HAL
archives-ouvertes.fr

A baby steps/giant steps Monte Carlo algorithm for computing roadmaps in smooth compact real hypersurfaces

Mohab Safey El Din, Éric Schost

▶ **To cite this version:**

Mohab Safey El Din, Éric Schost. A baby steps/giant steps Monte Carlo algorithm for computing roadmaps in smooth compact real hypersurfaces. Journal of Discrete and Computational Geometry, Springer, 2011, 45 (1), pp.181-220. <10.1007/s00454-009-9239-2>. <inria-00359748>

HAL Id: inria-00359748
https://hal.inria.fr/inria-00359748

Submitted on 9 Feb 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

A baby steps/giant steps Monte Carlo algorithm for computing roadmaps in smooth compact real hypersurfaces

Mohab Safey El Din — Eric Schost

N° 6832

Février 2009

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--6832--FR+ENG

A baby steps/giant steps Monte Carlo algorithm for computing roadmaps in smooth compact real hypersurfaces

Mohab Safey El Din*, Eric Schost†

Thème SYM — Systèmes symboliques
Équipe-Projet SALSA

Rapport de recherche n° 6832 — Février 2009 — 29 pages

Abstract: We consider the problem of constructing roadmaps of real algebraic sets. The problem was introduced by Canny to answer connectivity questions and solve motion planning problems. Given s polynomial equations with rational coefficients, of degree D in n variables, Canny's algorithm has a Monte Carlo cost of $s^n \log(s) D^{O(n^2)}$ operations in $\mathbb{Q}$; a deterministic version runs in time $s^n \log(s) D^{O(n^4)}$. The next improvement was due to Basu, Pollack and Roy, with an algorithm of deterministic cost $s^{d+1} D^{O(n^2)}$ for the more general problem of computing roadmaps of semi-algebraic sets ($d \leq n$ is the dimension of an associated object).

We give a Monte Carlo algorithm of complexity $(nD)^{O(n^{1.5})}$ for the problem of computing a roadmap of a compact hypersurface V of degree D in n variables; we also have to assume that V has a finite number of singular points. Even under these extra assumptions, no previous algorithm featured a cost better than $D^{O(n^2)}$.

Key-words: real solutions of polynomial systems, connectivity decision, robot motion planning

* Université Pierre et Marie Curie, Mohab.Safey@lip6.fr
† University of Western Ontario, eschost@uwo.ca

Centre de recherche INRIA Paris – Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex (France)
Téléphone : +33 1 39 63 55 11 — Télécopie : +33 1 39 63 53 30

Algorithme pas de bébé/pas de géant pour le calcul de cartes routières d'ensembles algébriques réels compacts

Résumé : On considère le problème du calcul de cartes routières dans des ensembles algébriques réels. Ce problème est introduit par Canny pour répondre à des questions de connexité et résoudre des problèmes de planification de trajectoires. Étant données s équations polynomiales à coefficients rationnels, de degré D en n variables, l'algorithme Monte-Carlo de Canny a une complexité bornée par $s^n \log(s) D^{O(n^2)}$ opérations dans $\mathbb{Q}$; sa version déterministe a une complexité bornée par $s^n \log(s) D^{O(n^4)}$. L'amélioration suivante est dûe à Basu, Pollack and Roy, dont l'algorithme déterministe a u coût $s^{d+1} D^{O(n^2)}$ pour le problème plus général du calcul de cartes routières d'ensembles semi-algébriques ($d \leq n$ est la dimension d'un objet algébrique associé au semi-algébrique étudié).

On donne ici un algorithme Monte-Carlo de complexité bornée par $(nD)^{O(n^{1.5})}$ pour le calcul de cartes routières dans une hypersurface réelle compact $V \subset \mathbb{R}^n$ de degré D ayant un nombre fini de points singuliers. Sous ces hypothèses, aucun algorithme précédent n'a de coût meilleur que $D^{O(n^2)}$.

Mots-clés : solutions réelles de systèmes polynomiaux, connexité, planification de trajectoires

1 Introduction

Motivation. Deciding connectivity properties in a semi-algebraic set S is an important problem that appears in many fields, such as motion planning [26]. This general problem is reduced to computations in dimension 1, *via* the computation of a semi-algebraic curve $\mathscr{R}$, that we call a *roadmap*. This curve should have a non-empty and connected intersection with each connected component of S: then, connecting two points in S is done by connecting these points to $\mathscr{R}$. Also, counting the connected components of S is reduced to counting those of $\mathscr{R}$. Hence, a roadmap is used as the skeleton of connectivity decision routines for semi-algebraic sets. In addition to its direct interest, the computation of roadmaps is also used in more general algorithms allowing us to obtain semi-algebraic descriptions of the connected components of semi-algebraic sets [7, Ch.15-16]. Thus, improvements on the complexity of computing roadmaps impact the complexity of many fundamental procedures of effective real algebraic geometry.

Prior results. The notion of a roadmap was introduced by Canny in [10, 11]; the resulting algorithm constructs a roadmap of a semi-algebraic set $S \subset \mathbb{R}^n$ defined by k equations and s inequalities of degree bounded by D, but does not construct a path linking points of S. Its complexity is $s^n \log(s) D^{O(n^4)}$ arithmetic operations, and a Monte Carlo version of it runs in time $s^n \log(s) D^{O(n^2)}$ (to estimate running times, we always use arithmetic operations). Several subsequent works [18, 16] gave algorithms of cost $(sD)^{n^{O(1)}}$; they culminate with the algorithm of Basu, Pollack and Roy [5, 6] of cost $s^{d+1} D^{O(n^2)}$, where d is the dimension of the algebraic set defined by the k equations. These algorithms reduce the general problem to the construction of a roadmap in a bounded and smooth hypersurface defined by a polynomial f of degree D; the coefficient of f lie in a field $\mathbf{Q}$ that contains several infinitesimal quantities (it is a purely transcendental extension of $\mathbb{Q}$).

Under the smoothness and compactness assumptions, and even in the simpler case of a polynomial f with coefficients in $\mathbb{Q}$, none of the previous algorithms features a cost lower than $D^{O(n^2)}$ and none of them returns a roadmap of degree lower than $D^{O(n^2)}$. In this paper, we give the first known estimates of the form $(nD)^{O(n^{1.5})}$ for this particular problem, in terms of output degree and running time.

All these previous works, and ours also, make use of computations of critical loci of projections and rely on geometric connectivity results for correctness. Before recalling the basics we need about algebraic sets and critical loci, we give precise definitions of roadmaps and state our main result.

Definitions and main result. The original definition (found in [7]) is as follows. Let S be a semi-algebraic set. A *roadmap* for S (in the sense of [7]) is a semi-algebraic set $\mathscr{R}$ of dimension at most 1 contained in S which satisfies the following conditions:

- RM_1 Each connected component of S has a non-empty and connected intersection with $\mathscr{R}$.

RM$_2$ For $x \in \mathbb{R}$, each connected component of S_x intersect $\mathscr{R}$, where S_x is the set of points of the form $(x, x_2, \ldots, x_n)$ in S.

We modify this definition (in particular by discarding RM$_2$), for the following reasons. First, it is coordinate-dependent: if $\mathscr{R}$ is a roadmap of S, it is not necessarily true that $\phi(\mathscr{R})$ is a roadmap of $\phi(S)$, for a linear change of coordinates ϕ. Besides, one interest of RM$_2$ is to make it possible to connect two points in S by adding additional curves to $\mathscr{R}$: condition RM$_2$ is well-adjusted to the connecting procedure given in [7], which we do not use here.
Hence, we propose a modification in the definition of roadmaps. We do not deal with semi-algebraic sets, but only with sets of the form $V \cap \mathbb{R}^n$, where $V \subset \mathbb{C}^n$ is an algebraic set. Our definition, like the previous one, allows us to count connected components and to construct paths between points in $V \cap \mathbb{R}^n$. We generalize the definition to higher-dimensional "roadmaps", since our algorithm computes such objects. Thus, we say that an algebraic set $\mathscr{R} \subset \mathbb{C}^n$ is an i-roadmap of V if:

RM$'_1$ Each connected component of $V \cap \mathbb{R}^n$ has a non-empty and connected intersection with $\mathscr{R} \cap \mathbb{R}^n$.

RM$'_2$ The set $\mathscr{R}$ is contained in V.

RM$'_3$ The set $\mathscr{R}$ has dimension i.

If $\dim(\mathscr{R}) = 1$, we simply say that $\mathscr{R}$ is a roadmap of V. Finally, it will be useful to add a finite set of control points $\mathscr{P}$ to our input, e.g. to test if the points of $\mathscr{P}$ are connected on $V \cap \mathbb{R}^n$. Then, $\mathscr{R}$ is a i-roadmap of $(V, \mathscr{P})$ if we also have:

RM$'_4$ The set $\mathscr{R}$ contains $\mathscr{P}$.

Hereafter, given a finite set $\mathscr{P}$, we write its cardinality δ_P (if $\mathscr{P} = \emptyset$, we take $\delta_P = 1$).

Theorem 1. *Given $f \in \mathbb{Q}[X_1, \ldots, X_n]$ such that $V(f) \cap \mathbb{R}^n$ is compact and has a finite number of singular points, and given a subset $\mathscr{P}$ of $V(f)$ of cardinality δ_P, one can compute a roadmap of $(V(f), \mathscr{P})$ of degree $\delta_P (nD)^{O(n^{1.5})}$ in Monte Carlo time ${\delta_P}^{O(1)} (nD)^{O(n^{1.5})}$.*

The probabilistic aspects of our algorithm are twofold: first, we choose random changes of variables to ensure nice geometric properties. Second, we need to solve systems of polynomial equations; for our purpose, the algorithm with the best adapted cost [20] is probabilistic as well. Remark that we can also deterministically compute a roadmap of $(V(f), \mathscr{P})$ of degree $\delta_P (nD)^{O(n^{1.5})}$: exhaustive searches in a large enough sample set enable us to deterministically find suitable changes of variables; then, deterministic polynomial system solving algorithms replace the use of [20].

We expect in further work to apply our techniques to the case where the input polynomial has coefficients in a field that contains infinitesimal quantities: similar generalizations, based on the Transfer Principle, are in [7, Ch. 12]. We hope to obtain general roadmap algorithms for semi-algebraic sets of cost $s^{O(d)} (nD)^{O(n^{1.5})}$ (using the notation of the previous paragraphs).

Algebraic sets. To describe our contribution, we need a few definitions. We define most of the notation needed below; for standard notions not recalled here, see [30, 22, 27, 13]. An *algebraic set* $V \subset \mathbb{C}^n$ is the set of common zeros of some polynomial equations $f_1, \ldots, f_s$ in variables $X_1, \ldots, X_n$; we write $V = V(f_1, \ldots, f_s)$. The dimension of V is the Krull dimension of $\mathbb{C}[X_1, \ldots, X_n]/I$, where I is the ideal $\langle f_1, \ldots, f_s \rangle$ in $\mathbb{C}[X_1, \ldots, X_n]$. The set V can be uniquely decomposed into *irreducible* components, which are algebraic sets as well; when they all have the same dimension, we say that V is *equidimensional*. The *degree* of an irreducible algebraic set $V \subset \mathbb{C}^n$ is the maximum number of intersection points between V and a linear space of dimension $n - \dim(V)$; the degree of an arbitrary algebraic set is the sum of the degrees of its irreducible components.

The tangent space to V at $\mathbf{x} \in V$ is the vector space $T_{\mathbf{x}}V$ defined by the equations $\mathrm{grad}(f, \mathbf{x}) \cdot \mathbf{v} = 0$, for all polynomials f that vanish on V. When V is equidimensional, the *regular points* on V as those points $\mathbf{x}$ where $\dim(T_{\mathbf{x}}V) = \dim(V)$; more generally, the regular points are those where the local ring of V at $\mathbf{x}$ is regular of dimension d. The *singular points* are all other points. The set of regular (resp. singular) points is denoted by $\mathrm{reg}(V)$ (resp. $\mathrm{sing}(V)$). The set $\mathrm{sing}(V)$ is an algebraic subset of V, of smaller dimension than V.

Polar varieties. Canny's algorithm is the best known approach to computing roadmaps. Given an algebraic set V, it proceeds by computing some critical curves on V, and studying some distinguished points on these curves. One of our contributions is the use of higher-dimensional critical loci, called *polar varieties*, that were introduced by Todd [29] and studied from the algorithmic point of view in [3, 4]. For positive integers $i \leq n$, we denote by Π_i the projection

$$\begin{array}{rccc} \Pi_i : & \mathbb{C}^n & \to & \mathbb{C}^i \\ & \mathbf{x} = (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_i). \end{array}$$

Then, the polar variety w_i is the set of critical points of Π_i on $\mathrm{reg}(V)$, that is, the set of all points $\mathbf{x} \in \mathrm{reg}(V)$ such that $\Pi_i(T_{\mathbf{x}}V) \neq \mathbb{C}^i$. The set w_i may not be an algebraic set if V has singular points; in this case, however, the set $W_i = w_i \cup \mathrm{sing}(V)$ is algebraic. By abuse of notation, we still call it a polar variety and we write $W_i = \mathrm{crit}(\Pi_i, V)$. Its expected dimension is $i - 1$.

If V is given as $V(f_1, \ldots, f_p)$, is equidimensional of dimension $d = n - p$, and if the ideal $\langle f_1, \ldots, f_p \rangle$ is radical, then W_i is the zero-set of $(f_1, \ldots, f_p)$ and of all minors of size p taken from the jacobian matrix $\mathrm{jac}(\mathbf{F}, [X_{i+1}, \ldots, X_n])$ of $\mathbf{F}$ in $X_{i+1}, \ldots, X_n$.

Using polar varieties. Given f of degree D and $V = V(f)$, assuming $V(f) \cap \mathbb{R}^n$ is smooth and compact, Canny's algorithm computes the critical curve $W_2 = \mathrm{crit}(\Pi_2, V)$. The compactness assumption ensures that W_2 intersects each connected component of $V \cap \mathbb{R}^n$, but not that these intersections are connected. The solution consists in choosing a suitable family $\mathscr{E} = \{x_1, \ldots, x_N\} \subset \mathbb{R}$ so that the union of W_2 and $\mathscr{C}' = V \cap \Pi_1^{-1}(\mathscr{E})$ is an $(n-2)$-roadmap of V.

To realize this, Canny's algorithm uses the following connectivity result: defining the (expectedly finitely many) points $\mathscr{C} = W_1 \cup \mathrm{crit}(\Pi_1, W_2)$, and taking their projection $\mathscr{E} = \Pi_1(\mathscr{C})$ in the construction above gives an $(n-2)$-roadmap of V of degree $D^{O(n)}$. Then, the algorithm recursively constructs a roadmap in $\Pi_1^{-1}(\mathscr{E}) \cap V$ following the same process; this is geometrically equivalent to

a recursive call with input $f(x, X_2, \ldots, X_n)$ for all $x \in \mathscr{E}$. At each recursive call, the number of control points we compute is multiplied by $D^{O(n)}$, but the dimension of the input decreases by 1 only. Thus, the depth of the recursion is n and the roadmap we get has degree $D^{O(n^2)}$.

Our algorithm relies on a new connectivity result that generalizes the one described above. We want to avoid the degree growth by performing recursive calls on inputs whose dimension has decreased by $i \gg 1$. To this end, instead of considering, as Canny did, the polar curve W_2 associated to a projection on a plane, we use polar varieties W_i of higher dimension. As above, we have to consider suitable fibers $V \cap \Pi_{i-1}^{-1}(\mathbf{x})$ to repair the defaults of connectivity of W_i. To achieve this, we use the following new result (Theorem 2 below): define $\mathscr{C} = W_1 \cup \mathrm{crit}(\Pi_1, W_i)$ and $\mathscr{C}' = V \cap \Pi_{i-1}^{-1}(\Pi_{i-1}(\mathscr{C}))$; under some crucial (but technical) assumptions, $W_i \cup \mathscr{C}'$ is a $\max(i-1, n-i)$-roadmap of V. This leads to a more complex recursive algorithm; the optimal cut-off we could obtain that ensured all necessary assumptions has $i \simeq \sqrt{n}$.

Outline of the paper; basic notation. Our algorithm is described in the next section. The final two sections sketch the proofs of two key points: the connectivity result mentioned above, and the fact that generic changes of variables suffice to ensure the assumptions needed by this connectivity result.

If X is a subset of either $\mathbb{C}^n$ or $\mathbb{R}^n$, and if A is a subset of $\mathbb{R}$, we write $X_A = X \cap \Pi_1^{-1}(A) \cap \mathbb{R}^n$. For x in $\mathbb{R}$, we use the particular cases $X_{<x} = X_{]-\infty,x)}$, $X_x = X_{\{x\}}$, $X_{\leq x} = X_{]-\infty,x]}$. Hereafter, a property is called *generic* if it holds in a Zariski-open dense subset of the corresponding parameter space.

2 Algorithm

Even though we are interested in roadmaps for hypersurfaces, the recursive structure of the algorithm requires that we consider systems of the form $\mathbf{F} = (f_1, \ldots, f_p)$ in $\mathbb{Q}[X_1, \ldots, X_n]$. After stating our connectivity result, we give a modification of Canny's algorithm for such systems, then use it as a subroutine for our main algorithm.

2.1 Main connectivity result and sketch of the algorithm

We say that the system $\mathbf{F}$ satisfies assumption $\mathbf{H}$ if

(*a*) the ideal $\langle f_1, \ldots, f_p \rangle$ is radical;

(*b*) $V = V(f_1, \ldots, f_p)$ is equidimensional of dimension $d = n - p$;

(*c*) $\mathrm{sing}(V)$ is finite;

(*d*) $V \cap \mathbb{R}^n$ is bounded.

These conditions are independent of the choice of coordinates. Next, we fix i in $\{2, \ldots, d-1\}$ and we say that $\mathbf{F}$ satisfies condition $\mathbf{H}'$ if the following holds:

(*a*) $\dim(V) = d$ and the extension $\mathbb{C}[X_1, \ldots, X_d] \to \mathbb{C}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_p \rangle$ is integral (*i.e.* V is in Noether position for Π_d);

(*b*) W_i is in Noether position for Π_{i-1} (same definition as above);

(*c*) W_1 is finite;

(*d*) $\mathrm{crit}(\Pi_1, W_i)$ is finite.

We will see that these new assumptions can be ensured by a generic change of variables for some values of p and i (but not all). Finally, we consider a finite subset of points $\mathscr{P}$ in V, and we define

- $\mathscr{C} = W_1 \cup \mathrm{crit}(\Pi_1, W_i) \cup \mathscr{P}$, which is finite under **H** and **H′**;
- $\mathscr{C}' = V \cap \Pi_{i-1}^{-1}(\Pi_{i-1}(\mathscr{C}))$, so that $\mathbf{x} \in V$ is in $\mathscr{C}'$ if and only if $\Pi_{i-1}(\mathbf{x})$ is in $\Pi_{i-1}(\mathscr{C})$.

The following theorem is proved in the next section; it is the key to our algorithms.

Theorem 2. *Let $d' = \max(i-1, d-i+1)$. Under assumptions* **H** *and* **H′**, *the following holds:*

1. *$\mathscr{C}' \cup W_i$ is a d'-roadmap of $(V, \mathscr{P})$;*
2. *$\mathscr{C}' \cap W_i$ is finite;*
3. *for all $\mathbf{x} \in \mathbb{C}^{i-1}$, the system $(f_1, \ldots, f_p, X_1 - x_1, \ldots, X_{i-1} - x_{i-1})$ satisfies assumption* **H**.

The idea of the algorithm is to compute W_i, the finite sets $\mathscr{C}$ and $\mathscr{C}' \cap W_i$ and to recursively compute roadmaps of $\mathscr{C}'$ and W_i, if their dimension is too high. For $\mathscr{C}'$, this will be possible by point 3 of the theorem, but for W_i this will be more delicate, since we may not be able to enforce **H**; this will restrict our choices for i and dictate the structure of the algorithm. The correctness of this recursive process follows from the following lemma.

Lemma 3. *With notation as above, if $\mathscr{R}_1$ and $\mathscr{R}_2$ are roadmaps of respectively $(W_i, (\mathscr{C}' \cap W_i) \cup \mathscr{P})$ and $(\mathscr{C}', (\mathscr{C}' \cap W_i) \cup \mathscr{P})$, then $\mathscr{R}_1 \cup \mathscr{R}_2$ is a roadmap of $(V, \mathscr{P})$.*

2.2 Preliminaries to the algorithms

Data representation. The outputs of our algorithms are sets of *rational parametrizations* of algebraic curves: if $\mathcal{C} \subset \mathbb{C}^n$ is an algebraic curve defined over $\mathbb{Q}$, such a parametrization consists in polynomials $Q = (q, q_0, \ldots, q_n)$ in $\mathbb{Q}[U, T]$ and two linear forms $\tau = \tau_1 X_1 + \cdots + \tau_n X_n$, $\eta = \eta_1 X_1 + \cdots + \eta_n X_n$ with coefficients in $\mathbb{Q}$, such that $\mathcal{C}$ is the Zariski closure of the set defined by

$$q(\eta, \tau) = 0, \qquad X_i = \frac{q_i(\eta, \tau)}{q_0(\eta, \tau)} \ \ (1 \le i \le n), \qquad q_0(\eta, \tau) \neq 0.$$

The degree of the curve $\mathcal{C}$ is written δ_Q; then, all polynomials in Q can be taken of degree $\delta_Q^{O(1)}$. By a slight abuse of language, we will say that a family of 1-dimensional parametrizations is a roadmap of a set V if the union of the curves they define is.

Finally, internally to the algorithm, we use a similar notion for 0-dimensional (*i.e.* finite) sets of points; then, all polynomials involved are univariate, and a

single linear form is needed [15, 23]. In this case, we write δ_Q for the number of points described by Q. If Q represents a set of points in $\mathbb{C}^e$ in variables $X_1, \ldots, X_e$, we write $Q(X_1, \ldots, X_e)$.

Quantities carried through recursive calls. To accommodate the recursive nature of the algorithm, we take as input a pair $[\mathbf{F}, Q]$, where $\mathbf{F}$ is as before and $Q(X_1, \ldots, X_e)$ is a 0-dimensional parametrization. We are interested in roadmaps of $V(\mathbf{F}, Q)$; this means that we restrict $X_1, \ldots, X_e$ to a finite number of possible values, that are solutions of Q

In this new context, we define analogues of $\mathbf{H}$ and $\mathbf{H}'$. Assumption $\mathbf{H}$ remains unchanged for $[\mathbf{F}, Q]$, up to replacing $V(\mathbf{F})$ by $V(\mathbf{F}, Q)$ and $n - p$ by $n - p - e$. To state $\mathbf{H}'$, for $\mathbf{x} = (x_1, \ldots, x_e)$ in $V(Q)$, we define $\mathbf{F}_\mathbf{x} = \mathbf{F}(x_1, \ldots, x_e, Y_1, \ldots, Y_{n-e}) \in \mathbb{C}[Y_1, \ldots, Y_{n-e}]$, for some new variables $Y_1, \ldots, Y_{n-e}$. Then we say that $[\mathbf{F}, Q]$ satisfies $\mathbf{H}'$ if for all $\mathbf{x}$ in $V(Q)$, $\mathbf{F}_\mathbf{x}$ satisfies $\mathbf{H}'$.

Subroutines. We use a function Solve for solving 0- and 1-dimensional polynomial systems; the result is a rational parametrization of the solutions. If the input has s equations of degree at most D (with $D \geq 1$), the algorithm of [20] performs this task in time $sD^{O(n)}$. The function Union (resp. Projection) computes a parametrization of the union (resp. a projection) of two (resp. one) 0-dimensional sets given by parametrizations; on inputs of degree at most δ, this takes time $\delta^{O(1)}$. Finally, we need algorithms for computing critical points, on two slightly different kinds of inputs:

- Given a parametrization R of a curve $\mathcal{C}$ in $\mathbb{C}^n$, CriticalPointsCurve(R, X_j) computes $\mathrm{crit}(\Pi_{X_j}, \mathcal{C})$, where Π_{X_j} is the projection on the X_j-axis. Due to the nice shape of our parametrizations, this can be done in time $\delta_R^{O(1)}$.
- Given a system $[\mathbf{F}, Q]$ that satisfies $\mathbf{H}$, CriticalPoints$(\mathbf{F}, X_j)$ computes $\mathrm{crit}(\Pi_{X_j}, V(\mathbf{F}, Q))$. This time, assumption $\mathbf{H}$ makes it possible to use directly the Jacobian matrix of $\mathbf{F}$ to perform this operation; this can be done in time $\delta_Q^{O(1)}(nD)^{O(n)}$.

2.3 Canny's algorithm revisited

We start with an algorithm close to Canny's. As opposed to Canny, we do not work with a single equation but with a system $\mathbf{F} = f_1, \ldots, f_p$ that satisfies $\mathbf{H}$; as Canny, we take $i = 2$ in the recursion. Indeed, given such a system, we will see that it is possible to ensure assumption $\mathbf{H}'$ through a generic change of variables for $i = 2$, but not for $i > 2$. As said above, we take a 0-dimensional parametrization $Q(X_1, \ldots, X_e)$ as input as well; then, our change of variables φ will leave $X_1, \ldots, X_e$ fixed and we denote by $\mathrm{GL}(n, e)$ the subset of $\mathrm{GL}_n(\mathbb{Q})$ satisfying this constraint. Our last input are the control points $\mathscr{P}$, given in the form of a 0-dimensional parametrization P.

Lemma 4. *Suppose that* $[\mathbf{F}, Q]$ *satisfies* $\mathbf{H}$*. After a generic change of variables in* $\mathrm{GL}(n, e)$*, the system* $[\mathbf{F}, Q]$ *satisfies* $\mathbf{H}$ *and* $\mathbf{H}'$ *for* $i = 2$*.*

CannyRoadmap$(\mathbf{F}, Q, P)$.

0. If $n - p - e = 1$, return Solve$([\mathbf{F}, Q])$
1. Apply a random change of variables $\varphi \in \mathrm{GL}(n, e)$

2. Let $\Delta = [p\text{-minors of jac}(\mathbf{F}, [X_{e+2}, \ldots, X_n])]$ and $\Delta' = [p\text{-minors of jac}(\mathbf{F}, [X_{e+3}, \ldots, X_n])]$
3. Let $R = \mathsf{Solve}([\mathbf{F}, \Delta, Q])$ and $R' = \mathsf{Solve}([\mathbf{F}, \Delta', Q])$
4. Let $S = \mathsf{CriticalPointsCurve}(R', X_{e+1})$
5. Let $Q' = \mathsf{Projection}(\mathsf{Union}([S, R, P]), [X_1, \ldots, X_{e+1}])$
6. Let $P' = \mathsf{Union}(\mathsf{Solve}([\mathbf{F}, \Delta', Q']), P)$
7. Let $R'' = \mathsf{CannyRoadmap}(\mathbf{F}, Q', P')$ (e increases by 1)
8. Undo the change of variables φ and return (R', R'')

To understand the algorithm, it is easier to consider that Q is empty and thus $e = 0$. Under $\mathbf{H}$ and $\mathbf{H}'$, the sets R and R' respectively describe W_1 and W_2, and S describes $\mathrm{crit}(\Pi_1, W_2)$. Then, Q' encodes the set $\Pi_1(\mathscr{C})$ of Subsection 2.1, and P' is the new set of control points $(\mathscr{C}' \cap W_1) \cup \mathscr{P}$. The algebraic set $V(\mathbf{F}, Q')$ equals $\mathscr{C}'$, to which we recursively apply $\mathsf{CannyRoadmap}$. Since R' describes W_2 and W_2 is a curve, there is no need to process it further, and we append it to the output.

Lemma 5. $\mathsf{CannyRoadmap}$ *computes a roadmap of* $(V(\mathbf{F}, Q), \mathscr{P})$ *of degree* $(\delta_Q + \delta_P)(nD)^{O(n(n-p-e))}$ *in Monte Carlo time* $(\delta_Q + \delta_P)^{O(1)}(nD)^{O(n(n-p-e))}$.

Once $\mathbf{H}$ and $\mathbf{H}'$ hold, correctness follows from Theorem 2; the domain where we pick φ is discussed in appendix p. 27. To estimate runtime, one first notes that the cost of steps $0 - 6$ is $(\delta_Q + \delta_P)^{O(1)}(nD)^{O(n)}$, and that we have $\delta_{Q'} + \delta_{P'} \leq (\delta_Q + \delta_P)(nD)^{O(n)}$. Since the depth of the recursion is $n - p - e$, this proves our claims. Remark that for $e = 0$ and $p = 1$, we recover Canny's result.

2.4 Main algorithm

We finally give our roadmap algorithm for a hypersurface $V(f)$, where f satisfies assumption $\mathbf{H}$. Here, we can ensure assumption $\mathbf{H}'$ in generic coordinates for many more choices of i. Using our modified version of Canny's algorithm, we obtain a baby steps/giant steps strategy by choosing $i \simeq \sqrt{n}$. As before, we also take a 0-dimensional parametrization $Q(X_1, \ldots, X_e)$ as input, and the control points $\mathscr{P}$ by means of a 0-dimensional parametrization P.

$\mathsf{Roadmap}(f, Q, P)$.

0. If $n - p - e \leq \sqrt{n}$, return $\mathsf{CannyRoadmap}(f, Q, P)$
1. Let $i = \lfloor \sqrt{n} \rfloor$
2. Apply a random change of variables $\varphi \in \mathrm{GL}(n, e)$.
3. Let $\Delta = [\partial f / \partial X_i \mid i \in [e+2, \ldots, n]]$, $\Delta' = [\partial f / \partial X_i \mid i \in [e+i+1, \ldots, n]]$ and $\mathbf{F} = (f, \Delta')$
4. Let $R = \mathsf{Solve}([f, \Delta, Q])$.
5. Let $S = \mathsf{CriticalPoints}([\mathbf{F}, Q], X_{e+1})$
6. Let $Q' = \mathsf{Projection}(\mathsf{Union}([S, R, P]), [X_1, \ldots, X_{e+i-1}])$

7. Let $P' = \mathsf{Union}(\mathsf{Solve}([\mathbf{F}, Q']), P)$
8. Let $R'' = \mathsf{CannyRoadmap}(\mathbf{F}, Q, P')$
9. Let $R''' = \mathsf{Roadmap}(f, Q', P')$ (e increases by $\lfloor\sqrt{n}\rfloor$)
10. Undo the change of variables φ and return (R'', R''')

Lemma 6. (using the notation of the algorithm) *Suppose that* $[f, Q]$ *satisfies* $\mathbf{H}$. *For* $i \leq n-p-e-1$, *after a generic change of variables in* $\mathrm{GL}(n, e)$, $[f, Q]$ *satisfies* $\mathbf{H}$ *and* $\mathbf{H}'$ *and* $[\mathbf{F}, Q]$ *satisfies* $\mathbf{H}$.

As before, we explain the computations with Q empty, so $e = 0$. Under $\mathbf{H}$ and $\mathbf{H}'$, R describes W_1 and S describes $\mathrm{crit}(\Pi_1, W_i)$; we do not actually compute a parametrization for W_i, since the equations $\mathbf{F}$ are well adapted for this computation. Then, Q' encodes the set $\Pi_{i-1}(\mathscr{C})$ of Subsection 2.1, and P' is the new set of control points $(\mathscr{C}' \cap W_i) \cup \mathscr{P}$. The equations (f, Q') describe $\mathscr{C}'$, to which we recursively apply $\mathsf{Roadmap}$. The equations $\mathbf{F}$ describe W_i, to which we apply the algorithm $\mathsf{CannyRoadmap}$ of the last section (this is valid, since $\mathbf{F}$ satisfies $\mathbf{H}$).

Lemma 7. $\mathsf{Roadmap}$ *computes a roadmap of* $(V(f, Q), \mathscr{P})$ *of degree* $(\delta_Q + \delta_P)(nD)^{O(n^{1.5})}$ *in Monte Carlo time* $(\delta_Q + \delta_P)^{O(1)}(nD)^{O(n^{1.5})}$.

As for $\mathsf{CannyRoadmap}$, correctness follows from Theorem 2. Initially, we take Q and P of degrees δ_Q and δ_P. After r recursive calls, we have $e \simeq r\sqrt{n}$, the degrees of the "local" Q and P have order $(\delta_Q+\delta_P)(nD)^{O(nr)}$, and the cost of the computation is $(\delta_Q + \delta_P)^{O(1)}(nD)^{O(nr)}$. We enter the function $\mathsf{CannyRoadmap}$ with $n-p-e \simeq \sqrt{n}$, so the cost of this call is $(\delta_Q+\delta_P)^{O(1)}(nD)^{O(nr)}(nD)^{O(n^{1.5})}$, and the degree its output is $(\delta_Q + \delta_P)(nD)^{O(nr)}(nD)^{O(n^{1.5})}$. Since the depth of the recursion is $r = O(\sqrt{n})$, this gives the result claimed in the introduction.

3 Proof of the connectivity result

We sketch the proof of the first point of Theorem 2. We focus on the connectivity property RM'_1, which is the hardest; the missing arguments are in appendix.

We reuse here the notation of Theorem 2 and we let $\mathscr{R} = \mathscr{C}' \cup W_i$. For x in $\mathbb{R}$, we say that property $\mathbf{P}(x)$ holds if for any connected component C of $V_{\leq x}$, $C \cap \mathscr{R}$ is non empty and connected. We will prove that for all x in $\mathbb{R}$, $\mathbf{P}(x)$ holds; taking $x \geq \max_{\mathbf{y} \in V \cap \mathbb{R}^n} \Pi_1(\mathbf{y})$ gives our result. To do so, we let $v_1 < \cdots < v_\ell$ be the projections $\Pi_1(v)$, for v in $\mathscr{C} \cap \mathbb{R}^n$ (recall that $\mathscr{C}$ is finite). The proof uses two intermediate results:

- if $\mathbf{P}(v_j)$ holds, then for x in (v_j, v_{j+1}), then $\mathbf{P}(x)$ holds;
- for x in $\mathbb{R}$, if $\mathbf{P}(x')$ holds for all $x' < x$, then $\mathbf{P}(x)$ holds.

Since for $x < \min_{\mathbf{y} \in V \cap \mathbb{R}^n} \Pi_1(\mathbf{y})$, property $\mathbf{P}(x)$ vacuously holds, the combination of these two results gives the claim above by an immediate induction.

As preliminaries, we consider an algebraic set $Z \subset \mathbb{C}^n$; for $x \in \mathbb{R}$, we are interested in the properties of the connected components of $Z_{<x}$ in the neighborhood of the hyperplane $\Pi_1^{-1}(x)$. The following result actually holds for Z in C^n, where C is the algebraic closure of a real closed field R.

Lemma 8. *Let x be in $\mathbb{R}$ and let $\gamma : A \to Z_{\leq x} - Z_x \cap \mathrm{crit}(\Pi_1, Z)$ be a continuous semi-algebraic map, where $A \subset \mathbb{R}^k$ is a non-empty connected semi-algebraic set. Then there exists a unique connected component B of $Z_{<x}$ such that $\gamma(A) \subset \overline{B}$.*

We continue with a statement in the vein of Morse's Lemma A [7, Th. 7.5]. The proof uses Ehresmann's fibration theorem (which relies on the integration of vector fields), so we need here our base fields to be $\mathbb{R}$ and $\mathbb{C}$.

Lemma 9. *Suppose that $\dim(Z) > 0$ and that $Z \cap \mathbb{R}^n$ is compact. Let $v < w$ be in $\mathbb{R}$ such that $Z_{(v,w]} \cap \mathrm{crit}(\Pi_1, Z) = \emptyset$, and let C be a connected component of $Z_{\leq w}$. Then, for all x in $[v, w]$, $C_{\leq x}$ is a connected component of $Z_{\leq x}$.*

We can then prove our claims. We start by the easier case: extending $\mathbf{P}$ from v_j to (v_j, v_{j+1}).

Lemma 10. *Let j be in $\{1, \ldots, \ell - 1\}$. If $\mathbf{P}(v_j)$ holds, then for x in (v_j, v_{j+1}), $\mathbf{P}(x)$ holds.*

Proof. Let x be in (v_j, v_{j+1}) and let C be a connected component of $V_{\leq x}$. We have to prove that $C \cap \mathscr{R}$ is non-empty and connected. We first establish that $C_{\leq v_j} \cap \mathscr{R}$ is non-empty and connected. Because there is no point in W_1 in $V_{(v_j,x]}$, applying Lemma 9 to V above the interval $(v_j, x]$ shows that $C_{\leq v_j}$ is a connected component of $V_{\leq v_j}$. So, using property $\mathbf{P}(v_j)$, we see that $C_{\leq v_j} \cap \mathscr{R}$ is non-empty and connected, as needed.

Next, we prove that for any connected component D of $C \cap W_i$, $D_{\leq v_j}$ is non-empty (and connected). Clearly, D is a connected component of $W_{i \leq x}$. Recall that W_i is an algebraic set of positive dimension, with $W_i \cap \mathbb{R}^n$ compact; besides, $\mathrm{crit}(\Pi_1, W_i)$ is empty above $(v_j, x]$. Applying Lemma 9 to $Z = W_i$, we see that $D_{\leq v_j}$ is non-empty (and connected).

To prove that $C \cap \mathscr{R}$ is connected, we prove that any $\mathbf{y}$ in $C \cap \mathscr{R}$ can be connected to a point in $C_{\leq v_j} \cap \mathscr{R}$ by a path in $C \cap \mathscr{R}$. This is sufficient to conclude, since we have seen that $C_{\leq v_j} \cap \mathscr{R}$ is connected. Let thus $\mathbf{y}$ be in $C \cap \mathscr{R}$. If $\mathbf{y}$ is in $C_{\leq v_j} \cap \mathscr{R}$, we are done. If $\mathbf{y}$ is in $C_{(v_j,x]} \cap \mathscr{R}$, it is actually in $C_{(v_j,x]} \cap W_i$, since $\mathscr{R}$ and W_i coincide above $(v_j, x]$. Let thus D be the connected component of $C \cap W_i$ containing $\mathbf{y}$. By the result of the previous paragraph, there exists a continuous path connecting $\mathbf{y}$ to a point $\mathbf{y}'$ in $D_{\leq v_j}$ by a path in D. Since D is in $C \cap \mathscr{R}$, we are done. □

Lemma 11. *Let x be in $\mathbb{R}$ such that for all $x' < x$, $\mathbf{P}(x')$ holds. Then $\mathbf{P}(x)$ holds.*

Proof. Let C be a connected component of $V_{\leq x}$; we have to prove that $C \cap \mathscr{R}$ is connected. If $\dim(C) = 0$, we are done, since C is a point and $C \cap \mathscr{R}$ is connected as it is non-empty (one checks that C is in W_1). Hence, we assume that $\dim(C) > 0$; from this, one deduces that $C_{<x}$ is not empty. Let then $B_1, \ldots, B_r$ be the connected components of $C_{<x}$; Lemma 24 (in appendix) proves that for $i \leq r$, $\overline{B_i} \cap \mathscr{R}$ is non-empty and connected.

Since $\overline{B_1} \cap \mathscr{R}$ is non-empty and contained in $C \cap \mathscr{R}$, the latter is non-empty. Let thus finally $\mathbf{y}_1$ and $\mathbf{y}_2$ be in $C \cap \mathscr{R}$; we need to connect them by a path in $C \cap \mathscr{R}$. Let $\gamma : [0, 1] \to C$ be a continuous semi-algebraic path that connects $\mathbf{y}_1$ to $\mathbf{y}_2$, and let $G = \gamma^{-1}(C_x \cap W_1)$ and $H = [0, 1] - G$. The connected components $g_1, \ldots, g_N$ of G are intervals and closed in $[0, 1]$ (and may be reduced to single

points); the connected components $h_1, \ldots, h_M$ of H are intervals that are open in $[0,1]$. Besides, these intervals are interleaved in $[0,1]$. For $1 \leq i \leq M$, we write $\ell_i = \inf(h_i)$ and $r_i = \sup(h_i)$; we also introduce $r_0 = 0$ and $\ell_{M+1} = 1$. To conclude the proof, we establish that:

1. for $1 \leq i \leq M$, $\gamma(\ell_i)$ and $\gamma(r_i)$ can be connected by a semi-algebraic path in $C \cap \mathscr{R}$;
2. for $0 \leq i \leq M$, $\gamma(r_i)$ and $\gamma(\ell_{i+1})$ can be connected by a semi-algebraic path in $C \cap \mathscr{R}$.

We prove the first point (the second one is easier). For $1 \leq i \leq M$, we first claim that there exists $j \leq r$ such that $\gamma(h_i)$ is in $\overline{B_j}$. Indeed, remark that since $\gamma(h_i)$ avoids $C_x \cap W_1$, it actually avoids the whole $V_x \cap W_1$ (because $\gamma(h_i)$ is contained in C). It follows from Lemma 8 that there exists a connected component B_j of $V_{<x}$ such that $\gamma(h_i) \subset \overline{B_j}$. Since γ is continuous, both $\gamma(\ell_i)$ and $\gamma(r_i)$ are in $\overline{B_j}$. On the other hand, both $\gamma(\ell_i)$ and $\gamma(r_i)$ are in $\mathscr{R}$. We justify it for ℓ_i: either $\ell_i = 0$, and we are done (because $\gamma(0) = \mathbf{y}$ is in $\mathscr{R}$), or $\ell_i > 0$, so that ℓ_i is in some interval g_ℓ (since then it does not belong to h_i), and thus $\gamma(\ell_i)$ is in $W_1 \subset \mathscr{R}$. Because $\overline{B_j} \cap \mathscr{R}$ is connected, $\gamma(\ell_i)$ and $\gamma(r_i)$ can be connected by a path in $\overline{B_j} \cap \mathscr{R}$, which is contained in $C \cap \mathscr{R}$. □

4 Proof of the genericity properties

The algorithms of Subsections 2.3 and 2.4 rely on the fact that assumption $\mathbf{H}'$ holds in generic coordinates. We discuss here the two cases we need (Lemmas 4 and 6) in the simplified case where Q is empty (the arguments carry over to the general cases). Thus, we let $\mathbf{F} = f_1, \ldots, f_p$ be a system that satisfies $\mathbf{H}$; recall that Lemma 4 discusses p arbitrary, and Lemma 6 has $p = 1$.

In both cases, in generic coordinates, W_i has dimension $i-1$ for all $i = 1, \ldots, n-p$ [3, 4]. Then, points (a) and (b) of assumption $\mathbf{H}'$ are established in [24] when $\mathrm{sing}(V) = \emptyset$. Since the assumption $\mathrm{sing}(V) = \emptyset$ was only used to ensure that W_i had dimension $i-1$, we obtain (a) and (b) in our case as well. Point (c) says that W_1 is finite; this follows from the previous claim with $i = 1$. Point (d), which says that in generic coordinates $\mathrm{crit}(\Pi_1, W_i)$ is finite, is the most delicate of these properties; in the general case where p and i are arbitrary, we do not know whether it always holds.

In Subsection 2.3, we have p arbitrary and $i = 2$: in this case, W_2 is generically a curve in Noether position for Π_1; this easily implies point (d), and thus finishes the proof of Lemma 4. In Subsection 2.4, for Lemma 6, we need the case where $p = 1$ and i is arbitrary. This turns out to be substantially harder; we sketch the proof in what follows.

We work with the parameter space $\mathbb{C}^i \times \mathbb{C}^{ni}$; to an element $(\mathbf{g}, \mathbf{e})$ of $\mathbb{C}^i \times \mathbb{C}^{ni}$, with $\mathbf{e} = (\mathbf{e}_1, \ldots, \mathbf{e}_i)$ and all $\mathbf{e}_k$ in $\mathbb{C}^n$, we associate the linear maps

$$\Pi_{\mathbf{e}} : \begin{array}{ccc} \mathbb{C}^n & \to & \mathbb{C}^i \\ \mathbf{x} = (x_1, \ldots, x_n) & \mapsto & (\mathbf{e}_1 \cdot \mathbf{x}, \ldots, \mathbf{e}_i \cdot \mathbf{x}) \end{array} \quad \text{and} \quad \rho_{\mathbf{g}} : \begin{array}{ccc} \mathbb{C}^i & \to & \mathbb{C} \\ \mathbf{y} = (y_1, \ldots, y_i) & \mapsto & \mathbf{g} \cdot \mathbf{y}. \end{array}$$

We also define $W_{\mathbf{e}} = \mathrm{crit}(\Pi_{\mathbf{e}}, V)$. We will prove that for a generic $\mathbf{e}$, $\mathrm{sing}(W_{\mathbf{e}})$ and $\mathrm{crit}(\rho_{\mathbf{g}_0} \circ \Pi_{\mathbf{e}}, W_{\mathbf{e}})$ are finite, with $\mathbf{g}_0 = (1, 0, \ldots, 0)$. Changing the coordinates to bring $\mathbf{e}$ to the first i unit vectors gives point (d) of assumption $\mathbf{H}'$ for Lemma 6 (the last statement of this lemma is discussed hereafter).

For $\mathbf{e} \in \mathbb{C}^{ni}$ and $i+1 \leq \ell \leq n$, let M_ℓ be the $(i+1)$-minor built on columns $1, \ldots, i, \ell$ of the matrix

$$\mathbf{M_e} = \begin{bmatrix} \mathbf{e}_1^t \\ \vdots \\ \mathbf{e}_i^t \\ \mathrm{grad}(f) \end{bmatrix}.$$

We say that property $\mathbf{a}_1(\mathbf{e})$ is satisfied if the following holds: $W_\mathbf{e}$ is the zero-set of $(f, M_{i+1}, \ldots, M_n)$, the Jacobian matrix of $(f, M_{i+1}, \ldots, M_n)$ has rank $n-i+1$ at all points of $W_\mathbf{e} - \mathrm{sing}(V)$, $W_\mathbf{e}$ is $(i-1)$-equidimensional and $\mathrm{sing}(W_\mathbf{e})$ is finite. Note that after changing coordinates to bring $\mathbf{e}$ to the first i unit vectors, this property implies the last claim of Lemma 6.

For $0 \leq j \leq i$, define next $S_j = \{\mathbf{x} \in \mathrm{reg}(V) \mid \dim(\Pi_\mathbf{e}(T_\mathbf{x}V)) = j\}$. The sets S_j form a partition of $\mathrm{reg}(V)$; we say that property $\mathbf{a}_2(\mathbf{e})$ is satisfied if for $j = 0, \ldots, i$, S_j is either empty or a non-singular constructible subset of $\mathrm{reg}(V)$. If $\mathbf{a}_2(\mathbf{e})$ holds, let $m(n,i,j) = \max(0, \dim(S_j) - n + 1 + j)$ and $M(n,i,j) = \dim(S_j)$. Then for $m(n,i,j) \leq \ell \leq M(n,i,j)$, define finally

$$S_{j,\ell} = \{\mathbf{x} \in S_j \mid \dim(\Pi_\mathbf{e}(T_\mathbf{x}S_j)) = \ell\}.$$

Under $\mathbf{a}_2(\mathbf{e})$, the sets $S_{j,\ell}$ form a partition of S_j. Then, property $\mathbf{a}_3(\mathbf{e})$ holds if for $j = 0, \ldots, i$ and $\ell = m(n,i,j), \ldots, M(n,i,j)$, $S_{j,\ell}$ is either empty or a non-singular constructible subset of S_j. The sets S_j and $S_{j,\ell}$ can be rewritten in terms of the standard notation of Thom-Boardman strata [28, 8]. Hence, Mather's transversality result for projections [21, 2, 1] implies the following lemma.

Lemma 12. *For a generic* $\mathbf{e}$ *in* $\mathbb{C}^{ni}$*, properties* $\mathbf{a}_1(\mathbf{e})$*,* $\mathbf{a}_2(\mathbf{e})$ *and* $\mathbf{a}_3(\mathbf{e})$ *are satisfied, and the inequality* $\dim(S_{j,\ell}) \leq \ell$ *holds for* $\ell \leq i-1$ *and* $m(n,i,j) \leq \ell \leq M(n,i,j)$*.*

Let now $\mathbf{E} = (\mathbf{E}_1, \ldots, \mathbf{E}_i)$ be ni indeterminates, that stand for the vectors $\mathbf{e} = (\mathbf{e}_1, \ldots, \mathbf{e}_i)$ and let $\mathbf{G} = (G_1, \ldots, G_i)$ be indeterminates for $\mathbf{g} = (g_1, \ldots, g_i)$. Let J be the Jacobian matrix of the polynomials $(f, M_{i+1}, \ldots, M_n)$, where we take partial derivatives in the variables $\mathbf{X}$ only. Let further $\mathbf{r}$ be the row vector of length n given by

$$\mathbf{r} = \begin{bmatrix} G_1 & \cdots & G_i \end{bmatrix} \begin{bmatrix} \mathbf{E}_1^t \\ \vdots \\ \mathbf{E}_i^t \end{bmatrix},$$

and let finally J' be the matrix obtained by adjoining the row $\mathbf{r}$ to J. We define the algebraic set $X \subset \mathbb{C}^i \times \mathbb{C}^{ni} \times \mathbb{C}^n$ as the set of all $(\mathbf{g}, \mathbf{e}, \mathbf{x}) \in \mathbb{C}^i \times \mathbb{C}^{ni} \times \mathbb{C}^n$ such that $f(\mathbf{x}) = M_{i+1}(\mathbf{x}, \mathbf{e}) = \cdots = M_n(\mathbf{x}, \mathbf{e}) = 0$ and all $(n+2-i)$-minors of $J'(\mathbf{g}, \mathbf{e}, \mathbf{x})$ vanish. Finally, we define the projections $\alpha : (\mathbf{g}, \mathbf{e}, \mathbf{x}) \mapsto (\mathbf{g}, \mathbf{e})$ and $\gamma : (\mathbf{g}, \mathbf{e}, \mathbf{x}) \mapsto \mathbf{e}$.

Lemma 13. *If* $\mathbf{a}_1(\mathbf{e})$*,* $\mathbf{a}_2(\mathbf{e})$ *and* $\mathbf{a}_3(\mathbf{e})$ *holds, then* $X \cap \gamma^{-1}(\mathbf{e})$ *has dimension at most* i

Let finally $Y \subset \mathbb{C}^i \times \mathbb{C}^{ni}$ be the Zariski closure of the set of all $(\mathbf{g}, \mathbf{e}) \in \mathbb{C}^i \times \mathbb{C}^{ni}$ such that the fiber $X \cap \alpha^{-1}(\mathbf{g}, \mathbf{e})$ is infinite. Lemma 13 is the key to the following result.

Lemma 14. *The set Y is a strict algebraic subset of $\mathbb{C}^i \times \mathbb{C}^{ni}$ and for $(\mathbf{g}, \mathbf{e})$ in $\mathbb{C}^i \times \mathbb{C}^{ni} - Y$, $\mathrm{crit}(\rho_{\mathbf{g}} \circ \Pi_{\mathbf{e}}, W_{\mathbf{e}})$ is finite.*

For any invertible $i \times i$ matrix $\mathbf{M}$, the defining equations of X are multiplied by a non-zero constant through the change of variables $(\mathbf{G}, \mathbf{E}, \mathbf{X}) \mapsto (\mathbf{M}^{-1}\mathbf{G}, \mathbf{ME}, \mathbf{X})$, so X is stabilized by this action. Thus, a point $(\mathbf{g}, \mathbf{e})$ in $\mathbb{C}^i \times \mathbb{C}^{ni}$ belongs to Y if and only if $(\mathbf{M}^{-1}\mathbf{g}, \mathbf{Me})$ does. One deduces that all points of Y locally look the same: since there exists a point $(\mathbf{g}, \mathbf{e})$ not in Y, and since Y is closed, there exists an open set $A \subset \{\mathbf{g}_0\} \times \mathbb{C}^{ni}$ such that $A \cap Y = \emptyset$, with $\mathbf{g}_0 = (1, 0, \ldots, 0)$; this is what we wanted.

References

[1] A. Alzati, E. Ballico, and G. Ottaviani. The theorem of Mather on generic projections for singular varieties. *Geom. Dedicata*, 85(1-3):113–117, 2001.

[2] A. Alzati and G. Ottaviani. The theorem of Mather on generic projections in the setting of algebraic geometry. *Manuscripta Math.*, 74(4):391–412, 1992.

[3] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

[4] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

[5] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets (extended abstract). In *STOC*, pages 168–173. ACM, 1996.

[6] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety. *Journal of the AMS*, 3(1):55–82, 1999.

[7] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, second edition, 2006.

[8] J. M. Boardman. Singularities of differentiable maps. *Publ. Math. Inst. Hautes Études Sci.*, 33:21–57, 1967.

[9] J.-P. Brasselet, J. Damon, L. D. Trang, and M. Oka, editors. *Singularities in geometry and topology*. World Scientific, 2007.

[10] J. Canny. *The complexity of robot motion planning*. PhD thesis, MIT, 1987.

[11] J. Canny. Computing roadmaps in general semi-algebraic sets. *The Computer Journal*, 36(5):504–514, 1993.

[12] J. Della Dora, C. Discrescenzo, and D. Duval. About a new method method for computing in algebraic number fields. In *EUROCAL 85 Vol. 2*, volume 204 of *LNCS*. Springer, 1985.

[13] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[14] N. Fitchas, M. Giusti, and F. Smietanski. Sur la complexité du théorème des zéros. In *Approximation and Optimization in the Caribbean II*, volume 8 of *Approximation and Optimization*, pages 247–329. Verlag Peter Lang, 1995.

[15] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In *Computational Algebraic Geometry and Commutative Algebra*, volume XXXIV of *Symposia Matematica*, pages 216–256. Cambridge University Press, 1993.

[16] L. Gournay and J.-J. Risler. Construction of roadmaps in semi-algebraic sets. *Appl. Alg. Eng. Comm. Comp.*, 4(4):239–252, 1993.

[17] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.

[18] J. Heintz, M.-F. Roy, and P. Solerno. Single exponential path finding in semi-algebraic sets II: The general case. In *Algebraic geometry and its applications, collections of papers from Abhyankar's 60-th birthday conference.* Purdue University, West-Lafayette, 1994.

[19] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute (extended abstract). In *STOC*, pages 262–272. ACM, 1980.

[20] G. Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *ISSAC'00*, pages 209–216. ACM, 2000.

[21] J. N. Mather. Generic projections. *Ann. of Math.*, 98:226–245, 1973.

[22] D. Mumford. *Algebraic Geometry I, Complex projective varieties.* Classics in Mathematics. Springer Verlag, 1976.

[23] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[24] M. Safey el Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *ISSAC'03*, pages 224–231. ACM, 2003.

[25] É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(5):349–393, 2003.

[26] J. Schwarz and M. Sharir. On the piano mover's problem II: General techniques for computing topological properties of real algebraic manifolds. *Adv. Appl. Math.*, 4:298–351, 1983.

[27] I. Shafarevich. *Basic Algebraic Geometry 1.* Springer Verlag, 1977.

[28] R. Thom. Les singularités des applications différentiables. *Ann. Inst. Fourier*, 6:43–87, 1955-56.

[29] J. A. Todd. The arithmetical invariants of algebraic loci. *Proc. Lond. Math. Soc.*, 43:190–225, 1937.

[30] O. Zariski and P. Samuel. *Commutative algebra.* Van Nostrand, 1958.

Appendix

We give the proofs of several of the results announced before; we usually do not repeat the necessary definitions, so we indicate to which page the reader should refer. We mostly follow the order in which the statements are made in the text; in a few cases, we modify the order to avoid excessive cross-referencing.

Completion of the proof of Theorem 2 on page 7

Lemma 15. *Let* $\mathbf{F} = (f_1, \ldots, f_p)$ *be a system that satisfies assumption* $\mathbf{H}$*, and let* $i \leq n - p$*. For all* $\mathbf{x} = (x_1, \ldots, x_{i-1})$ *in* $\mathbb{R}^{i-1}$*, the system* $\mathbf{F}_x = (f_1, \ldots, f_p, X_1 - x_1, \ldots, X_{i-1} - x_{i-1})$ *satisfies the following properties:*

- *the ideal* $I_{\mathbf{x}} = \langle \mathbf{F}_{\mathbf{x}} \rangle$ *is radical;*
- *the variety* $V_{\mathbf{x}}$ *it defines is equidimensional of dimension* $n - p - (i-1)$*;*
- $\mathrm{sing}(V_{\mathbf{x}})$ *is finite;*
- $V_{\mathbf{x}} \cap \mathbb{R}^n$ *is bounded.*

Besides, $V_{\mathbf{x}}$ *intersects* $W_i = \mathrm{crit}(\Pi_i, V(\mathbf{F}))$ *in finitely many points.*

Proof. Remark that $V_{\mathbf{x}}$ is either empty or of dimension at least $n - p - (i-1)$, by Krull's theorem. Let us show that it is not empty: since $V = V(\mathbf{F})$ is in Noether position for Π_d, for any $\mathbf{x}' = (x_1, \ldots, x_d)$, $\Pi_d^{-1}(\mathbf{x}') \cap V$ is not empty. A fortiori, $\Pi_{i-1}^{-1}(\mathbf{x}) \cap V$ is not empty, and thus all irreducible components of $V_{\mathbf{x}}$ have dimension at least $n - p - (i-1)$.

Let $\mathbf{y}$ be in $V_{\mathbf{x}}$. By construction, the Jacobian of $(f_1, \ldots, f_p, X_1 - x_1, \ldots, X_{i-1} - x_{i-1})$ has full rank if and only if $\mathbf{y}$ is in $W_i = W_i \cup \mathrm{sing}(V)$. However, since W_i is in Noether position for Π_{i-1}, $W_i \cap \Pi_{i-1}^{-1}(\mathbf{x})$ is finite (which gives the last assertion). Since $\mathrm{sing}(V)$ is finite as well, and since $n - p - (i-1) \geq 1$, each irreducible component of $V_{\mathbf{x}}$ contains a point $\mathbf{y}$ where the former Jacobian matrix has full rank. Consequently, we deduce that each irreducible component of $I_{\mathbf{x}}$ has dimension $n - p - (i-1)$ (by the Jacobian criterion) and that $I_{\mathbf{x}}$ is radical (by Macaulay's unmixedness theorem). We have thus established the first two points.

As a consequence, the singular points of $V_{\mathbf{x}}$ are the points where the rank of the former Jacobian drops; as we have seen, they are in $W_i \cap \Pi_{i-1}^{-1}(\mathbf{x})$, and thus in finite number. This gives the third point. The next point is obvious, since $V_{\mathbf{x}} \cap \mathbb{R}^n \subset V \cap \mathbb{R}^n$, and the latter is bounded. □

We can now complete the proof of Theorem 2. We start by proving that $\mathscr{C}' \cup W_i$ is a d'-roadmap of $(V, \mathscr{P})$. The connectivity property RM'_1 is established in Section 3. Property RM'_2 is clear from the construction. Next, the dimension of W_i is at most $i-1$ by point (b) of $\mathbf{H}'$. We have seen in the previous lemma that all fibers $\Pi_{i-1}^{-1} \cap V$ have dimension $n - p - (i-1)$; because $\mathscr{C}$ is finite by assumption $\mathbf{H}'$, this implies that $\dim(\mathscr{C}') = n - p - (i-1)$, and thus that $\dim(\mathscr{R}) = d'$. Thus, we have RM'_3. Finally, by construction, $\mathscr{P}$ is contained in $\mathscr{C}$, so obtain RM'_4.

The last propriety we need is that $\mathscr{C}' \cap W_i$ has dimension at most zero: this is the last assertion of the previous lemma.

Proof of Lemma 3 on page 7

We prove the following claim: *Suppose that $\mathscr{R}_1 \cup \mathscr{R}_2$ is a j-roadmap of $(V, \mathscr{P})$, with $\mathscr{R}_1 \cap \mathscr{R}_2$ finite. Let $\mathscr{R}'_1$ and $\mathscr{R}'_2$ be roadmaps of respectively $(\mathscr{R}_1, (\mathscr{R}_1 \cap \mathscr{R}_2) \cup \mathscr{P})$ and $(\mathscr{R}_2, (\mathscr{R}_1 \cap \mathscr{R}_2) \cup \mathscr{P})$. Then $\mathscr{R}'_1 \cup \mathscr{R}'_2$ is a roadmap of $(V, \mathscr{P})$.*

Lemma 16. *If $\mathscr{R}$ is an i-roadmap of V, then for each connected component C of $V \cap \mathbb{R}^n$, $C \cap \mathscr{R}$ is a connected component of $\mathscr{R} \cap \mathbb{R}^n$.*

Proof. We know that $C \cap \mathscr{R}$ is connected. Besides, C is both open and closed in $V \cap \mathbb{R}^n$, so that $C \cap \mathscr{R}$ is open and closed in $\mathscr{R} \cap \mathbb{R}^n$. □

Lemma 17. *If $\mathscr{R}$ is an i-roadmap of V and if $\mathscr{R}'$ is a j-roadmap of $\mathscr{R}$ then $\mathscr{R}'$ is a j-roadmap of V.*

Proof. Since the dimension of $\mathscr{R}'$ is j, it is sufficient to prove that for each connected component C of $V \cap \mathbb{R}^n$, $C \cap \mathscr{R}'$ is non empty and connected. Since $\mathscr{R}$ is a roadmap of V, $C \cap \mathscr{R}$ is a connected component of $\mathscr{R} \cap \mathbb{R}^n$ (Lemma 16). Since $\mathscr{R}'$ is a roadmap of $\mathscr{R}$, $C \cap \mathscr{R} \cap \mathscr{R}' = C \cap \mathscr{R}'$ is a connected component of $\mathscr{R}' \cap \mathbb{R}^n$. □

We can now prove our claim. By Lemma 17, it is sufficient to prove that $\mathscr{R}'_1 \cup \mathscr{R}'_2$ is a roadmap of $\mathscr{R}_1 \cup \mathscr{R}_2$. Let C be a connected component of $\mathscr{R}_1 \cup \mathscr{R}_2$. First, we prove that $C \cap (\mathscr{R}'_1 \cup \mathscr{R}'_2)$ is not empty. Indeed, C contains a connected component of either $\mathscr{R}_1$ or $\mathscr{R}_2$ (since it contains a point of say $\mathscr{R}_1$, it contains its connected component); and as such, C intersects either $\mathscr{R}'_1$ or $\mathscr{R}'_2$.

We prove now that $C \cap (\mathscr{R}'_1 \cup \mathscr{R}'_2)$ is connected. Consider a couple of points $\mathbf{x}, \mathbf{y}$ in $C \cap (\mathscr{R}'_1 \cup \mathscr{R}'_2)$. Since C is connected, there exists a continuous path $\gamma : [0,1] \to C$ such that $\gamma(0) = \mathbf{x}$ and $\gamma(1) = \mathbf{y}$. Since $\mathscr{R}_1 \cap \mathscr{R}_2$ is finite, we can reparametrize γ, to ensure that $\gamma^{-1}(\mathscr{R}_1 \cap \mathscr{R}_2)$ is finite. Denote by $t_1 < \cdots < t_r$ the set $\gamma^{-1}(\mathscr{R}_1 \cap \mathscr{R}_2)$ and let $t_0 = 0$ and $t_{r+1} = 1$. Then, we replace γ by a continuous path γ' defined on the segments $[t_i, t_{i+1}]$ as follows:

- For $1 \leq i < r$, $\gamma((t_i, t_{i+1}))$ is connected and contained in $\mathscr{R}_1 \cup \mathscr{R}_2 - \mathscr{R}_1 \cap \mathscr{R}_2$, so it is contained in (say) $\mathscr{R}_1$. By continuity, $\gamma([t_i, t_{i+1}])$ is contained in $\mathscr{R}_1$, and thus actually in a connected component C_i of $\mathscr{R}_1$, with $C_i \subset C$. Both $\gamma(t_i)$ and $\gamma(t_{i+1})$ are in $\mathscr{R}_1 \cap \mathscr{R}_2$, and thus in $\mathscr{R}'_1 \cap \mathscr{R}'_2$, and in particular in $\mathscr{R}'_1$. Since by definition $C_i \cap \mathscr{R}'_1$ is connected, there exists a continuous semi-algebraic path $\gamma' : [t_i, t_{i+1}] \to C_i \cap \mathscr{R}'_1$ with $\gamma'(t_i) = \gamma(t_i)$ and $\gamma'(t_{i+1}) = \gamma(t_{i+1})$.
- The case $i = 0$ needs to be taken care of only if $t_0 < t_1$, so that $\mathbf{x} = \gamma(t_0)$ is either in $\mathscr{R}_1$ or in $\mathscr{R}_2$, but not in both. As before, we start by remarking that $\gamma([t_0, t_1])$ is contained in a connected component C_0 of say $\mathscr{R}_1$, with $C_0 \subset C$. This implies that $\mathbf{x} = \gamma(t_0)$ is in $\mathscr{R}_1$; since $\mathbf{x}$ is in $\mathscr{R}'_1 \cup \mathscr{R}'_2$, it is actually in $\mathscr{R}'_1$. As before, $\gamma(t_1)$ is in $\mathscr{R}'_1$, and the conclusion follows as in the previous case. The case $i = r$ is dealt with similarly.

Proof of Lemma 8 on page 11

The following lemma is similar to Proposition 7.3 in [7]; the proof is a consequence of the semi-algebraic implicit function theorem. Hereafter, the closure notation $\overline{B}$ refers to the closure for the Euclidean topology.

Lemma 18. *Let* $\mathbf{x}$ *be in* $Z \cap \mathbb{R}^n - W_1$ *and let* $x_1 = \Pi_1(\mathbf{x})$. *There exists an open, semi-algebraic, connected neighborhood* $X(\mathbf{x})$ *of* $\mathbf{x}$ *such that* $X(\mathbf{x}) \cap Z_{<x_1}$ *is non-empty and connected, and* $X(\mathbf{x}) \cap Z_{x_1}$ *is contained in* $\overline{X(\mathbf{x}) \cap Z_{<x_1}}$.

Lemma 19. *Let* $\mathbf{y}$ *be in* $Z \cap \mathbb{R}^n - W_1$ *and let* $y_1 = \Pi_1(\mathbf{y})$. *There exists a unique connected component* $B(\mathbf{y})$ *of* $Z_{<y_1}$ *such that* $X(\mathbf{y}) \cap Z_{<y_1} \subset B(\mathbf{y})$. *Besides,* $B(\mathbf{y})$ *is the unique connected component of* $Z_{<y_1}$ *such that* $\mathbf{y}$ *is in* $\overline{B(\mathbf{y})}$.

Proof. Because $X(\mathbf{y}) \cap Z_{<y_1}$ is non-empty and connected (Lemma 18), it is contained in a connected component $B(\mathbf{y})$ of $Z_{<y_1}$. The connected components of $Z_{<y_1}$ are pairwise disjoint, so $B(\mathbf{y})$ is well-defined. By Lemma 18 again, $\mathbf{y}$ is in $\overline{X(\mathbf{y}) \cap Z_{<y_1}}$, and thus in $\overline{B(\mathbf{y})}$. Suppose finally that $\mathbf{y}$ is in $\overline{B'}$, for another connected component B' of $Z_{<y_1}$. Then, there exists a point of B' in $X(\mathbf{y})$, because $X(\mathbf{y})$ is open. This point is in $X(\mathbf{y}) \cap Z_{<y_1}$, and thus in $B(\mathbf{y})$ as well, a contradiction. □

Lemma 20. *Let* $\mathbf{y}$ *be in* $Z \cap \mathbb{R}^n - W_1$ *and let* $y_1 = \Pi_1(\mathbf{y})$. *For* $\mathbf{y}'$ *in* $X(\mathbf{y}) \cap (Z_{y_1} \cap \mathbb{R}^n - W_1)$, *we have* $B(\mathbf{y}') = B(\mathbf{y})$.

Proof. The reasoning is the same as in the previous lemma. We know that $\mathbf{y}'$ is in $\overline{B(\mathbf{y}')}$. Since $\mathbf{y}'$ is in $X(\mathbf{y})$ and $X(\mathbf{y})$ is open, there exists a point of $B(\mathbf{y}')$ in $X(\mathbf{y}) \cap Z_{<y_1}$. This point is in $B(\mathbf{y})$ as well, so $B(\mathbf{y}') = B(\mathbf{y})$. □

Lemma 21. *Let* x *be in* $\mathbb{R}$ *and let* γ *be a continuous semi-algebraic map* $A \to Z_x - W_1$, *where* $A \subset \mathbb{R}^k$ *is a connected set. Then, there exists a unique connected component* B *of* $Z_{<x}$ *such that for all* $\mathbf{a} \in A$, $\gamma(\mathbf{a}) \in \overline{B}$.

Proof. By Lemma 20, the map $\mathbf{a} \mapsto B(\gamma(\mathbf{a}))$ is locally constant, so it is constant. So, with $B = B(\gamma(\mathbf{a}_0))$, for some $\mathbf{a}_0$ in A, we have $B(\gamma(\mathbf{a})) = B$ for all $\mathbf{a}$ in A, and thus $\gamma(\mathbf{a}) \in \overline{B}$ for all $\mathbf{a}$ by Lemma 19. Uniqueness is a consequence of the second part of Lemma 19. □

We can now prove Lemma 8. Let thus γ be a continuous semi-algebraic map $A \to Z_{\leq x} - Z_x \cap W_1$, where $A \subset \mathbb{R}^k$ is a connected semi-algebraic set; we prove that $\gamma(A)$ is contained in the closure $\overline{B}$ of a connected component B of $Z_{<x}$. If $\gamma(A)$ is contained in $Z_{<x}$, then, since it is connected, it is contained in a uniquely defined connected component B of $Z_{<x}$, and we are done.

Else, let $G = \gamma^{-1}(Z_x)$, which is closed in A. We decompose it into its connected components $G_1, \ldots, G_N$. Because all G_i are closed in G, they are closed in A. Let also $H_1, \ldots, H_M$ be the connected components of $A - G$; hence, the H_j are open in A (because they are open in $A - G$, which is open in A). The sets G_i and H_j form a partition of A; we assign them some connected components of $Z_{<x}$.

- Since G_i is connected and $\gamma(G_i)$ is contained in $Z_x - W_1$, Lemma 21 shows that there exists a unique connected component $B(G_i)$ of $Z_{<x}$ such that for all $\mathbf{g}$ in G_i, $\gamma(\mathbf{g}) \in \overline{B(G_i)}$.
- Since H_j is connected and $\gamma(H_j)$ is contained in $Z_{<x}$, there exists a unique connected component $B(H_j)$ of $Z_{<x}$ that contains $\gamma(H_j)$. Since γ is continuous, for all $\mathbf{h}$ in the closure $\overline{H_j}$ of H_j in A, we still have $\gamma(\mathbf{h}) \in \overline{B(H_j)}$.

Since the sets G_i and H_j form a partition of A, we deduce from the previous construction a function $\mathbf{a} \mapsto B(\mathbf{a})$ in the obvious manner: if $\mathbf{a}$ is in G_i, we let $B(\mathbf{a}) = B(G_i)$; if $\mathbf{a}$ is in H_j, we let $B(\mathbf{a}) = B(H_j)$. It remains to prove that this function is constant on G; then, if we let B be the common value $B(\mathbf{a})$, for all $\mathbf{a}$ in G, $\gamma(\mathbf{a})$ is in $\overline{B}$ by construction (uniqueness is clear). To do so, it is sufficient to prove that for any $\mathbf{a}$ in A, there exists a neighborhood $N(\mathbf{a})$ of $\mathbf{a}$ such that for all $\mathbf{a}'$ in $N(\mathbf{a})$, $B(\mathbf{a}) = B(\mathbf{a}')$.

- If $\mathbf{a}$ is in some H_j, we are done, since H_j is open, and $\mathbf{a} \mapsto B(\mathbf{a})$ is constant on H_j.
- Else, $\mathbf{a}$ is in some G_i. Remark that $\mathbf{a}$ is the closure of no other $G_{i'}$, since the G_i are closed; however, $\mathbf{a}$ can belong to the closure of some H_j. For definiteness, let J be the set of indices such that $\mathbf{a}$ is in $\overline{H_j}$ for j in J, and let $e > 0$ be such that the open ball $B(\mathbf{a}, e)$ intersects no $G_{i'}$, for $i' \neq i$, and no $\overline{H_j}$, for j not in J. Since $\mathbf{a}$ is in G_i, we know that $\gamma(\mathbf{a})$ is in $\overline{B(G_i)}$; for j in J, since $\mathbf{a}$ is in $\overline{H_j}$, we also have that $\gamma(\mathbf{a})$ is in $\overline{B(H_j)}$. However, since $\gamma(\mathbf{a})$ is in $Z_x - W_1$, the second statement in Lemma 19 implies that $B(G_i) = B(H_j)$. Since every $\mathbf{a}'$ in $B(\mathbf{a}, e)$ is either in G_i or in some H_j with j in J, we are done.

This concludes the proof of Lemma 8. The following corollary will be used to prove Lemma 9.

Corollary 22. *Let x be in $\mathbb{R}$ such that $Z_x \cap W_1 = \emptyset$ and let C be a connected component of $Z_{\leq x}$. Then if $C_{<x}$ is non-empty, it is connected.*

Proof. Consider the inclusion map $C \to Z_{\leq x}$. Since $Z_x \cap W_1$ is empty, this map satisfies the assumptions of Proposition 8; this implies that there exists a unique connected component B of $Z_{<x}$ such that $C \subset \overline{B}$. This equality implies that $C_{<x}$ is contained in $\overline{B}_{<x}$; one easily checks that $B = \overline{B}_{<x}$, so that $C_{<x} \subset B$. Now, let B' be a connected component of $C_{<x}$, so that B' is actually a connected component of $Z_{<x}$. The inclusion $B' \subset C_{<x}$ implies $B' \subset C_{<x} \subset B$ and thus $B' = C_{<x} = B$. Since B is connected, $C_{<x}$ is, as claimed. □

Proof of Lemma 9 on page 11

Lemma 9 is a by-product of the following result.

Lemma 23. *Let $v < w$ be in $\mathbb{R}$ and let $A \subset (-\infty, w) \times \mathbb{R}^{n-1}$ be a connected, bounded semi-algebraic set such that $A_{(v,w)}$ is a non-empty, smooth manifold, closed in $(v, w) \times \mathbb{R}^{n-1}$ and such that Π_1 is a submersion on $A_{(v,w)}$. Then, for all x in $[v, w)$, $A_{\leq x}$ is non-empty and connected.*

First, we deduce Lemma 9 from Lemma 23. Let C be a connected component of $Z_{\leq w}$ and recall that we want to prove that for x in $[v, w]$, $C_{\leq x}$ is a connected component of $Z_{\leq x}$; of course, we can assume that $x < w$. Then, it suffices to prove that $C_{\leq x}$ is non-empty and connected; then it is a easily seen to be a connected component of $Z_{\leq x}$. If $C_{(v,w]}$ is empty, then for x in $[v, w)$, $C_{\leq x} = C$, so we are done. Hence, we assume that $C_{(v,w]}$ is non empty.

We verify here that all assumptions of Lemma 23 are satisfied, with $A = C_{<w}$. Since $C_{(v,w]}$ is non empty and $Z_w \cap W_1$ is empty, $C_{(v,w)}$ is non-empty:

either there is a point in $C_{(v,w)}$, or there is a point in C_w; this point is not in W_1, so the implicit function theorem shows that $C_{(v,w)}$ is not empty in this case as well. Besides, since $Z_w \cap W_1$ is empty, by Corollary 22, $C_{<w}$ is connected.

To summarize, $C_{<w}$ is a connected and bounded semi-algebraic set; $C_{(v,w)}$ is smooth and of positive dimension (because there is no point in W_1 in $C_{(v,w)}$), closed in $(v,w) \times \mathbb{R}^{n-1}$ (because $C_{(v,w)} = C \cap ((v,w) \times \mathbb{R}^{n-1})$ and C is closed). Besides, we claim that Π_1 is a submersion on $C_{(v,w)}$. First, remark that any point $\mathbf{x}$ of $C_{(v,w)}$, $T_{\mathbf{x}}C_{(v,w)} = T_{\mathbf{x}}Z \cap \mathbb{R}^n$. Since $\dim(Z) > 0$, and since there is no point of W_1 on $Z_{(v,w)}$, we know that $\Pi_1(T_{\mathbf{x}}Z) = \mathbb{C}$, which implies that $\Pi_1(T_{\mathbf{x}}Z \cap \mathbb{R}^n) = \mathbb{R}$. This establishes that Π_1 is a submersion on $C_{(v,w)}$. We can thus apply Lemma 23, which implies that $C_{\leq x}$ is non-empty and connected, as requested.

Hence, we are left to prove Lemma 23. Let us first check that $\Pi_1 : A_{(v,w)} \to (v,w)$ is a proper mapping for the topology induced by the Euclidean topology. By assumption, there exists a closed set $X \subset \mathbb{R}^n$ such that $A_{(v,w)} = X \cap ((v,w) \times \mathbb{R}^{n-1})$; since A is bounded, we can take X bounded as well. Let K be a compact set in (v,w), so that K is compact in $\mathbb{R}$ too. Then, $\Pi_1^{-1}(K) \cap A_{(v,w)} = X \cap (K \times \mathbb{R}^{n-1})$, which is compact in $\mathbb{R}^n$, and thus in $A_{(v,w)}$. So $\Pi_1 : A_{(v,w)} \to (v,w)$ is proper.

Let $\zeta \in (v,w)$ be such that A_ζ is not empty (such a ζ exists by assumption). We apply Ehresmann's fibration theorem [9, Th. 3.4] to the projection Π_1 (which is a proper submersion on $A_{(v,w)}$); this gives us a smooth diffeomorphism of the form

$$\begin{array}{rccc} \Psi : & A_{(v,w)} & \to & (v,w) \times A'_\zeta \\ & (\alpha, \mathbf{a}) & \mapsto & (\alpha, \psi(\alpha, \mathbf{a})), \end{array}$$

where $A'_\zeta \subset \mathbb{R}^{n-1}$ is the set $\{(x_2, \ldots, x_n) \mid (\zeta, x_2, \ldots, x_n) \in A_\zeta\}$ (recall that A_ζ lies in $\mathbb{R}^n$). For the whole length of this proof, vectors of the form $(\alpha, \mathbf{a})$ have α in $\mathbb{R}$ and $\mathbf{a}$ in $\mathbb{R}^{n-1}$.

We use Ψ to show that for $v < x < w$, $A_{\leq x}$ is non-empty and connected. Let thus x be fixed in (v,w), and let $(\zeta, \mathbf{z})$ be in A_ζ. Remark that $\Psi^{-1}(x, \mathbf{z})$ is in A_x, proving that $A_{\leq x}$ is non-empty. To prove connectedness, we use a similar process. Let $\mathbf{y}_0$ and $\mathbf{y}_1$ be in $A_{\leq x}$. Since A is connected, there exists a continuous path $\gamma : [0,1] \to A$, with $\gamma(t) = (\alpha(t), \mathbf{a}(t))$, that connects them. Let us replace γ by the path g defined as follows:

- $g(t) = \gamma(t)$ if $\alpha(t) \leq x$;
- $g(t) = \Psi^{-1}(x, \psi(\alpha(t), \mathbf{a}(t)))$ if $a(t) \geq x$.

The path $g(t)$ is well-defined, lies in $A_{\leq x}$ by construction, and connect $\mathbf{y}_0$ to $\mathbf{y}_1$. This establishes our connectivity claim.

Now, we can deal with the situation above v. We cannot directly use the fibration above, since it is not defined above v; instead, we will use a limiting process, that will rely on semi-algebraicity. To do so, we use a semi-algebraic fibration. Applying Hardt's semi-algebraic triviality theorem to the projection Π_1 on the semi-algebraic set $A_{<w}$ proves that there exist $z_0 = -\infty < z_1 < \cdots < z_m = w$ in $\mathbb{R} \cup \{-\infty\}$ such that above each interval $]z_i, z_{i+1}[$, there exists a semi-algebraic homeomorphism of the form

$$\begin{array}{rccc} \Phi_i : & A_{(z_i, z_{i+1})} & \to & (z_i, z_{i+1}) \times A'_{\rho_i} \\ & (\alpha, \mathbf{a}) & \mapsto & (\alpha, \phi_i(\alpha, \mathbf{a})). \end{array},$$

where ρ_i is (for instance) $(z_i+z_{i+1})/2$ and $A'_{\rho_i} \subset \mathbb{R}^{n-1}$ is $\{(x_2,\ldots,x_n) \mid (\rho_i,x_2,\ldots,x_n) \in A_{\rho_i}\}$.

Let i_0 be such that v is in $[z_{i_0}, z_{i_0+1})$ (so v can be an interior point, or coincide with z_{i_0}). To prove that $A_{\leq v}$ is non-empty, we actually prove that A_v is. Let $\mathbf{r}_{i_0}$ be such that $(\rho_{i_0}, \mathbf{r}_{i_0})$ is in $A_{\rho_{i_0}}$ (such a point exists, because $A_{\rho_{i_0}}$ is not empty, by the previous paragraphs). We define the function $\gamma : [0,1) \to A_{\leq x}$ by $\gamma(t) = \Phi_{i_0}^{-1}(tv+(1-t)\rho_i, (\rho_i, \mathbf{r}_i))$. This is a semi-algebraic, continuous, bounded function, so it can be extended by continuity at $t=1$ [7, Proposition 3.18]. Since $\gamma(t)$ is in $A_{[v,\rho_i]}$ for $t<1$, $\gamma(1)$ is in $A_{[v,\rho_i]}$ too; besides, $\Pi_1(\gamma(t)) = tv+(1-t)y_i$ for $t<1$, so $\Pi_1(\gamma(1)) = v$. Hence, $\gamma(1)$ is in A_v, as requested.

It remains to prove that $A_{\leq v}$ is connected. Let thus $\mathbf{y}_0$ and $\mathbf{y}_1$ be two points in $A_{\leq v}$. Since $A_{\leq \rho_i}$ is connected (first part of the proof) and semi-algebraic, $\mathbf{y}_0$ and $\mathbf{y}_1$ can be connected by a semi-algebraic path γ in $A_{\leq \rho_i}$. As we did previously, we replace γ by a better path g. Let ε be an infinitesimal, let A' be the extension of A over $\mathbb{R}\langle\varepsilon\rangle$ and let g be the path $[0,1] \subset \mathbb{R}\langle\varepsilon\rangle \to A'_{(v,w)}$ be defined as follows (where as before $\gamma(t) = (\alpha(t), \mathbf{a}(t))$)

- $g(t) = \gamma(t)$ if $\alpha(t) \leq v+\varepsilon$;
- $g(t) = \Phi_i^{-1}(v+\varepsilon, \phi_i(\alpha(t), \mathbf{a}(t)))$ if $\alpha(t) \geq v+\varepsilon$.

Obviously, g is well-defined (since γ has its image in $A_{\leq \rho_i}$) and continuous, bounded over $\mathbb{R}$ and semi-algebraic. Its image G is thus a connected semi-algebraic set, contained in $A'_{\leq v+\varepsilon}$. Let $G_0 = \lim_\varepsilon G$. By construction, $\mathbf{y}_0$ and $\mathbf{y}_1$ are in G_0, G_0 is contained in $A_{\leq v}$ and by [7, Proposition 12.43], G_0 is semi-algebraically connected. Our claim follows.

Statement and proof of Lemma 24 used on page 11

Lemma 24. *If $\mathbf{P}(x')$ holds for $x' < x$, then for $i \leq r$, $\overline{B_i} \cap \mathscr{R}$ is non-empty and connected.*

Let B be one of the connected components B_i of $C_{<x}$. Since B is actually a connected component of $V_{<x}$ and $V \cap \mathbb{R}^n$ is compact, B contains a point of W_1 (the minimal point for Π_1). Hence, $B \cap \mathscr{R}$, and thus $\overline{B} \cap \mathscr{R}$, are not empty. Next, we prove that any point $\mathbf{y}$ in $\overline{B} \cap \mathscr{R}$ can be connected to a point $\mathbf{z}$ in $B \cap \mathscr{R}$ by a path in $\overline{B} \cap \mathscr{R}$. Let us first justify that this is sufficient to establish the lemma.

Consider two points $\mathbf{y}, \mathbf{y}'$ in $\overline{B} \cap \mathscr{R}$ and suppose that they can be connected to some points $\mathbf{z}, \mathbf{z}'$ in $B \cap \mathscr{R}$ by paths in $\overline{B} \cap \mathscr{R}$. Since $\mathbf{z}$ and $\mathbf{z}'$ are in B, they can be connected by a path $\gamma : [0,1] \to B$. Let $x' = \max(\Pi_1(\gamma(t)))$, for t in $[0,1]$; x' is well defined by the continuity of γ, and satisfies $x' < x$. Then, both $\mathbf{z}$ and $\mathbf{z}'$ are in $B_{\leq x'}$, and they can be connected by a path in $B_{\leq x'}$; hence, they are in the same connected component B' of $B_{\leq x'}$. Now, B' is a connected component of $V_{\leq x'}$, which implies by property $\mathbf{P}(x')$ that $B' \cap \mathscr{R}$ is connected. Hence, $\mathbf{z}$ and $\mathbf{z}'$, which are in $B' \cap \mathscr{R}$, can be connected by a semi-algebraic path in $B' \cap \mathscr{R}$, and thus within $B \cap \mathscr{R}$. Summarizing, this proves that $\mathbf{y}$ and $\mathbf{y}'$ can be connected by a path in $\overline{B} \cap \mathscr{R}$, as requested.

We are thus left to prove the claim made in the first paragraph. Recall that $\mathscr{R}$ is the union of W_i and of $\mathscr{C}' = V \cap \Pi_{i-1}^{-1}(\Pi_{i-1}(\mathscr{C}))$, where $\mathscr{C} = W_1 \cup \mathrm{crit}(\Pi_1, W_i) \cup \mathscr{P}$. We first deal with points $\mathbf{y}$ in $\overline{B} \cap \mathscr{C}'$, and in a second time with points $\mathbf{y}$ in $\overline{B} \cap (W_i - \mathscr{C}')$.

Case 1. Let $\mathbf{y}$ be in $\overline{B} \cap \mathscr{C}'$. We can assume that $\mathbf{y}$ is not in B, since for $\mathbf{y}$ in B we can take $\mathbf{z} = \mathbf{y}$; since $\mathbf{y}$ is not in B, $\Pi_1(\mathbf{y}) = x$.

Since B is semi-algebraic, by the curve selection lemma, there exists a continuous semi-algebraic map $f : [0,1] \to \mathbb{R}^n$, with $f(0) = \mathbf{y}$ and $f(t) \in B$ for t in $(0,1]$. Let ε be a new infinitesimal and let $\mathsf{R} = \mathbb{R}\langle\varepsilon\rangle$; we let $\varphi = (\varphi_1, \ldots, \varphi_n) \in \mathsf{R}^n$ be the semi-algebraic germ of f at 0, so that $\lim_\varepsilon \varphi = \mathbf{y}$. We consider the semi-algebraic set $\mathsf{H} \subset \mathsf{R}^n$ defined by

$$\mathsf{H} \quad = \quad \{\mathbf{x} \in \mathsf{R}^n \mid \mathbf{x} \in \mathrm{ext}(B, \mathsf{R}) \text{ and } (x_1, \ldots, x_{i-1}) = (\varphi_1, \ldots, \varphi_{i-1})\},$$

where ext denotes the extension to R. Since for all t in $(0,1]$, $f(t)$ is in B, φ is in $\mathrm{ext}(B, \mathsf{R})$ by [7, Prop. 3.16], so that φ is in H; in particular, this proves that $\mathbf{y}$ is in $\lim_\varepsilon \mathsf{H}$. Remark also that H is bounded by an element of $\mathbb{R}$, and that any point in $\lim_\varepsilon \mathsf{H}$ is in $\overline{B} \cap \Pi_{i-1}^{-1}(\Pi_{i-1}(\mathbf{y}))$.

Let $\mathsf{H}_1, \ldots, \mathsf{H}_s \subset \mathsf{R}^n$ be the semi-algebraically connected components of H (which are well-defined because H is not empty); hence, the H_i are semi-algebraic sets. Because $\mathbf{y}$ is in $\lim_\varepsilon(\mathsf{H})$, we can assume that it is in $\lim_\varepsilon \mathsf{H}_1$. Next, since B is a semi-algebraically connected component of $V_{<x}$, by [7, Prop. 5.24], H_1 is a semi-algebraically connected component of $\mathrm{ext}(V, \mathsf{R}) \cap \Pi_{i-1}^{-1}(\varphi_1, \ldots, \varphi_{i-1})$. By the semi-algebraic implicit function theorem, this implies that there exists a point ψ in $\mathsf{H}_1 \cap \mathrm{crit}(\Pi_i, \mathrm{ext}(V, \mathsf{R}))$. Since polar varieties are defined by suitable Jacobian minors, this means that ψ is in $\mathsf{H}_1 \cap \mathrm{ext}(W_i, \mathsf{R})$. Because ψ is in H_1, it is in $\mathrm{ext}(B, \mathsf{R})$, and thus in $\mathrm{ext}(B \cap W_i, \mathsf{R})$.

Let $\mathbf{w} = \lim_\varepsilon \psi$ and let g be a representative of ψ, so that $g(0) = \mathbf{w}$. By [7, Prop. 3.16], there exists $t_0 > 0$ such that for all t in $(0, t_0)$, $g(t)$ is in $B \cap W_i$, which is contained in $\overline{B} \cap \mathscr{R}$. Defining $\mathbf{z} = g(t_0/2)$, we see that $\mathbf{z}$ and $\mathbf{w}$ are connected by a path in $\overline{B} \cap \mathscr{R}$.

Let $B_1 = \lim_\varepsilon \mathsf{H}_1$. Because H_1 is semi-algebraic, bounded over $\mathbb{R}$ and semi-algebraically connected, B_1 is closed, semi-algebraic and connected [7, Prop. 12.43]. Besides, we have seen above that it is contained in $\overline{B} \cap \Pi_{i-1}^{-1}(\Pi_{i-1}(\mathbf{y}))$. Finally, it contains both $\mathbf{y}$ and $\mathbf{w}$. Hence, $\mathbf{y}$ and $\mathbf{w}$ can be connected by a path in $B_1 \subset \overline{B} \cap \Pi_{i-1}^{-1}(\Pi_{i-1}(\mathbf{y}))$. Since $\mathbf{y}$ is in $\mathscr{C}'$, $\Pi_{i-1}^{-1}(\Pi_{i-1}(\mathbf{y}))$ is contained in $\mathscr{C}'$ too, and thus in $\mathscr{R}$. Connecting $\mathbf{y}$ to $\mathbf{w}$ and $\mathbf{w}$ to $\mathbf{z}$ (previous paragraph), we conclude the proof of our claim.

Case 2. Let now $\mathbf{y}$ be in $\overline{B} \cap (W_i - \mathscr{C}')$; as in case 1, we assume that $\mathbf{y}$ is not in B, so that $\Pi_1(\mathbf{y}) = x$. Since $\mathbf{y}$ is not in $\mathscr{C}'$, $\mathbf{y}$ is not in $\mathscr{C}$, and so not in $\mathrm{crit}(\Pi_1, W_i)$. Applying Lemma 18 to the algebraic set W_i, we see that $\mathbf{y}$ is in $\overline{W_{i<x}}$. By the curve selection lemma, this means that there exists a semi-algebraic path $\gamma : [0,1] \to W_i$ connecting a point $\mathbf{z}$ in $W_{i<x}$ to $\mathbf{y}$, with $\gamma(0) = \mathbf{z}$, $\gamma(1) = \mathbf{y}$ and $\gamma(t) \in W_{i<x}$ for $t < 1$.

The image of γ is in $\mathscr{R}$, so to conclude, it suffices to prove that $\gamma(t)$ is in $\overline{B}$ for all t. To do so, we will prove that $\gamma(t)$ is in B for all $t < 1$. We know that the image $\{\gamma(t) \mid t \in [0,1)\}$ is connected and contained in $V_{<x}$; hence, it is contained in a connected component B' of $V_{<x}$. We have to prove that $B' = B$. Because $\gamma(1) = \mathbf{y}$, we deduce that $\mathbf{y}$ is in $\overline{B'}$; on the other hand, we know that $\mathbf{y}$ is in $\overline{B}$. Since $\mathbf{y}$ is not in $\mathscr{C}$, it is not in W_1; as a consequence, we can apply Lemma 19, which shows that $B = B'$, as requested.

Proof of Lemma 12 on page 13

Property $\mathbf{a}_1(\mathbf{e})$ follows from the algebraic form of Sard's lemma; it is in [3]. Using our notation, Mather's transversality result [21, 2, 1] shows that for generic $\mathbf{e}$, $\mathbf{a}_2(\mathbf{e})$ and $\mathbf{a}_3(\mathbf{e})$ are satisfied, and the dimensions of S_j and $S_{j,\ell}$ are

$$\dim(S_j) = n-1-\nu_{n,i}(n-1-j), \quad \dim(S_{j,\ell}) = n-1-\nu_{n,i}(n-1-j, \dim(S_j)-\ell),$$

where the function $\nu_{n,i}$ is defined as follows. Considering two indices $r \geq s \geq 0$, we define $\mu(r,s)$ as the number of sequences $r' \geq s' \geq 0$, with $r' > 1$, and $r \geq r'$, $s \geq s'$; explicitly, $\mu(r,s) = r(s+1) - s(s-1)/2$. Then, we have

$$\begin{aligned} \nu_{n,i}(r) &= (i-n+1+r)r \\ \nu_{n,i}(r,s) &= (i-n+1+r)\mu(r,s) - (r-s)s \\ &= (i-n+1+r)(r(s+1) - \frac{s(s-1)}{2}) - (r-s)s. \end{aligned}$$

It remains to check that under these constraints, we always have $\dim(S_{j,\ell}) \leq \ell$ for $\ell \leq i-1$; this follows from a straightforward but tedious verification.

Proof of Lemma 13 on page 13

In all the rest of this paragraph, we fix $\mathbf{e}$ that satisfies the assumptions of Lemma 13, and we denote by $X_\mathbf{e}$ the intersection $X \cap \gamma^{-1}(\mathbf{e})$. Finally, we let $\beta_\mathbf{e} : (\mathbf{g}, \mathbf{e}, \mathbf{x}) \in X_\mathbf{e} \mapsto \mathbf{x} \in \mathbb{C}^n$ be the projection on the $\mathbf{X}$-coordinate.

Lemma 25. *For* $\mathbf{x}$ *in* $\mathrm{reg}(W_\mathbf{e})$ *and* $\mathbf{g}$ *in* $\mathbb{C}^i$, $(\mathbf{g}, \mathbf{x})$ *is in* $X_\mathbf{e}$ *if and only if* $\mathbf{x}$ *is in* $\mathrm{crit}(\rho_\mathbf{g} \circ \Pi_\mathbf{e}, W_\mathbf{e})$ *and the equality* $\dim(\Pi_\mathbf{e}(T_\mathbf{x} W_\mathbf{e})) + \dim(\beta_\mathbf{e}^{-1}(\mathbf{x})) = i$ *holds.*

Proof. Since $\mathbf{a}_1(\mathbf{e})$ holds,, the equations $f(\mathbf{X}), M_{i+1}(\mathbf{e}, \mathbf{X}), \ldots, M_n(\mathbf{e}, \mathbf{X})$ define the critical set $W_\mathbf{e}$ and for $\mathbf{x}$ in $\mathrm{reg}(W_\mathbf{e})$, the matrix $J(\mathbf{x})$ has rank $n-i+1$. The first claim follows readily. Thus, $\mathbf{g}$ is in $\beta_\mathbf{e}^{-1}(\mathbf{x})$ if and only if for all $\mathbf{v}$ in $T_\mathbf{x} W_\mathbf{e}$, $\rho_\mathbf{g}(\Pi_\mathbf{e}(\mathbf{v})) = 0$; equivalently, if for all $\mathbf{w}$ in $\Pi_\mathbf{e}(T_\mathbf{x} W_\mathbf{e})$, $\rho_\mathbf{g}(\mathbf{w}) = 0$. Since $\rho_\mathbf{g}(\mathbf{w}) = \mathbf{g} \cdot \mathbf{w}$, we are done. □

For $0 \leq \ell \leq i-1$, let $j_{\ell,1}, \ldots, j_{\ell,\kappa(\ell)}$ be the indices j such that $S_{j,\ell}$ is well-defined. Then, we define the constructible sets

$$T_\ell = S_{j_{\ell,1},\ell} \cup \cdots \cup S_{j_{\ell,\kappa(\ell)},\ell} \quad \text{and} \quad T'_\ell = T_0 \cup \cdots \cup T_\ell.$$

By Lemma 12, both T_ℓ and T'_ℓ are disjoint unions of non-singular locally closed sets of dimension at most ℓ. By Lemma 25, for $0 \leq \ell \leq i$, and for $\mathbf{x}$ in T_ℓ, the inequality $\dim(\beta_\mathbf{e}^{-1}(\mathbf{x})) \leq i - \ell$ holds. Remark that $W_\mathbf{e} = T'_{i-1} \cup \mathrm{sing}(W_\mathbf{e})$. Since $T'_{i-1} = T'_{i-2} \cup T_{i-1}$, we rewrite this as

$$W_\mathbf{e} = T'_{i-2} \cup T_{i-1} \cup \mathrm{sing}(W_\mathbf{e}), \tag{1}$$

where the union is disjoint. Going further, we can write for any $\ell \leq i-1$

$$T'_\ell \cup \mathrm{sing}(W_\mathbf{e}) = T'_{\ell-1} \cup T_\ell \cup \mathrm{sing}(W_\mathbf{e}). \tag{2}$$

Consider now an irreducible component X' of $X_\mathbf{e}$. By construction, $\beta_\mathbf{e}(X')$ is contained in $W_\mathbf{e}$. By (1), either $\beta_\mathbf{e}(X')$ is contained in $T'_{i-2} \cup \mathrm{sing}(W_\mathbf{e})$,

or $\beta_{\mathbf{e}}(X')$ intersects T_{i-1}. If $\beta_{\mathbf{e}}(X')$ intersects T_{i-1}, then there is a fiber of dimension at most 1. In this case, by the theorem on the dimension of fibers, $\dim(X') \leq 1 + \dim(T'_{i-1} \cup \mathrm{sing}(W_{\mathbf{e}}))$, and thus $\dim(X') \leq i$.

If $\beta_{\mathbf{e}}(X')$ is contained in $T'_{i-2} \cup \mathrm{sing}(W_{\mathbf{e}})$, then by (2), either $\beta_{\mathbf{e}}(X')$ is contained in $T'_{i-3} \cup \mathrm{sing}(W_{\mathbf{e}})$, or $\beta_{\mathbf{e}}(X')$ intersects T_{i-2}. If $\beta_{\mathbf{e}}(X')$ intersects T_{i-2}, then there is a fiber of dimension at most 2, so $\dim(X') \leq 2 + \dim(T'_{i-2} \cup \mathrm{sing}(W_{\mathbf{e}})) \leq i$. Continuing this way, we prove that $\dim(X') \leq i$.

Proof of Lemma 14 on page 14

Let $\mathcal{F}$ be the Zariski-open subset of $\mathbb{C}^{ni}$ underlying Lemma 12: for $\mathbf{e}$ in $\mathcal{F}$, $\mathbf{a}_1(\mathbf{e})$, $\mathbf{a}_2(\mathbf{e})$ and $\mathbf{a}_3(\mathbf{e})$ hold. Finally, recall the definitions of the projections $\alpha : (\mathbf{g}, \mathbf{e}, \mathbf{x}) \mapsto (\mathbf{g}, \mathbf{e})$ and $\gamma : (\mathbf{g}, \mathbf{e}, \mathbf{x}) \mapsto \mathbf{e}$. First, Y is obviously Zariski-closed. We continue by proving that it does not cover all of $\mathbb{C}^i \times \mathbb{C}^{ni}$: it is enough to prove it componentwise. Thus, we partition the set of irreducible components X' of X into some sets $E_0 \cup E_1 \cup E_2$, where

- E_0 is the set of irreducible components X' of X such that $\gamma(X')$ does not intersect $\mathcal{F}$;
- E_1 is the set of irreducible components X' of X such that $\alpha(X')$ intersects $\mathcal{F}$ and such that $\alpha(X')$ is dense in $\mathbb{C}^i \times \mathbb{C}^{ni}$;
- E_2 is the set of irreducible components X' of X such that $\alpha(X')$ intersects $\mathcal{F}$ and such that $\alpha(X')$ is not dense in $\mathbb{C}^i \times \mathbb{C}^{ni}$.

We want to prove that for all X', the set of infinite fibers of α in X' is contained in a strict Zariski-closed subset of $\mathbb{C}^i \times \mathbb{C}^{ni}$. For X' in E_0, $\gamma(X')$ is contained in a strict Zariski-closed subset of $\mathbb{C}^{ni}$, which implies that $\alpha(X')$ is contained in strict Zariski-closed subset of $\mathbb{C}^i \times \mathbb{C}^{ni}$. For X' in E_1, Lemma 13 and the theorem on the dimension of fibers imply that $\dim(X') \leq i + ni$; as a consequence, the set of infinite fibers is contained in a hypersurface. For X' in E_2, this is true by construction. This finishes the proof that Y is a strict Zariski-closed subset of $\mathbb{C}^i \times \mathbb{C}^{ni}$.

Let $(\mathbf{g}, \mathbf{e})$ be in $\mathbb{C}^i \times \mathbb{C}^{ni} - Y'$. Hence, $\mathbf{e}$ is in $\mathcal{F}$, so that the fiber $\alpha^{-1}(\mathbf{g}, \mathbf{e})$ meets no irreducible component X' of X that belongs to E_0. For all other components X' of X, since $(\mathbf{g}, \mathbf{e})$ is not in Y, $\alpha^{-1}(\mathbf{g}, \mathbf{e})$ intersects X' in a finite number of points. Hence, finally, $\alpha^{-1}(\mathbf{g}, \mathbf{e})$ intersects X in a finite number of points. By Lemma 25, this means that $\mathrm{crit}(\rho_{\mathbf{g}} \circ \Pi_{\mathbf{e}}, W_{\mathbf{e}})$ is finite, as requested.

Proof of Lemma 5 on page 9: correctness and runtime

In this paragraph, we prove that assuming **H** and **H′**, algorithm CannyRoadmap is correct; we also discuss its complexity. In all that follows, for $i \leq j$, we denote by $\Pi_{X_i,\ldots,X_j}$ the projection

$$\begin{array}{rccc} \Pi_{X_i,\ldots,X_j} : & \mathbb{C}^n & \to & \mathbb{C}^{j-i+1} \\ & \mathbf{x} = (x_1, \ldots, x_n) & \mapsto & (x_i, \ldots, x_j). \end{array}$$

First, we need a direct extension of Theorem 2 to the case of inputs of the form $[\mathbf{F}, Q]$, with $\mathbf{F} = f_1, \ldots, f_p$ and $Q(X_1, \ldots, X_e)$, so that we have $d = n - p - e$. As before, we are also given a set of control points $\mathscr{P}$ in $V = V(\mathbf{F}, Q)$. Then, extending the previous notation, we define, for $\mathbf{x} = (x_1, \ldots, x_e)$ in $V(Q)$:

- $V_{\mathbf{x}} = V(\mathbf{F}(x_1, \ldots, x_e, X_{e+1}, \ldots, X_n)) \subset \mathbb{C}^n$;
- $\mathscr{P}_{\mathbf{x}} = \mathscr{P} \cap V_{\mathbf{x}}$;
- $\mathscr{C}_{\mathbf{x}} = \mathrm{crit}(\Pi_{X_{e+1}}, V_{\mathbf{x}}) \cup \mathrm{crit}(\Pi_{X_{e+1}}, \mathrm{crit}(\Pi_{X_{e+1},\ldots,X_{e+i}}, V_{\mathbf{x}})) \cup \mathscr{P}_{\mathbf{x}}$;
- $\mathscr{C}'_{\mathbf{x}} = V_{\mathbf{x}} \cap \Pi^{-1}_{X_{e+1},\ldots,X_{e+i-1}}(\Pi_{X_{e+1},\ldots,X_{e+i-1}}(\mathscr{C}_{\mathbf{x}})) = V_{\mathbf{x}} \cap \Pi^{-1}_{X_1,\ldots,X_{e+i-1}}(\Pi_{X_1,\ldots,X_{e+i-1}}(\mathscr{C}_{\mathbf{x}}))$.

If $[\mathbf{F}, Q]$ satisfies $\mathbf{H}$ and $\mathbf{H}'$, then for all $\mathbf{x} \in V(Q)$, $\mathscr{C}_{\mathbf{x}}$ is finite.

Theorem 26. *Let $d' = \max(i-1, d-i+1)$. If $[\mathbf{F}, Q]$ satisfies $\mathbf{H}$ and $\mathbf{H}'$, then for all $\mathbf{x} = (x_1, \ldots, x_e)$ in $V(Q)$, the following holds:*

1. *$\mathscr{C}'_{\mathbf{x}} \cup \mathrm{crit}(\Pi_{X_{e+1},\ldots,X_{e+i}}, V_{\mathbf{x}}))$ is a d'-roadmap of $(V_{\mathbf{x}}, \mathscr{P}_{\mathbf{x}})$;*
2. *$\mathscr{C}'_{\mathbf{x}} \cap \mathrm{crit}(\Pi_{X_{e+1},\ldots,X_{e+i}}, V_{\mathbf{x}}))$ is finite;*
3. *for all $(x_{e+1}, \ldots, x_{e+i-1}) \in \mathbb{C}^{i-1}$, the system $(f_1, \ldots, f_p, X_1 - x_1, \ldots, X_{e+i-1} - x_{e+i-1})$ satisfies assumption $\mathbf{H}$.*

This theorem is a straightforward consequence of Theorem 2, applied to all algebraic sets $V_{\mathbf{x}}$. With this in mind, we start by analyzing a single level of algorithm CannyRoadmap.

Lemma 27. *Suppose that $[\mathbf{F}, Q]$ satisfies $\mathbf{H}$, and that after the change of variables φ, $[\mathbf{F}, Q]$ satisfies $\mathbf{H}'$ for $i = 2$. Then steps $0-6$ of algorithm* CannyRoadmap *take time $(\delta_Q + \delta_P)^{O(1)}(nD)^{O(n)}$; upon success, Q' and P' are 0-dimensional parametrizations that satisfy*

$$\delta_{Q'} + \delta_{P'} \leq (\delta_Q + \delta_P)(nD)^{O(n)}$$

and $[\mathbf{F}, Q']$ satisfies $\mathbf{H}$. Let finally $\mathscr{P}' \subset \mathbb{C}^n$ be the set described by P'. If the recursive call at step 7 computes a roadmap of $(V(\mathbf{F}, Q'), \mathscr{P}')$, then (R', R'') is a roadmap of $(V(\mathbf{F}, Q), \mathscr{P})$.

Proof. Let us write here $V = V(\mathbf{F}, Q)$. We start by proving correctness. Remark that the solution set of $(\mathbf{F}, \Delta, Q)$ is the union of the sets $\mathrm{crit}(\Pi_{X_{e+1}}, V_{\mathbf{x}})$. Similarly, the solution-set of $(\mathbf{F}, \Delta', Q)$ is the union of the critical set $\mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}})$, for the projection on the (X_{e+1}, X_{e+2})-axis. Because $\mathbf{H}'$ holds for $i = 2$, this set has dimension 1. Consequently, S describes the union of the critical points of $\Pi_{X_{e+1}}$ on the sets $\mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}})$. Because $\mathbf{H}'$ holds for $i = 2$, this set is finite. Then, Q' describes all the projections $\Pi_{X_1,\ldots,X_{e+1}}(\mathscr{C}_{\mathbf{x}})$.

By the first point of Theorem 26, each $\mathscr{C}'_{\mathbf{x}} \cup \mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}}))$ is a $(n-p-e-1)$-roadmap of $(V_{\mathbf{x}}, \mathscr{P}_{\mathbf{x}})$. Besides, P' describes a set $\mathscr{P}'$ which is the union of all set $(\mathscr{C}'_{\mathbf{x}} \cap \mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}})) \cup \mathscr{P}_{\mathbf{x}}$; it is finite by point 2 in Theorem 26.

We continue by remarking that point 3 in Theorem 26 shows that $[\mathbf{F}, Q']$ satisfies $\mathbf{H}$, which justifies the recursive call on step 7. Suppose now that we obtain as output a roadmap R'' of $(V(\mathbf{F}, Q'), \mathscr{P}')$, and we write R'' as the disjoint union of the sets $R''_{\mathbf{x}}$, for $\mathbf{x} \in V(Q)$, with $R''_{\mathbf{x}} = R'' \cap \Pi^{-1}_{X_1,\ldots,X_e}(\mathbf{x})$. By the claims of the first paragraph, the zero-set of $(\mathbf{F}, Q')$ is the union of all $\mathscr{C}'_{\mathbf{x}}$, which implies that each $R''_{\mathbf{x}}$ is a roadmap of $(\mathscr{C}'_{\mathbf{x}}, (\mathscr{C}'_{\mathbf{x}} \cap \mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}})) \cup \mathscr{P}_{\mathbf{x}})$. Applying Lemma 3, we deduce that each union $R''_{\mathbf{x}} \cup \mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}}))$ is a roadmap of $(V_{\mathbf{x}}, \mathscr{P}_{\mathbf{x}})$. This proves that (R', R'') is a roadmap of $(V, \mathscr{P})$.

Next, we estimate the degree of the output, assuming correctness. First, we fix $\mathbf{x}$ in $V(Q)$ and bound the degree of the various objects above $\mathbf{x}$, leaving aside the contribution of $\mathscr{P}$ for the moment. By Bézout's theorem, $V_{\mathbf{x}}$ has degree at most D^p, whereas the degrees of $\mathrm{crit}(\Pi_{X_{e+1}}, V_{\mathbf{x}})$ and $\mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}})$ are at most $D^p(pD)^{n-p} = p^{n-p}D^n$ (the latter estimate relies on the Bézout theorem of [19, Prop. 2.3]). Finally, since $\mathrm{crit}(\Pi_{X_{e+1},X_{e+2}}, V_{\mathbf{x}})$ is a curve of degree at most $p^{n-p}D^n$, the set of critical points of $\Pi_{X_{e+1}}$ on this curve has degree at most $p^{2n-2p}D^{2n}$.

Taking all $\mathbf{x}$ in $V(Q)$ into account, we deduce that the degrees of R and R' are both bounded by $\delta_Q p^{n-p}D^n$ and the degree of S is at most $\delta_Q p^{2n-2p}D^{2n}$, so that the degree of Q' is at most $2\delta_Q p^{2n-2p}D^{2n} + \delta_P$.

It remains to bound the degree of P'; we start by estimating the degree of $\mathsf{Solve}([Q', R'])$, which computes the intersection of $\Pi^{-1}_{X_1,\ldots,X_{e+1}}(\Pi_{X_1,\ldots,X_{e+1}}(V(S)\cup V(R)\cup\mathscr{P}))$ with the zero-set of R'. Above each value of $\mathbf{x}$ in $V(Q)$, the intersection has degree at most $(\delta_{P_{\mathbf{x}}} + 2p^{2n-2p}D^{2n})p^{n-p}D^n$, where $\delta_{P_{\mathbf{x}}}$ is the cardinality of $\mathscr{P}_{\mathbf{x}}$. Summing over all $\mathbf{x}$ in $V(Q)$ gives the upper bound

$$\delta_P p^{n-p}D^n + \delta_Q 2p^{3n-3p}D^{3n}$$

for the degree of $\mathsf{Solve}([Q', R'])$, and thus

$$\delta_P(1 + p^{n-p}D^n) + \delta_Q 2p^{3n-3p}D^{3n}$$

for the degree of P'. Taking into account the estimate on the degree of Q, we obtain the upper bounded announced in the lemma.

Finally, we estimate the running time, starting with the computation of R and R'. If we were to solve a system of the form $[\mathbf{F}, \Delta, X_1 - x_1, \ldots, X_e - x_e]$, the resolution algorithm of [20] would take time $(nD)^{O(n)}$. However, we need to solve slightly more complex systems of the form $[\mathbf{F}, \Delta, Q]$ or $[\mathbf{F}, \Delta', Q]$. Our strategy is to use dynamic evaluation techniques [12]: we apply the former algorithm over the product of fields $\mathbb{Q}[T]/q$, where q is the minimal polynomial of Q. If a division by zero occurs, we split q into two factors, and we run the computation again. The maximal number of splittings is δ_Q, so the overall cost is $\delta_Q^{O(1)}(nD)^{O(n)}$.

The critical points computation takes a similar time, since the form of the parametrization makes it possible for us to work with bivariate polynomials of degree $(nD)^{O(n)}$. The union and projection at step 5 take time $(\delta_Q + \delta_P)^{O(1)}(nD)^{O(n)}$, since they only involve computations with 0-dimensional ideals of that degree, given by rational parametrizations, and rational parametrizations for such objects can be computed (deterministically) in the required time using e.g. the algorithm of [23]. Solving the system $[\mathbf{F}, \Delta, Q']$ is done by the same dynamic evaluation strategy as before, and the final union computation raises no new difficulty. □

Remark that as soon as all changes of variables satisfy the assumptions of Lemma 4, the previous lemma shows that the whole algorithm CannyRoadmap correctly computes a roadmap of $V([\mathbf{F}, Q], \mathscr{P})$ in the requested time (the analysis of the overall computation time in on page 9). The probabilistic aspects are discussed further.

Proof of Lemma 7 on page 10: correctness and runtime

The proof of the running time estimates for our algorithm is quite similar to that given for our modified version of Canny's algorithm. In what follows, to simplify notation, we denote by $\mathbf{F}$ the system $[f, \Delta'] = [f, \partial f/\partial X_{e+i+1}, \ldots, \partial f/\partial X_n]$ used in the algorithm.

Lemma 28. *Suppose that $[f, Q]$ satisfies $\mathbf{H}$ and that after the change of variables φ, $[f, Q]$ satisfies $\mathbf{H}'$ and $[\mathbf{F}, Q]$ satisfies $\mathbf{H}$. Then steps $0-7$ of algorithm* Roadmap *take time $(\delta_Q + \delta_P)^{O(1)}(nD)^{O(n)}$; upon success, Q' and P' are 0-dimensional parametrizations that satisfy*

$$\delta_{Q'} + \delta_{P'} \leq (nD)^{O(n)}(\delta_Q + \delta_P)$$

and $[f, Q']$ satisfies assumption $\mathbf{H}$. Let finally $\mathscr{P}' \subset \mathbb{C}^n$ be the set described by P'. If additionally

- *the call to* CannyRoadmap *at step 8 computes a roadmap R'' of $(V(\mathbf{F}, Q), \mathscr{P}')$,*
- *the recursive call at step 9 computes a roadmap R''' of $(V(f, Q'), \mathscr{P}')$,*

then (R'', R''') is a roadmap of $(V(f, Q), \mathscr{P})$.

Proof. The proof follows exactly the same pattern as the one in Lemma 27. The only notable difference is that we directly use the defining system $[\mathbf{F}, Q]$ to compute the critical points of $\Pi_{X_{e+1}}$, which is possible since these equations satisfy $\mathbf{H}$. □

As for algorithm CannyRoadmap, as soon as all changes of variables satisfy the assumptions of Lemma 6, the previous lemma shows that the whole algorithm Roadmap correctly computes a roadmap of $V([f, Q], \mathscr{P})$ in the announced time.

Probabilistic aspects of our algorithms

Both algorithms CannyRoadmap and Roadmap start by choosing a random change of variable φ in a parameter space denoted by $\mathrm{GL}(n, e)$. Lemmas 4 and 6 show that success depends on choosing φ outside of some hypersurfaces of $\mathrm{GL}(n, e)$; what is missing is an estimate on the degrees of these hypersurfaces.

Let us assume that we initially call Roadmap with input a polynomial f of degree D, Q of degree δ_Q and P of degree δ_P; the following lemma gives a bound on the degree of the hypersurface to avoid which is valid at any step of the recursion. We give the bound in a big-O form for readability; all estimates could be made completely explicit.

Lemma 29. *Starting with conditions as above, at any recursive call to* CannyRoadmap *(resp.* Roadmap*), there exists a hypersurface H of degree at most $K(n, D, \delta_P, \delta_Q) = (\delta_Q + \delta_P)D^{O(n^2)}$ of $\mathrm{GL}(n, e)$ such that if $\varphi \in H$, the conclusions of Lemma 4 (resp. Lemma 6) are satisfied.*

Proof. A useful ingredient is a quantitative version of Sard's lemma [22, Prop. 3.6].

Lemma 30. *Suppose that $X \subset \mathbb{C}^K$ is an algebraic set defined by equations of degree Δ and that $\Phi : X \to \mathbb{C}^L$ is a polynomial map, given by means of equations of degree Δ as well. Suppose that $K, L \leq N$; then, $\Phi(\mathrm{reg}(X) \cap \mathrm{crit}(\Phi, X))$ is contained in a hypersurface of $\mathbb{C}^L$ of degree $\Delta^{O(N^2)}$.*

Proof. Remark that X has degree at most Δ^N. First we show that we can write $\mathrm{reg}(X) \cap \mathrm{crit}(\Phi, X)$ as $\mathrm{reg}(X) \cap Z$, for a suitable algebraic set $Z \subset X$. Let X' be the reunion of the irreducible components of X of maximal dimension d; we know that X' can be generated by $O(N)$ polynomials $g_1, \ldots, g_R$ of degree at most Δ^N, by [17, Prop. 3]. Then, we define Z by $g_1, \ldots, g_R$ and all $(K+L-d)$-minors of the Jacobian matrix matrix of $(g_1, \ldots, g_R, \Phi_1, \ldots, \Phi_L)$, and we easily verify the claim that $\mathrm{reg}(X) \cap \mathrm{crit}(\Phi, X) = \mathrm{reg}(X) \cap Z = (X - \mathrm{sing}(X)) \cap Z$.

By Bézout's theorem as in [19, Prop. 2.3], we obtain the bound $\Delta^{O(N^2)}$ for the degree of Z. Now, since Z is contained in X, we can rewrite $\mathrm{reg}(X) \cap \mathrm{crit}(\Phi, X)$ as $Z - \mathrm{sing}(X) \cap Z$. Consequently, a degree bound as above hold for the degree of the Zariski closure of $\mathrm{reg}(X) \cap \mathrm{crit}(\Phi, X)$, and for the degree of its image by φ (by Bézout's theorem again). □

We can now resume the proof of Lemma 29. Each time we enter the functions CannyRoadmap and Roadmap, the input polynomials (either the system $\mathbf{F} = f_1, \ldots, f_p$ or the unique equation f) have degree at most D and the 0-dimensional parametrization Q has degree $(\delta_Q + \delta_P)(nD)^{O(n^{1.5})}$. We consider all $\mathbf{x}$ in $V(Q)$ separately: each of them puts some constraints on φ, and φ must satisfy all of these constraints simultaneously.

If we prove that for a single $\mathbf{x} \in V(Q)$ the degree of the hypersurface to avoid in $\mathrm{GL}(n, e)$ is $D^{O(n^2)}$, then the degree of the union of all these hypersurfaces will be $(\delta_Q + \delta_P) D^{O(n^2)}$, as claimed. Concretely, after fixing $\mathbf{x} = (x_1, \ldots, x_e)$, we are left to quantify the claims that proved Lemmas 4 and 6 in Section 4; we apply them to the variety $V_{\mathbf{x}}$ defined by the input polynomials and the additional equations $X_1 = x_1, \ldots, X_e = x_e$. Note that all these equations have degree at most D.

The first step is a dimension statement for polar varieties in generic coordinates. This is proved in [3, 4] by means of an algebraic version of Thom's weak transversality result, applied to a generic projection Φ on $V_{\mathbf{x}}$. The weak transversality theorem is obtained by applying Sard's lemma to a subset S of $V_{\mathbf{x}} \times Y$, where Y is the parameter space where we pick our generic projection and S is defined by equations of degree $O(D)$. By Lemma 30, we obtain the degree bound $D^{O(n^2)}$ for the critical locus, as claimed.

The second step is a Noether position statement for polar varieties. Using a change of variables with formal entries (that is, new variables $\mathbf{U}$), we construct in [24, Sect. 2.3] some eliminating polynomials with coefficients that are rational functions of $\mathbf{U}$. Besides, we prove in [24, Sect. 2.4] that if the entries of the change of variables φ cancel none of the denominators of these coefficients, the polar varieties associated to $V_{\mathbf{x}}$ are in Noether position. The least common multiple of these denominators has degree $D^{O(n)}$ by [25, Prop. 1]; this gives the degree bound for this step as well.

As seen in Section 4, this is sufficient to conclude for Lemma 4. The most delicate step is to establish point (d) of assumption $\mathbf{H}'$ for Lemma 6. Recall that in Section 4 we defined a strict algebraic Y of $\mathbb{C}^i \times \mathbb{C}^{ni}$, such that the first i rows of the inverse of φ should avoid $((1, 0, \ldots, 0) \times \mathbb{C}^{ni}) \cap Y$. Hence, it is sufficient to bound the degree of Y by $D^{O(n^2)}$.

We reconsider the proof given above of Lemma 14 (and use freely all necessary notation). First, observe that the algebraic set X defined on page 13 has degree $D^{O(n)}$. We also recall that Y consists of the Zariski-closure of the

infinite fibers of a projection denoted by $\alpha : X \to \mathbb{C}^i \times \mathbb{C}^{ni}$. The irreducible components of X were classified into three groups, written E_0, E_1 and E_2. We prove that in all cases, the Zariski-closure of the set of the infinite fibers of α on X' has a degree at most that of X'.

- The image of a component X' in E_0 is contained in a strict algebraic subset of $\mathbb{C}^i \times \mathbb{C}^{ni}$; then, it can be enclosed in a hypersurface of degree bounded by that of X'. The same holds for the components in E_2.
- For a component X' in E_1, we saw that the projection $\alpha : X' \to \mathbb{C}^i \times \mathbb{C}^{ni}$ has a dense image and generically finite fibers. Let $\mathbb{C}(V_1, \ldots, V_{n+ni})$ be the function field of $\mathbb{C}^i \times \mathbb{C}^{ni}$, let $\mathbb{C}(X')$ be that of X', and let $M \in \mathbb{C}(V_1, \ldots, V_{i+ni})[T]$ be the monic minimal polynomial of a primitive element for the algebraic extension $\mathbb{C}(V_1, \ldots, V_{i+ni}) \to \mathbb{C}(X')$. It is known that the infinite fibers cancel one of the denominators of the coefficients of M [24]. Since the least common multiple of these denominators has degree at most the degree of X' [25], we are done.

At this stage, we have quantified Lemma 4 and the first part of Lemma 6; it remains to consider the last condition of that lemma (that the system $[\mathbf{F}, Q]$ satisfies assumption **H**). We mentioned in Section 4 that this property resulted from the validity of a condition written $\mathbf{a}_1(\mathbf{e})$, which itself is ensured by an application of Sard's lemma. The quantification is similar to the one we have seen before, and yields another contribution of the form $D^{O(n^2)}$. □

We conclude the probability analysis of our algorithms. At each level of the recursion, we draw all entries of our change of variables in a set of cardinality $\eta\, K(n, D, \delta_Q, \delta_P)$, where $K(n, D, \delta_Q, \delta_P)$ was defined in the previous lemma. By Zippel-Schwartz's zero avoidance lemma, the probability of success at this level is at least $(1 - 1/\eta)$. We need to draw at most n^2 changes of variables; hence, to obtain an overall probability of success of at least $1/2$, it suffices to take η polynomial in n.

It remains to discuss the probabilistic aspects of the algorithm of [20]; they are twofold. First, the success of that algorithm depends on the choice of a so-called *correct test sequence* [19], to perform zero-test of polynomials represented by straight-line programs. For all our applications of this subroutine, a single correct test sequence is needed; as pointed out in [14], one can construct one with probability of success at least $1/262144$. The second probabilistic aspect is due to a linear combination of the equations performed at the beginning of this subroutine. This aspect is analyzed in [20]. The conclusion is similar to what we obtained above for our change of variables: success is ensured if the coefficients of the linear combination avoid a hypersurface of degree $D^{O(n)}$.

Centre de recherche INRIA Paris – Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Centre de recherche INRIA Futurs : Parc Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399