_i \subset \mathbf{C}^{(d+1)n}$ such that if $\boldsymbol{\alpha} \in \Omega_i$ and $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1), \ldots, \varphi_{d+1}(\boldsymbol{X}, \boldsymbol{\alpha}_{d+1}))$, then the restriction of $\boldsymbol{\varphi}_{i-1}$ to $W_{\boldsymbol{\varphi}}(i, V)$ is a finite map.

Proof. Let $\boldsymbol{a} = (\boldsymbol{a}_i)_{1 \leq j \leq d+1}$, with $\boldsymbol{a}_j = (a_{j,1}, \ldots, a_{j,n})$ for all j, be $(d+1)n$ new indeterminates, and let $\mathbf{C}(\boldsymbol{a})$ be the field of rational fractions in the entries of $\boldsymbol{a}$. We let $\mathfrak{K}$ be the algebraic closure of $\mathbf{C}(\boldsymbol{a})$, and we denote by $V_{\mathfrak{K}} \subset \mathfrak{K}^n$ the extension of V to $\mathfrak{K}$. Let further

$$\phi_1(\boldsymbol{X}, a_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^{n} a_{1,k} x_k \quad \text{and} \quad \phi_j(\boldsymbol{X}, a_j) = \sum_{k=1}^{n} a_{j,k} x_k, \quad 2 \leq j \leq d+1$$

and define $\boldsymbol{\varphi} = (\phi_1, \ldots, \phi_{d+1})$ in $\mathbf{C}(\boldsymbol{a})[\boldsymbol{X}]$; as before, for $1 \leq i \leq d+1$, we write $\boldsymbol{\varphi}_i = (\phi_1, \ldots, \phi_i)$. We will prove the following property, which we call $\mathcal{P}(i)$, by decreasing mathematical induction, for $i = d+1, \ldots, 1$:

$\mathcal{P}(i)$: the restriction of $\boldsymbol{\varphi}_{i-1}$ to $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}})$ is a finite map.

Let us first see how to deduce the proposition from this claim; hence, we start by fixing i in $1, \ldots, d+1$ and assume that $\mathcal{P}(i)$ holds.

Since $\boldsymbol{\varphi}_i$ and $V_{\mathfrak{K}}$ are defined by polynomials with coefficients in $\mathbf{C}(\boldsymbol{a})$, it is also the case for $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}})$ by [SS17, Lemma A.2]. Then $\mathcal{P}(i)$ shows (via the discussion preceding Lemma 7.5.3) that the pullback $\widetilde{\boldsymbol{\varphi}}^*_{i-1} : \mathbf{C}(\boldsymbol{a})[z_1, \ldots, z_{i-1}] \to \mathbf{C}(\boldsymbol{a})[\boldsymbol{X}]/\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}}))$ is injective and integral.

- Injectivity means that the ideal generated by $\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}}))$ and $z_1 - \phi_1, \ldots, z_{i-1} - \phi_{i-1}$ in $\mathbf{C}(\boldsymbol{a})[z_1, \ldots, z_{i-1}, \boldsymbol{X}]$ has a trivial intersection with $\mathbf{C}(\boldsymbol{a})[z_1, \ldots, z_{i-1}]$. Then, this remains true for the restriction of $\boldsymbol{\varphi}_{i-1}$ to $W_{\boldsymbol{\varphi}}(i, V)$ for $\boldsymbol{\alpha}$ in a non-empty Zariski-open set in $\mathbf{C}^{(d+1)n}$. For instance, it is enough to ensure that the numerators and denominators of the coefficients of all polynomials appearing in a lexicographic Gröbner basis computation for the ideal above, in $\mathbf{C}(\boldsymbol{a})[z_1, \ldots, z_{i-1}, \boldsymbol{X}]$, do not vanish at $\boldsymbol{\alpha}$.
- Integrality means that there exist n monic polynomials $P_1, \ldots, P_n$ in $\mathbf{C}(\boldsymbol{a})[z_1, \ldots, z_{i-1}][s]$ such that all polynomials

$$P_j\left(\varphi_1, \ldots, \varphi_{i-1}, x_j\right), \quad 1 \leq j \leq n$$

belong to $\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}}))$ in $\mathbf{C}(\boldsymbol{a})[\boldsymbol{X}]$. Taking $G \in \mathbf{C}[\boldsymbol{a}]$ as the least common multiple of the denominators of all coefficients that appear in these membership relations, we

see that for $\boldsymbol{\alpha}$ in $\mathbf{C}^{(d+1)n}$, if $G(\boldsymbol{\alpha}) \neq 0$, $\boldsymbol{\varphi}_{i-1}$ makes $\mathbf{C}[\boldsymbol{X}]/\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i,V))$ integral over $\mathbf{C}[z_1,\ldots,z_{i-1}]$.

Initial case: $i = d+1$. We prove $\mathcal{P}(d+1)$. As $\mathrm{T}_{\boldsymbol{y}} V_{\mathfrak{K}}$ has dimension d, for every $\boldsymbol{y} \in \mathrm{reg}(V_{\mathfrak{K}})$, the polar variety $W_{\boldsymbol{\varphi}}(d+1, V_{\mathfrak{K}})$ is nothing but $V_{\mathfrak{K}}$ (since the latter only admits finitely many singular points); hence, we have to prove that the restriction of $\boldsymbol{\varphi}_d$ to $V_{\mathfrak{K}}$ is finite.

Let $y_1,\ldots,y_d$ be new variables and consider the algebraic set $V' \subset \mathbf{C}^{d+n}$ defined by $y_1 - \theta, y_2, \ldots, y_d$ and all polynomials f, for f in $\boldsymbol{I}(V)$; as above, we denote its extension to $\mathfrak{K}^{d+n}$ by $V'_{\mathfrak{K}}$. Apply Corollary 7.5.5 to V' (which is still of dimension d): we deduce that the restriction of $\boldsymbol{\varphi}_d$ to $V'_{\mathfrak{K}}$ is finite. Since $V'_{\mathfrak{K}}$ and $V_{\mathfrak{K}}$ are isomorphic (since $V'_{\mathfrak{K}}$ is a graph above $V_{\mathfrak{K}}$), we are done with this case.

Induction step: $1 \leq i \leq d$. Assume now that $\mathcal{P}(i+1)$ holds. Thus, the restriction of $\boldsymbol{\varphi}_i$ to a mapping $W_{\boldsymbol{\varphi}}(i+1, V_{\mathfrak{K}}) \to \mathfrak{K}^i$ is finite. By [Sha13, Theorem 1.12] this restriction is a Zariski-closed map so that, since $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}}) \subset W_{\boldsymbol{\varphi}}(i+1, V_{\mathfrak{K}})$, $\boldsymbol{\varphi}_i(W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}})) \subset \mathfrak{K}^i$ is an algebraic set and the restriction of $\boldsymbol{\varphi}_i$ to a mapping $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}}) \to \boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}}))$ is finite as well.

Let $\boldsymbol{Y} = (y_1,\ldots,y_i)$ be new indeterminates. Because these sets are defined over $\mathbf{C}(\boldsymbol{a})$, we deduce that the pullback $\mathbf{C}(\boldsymbol{a})[\boldsymbol{Y}]/\boldsymbol{I}(\boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}}))) \to \mathbf{C}(\boldsymbol{a})[\boldsymbol{X}]/\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}}))$ that maps y_j to φ_j (for all $j \leq i$) is injective and integral (Lemma 7.5.3).

On another hand, by the theorem on the dimension of the fibers [Sha13, Theorem 1.25], for any irreducible component C of $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}})$ and for a generic $\boldsymbol{y} \in \boldsymbol{\varphi}_i(C)$,

$$\dim C - \dim \boldsymbol{\varphi}_i(C) = \dim \boldsymbol{\varphi}_i^{-1}(\boldsymbol{y}) \cap C = 0$$

since, as a finite map, the restriction of $\boldsymbol{\varphi}_i$ to $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}})$ has finite fibers. By an algebraic version of Sard's theorem [SS17, Proposition B.2]

$$\dim\, \boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}})) \leq i - 1,$$

so that $\dim W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}}) \leq i - 1$ as well. Together with Lemma 7.5.1, this proves that both $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}})$ and its image $\boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}}))$ are either empty or equidimensional of dimension $i-1$. If they are empty, there is nothing to do, so suppose it is not the case.

Let $\boldsymbol{Z} = (z_1,\ldots,z_{i-1})$ and $\boldsymbol{\ell} = (\ell_1,\ldots,\ell_{i-1})$ be new indeterminates. Since $W_{\boldsymbol{\varphi}}(i, V_{\mathfrak{K}})$, and thus its image $\boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}}))$, are defined over $\mathbf{C}(\boldsymbol{a})$, we can apply Noether normalization to $\boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}}))$ (Proposition 7.5.4) with coefficients in $\mathbf{C}(\boldsymbol{a})$, and deduce that the $\mathbf{C}(\boldsymbol{a}, \boldsymbol{\ell})$-algebra homomorphism

$$\begin{aligned} \zeta\colon\ \mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{Z}] &\longrightarrow \mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{Y}]/\boldsymbol{I}(\boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}}))) \\ z_j &\longmapsto y_j + \ell_j y_i \mod \boldsymbol{I}(\boldsymbol{\varphi}_i(W_{\phi}(i, V_{\mathfrak{K}}))) \end{aligned}$$

is injective and integral. Besides, we deduce from Lemma 7.5.3 that after scalar extension, the ring homomorphism $\mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{Y}]/\boldsymbol{I}(\boldsymbol{\varphi}_i(W_\phi(i,V_{\mathfrak{K}})))\to\mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{X}]/\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i,V_{\mathfrak{K}}))$ that maps y_j to φ_j (for all $j\leq i$) is still injective and integral. If we set

$$\psi_j=\phi_j+\ell_j\phi_i\quad\text{for } 1\leq j\leq i-1\quad\text{and}\quad\psi_j=\phi_j\quad\text{for } i\leq j\leq d+1,\tag{7.4}$$

and finally $\boldsymbol{\psi}=(\psi_1,\dots,\psi_{d+1})\subset\mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{X}]$, then, by transitivity,

$$\begin{aligned}\boldsymbol{\psi}_{i-1}\colon\ \mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{Z}]&\longrightarrow\mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{X}]/\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i,V_{\mathfrak{K}}))\\ z_j&\longmapsto\psi_j(\boldsymbol{X})\mod\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i,V_{\mathfrak{K}}))\end{aligned}$$

is injective and integral as well.

Since the first i entries of $\boldsymbol{\psi}$ are elementary row operations of the first i entries of $\boldsymbol{\varphi}$, we deduce that $W_{\boldsymbol{\varphi}}(i,V_{\mathfrak{K}})=W_{\boldsymbol{\psi}}(i,V_{\mathfrak{K}})$. Besides, injecting the definition of the ϕ_j's in (7.4), one gets that $\boldsymbol{\psi}(\boldsymbol{X})=\boldsymbol{\varphi}(\boldsymbol{X},\boldsymbol{m})$, where

$$\boldsymbol{m}=(\boldsymbol{a}_1+\ell_1\boldsymbol{a}_i,\dots,\boldsymbol{a}_{i-1}+\ell_{i-1}\boldsymbol{a}_i,\boldsymbol{a}_i,\dots,\boldsymbol{a}_{d+1})$$

is a vector of $(d+1)n$ $\mathbf{C}$-algebraically independent elements of $\mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})$. Through the isomorphism $\mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})\to\mathbf{C}(\boldsymbol{m})$, we see that

$$\begin{aligned}\boldsymbol{\varphi}_{i-1}\colon\ \mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{Z}]&\longrightarrow\mathbf{C}(\boldsymbol{a},\boldsymbol{\ell})[\boldsymbol{X}]/\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i,V_{\mathfrak{K}}))\\ z_j&\longmapsto\phi_j(\boldsymbol{X})\mod\boldsymbol{I}(W_{\boldsymbol{\varphi}}(i,V_{\mathfrak{K}}))\end{aligned}$$

is injective and integral. From Lemma 7.5.3, we see that this precisely gives that the restriction of $\boldsymbol{\varphi}_{i-1}$ to $W_{\boldsymbol{\varphi}}(i,V_{\mathfrak{K}})$ is finite. This ends the proof of the induction step, and, by mathematical induction, of the proposition. □

7.5.3 Proof of the main proposition

We conclude by proving Proposition 7.2.3, which is a direct consequence of the previous results. Let V, θ and $2\leq\mathfrak{r}\leq d+1$ as given in the statement of the proposition.

Let Ω be the non-empty Zariski open subset of $\mathbf{C}^{(d+1)n}$ obtained as the intersection, for all $1\leq i\leq d+1$, of the Ω_i's given by application of Proposition 7.5.6. Let $\boldsymbol{a}=(\boldsymbol{a}_i)_{1\leq i\leq d+1}$, where $\boldsymbol{a}_i=(a_{i,1},\dots,a_{i,n})$ be $(d+1)n$ new indeterminates. By definition, there exists $\boldsymbol{f}=(f_1,\dots,f_p)\subset\mathbf{C}[\boldsymbol{a}]$, such that $\Omega=\mathbf{C}^{(d+1)n}-\boldsymbol{V}(\boldsymbol{f})$. Then, let $\Omega_{\mathfrak{l}}(V,\theta,\mathfrak{r})$ be the projection on the first $\mathfrak{r}n$ coordinates of Ω, it is the union, for all $\boldsymbol{\alpha}''\in\mathbf{C}^{(d+1-\mathfrak{r})n}$, of the non-empty Zariski open sets

$$\mathbf{C}^{\mathfrak{r}n}-\boldsymbol{V}\left(\boldsymbol{f}(\boldsymbol{a}',\boldsymbol{\alpha}'')\right),$$

where $\boldsymbol{a}'=(\boldsymbol{a}_1,\dots,\boldsymbol{a}_{\mathfrak{r}})$, hence a non-empty Zariski open subset of $\mathbf{C}^{\mathfrak{r}n}$.

Let $\boldsymbol{\alpha}'\in\Omega_{\mathfrak{l}}(V,\theta,\mathfrak{r})$ and $\boldsymbol{\varphi}=(\varphi_1(\boldsymbol{X},\boldsymbol{\alpha}'_1),\dots,\varphi_{\mathfrak{r}}(\boldsymbol{X},\boldsymbol{\alpha}'_{\mathfrak{r}}))$. Let $i\in\{1,\dots,\mathfrak{r}\}$ then, there exists $\boldsymbol{\alpha}''\in\mathbf{C}^{(d+1-\mathfrak{r})n}$ such that $(\boldsymbol{\alpha}',\boldsymbol{\alpha}'')\in\Omega_i$. Therefore by Proposition 7.5.6, the restriction of $\boldsymbol{\varphi}_{i-1}$ to $W_{\boldsymbol{\varphi}}(i,V)$ is finite.

In particular, by [Sha13, Section 5.3], the restriction of φ_{i-1} to $W_{\varphi}(i,V)$ is a Zariski-closed map that has finite fibers. Moreover, since $\mathrm{sing}(V)$ is finite, we deduce that $K_{\varphi}(i,V)\cap\varphi_{i-1}^{-1}(\boldsymbol{z})$ is finite for any $\boldsymbol{z}\in\mathbf{C}^{i-1}$. Finally, as a consequence, and by [Sha13, Theorem 1.12 and 1.25], $W_{\varphi}(i,V)$ is equidimensional of dimension $i-1$. It is worth noting that the latter can also be seen as a consequence of [Sha13, Theorem 1.25] and Lemma 7.5.1.

7.6 Proof of Proposition 7.2.13: atlases for polar varieties

This section is devoted to prove Proposition 7.2.13, that we recall below.

Proposition (7.2.13)**.** *Let $V,S\subset\mathbf{C}^n$ be two algebraic sets with V d-equidimensional and S finite and $\boldsymbol{\chi}$ be an atlas of (V,S). For $2\le\mathfrak{r}\le d+1$, let $\boldsymbol{\theta}=(\theta_1,\dots,\theta_{\mathfrak{r}})$ and $\boldsymbol{\xi}=(\xi_1,\dots,\xi_{\mathfrak{r}})$, and for $1\le j\le\mathfrak{r}$, let $\boldsymbol{\alpha}_j=(\alpha_{j,1},\dots,\alpha_{j,n})\in\mathbf{C}^n$ and*

$$\varphi_j(\boldsymbol{X},\boldsymbol{\alpha}_j)=\theta_j(\boldsymbol{X})+\sum_{k=1}^{n}\alpha_{j,k}x_k+\xi_j(\boldsymbol{\alpha}_j)\in\mathbf{C}[\boldsymbol{X}].$$

where $\theta_j\in\mathbf{C}[\boldsymbol{X}]$ and $\xi_j\colon\mathbf{C}^n\to\mathbf{C}$ is a polynomial map, with coefficients in $\mathbf{C}$.

There exists a non-empty Zariski open subset $\Omega_{\mathsf{W}}(\boldsymbol{\chi},V,S,\boldsymbol{\theta},\boldsymbol{\xi},\mathfrak{r})\subset\mathbf{C}^{\mathfrak{r}n}$ such that for every $\boldsymbol{\alpha}\in\Omega_{\mathsf{W}}(\boldsymbol{\chi},V,S,\boldsymbol{\theta},\boldsymbol{\xi},\mathfrak{r})$, writing $\boldsymbol{\varphi}=(\varphi_1(\boldsymbol{X},\boldsymbol{\alpha}),\dots,\varphi_{\mathfrak{r}}(\boldsymbol{X},\boldsymbol{\alpha}))$, the following holds. For i in $\{1,\dots,\mathfrak{r}\}$, either $W_{\boldsymbol{\varphi}}(i,V)$ is empty or

1. *$W_{\boldsymbol{\varphi}}(i,V)$ is an equidimensional algebraic set of dimension $i-1$;*
2. *if $2\le i\le(d+3)/2$, then $W_{\mathrm{atlas}}(\boldsymbol{\chi},V,S,\boldsymbol{\varphi},i)$ is an atlas of $(W_{\boldsymbol{\varphi}}(i,V),S)$ and $\mathrm{sing}(W_{\boldsymbol{\varphi}}(i,V))\subset S$.*

7.6.1 Regularity properties

In this subsection, we fix the three integers $(d,\mathfrak{r},i)$ such that $2\le\mathfrak{r}\le d+1\le n+1$ and $1\le i\le\mathfrak{r}$.

For $1\le j\le i$, let $a_j=(a_{j,1},\dots,a_{j,n})$ be new indeterminates, and let $\boldsymbol{A}=(a_j)_{1\le j\le i}$. For $1\le j\le i$, we will also denote by $\boldsymbol{A}_{\le j}$, the subfamily $(a_1,\dots,a_j)$. Finally, we consider sequences $\boldsymbol{h}=(h_1,\dots,h_c)\subset\mathbf{C}[\boldsymbol{X}]$, where $c=n-d$, and $\phi=(\phi_1,\dots,\phi_i)$ such that

$$\phi_j(\boldsymbol{X},a_j)=\theta_j(\boldsymbol{X})+\sum_{k=1}^{n}a_{j,k}x_k+\xi_j(a_j)\in\mathbf{C}[\boldsymbol{X},\boldsymbol{A}_{\le j}],$$

for $1\le j\le i$. We start by investigating the regular situation. The first step towards the proof of Proposition 7.2.13 is to establish the following statement.

Proposition 7.6.1. *There exists a non-empty Zariski open set $\Omega_i^{\boldsymbol{h}}\subset\mathbf{C}^{in}$, such that for all $\boldsymbol{\alpha}\in\Omega_i^{\boldsymbol{h}}$, and $\boldsymbol{\varphi}=\big(\phi_1(\boldsymbol{X},\boldsymbol{\alpha}_1),\dots,\phi_i(\boldsymbol{X},\boldsymbol{\alpha}_i)\big)\subset\mathbf{C}[\boldsymbol{X}]$, the following holds:*

1. *for all $\boldsymbol{y}\in\boldsymbol{V}_{reg}^{\circ}(\boldsymbol{h})$, there exists a c-minor m' of $\mathrm{Jac}(\boldsymbol{h})$ such that $m'(\boldsymbol{y})\neq0$;*

2. *the irreducible components of* $W_{\boldsymbol{\varphi}}(i, \boldsymbol{V}_{reg}(\boldsymbol{h}))$ *have dimension less than* $i-1$*;*

Assume now that $i \leq (d+3)/2$*, and let* m' *be any* c*-minor of* $\mathrm{Jac}(\boldsymbol{h})$ *and let* m'' *be any* $(c+i-1)$*-minors of* $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ *containing the rows of* $\mathrm{Jac}(\boldsymbol{\varphi}_i)$*. Then, the following holds:*

3. *for all* $\boldsymbol{y} \in \boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h})$ *there exists* m'' *as above, such that* $m''(\boldsymbol{y}) \neq 0$*;*

4. $W^{\circ}_{\boldsymbol{\varphi}}(i, \boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h}))$ *is defined on* $\mathcal{O}(m'm'')$ *by the vanishing of* $(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''))$*;*

5. $\mathrm{Jac}(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''))$ *has full rank* $n-(i-1)$ *on* $\mathcal{O}(m'm'') \cap W^{\circ}_{\boldsymbol{\varphi}}(i, \boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h}))$*.*

7.6.1.a. Rank estimates

We start by proving some genericity results on the ranks of some jacobian matrix. Two direct consequences (namely Corollaries 7.6.3 and 7.6.4) of Proposition 7.6.2 below will establish the third statement of Proposition 7.6.1.

Let $1 \leq p \leq n-1$ and $M(\boldsymbol{X}, \boldsymbol{A}_{\leq 1})$ be a $p \times n$ matrix with coefficients in $\mathbf{C}[\boldsymbol{X}, \boldsymbol{A}_{\leq 1}]$. For $1 \leq j \leq i$, let

$$J_j(\boldsymbol{X}, \boldsymbol{A}_{\leq j}) = \begin{bmatrix} & M(\boldsymbol{X}, \boldsymbol{A}_{\leq 1}) & \\ \partial_{x_1}\phi_1(\boldsymbol{X}, a_{1,1}) & \cdots & \partial_{x_n}\phi_1(\boldsymbol{X}, a_{1,n}) \\ \vdots & & \vdots \\ \partial_{x_1}\phi_j(\boldsymbol{X}, a_{j,1}) & \cdots & \partial_{x_n}\phi_j(\boldsymbol{X}, a_{j,n}) \end{bmatrix},$$

where for all $1 \leq k \leq i$ and $1 \leq \ell \leq n$, $\partial_{x_\ell}\phi_k = \frac{\partial \theta_k(\boldsymbol{X})}{\partial x_\ell} + a_{k,\ell} \in \mathbf{C}[\boldsymbol{X}, a_{k,\ell}]$. The Proposition 7.6.2 below generalizes [SS17, Proposition B.6]. Our proof follows the same pattern as the one of [SS17, Proposition B.6].

Proposition 7.6.2. *Assume that there exists a non-empty Zariski open subset* $\mathscr{E}_0 \subset \mathbf{C}^n$ *such that for all* $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h}) \times \mathscr{E}_0$*, the matrix* $M(\boldsymbol{y}, \boldsymbol{\alpha})$ *has full rank* p*. Then, for every*

$$1 \leq j \leq \min\{\, i,\, c-p+(d+3)/2 \,\},$$

there exists a non-empty Zariski open subset $\mathscr{E}_i \subset \mathbf{C}^{in}$ *such that for all* $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h}) \times \mathscr{E}_i$*,*

$$\operatorname{rank} M(\boldsymbol{y}, \boldsymbol{\alpha}) = p \quad \text{and} \quad \operatorname{rank} J_i(\boldsymbol{y}, \boldsymbol{\alpha}) \geq p+j-1.$$

Before proving the above proposition, we first give two direct consequences of it, whose conjunction proves the third item of Proposition 7.6.1. Taking $M = \mathrm{Jac}(\boldsymbol{h})$, the next lemma is a direct consequence of the definition of $\boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h})$.

Corollary 7.6.3. *If* $1 \leq i \leq (d+3)/2$ *then, there exists a non-empty Zariski open subset* $\mathscr{E}'_i \subset \mathbf{C}^{in}$ *such that for all* $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h}) \times \mathscr{E}'_i$*, the matrix* $\mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\alpha})}([\boldsymbol{h}, \phi])$ *has rank at least* $c+i-1$*.*

Besides we deduce the following more subtle consequence.

Corollary 7.6.4. *If $1 \leq i \leq (n+c+1)/2$ then, there exists a non-empty Zariski open subset $\mathscr{E}_i'' \subset \mathbf{C}^{in}$ such that for all $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}_{\text{reg}}^{\circ}(\boldsymbol{h}) \times \mathscr{E}_i''$, the matrix $\mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\alpha})}(\phi)$ has full rank i.*

Proof. Take $M = \mathrm{Jac}(\phi_1)$. The matrix $\mathrm{Jac}(\phi_1)$ has not full rank if, and only if, all the derivatives of ϕ_1 vanish at this point. Following the proof strategy of Lemma 7.6.6, let

$$Z^{\circ} = Z \cap \boldsymbol{V}_{\text{reg}}^{\circ}(\boldsymbol{h}) \subset \mathbf{C}^{n+n} \quad \text{where} \quad Z = \boldsymbol{V}\left(\boldsymbol{h}, \frac{\partial \phi_1}{\partial x_1}, \ldots, \frac{\partial \phi_1}{\partial x_n}\right).$$

whose following Jacobian matrix, has full rank $c+n$ at any $(\boldsymbol{y}, \boldsymbol{\alpha}) \in Z^{\circ}$

$$\mathrm{Jac}_{(\boldsymbol{X}, a_{1,1}, \ldots a_{1,n})}\left(\boldsymbol{h}, \frac{\partial \phi_1}{\partial x_1}, \ldots, \frac{\partial \phi_1}{\partial x_n}\right) = \left[\begin{array}{c|ccc} \mathrm{Jac}(\boldsymbol{h}) & \multicolumn{3}{c}{\boldsymbol{O}} \\ \hline * & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & 0 & \cdots & 1 \end{array}\right].$$

Hence, by the Jacobian criterion [Eis95, Theorem 16.19], Z° is either empty or a d-equidimensional locally closed set. Since $d < n$ by assumption, then the projection of Z° on the variables $\boldsymbol{A}_{\leq 1}$ is a proper subset of $\mathbf{C}^n$ and taking $\mathscr{E}_0$ as its complement allows us to conclude.

Indeed, for any $1 \leq i \leq (n+2)/2$, by Proposition 7.6.2, there exists a non-empty Zariski open subset $\mathscr{E}_i$ of $\mathbf{C}^{in}$ such that for all $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}_{\text{reg}}^{\circ}(\boldsymbol{h}) \times \mathscr{E}_i$,

$$\operatorname{rank} \mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\alpha})}(\phi_1, \ldots, \phi_i) = \operatorname{rank} \mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\alpha})}(\phi_1, \phi_1, \ldots, \phi_i) = 1 + i - 1 = i.$$

□

The rest of this paragraph is devoted to the proof of Proposition 7.6.2. Following the construction of the proof of [SS17, Proposition B.6], we proceed by induction on j. For all $1 \leq j \leq \min\{i, \lfloor c - p + (d+3)/2 \}$, we denote by R_j the statement of Proposition 7.6.2.

Initial case: $j = 1$. By assumption, there exists a non-empty Zariski open subset $\mathscr{E}_0 \subset \mathbf{C}^n$ such that for all $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}_{\text{reg}}^{\circ}(\boldsymbol{h}) \times \mathscr{E}_0$, the matrix $M(\boldsymbol{y}, \boldsymbol{\alpha}_1)$ has full rank p. Therefore, the matrix J_1, containing M, has rank at least p. This proves that R_1 holds.

Induction step: $2 \leq j \leq \min\{ i, c - p + (d+3)/2 \}$. Assume that R_{j-1} holds, and let us prove that so does R_j. Let $\mathfrak{M}$ be the set of ordered pairs $\mathfrak{m} = (\mathfrak{m}_r, \mathfrak{m}_c)$ where

- $\{1, \ldots, p\} \subset \mathfrak{m}_r \subset \{1, \ldots, p+j-1\}$
- $\mathfrak{m}_c \subset \{1, \ldots, n\}$
- $|\mathfrak{m}_r| = |\mathfrak{m}_c| = p + j - 2$

Then, for each such $\mathfrak{m}$, let $J_{\mathfrak{m}}$ be the square submatrix of J_j obtained by selecting the rows and the columns in respectively $\mathfrak{m}_r$ and $\mathfrak{m}_c$. Such a submatrix can also be obtained by removing from J_i, $n - p - j + 2$ columns and and two rows, which includes the last

row. Besides, let $\delta_{\mathfrak{m}} \in \mathbf{C}[\boldsymbol{X}, \boldsymbol{A}_{\leq j-1}]$ be the determinant of $J_{\mathfrak{m}}$, that is the $(p+j-2)$-minor of J_j associated to $\mathfrak{m}$. Finally, let Sub_j be the subset of $\mathfrak{m} \in \mathfrak{M}$ such that there exists $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}^{\circ}_{\text{reg}}(\boldsymbol{h}) \times \mathbf{C}^{jn}$ such that $\delta_{\mathfrak{m}}(\boldsymbol{y}, \boldsymbol{\alpha}) \neq 0$.

Lemma 7.6.5. *The set Sub_j, thus defined, is not empty.*

Proof. By induction assumption R_{j-1}, there exists a non-empty Zariski open subset $\mathscr{E}_{j-1} \subset \mathbf{C}^{(j-1)n}$ such that for all $(\boldsymbol{y}, \boldsymbol{\alpha}') \in \boldsymbol{V}^{\circ}_{\text{reg}}(\boldsymbol{h}) \times \mathscr{E}_{j-1}$, the matrix $J_{j-1}(\boldsymbol{y}, \boldsymbol{\alpha}')$ has rank at least $p+j-2$ and $M(\boldsymbol{y}, \boldsymbol{\alpha}')$ has full rank p. We deduce that there exists a non-zero $(p+j-2)$-minor of $J_{j-1}(\boldsymbol{y}, \boldsymbol{\alpha}')$ containing the rows of $M(\boldsymbol{y}, \boldsymbol{\alpha}')$. Then, by definition of $\mathfrak{M}$,

$$\forall (\boldsymbol{y}, \boldsymbol{\alpha}') \in \boldsymbol{V}^{\circ}_{\text{reg}}(\boldsymbol{h}) \times \mathscr{E}_{j-1},\ \exists \mathfrak{m} \in \mathfrak{M}, \quad \delta_{\mathfrak{m}}(\boldsymbol{y}, \boldsymbol{\alpha}') \neq 0, \tag{7.5}$$

where $\delta_{\mathfrak{m}} \in \mathbf{C}[\boldsymbol{X}, \boldsymbol{A}_{\leq j-1}]$. This proves, in particular, that Sub_j is not empty, as neither $\boldsymbol{V}_{\text{reg}}(\boldsymbol{h})$ nor $\mathscr{E}_{j-1}$ is empty. □

We now prove the following lemma, which is the key step in the proof of R_j.

Lemma 7.6.6. *For all $\mathfrak{m} \in \mathsf{Sub}_j$, there exists a non-empty Zariski open subset $\mathfrak{E}_{\mathfrak{m}} \subset \mathbf{C}^{jn}$ such that, for all $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h}) \times \mathfrak{E}_{\mathfrak{m}}$, if $\delta_{\mathfrak{m}}(\boldsymbol{y}, \boldsymbol{\alpha}) \neq 0$, then $J_j(\boldsymbol{y}, \boldsymbol{\alpha})$ has rank at least $p+j-1$.*

Proof. Let $\mathfrak{m} \in \mathsf{Sub}_j$, we proceed to show that the subset of the $\boldsymbol{\alpha} \in \mathbf{C}^{jn}$ such that, for all $\boldsymbol{y} \in \boldsymbol{V}^{\circ}_{\text{reg}}(\boldsymbol{h})$, $\delta_{\mathfrak{m}}(\boldsymbol{y}, \boldsymbol{\alpha}) \neq 0$ and $J_j(\boldsymbol{y}, \boldsymbol{\alpha})$ has rank at most $p+j-2$ is a *proper algebraic subset* of $\mathbf{C}^{jn}$. Then, taking the complement will give us $\mathfrak{E}_{\mathfrak{m}}$.

Up to reordering, assume that the rows and columns of J_j that are not in $J_{\mathfrak{m}}$ are the ones of respective indices $p+j-1, p+j$ (the last two rows) and $p-j+3, \ldots, n$ (the last $n-p+j-2$ columns). In other words, $(p+k, \ell) \notin \mathfrak{m}_r \times \mathfrak{m}_c$ for all $k \in \{j-1, j\}$ and $\ell \in \{p-j+3, \ldots, n\}$. For such k, ℓ, we denote by $\delta_{k,\ell}$ the minor of J_j obtained by adding to $J_{\mathfrak{m}}$ the row and column indexed by respectively $p+k$ and ℓ. Let $\boldsymbol{A}''$ be the subset of elements of $\boldsymbol{A}_{\leq}$ formed by the $2(n-p-j+2)$ indeterminates

$$a_{j-1,p-j+3}, \ldots, a_{j-1,n} \quad \text{and} \quad a_{j,p-i+3}, \ldots, a_{j,n},$$

and let $\boldsymbol{A}' = \boldsymbol{A}_{\leq j} - \boldsymbol{A}''$. Remark then that for any such $k \in \{j-1, j\}$ and $\ell \in \{p-j+3, \ldots, n\}$, by co-factor expansion there exists a polynomial $g_{k,\ell} \in \mathbf{C}[\boldsymbol{X}, \boldsymbol{A}']$ such that

$$\delta_{u,v} = \delta_{\mathfrak{m}} \cdot \frac{\partial \phi_k}{\partial x_\ell}(\boldsymbol{X}, a_{k,\ell}) + g_{k,\ell}(\boldsymbol{X}, \boldsymbol{A}') \tag{7.6}$$

Let $\boldsymbol{\delta}$ be the sequence of the $2(n-p-j+2)$ minors $\delta_{k,\ell}$. We proceed to prove that, the set of specialization values $\boldsymbol{\alpha} \in \mathbf{C}^{jn}$ of the genericity parameters (the entries of $\boldsymbol{A}_{\leq j}$), such that all these minors in $\boldsymbol{\delta}(\boldsymbol{X}, \boldsymbol{\alpha})$ are identically zero but not $\delta_{\mathfrak{m}}(\boldsymbol{X}, \boldsymbol{\alpha})$, is a proper algebraic subset of $\mathbf{C}^{jn}$. Hence, let t a new indeterminate and consider the locally closed set

$$Z^{\circ} = Z \cap \boldsymbol{V}^{\circ}_{\text{reg}}(\boldsymbol{h}) \subset \mathbf{C}^{n+jn+1} \quad \text{where} \quad Z = \boldsymbol{V}\left(\boldsymbol{h}, \boldsymbol{\delta}, 1 - t\delta_{\mathfrak{m}}\right).$$

One observes that if $(\boldsymbol{y}, \boldsymbol{\alpha}, t) \in Z^{\circ}$ then $\boldsymbol{y} \in \boldsymbol{V}^{\circ}_{\text{reg}}(\boldsymbol{h})$, $\delta_{\mathfrak{m}}(\boldsymbol{y}, \boldsymbol{\alpha}) \neq 0$ and all the $\delta_{k,\ell}$'s vanish.

We claim first that Z° is not empty. Indeed, since $\mathfrak{m} \in \mathsf{Sub}_j$, there exists $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}^\circ_{\mathrm{reg}}(\boldsymbol{h}) \times \mathbf{C}^{jn}$ such that $\delta_{\mathfrak{m}}(\boldsymbol{y}, \boldsymbol{\alpha}) \neq 0$. Since $\delta_{\mathfrak{m}} \in \mathbf{C}[\boldsymbol{X}, \boldsymbol{A}']$, it is independent of the entries of $\boldsymbol{A}''$. Besides, for any $k \in \{j-1, j\}$ and $\ell \in \{p-j+3, \ldots, n\}$,

$$\frac{\partial \phi_k}{\partial x_\ell}(\boldsymbol{y}, a_{k,\ell}) = \frac{\partial \theta_k}{\partial x_\ell}(\boldsymbol{X}) + a_{k,\ell} \in \mathbf{C}[\boldsymbol{X}][\boldsymbol{A}''] \tag{7.7}$$

is a non-constant polynomial in the entries of $\boldsymbol{A}''$. Then, according to (7.6), for every such k, ℓ, one can choose $\alpha_{k,\ell} \in \mathbf{C}$ such that $\delta_{k,\ell}(\boldsymbol{y}, \boldsymbol{\alpha}', \alpha_{k,\ell}) = 0$. Let $\widetilde{\boldsymbol{\alpha}}$ be the element of $\mathbf{C}^{jn}$ obtained by this choice, then

$$\left(\boldsymbol{y},\ \widetilde{\boldsymbol{\alpha}},\ 1/\delta_{\mathfrak{m}}(\boldsymbol{y}, \widetilde{\boldsymbol{\alpha}}) \right) \in Z^\circ.$$

We deduce that Z° is non-empty. We now estimate the dimension of Z° . According to (7.6) and (7.7) the following Jacobian matrix has full rank $c + 2(n-p-j+2)+1$ at every point of Z°:

$$\mathrm{Jac}_{(\boldsymbol{X}, \boldsymbol{A}', \boldsymbol{A}'', t)}(\boldsymbol{h}, \boldsymbol{\delta}, 1 - t\delta_{\mathfrak{m}}) = \left[\begin{array}{c|ccc|ccc|c} \mathrm{Jac}(\boldsymbol{h}) & \multicolumn{3}{c|}{\boldsymbol{O}} & \multicolumn{3}{c|}{\boldsymbol{O}} & 0 \\ \hline * & * & & * & \delta_{\mathfrak{m}} & 0 & \vdots & 0 \\ & & & & 0 & \ddots & 0 & \vdots \\ * & & * & & & 0 & \delta_{\mathfrak{m}} & 0 \\ \hline * & * & & * & * & * & * & \delta_{\mathfrak{m}} \end{array}\right].$$

Therefore, by the Jacobian criterion [Eis95, Theorem 16.19], Z° is an equidimensional locally closed set of dimension $jn - (n-p) + 2(j-2)$. Let $Z' \subset \mathbf{C}^{jn}$ be the Zariski closure of the projection of Z° on the coordinates associated to the variables $\boldsymbol{A}$, then

$$\dim Z' \leq \dim Z^\circ = jn + d - 2(n-p) + 2(j-2) < jn \qquad \text{since } j \leq c - p + (d+3)/2.$$

Hence Z' is a proper algebraic set of $\mathbf{C}^{jn}$, so that its complement $\mathscr{E}_{\mathfrak{m}}$ a non-empty Zariski open subset of $\mathbf{C}^{jn}$. Further, for any $(\boldsymbol{y}, \boldsymbol{\alpha}) \in \boldsymbol{V}^\circ_{\mathrm{reg}}(\boldsymbol{h}) \times \mathscr{E}_{\mathfrak{m}}$ such that $\delta_{\mathfrak{m}}$ does not vanish at $(\boldsymbol{y}, \boldsymbol{\alpha})$, the point

$$\left(\boldsymbol{y},\ \boldsymbol{\alpha},\ 1/\delta_{\mathfrak{m}}(\boldsymbol{y}, \boldsymbol{\alpha}) \right) \notin Z^\circ$$

otherwise $\boldsymbol{\alpha}$ would be in Z'. Hence, there exists (k, ℓ) as above such that $\delta_{k,\ell}(\boldsymbol{y}, \boldsymbol{\alpha}) \neq 0$, so that $J_j(\boldsymbol{y}, \boldsymbol{\alpha})$ has a non-zero $(c+j-1)$-minor, and then, has rank at least $c+j-1$. This proves the lemma. □

We can now conclude on the induction step as follows. Since, by Lemma 7.6.5, Sub_j is not empty, let

$$\mathscr{E}_j = (\mathscr{E}_{j-1} \times \mathbf{C}^n) \cap \bigcap_{\mathfrak{m} \in \mathsf{Sub}_j} \mathfrak{E}_{\mathfrak{m}},$$

where the $\mathfrak{E}_{\mathfrak{m}}$ are the non-empty Zariski open sets given by Lemma 7.6.6. Remark first that $\mathscr{E}_j$ is a non-empty Zariski open subset of $\mathbf{C}^{jn}$ since it is a finite intersection of non-empty Zariksi open sets. Let $(\boldsymbol{y}, \boldsymbol{\alpha}', \boldsymbol{\alpha}_j) \in \boldsymbol{V}^\circ_{\mathrm{reg}}(\boldsymbol{h}) \times \mathscr{E}_j$, as seen in (7.5), there exists $\mathfrak{m}_0 \in \mathsf{Sub}_j$ such

that $\delta_{\mathfrak{m}_0}(\boldsymbol{y}, \boldsymbol{\alpha}') \neq 0$. By construction, $\boldsymbol{\alpha} = (\boldsymbol{\alpha}', \boldsymbol{\alpha}_j)$ belongs to $\mathfrak{E}_{\mathfrak{m}_0}$ so that, by Lemma 7.6.6, $J_j(\boldsymbol{y}, \boldsymbol{\alpha})$ has rank at least $p + j - 1$. Besides, since $\boldsymbol{\alpha}' \in \mathscr{E}_{j-1}$, $M(\boldsymbol{y}, \boldsymbol{\alpha}')$ has full rank p.

In conclusion, we proved that R_j, which the induction step, and, by mathematical induction, this proves Proposition 7.6.2.

7.6.1.b. Dimension estimates

In this paragraph, we aim to prove the second point of Proposition 7.6.1, using transversality results. Let

$$\begin{array}{rccccccccccc} \Phi\colon & \mathbf{C}^n & \times & \mathbf{C}^{in} & \times & \mathbf{C}^c & \times & \mathbf{C}^i & \longrightarrow & \mathbf{C}^c & \times & \mathbf{C}^n \\ & (\ \boldsymbol{y} & , & \boldsymbol{\alpha} & , & \boldsymbol{\lambda} & , & \boldsymbol{\vartheta}\ ) & \longmapsto & \Big(\ \boldsymbol{h}(\boldsymbol{y}) & , & {}^t[\boldsymbol{\lambda}, \boldsymbol{\vartheta}] \cdot \mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\alpha})}(\boldsymbol{h}, \phi)\Big) \end{array}$$

and for any $\boldsymbol{\alpha} \in \mathbf{C}^{in}$, let $\Phi_{\boldsymbol{\alpha}} = (\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \mapsto \Phi(\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}, \boldsymbol{\alpha})$. The interest of such a map is illustrated by the following lemma. Let $\mathscr{A} \subset \mathbf{C}^{n+in+c+i}$ be the Zariski open subset of the elements $(\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta})$ where $\boldsymbol{\lambda} \neq \boldsymbol{O}$ and $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})$ has full rank.

Lemma 7.6.7. *Let $\boldsymbol{\alpha} \in \mathbf{C}^{in}$ and*

$$W^\circ_{\boldsymbol{\alpha}} = \Big\{\boldsymbol{y} \in \mathbf{C}^n \mid \boldsymbol{y} \in \boldsymbol{V}^\circ_{reg}(\boldsymbol{h}) \quad \textit{and} \quad \operatorname{rank} \mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\alpha})}(\boldsymbol{h}, \phi) \leq c + i - 1\Big\}.$$

Then $W^\circ_{\boldsymbol{\alpha}} = \pi_{\boldsymbol{X}}\big(\mathscr{A} \cap \Phi^{-1}_{\boldsymbol{\alpha}}(\boldsymbol{O})\big)$.

Proof. Let $\boldsymbol{\alpha} \in \mathbf{C}^{in}$ and $\boldsymbol{y} \in \boldsymbol{V}^\circ_{\mathrm{reg}}(\boldsymbol{h})$. Then $\boldsymbol{y} \in W^\circ_{\boldsymbol{\alpha}}$ if and only if $\mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\alpha})}(\boldsymbol{h}, \phi)$ has not full rank, which is equivalent to having a non-zero vector in its cokernel by duality. Besides, since $\boldsymbol{y} \in \boldsymbol{V}^\circ_{\mathrm{reg}}(\boldsymbol{h})$, the matrix $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})$ has full rank. Hence $\boldsymbol{y}$ belongs to $W^\circ_{\boldsymbol{\alpha}}$ if and only if there exists a non-zero vector $(\boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathbf{C}^{c+i}$ such that $\Phi(\boldsymbol{y}, \boldsymbol{\alpha}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) = 0$ and $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})$ has full rank. Finally $\boldsymbol{\vartheta}$ cannot be zero otherwise $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})$ would have a non-trivial left-kernel (containing $\boldsymbol{\lambda}$), and then would not be full rank. □

Lemma 7.6.8. *Let $\mathscr{A} \subset \mathbf{C}^{n+c+i}$ be the Zariski open subset of the elements $(\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta})$ where $\boldsymbol{\vartheta} \neq \boldsymbol{O}$ and $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})$ has full rank. There exists a non-empty Zariski open subset $\mathscr{D}_i \subset \mathbf{C}^{in}$ such that for all $\boldsymbol{\alpha} \in \mathscr{D}_i$, $\mathrm{Jac}_{(\boldsymbol{y},\boldsymbol{\lambda},\boldsymbol{\vartheta})} \Phi_{\boldsymbol{\alpha}}$ has full rank $c + n$ at any $(\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathscr{A} \cap \Phi^{-1}_{\boldsymbol{\alpha}}(\boldsymbol{O})$.*

Proof. We have

$$\mathrm{Jac}_{(\boldsymbol{X},\lambda,\vartheta,a_1,\ldots,a_i)} \Phi = \left[\begin{array}{c|c|ccc} \mathrm{Jac}(\boldsymbol{h}) & \boldsymbol{O} & \boldsymbol{O} & \cdots & \boldsymbol{O} \\ \hline * & * & \vartheta_1 I_n & \cdots & \vartheta_i I_n \end{array}\right]$$

where I_n is the identity matrix of size n. Let $\boldsymbol{\alpha} \in \mathbf{C}^{in}$, and $(\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathscr{A}$ such that the above Jacobian matrix has full rank $c + n$ at $(\boldsymbol{y}, \boldsymbol{\alpha}, \boldsymbol{\lambda}, \boldsymbol{\vartheta})$. Hence $\boldsymbol{O}$ is a regular value of Φ on $\mathscr{A} \times \mathbf{C}^{in}$. Therefore, by the Thom's weak transversality theorem [SS17, Proposition B.3], there exists a non-empty Zariski open subset $\mathscr{D}_i \subset \mathbf{C}^{in}$ such that for all $\boldsymbol{\alpha} \in \mathscr{D}_i$, $\boldsymbol{O}$ is a regular value of $\Phi_{\boldsymbol{\alpha}}$ on $\mathscr{A}$. In other words, for all $\boldsymbol{\alpha} \in \mathscr{D}_i$, the matrix $\mathrm{Jac}\, \Phi_{\boldsymbol{\alpha}}$ has full rank $c + n$ over $\mathscr{A} \cap \Phi^{-1}_{\boldsymbol{\alpha}}(\boldsymbol{O})$. □

Lemma 7.6.9. *Let $\mathscr{D}_i \subset \mathbf{C}^{in}$ be the non-empty Zariski subset defined in Lemma 7.6.8. Then, for all $\boldsymbol{\alpha} \in \mathscr{D}_i$, $W^\circ_{\boldsymbol{\alpha}}$ has dimension at most $i-1$.*

Proof. Let $\boldsymbol{\alpha} \in \mathscr{D}_i$ and suppose that $W^\circ_{\boldsymbol{\alpha}}$ is not empty. Then, according to Lemma 7.6.7, $\mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})$ is non-empty as well. By Lemma 7.6.8 and [SS17, Lemma A.1], $\mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})$ is a non-singular equidimensional locally closed set and

$$\dim\left(\mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})\right) = n + c + i - (c+n) = i.$$

Let C be the Zariski closure of $\mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})$ and $(C_j)_{1\le j\le \ell}$ be its irreducible components. For all $1 \le j \le \ell$, let T_j be the Zariski closure of $\pi_{\boldsymbol{X}}(C_j)$. Since $W^\circ_{\boldsymbol{\alpha}} \subset \bigcup_{1\le j\le \ell} T_j$, it is enough to prove that $\dim T_j \le i-1$ for all $1 \le j \le \ell$.

Fix $1 \le j \le \ell$. The restriction $\pi_{\boldsymbol{X}} \colon C_j \to T_j$ is a dominant regular map between two irreducible algebraic sets. Then one can apply the theorem on the dimension of fibers from [Sha13, Theorem 1.25] and claim that there exists a non-empty Zariski open subset Ω_1 of T_j such that

$$\forall \boldsymbol{z} \in \Omega_1,\ \dim\left(\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap C_j\right) = \dim C_j - \dim T_j = i - \dim T_j. \tag{7.8}$$

Then it is enough to prove that $\dim(\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap C_j) \ge 1$. Let $J' = \{1 \le k \le \ell \mid T_k = T_j\}$. Then it holds that

$$\Omega_2 = T_j - \bigcup_{k \notin J'} T_k$$

is a non-empty Zariski open subset of T_j. Besides, for all $\boldsymbol{z} \in \Omega_2$, $\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap C_j = \pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap C$ which is the Zariski closure of $\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap \mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})$ if and only if $\boldsymbol{z} \in W^\circ_{\boldsymbol{\alpha}}$ (otherwise it is empty).

However, by definition, $C'_j = \mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O}) \cap C_j$ is a non-empty Zariski open subset of C_j, and then $\pi_{\boldsymbol{X}}(C'_j)$ is a non-empty Zariski subset of T_j. Since it contains $\pi_{\boldsymbol{X}}(C'_j)$, the set $\Omega_3 = W^\circ_{\boldsymbol{\alpha}} \cap T_j$ is a non-empty Zariski open subset of T_j as well.

Now, let $\Omega = \Omega_1 \cap \Omega_2 \cap \Omega_3$, it is a non-empty (Zariski open) subset of T_j, and let $\boldsymbol{z} \in \Omega$. Since $\boldsymbol{z}$ is in Ω_3, it is in $W^\circ_{\boldsymbol{\alpha}}$ by definition. Besides, $\boldsymbol{z} \in \Omega_2$, so that

$$\dim(\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap C_j) = \dim\left(\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap \mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})\right).$$

Since $\boldsymbol{z} \in \Omega_1$, together with (7.8), one gets that

$$\forall \boldsymbol{z} \in \Omega,\quad \boldsymbol{z} \in W^\circ_{\boldsymbol{\alpha}} \quad \text{and} \quad \dim T_j = i - \dim\left(\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap \mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})\right), \tag{7.9}$$

Let $\boldsymbol{z} \in \Omega$, remark that

$$\pi_{\boldsymbol{X}}^{-1}(\boldsymbol{z}) \cap \mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O}) \ = \ \{\boldsymbol{z}\} \times \left(E_{\boldsymbol{z}} \cap \mathcal{O}(\vartheta_{e+1}, \ldots, \vartheta_i)\right)$$

where $E_{\boldsymbol{z}}$ is a linear subspace of $\mathbf{C}^{c+i}$. Indeed, $E_{\boldsymbol{z}}$ is defined by homogeneous linear equations in the entries of $(\boldsymbol{\lambda}, \boldsymbol{\vartheta})$. Since $\boldsymbol{z} \in W^\circ_{\boldsymbol{\alpha}} \subset \pi_{\boldsymbol{X}}(\mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O}))$, there exists a non-zero $(\boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathbf{C}^{c+i}$ such that $(\boldsymbol{z}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})$. Then $E_{\boldsymbol{z}}$ contains a non-zero vector, so that $\dim E_{\boldsymbol{z}} \ge 1$. Finally, injecting this inequality in (7.9) leads to $\dim T_j \le i-1$ as required. □

7.6.1.c. Proof of Proposition 7.6.1.

We can now tackle the proof of the main proposition of this subsection. Recall that we have fixed three integers $(d, \mathfrak{r}, i)$ such that $2 \leq \mathfrak{r} \leq d+1 \leq n+1$ and $1 \leq i \leq \mathfrak{r}$. Moreover, we consider polynomials $\boldsymbol{h} = (h_1, \ldots, h_c)$ in $\mathbf{C}[\boldsymbol{X}]$, where $c = n-d$. Finally, let $\phi = (\phi_1, \ldots, \phi_i)$, such that

$$\phi_j(\boldsymbol{X}, a_j) = \theta_j(\boldsymbol{X}) + \sum_{k=1}^{n} a_{j,k} x_k + \xi_j(a_j) \in \mathbf{C}[\boldsymbol{X}, \boldsymbol{A}_{\leq j}],$$

for all $1 \leq j \leq i$. Let $\Omega_i^{\boldsymbol{h}}$ be the non-empty Zariski open subset of $\mathbf{C}^{in}$ defined by

$$\Omega_i^{\boldsymbol{h}} = \begin{cases} \mathscr{D}_i \cap \mathscr{E}_i' \cap \mathscr{E}_i'' & \text{if } i \leq (d+3)/2; \\ \mathscr{D}_i & \text{else,} \end{cases}$$

where $\mathscr{D}_i$, $\mathscr{E}_i'$ and $\mathscr{E}_i''$ are the non-empty Zariski open sets given respectively by Lemma 7.6.8, Corollaries 7.6.3 and 7.6.4. Note that the assumptions of Corollary 7.6.4 since $d \leq n-1$.

Now let $\boldsymbol{\alpha} \in \Omega_i^{\boldsymbol{h}}$ and $\boldsymbol{\varphi} = (\phi_1(\boldsymbol{X}, \boldsymbol{\alpha}), \ldots, \phi_i(\boldsymbol{X}, \boldsymbol{\alpha}))$. The first item of the proposition is a direct consequence definition of $\boldsymbol{V}_{\text{reg}}^{\circ}(\boldsymbol{h})$. Besides, according to [SS17, Lemma A.2], the set $W_{\boldsymbol{\alpha}}^{\circ}$ defined in Lemma 7.6.7 is nothing but $W_{\boldsymbol{\varphi}}^{\circ}(i, \boldsymbol{V}_{\text{reg}}(\boldsymbol{h}))$, whose Zariski closure is $W_{\boldsymbol{\varphi}}^{\circ}(i, \boldsymbol{V}_{\text{reg}}(\boldsymbol{h}))$, by definition. Hence, since $\boldsymbol{\alpha} \in \mathscr{D}_i$, the second item is exactly the statement of Lemma 7.6.9.

Suppose now that $i \leq (d+3)/2$, so that $\boldsymbol{\alpha} \in \mathscr{E}_i' \cap \mathscr{E}_i''$. Hence, by Corollaries 7.6.3 and 7.6.4, for all $\boldsymbol{y} \in \boldsymbol{V}_{\text{reg}}^{\circ}(\boldsymbol{h})$,

$$\operatorname{rank} \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{\varphi}_i) = i \quad \text{and} \quad \operatorname{rank} \operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{h}, \boldsymbol{\varphi}_i) \geq c + i - 1.$$

Hence, there exists a $(c+i-1)$-minor m'' of $\operatorname{Jac}_{\boldsymbol{y}}(\boldsymbol{h}, \boldsymbol{\varphi}_i)$, containing the rows of $\operatorname{Jac}(\boldsymbol{\varphi}_i)$, that does not vanish at $\boldsymbol{y}$. This proves the third item.

In the remaining we proceed to prove the last two items. Let m' be a c-minor of $\operatorname{Jac}(\boldsymbol{h})$ and m'' be a $(c+i-1)$-minor of $\operatorname{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ containing the rows of $\operatorname{Jac}(\boldsymbol{\varphi}_i)$. Assume, without loss of generality, that m'' is not the zero polynomial. The next lemma establishes the second to last item of Proposition 7.6.1.

Lemma 7.6.10. *Let m' and m'' as above. The set $W_{\boldsymbol{\varphi}}^{\circ}(i, \boldsymbol{V}_{reg}^{\circ}(\boldsymbol{h}))$ is defined on $\mathcal{O}(m'm'')$ by the vanishing set of the polynomials $(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''))$. Equivalently,*

$$\mathcal{O}(m'm'') \cap W_{\boldsymbol{\varphi}}^{\circ}(i, \boldsymbol{V}_{reg}^{\circ}(\boldsymbol{h})) = \mathcal{O}(m'm'') \cap \boldsymbol{V}\big(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')\big).$$

Proof. Inside the Zariski open set $\mathcal{O}(m')$, the matrix $\operatorname{Jac}(\boldsymbol{h})$ has full rank, which implies by [SS17, Lemma A.2] that

$$\mathcal{O}(m') \cap W_{\boldsymbol{\varphi}}^{\circ}(i, \boldsymbol{V}_{\text{reg}}^{\circ}(\boldsymbol{h})) = \mathcal{O}(m') \cap \Big\{ \boldsymbol{y} \in \boldsymbol{V}(\boldsymbol{h}) \mid \operatorname{rank}(\operatorname{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i]) < c + i \Big\}.$$

Besides, by the exchange lemma [BGHM01, Lemma 1], if m is a $(c+i)$-minor of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$, then one can write

$$m''m = \sum_{j=1} \varepsilon_j m_j m''_j \quad \text{where } \varepsilon_j = \pm 1 \quad \text{and} \quad N \in \{1, \dots, d-i+1\}$$

and where m''_j (resp. m_j) is obtained by successively adding to m'' (resp. removing to m) the missing row and a missing column of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ that are in m. Remark that, for such a m, all the m''_j's are in $\mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')$, by definition.

Hence, for all $\boldsymbol{y} \in \boldsymbol{V}(\boldsymbol{h})$, if $m''(\boldsymbol{y}) \neq 0$, then all the $(c+i)$-minors of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ vanish at $\boldsymbol{y}$ if and only if all the polynomials of $\mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')$ vanish at $\boldsymbol{y}$. In other words:

$$\mathcal{O}(m'm'') \cap W^{\circ}_{\boldsymbol{\varphi}}(i, \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h})) = \mathcal{O}(m'm'') \cap \boldsymbol{V}\big(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')\big).$$

□

In order to prove the the last item of Proposition 7.6.1, we need introduce Lagrange systems for general polynomial applications. This generalizes, in some sense, the construction of [SS17, Subsection 5.1], also presented in Subsection 7.4.3.

Let $L_1, \dots, L_c$ and $T_1, \dots, T_i$ be new indeterminates, since $m'' \neq 0$, consider the ring of rational fractions $\mathbf{C}[\boldsymbol{X}, L_1, \dots, L_c, T_1, \dots, T_i]_{m''}$ that are of the form $f/(m'')^r$, for $f \in \mathbf{C}[\boldsymbol{X}, L_1, \dots, L_c, T_1, \dots, T_i]$ and $r \in \mathbb{N}$. This the localization ring at the multiplicative set $\{(m'')^r \mid r \in \mathbb{N}\}$.

Let $\mathcal{I}_W$ the ideal of $\mathbf{C}[\boldsymbol{X}, L_1, \dots, L_c, T_1, \dots, T_i]_{m''}$ generated by the entries of

$$\boldsymbol{h}, \quad [L_1, \dots, L_c, T_1, \dots, T_i] \cdot \begin{bmatrix} \mathrm{Jac}(\boldsymbol{h}) \\ \mathrm{Jac}(\boldsymbol{\varphi}_i) \end{bmatrix}.$$

The following lemma is an immediate generalization of [SS17, Proposition 5.2.].

Lemma 7.6.11. *Let $1 \leq \iota \leq c$ such that the index of the row of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$ not in m'' has index ι. Then there exist $(\lambda_j)_{1 \leq j \neq \iota \leq c}$ and $(\tau_j)_{1 \leq j \leq i}$ in $\mathbf{C}[\boldsymbol{X}]_{m''}$ such that $\mathcal{I}_W$ is generated by the entries of*

$$\boldsymbol{h}, \quad L_\iota \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''), \quad (L_j - \lambda_j L_\iota)_{1 \leq j \neq \iota \leq c}, \quad (T_j - \tau_j L_\iota)_{1 \leq j \leq i}. \tag{7.10}$$

Proof. For the sake of simplicity, suppose that m'' is the lower-left minor of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$, so that $\iota = 1$. Then $\mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')$ is the sequence of minors obtained by adding the first row and columns in the ones of index $c+i, \dots, n$. We denote by $M_1, \dots, M_{n-c-i+1}$ these minors. Then, we write

$$\mathrm{Jac}(\boldsymbol{h}, \boldsymbol{\varphi}_i) = \begin{pmatrix} \boldsymbol{u}_{1,c+i-1} & \boldsymbol{w}_{1,n-c-i+1} \\ \boldsymbol{m}_{c+i-1,c+i-1} & \boldsymbol{v}_{c+i-1,n-c-i+1} \end{pmatrix}$$

such that $m'' = \det(\boldsymbol{m})$ and the indices are the dimensions of the submatrices. As m'' is not zero, it is a unit of $\mathbf{C}[\boldsymbol{X}, L_1, \dots, L_c, T_1, \dots, T_i]_{m''}$, so that $\boldsymbol{m}$ has an inverse with coefficients

in the same ring, given by m''^{-1} and the cofactor matrix of $\boldsymbol{m}$. Hence $\mathcal{I}_W$ is generated by the entries of $\boldsymbol{h}$ and

$$[L_1,\dots,L_c,T_1,\dots,T_i]\cdot \mathrm{Jac}([\boldsymbol{h},\boldsymbol{\varphi}_i])\cdot \begin{bmatrix} \boldsymbol{m}^{-1} & \boldsymbol{O} \\ \boldsymbol{O} & 1 \end{bmatrix}\cdot \begin{bmatrix} I_{c+i-1} & -\boldsymbol{v} \\ \boldsymbol{O} & 1 \end{bmatrix}$$

$$= \quad [L_1,\dots,L_c,T_1,\dots,T_i]\cdot \begin{bmatrix} \boldsymbol{u}\boldsymbol{m}^{-1} & \boldsymbol{w}-\boldsymbol{u}\boldsymbol{m}^{-1}\boldsymbol{v} \\ I_{c+i-1} & \boldsymbol{O} \end{bmatrix},$$

where I_{c+i-1} is the identity matrix of size $c+i-1$. The first $c-1$ entries are the $L_j - [\boldsymbol{u}\boldsymbol{m}^{-1}]_j L_1$ for $1<j\le c$ and the i followings are the $T_j - [\boldsymbol{u}\boldsymbol{m}^{-1}]_j L_1$ for $1\le j\le i$. Hence taking $(\boldsymbol{\lambda},\boldsymbol{\tau}) = \boldsymbol{u}\boldsymbol{m}^{-1}$ gives the last terms in (7.10).

Finally, since $\boldsymbol{m}$ is invertible, we can compute the minors $M_1,\dots,M_{n-c-i+1}$ of $\mathrm{Jac}(\boldsymbol{h},\boldsymbol{\varphi}_i)$, using the block structure we described above (see e.g. [Ber09, Proposition 2.8.3] and [Sil00, Theorem 1]) to obtain that for all $1\le j\le n-c-i+1$,

$$M_j = (-1)^{c+i-1} m''[\boldsymbol{w}-\boldsymbol{u}\boldsymbol{m}^{-1}\boldsymbol{v}]_j.$$

Hence, the last $n-c-i+1$ entries are, except for the sign, $L_1M_1/m'',\dots,L_1M_{n-c-i+1}/m''$, we are done. □

The next lemma ends the proof of the last item Proposition 7.6.1, and then conclude the proof of the whole Proposition.

Lemma 7.6.12. *The Jacobian matrix associated to the polynomials in $(\boldsymbol{h},\mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h},i,m''))$ has full rank $n-(i-1)$ at every point of the set $\mathcal{O}(m'm'')\ \cap\ W^{\circ}_{\boldsymbol{\varphi}}(i,\boldsymbol{V}^{\circ}_{reg}(\boldsymbol{h}))$.*

Proof. Recall that $\boldsymbol{\varphi} = (\phi_1(\boldsymbol{X},\boldsymbol{\alpha}),\dots,\phi_i(\boldsymbol{X},\alpha))$, where $\boldsymbol{\alpha}\in\Omega^{\boldsymbol{h}}_i$. Then, remark that

$$\left(\boldsymbol{h}(\boldsymbol{X}),\quad [L_1,\dots,L_c,T_1,\dots,T_i]\cdot\begin{bmatrix}\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{h})\\ \mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{\varphi}_i)\end{bmatrix}\right) = \Phi_{\boldsymbol{\alpha}}\Big(\boldsymbol{X},L_1,\dots,L_c,T_1,\dots,T_i\Big),$$

where $\Phi_{\boldsymbol{\alpha}}$ is the polynomial map considered in Lemma 7.6.8. Let $(\lambda_j)_{1\le j\ne\iota\le c}$ and $(\tau_j)_{1\le j\le i}$ in $\mathbf{C}[\boldsymbol{X}]_{m''}$ given by Lemma 7.6.11.

Now fix $\boldsymbol{y}\in\mathcal{O}(m'm'')\cap W_{\boldsymbol{\varphi}}(i,\boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h}))$, and let $\boldsymbol{\lambda} = (\boldsymbol{\lambda}_j)_{1\le j\le c}$ and $\boldsymbol{\vartheta} = (\boldsymbol{\vartheta}_j)_{1\le j\le i}$ where

$$\boldsymbol{\lambda}_\iota = 1 \quad\text{and}\quad \boldsymbol{\lambda}_j = \lambda_j(\boldsymbol{y}) \text{ for all } 1\le j\ne\iota\le c,$$
$$\boldsymbol{\vartheta}_j = \tau_j(\boldsymbol{y}) \text{ for all } 1\le j\le i.$$

These are well defined since $m''(\boldsymbol{y})\ne 0$. Since $\boldsymbol{h}$ and $\mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h},i,m'')$ vanish at $\boldsymbol{y}$, by Lemma 7.6.10, all the polynomials in (7.10) vanish at $(\boldsymbol{y},\boldsymbol{\lambda},\boldsymbol{\vartheta})$. Moreover, according to Lemma 7.6.11 and the above remark, the polynomials in (7.10) and the entries of $\Phi_{\boldsymbol{\alpha}}(\boldsymbol{X},L_1,\dots,L_c,T_1,\dots,T_i)$ generates the same ideal $\mathcal{I}_W$ in $\mathbf{C}[\boldsymbol{X}]_{m''}$. Hence, since $m''(\boldsymbol{y})\ne 0$, the entries of $\Phi_{\boldsymbol{\alpha}}$ vanish at $(\boldsymbol{y},\boldsymbol{\lambda},\boldsymbol{\vartheta})$ as well, that is $\Phi_{\boldsymbol{\alpha}}(\boldsymbol{y},\boldsymbol{\lambda},\boldsymbol{\vartheta}) = \boldsymbol{O}$

Besides, since $\boldsymbol{y} \in \mathcal{O}(m')$, then $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h})$ has full rank. Then, $\boldsymbol{\vartheta}$ cannot be zero, since $\boldsymbol{\lambda} \neq \boldsymbol{O}\ \mathrm{Jac}(\boldsymbol{h})$ has a trivial left-kernel. Hence, according to the notation of Lemma 7.6.8, $(\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathscr{A} \cap \Phi_{\boldsymbol{\alpha}}^{-1}(\boldsymbol{O})$. Therefore, by Lemma 7.6.8, $\mathrm{Jac}\,\Phi_{\boldsymbol{\alpha}}$ has full rank $n+c$ at $(\boldsymbol{y}, \boldsymbol{\lambda}, \boldsymbol{\vartheta})$, as $\boldsymbol{\alpha} \in \mathscr{D}_i \subset \Omega_i^{\boldsymbol{h}}$.

Finally, remark that the sequence of polynomials in (7.10) has length $n+c$. Hence, since the latters generate the same ideal than the entries of the entries of $\Phi_{\boldsymbol{\alpha}}(\boldsymbol{X}, L_1, \ldots, L_c, T_1, \ldots, T_i)$, their Jacobian matrix has full rank $n+c$ at this point as well. Computing this Jacobian matrix the latter rank statement amounts to the Jacobian matrix of

$$\Big(\boldsymbol{h},\ \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')\Big)$$

having full rank $n-(i-1)$ at $\boldsymbol{y}$. □

7.6.2 Proof of Proposition 7.2.13

Let $V, S \subset \mathbf{C}^n$ be be two algebraic sets with V d-equidimensional and S finite, and let $\boldsymbol{\chi} = (\chi_j)_{1 \leq j \leq s}$ be an atlas of (V, S) with $\chi_j = (m_j, \boldsymbol{h}_j)$ for $1 \leq j \leq s$. According to [SS17, Lemma A.12], all the $\boldsymbol{h}_j$'s have same cardinality $c = n - d$.

Besides, let $2 \leq \mathfrak{r} \leq d+1$ and the sequences $\boldsymbol{\theta} = (\theta_1, \ldots, \xi_{\mathfrak{r}})$ and $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_{\mathfrak{r}})$ in $\mathbf{C}[\boldsymbol{X}]$. For $1 \leq j \leq \mathfrak{r}$, let $\boldsymbol{\alpha}_j = (\alpha_{j,1}, \ldots, \alpha_{j,n}) \in \mathbf{C}^n$ and

$$\varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \theta_j(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{j,k} x_k + \xi_j(\boldsymbol{\alpha}_j) \in \mathbf{C}[\boldsymbol{X}].$$

Then, for $1 \leq i \leq \mathfrak{r}$, we can apply Proposition 7.6.1 to the sequences $\boldsymbol{h}_j$, $\boldsymbol{\theta}$ and $\boldsymbol{\xi}$, there exist a non-empty Zariski open subset $\Omega(\boldsymbol{h}_j, i)$ of $\mathbf{C}^{in}$ such that for all $\boldsymbol{\alpha} \in \Omega(\boldsymbol{h}_j, i)$, the sequence $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}), \ldots, \varphi_i(\boldsymbol{X}, \boldsymbol{\alpha}))$ satisfies the statements of Proposition 7.6.1. Then we define the following non-empty Zariski open subset of $\mathbf{C}^{\mathfrak{r}n}$,

$$\Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, S, \boldsymbol{\theta}, \boldsymbol{\xi}, \mathfrak{r}) = \bigcap_{1 \leq i \leq \mathfrak{r}} \bigcap_{1 \leq j \leq s} \Omega(\boldsymbol{h}_j, i) \times \mathbf{C}^{(\mathfrak{r}-i)n}.$$

Fix now $\boldsymbol{\alpha} \in \Omega_{\mathsf{W}}(\boldsymbol{\chi}, V, S, \boldsymbol{\theta}, \boldsymbol{\xi}, \mathfrak{r})$ and $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}), \ldots, \varphi_{\mathfrak{r}}(\boldsymbol{X}, \boldsymbol{\alpha}))$. From now on, fix also $1 \leq i \leq \mathfrak{r}$ and suppose that $W_{\boldsymbol{\varphi}}(i, V)$ is not empty. In the following, and for conciseness, we might identify $\Omega(\boldsymbol{h}_j, i)$ to $\Omega(\boldsymbol{h}_j, i) \times \mathbf{C}^{(\mathfrak{r}-i)n}$. in a straightforward way. We start with the first item statement of Proposition 7.2.13. Again, it is proved through the properties of atlases, but when i is restricted to some values.

Lemma 7.6.13. *The algebraic set $W_{\boldsymbol{\varphi}}(i, V)$ is equidimensional of dimension $i-1$.*

Proof. By Lemma 7.2.7, for all $1 \leq j \leq s$, as χ_j is a chart of (V, S) then,

$$\mathcal{O}(m_j) \cap W_{\boldsymbol{\varphi}}(i, V) - S \ = \ \mathcal{O}(m_j) \cap W^{\circ}_{\boldsymbol{\varphi}}(i, \boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j)) - S.$$

Let $\boldsymbol{y} \in W_{\boldsymbol{\varphi}}(i, V) - S$. Since $\boldsymbol{y} \in V$, by property A_3 of the atlas $\boldsymbol{\chi}$, there exists $j \in \{1, \ldots, s\}$ such that $\boldsymbol{y} \in \mathcal{O}(m_j)$. Hence, by the above equality, in $\mathcal{O}(m_j) - S$, the irreducible component of $W_{\boldsymbol{\varphi}}(i, V)$ containing $\boldsymbol{y}$ coincides with the one of $W_{\boldsymbol{\varphi}}(i, \boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}_j))$ containing $\boldsymbol{y}$. Since these

irreducible components are equal over a non-empty Zariski open set, they have the same dimension (see e.g. [Ful08, Proposition 10.(1)]). By the second item of Proposition 7.6.1, since $\boldsymbol{\alpha} \in \Omega(\boldsymbol{h}_j, i)$, this dimension is less than $i-1$.

We just showed that the Zariski closure of $W_{\boldsymbol{\varphi}}(i,V) - S$ has dimension less than $i-1$. If $i = 1$, since S is finite this means that $W_{\boldsymbol{\varphi}}(i,V)$ is finite as well and we are done. If $i \geq 2$, then by Lemma 7.5.1, the irreducible components of $W_{\boldsymbol{\varphi}}(i,V)$ have dimension at least $i-1 \geq 1$ so that the Zariski closure of $W_{\boldsymbol{\varphi}}(i,V) - S$ is $W_{\boldsymbol{\varphi}}(i,V)$. Hence the irreducible components of $W_{\boldsymbol{\varphi}}(i,V)$ have dimension exactly $i-1$ □

We now prove a strict generalization of [SS17, Lemma B.12.] which gives the key arguments for the proof of the second item statement of Proposition 7.2.13.

Lemma 7.6.14. *Let $\chi = (m, \boldsymbol{h})$ be a chart of (V,S). Then for any c-minor m' of $\mathrm{Jac}(\boldsymbol{h})$ and any $(c+i-1)$-minor m'' of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$, containing the rows of $\mathrm{Jac}(\boldsymbol{\varphi}_i)$, the following holds.*

1. *The sets $\mathcal{O}(mm'm'') \cap W_{\boldsymbol{\varphi}}(i,V) - S$ and $\mathcal{O}(mm'm'') \cap \boldsymbol{V}(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m'')) - S$ coincides;*
2. *if they are not empty, then $W_{\mathrm{chart}}(\chi, m', m'')$ is a chart of $(W_{\boldsymbol{\varphi}}(i,V), S)$.*

Moreover, if $i \leq (d+3)/2$ then the following holds.

3. *The sets $\mathcal{O}(mm'm'') - S$, for all m', m'' as above, cover $\mathcal{O}(m) \cap V - S$;*
4. *the sets $\mathcal{O}(mm'm'') - S$, for all m', m'' as above, $\mathcal{O}(m) \cap W_{\boldsymbol{\varphi}}(i,V) - S$.*

Proof. By Lemma 7.2.7, since χ is a chart of (V,S),

$$\mathcal{O}(m) \cap W_{\boldsymbol{\varphi}}(i,V) - S = \mathcal{O}(m) \cap W^{\circ}_{\boldsymbol{\varphi}}(i, \boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h})) - S.$$

Besides, by the second to last item of Proposition 7.6.1, $W^{\circ}_{\boldsymbol{\varphi}}(i, \boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}))$ is defined in $\mathcal{O}(m'm'')$ by the vanishing of the polynomials $(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''))$, so that

$$\mathcal{O}(mm'm'') \cap W_{\boldsymbol{\varphi}}(i,V) - S = \mathcal{O}(mm'm'') \cap \boldsymbol{V}(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}_j, i, m'')) - S. \tag{7.11}$$

The first item is proved. Suppose now that the former sets are not-empty, we proceed to prove that $W_{\mathrm{chart}}(\chi, m', m'')$ is a chart of $(W_{\boldsymbol{\varphi}}(i,V), S)$. Property C_1 holds by assumption, while property C_2 of $W_{\mathrm{chart}}(\chi, m', m'')$ is exactly equation (7.11). Besides, since $(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}_j, i, m''))$ has length $n - i - 1 \leq n$, then C_3 holds as well. Finally, by the last item of Proposition 7.6.1, $\mathrm{Jac}(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''))$ has full rank on

$$\mathcal{O}(m'm'') \cap W^{\circ}_{\boldsymbol{\varphi}}(\boldsymbol{V}_{\mathrm{reg}}(\boldsymbol{h}), V).$$

Then, by (7.11), $\mathrm{Jac}(\boldsymbol{h}, \mathcal{H}_{\boldsymbol{\varphi}}(\boldsymbol{h}, i, m''))$ has full rank on $\mathcal{O}(mm'm'') \cap W_{\boldsymbol{\varphi}}(i,V) - S$. This proves that $W_{\mathrm{chart}}(\chi, m', m'')$ satisfies the last property C_4 of charts and the second statement of the lemma is proved.

Suppose now that $i \leq (d+3)/2$ and let $\boldsymbol{y} \in \mathcal{O}(m) \cap V - S$. Then, by property C_4 of χ, $\mathrm{Jac}(\boldsymbol{h})$ has full rank in $\boldsymbol{y}$, so that $\boldsymbol{y} \in \boldsymbol{V}^{\circ}_{\mathrm{reg}}(\boldsymbol{h})$. Therefore, by the first and third item of Proposition 7.6.1, there exists a c-minor m' of $\mathrm{Jac}(\boldsymbol{h})$ and a $(c+i-1)$-minor

m'' of $\mathrm{Jac}([\boldsymbol{h}, \boldsymbol{\varphi}_i])$, containing the rows of $\mathrm{Jac}(\boldsymbol{\varphi}_i)$, such that $(m'm'')(\boldsymbol{y}) \neq 0$. Hence $\boldsymbol{y} \in \mathcal{O}(mm'm'') - S$ and the third item of the lemma is proved.

Finally, if $\boldsymbol{y} \in \mathcal{O}(m) \cap W_{\boldsymbol{\varphi}}(i, V) - S$, then one still has $\boldsymbol{y} \in \mathcal{O}(mm'm'') - S$, as $W_{\boldsymbol{\varphi}}(i, V) \subset V$. This proves the last item. □

We can now prove the second statement of Proposition 7.2.13. With the above lemmas, it is mainly a matter of verification. Suppose that $2 \leq i \leq (d+3)/2$. We prove that $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, i)$ is an atlas of $(W_{\boldsymbol{\varphi}}(i, V), S)$. In the following, for $1 \leq j \leq s$, we refer to m'_j and m''_j as respectively a c-minor of $\mathrm{Jac}(\boldsymbol{h}_j)$ and a $(c+i-1)$-minor of $\mathrm{Jac}([\boldsymbol{h}_j, \boldsymbol{\varphi}_i])$, containing the rows of $\mathrm{Jac}(\boldsymbol{\varphi}_i)$.

A_1 : Since, by Lemma 7.6.13, $W_{\boldsymbol{\varphi}}(i, V)$ has dimension at least 1, it is not contained in S. In particular, there exists $1 \leq j \leq s$ such that $\mathcal{O}(m_j) \cap W_{\boldsymbol{\varphi}}(i, V) - S$ is not empty. Hence, by the third item of Lemma 7.6.14, there exist minors m'_j and m''_j such that $\mathcal{O}(m_j m'_j m''_j) \cap W_{\boldsymbol{\varphi}}(i, V) - S$ is not empty.

A_2 : For m_j,m'_j and m''_j as in the previous item, since $\mathcal{O}(m_j m'_j m''_j) \cap W_{\boldsymbol{\varphi}}(i, V) - S$ is not empty, then the second item of Lemma 7.6.14 shows that $W_{\mathrm{chart}}(\chi_j, m'_j, m''_j)$ is a chart of $(W_{\boldsymbol{\varphi}}(i, V), S)$.

A_3 : Let $\boldsymbol{y} \in W_{\boldsymbol{\varphi}}(i, V) - S$, by property A_3 of $\boldsymbol{\chi}$ there exists $1 \leq j \leq s$ such that $\boldsymbol{y} \in \mathcal{O}(m_j)$. Then, by the third item of Lemma 7.6.14, there exist m'_j and m''_j as in the previous points such that $\boldsymbol{y} \in \mathcal{O}(m_j m'_j m''_j)$. In particular $\mathcal{O}(m_j m'_j m''_j) \cap W_{\boldsymbol{\varphi}}(i, V) - S$ is not empty.

Hence $W_{\mathrm{atlas}}(\boldsymbol{\chi}, V, S, \boldsymbol{\varphi}, i)$ is an atlas of $(W_{\boldsymbol{\varphi}}(i, V), S)$, and since we proved that $W_{\boldsymbol{\varphi}}(i, V)$ is equidimensional, then by [SS17, Lemma A.12] $\mathrm{sing}(W_{\boldsymbol{\varphi}}(i, V)) \subset S$.

7.7 Proof of Proposition 7.2.16: atlases for fibers

This section is devoted to the proof of Proposition 7.2.16. We recall its statement below.

Proposition (7.2.16). *Let $V, S \subset \mathbf{C}^n$ be two algebraic sets with V d-equidimensional and S finite. Let $\boldsymbol{\chi}$ be an atlas of (V, S). Let $2 \leq \mathfrak{r} \leq d+1$ and $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_{\mathfrak{r}}) \subset \mathbf{C}[\boldsymbol{X}]$. For $2 \leq j \leq d$, let $\boldsymbol{\alpha}_j = (\alpha_{j,1}, \ldots, \alpha_{j,n}) \in \mathbf{C}^n$ and*

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{1,k} x_k \quad \text{and} \quad \varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \sum_{k=1}^{n} \alpha_{j,k} x_k$$

where $\theta \in \mathbf{C}[\boldsymbol{X}]$.

There exists a non-empty Zariski open subset $\Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, S, \theta, \mathfrak{r}) \subset \mathbf{C}^{\mathfrak{r}n}$ such that for every $\boldsymbol{\alpha} = (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_{\mathfrak{r}}) \in \Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, S, \theta, \mathfrak{r})$ and writing $\boldsymbol{\varphi} = (\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1), \ldots, \varphi_{\mathfrak{r}}(\boldsymbol{X}, \boldsymbol{\alpha}_{\mathfrak{r}}))$, the following holds. Let $0 \leq e \leq d$, $Q \in \mathbf{C}^e$ a finite subset and F_Q and S_Q be as in Definition 7.2.15. Then either F_Q is empty or

1. *S_Q is finite;*

2. *V_Q is an equidimensional algebraic set of dimension $d-e$;*

3. *$F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$ is an atlas of (F_Q, S_Q) and $\mathrm{sing}(F_Q) \subset S_Q$.*

Let V, S and $\boldsymbol{\chi} = (\chi_j)_{1\leq j\leq s}$ be as above, with $\chi_j = (m_j, \boldsymbol{h}_j)$ for $1 \leq j \leq s$. Consider and integer $2 \leq \mathfrak{r} \leq d+1$, we show in the following that it suffices to take $\Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, Q, S, \theta, \mathfrak{r})$ as the non-empty Zariski open subset $\Omega_{\mathsf{l}}(V, \theta, \mathfrak{r})$ of $\mathbf{C}^{\mathfrak{r}n}$ obtained by the application of Proposition 7.2.3 to V, θ and $\mathfrak{r}$.

Let $\boldsymbol{\alpha} \in \Omega_{\mathsf{F}}(\boldsymbol{\chi}, V, S, \theta, \mathfrak{r})$ and $\varphi = (\boldsymbol{\varphi}_1(\boldsymbol{X}, \boldsymbol{\alpha}), \ldots, \boldsymbol{\varphi}_{\mathfrak{r}}(\boldsymbol{X}, \boldsymbol{\alpha}))$ where for $2 \leq j \leq \mathfrak{r}$,

$$\varphi_1(\boldsymbol{X}, \boldsymbol{\alpha}_1) = \theta(\boldsymbol{X}) + \sum_{k=1}^{n} \alpha_{1,k} x_k \quad \text{and} \quad \varphi_j(\boldsymbol{X}, \boldsymbol{\alpha}_j) = \sum_{k=1}^{n} \alpha_{j,k} x_k$$

For $1 \leq e \leq \mathfrak{r}-1$, let $Q \subset \mathbf{C}^e$ be a finite set and F_Q, S_Q as in Definition 7.2.15. Suppose also that F_Q is not empty. We start with the following lemma, proving local statements on the fibers. It is a direct generalization of [SS17, Lemma C.1].

Lemma 7.7.1. *Let $1 \leq j \leq s$ and $m = m_j$, $\boldsymbol{h} = \boldsymbol{h}_j$ and $\chi = (m, \boldsymbol{h})$. Then either $\mathcal{O}(m) \cap F_Q$ is empty or χ is a chart of $(F_Q, Q, S_Q, \boldsymbol{\varphi})$, and S_Q is finite.*

Proof. Remark first that since $\boldsymbol{\alpha} \in \Omega(V, \theta)$, then by Proposition 7.2.3, the set

$$S_Q = \big(S \cup W_{\boldsymbol{\varphi}}(e, V)\big) \cap \boldsymbol{\varphi}_e^{-1}(Q)$$

is finite, since S and Q are. Assume now that $\mathcal{O}(m) \cap F_Q$ is not empty, then let us prove that χ is a chart of $(F_Q, Q, S_Q, \boldsymbol{\varphi})$.

C_1 : This holds by assumption.

C_2 : By property C_2 of χ, the sets F_Q and $\boldsymbol{V}(\boldsymbol{h})_{|\boldsymbol{\varphi}_e \in Q}$ coincide in $\mathcal{O}(m) - S$. But since $S \subset S_Q$ in $\boldsymbol{\varphi}_e^{-1}(Q)$ then these sets coincide in $\mathcal{O}(m) - S_Q$ as well.

C_3 : Since V is d-equidimensional, then by [SS17, Lemma A.12], $c = n - d$. Hence, since $e \leq \mathfrak{r} - 1 \leq d$, the inequality $e + c \leq n$ holds.

C_4 : Finally, let $\boldsymbol{y} \in \mathcal{O}(m) \cap F_Q - S_Q$. Since $\boldsymbol{y} \notin S_Q$ then $\boldsymbol{y} \notin W_{\boldsymbol{\varphi}}(e, V) \cap \boldsymbol{\varphi}_e^{-1}(Q)$, but since $\boldsymbol{y} \in \boldsymbol{\varphi}_e^{-1}(Q)$ then actually $\boldsymbol{y} \notin W_{\boldsymbol{\varphi}}(e, V)$. Hence since $\boldsymbol{y} \in \mathcal{O}(m)$, then by Lemma 7.2.6, $\mathrm{Jac}_{\boldsymbol{y}}(\boldsymbol{h}, \boldsymbol{\varphi}_e)$ has full rank $c + e$.

All the properties of charts being satisfied, we are done. □

We now proceed to prove Proposition 7.2.16. The first statement is given by Lemma 7.7.1. If $e = d$, then the second statement is satisfied by the last item Proposition 7.2.3, since $K_{\boldsymbol{\varphi}}(d+1, V) = V$. Assume now that $e < d$. By Krull's principal ideal Theorem [Eis95, Theorem B.] or equivalently the theorem on the dimension of fibers [Sha13, Theorem 1.25], all irreducible components of F_Q have dimension at least $d - e > 0$.

We now prove the last statement that is that $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$ is an atlas of $(F_Q, Q, S_Q, \boldsymbol{\varphi})$:

A_1 : Since F_Q has positive dimension and S_Q is finite, then $F_Q - S_Q$ is not empty. Since $F_Q \subset V$, then by property A_3 of $\boldsymbol{\chi}$, there exists $1 \leq j \leq s$ such that $\mathcal{O}(m_j) \cap F_Q - S_Q$ is not empty.

A_2 : Let $1 \leq j \leq s$ such that $\mathcal{O}(m_j) \cap F_Q - S_Q$ is not empty, then by Lemma 7.7.1, χ_j is a chart of $(F_Q, Q, S_Q, \boldsymbol{\varphi})$. Since the elements of $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$ are exactly such χ_j, we are done.

A_3 : Finally let $\boldsymbol{y} \in F_Q - S_Q$, since $\boldsymbol{y} \in \boldsymbol{\varphi}_e^{-1}(Q)$ then $\boldsymbol{y} \notin S$. Since $F_Q \subset V$, then by property A_3 of $\boldsymbol{\chi}$, there exists $1 \leq j \leq s$ such that $\boldsymbol{y} \in \mathcal{O}(m_j)$. In particular, $\mathcal{O}(m_j) \cap F_Q - S_Q$ is non-empty, so that $\chi_j \in F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$.

Hence, $F_{\mathrm{atlas}}(\boldsymbol{\chi}, V, Q, S, \boldsymbol{\varphi})$ is an atlas of $(F_Q, Q, S_Q, \boldsymbol{\varphi})$. In particular, since V is d-equidimensional, all the $\boldsymbol{h}_j$'s have same cardinality $c = n - d$ by [SS17, Lemma A.12]. Hence by [SS17, Lemma A.11], $F_Q - S_Q$ is a non-singular $(d - e)$-equidimensional locally closed set. Since F_Q has positive dimension and S_Q is finite, we deduce that F_Q is the Zariski closure of $F_Q - S_Q$ and then, is a $(d - e)$-equidimensional algebraic set, smooth outside S_Q. This concludes the proof of Proposition 7.2.16.

8 Answering connectivity queries on real algebraic curves

Abstract. As seen in the previous chapters, deciding connectivity queries in real algebraic sets of arbitrary dimension can be reduced to deciding such ones in the one-dimensional case i.e. on real algebraic curves, in the original space, using roadmaps. This leaves open the problem of efficiently solving the one-dimensional case.

In this chapter, we consider the problem of answering connectivity queries on a real algebraic curve. The curve is given as the real trace of an algebraic curve, assumed to be in generic position, and being encoded by a one-dimensional parametrization. The query points are given by a zero-dimensional parametrization.

We design an algorithm which counts the number of connected components of the real curve under study, and decides which query point lies in which connected component, in time quasi-linear in N^6, where N is the maximum of the degrees and coefficient bit-sizes of the polynomials given as input. Additionally, the algorithm maintains a cubic complexity in input size. Notably, this performance aligns with the best-known bound for computing the topology of real plane curves, in contrast to the prior algorithm for space curves, which has a complexity of order N^{20}.

The main novelty of this algorithm is the avoidance of the computation of the comprehensive topology of the curve.

This is joint work with Md N. Islam and A. Poteaux.

8.1 Introduction

In the previous chapters, we discussed the reduction of connectivity queries on real algebraic sets of arbitrary dimension, to such ones on one-dimensional semi-algebraic sets, in the original space, using roadmaps. This emphasizes the importance of efficiently solving the one-dimensional case. However, there is a lack of algorithms in the literature that are both general and have favorable complexity bounds for this problem. Indeed, the polynomial complexity class, in terms of the input curve's degree, is too coarse as the natural input for these algorithms will be roadmaps with degrees exponential in the number of variables.

Open problem for Chapter 8

In this chapter, we address the problem of designing an efficient algorithm for answering connectivity queries on real algebraic curves in $\mathbb{R}^n$, defined as real traces of algebraic curves of $\mathbb{C}^n$. More precisely, given representations of an algebraic curve $\mathscr{C}$ and a finite set $\mathcal{P}$ of points of $\mathscr{C}$, we want to compute a partition of $\mathcal{P}$, grouping the points lying in the same connected components of $\mathscr{C} \cap \mathbb{R}^n$, and count the number of such components.

Prior works. The above problem has been previously tackled only through the computation of a piecewise linear approximation sharing the same topology as the one of the curve under study. We refer to Subsection 5.3.3 of Chapter 5 for a more comprehensive overview of the literature on these approaches.

Assume that $\mathscr{C}$ is given as polynomials of magnitude (δ, τ). In $\mathbb{R}^2$, approaches using subdivision algorithms and variants of Cylindrical Algebraic Decomposition methods have been successful. Notably, [KS15, DDR+22] achieved a complexity $\widetilde{O}(\delta^5(\delta+\tau))$ by computing quantitative bounds on real root isolation. In $\mathbb{R}^3$, research progress has been relatively scarce, with only a few papers providing complexity bounds. [JC21] obtained the best-known complexity $\widetilde{O}(\delta^{19}(\delta+\tau))$. For real algebraic curves in $\mathbb{R}^n$, this relies on a variation of the Cylindrical Algebraic Decomposition algorithm of Collins [Col75] – see Section 5.1 of Chapter 5. This approach, described in [SS11], exhibits polynomial complexity in δ – see Theorem 5.3.4.

These approaches have limitations. Either they assume the ambient space to be of small dimension or they do not explicitly provide the constant factor in the exponent. This is due to the fact that they compute the comprehensive topology of the input curve, requiring the output to share the same topology as the one of the input.

Yet, to answer connectivity queries, it suffices for the output to share the same connectivity properties.

Main result. Consider a real field $\mathbf{Q}$, its real closure $\mathbf{R}$ and its algebraic closure $\mathbf{C}$. Let also $\boldsymbol{X} = (x_1, \ldots, x_n)$ be a sequence of indeterminates, where $n \geq 1$. In this chapter, $\mathscr{C}$ is an algebraic curve defined by polynomials with coefficients in $\mathbf{Q}$. For $1 \leq i \leq n$ we let $\pi_i : \mathbf{C}^n \to \mathbf{C}^i$ be the canonical projection on the first i variables. We note $\mathscr{C}_2 \subset \mathbf{C}^2$ and $\mathscr{C}_3 \subset \mathbf{C}^3$ the Zariski closures of respectively $\pi_2(\mathscr{C})$ and $\pi_3(\mathscr{C})$. We note e.g. $\mathscr{C}_\mathbf{R}$ and $\mathscr{C}_{2,\mathbf{R}}$, respectively the real traces of $\mathscr{C}$ and $\mathscr{C}_2$. Then, e.g. $\mathcal{K}(\pi_1, \mathscr{C}) \cap \mathbf{R}^n$ and $\mathcal{K}(\pi_1, \mathscr{C}_2) \cap \mathbf{R}^2$ will be denoted by $\mathcal{K}(\pi_1, \mathscr{C}_\mathbf{R})$ and $\mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbf{R}})$.

Under genericity assumptions, we reduce the study of a curve $\mathscr{C}_\mathbf{R}$ to the one of its image $\mathscr{C}_{3,\mathbf{R}}$ by the projection π_3, as their real traces generically share the same connectivity properties. Moreover, by refining the approach developed in [IP11] (based on [El 08]), we show that *one does not need to compute the topology of $\mathscr{C}_{3,\mathbf{R}}$ in order to answer connectivity queries*. More precisely, under genericity assumptions, that we make explicit below, we first compute the topology of $\mathscr{C}_{2,\mathbf{R}}$ i.e. an isotopic graph. Next, the connectivity of $\mathscr{C}_{3,\mathbf{R}}$ i.e. a homeomorphic graph, is deduced from the topology of $\mathscr{C}_{2,\mathbf{R}}$, adapting results from [El 08]. A geometric outcome is that the topological analysis needed to be done at some special points of $\mathscr{C}_{2,\mathbf{R}}$, which are called *apparent singularities*, can be much simplified when one only needs to answer connectivity queries. This has a significant impact on the complexity.

The set of *apparent singularities* of $\mathscr{C}_2$ is defined as $\mathrm{app}(\mathscr{C}_2) = \mathrm{sing}(\mathscr{C}_2) - \pi_2(\mathrm{sing}(\mathscr{C}))$. These are the singularities introduced by π_2. A singular point of $\mathscr{C}_2$ is called a node if it is an ordinary double point (see [El 08, §3.1]).

We now give a precise formulation of our genericity properties mentioned above, which can be seen as a generalization of the ones in [El 08]. For $\boldsymbol{x}$ in $\mathrm{reg}(\mathscr{C})$ – resp. $\mathrm{reg}(\mathscr{C}_2)$ – , we denote by $\mathrm{T}_{\boldsymbol{x}}\mathscr{C}$ – resp. $\mathrm{T}_{\boldsymbol{x}}\mathscr{C}_2$ – the tangent space to $\mathscr{C}$ – resp. $\mathscr{C}_2$ – at $\boldsymbol{x}$. These are here lines of $\mathbb{C}^n$ – resp. $\mathbb{C}^2$.

Let $\mathscr{C} \subset \mathbf{C}^n$ be an algebraic curve and $\mathcal{P} \subset \mathrm{reg}(\mathscr{C})$ be finite. The pair $(\mathscr{C}, \mathcal{P})$ satisfies (H) if:

(H_1) for $1 \leq i \leq n$, $\mathbf{Q}[\mathscr{C}]$ is integral over $\mathbf{Q}[\mathscr{C}_i]$, where $\mathscr{C}_i = \pi_i(\mathscr{C})$ is an algebraic curve;

(H_2) for all $\boldsymbol{x} \in \mathrm{reg}(\mathscr{C})$, $\pi_2(\mathrm{T}_{\boldsymbol{x}}\mathscr{C})$ is a tangent line to $\mathscr{C}_2$ at $\pi_2(\boldsymbol{x})$;

(H_3) the restriction of π_3 to $\mathscr{C}$ is injective;

(H_4) if $\boldsymbol{y} \in \mathrm{app}(\mathscr{C}_2)$ then

- (H_4') $\pi_2^{-1}(\boldsymbol{y}) \cap \mathscr{C}$ has cardinality 2;
- (H_4'') $\boldsymbol{y}$ is a node of $\mathscr{C}_2$;

(H_5) $\mathcal{K}(\pi_1, \mathscr{C}_2) \cup \pi_2(\mathcal{P})$ is finite and π_1 is injective on it;

(H_6) $\pi_2^{-1}(\pi_2(\boldsymbol{x})) \cap \mathscr{C} = \{\boldsymbol{x}\}$, for all $\boldsymbol{x} \in \mathcal{K}(\pi_1, \mathscr{C}) \cup \mathcal{P}$;

(H_7) there is a one-dimensional parametrization $\mathscr{R} = (\Omega, (x_1, x_2))$ encoding $\mathscr{C}$, with $\Omega = (\omega, x_1, x_2, \rho_3, \ldots, \rho_n) \subset \mathbf{Q}[x_1, x_2]$.

We omit $\mathcal{P}$ when the context is clear.

Contributions to the open problem

In Section 8.2, we prove that assumption (H) holds for an algebraic curve in *generic position* $\mathscr{C}$ that is, there is a Zariski open dense subset $\mathfrak{A}$ of $\mathrm{GL}_n(\mathbf{C})$ such that for any $A \in \mathfrak{A}$ the sheared curve $\mathscr{C}^A$ satisfies (H).

Theorem 8.1.1. *Let $\mathscr{R} \subset \mathbb{Z}[x_1, x_2]$ be a one-dimensional parametrization encoding an algebraic curve $\mathscr{C} \subset \mathbb{C}^n$ satisfying (H) and $\mathscr{P} \subset \mathbb{Z}[x_1]$ a zero-dimensional parametrization encoding a finite subset of $\mathscr{C}$. Let (δ, τ) and (μ, κ) be the magnitudes of $\mathscr{R}$ and $\mathscr{P}$, respectively.*
There exists an algorithm which, on input $\mathscr{R}$ and $\mathscr{P}$, computes a partition of the points of $\mathsf{Z}(\mathscr{P}) \cap \mathbb{R}^n$ lying in the same semi-algebraically connected component of $\mathscr{C} \cap \mathbb{R}^n$, using

$$\widetilde{O}(\delta^6 + \mu^6 + \delta^5\tau + \mu^5\kappa)$$

bit operations. In particular, it is cubic in the size of the input.

This is to be compared with the best complexity $\widetilde{O}(\delta^{19}(\delta + \tau))$ known to analyze the topology of curves in $\mathbb{R}^3$. Note that the dependency on n in the complexity bound is "hidden" within the potential degrees of the parametrizations and the corresponding algebraic sets. Indeed, according to Bézout's bound, an algebraic set, defined by polynomials, of degree at most D, can have degree at most D^n. We refer to Subsection 1.3.3 of Chapter 1 for an overview of the key ingredients of the algorithm presented in the following.

Outline of the chapter. In Section 8.2, we establish genericity conditions using secant varieties and Grassmanians to ensure the validity of assumption (H) after a generic linear coordinate change. Under these conditions, we present two key theoretical results that form the foundation of our algorithm.
The first result, in Section 8.3, identifies the finitely many apparent singularities in the projected curve $\mathscr{C}_2$, where local connectivity differs from that of $\mathscr{C}$. This involves Puiseux series expansion at the nodes of $\mathscr{C}_2$ to establish a straightforward criterion.
The second step, detailed in Section 8.4, analyzes local connectivity in the fiber of these apparent singularities to deduce the complete connectivity of $\mathscr{C}$ from $\mathscr{C}_2$'s topology. This process leverages tools from real algebraic geometry, such as infinitesimals, and exploits the local conic structure of semi-algebraic sets.
Finally, in Section 9.2, we describe the complexity of each algorithmic step and conclude with a formal proof of Theorem 8.1.1. Our analysis heavily relies on computations involving gcd and resultants, as well as complexity bounds for real root isolation of triangular bivariate polynomial systems.

8.2 Curves in generic position

We now prove that (H) holds for an algebraic curve in generic position $\mathscr{C}$ that is, there is an open dense subset $\mathfrak{A}$ of $\mathrm{GL}_n(\mathbf{C})$ such that for any $A \in \mathfrak{A}$ the sheared curve $\mathscr{C}^A$ satisfies (H). We refer to Subsection 2.4 of Chapter 2 for a detailed discussion on the notion of genericity. Note that in this section, $\mathbf{Q}$ can be any field of characteristic 0.

8.2.1 Generic projections of affine curves

The results below are well known in the case of smooth projective curves (see e.g. [Har77, IV. Thm 3.10] or [Mum95, §7B.] for $\mathbf{C} = \mathbb{C}$), and have been generalized subsequently in e.g. [HR79, KKBT08]. A version for complex singular affine space curves is proved in [FGT09, Prop 5.2] under regularity assumptions. We present here a generalization of [FGT09, Prop 5.2] for any singular (affine) algebraic curve, following the proof and using more general objects and results from the literature.

Let $n \geq 3$, $\mathscr{C} \subset \mathbf{C}^n$ an affine algebraic curve and $\mathcal{P} \subset \mathscr{C}$ a finite subset. Recall that we denote by $\mathbb{P}^n$ the projective space $\mathbb{P}^n(\mathbf{C})$, of dimension n over $\mathbf{C}$, and that its elements write as $[\boldsymbol{x}_0 \colon \cdots \colon \boldsymbol{x}_n]$. Let $\mathcal{H}^\infty = \{[\boldsymbol{x}_0 \colon \cdots \colon \boldsymbol{x}_n] \in \mathbb{P}^n \mid \boldsymbol{x}_0 = 0\}$ be the hyperplane at infinity with respect to the affine open chart given by $\mathbb{P}^n - \mathcal{H}^\infty$ (see e.g. [Har77, I.2]) We finally let $\overline{\mathscr{C}}$ be the projective closure of $\mathscr{C}$ in $\mathbb{P}^n$. These objects are introduced and discussed in Subsection 2.2, and we refer the reader for the following of this section.

We denote by $\mathbb{G}(1, n) = G(2, n+1)$ the Grassmanian of lines in $\mathbb{P}^n$, and, for $\boldsymbol{x} \neq \boldsymbol{y}$ in $\mathbb{P}^n$, by $\mathcal{L}(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{G}(1, n)$ the line containing $\boldsymbol{x}$ and $\boldsymbol{y}$. We first introduce some special line for $\overline{\mathscr{C}}$. Let $\boldsymbol{x}, \boldsymbol{y}$ be *distinct* points of $\overline{\mathscr{C}}$ and $s = \mathcal{L}(\boldsymbol{x}, \boldsymbol{y})$ then,

- the line s will be called the *secant line of* $\overline{\mathscr{C}}$ *determined by* $\boldsymbol{x}$ *and* $\boldsymbol{y}$;

- if s intersects $\overline{\mathscr{C}}$ in a third point, distinct from $\boldsymbol{x}, \boldsymbol{y}$, then s is called a *trisecant line of* $\overline{\mathscr{C}}$;
- if there are distinct $\boldsymbol{x}', \boldsymbol{y}' \in s \cap \operatorname{reg}(\overline{\mathscr{C}})$ such that $\mathrm{T}_{\boldsymbol{x}'}\overline{\mathscr{C}}$ and $\mathrm{T}_{\boldsymbol{y}'}\overline{\mathscr{C}}$ are coplanar, then it will be called a *secant line with coplanar tangents of* $\overline{\mathscr{C}}$.

Then, we define $\mathsf{Sec}(\overline{\mathscr{C}}), \mathsf{Tri}(\overline{\mathscr{C}})$ and $\mathsf{CoPl}(\overline{\mathscr{C}})$ as the sets of points in $\mathbb{P}^n$ that lie on respectively a secant, trisecant and secant with coplanar tangents of $\overline{\mathscr{C}}$. Finally, we denote by $\mathsf{Tg}(\overline{\mathscr{C}})$ the set of points in $\mathbb{P}^n$ that lie on the tangent line $\mathrm{T}_{\boldsymbol{x}}\overline{\mathscr{C}}$ for some $\boldsymbol{x} \in \operatorname{reg}(\overline{\mathscr{C}})$.

Lemma 8.2.1. *The sets* $\mathsf{Sec}(\overline{\mathscr{C}})$ *and* $\mathsf{Tg}(\overline{\mathscr{C}})$ *are algebraic sets of dimension* ≤ 3 *and* ≤ 2*, respectively. If, in addition,* $\overline{\mathscr{C}}$ *is not a plane curve, then* $\mathsf{Tri}(\overline{\mathscr{C}})$ *and* $\mathsf{CoPl}(\overline{\mathscr{C}})$ *are algebraic sets of dimension* ≤ 2*. Finally, none of these sets contains* $\mathcal{H}^\infty$.

Proof. Let $\overline{\mathscr{C}}_1, \ldots, \overline{\mathscr{C}}_m$ the irreducible components of $\overline{\mathscr{C}}$, $i, j \in \{1, \ldots, m\}$, possibly equal, and $\Sigma_{i,j} \subset \mathbb{G}(1, n)$ the Zariski closure of the image of

$$\overline{\mathscr{C}}_i \times \overline{\mathscr{C}}_j - \{(\boldsymbol{y}, \boldsymbol{y}) \mid \boldsymbol{y} \in \overline{\mathscr{C}}_i \cap \overline{\mathscr{C}}_j\}$$

through the map $(\boldsymbol{y}, \boldsymbol{z}) \mapsto \mathcal{L}(\boldsymbol{y}, \boldsymbol{z})$. As the image of a Cartesian product of two irreducible curves, $\Sigma_{i,j}$ is an irreducible algebraic set. Such a secant being uniquely determined by fixing two points in $\overline{\mathscr{C}}_i$ and $\overline{\mathscr{C}}_j$, $\Sigma_{i,j}$ has dimension ≤ 2 by [Sha13, Thm 1.25]. Then, if $\Sigma = \bigcup_{i,j} \Sigma_{i,j}$ is the secant variety of $\overline{\mathscr{C}}$, it has dimension ≤ 2 and contains the secant lines in $\mathbb{G}(1, n)$. As elements of $\mathbb{G}(1, n)$ are algebraic sets of dimension 1, $\mathsf{Sec}(\overline{\mathscr{C}})$ has Zariski closure of dimension ≤ 3.

Consider now, the set

$$\Gamma_i = \left\{ (\boldsymbol{u}, \boldsymbol{y}) \in \mathbb{P}^n \times \overline{\mathscr{C}}_i \text{ s.t. } \boldsymbol{y} \in \operatorname{reg}(\overline{\mathscr{C}}) \quad \text{and} \quad \boldsymbol{u} \in \mathrm{T}_{\boldsymbol{y}}\overline{\mathscr{C}} \right\}$$

and consider the projections $\varphi_i \colon \Gamma_i \to \mathbb{P}^n$ and $\psi_i \colon \Gamma_i \to \overline{\mathscr{C}}_i$. For all $\boldsymbol{y}$ in the Zariski open subset $\operatorname{reg}(\overline{\mathscr{C}}) \cap \overline{\mathscr{C}}_i$ of $\mathscr{C}_i$, $\psi_i^{-1}(\boldsymbol{y})$ is exactly $\mathrm{T}_{\boldsymbol{y}}\overline{\mathscr{C}}$, which has dimension 1. Hence, by [Sha13, Thm 1.25], $\varphi_i(\Gamma_i)$ has Zariski closure of dimension ≤ 2. Since $\mathsf{Tg}(\overline{\mathscr{C}}) = \cup_i \varphi_i(\Gamma_i)$, we are done.

Assume now, that $\overline{\mathscr{C}}$ is not a plane curve then, by [KKBT08, Thm 2], the set of trisecant lines of $\overline{\mathscr{C}}$ is a subset of $\mathbb{G}(1, n)$ whose Zariski closure has dimension ≤ 1. Then, as seen above, $\mathsf{Tri}(\overline{\mathscr{C}})$ has Zariski closure of dimension ≤ 2.

Now, let $M_{i,j}$ be the subset of $\Sigma_{i,j}$ consisting of secant lines intersecting $\overline{\mathscr{C}}$ at points whose tangents are all contained in the same plane. We are going to prove that the Zariski closure of $M_{i,j}$ has dimension ≤ 1. Together with the dimension bound on $\mathsf{Tri}(\overline{\mathscr{C}})$, this will bound the dimension of $\mathsf{CoPl}(\overline{\mathscr{C}})$.

Suppose first that $\overline{\mathscr{C}}_i$ and $\overline{\mathscr{C}}_j$ are not coplanar components. Then, there is $\boldsymbol{y} \in \overline{\mathscr{C}}_i - \operatorname{sing}(\overline{\mathscr{C}})$ such that $l = \mathrm{T}_{\boldsymbol{y}}\overline{\mathscr{C}}$ and $\overline{\mathscr{C}}_j$ are not coplanar. If $\mathfrak{p}_l \colon \mathbb{P}^n \to \mathbb{P}^{n-2}$ denotes the projection of center l, then $\mathfrak{p}_l(\overline{\mathscr{C}}_j)$ is not a point. As $\overline{\mathscr{C}}_j$ is irreducible, and by [Sha13, Thm 1.25], the Zariski closure $\mathcal{R}$ of $\mathfrak{p}_l(\overline{\mathscr{C}}_j)$ is an irreducible algebraic subset of $\mathbb{P}^{n-2}$ of dimension 1. Hence, by [Sha13, Thm 1.25] again, there is a finite set $K_1 \subset \mathbb{P}^{n-2}$ such that for all $\boldsymbol{w} \in \mathcal{R} \backslash K_1$,

$$\mathfrak{p}_l^{-1}(\boldsymbol{w}) \cap \overline{\mathscr{C}}_j$$

is finite. Besides, by Sard's Theorem [Sha13, Thm 2.27], there exists a finite set $K_2 \subset \mathbb{P}^{n-2}$ such that $\mathcal{R}\backslash K_2$ does not contain any critical value of the restriction of $\mathfrak{p}_l$ to $\overline{\mathscr{C}}_j$. Then, for $\boldsymbol{w}$ in $\mathcal{R}\backslash[K_1 \cup K_2 \cup \mathfrak{p}_l(\mathrm{sing}(\overline{\mathscr{C}}))]$,

$$\mathfrak{p}_l^{-1}(\boldsymbol{w}) \cap \overline{\mathscr{C}}_j = \{\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k\}$$

with $k \geq 1$, and for all $1 \leq i \leq k$, $\boldsymbol{z}_i \in \mathrm{reg}(\overline{\mathscr{C}})$ and $\mathfrak{p}_l(\mathrm{T}_{\boldsymbol{z}_i}\,\overline{\mathscr{C}})$ has dimension 1. Hence, $\boldsymbol{y}$ and $\boldsymbol{z}_i$ have no coplanar tangents for all $1 \leq i \leq k$. In particular, the secant line $\mathcal{L}(\boldsymbol{y}, \boldsymbol{z}_1)$ contains two points having no coplanar tangents so that

$$\mathcal{L}(\boldsymbol{y}, \boldsymbol{z}_1) \in \Sigma_{i,j} - M_{i,j},$$

and then $M_{i,j} \subsetneq \Sigma_{i,j}$. In conclusion, the Zariski closure of $M_{i,j}$ is a proper algebraic subset, and since $\Sigma_{i,j}$ is irreducible, this closure has dimension ≤ 1.

If now $\overline{\mathscr{C}}_i$ and $\overline{\mathscr{C}}_j$ are coplanar, $\Sigma_{i,j}$ is the Zariski closure of $M_{i,j}$ and one of the following holds. If $i = j$ and $\overline{\mathscr{C}}_i$ is a line, then $\Sigma_{i,j}$ is reduced to the line associated to $\overline{\mathscr{C}}_i$ and has dimension 0. Else, there exists a unique plane $S_{i,j}$ containing $\overline{\mathscr{C}}_i$ and $\overline{\mathscr{C}}_j$, so that any line of $\Sigma_{i,j}$ must be contained in $S_{i,j}$. In both cases, $\Sigma_{i,j}$, thus the closure of $M_{i,j}$, have dimension ≤ 1. Then, the Zariski closure of the union M of all $M_{i,j}$ for $i, j \in \{1, \ldots, m\}$, is an algebraic subset of $\mathbb{G}(1, n)$ of dimension ≤ 1 as requested.

Remark now that a secant with coplanar tangents is either a trisecant, or a secant intersecting $\overline{\mathscr{C}}$ in exactly two regular points with coplanar tangents. Hence, the set of secants with coplanar tangents of $\overline{\mathscr{C}}$ is contained in the union of M and the set of trisecant lines of $\overline{\mathscr{C}}$. By the previous discussion, it has dimension ≤ 1, so that the Zariski closure of $\mathsf{CoPl}(\overline{\mathscr{C}})$ has dimension ≤ 2.

Since $\overline{\mathscr{C}} - \mathcal{H}^\infty$ can be identified with $\mathscr{C}$, the former is a Zariski open subset of $\overline{\mathscr{C}}$, so that $\overline{\mathscr{C}} \cap \mathcal{H}^\infty$ is finite. In particular, $\mathcal{H}^\infty$ contains finitely many secant or tangent lines of $\overline{\mathscr{C}}$ and then, cannot be contained in $\mathsf{Sec}(\overline{\mathscr{C}})$ or $\mathsf{Tg}(\overline{\mathscr{C}})$. Since $\mathsf{Tri}(\overline{\mathscr{C}})$ and $\mathsf{CoPl}(\overline{\mathscr{C}})$ are contained in $\mathsf{Sec}(\overline{\mathscr{C}})$, they cannot contain $\mathcal{H}^\infty$ as well. □

In the following, for $0 \leq r \leq n-1$, we denote by $\mathbb{G}(r, n-1) = G(r+1, n)$ the set of r-dimensional projective linear subspaces of $\mathcal{H}^\infty$. Recall that using Plücker embedding (see e.g. [Sha13, Example 1.24]), $\mathbb{G}(r, n-1)$ can be embedded in $\mathbb{P}^{\binom{n}{r+1}-1}$ as an irreducible algebraic set of dimension $(r+1)(n-r)$. The next lemma is then a direct consequence of [Sha13, Thm 1.25].

Lemma 8.2.2. *Let $X \subset \mathcal{H}^\infty$ be an algebraic set of dimension $m \leq n-1$. Then, for any $i \geq m$ there exists a non-empty Zariski open subset $\mathfrak{E}_i$ of $\mathbb{G}(n-1-i, n-1)$ such that for every $E \in \mathfrak{E}_i$, the set $E \cap X$ is finite and, if $i > m$, it is empty.*

Recall that $\mathcal{P}$ is a finite set of control points in $\overline{\mathscr{C}} - \mathrm{sing}(\overline{\mathscr{C}})$.

Proposition 8.2.3. *If $\overline{\mathscr{C}}$ is not a plane curve, then for all $1 \leq i \leq n-1$, there exists a non-empty Zariski open subset $\mathfrak{E}_i$ of $\mathbb{G}(n-1-i, n-1)$ such that for all $E \in \mathfrak{E}_i$, the following holds. Let $\mathfrak{p}_E : \overline{\mathscr{C}} \to \mathbb{P}^i$ be the projection with center E, then $\mathfrak{p}_E$ is a finite regular map and*

(*i*) *for all* $\boldsymbol{x} \in \mathcal{P}$, $\mathfrak{p}_E(\mathrm{T}_{\boldsymbol{x}}\,\overline{\mathscr{C}})$ *is a projective line of* $\mathbb{P}^i$.

If, in addition, $i \geq 2$ *then,*

(*ii*) *item* (*i*) *holds for any* $\boldsymbol{x} \in \operatorname{reg}\overline{\mathscr{C}}$*;*

(*iii*) *for any* $\boldsymbol{x} \in \overline{\mathscr{C}}$*, there exists at most one point* $\boldsymbol{x}' \in \overline{\mathscr{C}}$*, distinct from* $\boldsymbol{x}$*, such that* $\mathfrak{p}_E(\boldsymbol{x}) = \mathfrak{p}_E(\boldsymbol{x}')$*;*

(*iv*) *there exists finitely many such pairs* $(\boldsymbol{x}, \boldsymbol{x}')$*, all satisfying* $\boldsymbol{x}, \boldsymbol{x}' \in \operatorname{reg}(\overline{\mathscr{C}}) - \mathcal{P}$ *and* $\mathfrak{p}_E(\mathrm{T}_{\boldsymbol{x}}\,\overline{\mathscr{C}}) \neq \mathfrak{p}_E(\mathrm{T}_{\boldsymbol{x}'}\,\overline{\mathscr{C}})$*;*

(*v*) *if* $i \geq 3$*, there is no such pair.*

Proof. Fix $1 \leq i \leq n-1$ and suppose that $\overline{\mathscr{C}}$ is not plane. As a proper Zariski closed set of $\overline{\mathscr{C}}$,

$$X_1 := \mathcal{H}^\infty \cap \overline{\mathscr{C}}$$

is finite. By Lemma 8.2.2, as $i > 0$, there is a non-empty Zariski open subset $\mathfrak{E}_1$ of $\mathbb{G}(n-1-i, n-1)$ such that for all $E \in \mathfrak{E}_1$, $E \cap X_1$ is empty. Moreover, any $(n-i)$-dimensional space containing E cannot contain an irreducible component of $\overline{\mathscr{C}}$ (it would be a line, intersecting E at some point of $E \cap \overline{\mathscr{C}} = E \cap X_1$, which is empty). Thus, the projection with center $E \in \mathfrak{E}_1$ induces a finite map on $\overline{\mathscr{C}}$, regular by definition.

According to Lemma 8.2.1, the set of points lying on a tangent or a trisecant line of $\overline{\mathscr{C}}$ is an algebraic set of dimension ≤ 2. Since $\mathcal{H}^\infty$ contains finitely many such tangents or trisecants,

$$X_2 = (\mathsf{Tg}(\overline{\mathscr{C}}) \cup \mathsf{Tri}(\overline{\mathscr{C}})) \cap \mathcal{H}^\infty$$

has dimension at most 1. By Lemma 8.2.2, as $i \geq 1$, there exists a non-empty Zariski open subset $\mathfrak{E}_2$ of $\mathbb{G}(n-1-i, n-1)$ such that any $E \in \mathfrak{E}_2$ intersects finitely many points of $\mathsf{Tg}(\overline{\mathscr{C}}) \cup \mathsf{Tri}(\overline{\mathscr{C}})$. Besides, there are finitely many tangents intersecting the finite set $\mathcal{P}$, so that by Lemma 8.2.2, up to intersecting $\mathfrak{E}_2$ with a non-empty Zariski open subset of $\mathbb{G}(n-1-i, n-1)$, one can assume that none of these tangents intersect $\mathcal{P}$. This proves (*i*).

Assume now $i \geq 2$. By Lemma 8.2.2, no $E \in \mathfrak{E}_2$ intersects points in $\mathsf{Tg}(\overline{\mathscr{C}}) \cup \mathsf{Tri}(\overline{\mathscr{C}})$. In particular, any $(n-i)$-dimensional space containing E cannot contain a tangent nor a trisecant, and, as seen above, this means that no tangent, or three distinct points, are mapped to one point. This proves respectively (*ii*) and (*iii*).

According to Lemma 8.2.1, the set

$$X_3 = \mathsf{Sec}(\overline{\mathscr{C}}) \cap \mathcal{H}^\infty$$

of points in $\mathcal{H}^\infty$, lying on a secant line of $\overline{\mathscr{C}}$, is algebraic of dimension ≤ 2. By Lemma 8.2.2 ($i \geq 2$), there is a non-empty Zariski open subset $\mathfrak{E}_3$ of $\mathbb{G}(n-1-i, n-1)$ such that any $E \in \mathfrak{E}_3$ contains finitely many points lying on a secant line of $\overline{\mathscr{C}}$ i.e., as before, there are finitely many pairs of points which are mapped to the same point in $\mathbb{P}^i$.

Besides, the set of secants intersecting $\mathrm{sing}(\overline{\mathscr{C}}) \cup \mathcal{P}$ is a proper algebraic subset of the secant variety of $\overline{\mathscr{C}}$. Hence, by Lemma 8.2.2, up to intersecting $\mathfrak{E}_3$ with a non-empty Zariski open subset of $\mathbb{G}(n-1-i, n-1)$, one can assume that none of these secants intersect $\mathrm{sing}(\overline{\mathscr{C}}) \cup \mathcal{P}$.

Finally, by Lemma 8.2.2, as $\mathsf{CoPl}(\overline{\mathscr{C}}) \cap \mathcal{H}^\infty$ has dimension ≤ 1. As seen above, up to intersecting $\mathfrak{E}_3$ with a non-empty Zariski open subset of $\mathbb{G}(n-1-i, n-1)$, one can assume that these secants intersect $\overline{\mathscr{C}}$ at points with no coplanar tangents, which cannot be mapped to the same line. All in all, for any $E \in \mathfrak{E}_3$, (iv) holds.

According to Lemma 8.2.2, if moreover $i \geq 3$, no $E \in \mathfrak{E}_3$ intersects points in $\mathsf{Sec}(\overline{\mathscr{C}})$ that is, no two distinct points are mapped to the same image. This proves (v). Taking $\mathfrak{E}_i = \mathfrak{E}_1 \cap \mathfrak{E}_2 \cap \mathfrak{E}_3$ finally ends the proof. □

We can now state the affine counterpart of Proposition 8.2.3.

Corollary 8.2.4. *There exists a non-empty Zariski open set $\mathfrak{A}$ of $\mathrm{GL}_n(\mathbf{C})$ such that for all $A \in \mathfrak{A}$ and $1 \leq i \leq n$, the following holds: the restriction of π_i to $\mathscr{C}^A$ is a finite morphism, and*

(i) *for all $\boldsymbol{x} \in \mathcal{P}^A$, $\pi_i(\mathrm{T}_{\boldsymbol{x}}\,\mathscr{C}^A)$ is a line of $\mathbf{C}^i$.*

If, in addition, $i \geq 2$ then,

(ii) *item (i) holds for any $\boldsymbol{x} \in \mathrm{reg}(\mathscr{C}^A)$;*

(iii) *the restriction of π_i to $\mathscr{C}^A$ is not injective at $\boldsymbol{x}$ if and only if $i = 2$ and $\pi_2(\boldsymbol{x}) \in \mathrm{app}(\mathscr{C}_2^A)$;*

(iv) *$\mathrm{app}(\mathscr{C}_2^A)$ contains only nodes, with exactly two preimages through π_2, none of them being in $\mathcal{P}^A$;*

Proof. If $\mathscr{C}$ is a plane curve, it is straightforward. Suppose from now on $n \geq 3$ and $\mathscr{C}$ not plane.

If $i = n$, there is nothing to prove, so let $1 \leq i \leq n-1$. Let $\overline{\mathscr{C}}$ be the projective closure of $\mathscr{C}$, which is not a plane either and let $\mathfrak{E}_i$ be the non-empty Zariski open subset of $\mathbb{G}(n-1-i, n-1)$ given by Proposition 8.2.3.

According to Plücker embedding, there exists a surjective regular map from the set of i linearly independent vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i$ of $\mathbf{C}^n$ to the set of $(n-1-i)$-dimensional (projective) linear subspaces of $\mathcal{H}^\infty$, defined by

$$x_0 = 0 \quad \text{and} \quad \boldsymbol{a}_{j,1}x_1 + \cdots + \boldsymbol{a}_{j,n}x_n = 0 \ \text{ for } \ 1 \leq j \leq i.$$

Hence, there exists a non-empty Zariski open set $\mathfrak{A}_i$ of $\mathrm{GL}_n(\mathbf{C})$ of matrices A such that the first i rows of A^{-1} are mapped to some $E \in \mathfrak{E}_i$, through the above map. Moreover, for any $A \in \mathfrak{A}_i$ the following holds. Consider,

$$\widetilde{A} = \begin{bmatrix} 1 & \boldsymbol{O} \\ \boldsymbol{O} & A \end{bmatrix},$$

and for $1 \leq j \leq n$, let $\boldsymbol{a}_j = (\boldsymbol{a}_{j,1}, \ldots, \boldsymbol{a}_{j,n})$ be the rows of A. If $L_0 = x_0$ and for $1 \leq j \leq i$, $L_j = \boldsymbol{a}_{j,1}x_1 + \cdots + \boldsymbol{a}_{j,n}x_n$, then the equations $L_0, \ldots, L_i$ define a projective linear subspace E of $\mathcal{H}^\infty$, such that $E \in \mathfrak{E}_i$ and, by definition (see e.g. [Sha13, Example 1.27]),

$$\begin{array}{rccc} \mathfrak{p}_E : & \widetilde{\overline{\mathscr{C}^A}} & \to & \mathbb{P}^i \\ & \boldsymbol{x} & \mapsto & [\boldsymbol{x}_0 : \cdots : \boldsymbol{x}_i] \end{array}.$$

Therefore, the restriction of $\mathfrak{p}_E$ to the affine chart $\mathbb{P}^n - \mathcal{H}^\infty$ can be identified with the restriction of π_i to $\mathscr{C}^A$. According to Proposition 8.2.3, the restriction of π_i to $\mathscr{C}^A$ is a finite morphism satisfying item (i). Assume now that $i \geq 2$ then, assertion (ii) is a direct consequence of item (ii) of Proposition 8.2.3.

Besides, let $\boldsymbol{x} \in \mathscr{C}^A$ such that there is $\boldsymbol{x}' \in \mathscr{C}^A$ satisfying $\boldsymbol{x}' \neq \boldsymbol{x}$ and $\pi_i(\boldsymbol{x}) = \pi_i(\boldsymbol{x}')$. Then, by Proposition 8.2.3, (iii) to (v), $\boldsymbol{x}'$ is unique, both $\boldsymbol{x}, \boldsymbol{x}' \notin \operatorname{sing}(\mathscr{C}^A) \cup \mathcal{P}^A$, and necessarily $i = 2$. Moreover, $\mathrm{T}_{\boldsymbol{x}}\mathscr{C}^A$ and $\mathrm{T}_{\boldsymbol{x}'}\mathscr{C}^A$ map to distinct lines of $\mathbf{C}^2$, crossing at $\pi_2(\boldsymbol{x})$: it is a node.

Hence, $\boldsymbol{x} \in \operatorname{app}(\mathscr{C}_2^A)$ and $\pi_2(\boldsymbol{x})$ is a node, with exactly two preimages, none of them being in $\mathcal{P}^A$. Conversely from Proposition 8.2.3, (ii), all points of $\operatorname{app}(\mathscr{C}_2^A)$ have at least two preimages in $\mathscr{C}^A$. This proves (iii) and (iv). Taking $\mathfrak{A} = \bigcap_{i=1}^{n-1} \mathfrak{A}_i$ concludes. □

8.2.2 Recovering (H)

Proposition 8.2.5. *Let $\mathscr{C} \subset \mathbf{C}^n$ be an algebraic curve and a finite subset $\mathcal{P} \subset \operatorname{reg}(\mathscr{C})$. There exists a non-empty Zariski open set $\mathfrak{A} \subset \mathrm{GL}_n(\mathbf{C})$ such that, for any $A \in \mathfrak{A}$, $(\mathscr{C}^A, \mathcal{P}^A)$ satisfies* (H).

Proof. Let $\mathfrak{A}_1 \subset \mathrm{GL}_n(\mathbf{C})$ be the non-empty Zariski open subset defined in Corollary 8.2.4 and let $A \in \mathfrak{A}_1$. For all $1 \leq i \leq n$, the restriction of π_i to $\mathscr{C}^A$ is a finite morphism, so that $\mathscr{C}_i^A = \pi_i(\mathscr{C}^A)$ is an algebraic curve. Since $\mathbf{C}$ is integral over $\mathbf{Q}$, the extension $\mathbf{Q}[\mathscr{C}_i^A] \hookrightarrow \mathbf{Q}[\mathscr{C}^A]$ is integral as well: (H_1) is satisfied. Applying Corollary 8.2.4, for $i = 3$ and $i = 2$ shows that the curve $\mathscr{C}^A$ satisfies respectively (H_3) on the one hand and (H_2) and (H_4) on the other.

Let $\mathtt{A} = (\mathfrak{a}_{i,j})_{1 \leq i,j \leq n}$ and t be new indeterminates, the former ones standing for the entries of a square matrix of size $n \times n$. Since $\mathfrak{A}_1$ is non-empty and Zariski open, there exists a non-zero polynomial $F \in \mathbf{C}[\mathtt{A}]$, such that $A \in \mathfrak{A}_1$ if $F(A) \neq 0$. Besides, according to [BE02, §4.2] (or [GE96, §3.2]), there exists a non-zero polynomial $G \in \mathbf{C}[\mathtt{A}, t]$ such that, if $F(A) \neq 0$ and $G(A, b) \neq 0$ then, for

$$B = \begin{bmatrix} 1 & b & \boldsymbol{O} \\ 0 & 1 & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{O} & I_{n-2} \end{bmatrix},$$

the curve $\mathscr{C}_2^{BA}$ is a plane curve in generic position in the sense of [BE02, §4.2] and [El 08, Def 3.3]. In particular, π_1 maps no tangent line of any singular point of $\mathscr{C}_2$ to a point and its

restriction of π_1 to the finite set $W^\circ(\pi_1, \mathscr{C}_2^{BA})$ is injective. Let $\mathcal{P}_2 = \pi_2(\mathcal{P})$. As $\mathcal{P}_2 \cup \mathrm{sing}(\mathscr{C}_2)$ is finite, we can assume that π_1 is injective on $\mathcal{P}_2^{BA} \cup \mathrm{sing}(\mathscr{C}_2^{BA})$ as well. But, for any $\boldsymbol{x} \in W^\circ(\pi_1, \mathscr{C}_2^{BA})$, $\pi_1(\boldsymbol{x})$ is a point, so that $\boldsymbol{x}$ is neither in $\mathrm{sing}(\mathscr{C}_2^{BA})$ nor $\mathcal{P}_2^{BA}$, by genericity of $\mathscr{C}_2^{BA}$ and item (i) of Corollary 8.2.4 respectively. Then, let $b \in \mathbf{C}$ such that $G(\mathtt{A}, b)$ is not zero and let B be as above. The subset $\mathfrak{A}_2 \subset \mathrm{GL}_n(\mathbf{C})$ of elements of the form BA' where $F(A')G(A', b) \neq 0$ is a non-empty Zariski open subset. Moreover, for any $A \in \mathfrak{A}_2$, $\mathscr{C}^A$ satisfies (H_5).

Take $A \in \mathfrak{A}_1 \cap \mathfrak{A}_2$ and let $\boldsymbol{x} \in \mathcal{K}(\pi_1, \mathscr{C}^A) \cup \mathcal{P}^A$ and $\boldsymbol{y} = \pi_2(\boldsymbol{x})$. Suppose there is $\boldsymbol{x}' \in \mathscr{C}^A$ such that $\boldsymbol{x}' \neq \boldsymbol{x}$ and $\pi_2(\boldsymbol{x}') = \boldsymbol{y}$. By (iii), $\boldsymbol{x} \in W^\circ(\pi_1, \mathscr{C}^A)$ and $\boldsymbol{y}$ is a node in $\mathrm{app}(\mathscr{C}_2^A)$, with vertical tangent line $\pi_2(\mathrm{T}_{\boldsymbol{x}}\mathscr{C}^A)$: this is impossible by above ($A \in \mathfrak{A}_2$, so that $\mathscr{C}_2^A$ is in generic position). Therefore, $\mathscr{C}^A$ satisfies (H_6).

We proceed similarly for (H_7). Let $A \in \mathfrak{A}_1$. By (H_1), $\mathscr{C}^A$ is in Noether position (for π_1). Let $\mathtt{D} = (\mathfrak{d}_3, \ldots, \mathfrak{d}_n)$ be new variables. By [DL08, Cor 3.4 & 3.5], there is $H \in \mathbf{C}[\mathtt{A}, \mathtt{D}]$ non-zero such that, if $F(A) \neq 0$ and $H(A, \boldsymbol{d}) \neq 0$, then the following holds: if $\mu_{\boldsymbol{d}} = x_2 + \boldsymbol{d}_3 x_3 + \cdots + \boldsymbol{d}_n x_n$ is a linear form, then there is $\mathscr{R} = (\omega, \rho_1, \ldots, \rho_n) \subset \mathbf{Q}[x_1, v]$ such that $(\mathscr{R}, x_1, \mu_{\boldsymbol{d}})$ is a one-dimensional parametrization encoding $\mathscr{C}^A$. Let $\boldsymbol{d} \in \mathbf{C}^{n-1}$ such that $H(\mathtt{A}, \boldsymbol{d})$ is not zero and

$$C = \begin{bmatrix} 1 & \boldsymbol{O} & \boldsymbol{O} \\ 0 & 1 & \boldsymbol{d} \\ \boldsymbol{O} & \boldsymbol{O} & I_{n-2} \end{bmatrix}.$$

The subset $\mathfrak{A}_3 \subset \mathrm{GL}_n(\mathbf{C})$ of elements, of the form CA', where $F(A')$ and $H(A', \boldsymbol{c})$ are both not zero, is a non-empty Zariski open subset where $\mathscr{C}^A$ satisfies (H_7).

Finally, for $A \in \mathfrak{A} := \mathfrak{A}_1 \cap \mathfrak{A}_2 \cap \mathfrak{A}_3$, $\mathscr{C}^A$ satisfies (H). □

8.3 Detect apparent singularities

We generalize the criterion of [El 08] used to identify apparent singularities in plane projection of space curve. We keep notations given in Section 8.1, and **assume for the rest of the document that** $(\mathscr{C}, \mathcal{P})$ **satisfies** (H). We start by an adapted version of [El 08, Lemma 4.1] (the equivalence relation modulo $\boldsymbol{I}(\mathscr{C})$ is denoted $\equiv$). Note that in this section, $\mathbf{Q}$ can be any field of characteristic 0.

Lemma 8.3.1. *Let (α, β) be a node of $\mathscr{C}_2$. There are exactly two power-series $y_1, y_2 \in \mathbf{C}[[x_1 - \alpha]]$ such that for $i = 1, 2$, if $z_i = \frac{\rho_3(x_1, y_i)}{\partial_{x_2}\omega(x_1, y_i)}$ then:*

1. *$\omega(x_1, y_i) \equiv 0$ and $y_i(\alpha) = \beta$ but $y_1'(\alpha) \neq y_2'(\alpha)$;*
2. *$h(x_1, y_i, z_i) \equiv 0$ for any $h \in \boldsymbol{I}(\mathscr{C}) \cap \mathbf{Q}[x_1, x_2, x_3]$ and $z_i \in \mathbf{C}[[x_1 - \alpha]]$.*

Proof. According to (H_5) and (H_7), $\mathscr{C}_2$ is in generic position in the sense of [GE96, Def 3.1]. As (α, β) is a node of $\mathscr{C}_2 = \boldsymbol{V}(\omega)$, then β is a double root of $\omega(\alpha, x_2)$ by [GE96, Prop 2.1 & Thm 3.1]. From the Puiseux theorem (see e.g. [Eis95, Cor 13.16]), there are exactly two

Puiseux series y_1, y_2 of $\mathscr{C}_2$ at (α, β). And for $i = 1, 2$, from [El 08, §3.2], $y_i \in \mathbf{C}[[x_1 - \alpha]]$, hence, $\omega(x_1, y_i) \equiv 0$ and $y_i(\alpha) = \beta$. Besides, as (α, β) is a node, we have $y_1'(\alpha) \neq y_2'(\alpha)$. This concludes the proof of assertion (1).

Let $h \in \boldsymbol{I}(\mathscr{C}) \cap \mathbf{Q}[x_1, x_2, x_3]$. By Euclidean division, there are $u, r \in \mathbf{Q}[x_1, x_2]$ and $m \geq 0$ such that

$$(\partial_{x_2}\omega)^m \cdot h = u(\partial_{x_2}\omega \cdot x_3 - \rho_3) + r.$$

Since $\boldsymbol{I}(\mathscr{C}) \cap \mathbf{Q}[x_1, x_2] = \int\omega$, ω divides r in $\mathbf{Q}[x_1, x_2]$, so that,

$$(\partial_{x_2}\omega(x_1, y_i))^m \cdot h(x_1, y_i, z_i) \equiv 0,$$

for $i = 1, 2$. As $\partial_{x_2}\omega(x_1, y_i)$ cannot be identically zero - $\mathcal{K}(\pi_1, \mathscr{C}_2)$ is finite by (H_5), $h(x_1, y_i, z_i) \equiv 0$.

Finally, by (H_1), $\mathbf{Q}[\mathscr{C}_3]$ is integral over $\mathbf{Q}[\mathscr{C}_2]$, so that there is

$$h_0 \in \boldsymbol{I}(\mathscr{C}_3) = \boldsymbol{I}(\mathscr{C}) \cap \mathbf{Q}[x_1, x_2, x_3]$$

monic in x_3. From above, for $i = 1, 2$, $h_0(x_1, y_i, z_i) \equiv 0$ and z_i is integral over $\mathbf{C}[[x_1 - \alpha]]$. As $\mathbf{C}$ is an algebraically closed field of characteristic 0, $\mathbf{C}[[x_1 - \alpha]]$ is integrally closed [Eis95, Cor 13.15]. Thus, as a fraction, $z_i \in \mathbf{C}[[x_1 - \alpha]]$. □

Proposition 8.3.2. *The following assertions are equivalent:*

1. $\boldsymbol{y} \in \mathrm{app}(\mathscr{C}_2)$;
2. $\boldsymbol{y}$ *is a node of* $\mathscr{C}_2$ *and*

$$(\partial^2_{x_2}\omega \cdot \partial_{x_1}\rho_3 - \partial^2_{x_1x_2}\omega \cdot \partial_{x_2}\rho_3)(\boldsymbol{y}) \neq 0. \tag{8.1}$$

Proof. Assume that $\boldsymbol{y} = (\alpha, \beta)$ is a node. We first prove that if (8.1) holds then, there are two distinct points of $\mathscr{C}$ that project on $\boldsymbol{y}$. By Lemma 8.3.1, there exist $y_1, y_2 \in \mathbf{C}[[x_1 - \alpha]]$ such that $y_1'(\alpha) \neq y_2'(\alpha)$ and $y_i(\alpha) = \beta$ and $\omega(x_1, y_i) \equiv 0$, for $i = 1, 2$. For $i = 1, 2$ let $z_i = \frac{\rho_3(x_1, y_i)}{\partial_{x_2}\omega(x_1, y_i)}$. By Lemma 8.3.1,

$$\partial_{x_2}\omega(x_1, y_i) \cdot z_i \equiv \rho_3(x_1, y_i).$$

Since $z_i \in \mathbf{C}[[x_1 - \alpha]]$, by derivation and evaluation in $x_1 = \alpha$,

$$\big(\partial^2_{x_1x_2}\omega(\boldsymbol{y}) + y_i'(\alpha)\partial^2_{x_2}\omega(\boldsymbol{y})\big)z_i(\alpha) = \partial_{x_1}\rho_3(\boldsymbol{y}) + y_i'(\alpha)\partial_{x_2}\rho_3(\boldsymbol{y}). \tag{8.2}$$

By Lemma 8.3.1, $\omega(x_1, y_i) \equiv 0$. Differentiating twice and evaluating in α, we get

$$\partial^2_{x_1}\omega(\boldsymbol{y}) + 2y_i'(\alpha)\partial^2_{x_1x_2}\omega(\boldsymbol{y}) + y_i'(\alpha)^2\partial^2_{x_2}\omega(\boldsymbol{y}) = 0.$$

Since $y_1'(\alpha) \neq y_2'(\alpha)$ by Lemma 8.3.1, they are simple roots of

$$\partial^2_{x_1}\omega(\boldsymbol{y}) + 2U\partial^2_{x_1x_2}\omega(\boldsymbol{y}) + U^2\partial^2_{x_2}\omega(\boldsymbol{y}) \in \mathbf{C}[U].$$

Therefore,

$$\partial^2_{x_1x_2}\omega(\boldsymbol{y}) + y_i'(\alpha)\partial^2_{x_2}\omega(\boldsymbol{y}) \neq 0. \tag{8.3}$$

Now let $H\colon \mathbf{C} \to \mathbf{C}$ such that for all $t \in \mathbf{C}$

$$H(t) = \frac{\partial_{x_1}\rho_3(\boldsymbol{y}) + t \cdot \partial_{x_2}\rho_3(\boldsymbol{y})}{\partial^2_{x_1x_2}\omega(\boldsymbol{y}) + t \cdot \partial^2_{x_2}\omega(\boldsymbol{y})}.$$

Using (8.2) and according to (8.3), $H(y_i'(\alpha)) = z_i(\alpha)$ for $i = 1, 2$. But H is either bijective or constant, whether (8.1) respectively holds or not. As $y_1'(\alpha) \neq y_2'(\alpha)$, (8.1) holds if and only if $z_1(\alpha) \neq z_2(\alpha)$. By Lemma 8.3.1, (2), $\boldsymbol{z}_1 = (\alpha, \beta, z_1(\alpha))$ and $\boldsymbol{z}_2 = (\alpha, \beta, z_2(\alpha))$ are points of $\mathscr{C}_3$ projecting on $\boldsymbol{y}$. From (H_3), there are $\boldsymbol{x}, \boldsymbol{x}'$ in $\mathscr{C}$ that project on resp. $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$. They are distinct if and only if (8.1) holds.

We can now prove the equivalence statement. We just proved that, if $\boldsymbol{y}$ is a node and (8.1) holds then, $\boldsymbol{y}$ is the projection of two distinct points, that cannot be singular by (H_5). Conversely, either $\boldsymbol{y}$ is not a node, and we conclude by (H_4) or, by the above discussion, it is the projection of a point of $\mathscr{C}$, with two distinct tangent lines (that project on the ones of $\boldsymbol{y}$). Hence, $\boldsymbol{y}$ is the projection of a singular point and then, not in $\mathrm{app}(\mathscr{C}_2)$, by definition. □

8.4 Connectivity recovery

We now investigate the connectivity relation between $\mathscr{C}_{\mathbf{R}}$ and $\mathscr{C}_{2,\mathbf{R}}$. The following lemma is partly adapted from [El 08, Lemma 6.2].

Lemma 8.4.1. *Let $\boldsymbol{x} = (\boldsymbol{x}_1 \ldots, \boldsymbol{x}_n) \in \mathcal{K}(\pi_1, \mathscr{C})$, then $\boldsymbol{x} \in \mathbf{R}^n$ if and only if $\boldsymbol{x}_1 \in \mathbf{R}$, and $\mathcal{K}(\pi_1, \mathscr{C}_2) - \mathrm{app}(\mathscr{C}_2) = \pi_2\big(\mathcal{K}(\pi_1, \mathscr{C})\big)$.*

Proof. The second point is a direct consequence of (H_2), as the non-singular critical points of $\mathscr{C}$ project to the ones of $\mathscr{C}_2$.

Let $\boldsymbol{x} \in \mathcal{K}(\pi_1, \mathscr{C})$, and assume $\boldsymbol{x}_1 \in \mathbf{R}$. By [GE96, Prop 3.1], as $\mathscr{C}$ is in generic position, computing sub-resultant sequences gives a rise to $\sigma_2 \in \mathbf{Q}[x_1]$ such that $\boldsymbol{x}_2 = \sigma_2(\boldsymbol{x}_1) \in \mathbf{R}$. By ($\mathsf{H}_6$), the line $\boldsymbol{V}(x_1 - \boldsymbol{x}_1, x_2 - \boldsymbol{x}_2)$ intersects $\mathscr{C}$ at exactly one point. Hence, by [CLO15, Thm 3.2], computing a Gröbner basis of the ideal

$$\boldsymbol{I}(\mathscr{C}) + \int x_1 - \boldsymbol{x}_1, x_2 - \boldsymbol{x}_2 \subset \mathbf{R}[\boldsymbol{X}]$$

with respect to the lexicographic order $x_1 \prec \cdots \prec x_n$ gives a rise to $n-2$ polynomials $\sigma_3, \ldots, \sigma_n$ such that $\sigma_i \in \mathbf{R}[x_1, \ldots, x_{i-1}]$ and $\sigma_i(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{i-1}) = \boldsymbol{x}_i$, for $3 \leq i \leq n$. Hence, the triangular system formed by the σ_i's raises polynomials $\tau_2, \ldots, \tau_n \in \mathbf{R}[x_1]$ such that $\boldsymbol{x}_i = \tau_i(\boldsymbol{x}_1)$ for $i \geq 2$, thus $\boldsymbol{x} \in \mathbf{R}^n$. The converse is straightforward. □

The following lemma shows that, except at apparent singularities, the real traces of $\mathscr{C}$ and $\mathscr{C}_2$ share the same connectivity properties.

Lemma 8.4.2. *The restriction of π_2 to $\mathscr{C}_{\mathbf{R}} - \pi_2^{-1}(\mathrm{app}(\mathscr{C}_2))$ is a semi-algebraic homeomorphism of inverse φ_2, defined on $\mathscr{C}_{2,\mathbf{R}} - \mathrm{app}(\mathscr{C}_2)$ such that*

$$\text{for all } \boldsymbol{y} \notin \mathcal{K}(\pi_1, \mathscr{C}_2), \quad \varphi_2(\boldsymbol{y}) = \Big(\boldsymbol{y}, \frac{\rho_3(\boldsymbol{y})}{\partial_{x_2}\omega(\boldsymbol{y})}, \dots, \frac{\rho_n(\boldsymbol{y})}{\partial_{x_2}\omega(\boldsymbol{y})}\Big).$$

Proof. Consider $\boldsymbol{y} \in \mathscr{C}_{2,\mathbf{R}} - \mathrm{app}(\mathscr{C}_2)$. As $\mathscr{C}_2 = \boldsymbol{V}(\omega)$, either $\partial_{x_2}\omega(\boldsymbol{y})$ is non-zero or $\boldsymbol{y} \in \mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbf{R}}) - \mathrm{app}(\mathscr{C}_2)$. In the latter case, according to Lemma 8.4.1

$$\pi_2^{-1}(\boldsymbol{y}) \cap \mathscr{C} \subset \mathcal{K}(\pi_1, \mathscr{C}_{\mathbf{R}}).$$

By (H_6) there is a unique $\boldsymbol{x} \in \mathcal{K}(\pi_1, \mathscr{C}_{\mathbf{R}}) - \pi_2^{-1}(\mathrm{app}(\mathscr{C}_2))$ such that $\pi_2(\boldsymbol{x}) = \boldsymbol{y}$. Let $\varphi_2 : \mathscr{C}_{2,\mathbf{R}} - \mathrm{app}(\mathscr{C}_2) \to \mathbf{R}^n$ be defined as:

- ▷ **if** $\boldsymbol{y} \in \mathcal{K}(\pi_1, \mathscr{C}_2) - \mathrm{app}(\mathscr{C}_2)$, then $\varphi_2(\boldsymbol{y})$ is the unique $\boldsymbol{x}$ satisfying $\pi_2(\boldsymbol{x}) = \boldsymbol{y}$;
- ▷ **else** $\varphi_2(\boldsymbol{y}) = \big(\boldsymbol{y}, (\rho_3/\partial_{x_2}\omega)(\boldsymbol{y}), \dots, (\rho_n/\partial_{x_2}\omega)(\boldsymbol{y})\big)$.

Since its graph is a semi-algebraic set by construction, φ_2 is a semi-algebraic map according to [BPR06, §2.5.2]. Moreover, if $\boldsymbol{y} \in \mathscr{C}_{2,\mathbf{R}} - \mathrm{app}(\mathscr{C}_2)$, then $\varphi_2(\boldsymbol{y})$ is the unique element of $\mathscr{C}_{\mathbf{R}} - \pi_2^{-1}(\mathrm{app}(\mathscr{C}_2))$ such that $\pi_2(\varphi_2(\boldsymbol{y})) = \boldsymbol{y}$.

Since $\partial_{x_2}\omega(\boldsymbol{y})$ does not vanish on this set, φ_2 is continuous on $\mathscr{C}_{2,\mathbf{R}} - \mathcal{K}(\pi_1, \mathscr{C}_2)$. We prove that it is continuous everywhere. Let $\boldsymbol{y} \in \mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbf{R}}) - \mathrm{app}(\mathscr{C}_2)$ and suppose there is a semi-algebraic path $\gamma : [0,1] \to \mathscr{C}_{2,\mathbf{R}}$, such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(t) \in \mathscr{C}_{2,\mathbf{R}} - \mathcal{K}(\pi_1, \mathscr{C}_2)$, for all $t > 0$. Consider the semi-algebraic path $\tau : t \in (0,1] \mapsto \varphi_2(\gamma(t)) \in \mathscr{C}_{\mathbf{R}}$. Since π_2 is a proper map by (H_1), τ is bounded. Thus, by [BPR06, Prop 3.21], τ can be continuously extended in $t = 0$ and by continuity, $\tau(0) \in \mathscr{C}_{\mathbf{R}}$ and $\pi_2(\tau(0)) = \pi_2(\varphi_2(\boldsymbol{y})) = \boldsymbol{y}$. Hence, by uniqueness $\tau(0) = \varphi_2(\boldsymbol{y})$ and, by [BPR06, Prop 3.6 & 3.20], φ_2 is continuous in $\boldsymbol{y}$. Since $\mathcal{K}(\pi_1, \mathscr{C}_2)$ is finite, no such path γ exists if and only if both $\boldsymbol{y}$ and $\boldsymbol{x}$ are isolated points so that φ_2 is trivially continuous at $\boldsymbol{y}$.

In conclusion, φ_2 is a semi-algebraic map, continuous on $\mathscr{C}_{2,\mathbf{R}} - \mathrm{app}(\mathscr{C}_2)$, of inverse the restriction of π_2 to $\mathscr{C}_{\mathbf{R}} - \pi_2^{-1}(\mathrm{app}(\mathscr{C}_2))$ by Lemma 8.4.1. Hence, this latter restriction is a semi-algebraic homeomorphism, as stated. □

It remains to investigate how the connectivity of the real traces of $\mathscr{C}$ and $\mathscr{C}_2$ are related close to apparent singularities. Recall that an (ambient) isotopy of $\mathbf{R}^n$ is a continuous map $\mathcal{H} \colon \mathbf{R}^n \times [0,1] \to \mathbf{R}^n$ such that $\boldsymbol{y} \mapsto \mathcal{H}(\boldsymbol{y}, 0)$ is the identity map and $\boldsymbol{y} \mapsto \mathcal{H}(\boldsymbol{y}, t)$ is a homeomorphism for $t \in [0,1]$. Then two subsets Y and Z of $\mathbf{R}^n$ are isotopy equivalent if there is an isotopy $\mathcal{H}$ of $\mathbf{R}^n$ such that $\mathcal{H}(Y, 1) = Z$.

Recall also that a graph $\mathscr{G}$ is the data of a set $\mathcal{V}$ of vertices, together with a set $\mathcal{E}$ of edges $\{\boldsymbol{v}, \boldsymbol{v}'\}$, where $\boldsymbol{v}, \boldsymbol{v}' \in \mathcal{V}$. For any $\boldsymbol{y}, \boldsymbol{y}' \in \mathbf{R}^2$, we will denote by $[\boldsymbol{y}, \boldsymbol{y}']$, the closed line segment $\{(1-t)\boldsymbol{y} + t\boldsymbol{y}', t \in [0,1]\}$. Then, if $\mathcal{V} \subset \mathbf{R}^2$, we call the piecewise linear curve, denoted $\mathscr{C}_{\mathscr{G}}$, associated to $\mathscr{G}$ the union of $[\boldsymbol{v}, \boldsymbol{v}']$ for all $\{\boldsymbol{v}, \boldsymbol{v}'\} \in \mathcal{E}$. In the following, we note $\mathcal{P}_2 = \pi_2(\mathcal{P})$.

Definition 8.4.3. Let $\mathscr{G}_2 = (\mathcal{V}_2, \mathcal{E}_2)$ be a graph, with $\mathcal{V}_2 \subset \mathbf{R}^2$. Then we say that $\mathscr{G}_2$ is a *real topology graph* of $(\mathscr{C}_2, \mathcal{P}_2)$ if

1. $\mathscr{C}_{2,\mathbf{R}}$ is isotopy equivalent to $\mathscr{C}_{\mathscr{G}_2}$;
2. the points of $\mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbf{R}}) \cup \mathcal{P}_{2,\mathbf{R}}$ are embedded in $\mathcal{V}_2$;
3. no two points of $\mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbf{R}})$ have adjacent vertices in $\mathscr{G}$.

For the rest of this section, let $\mathscr{G}_2$ be a *real topology graph* of $(\mathscr{C}_2, \mathcal{P}_2)$, $\mathcal{H}$ the induced isotopy and, for $t \in [0,1]$, $\mathcal{H}_t : \boldsymbol{y} \in \mathbf{R}^2 \to \mathcal{H}(\boldsymbol{y}, t)$, so that $\mathcal{H}_1(\mathscr{C}_{\mathscr{G}_2}) = \mathscr{C}_{2,\mathbf{R}}$.

Consider semi-algebraic paths $\gamma_1, \ldots, \gamma_4$ in $\mathbf{R}^2$, all starting from a unique point $\boldsymbol{p} \in \mathbf{R}^2$, and not intersecting each other elsewhere (see Figure 8.1), so that the γ_i's can be pairwise associated with respect to their unique *opposite branch at* $\boldsymbol{p}$: given an orientation of $\mathbf{R}^2$ and a sufficiently small circle centered at $\boldsymbol{p}$, we arrange the $\gamma_i's$ around $\boldsymbol{p}$ with respect to their unique intersection with this circle [BCR98, Thm 9.3.6]; we then pairwise associate them to the one after next in the above arrangement (it does not depend on the chosen orientation). Up to reindexing, say that (γ_1, γ_3) and (γ_2, γ_4) are the *unique pairs of opposite branches at* $\boldsymbol{p}$.

The next lemma follows directly from classical results in knots and braids theory, see [BZ02, Prop 1.9-10] for the key arguments.

Lemma 8.4.4. *Let the γ_i's as above, and any isotopy $\widetilde{\mathcal{H}}$ of $\mathbf{R}^2$. The curves $(\widetilde{\mathcal{H}}_1(\gamma_1), \widetilde{\mathcal{H}}_1(\gamma_3))$ and $(\widetilde{\mathcal{H}}_1(\gamma_2), \widetilde{\mathcal{H}}_1(\gamma_4))$ do not intersect each other, except at $\widetilde{\mathcal{H}}_1(\boldsymbol{p})$. They are the unique pairs of opposite branches at this point.*

This property allows us to deduce relations between edges of $\mathscr{G}_2$, from relations between the associated branches of $\mathscr{C}_{2,\mathbf{R}}$.

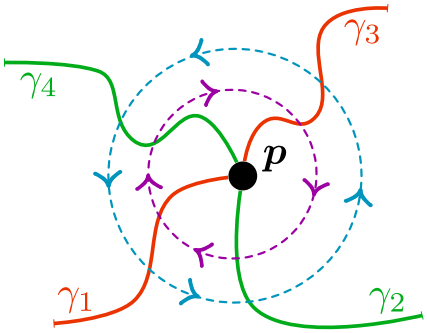


Figure 8.1. *The figure illustrates the context of Lemma 8.4.4 with two possible ordering of the branches; the braid structure appears here clearly.*

Lemma 8.4.5. *Let $\boldsymbol{y} = (\alpha, \beta) \in \mathrm{app}(\mathscr{C}_{2,\mathbf{R}})$. There are exactly five distinct vertices $\boldsymbol{v}_0, \ldots, \boldsymbol{v}_4 \in \mathcal{V}_2$ such that $\mathcal{H}_1(\boldsymbol{v}_0) = \boldsymbol{y}$ and for $1 \leq i \leq 4$:*

1. *$\{\boldsymbol{v}_0, \boldsymbol{v}_i\} \in \mathcal{E}_2$ and $\mathcal{H}_1(\boldsymbol{v}_i) \notin \mathrm{app}(\mathscr{C}_2)$;*
2. *if $e_i = [\boldsymbol{v}_0, \boldsymbol{v}_i]$, the $e_i's$ do not cross each other except at $\boldsymbol{v}_0$;*
3. *there exists unique semi-algebraic paths $\tau_1, \ldots, \tau_4$ such that for*

$$\tau_i : [0,1] \to \mathscr{C}_{\mathbf{R}}, \quad \begin{cases} \pi_2(\tau_i([0,1])) = \mathcal{H}_1(e_i) \\ \pi_2(\tau_i(0)) = \boldsymbol{y} \end{cases}$$

4. *assume that* (e_1, e_3) *and* (e_2, e_4) *are the two unique pairs of opposite edges of* $\mathscr{G}_2$ *at* $\boldsymbol{v}_0$. *Then, there exist* $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$ *in* $\pi_2^{-1}(\boldsymbol{y}) \cap \mathscr{C}_{\mathbf{R}}$, *such that* $\boldsymbol{x}_1 = \tau_1(0) = \tau_3(0)$ *and* $\boldsymbol{x}_2 = \tau_2(0) = \tau_4(0)$.

Proof. Let $\boldsymbol{v}_0 = \mathcal{H}_1^{-1}(\boldsymbol{y})$. As $\boldsymbol{y}$ is a node, there are exactly four distinct vertices $\boldsymbol{v}_1, \dots, \boldsymbol{v}_4 \in \mathcal{V}_2$ such that $\{\boldsymbol{v}_0, \boldsymbol{v}_i\} \in \mathcal{E}_2$, for $1 \leq i \leq 4$. Indeed, for $1 \leq i \leq 4$, let

$$e_i : t \in [0,1] \mapsto \boldsymbol{v}_0 + t(\boldsymbol{v}_i - \boldsymbol{v}_0) \in \mathbf{R}^2$$

and $\gamma_i = \mathcal{H}_1 \circ e_i$. Then the γ_i's are the four branches of $\mathscr{C}_{2,\mathbf{R}}$ incident in $\boldsymbol{y}$. Remark that, by the third item of Definition 8.4.3, none of the $\mathcal{H}_1(\boldsymbol{v}_i)$'s lie in $\mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbf{R}})$, since $\mathcal{H}_1(\boldsymbol{v}_0) = \boldsymbol{y}$ does. Besides, by the second item, the γ_i's do not intersect $\mathcal{K}(\pi_1, \mathscr{C}_2)$, except in $\boldsymbol{y}$.

In particular, the $\gamma_i's$ do not contain points of $\mathrm{app}(\mathscr{C}_2)$ and intersect each other only at $\boldsymbol{y}$. Hence, by Lemma 8.4.4, through $\mathcal{H}_1$, the e_i's intersect each other only at $\boldsymbol{v}_0$.

Besides, let $i \in \{1, \dots, 4\}$, and for $0 < t \leq 1$, let $\tau_i(t) = \varphi_2(\gamma_i(t))$, where φ_2 is defined in Lemma 8.4.2. It is a well-defined semi-algebraic path by the above discussion. Moreover, by Lemma 8.4.2, $\tau_i(t) \in \mathscr{C}_{\mathbf{R}}$ and $\pi_2(\tau(t)) = \gamma(t) = \mathcal{H}_1(e_i(t))$, for all $0 < t \leq 1$. Since π_2 is a proper map by (H_1), [BPR06, Prop 3.21] implies that τ_i can be continuously extended in $t = 0$. Moreover, by continuity, $\pi_2(\tau_i(0)) = \boldsymbol{y}$.

Finally, $\boldsymbol{y}$ being a node, there exist points $\theta_1 \neq \theta_2$ in $\mathbf{R}^2$ and $1 \leq i_1, i_2, i_3, i_4 \leq 4$ such that,

$$\theta_1 = \gamma'_{i_1}(0) = \gamma'_{i_3}(0) \quad \text{and} \quad \theta_2 = \gamma'_{i_2}(0) = \gamma'_{i_4}(0).$$

This means that the branches $(\gamma_{i_1}, \gamma_{i_3})$ and $(\gamma_{i_2}, \gamma_{i_4})$ are the two pairs of opposite branches of $\mathscr{C}_2$ at $\boldsymbol{y}$. Then, by Lemma 8.4.4, (e_{i_1}, e_{i_3}) and (e_{i_2}, e_{i_4}) are the two pairs of opposite edges of $\mathscr{G}_2$ at $\boldsymbol{y}$. For the sake of clarity assume, without loss of generality that $i_k = k$ for all $1 \leq k \leq 4$. By continuity, there exist $\vartheta_1 \neq \vartheta_2$ in $\mathbf{R}^n$ such that

$$\vartheta_1 = \tau'_1(0) = \tau'_3(0) \quad \text{and} \quad \vartheta_2 = \tau'_2(0) = \tau'_4(0),$$

and $\tau_i(0) \in \pi_2^{-1}(\boldsymbol{y}) \cap \mathscr{C}_{\mathbf{R}}$ for $1 \leq i \leq 4$. But as $\boldsymbol{y} \in \mathrm{app}(\mathscr{C}_2)$, $\pi_2^{-1}(\boldsymbol{y}) \cap \mathscr{C}$ contains two distinct non-singular points, of distinct tangent lines, by (H_2) and (H_4). Since the $\tau'_i(0)$'s are tangent lines of $\mathscr{C}$, necessarily, $\tau_1(0)$ and $\tau_3(0)$ are equal to one of these points, while $\tau_2(0)$ and $\tau_4(0)$ are equal to the other one (if multiple branches converge at a point or the tangent lines differ, it becomes singular). □

If $\mathcal{V}_{\mathsf{app}} = \mathcal{H}_1^{-1}(\mathrm{app}(\mathscr{C}_2)) \subset \mathcal{V}_2$ is the subset of apparent nodes, then Lemma 8.4.5 provides a procedure to compute a new graph $\mathscr{G}$, from which we can deduce connectivity queries on $\mathscr{C}$.

Definition 8.4.6. Let NodeResolution be the procedure that takes as input $\mathscr{G}_2$ and $\mathcal{V}_{\mathsf{app}}$ as above and outputs the graph $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ as follows (we keep notations of Lemma 8.4.5).

1. For all $\boldsymbol{v} \in \mathcal{V}_{\mathsf{app}}$, compute the adjacent vertices $\boldsymbol{v}_1, \dots, \boldsymbol{v}_4$ of $\boldsymbol{v}$, indexed such that (e_1, e_3) and (e_2, e_4) are opposite edges.
2. Remove $\boldsymbol{v}$ from $\mathcal{V}_2$ and replace the four edges $(\{\boldsymbol{v}, \boldsymbol{v}_k\})_{1 \leq k \leq 4}$ by the two edges $(\{\boldsymbol{v}_j, \boldsymbol{v}_{j+2}\})_{k=1,2}$, as depicted in Figure 8.2.

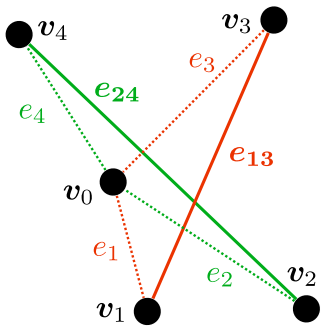


Figure 8.2. *This illustration shows how NodeResolution (Definition 8.4.6) modifies $\mathscr{G}_2$ at vertices of $\mathcal{V}_{\text{app}}$. Here, the dotted and solid lines represent the edges of $\mathscr{G}_2$ and $\mathscr{G}$, respectively.*

We say that $v, v' \in \mathcal{V}$ are connected in a graph $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ if there exists an ordered sequence $(v_0, \dots, v_{N+1})$ of vertices in $\mathcal{V}$ such that $v_0 = v$, $v_{N+1} = v'$ and $\{v_i, v_{i+1}\} \in \mathcal{E}$, for all $0 \leq i \leq N$.

Proposition 8.4.7. *Let $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ be the graph output by NodeResolution, on input $\mathscr{G}_2$ and $\mathcal{V}_{\text{app}}$. Then,*

1. $\pi_2(\mathcal{P}_{\mathbf{R}}) \subset \mathcal{H}_1(\mathcal{V})$;

2. *$y, y' \in \mathcal{P}_{\mathbf{R}}$ are semi-algebraically connected in $\mathscr{C}_{\mathbf{R}}$ if and only if $\mathcal{H}_1^{-1}(\pi_2(y))$ and $\mathcal{H}_1^{-1}(\pi_2(y'))$ are connected in $\mathscr{G}$.*

Proof. (H5) and (H6) imply $\pi_2(\mathcal{P}) \cap \mathcal{H}_1(\mathcal{V}_{\text{app}}) = \emptyset$. Then $\mathcal{P}_{2,\mathbf{R}} = \pi_2(\mathcal{P}_{\mathbf{R}})$ as π_2 is injective on $\mathcal{P}$, and, by definition, $\mathcal{P}_{2,\mathbf{R}} \subset \mathcal{V}$.

We now deal with the second statement. Let $x, x' \in \mathcal{P}_{\mathbf{R}}$ and

$$v = \mathcal{H}_1^{-1}(\pi_2(x)) \quad \text{and} \quad v' = \mathcal{H}_1^{-1}(\pi_2(x'))$$

in $\mathcal{V}$. Assume first that v and v' are connected in $\mathscr{G}$. Then there exist $v_1, \dots, v_N \in \mathcal{V}$ such that, if $v_0 = v$ and $v_{N+1} = v'$, then $\{v_i, v_{i+1}\} \in \mathcal{E}$ and $\mathcal{H}_1(v_i) \notin \text{app}(\mathscr{C}_2)$ for $0 \leq i \leq N+1$. Fix $i \in \{0, \dots, N\}$. By Lemma 8.4.2, $x_i = \varphi_2(\mathcal{H}_1(v_i))$ and $x_{i+1} = \varphi_2(\mathcal{H}_1(v_{i+1}))$ are well-defined in $\mathscr{C}_{\mathbf{R}}$

If $\{v_i, v_{i+1}\} \in \mathcal{E}_2$ then, $\mathcal{H}_1([v_i, v_{i+1}]) \cap \text{app}(\mathscr{C}_2) = \emptyset$, and, by Lemma 8.4.2, x_i and x_{i+1} are semi-algebraically connected in $\mathscr{C}_{\mathbf{R}}$ through φ_2. Otherwise, $\{v_i, v_{i+1}\} \notin \mathcal{E}_2$, and, by construction of $\mathscr{G}$, there exists $w \in \mathcal{V}_{\text{app}}$ such that $\{v_i, w\}$ and $\{w, v_{i+1}\}$ are in $\mathcal{E}_2$. However, since $\{v_i, v_{i+1}\} \in \mathcal{E}$, then, according to the construction of $\mathscr{G}$,

$$e_i = [w, v_i] \quad \text{and} \quad e_{i+1} = [w, v_{i+1}]$$

are opposite edges of $\mathscr{G}_2$ at w. Hence, by items *(2)* and *(3)* of Lemma 8.4.5, there exists a semi-algebraic path $\tau : [-1, 1] \to \mathscr{C}_{\mathbf{R}}$ connecting x_i to x_{i+1}. All in all, by transitivity, $x_0 = x$ and $x_{N+1} = x'$ are semi-algebraically connected in $\mathscr{C}_{\mathbf{R}}$, and we are done.

Conversely, suppose that $\boldsymbol{x}$ and $\boldsymbol{x}'$ are semi-algebraically connected in $\mathscr{C}_{\mathbf{R}}$ and let $\tau : [0,1] \to \mathscr{C}_{\mathbf{R}}$ be a semi-algebraic path such that $\tau(0) = \boldsymbol{x}$ and $\tau(1) = \boldsymbol{x}'$. Let $\gamma = \pi_2 \circ \tau$, and

$$\{t_1, \ldots, t_N\} = \gamma^{-1}\big(\mathcal{H}_1(\mathcal{V}_2)\big) \subset (0,1)$$

such that $t_1 < \ldots < t_N$. Let $t_0 = 0$, $t_{N+1} = 1$ and for $0 \leq i \leq N+1$, $\boldsymbol{v}_i = \mathcal{H}_1^{-1}(\gamma(t_i)) \in \mathcal{V}_2$. By assumption, $\{\boldsymbol{v}_i, \boldsymbol{v}_{i+1}\} \in \mathcal{E}_2$ for all $i \in \{0, \ldots, N\}$. Let us prove by induction that for $0 \leq i \leq N+1$, either $\boldsymbol{v}_i \in \mathcal{V}_{\mathsf{app}}$ or $\boldsymbol{v}_i$ is connected to $\boldsymbol{v}_0$ in $\mathscr{G}$. If $i = 0$, there is nothing to prove, so let $1 \leq i \leq N$ and suppose that the statement holds for all $0 \leq j < i$.

Assume $\boldsymbol{v}_{i+1} \notin \mathcal{V}_{\mathsf{app}}$. Then, either $\boldsymbol{v}_i \notin \mathcal{V}_{\mathsf{app}}$, and, by induction hypothesis, $\boldsymbol{v}_{i+1}$ and $\boldsymbol{v}_0$ are connected, through $\boldsymbol{v}_i$, in $\mathscr{G}$. Either $\boldsymbol{v}_i \in \mathcal{V}_{\mathsf{app}}$ and, by Lemma 8.4.5, there are exactly four distinct $\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3, \boldsymbol{w}_4 \in \mathcal{V} - \mathcal{V}_{\mathsf{app}}$ such that $\{\boldsymbol{v}_i, \boldsymbol{w}_j\} \in \mathcal{E}_2$, for $1 \leq j \leq 4$. Assume, without loss of generality, that $\boldsymbol{v}_{i+1} = \boldsymbol{w}_1$. Then, there is $j_1 \in \{2,3,4\}$ such that $\boldsymbol{v}_{i-1} = \boldsymbol{w}_{j_1}$. Using the notation of Lemma 8.4.5, assume, without loss of generality, that $e_3 = [\boldsymbol{v}_i, \boldsymbol{w}_3]$ is the opposite branch of $e_1 = [\boldsymbol{v}_i, \boldsymbol{w}_1]$ in $\mathscr{G}_2$ at $\boldsymbol{v}_i$. Then, by items *(2)* and *(3)* of Lemma 8.4.5, we have $j_0 = 3$, since $\tau([t_{i-1}, t_i])$ is connected to $\tau([t_i, t_{i+1}])$. By construction of $\mathscr{G}$, $\boldsymbol{w}_1 = \boldsymbol{v}_{i+1}$ is connected to $\boldsymbol{w}_3 = \boldsymbol{v}_{i-1}$ in $\mathscr{G}$, so that, by induction, $\boldsymbol{v}_{i+1}$ is connected to $\boldsymbol{v}_0$, through $\boldsymbol{v}_{i-1}$. Hence, $\boldsymbol{v} = \boldsymbol{v}_{N+1}$ and $\boldsymbol{v}' = \boldsymbol{v}_0$ are connected in $\mathscr{G}$, proving the converse. □

Proposition 8.4.7 also implies that $\mathscr{G}$ and $\mathscr{C}_{\mathbf{R}}$ share the same number of semi-algebraically connected components. Therefore, by computing $\mathscr{G}$, one can determine this number and answer connectivity queries on $\mathcal{P}_{\mathbf{R}}$.

8.5 Algorithm

We now provide an algorithm for solving connectivity queries over real algebraic curves, whose different steps correspond sequentially, except for one, to the different sections of this chapter.

Given a sequence of polynomials defining an algebraic curve, the first step is to perform a linear change of variable, generic enough to ensure assumption (H), and to compute a one-dimensional parametrization encoding it. Answering connectivity queries on the sheared curve is equivalent to do so on the original curve. By [GM19, Thm 6.18] (or [SS17, Prop 6.3]), computing such a parametrization has complexity cubic in the degree of the curve, thus bounded by our overall complexity. Besides, according to [SS17, § J], changing variables in zero and one-dimensional parametrizations has similar complexity. Hence, for the sake of clarity, we omit these two steps.

Following the state of the art of curve topology computation, we consider polynomials with integer coefficients, so that $\mathbf{Q} = \mathbb{Q}$, $\mathbf{R} = \mathbb{R}$ and $\mathbf{C} = \mathbb{C}$. Moreover, we denote by $\preceq_1$ the preorder on points of $\mathbb{R}^n$ w.r.t. the first coordinate, when they are distinct.

8.5.1 Subroutines

We assume that $\mathscr{R} = (\omega, \rho_3, \ldots, \rho_n)$ has coefficients in $\mathbb{Z}$ and magnitude (δ, τ), and consider a zero-dimensional parametrization $\mathscr{P} = (\lambda, \vartheta_2, \ldots, \vartheta_n)$, with coefficients in $\mathbb{Z}$ and magnitude

(μ, κ) encoding $\mathcal{P}$. Note that $\mathscr{R}_2 = (\omega, \rho_2)$ and $\mathscr{P}_2 = (\lambda, \vartheta_2)$ are parametrizations encoding respectively $\mathscr{C}_2$ and $\mathcal{P}_2$. We denote further $R = \mathrm{Res}_{x_2}(\omega, \partial_{x_2}\omega)$. Since, by (H$_7$), ω is monic in x_2, its roots are exactly the abscissas of $\mathcal{K}(\pi_1, \mathscr{C}_2)$. From (H$_5$), points of $\mathrm{app}(\mathscr{C}_2)$ can be identified by their abscissa, which, following Proposition 8.3.2, can be reduced to gcd computations.

Proposition 8.5.1. *There exists an algorithm ApparentSingularities taking as input $\mathscr{R}$, as above, and computing a square-free polynomial $q_{\mathrm{app}} \in \mathbb{Z}[x_1]$, of magnitude $(\delta^2, \widetilde{O}(\delta^2 + \delta\tau))$ such that*

$$\mathrm{app}(\mathscr{C}_2) = \{(\alpha, \beta) \in \mathcal{K}(\pi_1, \mathscr{C}_2) \mid q_{\mathrm{app}}(\alpha) = 0\},$$

using $\widetilde{O}(\delta^6 + \delta^5\tau)$ bit operations.

Proof. Let $(\alpha, \beta) \in \mathcal{K}(\pi_1, \mathscr{C}_2)$. According to [El 08, Thm 3.2.(ii)], since $\mathscr{C}$ satisfies (H), (α, β) is a node if and only if α is a double root of R, i.e. if and only if α is a root of

$$q = \gcd(R^*, R') / \gcd(R^*, R', R''),$$

where R^* is the square-free part of R. Moreover, let $(\mathrm{sr}_1, \mathrm{sr}_{1,0})$ be the first subresultant sequence of $(\omega, \partial_{x_2}\omega)$. By [GE96, Thm 3.1], if $q(\alpha) = 0$ then, $\mathrm{sr}_1(\alpha) \neq 0$, and

$$\mathrm{sr}_1(\alpha) \cdot \beta = -\mathrm{sr}_{1,0}(\alpha).$$

Let $A(x_1, x_2)$ be the polynomial on the left-hand side of (8.1) in Proposition 8.3.2, and u be a new indeterminate. Let $\widetilde{A}(x_1, x_2, u)$ be the homogenization of A in x_2, and $B = \widetilde{A}(x_1, -\mathrm{sr}_{1,0}, \mathrm{sr}_1)$. Then, from Proposition 8.3.2, the square-free polynomial

$$q_{\mathrm{app}} = q / \gcd(q, B)$$

vanishes at α if and only if $(\alpha, \beta) \in \mathrm{app}(\mathscr{C}_2)$, as required.

We now deal with the quantitative bounds. By [MSW15, Lemma 14], R, R^*, sr_1 and $\mathrm{sr}_{1,0}$ have magnitude $(\delta^2, \widetilde{O}(\delta^2 + \delta\tau))$ and can be computed using $\widetilde{O}(\delta^6 + \delta^5\tau)$ bit operations. Hence, by [GG13, Cor 11.14] and [MSW15, Lemma 12], computing $\gcd(R^*, R')$, $\gcd(R^*, R', R'')$ and then q can be done using $\widetilde{O}(\delta^4 + \delta^3\tau)$ bit operations. Moreover, by [MSW15, Lemma 11], q has magnitude $(\delta^2, \widetilde{O}(\delta^2 + \delta\tau))$.

Besides, $\widetilde{A}$ has magnitude $(O(\delta), \widetilde{O}(\tau))$, so that B has magnitude

$$\big(\widetilde{O}(\delta^3), \widetilde{O}(\delta^3 + \delta^2\tau)\big).$$

Hence, by [GG13, Cor 11.14] computing, $\gcd(q, B)$ requires $\widetilde{O}(\delta^6 + \delta^5\tau)$ bit operations. From this, computing q_{app} costs $\widetilde{O}(\delta^4 + \delta^3\tau)$ bit operations, by [DDR$^+$22, Prop 2.15]. Finally, q_{app} has magnitude $(\delta^2, \widetilde{O}(\delta^2 + \delta\tau))$, by [MSW15, Lemma 11]. □

Suppose now that the polynomial q_{app}, from Proposition 8.5.1, has been computed. We can compute a real topology graph of $(\mathscr{C}_2, \mathcal{P}_2)$, while identifying the vertices corresponding to $\mathrm{app}(\mathscr{C}_2)$ and $\mathcal{P}_2$.

Proposition 8.5.2. *There exists an algorithm Topo2D taking as input $\mathscr{R}$, $\mathscr{P}_2$ and q_{app} as above and computing $\mathscr{G} = (\mathcal{V}, \mathcal{E})$, a real topology graph of $(\mathscr{C}_2, \mathcal{P}_2)$, of size at most $O(\delta^3 + \delta\mu)$, using*

$$\widetilde{O}(\delta^6 + \delta^5\tau + \mu^6 + \mu^5\kappa)$$

bit operations. It also outputs sequences $\mathscr{V}_{\text{app}}$ and $\mathscr{V}_{\mathscr{P}}$, of elements of $\mathcal{V}$, that are in one-to-one correspondence with resp. the points of $\text{app}(\mathscr{C}_{2,\mathbb{R}})$ and $\mathcal{P}_{2,\mathbb{R}}$, ordered with respect to $\preceq_1$.

Proof. According to [KS15, Thm 14], and more recently [DDR+22, Thm 1.1], there is an algorithm that computes a planar graph $\mathscr{G}$, whose associated piecewise linear curve $\mathscr{C}_{\mathscr{G}}$, is isotopy equivalent to $\mathscr{C}_{2,\mathbb{R}}$, using $\widetilde{O}(\delta^6 + \delta^5\tau)$ bit operations. Under slight modifications, these algorithms can compute the claimed output of Topo2D, within the same complexity bounds. For clarity, we only consider the algorithm of [DDR+22], that we roughly describe.

Let $\alpha_1 < \cdots < \alpha_N$ be the abscissas of the points of $\mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbb{R}})$. They are distinct by ($\mathsf{H}_5$). [DDR+22, Prop 2.24] first computes disjoint isolating intervals for each α_i. Then, [DDR+22, Prop 3.13] isolates the ordinates of the points above each α_i. This process gives rise to isolating boxes, which stand for vertices in the final graph. The algorithm eventually connects these boxes to separating vertices above regular values in the intervals (α_j, α_{j+1}). The latter is done by counting the number of incoming left and right branches in each box. For points of $\mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbb{R}})$, it is tackled by [DDR+22, §4.2-4], while for others it is straightforward (exactly one branch from each side).

The above process computes a graph $\mathscr{G} = (\mathcal{V}, \mathcal{E})$, such that $\mathscr{C}_{\mathscr{G}}$ is isotopy equivalent to $\mathscr{C}_{2,\mathbb{R}}$. Remark that $\mathcal{V}$ contains a subset $\mathcal{V}_{\mathcal{K}}$ of vertices associated to the unique point of $\mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbb{R}})$ above the α_i's, all separated by vertices associated to regular points. Moreover, by Proposition 8.5.1, $\mathcal{V}_{\text{app}}$ is exactly the subset of $\mathcal{V}_{\mathcal{K}}$, associated to the α_i's where q_{app} vanishes. Then, according to [DDR+22, Prop 2.24] and Proposition 8.5.1, one can compute disjoint isolating intervals of the roots of R and q_{app} and identify all common roots, using

$$\widetilde{O}(\delta^6 + \delta^5\tau)$$

bit operations. This gives $\mathscr{V}_{\text{app}}$.

Hence, it remains to show that introducing vertices for control points $\mathcal{P}_{2,\mathbb{R}}$ (together with those above and below) can be done in the claimed bound. First, recall that $\mathcal{D} = (\lambda, \vartheta_2)$ encodes $\mathcal{P}_2$. According to [DDR+22, Prop 2.24] again, we can compute disjoint isolating intervals for all distinct (by (H_5)) real roots of λ and R, using at most

$$\widetilde{O}(\delta^6 + \delta^5\tau + \mu^6 + \mu^5\kappa)$$

bit operations. Next, let $g(x_1, x_2) = \lambda' \cdot x_2 - \vartheta_2$. It is a bivariate polynomial with magnitude (μ, κ). Then, according to [DDR+22, Prop 3.14], for each root β of λ, we can compute isolating intervals for all roots $\boldsymbol{x}_2$ of $(\omega \cdot g)(\beta, \boldsymbol{x}_2)$, and identify the unique common roots, within the same complexity bound. This gives $\mathscr{V}_{\mathscr{P}}$. Moreover, since $\mathcal{P} \cap \mathcal{K}(\pi_1, \mathscr{C}_{2,\mathbb{R}}) = \emptyset$, as seen above, the connection step for the introduced vertices is straightforward, and does not affect the complexity bound.

Finally, since we consider at most $\delta^2 + \mu$ fibers, each of them containing at most δ points then, taking in account the regular separating fibers, we get at most $O(\delta^3 + \delta\mu)$ vertices and edges. □

8.5.2 The algorithm

Let IndConnectComp be an algorithm taking as input a graph $\mathscr{G} = (\mathcal{V}, \mathcal{E})$, and a sequence $\mathscr{V} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_N)$ of vertices of $\mathscr{G}$. It outputs a partition $I_1, \ldots, I_s$ of $\{1, \ldots, N\}$, grouping the indices of the $\boldsymbol{v}_i$'s lying in the same connected components of $\mathscr{G}$.

Algorithm 3 ConnectCurve

Input: $\mathscr{R} = (\omega, \rho_3, \ldots, \rho_n) \subset \mathbb{Z}[x_1, x_2]$ encoding an algebraic curve $\mathscr{C} \subset \mathbb{C}^n$ and $\mathscr{P} = (\lambda, \vartheta_2, \ldots, \vartheta_n) \subset \mathbb{Z}[x_1]$ encoding points $\boldsymbol{p}_1 \preceq_1 \cdots \preceq_1 \boldsymbol{p}_\mu$ of $\mathscr{C}_\mathbb{R}$, such that $(\mathscr{C}, \mathcal{P})$ satisfies (H).

Output: a partition of $\{1, \ldots, \mu\}$ grouping the indices of the $\boldsymbol{p}_i$'s lying in the same semi-algebraically connected component of $\mathscr{C}_\mathbb{R}$.

1: $\mathscr{P}_2 \leftarrow (\lambda, \vartheta_2)$;
2: $q_{\text{app}} \leftarrow$ ApparentSingularities$(\mathscr{R})$
3: $[\mathscr{G}_2,\ \mathscr{V}_{\text{app}},\ \mathscr{V}_{\mathscr{P}}] \leftarrow$ Topo2D$(\mathscr{R},\ \mathscr{P}_2,\ q_{\text{app}})$;
4: $\mathscr{G} \leftarrow$ NodeResolution$(\mathscr{G}_2,\ \mathscr{V}_{\text{app}})$;
5: **return** IndConnectComp$(\mathscr{V}_{\mathscr{P}}, \mathscr{G})$;

The rest of the chapter is then devoted to the proof of Theorem 8.1.1, that is the correction and complexity bound of the above algorithm.

Proof of Proof of Theorem 8.1.1. Let $\mathscr{R} = (\omega, \rho_3, \ldots, \rho_n) \subset \mathbb{Z}[x_1, x_2]$ be a one-dimensional parametrization of magnitude (δ, τ) encoding an algebraic curve $\mathscr{C} \subset \mathbb{C}^n$ and $\mathscr{P} = (\lambda, \vartheta_2, \ldots, \vartheta_n) \subset \mathbb{Z}[x_1]$ be a zero-dimensional parametrization of magnitude (μ, κ) encoding points of $\mathscr{C}_\mathbb{R}$, such that $(\mathscr{C}, \mathcal{P})$ satisfies (H). Suppose, without loss of generality that $\mathcal{P} = \{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_\mu\}$, with $\boldsymbol{p}_1 \preceq_1 \cdots \preceq_1 \boldsymbol{p}_\mu$.

On input $\mathscr{R}$ and $\mathscr{P}$, algorithm ConnectCurve perform the following operations:

Step 1. According to the definition of zero-dimensional parametrizations,

$$\mathcal{P} = \left\{ \left(\boldsymbol{y}_1, \frac{\vartheta_2}{\partial_u \lambda}(\boldsymbol{y}_1), \ldots, \frac{\vartheta_n}{\partial_u \lambda}(\boldsymbol{y}_1) \right) \in \mathbf{C}^n \mid \lambda(\boldsymbol{y}_1) = 0 \right\},$$

so that $\mathscr{P}_2 = (\lambda, \vartheta_2)$ is a zero-dimensional parametrization of magnitude (μ, κ) encoding $\mathcal{P}_2 = \pi_2(\mathcal{P})$. This step has constant bit complexity $O(1)$.

Step 2. According to Proposition 8.5.1, on input $\mathscr{R}$, the algorithm ApparentSingularities outputs a square-free polynomial $q_{\text{app}} \in \mathbb{Z}[x_1]$, of magnitude $(\delta^2, \widetilde{O}(\delta^2 + \delta\tau))$ such that

$$\text{app}(\mathscr{C}_2) = \{(\alpha, \beta) \in \mathcal{K}(\pi_1, \mathscr{C}_2) \mid q_{\text{app}}(\alpha) = 0\},$$

using $\widetilde{O}(\delta^6 + \delta^5\tau)$ bit operations.

Step 2. According to Proposition 8.5.2, on input $\mathscr{R}$, $\mathscr{P}_2$ and q_{app} as above the algorithm Topo2D computes $\mathscr{G}_2 = (\mathcal{V}, \mathcal{E})$, a real topology graph of $(\mathscr{C}_2, \mathcal{P}_2)$, of size at most $O(\delta^3 + \delta\mu)$, using

$$\widetilde{O}(\delta^6 + \delta^5\tau + \mu^6 + \mu^5\kappa)$$

bit operations. It also outputs sequences $\mathscr{V}_{\text{app}}$ and $\mathscr{V}_{\mathscr{P}}$, of elements of $\mathcal{V}$, that are in one-to-one correspondence with respectively the points of $\text{app}(\mathscr{C}_{2,\mathbb{R}})$ and $\mathcal{P}_{2,\mathbb{R}}$, ordered with respect to $\preceq_1$.

Step 4. Let $\mathscr{G}$ be the graph output by the procedure NodeResolution, on input $\mathscr{G}_2$, as described in Definition 8.4.6. This procedure perform an operation of constant bit complexity at each vertex of $\mathscr{V}_{\text{app}}$, that has cardinality the one of $\text{app}(\mathscr{C}_{2,\mathbb{R}})$ by Proposition 8.5.2. According to Proposition 8.5.1, this latter cardinality is bounded by δ^2, so that bit complexity of this step is $O(\delta^2)$.

Step 5. Finally, let $I_1, \ldots, I_s$ be the subsets output by the procedure IndConnectComp, on input $\mathscr{V}_{\mathscr{P}}$ and $\mathscr{G}$. According to e.g. [CLRS09, §22.2] this procedure has bit complexity linear in the size of $\mathscr{G}$, that is $O(\delta^3 + \delta\mu)$.

According to Proposition 8.5.2, $\mathscr{V}_{\mathscr{P}} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\mu)$ is in one-to-one correspondence with $\mathcal{P}_{2,\mathbb{R}} = (\boldsymbol{p}_1, \ldots, \boldsymbol{v}_\mu)$. Hence, by the correction of IndConnectComp, $I_1, \ldots, I_s$ is a partition of $\{1, \ldots, \mu\}$.

Without loss of generality, suppose that the one-to-one correspondence between $\mathscr{V}_{\mathscr{P}}$ and $\mathcal{P}_{2,\mathbb{R}}$ associates $\boldsymbol{v}_i$ to $\boldsymbol{p}_i$, for all $1 \leq i \leq \mu$. Let $i, j \in \{1, \ldots, \mu\}$. According to the correction of IndConnectComp, i and j belong to the same $I_k \in \{I_1, \ldots, I_s\}$ if and only if $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$ belong to the same connected component of $\mathscr{G}$, and according to Proposition 8.4.7, this holds if and only if $\boldsymbol{p}_i$ and $\boldsymbol{p}_j$ belong to the same semi-algebraically connected component of $\mathscr{C}_{\mathbb{R}}$.

Therefore, the subsets $I_1, \ldots, I_s$ output by algorithm ConnectCurve is a partition of $\{1, \ldots, \mu\}$ grouping the integers that correspond to ranks, with respect to $\preceq_1$, of points in $\mathcal{P}_{\mathbb{R}}$ that belong to the same semi-algebraically connected component of $\mathscr{C}_{\mathbb{R}}$. This is equivalent to a partition of the points of $\mathcal{P}_{\mathbb{R}}$ as these have distinct first coordinate, and one can order them by univariate root isolation, using $\widetilde{O}\left(\mu^3 + \kappa\mu^2\right)$ bit operations according to [KS15, Theorem 5]. This fits within the overall complexity bound of ConnectCurve. □

As mentioned before, the number of connected components of the graph $\mathscr{G}$ computed equals the number of semi-algebraically connected components of $\mathscr{C}_{\mathbb{R}}$. As an extension, for curves given as unions, Algorithm 3 can be applied to each curve, where query points are extended to include pairwise common intersection points. The resulting subsets are then merged based on their shared points.

9 Real algebraic geometry in action: application to robotics

Abstract. In the previous chapters, we improved the different algorithmic steps to answer connectivity queries on real algebraic sets, which is a key subroutine of computational real algebraic geometry. In this chapter, we illustrate the application of real algebraic geometry and its algorithmic subroutines to solve an open problem in robotics: the identification of cuspidal robots.

Cuspidal robots are the ones with at least two inverse kinematic solutions that can be connected by a singularity-free path. Deciding the cuspidality of generic 3R robots has been studied in the past, but extending the study to six-degree-of-freedom robots can be a challenging problem. Many robots can be modeled as a polynomial map together with a real algebraic set so that the notion of cuspidality can be extended to these data.

We design an algorithm that, on input a polynomial map in n indeterminates, and s polynomials in the same indeterminates, describing a real algebraic set $V_{\mathbb{R}}$ of dimension d, decides the cuspidality of the restriction of the map to $V_{\mathbb{R}}$. Moreover, if D and τ are, respectively, the maximum degree and the maximum bit size of the coefficients of the input polynomials, this algorithm runs in time quasi-linear in τ and polynomial in $((s+d)D)^{O(n^2)}$.

It relies on many high-level algorithms in computer algebra which use advanced methods on real algebraic sets and critical loci of polynomial maps, including roadmap algorithms. As far as we know, this is the first algorithm that tackles the cuspidality problem from a general point of view.

This is joint work with D. Chablat, M. Safey El Din, D. Salunkhe and P. Wenger.

9.1 Introduction

Cuspidal robots were discovered at the end of the eighties [PCI88]. A cuspidal robot can move from one of its inverse kinematic solutions to another one without meeting a singular configuration, that is a configuration where it loses degrees of freedom. A major consequence is that determining in which solution the robot operates during motion planning trajectories for cuspidal robots is more challenging than for noncuspidal ones [Wen04]. Knowing whether a robot under design is cuspidal or not is thus of primary importance.

Most existing industrial robots are known to be noncuspidal because they rely on some specific geometric design rules such as their last three joint axes intersecting at a common point [Wen97]. Recently, however, new robots have been proposed that do not follow the aforementioned design rule, which, in turn, could make them cuspidal[1]. Hence, obtaining

[1] See e.g. https://achille0.medium.com/why-has-no-one-heard-of-cuspidal-robots-fa2fa60ffe9b

an algorithm for deciding cuspidality is of first importance in this context of mechanism design.

Problem statement. Let $\boldsymbol{f} = (f_1, \dots, f_s)$ be a sequence of polynomials in $\mathbb{Q}[x_1, \dots, x_n]$ and $V = \boldsymbol{V}(\boldsymbol{f}) \subset \mathbb{C}^n$ be the algebraic set it defines (i.e. the set of common complex solutions to the f_i's). We denote by $V_{\mathbb{R}} = V \cap \mathbb{R}^n$ the real trace of V. Let $\mathcal{R} = (r_1, \dots, r_d)$ be a sequence of polynomials in $\mathbb{Q}[x_1, \dots, x_n]$. By a slight abuse of notation, we still denote by $\mathcal{R}$ the map

$$\mathcal{R} : \boldsymbol{y} \in \mathbb{C}^n \mapsto (r_1(\boldsymbol{y}), \dots, r_d(\boldsymbol{y})) \in \mathbb{C}^d,$$

and $\mathcal{R}_{|V_{\mathbb{R}}}$ denotes the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. Many robots can be represented with such a map $\mathcal{R}$. Indeed, these are polynomial maps that map the configuration of their joints, which are usually lengths and angles, to the position of their end-effector. However, due to the Cartesian parametrization of many problems, robots behave as polynomial maps in the cosines and sines of the angles. Then, replacing the occurrences of $\cos$ and $\sin$ by new variables c and s, and adding $c^2 + s^2 - 1$ to $\boldsymbol{f}$, one gets a formulation as the one previously described.

We denote by $\mathcal{K}(\mathcal{R}, V)$ the union of the set of *critical points* of the restriction of $\mathcal{R}$ to V and the set of *singular points* of V. We refer to Section 2.5 of Chapter 2 for a precise introduction to these objects. Following the formalism introduced in [Wen92], we then propose the following formulation of the cuspidality decision problem.

Definition 9.1.1. The map $\mathcal{R}_{|V_{\mathbb{R}}}$ is *cuspidal* if there exist two distinct points $\boldsymbol{y}$ and $\boldsymbol{y}'$ in $V_{\mathbb{R}}$ such that the following holds:

(i) $\mathcal{R}(\boldsymbol{y}) = \mathcal{R}(\boldsymbol{y}')$;

(ii) $\boldsymbol{y}$ and $\boldsymbol{y}'$ are semi-algebraically path connected in $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$.

If two such points $\boldsymbol{y}$ and $\boldsymbol{y}'$ exist, we say that they form a *cuspidal pair* of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. Note that such a pair is not unique in general.

The above definition goes back to some original works in robotics and mechanism design which we present below. The cuspidality decision problem can be then formulated as follows.

Open problem for Chapter 9

On input $\boldsymbol{f}$ and $\mathcal{R}$ as above, decide whether $\mathcal{R}_{|V_{\mathbb{R}}}$ is cuspidal.

Prior works. Cuspidal robots have been studied mostly for a specific family of robots made with three revolute joints mutually orthogonal [Wen07]. Such robots were shown to be cuspidal if and only if they have at least one cusp point in their workspace [EOW95, SSC+22]. Accordingly, an algorithm can be designed as follows. On input the inverse kinematic polynomial associated with the robot at hand, it counts the number of triple roots of this polynomial. If this number is nonzero, it means that the robot has at least one cusp and is thus cuspidal [Cor05]. We refer to [WC22] for a recent overview on cuspidal robots.

However, for a general robot, no necessary and sufficient condition is known to decide if this robot is cuspidal or not. Thus, no general algorithm has been devised that can decide if a given arbitrary robot is cuspidal or not.

In the whole chapter, we make the following assumption:

(A_{cusp}) the ideal generated by $\boldsymbol{f}$, which we denote by $\langle \boldsymbol{f} \rangle$, is radical and equidimensional of dimension d and $V_{\mathbb{R}}$ is not contained in the singular set of V.

The first two parts of this regularity assumption allow one to conveniently describe the critical locus $\mathcal{K}(\mathcal{R}, V)$ by the mean of minors of the Jacobian matrix $\mathrm{Jac}[\boldsymbol{f}, \mathcal{R}]$. Moreover, the second part ensures that the dimension of the real algebraic set $V_{\mathbb{R}}$ matches the one of V. This can be restated as: the Jacobian matrix $\mathrm{Jac}(\boldsymbol{f})$ has maximal rank $n-d$ in at least one point of $V_{\mathbb{R}}$ and at all points of a Zariski dense subset of V. Note this assumption can be satisfied using algorithms whose complexities are bounded by the one of our main algorithm – see [SYZ21].

Contribution. In this chapter, we design an algorithm for deciding the cuspidality on input $\boldsymbol{f}$ and $\mathcal{R}$ as above, satisfying the above regularity assumption (A_{cusp}). Moreover, when the restriction of the map $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal, the algorithm has the ability to output a witness of cuspidality, i.e. a cuspidal pair and an encoding of a semi-algebraic path that connects them in $V_{\mathbb{R}}$ without meeting $\mathcal{K}(\mathcal{R}, V)$.

We also analyze the bit complexity of this algorithm and prove that cuspidality can be decided in time singly exponential in n, polynomial in the maximum degree of the input polynomials, the integer d and quasi-linear in the maximum bit size of the input coefficients. We refer to Section 3.1 of Chapter 3 for definitions and discussions on (bit) complexity and quantitative bounds associated to polynomials. This leads to the following statement.

Contribution to the open problem

Theorem 9.1.2. *Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\mathcal{R} = (r_1, \ldots, r_d)$ be two sequences of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$, let $V = \boldsymbol{V}(\boldsymbol{f})$ and $V_{\mathbb{R}} = V \cap \mathbb{R}^n$. Let D be the maximum degree of these polynomials and let τ be a bound on the bit size of the coefficients of the input polynomials. Then, under assumption (A_{cusp}), one can decide the cuspidality of the restriction of the map $\mathcal{R}$ to $V_{\mathbb{R}}$ using at most*

$$\widetilde{O}(\tau)\,((s+d)D)^{O(n^2)}$$

bit operations.

To provide an algorithmic solution to the cuspidality decision problem, we apply a semi-algebraic version of Thom's isotopy lemma from [CS92]. This lemma allows us to define regions in which the fibers of $\mathcal{R}$ exhibit the same topological properties, i.e., they are semi-algebraic homeomorphic to each other. For a comprehensive introduction to this advanced theorem in real algebraic geometry, please refer to Section 4.4 in Chapter 4.

These regions are delineated by the shared non-vanishing of polynomials $g_1, \ldots, g_q$, which are computed using two-block real quantifier elimination. Subsequently, finding representatives for each of these regions defined by these polynomials involves computing sample points in the semi-algebraically connected components of the complement of $\boldsymbol{V}(g_1) \cup \cdots \cup \boldsymbol{V}(g_q)$. This process relies on the critical point method, extensively discussed in Section 5.2 of Chapter 5.

We then face the task of deciding the existence of cuspidal pairs within the fibers of these finitely many representatives. This reduces to solving finitely many connectivity queries in a semi-algebraic set. As extensively discussed in previous chapters, this challenge is addressed using roadmap algorithms. These algorithms also rely on advanced critical point methods and are presented more succinctly in Section 5.3 of Chapter 5.

We also addressed a proof of concept by setting up a prototype implementation of this algorithm in the computer algebra system Maple, whose application to two robots are presented in Section 9.3.

Structure of the chapter. Section 9.2 is devoted to the formal description of our algorithm and its proof of correctness. The complexity analysis is completed in the Subsection 9.2.4. Finally, Section 9.3 illustrates how our algorithm runs on a concrete application from robotics.

9.2 Algorithm

In this section, after introducing the subroutines we will use, we present our main algorithm, that is Algorithm 4, and prove its correction, as well as a complexity bound. This algorithm takes as input $\boldsymbol{f}$ and $\mathcal{R}$ as above, satisfying (A_{cusp}) and decides the cuspidality of the restriction of $\mathcal{R}$ to the real solution set $V_{\mathbb{R}} = V \cap \mathbb{R}^n$ where $V = \boldsymbol{V}(\boldsymbol{f})$.

We first introduce some objects and notations. Recall that $\mathcal{K}(\mathcal{R}, V)$ denotes the union of the set of *critical points* of the restriction of $\mathcal{R}$ to V and the set of *singular points* of V. Further, we denote by $\mathcal{S}_{\text{val}}(\mathcal{R}, V)$ the set of *singular values* of the restriction of $\mathcal{R}$ to V, i.e. the image by $\mathcal{R}$ of the set $\mathcal{K}(\mathcal{R}, V)$:

$$\mathcal{S}_{\text{val}}(\mathcal{R}, V) = \mathcal{R}(\mathcal{K}(\mathcal{R}, V)).$$

Under assumption (A_{cusp}), the set $\mathcal{K}(\mathcal{R}, V)$ is the set of common complex solutions to the polynomials in $\boldsymbol{f}$ and the set of minors of size n of the Jacobian matrix $\mathrm{Jac}[\boldsymbol{f}, \mathcal{R}]$ associated to $\boldsymbol{f}, \mathcal{R}$ (see e.g. [SS17, Lemma A.2.]).

The restriction of the map $\mathcal{R}$ to V is said to be proper at a point $\boldsymbol{y} \in \mathbb{C}^d$ if there exists a ball $B \subset \mathbb{C}^d$ containing $\boldsymbol{y}$ such that $\mathcal{R}^{-1}(B) \cap V$ is closed and bounded. The restriction of $\mathcal{R}$ to V is said to be proper if it is proper at every point of $\mathbb{C}^d$.

We denote by $\mathcal{P}_\infty(\mathcal{R}, V)$ be the set of points of $\mathbb{C}^d$ at which $\mathcal{R}$ is *not* proper. According to [Jel99, Theorem 3.8.] it is contained in a proper algebraic set of $\mathbb{C}^d$.

Finally we denote by $\mathcal{A}_{\text{typ}}(\mathcal{R}, V)$ the set of *atypical values* of the restriction of $\mathcal{R}$ to V, that is the union $\mathcal{S}_{\text{val}}(\mathcal{R}, V) \cup \mathcal{P}_\infty(\mathcal{R}, V)$, and let

$$\mathcal{S}_{\text{pec}}(\mathcal{R}, V) = \mathcal{R}^{-1}(\mathcal{A}_{\text{typ}}(\mathcal{R}, V)) \cap V$$

the set of *special points* of the restriction of $\mathcal{R}$ to V that map to atypical values. We denote by $\overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^{z}$ the Zariski closure in $\mathbb{C}^d$ of the set of atypical values.

9.2.1 Subroutines

The algorithm we design in this paper for deciding cuspidality relies on a family of high-level subroutines for solving polynomial systems over the reals with different specifications. These are carefully presented and discussed in Sections 5.2 and 5.3 of Chapter 5.

The first routine SAMPLEPOINTS we use takes as input a polynomial system of equations and s inequalities in $\mathbb{Q}[x_1, \ldots, x_n]$ and returns a zero-dimensional parametrization of at least one point per connected component of the real solution set to the input system. When the input polynomials have degree at most D, this can be done in time singly exponential in n and polynomial in D and s. The specifications of such a procedure are detailed in Theorem 5.2.1 of Chapter 5.

Besides, we will also use a variant SAMPLEPOINTSRATIONAL from [LS22], that takes as input a polynomial system of s inequations and output rational points in at least one point per connected component of the real solution set to the input system. This is done within the same complexity bounds. Again, the specifications can be found in Theorem 5.2.3 of Chapter 5.

Such procedures rely on the critical point method introduced in [GV88] and developed in [SS03a, BPR06, LS22]. A comprehensive overview as well as historical considerations can be found in Section 5.2 of Chapter 5.

The second subroutine ROADMAP we rely on, still takes as input a polynomial system of equations and s inequalities, as well as a zero-dimensional parametrization encoding some query points in the solution set $S \subset \mathbb{R}^n$ to the input system. It then computes an one-dimensional parametrization for a semi-algebraic curve, called a roadmap, which has a non-empty and connected intersection with all connected components of S and contains all the query points. This is done in bit complexity singly exponential in n, polynomial in D and s.

As seen in the previous chapter, the computation of such roadmaps relies on more advanced critical point methods initiated by Canny in [Can88a, Can91, Can93] and continuously improved in [BPR00, SS11, BR14, BRSS14, SS17] as well as in this document. We refer to Subsection 5.3.2 of Chapter 5 for historic discussion of these algorithms.

The third subroutine GRAPHISOTOP takes as input a one-dimensional parametrization encoding an algebraic curve, as well as s inequalities, and a zero-dimensional parametrization encoding some query points on the curve, satisfying the inequalities. It computes a piecewise linear approximation that is isotopy equivalent to the semi-algebraic curve defined by the subset of the input algebraic curve satisfying the input inequalities. Moreover, the vertices of this approximation are in one-to-one correspondence with the input query points. The output of the algorithm also includes a procedure $\text{VERT}_{\mathscr{G}}$ that on input a zero-dimensional parametrization encoding a subset of the query points, output the associated vertices in the approximation. This is done in bit complexity polynomial in the degree of the input curve and the number of query points and linear in s. We refer to Subsection 5.3.3 of Chapter 5 for detailed discussion on this algorithm, and in particular to Theorem 5.3.4 for the precise specifications and complexity bounds.

In addition to the above high-level procedures, we present hereafter basic subroutines that we use to manipulate rational parametrizations, polynomials and graphs. In the following, $\mathscr{P}_\emptyset$ will denote a zero-dimensional parametrization of $\mathbb{R}^n$ encoding the empty set, and $()$ will denote the empty sequence. Besides, given a polynomial sequence $\boldsymbol{h} = (h_i)_{1\leq i\leq \iota}$ we will note $\pm\boldsymbol{h} = (\pm h_i)_{1\leq i\leq \iota}$.

The procedure UNION takes as input two zero-dimensional parametrizations $\mathscr{P}$ and $\mathscr{P}'$ of degree $\delta_{\mathscr{P}}$ and $\delta_{\mathscr{P}'}$ and returns a zero-dimensional parametrization of $Z(\mathscr{P}) \cup Z(\mathscr{P}')$ of degree $\delta_{\mathscr{P}} + \delta_{\mathscr{P}'}$. See [SS17, Lemma J.3.] for a description of this procedure.

The procedures CRIT and ATYPICALVALUES take as input a polynomial map $\mathcal{R}$ and a finite sequence of polynomials $\boldsymbol{h}$. Assuming that $\boldsymbol{h}$ satisfies assumption (A_{cusp}), these two procedures output finite sequences of polynomials whose complex zero-sets are respectively $\mathcal{K}(\mathcal{R}, \boldsymbol{V}(\boldsymbol{h}))$ and a proper subset of $\mathbb{C}^d$ containing $\overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, \boldsymbol{V}(\boldsymbol{h}))}^Z$. We refer to [SS17, Lemma A.2] for a description of CRIT. The latter is obtained using more involved algebraic elimination routine we describe in the Subsection 9.2.4.

Let $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ be a graph and let $v, v' \in \mathcal{V}$ be two vertices. We say that v and v' are connected in $\mathscr{G}$ if there exists a sequence $(v_1, \ldots, v_m)$ of vertices in $\mathcal{V}$ such that for all $1 \leq i < m$,

$$v_1 = v, \quad v_2 = v' \quad \text{and} \quad \{v_i, v_{i+1}\} \in \mathcal{E}.$$

The procedure GRAPHCONNECTED takes as input $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ and (v, v') and outputs `True` if and only if v and v' are connected in $\mathscr{G}$. Else it outputs `False`. This subroutine is classic among graph problems, and can be done using well-know algorithms such as the breadth-first search algorithm [CLRS09, Section 22.2].

9.2.2 Algorithm description

We now turn to the description of our main algorithm as below. It proceeds by computing a zero-dimensional parametrization $\mathscr{P}$ of a set of points that provides cuspidal pairs of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ whenever such a pair exists. In other words, if no cuspidal pair can be found among $Z(\mathscr{P})$, then the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ is not cuspidal.

Hence, to solve our cuspidality problem, it suffices to compute a graph which is isotopy equivalent to a roadmap of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ connecting the points of $Z(\mathscr{P})$ that lie in the same semi-algebraically connected component of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$.

9.2.3 Correctness proof

The correction of Algorithm 4 is stated by the following proposition.

Proposition 9.2.1. *Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\mathcal{R} = (r_1, \ldots, r_d)$ be two sequences of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$, let $V = \boldsymbol{V}(\boldsymbol{f})$ and $V_{\mathbb{R}} = V \cap \mathbb{R}^n$. Then, under assumption (A_{cusp}), the restriction of the map $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal if and only if, with inputs $\boldsymbol{f}$ and $\mathcal{R}$, Algorithm 4 outputs* `True`.

The rest of this section is devoted to prove this correctness statement. We assume by now the assumptions of Proposition 9.2.1 to hold.

Algorithm 4 Cuspidality algorithm

Input: Two sequences $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\mathcal{R} = (r_1, \ldots, r_d)$ of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ that satisfy assumption ($\mathrm{A}_{\mathrm{cusp}}$).

Output: A decision, `True` or `False`, on the cuspidality of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}} = V \cap \mathbb{R}^n$ where $V = \boldsymbol{V}(\boldsymbol{f})$.

$\boldsymbol{g} = (g_1, \ldots, g_p) \leftarrow$ AtypicalValues$(\mathcal{R}, \boldsymbol{f})$;
$\mathcal{Q} \leftarrow$ SamplePointsRational$\left(g_1^2 + \cdots + g_p^2\right)$;
$\mathscr{P} \leftarrow \mathscr{P}_{\emptyset}$;
for $\boldsymbol{q} = (\boldsymbol{q}_1, \ldots, \boldsymbol{q}_d) \in \mathcal{Q}$ **do**
    $\mathcal{R}_{\boldsymbol{q}} \leftarrow (r_1 - \boldsymbol{q}_1, \ldots, r_d - \boldsymbol{q}_d)$;
    $\mathscr{P}_{\boldsymbol{q}} \leftarrow$ SamplePoints$((\boldsymbol{f}, \mathcal{R}_{\boldsymbol{q}}), ())$;
    $\mathscr{P} \leftarrow$ Union$(\mathscr{P}, \mathscr{P}_{\boldsymbol{q}})$;
end for
$\Delta \leftarrow$ Crit$(\mathcal{R}, \boldsymbol{f})$;
$\mathscr{R} \leftarrow$ Roadmap$(\boldsymbol{f}, \pm\Delta, \mathscr{P})$;
$\left(\mathscr{G} = (\mathcal{V}, \mathcal{E}), \mathrm{Vert}_{\mathscr{G}}\right) \leftarrow$ GraphIsotop$(\mathscr{R}, \pm\Delta, \mathscr{P})$;
for $\boldsymbol{q} \in \mathcal{Q}$ **do**
    $\mathcal{V}_{\boldsymbol{q}} \leftarrow \mathrm{Vert}_{\mathscr{G}}(\mathscr{P}_{\boldsymbol{q}})$;
    for $(\boldsymbol{v}_1, \boldsymbol{v}_2) \in \mathcal{V}_{\boldsymbol{q}}^2$ **do**
        if GraphConnected$((\boldsymbol{v}_1, \boldsymbol{v}_2), \mathscr{G})$ and $\boldsymbol{v}_1 \neq \boldsymbol{v}_2$ **then**
            return `True`;
        end if
    end for
end for
return `False`.

Note that fibers of the restriction of $\mathcal{R}$ to V are generically finite by [Sha13, Theorem 1.25], and in particular by [SS17, Lemma A.2], for every $\boldsymbol{p} \in \mathbb{C}^d - \mathcal{A}_{\mathrm{typ}}(\mathcal{R}, V)$, the fiber $\mathcal{R}^{-1}(\boldsymbol{p}) \cap V$ is finite.

We start by an elementary lemma establishing that two distinct "regular" points of $\mathcal{R}$ on $V_{\mathbb{R}}$, having the same image through $\mathcal{R}$, must be separated by $\mathcal{S}_{\mathrm{pec}}(\mathcal{R}, V)$.

Lemma 9.2.2. *Let $\boldsymbol{y}$ and $\boldsymbol{y}'$ be two distinct points of $V_{\mathbb{R}} - \mathcal{S}_{\mathrm{pec}}(\mathcal{R}, V)$ such that $\mathcal{R}(\boldsymbol{y}) = \mathcal{R}(\boldsymbol{y}')$. Then $\boldsymbol{y}$ and $\boldsymbol{y}'$ belong to distinct semi-algebraically connected components of $V_{\mathbb{R}} - \mathcal{S}_{\mathrm{pec}}(\mathcal{R}, V)$.*

Proof. Let us proceed by contradiction and suppose there exists a path $\gamma\colon [0,1] \to V_{\mathbb{R}} - \mathcal{S}_{\mathrm{pec}}(\mathcal{R}, V)$ such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(1) = \boldsymbol{y}'$. By definition, $\mathcal{R}(\gamma([0,1])) \subset \mathbb{R}^d - \overline{\mathcal{A}_{\mathrm{typ}}(\mathcal{R}, V)}^z$

Let C be the semi-algebraically connected component of $\mathbb{R}^d - \overline{\mathcal{A}_{\mathrm{typ}}(\mathcal{R}, V)}^z$ that contains $\mathcal{R}(\gamma([0,1]))$. According to Theorem 4.4.17, there exists a homeomorphism

$$\begin{array}{rccccc} \Psi\colon & \mathcal{R}^{-1}(C) \cap V_{\mathbb{R}} & \to & C & \times & \mathcal{R}^{-1}(\mathcal{R}(\boldsymbol{y})) \cap V_{\mathbb{R}} \\ & \boldsymbol{z} & \mapsto & (\mathcal{R}(\boldsymbol{z}) & , & \Psi_0(\boldsymbol{z}) \quad) \end{array},$$

such that the image of any semi-algebraically connected component of $\mathcal{R}^{-1}(C) \cap V_{\mathbb{R}}$, through Ψ_0, is a singleton. Since $\gamma([0,1])$ is contained in $\mathcal{R}^{-1}(C) \cap V_{\mathbb{R}}$, then $\boldsymbol{y}$ and $\boldsymbol{y}'$ belong to the same semi-algebraically connected component of $\mathcal{R}^{-1}(C) \cap V_{\mathbb{R}}$, so that $\Psi_0(\boldsymbol{y}) = \Psi_0(\boldsymbol{y}')$. Since $\mathcal{R}(\boldsymbol{y}) = \mathcal{R}(\boldsymbol{y}')$, then $\boldsymbol{y} = \boldsymbol{y}'$ by injectivity of Ψ. This contradicts the assumption $\boldsymbol{y} \neq \boldsymbol{y}'$ and proves the Lemma. □

In other words, any potential cuspidal pair must contain points from different semi-algebraically connected components of the complement of $\mathcal{S}_{\text{pec}}(\mathcal{R}, V)$ in $V_{\mathbb{R}}$. This leads naturally to the following construction that we call here a *cuspidality graph*.

Definition 9.2.3. Let $\mathcal{V} \subset \mathbb{R}^n$ and $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a graph. Then we say that $\mathcal{G}$ is a *cuspidality graph* of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ if the following holds.

(i) The set $\mathcal{V}$ is contained in $V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$ and intersects every semi-algebraically connected component of $V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$.

(ii) Let $\boldsymbol{v}, \boldsymbol{v}' \in \mathcal{V}$ be such that $\mathcal{R}(\boldsymbol{v}) = \mathcal{R}(\boldsymbol{v}')$. Then $\boldsymbol{v}$ and $\boldsymbol{v}'$ are semi-algebraically connected in $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ if and only if they are in $\mathcal{G}$.

(iii) Let $\boldsymbol{v} \in \mathcal{V}$, then $\mathcal{R}^{-1}\left(\mathcal{R}(\boldsymbol{v})\right) \cap V_{\mathbb{R}} \subset \mathcal{V}$.

Remark that it is straightforward that such a graph exists, and, under assumption (A_{cusp}), it can be supposed to be finite since $V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$ has finitely many semi-algebraically connected components and $\mathcal{R}$ has finite fibers out of $\mathcal{A}_{\text{typ}}(\mathcal{R}, V)$.

Then the following result reduces the problem of deciding the cuspidality of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ to a connectivity problem on a finite graph.

Lemma 9.2.4. *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a cuspidality graph of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. Then the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal if and only if there exist two distinct vertices $\boldsymbol{v}, \boldsymbol{v}' \in \mathcal{V}$, connected in $\mathcal{G}$, and such that $\mathcal{R}(\boldsymbol{v}) = \mathcal{R}(\boldsymbol{v}')$.*

Proof. If such points $\boldsymbol{v}$ and $\boldsymbol{v}'$ exist, they form a cuspidal pair of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$, so that this map is cuspidal.

Conversely, suppose that the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal so that there exist two distinct points $\boldsymbol{y}$ and $\boldsymbol{y}'$ in $V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$ having the same image through $\mathcal{R}$ and that belong to the same semi-algebraically connected component C of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$. Then, by Lemma 9.2.2, there exist two distinct semi-algebraically connected components H and H' of $V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$ such that $\boldsymbol{y} \in H$ and $\boldsymbol{y}' \in H'$. Remark that both H and H' are contained in C since H and H' are two semi-algebraically connected subsets of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ that have a non-empty intersection with C.

By the first item of Definition 9.2.3, $\mathcal{V} \cap H$ is not empty. Then let $\boldsymbol{v} \in \mathcal{V} \cap H$, one has $\boldsymbol{v} \in C$ by the above remark. Hence, by the second item of Definition 9.2.3, one only need to prove the existence of $\boldsymbol{v}' \in \mathcal{V} \cap H'$ such that $\mathcal{R}(\boldsymbol{v}) = \mathcal{R}(\boldsymbol{v}')$.

Since H is semi-algebraically connected, there exists a path $\gamma\colon [0,1] \to H$ such that $\gamma(0) = \boldsymbol{y}$ and $\gamma(1) = \boldsymbol{v}$. Recalling that $H \subset V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$, then

$$\mathcal{R}(\gamma([0,1]) \cap \mathcal{A}_{\text{typ}}(\mathcal{R}, V) = \emptyset.$$

Let T be the semi-algebraically connected component of $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z$ that contains $\mathcal{R}(\gamma([0,1]))$. According to Theorem 4.4.17, there exists a homeomorphism

$$\begin{array}{rccccc} \Psi\colon & \mathcal{R}^{-1}(T) \cap V_{\mathbb{R}} & \to & T & \times & \mathcal{R}^{-1}(\mathcal{R}(\boldsymbol{y})) \cap V_{\mathbb{R}} \\ & \boldsymbol{z} & \mapsto & (\mathcal{R}(\boldsymbol{z}) & , & \Psi_0(\boldsymbol{z}) \quad) \end{array},$$

such that the image of any semi-algebraically connected component of $\mathcal{R}^{-1}(T) \cap V_{\mathbb{R}}$, through Ψ_0, is a singleton. In particular since $\boldsymbol{v} \in H$, then $\Psi(\boldsymbol{v}) = (\mathcal{R}(\boldsymbol{v}), \Psi_0(\boldsymbol{y}))$.

Let $\boldsymbol{v}' = \Psi^{-1}(\mathcal{R}(\boldsymbol{v}), \Psi_0(\boldsymbol{y}'))$. By definition, $\mathcal{R}(\boldsymbol{v}') = \mathcal{R}(\boldsymbol{v})$, so that by the last item of Definition 9.2.3, $\boldsymbol{v}' \in \mathcal{V}$. Finally, remark that the path

$$\begin{array}{rccc} \gamma'\colon & [0,1] & \to & \mathcal{R}^{-1}(T) \cap V_{\mathbb{R}} \\ & t & \mapsto & \Psi^{-1}(\mathcal{R}(\gamma(t)), \Psi_0(\boldsymbol{y}')) \end{array},$$

is defined for all $t \in [0,1]$ and $\gamma'(0) = \boldsymbol{y}' \in H'$. Hence $\boldsymbol{v}' = \gamma'(1) \in H'$ since H' is semi-algebraically connected.

In conclusion, there exist $\boldsymbol{v}$ and $\boldsymbol{v}'$ in $\mathcal{V}$ having the same image through $\mathcal{R}$, such that $\boldsymbol{v} \neq \boldsymbol{v}'$ since $H \cap H' = \emptyset$. Moreover, since $H \cup H' \subset C$, then by the second point of Definition 9.2.3, $\boldsymbol{v}$ and $\boldsymbol{v}'$ are connected in $\mathscr{G}$. The equivalence is established. □

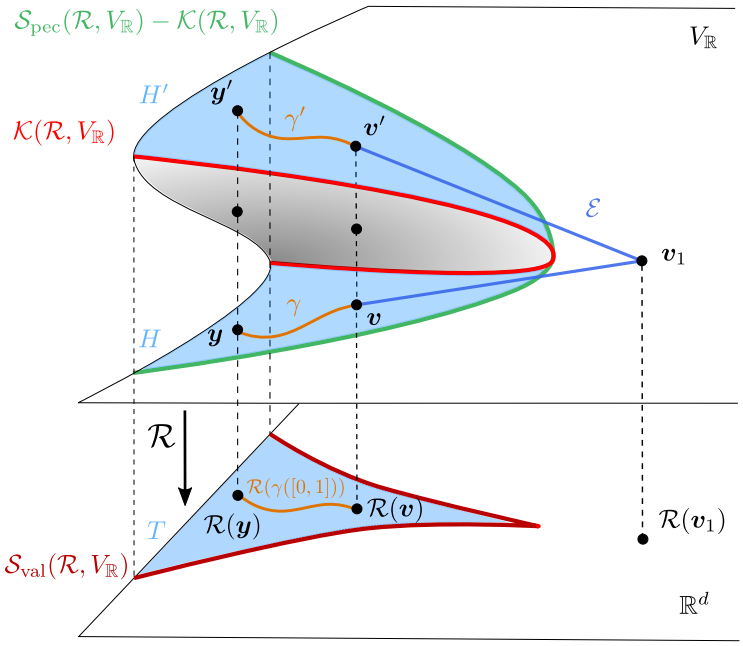


Figure 9.1. Illustration with $n = 3$ and $d = 2$ of the proof of Lemma 9.2.4 where $\mathcal{R}$ is the projection of the surface $V_{\mathbb{R}} \subset \mathbb{R}^n$ drawn above the plane $\mathbb{R}^d$ on the figure. Given a cuspidality graph $\mathcal{G} = \big(\{\boldsymbol{v}, \boldsymbol{v}', \boldsymbol{v}_1\},\ \mathcal{E}\big)$ and a cuspidal pair formed by $\boldsymbol{y}$ and $\boldsymbol{y}'$, one finds, using Theorem 4.4.17, two vertices $\boldsymbol{v}$ and $\boldsymbol{v}'$ that satisfy the statement.

Finally, we prove that taking the inverse image of a specific sample set of points is enough to satisfy the first item of Definition 9.2.3.

Lemma 9.2.5. *Let $\mathcal{Q} \subset \mathbb{R}^d$ that intersects every semi-algebraically connected component of $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z$ and let $\mathcal{P} = V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\mathcal{Q})$. Then $\mathcal{P}$ intersects every semi-algebraically connected component of $V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$.*

Proof. Let H be a semi-algebraically connected component of $V_{\mathbb{R}} - \mathcal{S}_{\text{pec}}(\mathcal{R}, V)$ we need to prove that $H \cap \mathcal{P}$ is not empty. Let $\boldsymbol{y} \in H$, and let T be the semi-algebraically connected component of $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z$ that contains $\mathcal{R}(\boldsymbol{y})$. By assumption, there exists $\boldsymbol{p} \in \mathcal{P} \cap T$. Let $\sigma\colon [0,1] \to H$ be a path such that $\sigma(0) = \mathcal{R}(\boldsymbol{y})$ and $\sigma(1) = \boldsymbol{p}$. Since σ lie in $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z$, the path $\sigma([0,1])$ is still contained in T. Then according to Theorem 4.4.17, there exists a homeomorphism

$$\begin{array}{rccccc} \Psi\colon & \mathcal{R}^{-1}(T) \cap V_{\mathbb{R}} & \to & T & \times & \mathcal{R}^{-1}(\mathcal{R}(\boldsymbol{y})) \cap V_{\mathbb{R}} \\ & \boldsymbol{z} & \mapsto & (\mathcal{R}(\boldsymbol{z}) & , & \Psi_0(\boldsymbol{z}) \quad) \end{array},$$

such that the image of any semi-algebraically connected component of $\mathcal{R}^{-1}(T) \cap V_{\mathbb{R}}$, through Ψ_0, is a singleton.

Let $\gamma\colon t \in [0,1] \mapsto \Psi^{-1}(\sigma(t), \Psi_0(\boldsymbol{y}))$, it satisfies $\gamma(0) = \boldsymbol{y} \in H$. Since H is semi-algebraically connected, then $\boldsymbol{v} = \gamma(1)$ belongs to H. Moreover, since $\sigma(1) = \boldsymbol{p}$, then by uniqueness $\mathcal{R}(\boldsymbol{v}) = \boldsymbol{p}$ so that $\boldsymbol{v} \in \mathcal{P}$ and $H \cap \mathcal{P}$ is not empty as claimed. □

We can now proceed to prove the correction of Algorithm 4.

Proof of Proposition 9.2.1. Let $\boldsymbol{g}, \mathcal{Q}, \mathscr{P}, \Delta, \mathscr{R}$ and $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ be the data obtained in the execution of Algorithm 4. Let us prove that we can derive from $\mathscr{G}$ a graph $\widetilde{\mathscr{G}}$ that is a cuspidal graph of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. Then, using this fact and Lemma 9.2.4, we prove that the tests on $\mathscr{G}$ that are operated in Algorithm 4, are enough to conclude on the cuspidality of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. Remark that according to the description of the subroutines AtypicalValues and Crit, the following holds

$$\overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z = \boldsymbol{V}(\boldsymbol{g}), \quad V \cap \mathcal{R}^{-1}(\mathcal{Q}) = \bigcup_{\boldsymbol{q} \in \mathcal{Q}} \boldsymbol{V}(\boldsymbol{f}, \mathcal{R} - \boldsymbol{q})$$
$$\text{and} \quad \mathcal{K}(\mathcal{R}, V) = \boldsymbol{V}(\boldsymbol{f}, \Delta).$$

Then, according to the first item of Theorem 5.3.4 there exists an isotopy $\mathcal{H}$ of $\mathbb{R}^n$ such that $\mathcal{H}(\mathscr{C}_{\mathscr{G}}, 1) = Z(\mathscr{R}) \cap \mathbb{R}^n - \mathcal{K}(\mathcal{R}, V)$ where $\mathscr{C}_{\mathscr{G}}$ is the piecewise linear curve of $\mathbb{R}^n$ associated to $\mathscr{G}$. We denote further $\boldsymbol{y} \mapsto \mathcal{H}(\boldsymbol{y}, 1)$ by $\mathcal{H}_1$. Let $\widetilde{\mathcal{V}} = \mathcal{H}_1(\mathcal{V})$ and

$$\widetilde{\mathcal{E}} = \{\{\mathcal{H}_1(\boldsymbol{v}), \mathcal{H}_1(\boldsymbol{v}')\} \mid \{\boldsymbol{v}, \boldsymbol{v}'\} \in \mathcal{E}\}.$$

Let $\widetilde{\mathscr{G}} = (\widetilde{\mathcal{V}}, \widetilde{\mathcal{E}})$ be the graph thus defined. According to the second item of Theorem 5.3.4 the equality $\widetilde{\mathcal{V}} = Z(\mathscr{P}) \cap \mathbb{R}^n$ holds since

$$Z(\mathscr{P}) \subset \mathcal{R}^{-1}(\mathcal{Q}) \quad \text{and} \quad \mathcal{Q} \cap \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z = \emptyset.$$

Moreover the following map is a bijection

$$\begin{array}{rccc} \mathcal{H}_1 \times \mathcal{H}_1 : & \mathcal{E} & \to & \widetilde{\mathcal{E}} \\ & \{\boldsymbol{v}, \boldsymbol{v}'\} & \mapsto & \{\mathcal{H}_1(\boldsymbol{v}), \mathcal{H}_1(\boldsymbol{v}')\} \end{array}.$$

Let us show that $\widetilde{\mathscr{G}}$ is a cuspidality graph of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$.

By Theorem 5.2.3, the finite set $\mathcal{Q} \subset \mathbb{R}^d$ intersects every semi-algebraically connected component of $\mathbb{R}^d - \overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z$. Then by Lemma 9.2.5, every semi-algebraically connected component of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ has a non-empty intersection with $V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\mathcal{Q})$. As $\mathcal{Q}$ is finite and does not intersect $\mathcal{S}_{\text{val}}(\mathcal{R}, V)$, the set $V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\mathcal{Q})$ is a finite union of the sets $V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\boldsymbol{q})$, which are finite by [SS17, Lemma A.2]. Hence $V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\mathcal{Q})$ is finite so that its semi-algebraically connected components are reduced to its points. Hence by Theorem 5.2.1, $V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\mathcal{Q})$ is equal to $Z(\mathscr{P}) \cap \mathbb{R}^n$ which is itself equal to $\widetilde{\mathcal{V}}$. Therefore, $\widetilde{\mathscr{G}}$ satisfies the first item of Definition 9.2.3.

Let $\boldsymbol{v}, \boldsymbol{v}' \in \widetilde{\mathcal{V}}$. According to Theorem 5.3.3, since $\boldsymbol{v}$ and $\boldsymbol{v}'$ are in $Z(\mathscr{P}) \cap \mathbb{R}^n$, they are connected in $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ if and only if they are connected in

$$Z(\mathscr{R}) \cap \mathbb{R}^n - \mathcal{K}(\mathcal{R}, V).$$

However by Theorem 5.3.4, since $Z(\mathscr{P}) \subset Z(\mathscr{R})$, then $\boldsymbol{v}$ and $\boldsymbol{v}'$ are connected in $Z(\mathscr{R}) \cap \mathbb{R}^n - \mathcal{K}(\mathcal{R}, V)$ if and only if $\mathcal{H}_1^{-1}(\boldsymbol{v})$ and $\mathcal{H}_1^{-1}(\boldsymbol{v}')$ are connected in $\mathscr{G}$. But the latter statement is equivalent to saying that $\boldsymbol{v}$ and $\boldsymbol{v}'$ are connected in $\widetilde{\mathscr{G}}$ since $\mathcal{H}_1 \times \mathcal{H}_1$ is a bijection. Therefore, $\widetilde{\mathscr{G}}$ satisfies the second item of Definition 9.2.3.

Finally $\widetilde{\mathscr{G}}$ satisfies the last item of Definition 9.2.3 since for all $\boldsymbol{v} \in \widetilde{\mathcal{V}}$,

$$V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\mathcal{R}(\boldsymbol{v})) \subset V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\mathcal{Q}) = Z(\mathscr{P}) \cap \mathbb{R}^n = \widetilde{\mathcal{V}}.$$

In conclusion, $\widetilde{\mathscr{G}}$ is a cuspidal graph of the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$. Let us prove now that, the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal if and only if, on inputs $\boldsymbol{f}$ and $\mathcal{R}$, Algorithm 4 outputs `True`.

If Algorithm 4 outputs `True`, there exists $\boldsymbol{q} \in \mathcal{Q}$ and $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{V}_{\boldsymbol{q}}$ that are connected in $\mathscr{G}$. Let $\boldsymbol{v} = \mathcal{H}_1(\boldsymbol{v}_1)$ and $\boldsymbol{v}' = \mathcal{H}_1(\boldsymbol{v}_2)$, then by definition of $\widetilde{\mathcal{V}}$, $\boldsymbol{v}$ and $\boldsymbol{v}'$ are in $\widetilde{\mathcal{V}}$. According to Theorem 5.3.4 and the definition of the procedure $\textsc{Vert}_{\mathscr{G}}$, since $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{V}_{\boldsymbol{q}}$, then $\mathcal{R}(\boldsymbol{v}) = \mathcal{R}(\boldsymbol{v}') = \boldsymbol{q}$. Besides, by definition of $\widetilde{\mathcal{E}}$, $\boldsymbol{v}$ and $\boldsymbol{v}'$ are connected in $\widetilde{\mathscr{G}}$ so that by Lemma 9.2.4, the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal.

Conversely, suppose that the restriction of $\mathcal{R}$ to $V_{\mathbb{R}}$ is cuspidal. Then by Lemma 9.2.4 there exist two distinct points $\boldsymbol{v}, \boldsymbol{v}' \in \widetilde{\mathcal{V}}$, connected in $\widetilde{\mathscr{G}}$, such that $\mathcal{R}(\boldsymbol{v}) = \mathcal{R}(\boldsymbol{v}')$. Since $\mathcal{R}(\widetilde{\mathcal{V}}) \subset \mathcal{Q}$, there exists $\boldsymbol{q} \in \mathcal{Q}$ such that $\boldsymbol{q} = \mathcal{R}(\boldsymbol{v}) = \mathcal{R}(\boldsymbol{v}')$. For such a point $\boldsymbol{q}$ let $\mathscr{P}_{\boldsymbol{q}}$ and $\mathcal{V}_{\boldsymbol{q}}$ computed in Algorithm 4 at respectively step 2 and step 13. Recall that $\mathscr{P}_{\boldsymbol{q}}$ is the zero-dimensional parametrization encoding $V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\boldsymbol{q})$ and $\mathcal{V}_{\boldsymbol{q}}$ the subset of vertices of $\mathcal{V}$, that are associated to the points of $V_{\mathbb{R}} \cap \mathcal{R}^{-1}(\boldsymbol{q})$ through $\mathcal{H}_1$. Hence according to

Theorem 5.3.4 and the description of $\text{VERT}_{\mathscr{G}}$, $\mathcal{H}_1^{-1}(\boldsymbol{v})$ and $\mathcal{H}_1^{-1}(\boldsymbol{v}')$ are distinct and belong to $\mathcal{V}_{\boldsymbol{q}}$. Since $\boldsymbol{v}$ and $\boldsymbol{v}'$ are connected in $\widetilde{\mathscr{G}}$, then so are

$$\mathcal{H}_1^{-1}(\boldsymbol{v}) \quad \text{and} \quad \mathcal{H}_1^{-1}(\boldsymbol{v}')$$

in $\mathscr{G}$. Hence $\text{GRAPHCONNECTED}\big((\mathcal{H}_1^{-1}(\boldsymbol{v}), \mathcal{H}_1^{-1}(\boldsymbol{v}')), \mathcal{G}\big)$ will outputs `True` so that Algorithm 4 outputs `True`. □

9.2.4 Complexity analysis

This section is devoted to the proof of the following proposition. Together with Proposition 9.2.1, it establishes Theorem 9.1.2.

Proposition 9.2.6. *Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\mathcal{R} = (r_1, \ldots, r_d)$ be two sequences of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ and D be the maximum degree of these polynomials. Let τ be a bound on the bit size of the coefficients of the input polynomials. Then, under assumption (A_{cusp}), with inputs $\boldsymbol{f}$ and $\mathcal{R}$, the execution of Algorithm 4 terminates using at most*

$$\tau^\star((s+d)D)^{O(n^2)}$$

bit operations.

Proof. Fix $\boldsymbol{f}$ and $\mathcal{R}$, we note $V = \boldsymbol{V}(\boldsymbol{f})$ and $V_{\mathbb{R}} = V \cap \mathbb{R}^n$. Assume that assumption (A_{cusp}) holds that is that V is equidimensional of dimension d. Let δ and μ be the maximum degree of the polynomials in respectively $\boldsymbol{f}$ and $\mathcal{R}$ so that $D = \max\{\delta, \mu\}$, and let τ be a bound on the bitsize of the input coefficients. We proceed by considering each step of Algorithm 4.

Step 1. The first step of the algorithm consists in computing polynomials whose complex zero-set is the Zariski closure of the set of atypical values. According to [JK05, Theorem 4.1.], the set $\mathcal{A}_{\text{typ}}(\mathcal{R}, V)$ is contained in an hypersurface of $\mathbb{C}^d$ degree bounded by

$$\delta^{n-d}\left(n\delta + d(\mu - \delta)\right)^d.$$

Then, the polynomials in the finite sequence $\boldsymbol{g}$, given by the call to ATYPICALVALUES, have degree bounded by $n^d D^n$. To compute a polynomial defining them, we rely on the quantifier elimination algorithm in [BPR06, Chap. 14]. Precisely, the set of non-properness can be defined naturally by a quantified formula expressing that y is in the set of non-properness if and only if for any $r > 0$ there exists $\epsilon > 0$ such that for any $y' \in \mathbb{R}^d$ and $x' \in \mathcal{R}^{-1}(\boldsymbol{y}') \cap V_{\mathbb{R}}$, $\|y - y'\|^2 < \epsilon$ implies that $\|x'\| > r$. There is one alternate of quantifiers with blocks of quantified variables of lengths $1, n + d + 1$. Solving such a quantifier elimination problem is done using $\tau(sD)^{O((n+d)d)} \subset \tau(sD)^{O(nd)}$ bit operations by [BPR06, Theorem 14.22] and it outputs $(sD)^{O(nd)}$ polynomials of degree in $D^{O(n)}$. Computing a polynomial encoding the critical values is done still using quantifier elimination but in an even simpler way: these are the projections of the values of $\mathcal{R}$ taken at the system $f_1, \ldots, f_s$ and the $n - d + 1$ minors of the Jacobian matrix associated to $\boldsymbol{f}, \mathcal{R}$.

Step 2. Since $\overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^{Z} = \boldsymbol{V}(\boldsymbol{g})$, then by Theorem 5.2.3, the call to SAMPLEPOINTSRATIONAL outputs a set $\mathcal{Q}$ of cardinality N bounded by $n^{O(d^2)}D^{O(nd)}$, using at most

$$\tau n^{O(d^2)}D^{O(nd)}$$

bit operations. We denote further $\mathcal{Q} = \{\boldsymbol{q}^1, \ldots, \boldsymbol{q}^N\}$.

Steps 4-8. Suppose that in the **for** loop, we consider successively $\boldsymbol{q}^1$ to $\boldsymbol{q}^N$. Let $0 \leq i \leq N$, and let $\delta_{\mathscr{P},i}$ be the degree of $\mathscr{P}$ at the end of the i-th iteration. By Theorem 5.2.1, for every $1 \leq i \leq N$, at step 6, SAMPLEPOINTS$((\boldsymbol{f}, \mathcal{R} - \boldsymbol{q}_i), 0)$ returns a zero-dimensional parametrization of degree bounded by $D^{O(n)}$. Then, we have

$$\delta_{\mathscr{P},i} \leq \delta_{\mathscr{P},i-1} + D^{O(n)}.$$

Since $\delta_{\mathscr{P},0} = 0$ then $\delta_{\mathscr{P},N}$ is bounded by $n^{O(d^2)}D^{O(nd)}$ since N is bounded by $n^{O(d^2)}D^{O(nd)}$. Since the input has constant size, each call of SAMPLEPOINTS, at step 6, costs at most $\tau D^{O(n)}$ bit operations. Besides, since the $\delta_{\mathscr{P},i}$'s are in increasing order, according to [SS17, Lemma J.4.], each call to UNION, at step 7, is polynomial in $\delta_{\mathscr{P},N}$.

Therefore, at step 8, $\mathscr{P}$ has degree $\delta_{\mathscr{P}}$ bounded by $n^{O(d^2)}D^{O(nd)}$ and the total loop execution is using at most $\tau n^{O(d^2)}D^{O(nd)}$ bit operations.

Step 9. Next, CRIT$(\mathcal{R}, \boldsymbol{f})$ returns a sequence of polynomials Δ by computing the determinant of all the $n \times n$ submatrices $\text{Jac}[\boldsymbol{f}, \mathcal{R}]$ according to [SS17, Lemma A.2.]. One sees that there are $\binom{s+d}{n}$ such minors, which have degrees bounded by $n(D-1)$.

Step 10. According to the previous step, and by Theorem 5.3.3, ROADMAP$(\boldsymbol{f}, \pm\Delta, \mathscr{P})$ returns a one-dimensional rational parametrization $\mathscr{R}$ using at most

$$\tau^\star \binom{s+d}{n}^{O(n)} n^{O(d^2)}D^{O(nd)}(nD)^{O(n^2)}$$

bit operations which is then bounded by $\tau^\star((s+d)D)^{O(n^2)}$. Moreover the degree of $\mathscr{R}$ is bounded by $((s+d)D)^{O(n^2)}$.

Step 11. According to the previous step, and by Theorem 5.3.4, the call to GRAPHISOTOP, with input $(\boldsymbol{f}, \pm\Delta, \mathscr{P})$, costs at most

$$\tau^\star((s+d)D)^{O(n^2)}$$

bit operations.

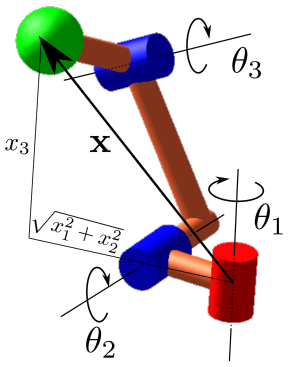
Steps 12-19. At each iteration, the call to VERT$_{\mathscr{G}}$ at step 13 requires a number of operations which is polynomial in $\delta_{\mathscr{P}}$. Besides the procedure GRAPHCONNECTED, who has bit complexity linear in $\delta_{\mathscr{P}}$ is called at most N times in the **for** loop of steps 14-18. Hence, the **for** loop of steps 12-19 requires at most $n^{O(d^2)}D^{O(nd)}$ bit operations.

In conclusion the whole execution of Algorithm 4 uses at most $\tau^\star((s+d)D)^{O(n^2)}$ bit operations, which proves the proposition. □

9.3 Two examples: Orthogonal 3R serial robots

The cuspidal behaviour of 3R serial robots has been analyzed extensively in the past [EOW95, WEO96]. In this section, we present two examples of orthogonal 3R serial robots in order to put forth the application of the algorithm. Recall that such robots are modeled as a map that maps the joint angles of the robot to the position of the end-effector. The joint angles belong to the so-called the joint space, while the set of the positions of the end-effector is called the workspace. We refer to Subsection 1.1.2 of Chapter 1 for a quick introduction to robotics.

Both robots considered in this section are orthogonal 3R serial robots like the one depicted in the opposite figure. Such a robot is defined by its D-H parameters (see [HD64, SSC+22]), that is the data of lengths $d = (d_1, d_2, d_3)$ and $a = (a_1, a_2, a_3)$ and angles, fixed here as $\alpha = (\pi/2, -\pi/2, 0)$.



The first robot is defined by $d = (0, 1, 0)$ and $a = (1, 2, 3/2)$ and is similar to the one discussed in [EOW95] and is *known to be cuspidal*. From [SSC+22], the robot can be associated to this kinematic map,

$$\begin{array}{rccc} \mathcal{K}: & \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ & \boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3) & \longmapsto & \big(x_1(\boldsymbol{\theta}), x_2(\boldsymbol{\theta}), x_3(\boldsymbol{\theta})\big) \end{array}$$

where for all $(\theta_1, \theta_2, \theta_3) \in \mathbb{R}^3$,

$$\begin{aligned} x_1(\theta_1, \theta_2, \theta_3) &= \frac{1}{2} c_1 c_2 (3c_3 + 4) - \frac{1}{2} s_1 (3s_3 + 2) + c_1 \\ x_2(\theta_1, \theta_2, \theta_3) &= \frac{1}{2} s_1 c_2 (3c_3 + 4) + \frac{1}{2} c_1 (3s_3 + 2) + s_1 \\ x_3(\theta_1, \theta_2, \theta_3) &= -\frac{1}{2} s_2 (3c_3 + 4) \end{aligned}$$

and for $i \in \{1, 2, 3\}$, $c_i = \cos(\theta_i)$ and $s_i = \sin(\theta_i)$.

Besides, the second robot is obtained from the first one by varying the lengths: $d = (0, 13/10, 0)$ and $a = (3, 11/10, 3/2)$, and we show that it is not cuspidal. Note that, according to [SSC+22], this non-cuspidal nature can also be proved more directly. Similarly, we consider its kinematic map

$$\begin{array}{rccc} \widetilde{\mathcal{K}}: & \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ & \boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3) & \longmapsto & \big(\widetilde{x}_1(\boldsymbol{\theta}), \widetilde{x}_2(\boldsymbol{\theta}), \widetilde{x}_3(\boldsymbol{\theta})\big) \end{array}$$

where for all $(\theta_1, \theta_2, \theta_3) \in \mathbb{R}^3$,

$$\begin{aligned} \widetilde{x}_1(\theta_1, \theta_2, \theta_3) &= \frac{1}{10} c_1 c_2 (15c_3 + 11) - \frac{1}{10} s_1 (15s_3 + 13) + 3c_1 \\ \widetilde{x}_2(\theta_1, \theta_2, \theta_3) &= \frac{1}{10} s_1 c_2 (15c_3 + 11) + \frac{1}{10} c_1 (15s_3 + 13) + 3s_1 \\ \widetilde{x}_3(\theta_1, \theta_2, \theta_3) &= -\frac{1}{10} s_2 (15c_3 + 11). \end{aligned}$$

The singular postures of the first (resp. second) robot are the points $(\theta_1, \theta_2, \theta_3) \in \mathbb{R}^3$ where the determinant of the Jacobian matrix $\mathrm{Jac}\,\mathcal{K}$ of $\mathcal{K}$ (resp. $\mathrm{Jac}\,\widetilde{\mathcal{K}}$ of $\widetilde{\mathcal{K}}$), vanishes. Let $\boldsymbol{f} = (f_1, f_2, f_3)$ and $\mathcal{R} = (r_1, r_2, r_3)$ (resp. $\widetilde{\mathcal{R}} = (\widetilde{r}_1, \widetilde{r}_2, \widetilde{r}_3)$) be sequences of polynomials in $\mathbb{Q}[c_1, s_1, c_2, s_2, c_3, s_3]$ where for all $i \in \{1, 2, 3\}$

$$f_i = c_i^2 + s_i^2 - 1 \quad \text{and} \quad r_i = x_i(\theta_1, \theta_2, \theta_3) \quad \big(\text{resp. } \widetilde{r}_i = \widetilde{x}_i(\theta_1, \theta_2, \theta_3)\big).$$

Then, the points $(\theta_1, \theta_2, \theta_3) \in \mathbb{R}^3$ annihilating $\det(\mathrm{Jac}\,\mathcal{K})$ (resp. $\det(\mathrm{Jac}\,\widetilde{\mathcal{K}})$) are exactly the points of $\mathbb{R}^3$ such that $(c_1, s_1, c_2, s_2, c_3, s_3) \in V_{\mathbb{R}}$ and the matrix $\mathrm{Jac}[\boldsymbol{f}, \mathcal{R}]$ (resp. $\mathrm{Jac}[\boldsymbol{f}, \widetilde{\mathcal{R}}]$) has not full rank. Since $\boldsymbol{f}$ satisfies assumption ($\mathrm{A}_{\mathrm{cusp}}$), the latter points are exactly the points of $\mathcal{K}(\mathcal{R}, \boldsymbol{V}(\boldsymbol{f})) \cap \mathbb{R}^n$ (resp. $\mathcal{K}(\widetilde{\mathcal{R}}, \boldsymbol{V}(\boldsymbol{f})) \cap \mathbb{R}^n$).

Therefore, the first (resp. second) robot can be also modeled as the restriction of the polynomial map associated to $\mathcal{R}$ (resp. $\widetilde{\mathcal{R}}$) to the real algebraic set $V_{\mathbb{R}} = V \cap \mathbb{R}^n$, where $V = \boldsymbol{V}(\boldsymbol{f})$, and deciding the cuspidality of this map amounts to decide the cuspidality of the robot. Since assumption ($\mathrm{A}_{\mathrm{cusp}}$) is satisfied, we can apply Algorithm 4 to $\boldsymbol{f}$ and $\mathcal{R}$ (resp. $\widetilde{\mathcal{R}}$) and make this decision.

The set $\mathcal{K}(\mathcal{R}, V)$ (resp $\mathcal{K}(\widetilde{\mathcal{R}}, V)$) is defined by the vanishing of the following polynomial

$$\Delta = 6(3c_3 + 4)(c_2c_3 - 2c_2s_3 - s_3)$$
$$\Big(\text{resp. } \widetilde{\Delta} = 3(15c_3 + 11)(13c_2c_3 - 11c_2s_3 - 30s_3)\Big).$$

Remark that this polynomial does not depend on c_1 nor s_1. Since V is bounded by design, the restriction of $\mathcal{R}$ (resp. $\widetilde{\mathcal{R}}$) to V is proper so that $\mathcal{A}_{\mathrm{typ}}(\mathcal{R}, V) = \mathcal{R}(\mathcal{K}(\mathcal{R}, V))$ (resp. $\mathcal{A}_{\mathrm{typ}}(\widetilde{\mathcal{R}}, V) = \widetilde{\mathcal{R}}(\mathcal{K}(\widetilde{\mathcal{R}}, V))$). Hence the polynomial whose zero-set is $\overline{\mathcal{A}_{\mathrm{typ}}(\mathcal{R})}^Z$ (resp. $\overline{\mathcal{A}_{\mathrm{typ}}(\widetilde{\mathcal{R}})}^Z$) does not depend on c_1 nor s_1 as well. The computation of this polynomial can be done by algebraic elimination and can be found in [EOW95].

The application of Algorithm 4 gives rise to two main sets. First, the computation of a sample set of points that meets every semi-algebraically connected component of $\mathbb{R}^3 - \overline{\mathcal{A}_{\mathrm{typ}}(\mathcal{R}, V)}^Z$ (resp. $\mathbb{R}^3 - \overline{\mathcal{A}_{\mathrm{typ}}(\widetilde{\mathcal{R}}, V)}^Z$), is done trough the WitnessPoints function, which is available in Maple 2020. One can also use the symbolic RAGlib[2] software written with the computer algebra programming language Maple. The output set $\mathcal{P}$ (resp. $\widetilde{\mathcal{P}}$) is represented in Figure 9.2 where we adopted a two dimensional representation. Since $\rho = \sqrt{x_1^2 + x_2^2}$ and x_3 do not depend on c_1 nor s_1, as well as the polynomial defining $\overline{\mathcal{A}_{\mathrm{typ}}(\mathcal{R}, V)}^Z$ (resp. $\overline{\mathcal{A}_{\mathrm{typ}}(\widetilde{\mathcal{R}}, V)}^Z$), it makes sense to look at the projection of $\overline{\mathcal{A}_{\mathrm{typ}}(\mathcal{R})}^Z$ and $\mathcal{P}$ (resp. $\overline{\mathcal{A}_{\mathrm{typ}}(\widetilde{\mathcal{R}}, V)}^Z$ and $\widetilde{\mathcal{P}}$) on the plane associated to (ρ, x_3).

Then, taking the inverse solutions of these points through $\mathcal{R}$ (resp. $\widetilde{\mathcal{R}}$), we compute a roadmap of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ (resp. $V_{\mathbb{R}} - \mathcal{K}(\widetilde{\mathcal{R}}, V)$) passing through these points. Hence one can easily identify points that belong to the same semi-algebraically connected component of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ (resp. $V_{\mathbb{R}} - \mathcal{K}(\widetilde{\mathcal{R}}, V)$). Hereafter we describe briefly how do we compute

[2] RAGlib: https://www-polsys.lip6.fr/~safey/RAGLib/

this roadmap. The first step consists in deforming the semi-algebraic set $S = V_{\mathbb{R}} - \boldsymbol{V}(\Delta)$ (resp. $\widetilde{S} = V_{\mathbb{R}} - \boldsymbol{V}(\widetilde{\Delta})$) into the closed semi-algebraic set that is the union of

$$\begin{array}{rl} & S^+ = V_{\mathbb{R}} \cap \{\boldsymbol{x} \in \mathbb{R}^6 \mid \Delta \geq \epsilon\} \\ \text{and} & S^- = V_{\mathbb{R}} \cap \{\boldsymbol{x} \in \mathbb{R}^6 \mid \Delta \leq -\epsilon\} \end{array} \left(\text{resp.} \quad \begin{array}{rl} & \widetilde{S}^+ = V_{\mathbb{R}} \cap \{\boldsymbol{x} \in \mathbb{R}^6 \mid \widetilde{\Delta} \geq \epsilon\} \\ \text{and} & \widetilde{S}^- = V_{\mathbb{R}} \cap \{\boldsymbol{x} \in \mathbb{R}^6 \mid \widetilde{\Delta} \leq -\epsilon\} \end{array} \right)$$

with ϵ small enough. Since $V_{\mathbb{R}}$ is bounded by design, according to [Can93] or [CSS23, Proposition 3.5], computing a roadmap of this deformation is enough to obtain a roadmap of S (resp. $\widetilde{S}$). This is done using classical computation of critical loci of projections and fibers of a projection to repair connectivity failures as described in e.g. [Can88a, Can93]. Moreover we add fibers that pass through the points of $\mathcal{P}$ (resp. $\widetilde{\mathcal{P}}$) to determine the semi-algebraically connected component of S (resp. $\widetilde{S}$) where they belong.

In Figure 9.3 we draw roadmaps for the projections of $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ and $V_{\mathbb{R}} - \mathcal{K}(\widetilde{\mathcal{R}}, V)$ on the plane associated to (c_2, s_2, c_3, s_3) that are obtained through the above process. Indeed since the polynomials Δ and $\widetilde{\Delta}$ do not depend on c_1 nor s_1, we choose to restrict our connectivity description on this projection, since extending it to the whole space is immediate. Finally, since the projection of $V_{\mathbb{R}}$ on (c_2, s_2, c_3, s_3) is two dimensional, we choose to plot instead the angles θ_1, θ_2 that are, modulo 2π, uniquely associated to the data computed.

For the first robot, one the left image of Figure 9.3 are represented four inverse solutions of one point of $\mathcal{P}$. Among these points, one observes that two pairs of points are lying on the same connected component (same color) of the roadmap. Hence, both of them are cuspidal pairs, and *the first robot is cuspidal*.

For the second robot, the preimages are associated to their image in $\widetilde{\mathcal{P}}$ that has the same shape (disk, diamond or square) in the right image of Figure 9.2. While the square point has no preimages, the diamond one has two, which belong to different connected component of the roadmap, and the square point has four preimages, each of them in a different component. Hence, according to Proposition 9.2.1, *the second robot is not cuspidal*.

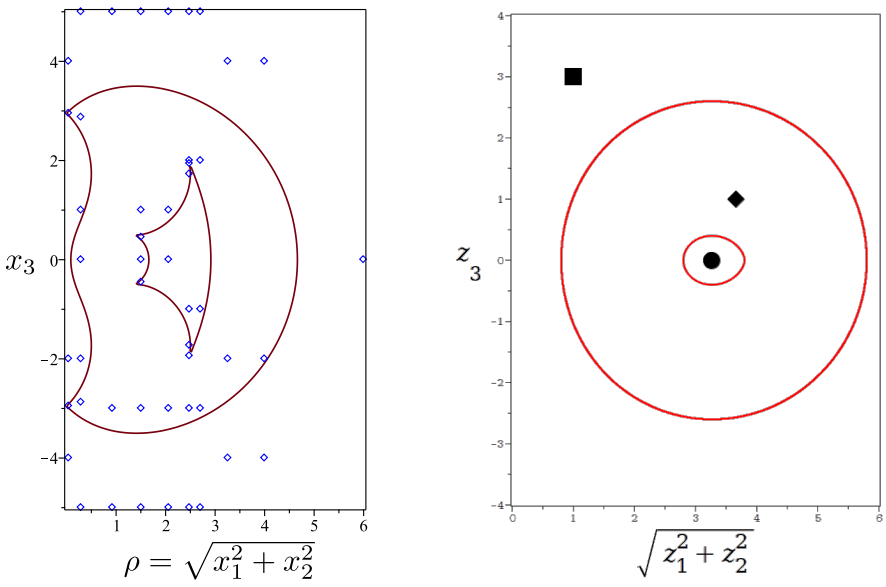


Figure 9.2. Projections on the plane (ρ, x_3) of the sets atypical values (red curve) of the orthogonal 3R serial robots under study together with points $\mathcal{P}$ (left) and $\widetilde{\mathcal{P}}$ (right) output by WITNESSPOINTS, that meet every connected component of the complement of respectively $\overline{\mathcal{A}_{\text{typ}}(\mathcal{R}, V)}^z$ (left) and $\overline{\mathcal{A}_{\text{typ}}(\widetilde{\mathcal{R}}, V)}^z$ (right). On the left, the full output $\mathcal{P}$ for the first robot is represented as blue diamonds. On the right, for the sake of our discussion, we represented a subset of $\widetilde{\mathcal{P}}$ with exactly one point in each connected component.

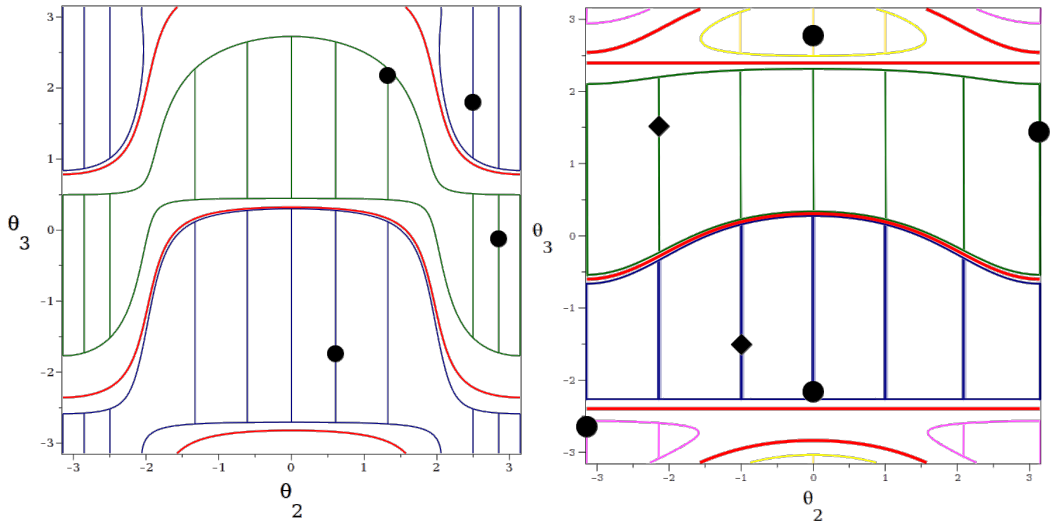


Figure 9.3. Representation of points in $V_{\mathbb{R}} - \mathcal{K}(\mathcal{R}, V)$ (left) and $V_{\mathbb{R}} - \mathcal{K}(\widetilde{\mathcal{R}}, V)$ (right) that map to points in respectively $\mathcal{P}$ and $\widetilde{\mathcal{P}}$ through respectively $\mathcal{R}$ and $\widetilde{\mathcal{R}}$. and associated roadmaps The red lines represent respectively the sets $\boldsymbol{V}(\Delta)$ and $\boldsymbol{V}(\widetilde{\Delta})$. Roadmaps of the projection of $S^+ \cup S^-$ (left) and $\widetilde{S}^+ \cup \widetilde{S}^-$, containing these points, are represented a lines of distinct colors, one for each connected component. The coordinates are the angles that are associated to the projection on the plane associated to (c_2, s_2, c_3, s_3) of the sets under consideration.

Bibliography

[ABRW96] M.-E. Alonso, E. Becker, M. F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications*, pages 1–15, Basel, 1996. Birkhäuser Basel.

[ACM84a] 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.

[ACM84b] D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical Algebraic Decomposition II: An Adjacency Algorithm for the Plane. *SIAM Journal on Computing*, 13(4):878–889, 1984.

[ACM85] D. S. Arnon, G. E. Collins, and S. McCallum. An adjacency algorithm for cylindrical algebraic decompositions of three-dimensional space. In B. F. Caviness, editor, *EUROCAL '85*, pages 246–261, Berlin, Heidelberg, 1985. Springer Berlin Heidelberg.

[AGK97] B. Amrhein, O. Gloor, and W. Küchlin. On the walk. *Theoretical Computer Science*, 187(1):179–202, 1997.

[AH74] A. V. Aho and J. E. Hopcroft. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Longman Publishing Co., Inc., USA, 1st edition, 1974.

[AL94] W. Adams and P. Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, 1994.

[AMW08] L. Alberti, B. Mourrain, and J. Wintz. Topology and arrangement computation of semi-algebraic planar curves. *Computer Aided Geometric Design*, 25(8):631–651, 2008. Computer Graphics and Applications.

[Arn88] D. S. Arnon. A cluster-based cylindrical algebraic decomposition algorithm. *Journal of Symbolic Computation*, 5(1):189–212, 1988.

[ARS02] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[AS05] J. G. Alcázar and J. R. Sendra. Computation of the topology of real algebraic space curves. *Journal of Symbolic Computation*, 39(6):719–744, 2005.

[AY03] H. Anai and H. Yanami. Synrac: A maple-package for solving real algebraic constraints. In P. M. A. Sloot, D. Abramson, A. V. Bogdanov, J. J. Dongarra,

A. Y. Zomaya, and Y. E. Gorbachev, editors, *Computational Science — ICCS 2003*, pages 828–837, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[Bar97] A. I. Barvinok. On the betti numbers of semialgebraic sets defined by few quadratic inequalities. *Mathematische Zeitschrift*, 225(2):231–244, 6 1997.

[Bas99a] S. Basu. On bounding the betti numbers and computing the euler characteristic of semi-algebraic sets. *Discrete & Computational Geometry*, 22(1):1–18, Jul 1999.

[Bas99b] S. Basu. New Results on Quantifier Elimination over Real Closed Fields and Applications to Constraint Databases. *J. ACM*, 46(4):537–555, jul 1999.

[Bas03] S. Basu. Different bounds on the different betti numbers of semi-algebraic sets. *Discrete & Computational Geometry*, 30(1):65–85, May 2003.

[Bas17] S. Basu. Algorithms in real algebraic geometry: A survey. In *Real algebraic geometry*, volume 5 of *Panoramas et synthèses*, pages 107–153. Société Mathématique de France, 2017.

[BBH+17] D. A. Brake, D. J. Bates, W. Hao, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Algorithm 976: Bertini_real: Numerical decomposition of real algebraic curves and surfaces. *ACM Trans. Math. Softw.*, 44(1), jul 2017.

[BCGY08] M. Burr, S. W. Choi, B. Galehouse, and C. K. Yap. Complete subdivision algorithms, ii: Isotopic meshing of singular algebraic curves. In *Proceedings of the Twenty-First International Symposium on Symbolic and Algebraic Computation*, ISSAC '08, page 87–94, New York, NY, USA, 2008. Association for Computing Machinery.

[BCR98] J. Bochnack, M. Coste, and M.-F. Roy. *Real Algebraic Geometry*, volume 3 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, Heidelberg, 1st edition, 1998.

[BCS97] P. Bürgisser, M. Clausen, , and M. A. Shokrollahi. Algebraic Complexity Theory. 1997.

[BD07] C. W. Brown and J. H. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. ISSAC '07, page 54–60, New York, NY, USA, 2007. Association for Computing Machinery.

[BDLW98] M. Benedikt, G. Dong, L. Libkin, and L. Wong. Relational expressive power of constraint query languages. *J. ACM*, 45(1):1–34, jan 1998.

[BDRH+13] G. M. Besana, S. Di Rocco, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Cell decomposition of almost smooth real algebraic surfaces. *Numerical Algorithms*, 63(4):645–678, 2013.

[BE02] D. Bouziane and M. El Kahoui. Computation of the dual of a plane projective curve. *Journal of Symbolic Computation*, 34(2):105–117, 2002.

[BEKS13] E. Berberich, P. Emeliyanenko, A. Kobel, and M. Sagraloff. Exact symbolic-numeric computation of planar algebraic curves. *Theoretical Computer Science*, 491:1–32, 2013.

[Ber09] D. S. Bernstein. *Matrix Mathematics: Theory, Facts, and Formulas*. Princeton University Press, Princeton, 2nd edition, 2009.

[BES21] J. Berthomieu, C. Eder, and M. Safey El Din. msolve: A Library for Solving Polynomial Systems. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, ISSAC '21, page 51–58, New York, NY, USA, 2021. Association for Computing Machinery.

[BES23] J. Berthomieu, C. Eder, and M. Safey El Din. New efficient algorithms for computing Gröbner bases of saturation ideals (F4SAT) and colon ideals (Sparse-FGLM-colon). *(preprint)*, 2023.

[BGH+10] 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.

[BGHM97] B. Bank, M. Giusti, J. Heintz, and G. Mbakop. Polar varieties, real equation solving, and data structures: The hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

[BGHM01] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

[BGHP04] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo. Generalized polar varieties and an efficient real elimination. *Kybernetika*, 40(5):519–550, 2004.

[BGHP05] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo. Generalized polar varieties: Geometry and algorithms. *Journal of complexity*, 21(4):377–412, 2005.

[BK09] A. Bostan and M. Kauers. The complete generating function for gessel walks is algebraic. *Proceedings of the American Mathematical Society*, 138:3063–3078, 2009.

[BLS88] L. Babai, E. Luks, and A. Seress. Fast management of permutation groups. In *29th Annual Symposium on Foundations of Computer Science*, pages 272–282, 1988.

[BM20] C. W. Brown and S. McCallum. Enhancements to lazard's method for cylindrical algebraic decomposition. In F. Boulier, M. England, T. M. Sadykov, and E. V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing*, pages 129–149, Cham, 2020. Springer International Publishing.

[BOKR84] M. Ben-Or, D. Kozen, and J. Reif. The complexity of elementary algebra and geometry. In *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing*, STOC '84, page 457–464, New York, NY, USA, 1984. Association for Computing Machinery.

[BPR96a] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, nov 1996.

[BPR96b] S. Basu, R. Pollak, and M.-F. Roy. On the number of cells defined by a family of polynomials on a variety. *Mathematika*, 43(1):120–126, 1996.

[BPR97] S. Basu, R. Pollack, and M.-F. Roy. On computing a set of points meeting every cell defined by a family of polynomials on a variety. *Journal of Complexity*, 13(1):28–37, 1997.

[BPR98] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 341–350, Vienna, 1998. Springer Vienna.

[BPR00] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety. *Journal of the American Mathematical Society*, 13(1):55–82, 2000.

[BPR05] S. Basu, R. Pollack, and M.-F. Roy. On the betti numbers of sign conditions. In *Proceedings of the American Mathematical Society*, volume 133, pages 965–974 (electronic), 2005.

[BPR06] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*. Algorithms and Computation in Mathematics. Springer International Publishing, 2nd revised and extended 2016 edition, 2006.

[BR14] S. Basu and M.-F. Roy. Divide and conquer roadmap for algebraic sets. *Discrete & Computational Geometry*, 52(2):278–343, 2014.

[BR18] S. Basu and C. Riener. On the Isotypic Decomposition of Cohomology Modules of Symmetric Semi-algebraic Sets: Polynomial Bounds on Multiplicities. *International Mathematics Research Notices*, 2020(7):2054–2113, 04 2018.

[Bra00] J. Brasselet. Milnor classes via polar varieties. *Singularities in algebraic and analytic geometry*, pages 181–187, 2000.

[Bro99] C. W. Brown. *Solution Formula Construction for Truth Invariant Cad's*. PhD thesis, University of Delaware, USA, 1999.

[Bro01] C. W. Brown. Improved projection for cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 32(5):447–465, 2001.

[Bro03] C. W. Brown. Qepcad b: A program for computing with semi-algebraic sets using cads. *SIGSAM Bull.*, 37(4):97–108, dec 2003.

[BRSS14] S. Basu, M.-F. Roy, M. Safey El Din, and É. Schost. A baby step–giant step roadmap algorithm for general algebraic sets. *Foundations of Computational Mathematics*, 14(6):1117–1172, 2014.

[BS83] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoretical computer science*, 22(3):317–330, 1983.

[BS87] D. Bayer and M. Stillman. A theorem on refining division orders by the reverse lexicographic order. *Duke Mathematical Journal*, 55(2):321 – 328, 1987.

[Buc65] B. Buchberger. *Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal*. PhD thesis, Universitat Insbruck, 1965.

[Buc70] B. Buchberger. Ein algorithmisches kriterium für die lösbarkeit eines algebraischen gleichungssystems. *Aequationes Mathematicae*, 4:374–383, 01 1970.

[Buc76] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 10(3):19–29, aug 1976.

[Buc79] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of gröbner-bases. In E. W. Ng, editor, *Symbolic and Algebraic Computation*, pages 3–21, Berlin, Heidelberg, 1979. Springer Berlin Heidelberg.

[Buc85] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. pages 184–232. 01 1985.

[Buc01] B. Buchberger. Gröbner bases and systems theory. *Multidimensional Systems and Signal Processing*, 12(3):223–251, 2001.

[BW93] T. Becker and V. Weispfenning. *Gröbner bases*. Graduate Texts in Mathematics. Springer New York, NY, 1993.

[BZ02] G. Burde and H. Zieschang. *Knots*. De Gruyter, Berlin, New York, 2nd revised and extended 2003 edition, 2002.

[Can88a] J. Canny. *The complexity of robot motion planning*. MIT press, 1988.

[Can88b] J. Canny. Constructing roadmaps of semi-algebraic sets i: Completeness. *Artificial Intelligence*, 37(1-3):203–222, 1988.

[Can88c] J. Canny. Some algebraic and geometric computations in pspace. STOC '88, page 460–467, New York, NY, USA, 1988. Association for Computing Machinery.

[Can91] J. F. Canny. Computing roadmaps of general semi-algebraic sets. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 94–107. Springer, 1991.

[Can93] J. Canny. Computing roadmaps of general semi-algebraic sets. *The Computer Journal*, 36(5):504–514, 1993.

[Can95] J. Canny. A toolkit for non-linear algebra. In *Proceedings of the Workshop on Algorithmic Foundations of Robotics*, WAFR, page 513–535, USA, 1995. A. K. Peters, Ltd.

[CGH88] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In T. Mora, editor, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 131–151, Berlin, Heidelberg, 1988. Springer Berlin Heidelberg.

[CGH91] L. Caniglia, A. Galligo, and J. Heintz. Equations for the projective closure and effective nullstellensatz. *Discrete Applied Mathematics*, 33(1):11–23, 1991.

[CGV92] J. Canny, D. Y. Grigor'ev, and N. N. Vorobjov. Finding connected components of a semialgebraic set in subexponential time. *Applicable Algebra in Engineering, Communication and Computing*, 2(4):217–238, 1992.

[CH91] G. E. Collins and H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation*, 12(3):299–328, 1991.

[CJL13] J.-S. Cheng, K. Jin, and D. Lazard. Certified rational parametric approximation of real algebraic space curves with local generic position method. *Journal of Symbolic Computation*, 58:18–40, 2013.

[CKM97] S. Collart, M. Kalkbrener, and D. Mall. Converting Bases with the Gröbner Walk. *Journal of Symbolic Computation*, 24(3):465–469, 1997.

[CLH+05] H. Choset, K. M. Lynch, S. Hutchinson, G. Kantor, W. Burgard, L. E. Kavraki, and S. Thrun. *Principles of Robot Motion*. Intelligent Robotics and Autonomous Agents series. MIT Press, Cambridge, MA, 2005.

[CLO15] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Cham, 4th edition, 2015.

[CLP+10] J. Cheng, S. Lazard, L. Peñaranda, M. Pouget, F. Rouillier, and E. Tsigaridas. On the topology of real algebraic plane curves. *Mathematics in Computer Science*, 4:113–137, 2010.

[CLRS09] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to algorithms*. MIT press, third edition, 2009.

[CM14] C. Chen and M. Moreno Maza. Quantifier elimination by cylindrical algebraic decomposition based on regular chains. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, page 91–98, New York, NY, USA, 2014. Association for Computing Machinery.

[CM16] C. Chen and M. Moreno Maza. Quantifier elimination by cylindrical algebraic decomposition based on regular chains. *Journal of Symbolic Computation*, 75:74–93, 2016. Special issue on the conference ISSAC 2014: Symbolic computation and computer algebra.

[Col75] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In H. Brakhage, editor, *Automata Theory and Formal Languages*, pages 134–183, Berlin, Heidelberg, 1975. Springer Berlin Heidelberg.

[Cor05] S. Corvez. *Study of polynomial system: contribution to the classification of a family of manipulators and calculating the intersection of A-spline curve*. PhD thesis, University of Rennes, Rennes, France, may 2005.

[CPHM01] D. Castro, L. Pardo, K. Hägele, and J. Morais. Kronecker's and Newton's Approaches to Solving: A First Comparison. *Journal of Complexity*, 17(1):212–303, 2001.

[CPS+22] D. Chablat, R. Prébet, M. Safey El Din, D. H. Salunkhe, and P. Wenger. Deciding cuspidality of manipulators through computer algebra and algorithms in real algebraic geometry. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22, page 439–448, New York, NY, USA, 2022. Association for Computing Machinery.

[CR04] S. Corvez and F. Rouillier. Using computer algebra tools to classify serial manipulators. In F. Winkler, editor, *Automated Deduction in Geometry*, pages 31–43, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[CS92] M. Coste and M. Shiota. Nash triviality in families of nash manifolds. *Inventiones mathematicae*, 108(1):349–368, 1992.

[CS95] M. Coste and M. Shiota. Thom's first isotopy lemma: a semialgebraic version, with uniform bound. In *Real Algebraic and Analytic Geometry*, De Gruyter Proceedings in Mathematics, pages 83–101, Berlin – New York, 1995.

[CSS20] J. Capco, M. Safey El Din, and J. Schicho. Robots, computer algebra and eight connected components. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, pages 62–69, 2020.

[CSS23] J. Capco, M. Safey El Din, and J. Schicho. Positive dimensional parametric polynomial systems, connectivity queries and applications in robotics. *Journal of Symbolic Computation*, 115:320–345, 2023.

[CWF20] C. Chen, W. Wu, and Y. Feng. Numerical roadmap of smooth bounded real algebraic surface. *Computer Aided Geometric Design*, 79:101858, 2020.

[DDR+22] D. N. Diatta, S. Diatta, F. Rouillier, M.-F. Roy, and M. Sagraloff. Bounds for polynomials on algebraic numbers and application to curve topology. *Discrete & Computational Geometry*, 67(3):631–697, 2022.

[Dem00] M. Demazure. *Bifurcations and Catastrophes*. Springer Berlin, Heidelberg, 2000.

[DET07] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the complexity of real solving bivariate systems. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*, ISSAC '07, pages 127–134, New York, NY, USA, 2007. Association for Computing Machinery.

[DET09] D. I. Diochnos, I. Z. Emiris, and E. P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *Journal of Symbolic Computation*, 44(7):818–835, 2009.

[DH88] J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation*, 5(1):29–35, 1988.

[DH17] M. Dehghani Darmian and A. Hashemi. Parametric FGLM algorithm. *Journal of Symbolic Computation*, 82:38–56, 2017.

[Dia09] D. N. Diatta. *Calcul effectif de la topologie de courbes et surfaces algébriques réelles*. PhD thesis, Université de Limoges, 2009.

[DL78] R. A. Demillo and R. J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, 1978.

[DL08] C. Durvye and G. Lecerf. A concise proof of the Kronecker polynomial system solver from scratch. *Expositiones Mathematicae*, 26(2):101–139, 2008.

[DMR08] D. N. Diatta, B. Mourrain, and O. Ruatta. On the computation of the topology of a non-reduced implicit space curve. In *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 47–54, 2008.

[DMR12] D. N. Diatta, B. Mourrain, and O. Ruatta. On the isotopic meshing of an algebraic implicit surface. *Journal of Symbolic Computation*, 47(8):903–925, 2012.

[Dri98] L. P. D. v. d. Dries. *Tame Topology and O-minimal Structures*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1998.

[DRR14] D. N. Diatta, F. Rouillier, and M.-F. Roy. On the computation of the topology of plane curves. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, pages 130–137, 2014.

[DS97] A. Dolzmann and T. Sturm. Redlog: Computer algebra meets computer logic. *SIGSAM Bull.*, 31(2):2–9, jun 1997.

[DS04] X. Dahan and E. Schost. Sharp Estimates for Triangular Sets. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, page 103–110, New York, NY, USA, 2004. Association for Computing Machinery.

[Duv89] D. Duval. Rational puiseux expansions. *Compositio Mathematica*, 70(2):119–154, 1989.

[EF17] C. Eder and J.-C. Faugère. A survey on signature-based algorithms for computing gröbner bases. *Journal of Symbolic Computation*, 80:719–784, 2017.

[EGS23] J. Elliott, M. Giesbrecht, and E. Schost. Bit complexity for computing one point in each connected component of a smooth real algebraic set. *Journal of Symbolic Computation*, 116:72–97, 2023.

[EHV92] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Inventiones mathematicae*, 110:207–235, 1992.

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150. Springer-Verlag, New York, 1995.

[EKW07] A. Eigenwillig, M. Kerber, and N. Wolpert. Fast and exact geometric analysis of real algebraic plane curves. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*, pages 151–158, 2007.

[El 08] M. El Kahoui. Topology of real algebraic space curves. *Journal of Symbolic Computation*, 43(4):235–258, 2008.

[ELLS07] H. Everett, S. Lazard, D. Lazard, and M. Safey El Din. The voronoi diagram of three lines. In *Proceedings of the Twenty-Third Annual Symposium on Computational Geometry*, SCG '07, page 255–264, New York, NY, USA, 2007. Association for Computing Machinery.

[ELLS09] H. Everett, D. Lazard, S. Lazard, and M. Safey El Din. The voronoi diagram of three lines. *Discrete & Computational Geometry*, 42(1):94–130, 2009.

[EN62] J. A. Eagon and D. G. Northcott. Ideals defined by matrices and a certain complex associated with them. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, 269(1337):188–204, 1962.

[EOW95] J. El Omri and P. Wenger. How to recognize simply a non-singular posture changing 3-DOF manipulator. In *Proc. 7th Int. Conf. on Advanced Robotics*, pages 215–222, 1995.

[Esc01] J. Escribano. Nash triviality in families of Nash mappings. *Annales de l'Institut Fourier*, 51(5):1209–1228, 2001.

[Fau99] J.-C. Faugère. A new efficient algorithm for computing gröbner bases (f4). *Journal of Pure and Applied Algebra*, 139(1):61–88, 1999.

[Fau02] J. C. Faugère. A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, page 75–83, New York, NY, USA, 2002. Association for Computing Machinery.

[Fau10] J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In K. Fukuda, J. v. d. Hoeven, M. Joswig, and N. Takayama, editors, *Mathematical Software – ICMS 2010*, pages 84–87, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[FdSMR98] J.-C. Faugère, F. de Saint-Martin, and F. Rouillier. Design of regular nonseparable bidimensional wavelets using grobner basis techniques. *IEEE Transactions on Signal Processing*, 46(4):845–856, 1998.

[Fer22] A. Ferguson. *Exact algorithms for polynomial optimisation*. PhD thesis, Sorbonne Université, Paris, France, october 2022.

[FGLM93] J. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[FGT09] E. Fortuna, P. Gianni, and B. Trager. Generators of the ideal of an algebraic space curve. *Journal of Symbolic Computation*, 44(9):1234–1254, 2009.

[FJ03] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases. In D. Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, pages 44–60, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[FJLT07] K. Fukuda, A. Jensen, N. Lauritzen, and R. Thomas. The generic Gröbner walk. *Journal of Symbolic Computation*, 42(3):298–312, 2007.

[FM17] J.-C. Faugère and C. Mou. Sparse FGLM algorithms. *Journal of Symbolic Computation*, 80:538–569, 2017.

[FMRS08] J.-C. Faugère, G. Moroz, F. Rouillier, and M. Safey El Din. Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities. In *Proceedings of the Twenty-First International Symposium on Symbolic and Algebraic Computation*, ISSAC '08, pages 79–86, New York, NY, USA, 2008. Association for Computing Machinery.

[FRPM06] I. A. Fotiou, P. Rostalski, P. A. Parrilo, and M. Morari. Parametric optimization and optimal control using algebraic geometry methods. *International Journal of Control*, 79(11):1340–1358, 2006.

[FT22] E. Feliu and M. L. Telek. On generalizing descartes' rule of signs to hypersurfaces. *Advances in Mathematics*, 408:108582, 2022.

[Ful98] W. Fulton. *Intersection Theory*, volume 2. Springer, New York, NY, 2nd edition, 1998.

[Ful08] W. Fulton. *Algebraic curves*. 2008.

[GCMT02] O. Grellier, P. Comon, B. Mourrain, and P. Trebuchet. Analytical blind channel identification. *IEEE Transactions on Signal Processing*, 50(9):2196–2207, 2002.

[GE96] L. González-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *Journal of Complexity*, 12(4):527–544, 1996.

[GG13] J. v. z. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013.

[GGV10] S. Gao, Y. Guan, and F. Volny. A new incremental algorithm for computing groebner bases. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, page 13–19, New York, NY, USA, 2010. Association for Computing Machinery.

[GHM+98] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstem, and L. M. Pardo. Straight-line programs in geometric elimination theory. *Journal of pure and applied algebra*, 124(1-3):101–146, 1998.

[GHMM23] A. K. Goharshady, S. Hitarth, F. Mohammadi, and H. J. Motwani. Algebro-geometric algorithms for template-based synthesis of polynomial programs. In *Proceedings of the ACM on Programming Languages*, volume 7, pages 727–756, New York, NY, USA, 2023. Association for Computing Machinery.

[GHMP95] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. When polynomial equation systems can be "solved" fast? In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 205–231. Springer, 1995.

[GHMP97] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. Le rôle des structures de données dans les problèmes d'élimination. *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics*, 325(11):1223–1228, 1997.

[GKP94] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison Wesley, 2nd edition, 1994.

[GLMT05] G. Gatellier, A. Labrouzy, B. Mourrain, and J.-P. Técourt. Computing the topology of three-dimensional algebraic curves. *Computational methods for algebraic spline surfaces*, pages 27–43, 2005.

[GLS01] M. Giusti, G. Lecerf, and B. Salvy. A gröbner free alternative for polynomial system solving. *Journal of complexity*, 17(1):154–211, 2001.

[GM88] R. Gebauer and H. M. Möller. On an installation of buchberger's algorithm. *Journal of Symbolic Computation*, 6(2):275–286, 1988.

[GM89] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using groebher bases. In L. Huguet and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 247–257, Berlin, Heidelberg, 1989. Springer Berlin Heidelberg.

[GM19] N. Giménez and G. Matera. On the bit complexity of polynomial system solving. *Journal of Complexity*, 51:20–67, 2019.

[GMN+91] A. Giovini, T. Mora, G. Niesi, L. Robbiano, and C. Traverso. "one sugar cube, please" or selection strategies in the buchberger algorithm. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation*,

ISSAC '91, page 49–54, New York, NY, USA, 1991. Association for Computing Machinery.

[GNBS22] J. García Fontán, A. Nayak, S. Briot, and M. Safey El Din. Singularity analysis for the perspective-four and five-line problems. *International Journal of Computer Vision*, 130(4):909–932, 4 2022.

[GNS23] S. Gopalakrishnan, V. Neiger, and M. Safey El Din. Refined f5 algorithms for ideals of minors of square matrices. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, ISSAC '23, page 270–279, New York, NY, USA, 2023. Association for Computing Machinery.

[GR93] L. Gournay and J.-J. Risler. Construction of roadmaps in semi-algebraic sets. *Applicable Algebra in Engineering, Communication and Computing*, 4(4):239–252, 1993.

[GTZ88] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2):149–167, 1988.

[GV88] D. Y. Grigoriev and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *Journal of symbolic computation*, 5(1-2):37–64, 1988.

[GV92] D. Grigoryev and N. Vorobjov. Counting connected components of a semialgebraic set in subexponential time. *Computational Complexity*, 2:133–186, 06 1992.

[GV05] A. Gabrielov and N. Vorobjov. Betti numbers of semialgebraic sets defined by quantifier-free formulae. *Discrete & Computational Geometry*, 33(3):395–401, 2005.

[GV09] A. Gabrielov and N. Vorobjov. Approximation of definable sets by compact families, and upper bounds on homotopy and homology. *Journal of the London Mathematical Society*, 80(1):35–54, 2009.

[GWDPL76] C. G. Gibson, K. Wirthmüller, A. A. Du Plessis, and E. J. Looijenga. *Topological stability of smooth mappings*, volume 552. Springer, 1st edition, 1976.

[HAB+17] T. Hales, M. Adams, G. Bauer, T. D. Dang, J. Harrison, L. T. Hoang, C. Kaliszyk, V. Magron, S. McLaughlin, T. T. Nguyen, et al. A formal proof of the kepler conjecture. *Forum of Mathematics, Pi*, 5:e2, 2017.

[Har77] R. Hartshorne. *Algebraic Geometry*. Graduate texts in mathematics. Springer New York, NY, 1977.

[Har80] R. M. Hardt. Semi-algebraic local-triviality in semi-algebraic mappings. *American Journal of Mathematics*, 102(2):291–302, 1980.

[HD64] R. S. Hartenberg and J. Denavit. *Kinematic synthesis of linkages*. McGraw-Hill series in mechanical engineering. McGraw-Hill, New York San Francisco Toronto [etc, 1964.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983.

[HHPS21] A. Hashemi, J. Heintz, L. M. Pardo, and P. Solernó. On bézout inequalities for non-homogeneous polynomial ideals. *Journal of Symbolic Computation*, 106:1–22, 2021.

[HMP00] H. Hirukawa, B. Mourrain, and Y. Papegay. A symbolic-numeric silhouette algorithm. In *Proceedings. 2000 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2000) (Cat. No.00CH37113)*, volume 3, pages 2358–2365, 2000.

[Hon91] H. Hong. Comparison of several decision algorithms for the existential theory of the reals. Technical report, RISC Linz, 1991.

[Hon92] 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, page 177–188, New York, NY, USA, 1992. Association for Computing Machinery.

[Hon10] H. Hong. Connectivity in semi-algebraic sets. In *12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 4–7, 2010.

[HR79] A. Holme and J. Roberts. Pinch-points and multiple locus of generic projections of singular varieties. *Advances in Mathematics*, 33(3):212–256, 1979.

[HRS90] J. Heintz, M.-F. Roy, and P. Solernó. Sur la complexité du principe de Tarski-Seidenberg. *Bulletin de la Société Mathématique de France*, 118(1):101–126, 1990.

[HRS93] J. Heintz, M.-F. Roy, and P. Solernó. On the Theoretical and Practical Complexity of the Existential Theory of Reals. *The Computer Journal*, 36(5):427–431, 01 1993.

[HRS94a] J. Heintz, M.-F. Roy, and P. Solernó. Single exponential path finding in semi-algebraic sets, part ii: The general case. In C. L. Bajaj, editor, *Algebraic Geometry and its Applications: Collections of Papers from Shreeram S. Abhyankar's 60th Birthday Conference*, pages 449–465. Springer New York, New York, NY, 1994.

[HRS94b] J. Heintz, M.-F. Roy, and P. Solernó. Description of the connected components of a semialgebraic set in single exponential time. *Discrete & Computational Geometry*, 11(2):121–140, Feb 1994.

[HRSS20] H. Hong, J. Rohal, M. Safey El Din, and E. Schost. Connectivity in semi-algebraic sets i, 2020. preprint.

[HS12] H. Hong and M. Safey El Din. Variant quantifier elimination. *Journal of Symbolic Computation*, 47(7):883–901, 2012. International Symposium on Symbolic and Algebraic Computation (ISSAC 2009).

[HSR89] J. Heintz, P. Solernó, and M.-F. Roy. On the complexity of semialgebraic sets. In *IFIP Congress*, 1989.

[IC14] R. Iraji and H. Chitsaz. Nuroa: A numerical roadmap algorithm. *53rd IEEE Conference on Decision and Control*, pages 5359–5366, 2014.

[IP11] M. N. Islam and A. Poteaux. Connectivity queries on curves in Rn. *ACM Communications in Computer Algebra*, 45(1/2):117–118, 2011.

[IPP23] M. N. Islam, A. Poteaux, and R. Prébet. Algorithm for connectivity queries on real algebraic curves. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, ISSAC '23, page 345–353, New York, NY, USA, 2023. Association for Computing Machinery.

[IYA14] H. Iwane, H. Yanami, and H. Anai. Synrac: A toolbox for solving real algebraic constraints. In H. Hong and C. Yap, editors, *Mathematical Software – ICMS 2014*, pages 518–522, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[JC21] K. Jin and J. Cheng. On the complexity of computing the topology of real algebraic space curves. *Journal of Systems Science and Complexity*, 34(2):809–826, 2021.

[Jel99] Z. Jelonek. Testing sets for properness of polynomial mappings. *Mathematische Annalen*, 315(1):1–35, 1999.

[JK05] Z. Jelonek and K. Kurdyka. Quantitative generalized bertini-sard theorem for smooth affine varieties. *Discrete & Computational Geometry*, 34(4):659–678, 2005.

[JW18] T. Jordán and W. Whiteley. Global rigidity. In *Handbook of Discrete and Computational Geometry (third edition)*, pages 1661–1694. CRC Press, 2018.

[Kal85] E. Kaltofen. Computing with polynomials given by straight-line programs ii sparse factorization. In *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, volume 26, pages 450–458, 1985.

[Kal88] E. Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *J. ACM*, 35(1):231–264, jan 1988.

[Kal89] E. L. Kaltofen. Factorization of polynomials given by straight-line programs. *Adv. Comput. Res.*, 5:375–412, 1989.

[KB78] C. Kollreider and B. Buchberger. An improved algorithmic construction of gröbner-bases for polynomial ideals. *SIGSAM Bull.*, 12(2):27–36, may 1978.

[KKBT08] J. Y. Kaminski, A. Kanel-Belov, and M. Teicher. Trisecant lemma for non equidimensional varieties. *Journal of Mathematical Sciences*, 149(2):1087–1097, 2008.

[KKZS09] M. Kauers, C. Koutschan, D. Zeilberger, and R. P. Stanley. Proof of ira gessel's lattice path conjecture. In *Proceedings of the National Academy of Sciences of the United States of America*, volume 106, pages 11502–11505. National Academy of Sciences, 2009.

[Kön03] J. König. Einleitung in die allgemeine Theorie der algebraischen Groöszen. 1903.

[KOS00] K. Kurdyka, P. Orro, and S. Simon. Semialgebraic Sard Theorem for Generalized Critical Values. *Journal of Differential Geometry*, 56(1):67 – 92, 2000.

[Kri02] T. Krick. Straight-line programs in polynomial equation solving. *Foundations of computational mathematics: Minneapolis*, 312:96–136, 2002.

[Kro82] L. Kronecker. Grundzüge einer arithmetischen theorie der algebraischen grössen. pages 1–122, 1882.

[KRS16] A. Kobel, F. Rouillier, and M. Sagraloff. Computing Real Roots of Real Polynomials ... and Now For Real! In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, page 303–310, New York, NY, USA, 2016. Association for Computing Machinery.

[KS99] A. Kipnis and A. Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In M. Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, pages 19–30, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[KS12] M. Kerber and M. Sagraloff. A worst-case bound for topology computation of algebraic curves. *Journal of Symbolic Computation*, 47(3):239–258, 2012.

[KS15] A. Kobel and M. Sagraloff. On the complexity of computing with planar algebraic curves. *Journal of Complexity*, 31(2):206–236, 2015.

[Kun85] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Friedr. Vieweg & Sohn, 1985.

[Lag11] J. C. Lagarias, editor. *The Kepler Conjecture: The Hales-Ferguson Proof*. Springer, New York, NY, 1 edition, 2011.

[Lan02] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer, New York, NY, 3rd edition, 2002. Originally published by Addison-Wesley, 1993.

[Las01] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.

[Lat91] J.-C. Latombe. *Robot Motion Planning*. The Springer International Series in Engineering and Computer Science. Springer New York, NY, 1 edition, 1991.

[Lau98] J.-P. Laumond, editor. *Robot Motion Planning and Control*. Lecture Notes in Control and Information Sciences. Springer Berlin, Heidelberg, 1998.

[LaV06] S. M. LaValle. *Planning Algorithms*. Cambridge University Press, Cambridge, 2006.

[Laz83] D. Lazard. Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *Computer Algebra*, pages 146–156, Berlin, Heidelberg, 1983. Springer Berlin Heidelberg.

[Laz92] D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13(2):117–131, 1992.

[Laz94] D. Lazard. An improved projection for cylindrical algebraic decomposition. In C. L. Bajaj, editor, *Algebraic Geometry and its Applications: Collections of Papers from Shreeram S. Abhyankar's 60th Birthday Conference*, pages 467–476. Springer New York, New York, NY, 1994.

[Laz21] D. Lazard. Degree of a polynomial ideal and bézout inequalities. Preprint, 2021.

[Le21] H. P. Le. *On solving parametric polynomial systems and quantifier elimination over the reals : algorithms, complexity and implementations*. PhD thesis, Sorbonne Université, Paris, France, december 2021.

[Lec00] G. Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, ISSAC '00, page 209–216, New York, NY, USA, 2000. Association for Computing Machinery.

[Lec02] Lecerf, G. Kronecker, a Magma library for geometric polynomial solving , 1999–2002. (Not maintained).

[Lec03] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4):564–596, 2003.

[Lec12] Lecerf, G. Geomsolvex, a Mathemagix library for geometric polynomial system solving, 2012.

[LL91] Y. N. Lakshman and D. Lazard. On the complexity of zero-dimensional algebraic systems. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry*, pages 217–225. Birkhäuser Boston, Boston, MA, 1991.

[LMP08] C. Liang, B. Mourrain, and J.-P. Pavone. Subdivision methods for the topology of 2d and 3d implicit curves. In B. Jüttler and R. Piene, editors, *Geometric Modeling and Algebraic Geometry*, pages 199–214. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[Loj64] S. Lojasiewicz. Triangulation of semi-analytic sets. *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze*, 18(4):449–474, 1964.

[LRS04] C. Le Guernic, F. Rouillier, and M. Safey El Din. On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities. In L. Gonzalez-Vega and T. Recio, editors, *Proceedings of EACA'04 Conference*, 2004.

[LS93] R. Liska and S. Steinberg. Applying Quantifier Elimination to Stability Analysis of Difference Schemes. *The Computer Journal*, 36(5):497–503, 01 1993.

[LS21] H. P. Le and M. Safey El Din. Faster one block quantifier elimination for regular polynomial systems of equations. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, ISSAC '21, page 265–272, New York, NY, USA, 2021. Association for Computing Machinery.

[LS22] H. P. Le and M. Safey El Din. Solving parametric systems of polynomial equations over the reals through hermite matrices. *Journal of Symbolic Computation*, 112:25–61, 2022.

[LSdW20] H. P. Le, M. Safey El Din, and T. de Wolff. Computing the real isolated points of an algebraic hypersurface. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, ISSAC '20, page 297–304, New York, NY, USA, 2020. Association for Computing Machinery.

[Mac16] F. S. Macaulay. *The Algebraic Theory of Modular Systems*. Cambridge University Press, 1916.

[McC88] S. McCallum. An improved projection operation for cylindrical algebraic decomposition of three-dimensional space. *Journal of Symbolic Computation*, 5(1):141–161, 1988.

[Mil64] J. W. Milnor. On the betti numbers of real varieties. In *Proceedings of the American Mathematical Society*, pages 275–280, 1964.

[Mon75] L. Monk. *Elementary-recursive Decision Procedures*. PhD thesis, 1975.

[Mor22] G. Moroz. New data structure for univariate polynomial approximation and applications to root isolation, numerical multipoint evaluation, and other problems. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1090–1099, Los Alamitos, CA, USA, feb 2022. IEEE Computer Society.

[Mot70] T. S. Motzkin. The Real Solution Set of a System of Algebraic Inequalities is the Projection of a Hypersurface in One more Dimension. In O. Shisha, editor, *Proc. 1967 Symp. Inequalities II*, pages 251–254. New York: Academic Press, 1970.

[MPL23] Y. d. Mont-Marin, J. Ponce, and J.-P. Laumond. A minimum swept-volume metric structure for configuration space. In *2023 IEEE International Conference on Robotics and Automation (ICRA)*, pages 3686–3692, 2023.

[MR88] T. Mora and L. Robbiano. The gröbner fan of an ideal. *Journal of Symbolic Computation*, 6(2):183–208, 1988.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[MS06] M. Mezzarobba and M. Safey El Din. Computing roadmaps in smooth real algebraic sets. In *Transgressive Computing 2006*, pages 327–338, 2006.

[MSW15] K. Mehlhorn, M. Sagraloff, and P. Wang. From approximate factorization to root isolation with application to cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 66:34–69, 2015.

[Mum95] D. Mumford. *Algebraic geometry I*. Classics in Mathematics. Springer Science & Business Media, 1995.

[Nai21] A. S. Nair. *Curtains in Cylindrical Algebraic Decomposition*. PhD thesis, University of Bath, nov 2021.

[NS17] G. Nawratil and J. Schicho. Self-motions of pentapods with linear platform. *Robotica*, 35(4):832–860, 2017.

[Ole51] O. A. Oleinik. Estimates of the betti numbers of real algebraic hypersurfaces. *Mat. Sb. (N.S.)*, 28 (70):635–640, 1951.

[OP49] O. Oleinik and I. Petrovsky. On the topology of real algebraic surfaces. *Izvestiya Akademii Nauk SSSR*, 13:389–402, 1949.

[Par95] L. M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, M. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 33–69, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[PCI88] V. Parenti-Castelli and C. Innocenti. Position analysis of robot manipulators: Regions and subregions. In *Proceedings of 1988 conference on Advances in Robot Kinematics*, pages 151–158, Ljubljana, sep 1988.

[Per11] D. Perrucci. Linear solving for sign determination. *Theoretical Computer Science*, 412(35):4715–4720, 2011.

[Pie78] R. Piene. Polar classes of singular varieties. *Annales scientifiques de l'École Normale Supérieure*, Ser. 4, 11(2):247–276, 1978.

[Poh65] W. F. Pohl. Extrinsic complex projective geometry. In A. Aeppli, E. Calabi, and H. Röhrl, editors, *Proceedings of the Conference on Complex Analysis*, pages 18–29, Berlin, Heidelberg, 1965. Springer Berlin Heidelberg.

[Por71] I. R. Porteous. Todd's canonical classes. In C. Wall, editor, *Proceedings of Liverpool Singularities — Symposium I*, pages 308–312, Berlin, Heidelberg, 1971. Springer Berlin Heidelberg.

[PSS24] R. Prébet, M. Safey El Din, and E. Schost. Computing roadmaps in unbounded smooth real algebraic sets I: Connectivity results. *Journal of Symbolic Computation*, 120:102234, 2024.

[Rab30] J. Rabinowitsch. Zum Hilbertschen Nullstellensatz. *Mathematische Annalen*, 102:520–520, 1930.

[Rab97] P. J. Rabier. Ehresmann fibrations and palais-smale conditions for morphisms of finsler manifolds. *Annals of Mathematics*, 146(3):647–691, 1997.

[Rei79] J. H. Reif. Complexity of the mover's problem and generalizations. In *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)*, pages 421–427, 1979.

[Ren92] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. part i: Introduction. preliminaries. the geometry of semi-algebraic sets. the decision problem for the existential theory of the reals. *Journal of Symbolic Computation*, 13(3):255–299, 1992.

[Rob86] L. Robbiano. On the theory of graded structures. *Journal of Symbolic Computation*, 2(2):139–170, 1986.

[Roc18] D. S. Roche. What can (and can't) we do with sparse polynomials? In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, ISSAC '18, pages 25–30, New York, NY, USA, 2018. Association for Computing Machinery.

[Rou99] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. 9(5):433–461, 1999.

[Roy96] M.-F. Roy. Basic algorithms in real algebraic geometry and their complexity: from sturm's theorem to the existential theory of reals. In F. Broglia, editor, *Lectures in Real Geometry*, pages 1–68. De Gruyter, Berlin, Boston, 1996.

[RRS00] 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. *Journal of Complexity*, 16(4):716–750, 2000.

[RS90] M.-F. Roy and A. Szpirglas. Complexity of computation on real algebraic numbers. *Journal of Symbolic Computation*, 10(1):39–51, 1990.

[RS12] B. Roune and M. Stillman. Practical gröbner basis computation. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, page 203–210, New York, NY, USA, 2012. Association for Computing Machinery.

[RZ04] F. Rouillier and P. Zimmermann. Efficient isolation of polynomial's real roots. *Journal of Computational and Applied Mathematics*, 162(1):33–50, 2004. Proceedings of the International Conference on Linear Algebra and Arithmetic 2001.

[SA84] M. Sharir and E. Ariel-Sheffi. On the Piano Movers' problem: IV. Various decomposable two-dimensional motion-planning problems. *Communications on Pure and Applied Mathematics*, 37(4):479–493, 1984.

[Saf01] M. Safey El Din. *Résolution réelle des systèmes polynomiaux de dimension positive*. PhD thesis, Université Paris 6, January 2001.

[Saf05] M. Safey El Din. Finding sampling points on real hypersurfaces is easier in singular situations. In *MEGA 2005 - 8th International Symposium on Effective Methods in Algebraic Geometry*, may 2005.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, oct 1980.

[Sch03] É. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):349–393, Feb 2003.

[SED07] M. Safey El Din. Testing sign conditions on a multivariate polynomial and applications. *Mathematics in Computer Science*, 1(1):177–207, 2007.

[Sei54] A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, 60(2):365–374, 1954.

[Sev02] F. Severi. Sulle intersezioni delle varieta algebriche e sopra i loro caratteri e singolarita proiettive. *Mem. Accad. Sci. Torino*, 52(6):61–118, 1902.

[Sev32] F. Severi. La serie canonica e la teoria delle serie principali di gruppi di punti sopra una supericie algebrica. *Commentarii Mathematici Helvetici*, 4(1), 1932.

[Sha13] I. R. Shafarevich. *Basic algebraic geometry*, volume 1. Springer, 2013.

[Sil00] J. R. Silvester. Determinants of block matrices. *The Mathematical Gazette*, 84(501):460–467, 2000.

[SM16] M. Sagraloff and K. Mehlhorn. Computing real roots of real polynomials. *Journal of Symbolic Computation*, 73:46–86, 2016.

[SS83a] J. T. Schwartz and M. Sharir. On the "piano movers"' problem I. The case of a two-dimensional rigid polygonal body moving amidst polygonal barriers. *Communications on Pure and Applied Mathematics*, 36(3):345–398, 1983.

[SS83b] J. T. Schwartz and M. Sharir. On the Piano Movers' Problem: III. Coordinating the Motion of Several Independent Bodies: The Special Case of Circular Bodies Moving Amidst Polygonal Barriers. *The International Journal of Robotics Research*, 2(3):46–75, 1983.

[SS83c] J. T. Schwartz and M. Sharir. On the "piano movers" problem. II. General techniques for computing topological properties of real algebraic manifolds. *Advances in applied Mathematics*, 4(3):298–351, 1983.

[SS84] J. T. Schwartz and M. Sharir. On the piano movers' problem: V. The case of a rod moving in three-dimensional space amidst polyhedral obstacles. *Communications on Pure and Applied Mathematics*, 37(6):815–848, 1984.

[SS03a] M. Safey El Din and E. Schost. Polar Varieties and Computation of One Point in Each Connected Component of a Smooth Real Algebraic Set. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ISSAC '03, page 224–231, New York, NY, USA, 2003. Association for Computing Machinery.

[SS03b] 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*, ISSAC '03, page 240–247, New York, NY, USA, 2003. Association for Computing Machinery.

[SS04] M. Safey El Din and E. Schost. Properness defects of projections and computation of at least one point in each connected component of a real algebraic set. *Discrete & Computational Geometry*, 32(3):417–430, 2004.

[SS11] M. Safey El Din and É. Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete & Computational Geometry*, 45(1):181–220, 2011.

[SS17] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM (JACM)*, 63(6):1–37, 2017.

[SS18] M. Safey El Din and E. Schost. Bit complexity for multi-homogeneous polynomial system solving - Application to polynomial minimization. *Journal of Symbolic Computation*, 87:176–206, 2018.

[SSC+22] D. H. Salunkhe, C. Spartalis, J. Capco, D. Chablat, and P. Wenger. Necessary and sufficient condition for a generic 3R serial manipulator to be cuspidal. *Mechanism and Machine Theory*, 171:104729, 2022.

[SSH86] J. T. Schwartz, M. Sharir, and J. E. Hopcroft, editors. *Planning, Geometry, and Complexity of Robot Motion*. Ablex Publishing Corp., USA, 1986.

[Str06] A. W. Strzeboński. Cylindrical algebraic decomposition using validated numerics. *Journal of Symbolic Computation*, 41(9):1021–1038, 2006.

[SW05] R. Seidel and N. Wolpert. On the exact computation of the topology of real algebraic curves. In *Proceedings of the twenty-first annual symposium on Computational geometry*, pages 107–115, 2005.

[SYZ21] M. Safey El Din, Z.-H. Yang, and L. Zhi. Computing real radicals and s-radicals of polynomial systems. *Journal of Symbolic Computation*, 102:259–278, 2021.

[Tar51] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley, 1951.

[Tei82] B. Teissier. Varietes polaires ii multiplicites polaires, sections planes, et conditions de whitney. In J. M. Aroca, R. Buchweitz, M. Giusti, and M. Merle, editors, *Algebraic Geometry*, Berlin, Heidelberg, 1982. Springer Berlin Heidelberg.

[Tei88] B. Teisser. Quelques points de l'histoire des variétés polaires, de Poncelet à nos jours. *Sém. Annales Univ. Blaise Pascal*, 4, 1988.

[Tho65] R. Thom. Sur l'homologie des variétés algébriques réelles. In *Differential and Combinatorial Topology*, pages 255–265. Princeton Univ. Press, Princeton, NJ, 1965.

[Tiw10] A. Tiwari. Theory of reals for verification and synthesis of hybrid dynamical systems. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, page 5–6, New York, NY, USA, 2010. Association for Computing Machinery.

[Tod38] J. A. Todd. The arithmetical invariants of algebraic loci. volume 43, pages 190–225, 1938.

[Tra96] C. Traverso. Hilbert functions and the buchberger algorithm. *Journal of Symbolic Computation*, 22(4):355–376, 1996.

[Tra00] Q.-N. Tran. A fast algorithm for gröbner basis conversion and its applications. *Journal of Symbolic Computation*, 30(4):451–467, 2000.

[Tri78] W. Trinks. Über B. Buchbergers verfahren, systeme algebraischer gleichungen zu lösen. *Journal of Number Theory*, 10(4):475–488, 1978.

[VG90] N. Vorobjov and D. Y. Grigoriev. Determination of the number of connected components of a semi-algebraic set in subexponential time. *Dokl. Akad. Nauk SSSR*, 314(5), 1990.

[Wal78] R. J. Walker. *Algebraic curves*, volume 58. Springer New York, NY, 1978. Originally published by Princeton University Press, 1950.

[WC22] P. Wenger and D. Chablat. A Review of Cuspidal Serial and Parallel Manipulators. *Journal of Mechanisms and Robotics*, 15(4):040801, 11 2022.

[Wen92] P. Wenger. A New General Formalism for the Kinematic Analysis of All Nonredundant Manipulators. In *Proceedings of the 1992 IEEE International Conference on Robotics and Automation*, pages 442–447, Nice, France, May 1992.

[Wen97] P. Wenger. Design of cuspidal and noncuspidal manipulators. In *Proceedings of IEEE Int. Conf. Rob. and Aut.*, pages 2172–2177, 1997.

[Wen04] P. Wenger. Uniqueness Domains and Regions of Feasible Paths for Cuspidal Manipulators. *IEEE Transactions on Robotics*, 20(4):745–750, aug 2004.

[Wen07] P. Wenger. Cuspidal and noncuspidal robot manipulators. *Robotica*, 25(6):677–689, 2007.

[WEO96] P. Wenger and J. El Omri. Changing posture for cuspidal robot manipulators. In *Proceedings of IEEE International Conference on Robotics and Automation*, volume 4, pages 3173–3178, Minneapolis, MN, USA, 1996. IEEE.

[WR13] W. Wu and G. Reid. Finding points on real solution components and applications to differential polynomial systems. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, ISSAC '13, page 339–346, New York, NY, USA, 2013. Association for Computing Machinery.

[Wüt76] H. R. Wüthrich. Ein entscheidungsverfahren für die theorie der reell-abgeschlossenen körper. In V. Strassen, editor, *Komplexität von Entscheidungsproblemen Ein Seminar*, pages 138–162. Springer Berlin Heidelberg, Berlin, Heidelberg, 1976.

[YA07a] H. Yanami and H. Anai. The maple package synrac and its application to robust control design. *Future Generation Computer Systems*, 23(5):721–726, 2007.

[YA07b] H. Yanami and H. Anai. SyNRAC: A Maple Toolbox for Solving Real Algebraic Constraints. *ACM Commun. Comput. Algebra*, 41(3):112–113, sep 2007.

[YSCG22] A. G. Yabo, M. Safey El Din, J.-B. Caillau, and J.-L. Gouzé. Stability analysis of a bacterial growth model through computer algebra. Preprint, 2022.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In E. W. Ng, editor, *Symbolic and Algebraic Computation*, pages 216–226, Berlin, Heidelberg, 1979. Springer Berlin Heidelberg.