Solving Parametric Polynomial Systems

Daniel Lazard

SALSA project - Laboratoire d'Informatique de Paris VI and INRIA Rocquencourt

Email: `Daniel.Lazard@lip6.fr`

Fabrice Rouillier

SALSA project - INRIA Rocquencourt and Laboratoire d'Informatique de Paris VI

Email: `Fabrice.Rouillier@inria.fr`

Abstract

We present a new algorithm for solving basic parametric constructible or semi-algebraic systems like $\mathcal{C} = \{x \in \mathbb{C}^n, p_1(x) = 0, ..., p_s(x) = 0, f_1(x) \neq 0, ..., f_l(x) \neq 0\}$ or $\mathcal{S} = \{x \in \mathbb{R}^n, p_1(x) = 0, ..., p_s(x) = 0, f_1(x) > 0, ..., f_l(x) > 0\}$, where $p_i, f_i \in \mathbb{Q}[U, X]$, $U = [U_1, ..., U_d]$ is the set of parameters and $X = [X_{d+1}, ..., X_n]$ the set of unknowns.

If Π_U denotes the canonical projection onto the parameter's space, solving $\mathcal{C}$ or $\mathcal{S}$ is reduced to the computation of submanifolds $\mathcal{U} \subset \mathbb{C}^d$ (resp. $\mathcal{U} \subset \mathbb{R}^d$) such that $(\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}$ (we say that $\mathcal{U}$ has the $(\Pi_U, \mathcal{C})$-*covering property*). This guarantees that the cardinality of $\Pi_U^{-1}(u) \cap \mathcal{C}$ is constant on a neighborhood of u, that $\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}$ is a finite collection of sheets and that Π_U is a local diffeomorphism from each of these sheets onto $\mathcal{U}$.

We show that the complement in $\overline{\Pi_U(\mathcal{C})}$ (the closure of $\Pi_U(\mathcal{C})$ for the usual topology of $\mathbb{C}^n$) of the union of the open subsets of $\overline{\Pi_U(\mathcal{C})}$ which have the $(\Pi_U, \mathcal{C})$-covering property is a Zariski closed and thus is the *minimal discriminant variety of* $\mathcal{C}$ *wrt.* Π_U, denoted W_D. We propose an algorithm to compute W_D efficiently.

The variety W_D can then be used to solve the parametric system $\mathcal{C}$ (resp. $\mathcal{S}$) as long as one can describe $\overline{\Pi_U(\mathcal{C})} \setminus W_D$ (resp. $\mathbb{R}^d \cap (\overline{\Pi_U(\mathcal{C})} \setminus W_D)$), which can be done by using critical points method or an "open" Cylindrical Algebraic Variety.

1 Introduction

In this article, we propose a new algorithm for studying basic constructible (resp. semi-algebraic) sets defined as systems of equations and inequations (resp. inequalities) with rational coefficients and depending on parameters. The following notations will be used:

Notation 1. *Let us consider the basic semi-algebraic set*

$$\mathcal{S} = \{x \in \mathbb{R}^n \quad , \quad p_1(x) = 0, ..., p_s(x) = 0, f_1(x) > 0, ... f_l(x) > 0\}$$

and the basic constructible set

$$\mathcal{C} = \{x \in \mathbb{C}^n \quad , \quad p_1(x) = 0, ..., p_s(x) = 0, f_1(x) \neq 0, ... f_l(x) \neq 0\}$$

where p_i, f_j are polynomials with rational coefficients.

- *$[U, X] = [U_1, ...U_d, X_{d+1}, ...X_n]$ is the set of indeterminates or variables, while $U = [U_1, ...U_d]$ is the set of parameters and $X = [X_{d+1}, ...X_n]$ the set of unknowns;*
- *$\mathcal{E} = \{p_1, ...p_s\}$;*

- *$\mathcal{F} = \{f_1, \ldots f_l\}$;*
- *For any $u \in \mathbb{C}^d$, ϕ_u is the specialization map $U \longrightarrow u$;*
- $\Pi_U\colon \begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C}^d \\ (u_1, \ldots u_d, x_{d+1}, \ldots, x_d) & \mapsto & (u_1, \ldots, u_d) \end{array}$ *denotes the canonical projection on the parameter's space;*
- *Given any ideal I we denote by $\boldsymbol{V}(I) \subset \mathbb{C}^n$ the associated (algebraic) variety. If a variety is defined as the zero set of polynomials with coefficients in $\mathbb{Q}$ we call it a $\mathbb{Q}$-algebraic variety; we extend naturally this notation in order to talk about $\mathbb{Q}$-irreducible components, $\mathbb{Q}$-Zariski closure, ...*
- *for any constructible set $\mathcal{V} \subset \mathbb{C}^n$, $\bar{\mathcal{V}}$ denotes its topological closure for the usual topology of $\mathbb{C}^n$ or equivalently (according to [18] Theorem 2.33 or [19], I.10 Corollary 1) its $\mathbb{C}$-Zariski closure. Moreover, as the sets we consider are proven to be defined by polynomials with rational coefficients, the same notation is also used for the $\mathbb{Q}$-Zariski closures.*

Solving a parametric system may have different meanings depending on the studied problem : counting the roots wrt the parameters, finding simpler expressions, etc.. Independently from the final objective, one needs, in most cases, to characterize open (preferably connected) subsets in the parameter's space over which the number of solutions of the system is constant : this is required for counting the roots wrt the parameters but also, for example, for computing rational parameterizations. In the case where $\overline{\Pi_U(\mathcal{C})} = \mathbb{C}^d$, denoting by $\mathcal{U}$ any open subset in the parameter's space with the above property, it is easy to show that $\mathcal{U}$ can not intersect properly (the intersection is not $\mathcal{U}$ itself) some remarkable subsets of $\overline{\Pi_U(\mathcal{C})}$ such as $\overline{\Pi_U(\mathcal{C})} \setminus \Pi_U(\mathcal{C})$, the projection of the singular points, critical values of Π_U, points with infinite fibers, etc.

Discriminant varieties

In the first part of this paper, we study these subsets in the general complex case ($\mathcal{C}$ without assumption on $\overline{\Pi_U(\mathcal{C})}$) and show that their union, defined as the *minimal discriminant variety of $\mathcal{C}$ wrt* Π_U in the text, is $\mathbb{Q}$-Zariski closed. In short, the complementary of the minimal discriminant variety W_D in $\overline{\Pi_U(\mathcal{C})}$ is a finite union of δ-dimensional submanifolds ($\delta = \dim(\overline{\Pi_U(\mathcal{C})})$ such that $\Pi_U\colon \mathcal{C} \longrightarrow \Pi_U(\mathcal{C}) \setminus W_D$ is an (analytic unramified) cover, and, reciprocally, any δ-dimensional submanifold $\mathcal{U} \subset \Pi_U(\mathcal{C})$ covered by $(\Pi_U, \mathcal{C})$ (such that $\Pi_U\colon \Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C} \longrightarrow \mathcal{U}$ is a cover) does not meet W_D. Poorly speaking, the complementary of the minimal discriminant variety in $\Pi_U(\mathcal{C})$ can be viewed as the projection of the "generic solutions" of $\mathcal{C}$ (the fibers keep a finite constant number of points under an infinitesimal deformation). We additionally show that the minimal discriminant variety can be naturally decomposed as the union of several well identified $\mathbb{Q}$-Zariski closed subsets allowing thus to decompose the problem as well as the computations.

The minimal discriminant variety is an optimal intrinsic object but it can be replaced for many problems by a larger $\mathbb{Q}$-Zariski closed subset containing it, keeping the cover of a dense subset (in $\Pi_U(\mathcal{C})$) of generic solutions by $(\Pi_U, \mathcal{C})$: we name such varieties (non necessarily minimal) *discriminant varieties of $\mathcal{C}$ wrt* Π_U.

The computation of a discriminant variety W_D can be viewed as a preprocessing which splits a system into two subsystems : $(\mathcal{C} \setminus \Pi_U^{-1}(W_D)) \cup (\mathcal{C} \cap \Pi_U^{-1}(W_D))$. The first component is a set of "generic" points of $\mathcal{C}$ (it is empty or has the same dimension as $\mathcal{C}$) while the second one has dimension less or has less irreducible components (when $\dim(\Pi_U(\mathcal{C})) < d$) than $\mathcal{C}$ as long as the system has not an infinite number of solutions for almost all the parameters' values.

In most applications, describing the generic solutions is sufficient since, as we will see in detail later, the other ones mainly correspond to parameters' values whose fibers have an infinite number of points or belong to the projection of components of small dimension with no practical meanings. The non generic solutions can theoretically be studied by applying recursively the same strategy on $(\mathcal{C} \cap \Pi_U^{-1}(W_D))$ so that one could propose a full algorithm for studying all the solutions of a given parametric systems. Such a recursive study is not addressed in the present paper since a careful study requires much more work, in particular to, at least, specify properly the output(s). We thus focus on the study of the "generic" solutions and we mainly propose a strategy for discussing the number of solutions of a parametric system wrt the parameters' values.

Computing Discriminant Varieties in the complex case

In the second part of this article, we propose an algorithm for computing (minimal or non minimal) discriminant varieties in the complex case $(\mathcal{C})$. Our first goal is to propose an efficient solution for a large class of systems : those which are generally zero-dimensional and radical for almost all the specializations of the parameters and defined by a set of equations and inequations (or inequalities) which contains as many equations as unknowns. These systems represents the large class of problems which can (theoretically) be solved numerically for almost all the parameter's values by applying standard algorithm such as Newton's method : they will be called *well behaved systems* in the text. We show that, for such systems, some of the components of the minimal discriminant variety are empty or embedded in some others, making easier the computation of the minimal discriminant variety. For example, one major problem, in practice, is to compute critical values and images of singular points. Using the classical argument on the maximal rank of the minors of some Jacobian matrices supposes working with equidimensional varieties and, basically, assumes that there are represented by radical ideals, which is generally not the case even for well behaved systems. For solving the general case, an easy solution would be to systematically decompose the studied ideals in order to fit such requirements (mainly decomposing as the intersection of radical and equidimensional ideals) but this would have dramatical effects on the efficiency of the proposed solution in most usual situations and, in particular, in the case of well-behaved systems. We better propose an adaptive algorithm which is able to detect automatically and efficiently the favorable/unfavorable situations performing hard computations such as decomposing some ideals only when necessary but also keeping track on the end-user query (no need for example in many situation to compute a minimal discriminant variety).

The real case

The third part of the article is devoted to the real case $(\mathcal{S})$. Over the reals, the subset of parameters which are not contained in a submanifold (of dimension $\dim(\Pi_U(\mathcal{S}))$) covered by $(\Pi_U, \mathcal{S})$ is not, in general, an algebraic variety but a semi-algebraic set. Denoting by $W \cap \mathbb{R}^d$ the real counterpart of any discriminant variety W of the associated complex problem $(\mathcal{C})$ we show that either $\dim(\mathcal{S}) < \dim(\mathcal{C})$ or $W \cap \mathbb{R}^d$ is (non necessarily minimal) real *discriminant variety* of $\mathcal{S}$ (its complementary in $\Pi_U(\mathcal{S})$ is covered by $(\Pi_U, \mathcal{S})$). The first case is easy to detect in practice and occurs when the (real) dimension of $\mathcal{S}$ is less than the dimension of $\mathcal{C}$: one can then compute a Zariski closed set W' such that $\dim(\mathcal{C} \cap \Pi_U^{-1}(W)) < \dim(\mathcal{C})$ and $\mathcal{S} \subset \mathcal{C} \cap \Pi_U^{-1}(W)$ and thus replace $\mathcal{C}$ by $\mathcal{C} \cap \Pi_U^{-1}(W)$ and $\mathcal{S}$ by $\mathcal{S} \cap \Pi_U^{-1}(W)$ (which remains to increase the number of equations).

Using Discriminant Varieties

The fourth section of the present papers show how to use discriminant varieties in order to count the roots of a system wrt the parameters' values.

According to the definition of the discriminant variety, counting the number of roots of $\mathcal{C}$ (or $\mathcal{S}$) wrt to the parameters' values amounts to describe the connected components of $\Pi_U(\mathcal{C}) \setminus W_D$ (or $\Pi_U(\mathcal{S}) \setminus (W_D \cap \mathbb{R}^d)$) : if $\mathcal{U}$ denotes such a component, the constant (finite) number of roots of $\mathcal{C}$ over $\mathcal{U}$ is the number of roots of any specialization $\phi_u(\mathcal{C})$, $u \in \mathcal{U}$. Excepted in the case where $d=1$, the description of W_D is thus not sufficient for many applications : additional computations are required to fully answer to the end-user query (for example discussing the number of solutions wrt the parameters' values) which mostly concerns the real case ($\mathcal{S}$). For a qualitative answer, one may, for example, compute one point on each connected components of $\Pi_U(\mathcal{S}) \setminus W_D$ (see [2],[22],[23],[3] for possible algorithms) and then solve the specializations of the studied system at these sample points (using zero dimensional solvers such as [20], [12] or [25]) to get the possible numbers of roots over the connected subsets which do not meet the discriminant variety. In particular, this allows to compute the maximal or minimal number of "generic" roots of the parametric system.

In most applications however, one needs to provide a full and explicit description of these connected components. Up to our knowledge, the only admissible way to provide a usable output is to compute a cylindrical description. In the absolute, a Cylindrical Algebraic Decomposition (CAD [5]) of the parameter's space, compatible with the polynomials defining the discriminant variety, would provide a satisfactory output (more details are given below). Since we are interested only in computing the cells of highest dimension, we use a dedicated variant of the CAD (as in [7]) to describe only $\Pi_U(\mathcal{S}) \setminus W_D$ instead of computing a full decomposition of $\mathbb{R}^d$ compatible with the polynomials used to define $\Pi_U(\mathcal{S}) \setminus W_D$.

Discriminant varieties vs existing strategies for "solving" parametric systems

- *Solutions based on triangular sets for systems of equations* (see [26] for a general overview). A good way for solving parametric systems of equations ($\mathcal{F} \neq 0$) is to decompose them as solutions of a finite union of so called regular and separable triangular sets (or simply lexicographic Gröbner bases in some special cases) such as defined in [1] :

  - $\mathcal{T}_j = \{f_{j,d}(U_1, ..., U_d), f_{j,d+1}(U_1, ..., U_d, X_{d+1}), f_{j,d+2}(U_1, ..., U_d, X_{d+1}, X_{d+2}), ..., f_{j,n}(U_1, ..., U_d, X_{d+1}, ..., X_n)\}$, where some $f_{j,i}$ could be identically null. $\mathcal{T}_j$ is said to be regular (resp. separable) if $\mathrm{LM}_{X_i}(f_{j,i})$ (resp. $\frac{\partial f_{j,i}}{\partial X_i}$) does not vanish on an irreducible component of $\mathbf{V}(\mathcal{T}_j)$, $\mathrm{LM}_{X_i}(f_{j,i})$ being the leading monomial of $f_{j,i}$ wrt the variable X_i.

  Regular and separable triangular sets thus provide a quite "simple" description (by means of a tower of field extensions) of their solutions outside the zero set of $\mathrm{LM}_{X_i}(f_{j,i})$ and $\frac{\partial f_{j,i}}{\partial X_i}$, which forms a (non minimal) discriminant variety. The union of the discriminant varieties of the triangular components of a decomposition as well as the projections of the intersections of these components forms a discriminant variety which depends on the kind of triangular sets computed (Kalkbrenner, Lazard, etc.) and the ordering used on the variables.

- *Rational parameterizations* ([24]). With the end-user point a view, a rational parametrization is certainly the most friendly simplification for parametric systems. It may be viewed as a particular case of triangular system in t he case of consistent parametric systems : modulo a generic linear change of variables (or equivalently introducing a new variable T which is a linear combination of the others), a rational parametrization of the zero set of a parametric system (generically zero-dimensional of dimension d) may have generically the following shape

  - $\mathcal{R} = \{f_t(U_1, \ldots, U_d, T), X_{d+1} = \frac{g_{d+1}(U_1, \ldots, U_d, T)}{g(U_1, \ldots, U_d, T)}, \ldots, X_n = \frac{g_n(U_1, \ldots, U_d, T)}{g(U_1, \ldots, U_d, T)}\}$.

As for triangular systems, a rational parametrization of the solution set of a consistent parametric system gives a simple representation of the solution set of a system of equations outside the zero set of $\mathrm{LM}_T(f_t)$ and $\frac{\partial f_t}{\partial T}$ whose projection on the parameter's space forms a discriminant variety. This discriminant variety is not minimal in general since it depends on the linear generic change of variable's performed (it contains the U - coordinates of the points on which the projection canonically associated with the "generic" change of variables is not injective).

- *Algorithms using Comprehensive Gröbner bases.* A comprehensive Gröbner basis (notion introduced in [27]) is a set of polynomial which is a Gröbner basis for all specializations of the parameters. Such an object can not directly be used for discussing the number of solutions wrt parameter's values or computing "rational" parameterizations (the basic purpose is to study specializations without computing their Gröbner basis) but there exist some algorithms extending classical methods for zero-dimensional systems in the case of consistent parametric systems which exploit such structures. For example ([28]), counting roots can be done by constructing the so called Hermite's quadratic form (with parametric coefficients) and computing its rank, which induces case distinctions depending on parameter's values which are sets of inequations and equations. These sets can not define a minimal discriminant variety in general since they strongly depend on the monomial ordering used (Gröbner basis computation) and on the order some tests are performed (pivot in the reduction of the quadratic form).

  Note : the notion of discriminant ideal, introduced in [17] for improving the computation of comprehensive Gröbner basis is not linked to our notion of minimal discriminant variety.

- *Cylindrical Algebraic Decompositions* ([5]). Given the polynomials of $\mathcal{E}$ and $\mathcal{F}$, the CAD computes a partition of the ambient space $\mathbb{C}^n$ or $\mathbb{R}^n$ into cells (homeomorphic to bowls of various dimensions) on which these polynomials have constant signs. The basic algorithm first eliminates variables one by one (projection step) by computing, at each step, a discriminant variety wrt the remaining variables of the set of inequations constituted by all the polynomials computed at the precedent step. When eliminating first the indeterminates, one obtains, after $n-d$ steps a discriminant variety of the union of all the constructible sets which can be defined by the polynomials given as input. This discriminant variety is obviously not minimal in most cases.

Complexity issues

We do not address the problem of computing the complexity of the algorithm or of the size of its output in this paper. The minimal discriminant variety being an optimal object (at least in the complex case) the study of its complexity is of high interest but will be the subject of another contribution. One starting point can be found in [13] : the authors compute the distribution of so called vectors of multiplicities of a parametric constructible set wrt to the parameters' values using Gröbner bases. In short, they compute a partition of the parameter's space in subsets where the fibers have a constant (finite) number of points with constant multiplicities. This partition is given as a union of non overlapping constructible sets and one can thus easily deduce from this output a (non minimal) discriminant variety. Results from [13] show that if the degrees of the polynomials of $\mathcal{E} \cup \mathcal{F}$ are bounded by D, then the degrees of the polynomials defining the the discriminant variety are bounded by $D^{O(n^2)}$ and, moreover, the running time of the related algorithm is less than $D^{O(n^2 d)}$.

2 Discriminant varieties in the complex case

In this section, we will need to use two topologies on $\mathbb{C}^n$: the usual one and the Zariski one. The closure of any constructible set $\mathcal{C}$ will be denoted by $\bar{\mathcal{C}}$ in both cases since they coincide according to [19]. Let us start with a precise definition of a discriminant variety of $\mathcal{C}$ wrt. Π_U :

Definition 2. *Let δ be the dimension of $\overline{\Pi_U(\mathcal{C})} = \overline{\Pi_U(\bar{\mathcal{C}})}$. An algebraic variety W is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U if and only if:*

- *W is contained in $\overline{\Pi_U(\mathcal{C})}$*
- *$W = \overline{\Pi_U(\mathcal{C})}$ if and only if $\Pi_U^{-1}(u) \cap \mathcal{C}$ is infinite or empty for almost all $u \in \Pi$;*
- *The connected components $\mathcal{U}_1, \ldots \mathcal{U}_k$ of $\overline{\Pi_U(\mathcal{C})} \setminus W$ are analytic submanifolds of dimension δ (if $\Pi_U(\mathcal{C})$ is d-dimensional, this condition is automatically satisfied, this is especially the case when $\overline{\Pi_U(\mathcal{C})} = \mathbb{C}^d$);*
- *For $i = 1 \ldots k$, $(\Pi_U^{-1}(\mathcal{U}_i) \bigcap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}_i$.*

If W is a discriminant variety, $(\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}$ for $\mathcal{U} \in \{\mathcal{U}_1, \ldots, \mathcal{U}_k\}$, which implies that:

- there exist a finite set of indexes $\mathcal{I}$ and disjoint connected subsets $(\mathcal{V}_i)_{i \in \mathcal{I}}$ of $\mathcal{C}$ such that $\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C} = \bigcup_{i \in \mathcal{I}} \mathcal{V}_i$;
- Π_U is a local diffeomorphism from $\mathcal{V}_i$ onto $\mathcal{U}$;

Since $\mathcal{C}$ is a constructible set, for any $u \notin W$, the discrete set $\Pi_U^{-1}(u) \bigcap \mathcal{C}$ is necessarily finite. In particular, W contains the projection of every component of dimension $> \delta$ of $\mathcal{C}$.

If O_{sd} is the projection (image by Π_U) of the irreducible components of $\bar{\mathcal{C}}$ of dimension $< \delta$, then O_{sd} is necessarily contained in W.

If O_∞ is the set of the $u \in \overline{\Pi_U(\mathcal{C})}$ such that $\Pi_U^{-1}(\mathcal{U}) \bigcap \bar{\mathcal{C}}$ is not compact for any compact neighborhood $\mathcal{U}$ of u, then $\mathcal{O}_\infty \subset W$. In fact, if $\mathcal{U} \subset \overline{\Pi_U(\mathcal{C})} \setminus W$ is a compact neighborhood of a point of $\overline{\Pi_U(\mathcal{C})} \setminus W$, then $\Pi_U^{-1}(\mathcal{U}) \bigcap \bar{\mathcal{C}}$ is compact since the restriction of Π_U on each $\mathcal{V}_i$ is a local diffeomorphism.

If O_c is the union of the critical values of Π_U (in restriction to the regular locus of $\mathcal{C}$) and of the images by Π_U of the singular point of $\mathcal{C}$, O_c is also contained in W since the restriction of Π_U to $\mathcal{V}_i$ is a local diffeomorphism. On may notice that the critical values of Π_U on the components of $\bar{\mathcal{C}}$ of dimension $\neq \delta$ are contained in $O_{sd} \cup O_\infty$. Thus, one may restrict O_c to the critical values and images by Π_U of the singular points of $\mathcal{C}$ in restriction to the union of the components of dimension δ.

Notation 3. *We denote by critical values "at large" of Π_U the union of the critical values of Π_U (in restriction to the regular locus of $\bar{\mathcal{C}}$) and of the projection of the singular locus of $\bar{\mathcal{C}}$.*

If $x \in \bar{\mathcal{C}} \setminus \mathcal{C}$, then $\Pi_U(x) \in W$ since Π_U is a local diffeomorphism.

Finally, if W_{sing} is the singular locus of $\overline{\Pi_U(\mathcal{C})}$, then, by definition, $W_{sing} \subset W$. One may notice that in many applications, $d = \delta$, which means that $\overline{\Pi_U(\mathcal{C})} = \mathbb{C}^d$ and implies $W_{sing} = \emptyset$.

The following lemma summarizes these properties and definitions:

Lemma 4. *Let $\mathcal{C}$ be a constructible set defined as in Notation 1 and $\bar{\mathcal{C}}$ be its closure in $\mathbb{C}^n$ (for the usual topology or for the Zariski topology). Let us define:*

- *O_{sd} the projection of the irreducible components of $\bar{\mathcal{C}}$ of dimension less than δ;*
- *O_c the critical values "at large" of Π_U in restriction to $\bar{\mathcal{C}}$.*
- *O_∞ the set of points $u \in \overline{\Pi_U(\mathcal{C})}$ such that $\Pi_U^{-1}(\mathcal{U}) \bigcap \bar{\mathcal{C}}$ is not compact for any compact neighborhood $\mathcal{U}$ of u in $\overline{\Pi_U(\mathcal{C})}$;*
- *$O_{\mathcal{F}}$ (resp. O_{F_i}) the projection of the intersection of $\bar{\mathcal{C}}$ with the hypersurface defined by $\prod_{i=1}^s f_i$ (resp. by f_i);*
- *O_{sing} the singular locus of $\overline{\Pi_U(\mathcal{C})}$.*

Then, if W is a discriminant variety of $\mathcal{C}$ wrt Π_U, we have $O_{sd} \cup O_c \cup O_\infty \cup O_{\mathcal{F}} \cup W_{sing} \subset W$.

We will now show that $O_{sd} \cup O_c \cup O_\infty \cup O_{\mathcal{F}} \cup O_{sing}$ is a discriminant variety, and thus the smallest one. In addition, we will give an algebraic characterization of this smallest discriminant variety, making possible its computation (described in the next section). Finally, we will show that this minimal discriminant variety has a dimension smaller than $\delta = \dim(\overline{\Pi_U(\mathcal{C})})$ if and only if the projection by Π_U of the irreducible components of dimension $> \delta$ of $\bar{\mathcal{C}}$ has dimension $< \delta$.

We first show that $O_{sing} \cup O_{sd} \cup O_c \cup O_\infty \cup O_{\mathcal{F}}$ is a $\mathbb{Q}$-algebraic variety. As we will have to consider the $\mathbb{Q}$-Zariki closures of these components, we introduce the following notation:

Notation 5. *For any set $O_.$, we denote by $W_.$ its $\mathbb{Q}$-Zariski closure. For example, W_c will be the $\mathbb{Q}$-Zariski closure of O_c. Note that we obviously have $W_{\text{sing}} = O_{\text{sing}}$.*

A key point is to show that $O_\infty = W_\infty$:

Lemma 6. *The set O_∞ is $\mathbb{Q}$-Zariski closed. More precisely, it is equal to $W_\infty := \pi(\bar{\mathcal{C}}^{\mathbb{P}} \bigcap \mathcal{H}_\infty)$, where:*

- *$\mathbb{P}^{n-d}$ is the projective space associated to $\mathbb{C}^{n-d}$;*
- *$\bar{\mathcal{C}}^{\mathbb{P}}$ is the projective closure of $\mathcal{C}$ in $\mathbb{C}^d \times \mathbb{P}^{n-d}$;*
- *$\mathcal{H}_\infty$ is the hyperplane at infinity in $\mathbb{C}^d \times \mathbb{P}^{n-d}$, i.e. $\mathcal{H}_\infty = \left(\mathbb{C}^d \times \mathbb{P}^{n-d}\right) \setminus \left(\mathbb{C}^d \times \mathbb{C}^{n-d}\right)$;*
- *π is the canonical projection from $\mathbb{C}^d \times \mathbb{P}^{n-d}$ to $\mathbb{C}^d$.*

Proof. According to [8] (Corollary 10 p. 389), if $\mathcal{C} \subset \mathbb{C}^n$ is any constructible set, then $\bar{\mathcal{C}} = \bar{\mathcal{C}}$ and $\overline{\Pi_U(\mathcal{C})} = \overline{\Pi_U(\mathcal{C})}$ (see [19]) and $\overline{\Pi_U(\bar{\mathcal{C}})} = \overline{\Pi_U(\mathcal{C})} = \pi(\bar{\mathcal{C}}^{\mathbb{P}})$. Since $\bar{\mathcal{C}}$ is the affine part of $\bar{\mathcal{C}}^{\mathbb{P}}$, then:

$$\overline{\Pi_U(\bar{\mathcal{C}})} = W_\infty \cup \Pi_U(\bar{\mathcal{C}}). \tag{1}$$

According to [18], W_∞ is a $\mathbb{C}$-algebraic variety since it is the projection on the affine space $\mathbb{C}^d$ of a $\mathbb{C}$-variety of $\mathbb{C}^d \times \mathbb{P}^{n-d}$. Moreover, it is a $\mathbb{Q}$-variety since it can be written as the intersection of $\mathbb{Q}$-varieties.

Let $u \in \overline{\Pi_U(\mathcal{C})}$. If $u \notin W_\infty$, then according to (1), there exist a compact neighborhood $\mathcal{U} \subset \Pi_U(\bar{\mathcal{C}})$ of u such that $\mathcal{U} \cap W_\infty = \emptyset$, and thus $\Pi_U^{-1}(\mathcal{U}) \cap \bar{\mathcal{C}} = \pi^{-1}(\mathcal{U}) \cap \bar{\mathcal{C}}^{\mathbb{P}}$ viewing the affine space $\mathbb{C}^n$ as an open subspace of the projective space $\mathbb{P}^n$. Since π is continuous $\Pi_U^{-1}(\mathcal{U}) \bigcap \bar{\mathcal{C}}$ is then compact, which shows that $u \notin O_\infty$ and $O_\infty \subset W_\infty$.

On the other hand, if u belongs to W_∞, there exist, by definition of W_∞, an element t of $\mathbb{P}^{n-d}$ such that $(u,t) \in \bar{\mathcal{C}}^{\mathbb{P}} \cap \mathcal{H}_\infty$. By definition of $\bar{\mathcal{C}}^{\mathbb{P}}$, any neighborhood of (u,t) in $\mathbb{C}^d \times \mathbb{P}^{n-d}$ meets $\bar{\mathcal{C}}$, which implies that the reciprocal image by Π_U of any compact neighborhood of u intersects $\bar{\mathcal{C}}$ and is not compact since it is different from its closure in $\mathbb{C}^d \times \mathbb{P}^{n-d}$. Thus $W_\infty \subset O_\infty$. □

The sets O_{sd} and O_c are not Zariski closed in general, but they are projections of $\mathbb{Q}$-Zariski closed subsets of $\bar{\mathcal{C}}$. Thus, according to the relation (1), we have $\overline{O_{\text{sd}}} \setminus O_{\text{sd}} \subset W_\infty$ and $\overline{O_c} \setminus O_c \subset W_\infty$, which shows :

Lemma 7. *$O_{sd} \bigcup O_c \bigcup O_\infty$ is $\mathbb{Q}$-Zariski closed. More precisely :*

$$O_{sd} \bigcup O_c \bigcup O_\infty = W_{sd} \bigcup W_c \bigcup W_\infty$$

By definition, W_{sing}, W_{sd} and W_c are closed subsets of dimension $< \delta$; thus, $O_{sing} \bigcup O_{sd} \bigcup O_c \bigcup O_\infty$ is a closed set which is strictly contained in $\overline{\Pi_U(\mathcal{C})}$ if and only if $W_\infty = O_\infty$ is strictly contained in $\overline{\Pi_U(\mathcal{C})}$.

If $\mathcal{D}$ is a connected component of $\bar{\mathcal{C}}$, a polynomial $f_i \in \mathcal{F}$ can not be identically null on $\mathcal{D}$ (by definition of $\mathcal{C}$). Thus $\overline{\Pi_U(\boldsymbol{V}(f_i) \cap \bar{\mathcal{C}})}$is a strict subset of $\overline{\Pi_U(\mathcal{C})}$. Using again (1), $O_{\mathcal{F}}$ is the projection of an algebraic set contained in $\bar{\mathcal{C}}$ and $(\overline{O_{\mathcal{F}}} \setminus O_{\mathcal{F}}) \subset W_\infty$. Setting $W_{\mathcal{F}} = \bar{\mathcal{F}}$, we obtain the following result:

Lemma 8. *The set $O_\infty \bigcup O_{\mathcal{F}}$ is $\mathbb{Q}$-Zariski closed and is contained in every discriminant variety of $\mathcal{C}$. Therefore,*

$$O_{sing} \bigcup O_{sd} \bigcup O_c \bigcup O_\infty \bigcup O_{\mathcal{F}} = W_{sing} \bigcup W_{sd} \bigcup W_c \bigcup W_\infty \bigcup W_{\mathcal{F}}$$

is also $\mathbb{Q}$-Zariski closed.

According to this lemma, we have defined a $\mathbb{Q}$-algebraic variety which is contained in any discriminant variety. It remains to show that this object is itself a discriminant variety:

Theorem 9. *$W_D = O_{sing} \bigcup O_{sd} \bigcup O_c \bigcup O_\infty \bigcup O_{\mathcal{F}} = W_{sing} \bigcup W_{sd} \bigcup W_c \bigcup W_\infty \bigcup W_{\mathcal{F}}$ is the smallest discriminant variety of $\mathcal{C}$ w.r.t. Π_U.*

Proof. The only thing to prove is that, $\forall u \in \overline{\Pi_U(\mathcal{C})} \setminus W_D$, there exist a sub-manifold $\mathcal{U} \subset \overline{\Pi_U(\mathcal{C})}$ of dimension δ containing u and such that $(\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}$.

If $W_\infty = \overline{\Pi_U(\mathcal{C})}$, then $W_D = \overline{\Pi_U(\mathcal{C})}$ and the lemma is proved. Let us now suppose that $W_\infty \neq \overline{\Pi_U(\mathcal{C})}$. In that case, W_D is strictly contained in $\overline{\Pi_U(\mathcal{C})}$ (the other components of W_D have dimension $< \delta$).

By definition $W_\infty \subset W_D$, and thus $\Pi_U^{-1}(u) \bigcap \mathcal{C}$ is a non empty compact set for any $u \notin W_D$. It is therefore finite. More generally, by continuity of Π_U, if $\mathcal{U}$ is a compact neighborhood of u in $\overline{\Pi_U(\mathcal{C})}$ which does not meet W_D, then $\Pi_U^{-1}(\mathcal{U}) \bigcap \bar{\mathcal{C}}$ is compact. Since $W_{sing} \subset W_D$, there always exist a neighborhood $\mathcal{U}$ of u contained in Π_U that is a sub-manifold of dimension δ.

Let u be a point in $\overline{\Pi_U(\mathcal{C})} \setminus W_D$ and $\mathcal{U}$ a compact neighborhood of u such that $\mathcal{U} \bigcap W_D = \emptyset$. Let $\mathcal{D}$ be a connected component of $\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}$. Since $\mathcal{D}$ is compact, if $\mathcal{D}$ does not meet $\Pi_U^{-1}(u)$, we can restrict $\mathcal{U}$ to a sub-manifold $\mathcal{U}' \subset \mathcal{U}$ containing u and such that $\Pi_U^{-1}(\mathcal{U}') \bigcap \mathcal{D} = \emptyset$. Similarly, we can suppose that all the connected components of $\Pi_U^{-1}(\mathcal{U}) \bigcap \mathcal{C}$ intersect $\Pi_U^{-1}(u)$. Since $u \notin O_\infty \bigcup O_{sd}$, these components have dimension δ. Since $u \notin O_c$, the implicit functions theorem applies. After having possibly reduced $\mathcal{U}$, Π_U then defines a $\mathbb{C}^\infty$-diffeomorphism between each of these connected components and $\mathcal{U}$ and thus, $(\Pi_U^{-1}(\mathcal{U}), \Pi_U)$ is an analytic covering of $\mathcal{U}$. □

3 Algorithms in the complex case

In this section, we propose a general algorithm for computing the minimal discriminant variety of any basic constructible set.

Given any ideal $I \subset \mathbb{Q}[U, X]$ such that $\boldsymbol{V}(I) = \bar{\mathcal{C}}$, we will first recall how to compute d, δ, $I \cap \mathbb{Q}[U]$ (Algorithm PREPROCESSING) and how to compute the generators of ideals $I_{\mathcal{F}}, I_\infty \subset \mathbb{Q}[U]$ such that $\boldsymbol{V}(I_\infty) = W_\infty$ and $\boldsymbol{V}(I_{\mathcal{F}}) = W_{\mathcal{F}}$ (Algorithm PROPENESSDEFECTS) without any assumption on $\mathcal{E}$.

The computation of the other components of W_D (or of any discriminant variety) depends strongly on the properties of I. In short, the computation of W_c, W_{sing} or W_{sd} may require to decompose I into equidimensional and radical components. Such a preprocessing is, in practice, too costly (according to the current state of the art) when dealing with large systems and must be avoided when possible.

Notation 10. *Let $I \subset \mathbb{Q}[Y]$ be an ideal, $Y' \subset Y$ a set of variables, $k \leq \#Y'$ a positive integer. We denote by $\mathrm{Jac}_{Y'}^k(I)$ the ideal generated by all the minors of dimension k of the Jacobian matrix wrt the Y' of any system of generators of I.*

We will show that there are only few practical cases where the computation of a decomposition of I or of its radical may be useful and we will propose an adaptive algorithm performing such costly operations only when required.

Let us consider, for example, the computation of W_c. If I is prime, W_c is the zero set of $(I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]$. This characterization can be extended to equidimensional and radical ideals but not to the general case (consider for example the system $P^2 = 0$ where P is a non constant polynomial in $\mathbb{Q}[U, X]$). For many parametric systems coming from applications, $\phi_u(\mathcal{E})$ can be numerically solved for almost all $u \in \mathbb{R}^d$ using simple versions of Newton's algorithm. This means in particular that $d = \delta$, $s = n - \delta$ and that $\langle \phi_u(\mathcal{E}) \rangle$ is radical and zero-dimensional for almost all $u \in \mathbb{R}^d$. For this class of systems, $\langle \mathcal{E} \rangle$ may be not radical nor equidimensional, but we always have $W_{\text{sd}} = W_{\text{sing}} = \emptyset$.

We will show that even when $W_c \not\subset (I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]$, such systems always satisfy $W_D = W_{\mathcal{F}} \cup W_\infty \cup \boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]))$ and there is no need to decompose I nor to compute its radical. More generally, we will characterize a class of systems for which $W_D = W_{\mathcal{F}} \cup W_\infty \cup \boldsymbol{V}(I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]) \cup \boldsymbol{V}(I \cap \mathbb{Q}[U] + \mathrm{Jac}_U^{d-\delta}(I \cap \mathbb{Q}[U]))$ and propose an algorithm (Algorithm CORE) that first checks if a problem belongs to this class and, if it does, computes straightforwardly its minimal discriminant variety.

If this algorithm detects that the problem does not belong to this favorable class, there are many situations where $W' = W_{\mathcal{F}} \cup W_\infty \cup \boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]) \cup \boldsymbol{V}(I \cap \mathbb{Q}[U] + \mathrm{Jac}_U^{d-\delta}(I \cap \mathbb{Q}[U]))$ is a large discriminant variety or a large discriminant variety where the components of W_{sd} are missing. Even in the latter case, this variety may be an acceptable answer : W' is then a discriminant variety of the union of the components of dimension $\geq \delta$ of $\mathcal{C}$. Also, over each connected open subset of $\mathcal{U} \subset \left(\overline{\Pi_U(\mathcal{C})} \setminus W'\right)$, the number of solutions is constant for all the parameters of $\mathcal{U}$ that do not belong to W_{sd} (and thus for almost all the parameters of $\mathcal{U}$). For many applications, this information is sufficient and there is no need to compute a discriminant variety. In section 5.2, for example, the parameters represent the lengths of some physical components of a robot : because of unavoidable manufacturing errors, it does not make sense to study the case where they belong to a strict Zariski closed subset of the parameter's space.

In the proposed general algorithm, such subjective elements of decision are set by the user. The computations are dynamically driven by these informations as well as the (algebraic or geometrical) properties detected at each step.

3.1 Conditions free computations (Algorithms PREPROCESSING and PROPERNESSDEFECTS)

Most of the components of the minimal discriminant variety are the $\mathbb{Q}$-Zariski closure of the projection by Π_U of some algebraic variety V; if I is an ideal which defines this variety ($\boldsymbol{V}(I) = V$), then $\overline{\Pi_U(V)} = \boldsymbol{V}(I \bigcap \mathbb{Q}[U])$. If G is a Gröbner basis of I for a monomial ordering which eliminates X, then $G \bigcap \mathbb{Q}[U]$ is a Gröbner basis of $I \bigcap \mathbb{Q}[U]$, and this is the simplest way to compute $\overline{\Pi_U(V)}$. In practice, the most efficient monomial ordering is a block ordering which is the Degree Reverse Lexicographic one (DRL) on each block :

Notation 11. *Let $Y = [U_1, ..., U_d, X_{d+1}, ..., X_n]$. If $<_U$ (resp. $<_X$) is an admissible monomial ordering for the monomials depending on the variables U (resp. X), then $<_{U,X} = (<_U, <_X)$ will denote the product of orderings such that $U_i <_{U,X} X_i$ for $U_i \in U$ and $X_i \in X$.*

For any polynomial $g \in \mathbb{Q}[U, X]$, $\mathrm{LM}_{<_X}(g)$ (resp. $\mathrm{LC}_{<_X}(g)$), will denote the (monic) leading monomial (resp. the leading coefficient) with respect to $<_X$ of g viewed as a polynomial in the variables X with coefficients in $\mathbb{Q}[U]$. Note that with this notation, $\mathrm{LC}_{<_X}(g)$ is a polynomial in U.

According to [8] we have:

Proposition 12. *Let G be a Gröbner basis of an ideal $I \subset \mathbb{Q}[U, X]$ w.r.t. $<_{U,X}$, then $G \bigcap \mathbb{Q}[U]$ is a Gröbner basis of $I \bigcap \mathbb{Q}[U]$ w.r.t. $<_U$.*

Let T be a new indeterminate, then $\overline{\boldsymbol{V}(I) \setminus \boldsymbol{V}(f)} = \boldsymbol{V}((I + \langle T f - 1\rangle) \bigcap \mathbb{Q}[U, X])$. If $G' \subset \mathbb{Q}[U, X, T]$ is a Gröbner basis of $I + \langle T f - 1\rangle$ with respect to $<_{(U,X),T}$ then $G' \bigcap \mathbb{Q}[U, T]$ is a Gröbner basis of $I: f^\infty := (I + \langle T f - 1\rangle) \bigcap \mathbb{Q}[U, X]$ w.r.t. $<_{(U,X)}$. The variety $\overline{\boldsymbol{V}(I) \setminus \boldsymbol{V}(f)}$ and the ideal $I: f^\infty$ are usually called the saturations of $\boldsymbol{V}(I)$ and I by f.

These well known results reduce the computation of ideals defining $\bar{\mathcal{C}}$, $\overline{\Pi_U(\mathcal{C})}$, δ and $W_{\mathcal{F}}$ to single Gröbner bases computation for block orderings: The ideal I such that $\boldsymbol{V}(I) = \bar{\mathcal{C}}$ is the saturation of $\langle \mathcal{E} \rangle$ by $\prod_{i=1}^l f_i$ (or successively by each f_i). We can represent $\overline{\Pi_U(\mathcal{C})}$ as $\boldsymbol{V}(I \bigcap \mathbb{Q}[U])$, and its dimension δ is, in practice, easily deduced from the Gröbner basis, although this is a NP-complete problem [8]. Finally, $W_{\mathcal{F}} = \boldsymbol{V}((I + \langle \prod_{i=1}^l f_i \rangle) \bigcap \mathbb{Q}[U])$ or equivalently $W_{\mathcal{F}} = \boldsymbol{V}((\langle \mathcal{E} \rangle : (\prod_{i=1}^l f_i) + \langle \prod_{i=1}^l f_i \rangle) \bigcap \mathbb{Q}[U])$.

Remark 13. The computation of $\langle\mathcal{E}\rangle : (\prod_{i=1}^{l} f_i)$ can be avoided in several situations :

- if $(\langle\mathcal{E}\rangle + \langle \prod_{i=1}^{l} f_i\rangle) \bigcap \mathbb{Q}[U]$ has dimension $< \delta$: in such a case the irreducible components of $\boldsymbol{V}(\langle\mathcal{E}\rangle)$ that belong to $\boldsymbol{V}(\prod_{i=1}^{l} f_i)$ have a projection of dimension $< \delta$ and so belong to $\Pi_U^{-1}(W_{\mathrm{sd}} \bigcup W_\infty)$.
- if $\prod_{i=1}^{l} f_i \in \langle\mathcal{E}\rangle$ (which can easily be tested by the testing the equality of the Gröbner bases of $\langle\mathcal{E}\rangle$ and $\langle\mathcal{E}\rangle + \langle \prod_{i=1}^{l} f_i\rangle$) then $\overline{\Pi_U(\mathcal{C})} = \emptyset$ (the system has no solutions).

The algorithm PREPROCESSING, detailed in section 7, uses the above results for computing δ, $W_{\mathcal{F}}$, $\bar{\mathcal{C}}$ and $\overline{\Pi_U(\mathcal{C})}$ and the later remark for optimizing the computations. Its specifications are the following :

Algorithm PREPROCESSING

- **Input** : $\mathcal{E}, \mathcal{F}, U, X$
- **Output** : $\delta, G, G_\Pi, G_{\mathcal{F}}$ such that
  - G is a reduced Gröbner basis for $<_{U,X}$ such that $\mathcal{C} \cap \Pi_U^{-1}(\overline{\Pi_U(\mathcal{C})} \setminus W_{\mathcal{F}}) = \boldsymbol{V}(\langle G\rangle) \cap \Pi_U^{-1}(\overline{\Pi_U(\mathcal{C})} \setminus W_{\mathcal{F}})$;
  - G_Π, $G_{\mathcal{F}}$ are reduced Gröbner bases for $<_U$ such that $\boldsymbol{V}(\langle G_\Pi\rangle) = \overline{\Pi_U(\mathcal{C})}$ and $\boldsymbol{V}(\langle G_{\mathcal{F}}\rangle) = W_{\mathcal{F}}$;

We are now going to prove that we can represent W_∞ as the zeros of some Gröbner bases, which may be extracted without any further computation from those already computed by the PREPROCESSING algorithm.

Theorem 14. *Let G be a reduced Gröbner basis of any ideal I such that $\boldsymbol{V}(I) = \bar{\mathcal{C}}$, computed wrt a product ordering $<_{U,X}$ where $<_X$ is the Degree Reverse Lexicographic ordering s.t. $X_{d+1} < \ldots < X_n$. We define $\mathcal{E}_i^\infty = \{\mathrm{LM}_{<_X}(g) \mid g \in G \ , \ \exists m \geq 0, \ \ \mathrm{LM}_{<_X}(g) = X_i^m\}$, and $\mathcal{E}_0 = G \bigcap \mathbb{Q}[U]$. Then:*

- *$\mathcal{E}_0$ is a Gröbner basis of $I \bigcap \mathbb{Q}[U]$ w.r.t. $<_U$ and $\mathcal{E}_0 \subset \mathcal{E}_i^\infty$ for $i = d+1 \ldots n$;*
- *$\mathcal{E}_i^\infty$ is a Gröbner basis of some ideal $I_i^\infty \subset \mathbb{Q}[U]$ w.r.t. $<_U$;*
- *$W_\infty = \bigcup_{i=d+1}^{n} \boldsymbol{V}(I_i^\infty)$.*

Proof. The first item is a direct consequence of the definition of $\mathcal{E}_0$ and $\mathcal{E}_i^\infty$ and of Proposition 12.

Let $p \in \mathbb{Q}[U, X]$. We say that p is a X-homogeneous polynomial of degree k if $p = \sum_{|\alpha|=k} h_\alpha(U) X^\alpha$. Let T be a new variable. We define the (X, T)-homogenization of p as being the (X, T)-homogeneous polynomial $p^h = \mathbb{Q}[T, U, X]$ of degree degree(p, X) such that $p^h(U, X, 1) = p$. By extension, if G is a set of polynomials of $\mathbb{Q}[U, X]$, G^h is the set of (X, T)-homogenizations of the elements of G and if I is an ideal of $\mathbb{Q}[U, X]$, I^h is the (X, T)-homogeneous ideal generated by the (T, X)-homogenizations of polynomials of I. If G is a Gröbner basis of I for $<_{U,X}$ then G^h is a Gröbner basis of I^h for the ordering $<_h$ such that $U^{\alpha_1} X^{\beta_1} T^{\gamma_1} <_h U^{\alpha_2} X^{\beta_2} T^{\gamma_2}$ if and only if ($\gamma_1 = \gamma_2$ and $U^{\alpha_1} X^{\beta_1} <_{U,X} U^{\alpha_2} X^{\beta_2}$) or ($\gamma_1 < \gamma_2$), and we have $\overline{\boldsymbol{V}(I)}^{\mathbb{P}} = \boldsymbol{V}(G^h) = \boldsymbol{V}(I^h)$ ([8] Theorem 4 p. 375).

In the following, we need to consider the specialization map:

$$\begin{array}{cccc} \Psi_j^a\colon & \mathbb{Q}[T, U, X] & \longrightarrow & \mathbb{Q}[U, X_{j+1}, \ldots X_n] \\ & T & \mapsto & 0 \\ & X_{d+1} & \mapsto & 0 \\ & \vdots & & \vdots \\ & X_{j-1} & \mapsto & 0 \\ & X_j & \mapsto & 1 \end{array}$$

The definition of the Degree Reverse Lexicographic ordering makes almost immediate the following lemma from which the remainder of the proof will be easily deduced.

Lemma 15. *Let $g \in \mathbb{Q}[U, X]$; then :*

- *The ordering w.r.t. $<_{U,X}$ of the monomials in g is the same as the ordering of their images in $\Psi_j^a(g^h)$, using as convention that monomials with a null image are the smallest ones in g.*
- *If $\Psi_j^a(\mathrm{LM}_{<_{U,X}}(g^h)) = 0$ then $\Psi_j^a(g^h) = 0$.*
- *$\Psi_j^a(g^h) = 0$ if and only if $\mathrm{LM}_{<_{U,X}}(g)$ depends on $\{X_1, \ldots, X_{j-1}\}$.*
- *If $\Psi_j^a(g^h) \neq 0$ then $\Psi_j^a(g^h) \in \mathbb{Q}[U]$ if and only if $\mathrm{LM}_{<_X}(g)$ is a power of X_j.*

Moreover, if G is a reduced Gröbner basis of the ideal I for the monomial ordering $<_{U,X}$ then $\Psi_j^a(G^h)$ is a reduced Gröbner basis of $\Psi_j^a(I^h)$ for the same ordering.

Proof. The last assertion is an immediate consequence of the first ones: the proofs that G and $\Psi_j^a(G^h)$ are reduced Gröbner bases are exactly the same, as they involve only the ordering and the leading terms of the polynomials.

The other assertions are immediate consequence of the definition of the Degree Reverse Lexicographical ordering. For any set of variables $Y = Y_1, \ldots, Y_n$ it is defined as: $Y_1^{a_1} \cdots Y_n^{a_n} < Y_1^{b_1} \cdots Y_n^{b_n}$ if and only if $\sum_1^n a_i < \sum_1^n b_i$ or $\sum_1^n a_i = \sum_1^n b_i$ and there is an index j such that $a_j > b_j$ and $\forall i < j, \quad a_i = b_i$. □

Since $W_\infty = \pi(\bar{\mathcal{C}}^{\mathbb{P}} \bigcap \mathcal{H}_\infty)$, we want to compute the zeroes of I^h which have a null T-coordinate and at least a non zero X-coordinate. Let $\alpha = (0, u_1, \ldots, u_d, \alpha_{d+1}, \ldots, \alpha_n)$ be such a zero, and suppose that j is the smallest index such that $\alpha_i \neq 0$. Since the polynomials in I^h are homogeneous, α is a zero of I^h if and only if $\alpha' = (0, u_1, \ldots, u_d, \alpha_{j+1}/\alpha_j, \ldots, \alpha_n/\alpha_j)$ is a zero of $\Psi_j^a(I^h)$, which shows that :

$$W_\infty = \bigcup_{j=d+1}^{n} \overline{\Pi_U(\boldsymbol{V}(\langle \Psi_j^a(I^h) \rangle))} = \bigcup_{j=d+1}^{n} \boldsymbol{V}(\langle \Psi_j^a(I^h) \bigcap \mathbb{Q}(U) \rangle)$$

The above lemma shows that $\mathcal{E}_j^\infty = \Psi_j^a(G^h) \bigcap \mathbb{Q}(U)$ is a Gröbner basis of the ideal $\langle \Psi_j^a(I^h) \bigcap \mathbb{Q}(U) \rangle$, which proves the second and the third items of the theorem. □

Starting from a Gröbner basis of I ($\boldsymbol{V}(I) = \bar{\mathcal{C}}$) for $<_{U,X}$, where $<_U$ and $<_X$ are Degree Reverse Lexicographic orderings, the computation of $I_\infty = \cap_{i=0}^n I_i^\infty$ of Theorem 14 is easy. the specifications of the related algorithm (detailed in section 7) are the following :

Algorithm PROPERNESSDEFECTS

- **Input** : G,U,X where G a reduced Gröbner of basis (output from Algorithm PREPROCESSING) w.r.t $<_{U,X}$ where $<_U$ and $<_X$ are Degree Reverse Lexicographic orderings;
- **Output** : $G_i^\infty, i = d+1 \ldots n$ such that
  - G_i^∞ is a Gröbner basis for $<_U$;
  - $W_\infty = \cup_{i=0}^{n-d} \boldsymbol{V}(\langle G_i^\infty \rangle)$.

3.2 The algorithm CRITICAL

In this section, we suppose that I is the ideal defining $\bar{\mathcal{C}}$ (see specifications of the algorithm in the above section). As recall in the introduction of this section, computing the singular locus (or the critical values of a projection like Π_U) of an algebraic variety is not straightforward when the ideal defining it is not prime or at least equidimensional and radical (W_c may not be equal nor contained in $\boldsymbol{V}(I + \mathrm{Jac}_X^{n-\delta}(I))$). In this section, our goal is to characterize the cases where W_c and W_{sing} can be replaced by $\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])$ and $\boldsymbol{V}((I \cap \mathbb{Q}[U]) + \mathrm{Jac}_U^{d-\delta}(I \cap \mathbb{Q}[U]))$ for computing a (non necessarily strict) discriminant variety.

The following proposition shows that there is no mathematical need to fully decompose I into radical and equidimensional components :

Proposition 16. *Let* $I = \cap_{i=1}^{i_1} Q_i \cap_{i=1}^{i_2} Q'_i$ *be a minimal primary decomposition of* I *where* $\{Q_i, i = 1, \ldots, i_1\}$ *are the primary components such that* $\dim(Q_i) = \dim(Q_i \cap \mathbb{Q}[U]) = \delta$*, and suppose that* $W_D = W_\infty \cup W_{\mathrm{sd}} \cup W_{\mathrm{sing}} \cup W_{\mathcal{F}} \cup W_c$ *is the minimal discriminant variety of* $\bar{\mathcal{C}}$ *w.r.t.* Π_U*.*

If $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) < \delta$*, then*

- $Q_i = \sqrt{Q_i}$ *for* $i = 1, \ldots, i_1$*;*
- $\dim(W_\infty) < \delta$*;*
- *if* $J = \cap_{i=1}^{i_1} Q_i$*, then* $W_D = W_\infty \cup W_{\mathrm{sd}} \cup W_{\mathcal{F}} \cup \boldsymbol{V}((J + \mathrm{Jac}_X^{n-\delta}(J)) \cap \mathbb{Q}[U]) \cup \boldsymbol{V}((J \cap \mathbb{Q}[U]) + \mathrm{Jac}_U^{d-\delta}(J \cap \mathbb{Q}[U]))$ *and* $\dim(W_D) < \delta$*.*

Proof. If $Q_i \neq \sqrt{Q_i}$ for some i, then $\mathrm{Jac}_X^{n-\delta}(I)$ vanishes on $\boldsymbol{V}(Q_i)$, and thus $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) \geq \delta$, which contradicts the hypothesis and proves the first item.

If $\dim(W_\infty) = \delta$, then there exist an index i, $1 \leqslant i \leqslant i_2$ such that $\dim(Q'_i) \geq \delta$ and $\dim(Q'_i \cap \mathbb{Q}[U]) = \delta$. In that case, the Jacobian matrix wrt X associated to any set of generators of I has rank lower than $n - \delta$ on $\boldsymbol{V}(Q'_i)$ and thus $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) \geq \delta$, which contradicts the hypothesis and proves the second item.

For any algebraic variety $\mathcal{V}$, we denote by $\mathrm{Crit}(\mathcal{V})$ the union of the singular points of $\mathcal{V}$ and of the critical points of Π_U in restriction to the regular locus of $\mathcal{V}$.

If $p \in \mathrm{Crit}(\boldsymbol{V}(I))$ and $\Pi_U(p) \notin (W_\infty \cup W_{\mathrm{sd}})$, then $p \in \mathrm{Crit}(\boldsymbol{V}(J))$. Moreover, since J is equidimensional and radical, then $\mathrm{Crit}(J) = \boldsymbol{V}(J + \mathrm{Jac}_X^{n-\delta}(J))$ and has dimension less than δ. Also, $W_c \cup W_\infty \cup W_{\mathrm{sd}} = \overline{\Pi_U(\mathrm{Crit}(\boldsymbol{V}(I)))} \cup W_\infty \cup W_{\mathrm{sd}} = W_\infty \cup W_{\mathrm{sd}} \cup \overline{\Pi_U(\boldsymbol{V}(J + \mathrm{Jac}_X^{n-\delta}(J)))} = W_\infty \cup W_{\mathrm{sd}} \cup \boldsymbol{V}((J + \mathrm{Jac}_X^{n-\delta}(J)) \cap \mathbb{Q}[U])$. Similarly, one has $W_{\mathrm{sing}} \cup W_\infty \cup W_{\mathrm{sd}} = W_\infty \cup W_{\mathrm{sd}} \cup \boldsymbol{V}((J \cap \mathbb{Q}[U]) + \mathrm{Jac}_X^{n-\delta}(J \cap \mathbb{Q}[U]))$ which shows the third item. $\square$

For practical issues, we will better use the following corollary :

Corollary 17. *Using the notations of Proposition 16, If* $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) < \delta$*, then*

- $W' = W_\infty \cup W_{\mathrm{sd}} \cup W_{\mathcal{F}} \cup \boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]) \cup \boldsymbol{V}((I \cap \mathbb{Q}[U]) + \mathrm{Jac}_U^{d-\delta}(I \cap \mathbb{Q}[U]))$ *is a discriminant variety of* $\bar{\mathcal{C}}$ *wrt* Π_U *and* $\dim(W') < \delta$*;*
- *If* $\nexists Q'_i$ *such that* $\exists Q_j$ *with* $\sqrt{Q_j} \subset \sqrt{Q'_i}$*, then* W' *is the minimal discriminant variety of* $\bar{\mathcal{C}}$ *wrt* Π_U*.*

Proof. If $\nexists Q'_i$ such that $\exists Q_j$ with $\sqrt{Q_j} \subset \sqrt{Q'_i}$, then $\Pi_U(\boldsymbol{V}(Q'_i)) \subset W_\infty \cup W_{\mathrm{sd}}, \forall i = 1 \ldots i_2$ so that $W' = W_D$, which shows the second item.

Without lost of generality, we suppose there exist an index i_3 with $1 \leq i_3 \leq i_2$, such that $\exists Q_j$ with $\sqrt{Q_j} \subset \sqrt{Q'_i}$ if and only if $i \leq i_3$, and we set $Q' = \cap_{i=1}^{i_3} Q'_i$ and $Q'' = \cap_{i=i_3+1}^{i_2} Q'_i$. We then have : $I = J \cap Q' \cap Q''$, so that $W' = W_{\mathcal{F}} \cup W_{\mathrm{sd}} \cup W_\infty \cup \boldsymbol{V}((J \cap Q' + \mathrm{Jac}_X^{n-\delta}(J \cap Q')) \cap \mathbb{Q}[U]) \cup \boldsymbol{V}((J \cap Q' \cap \mathbb{Q}[U]) + \mathrm{Jac}_U^{d-\delta}(J \cap Q' \cap \mathbb{Q}[U]))$ and $\dim(W') < \delta$ since $\dim(\Pi_U(\boldsymbol{V}(Q'))) < \delta$, which shows that W' is a discriminant variety. $\square$

The condition of the second item is not easy to check in practice in the general case, but it can be simplified for a large class of systems:

Corollary 18. *Using the notations of Proposition 16, if* $I = \langle f_1, \ldots, f_{n-\delta} \rangle$ *and if* $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) < \delta$*, then* $W_{\mathrm{sd}} = \emptyset$ *and* W' *is the minimal discriminant variety of* $\bar{\mathcal{C}}$ *wrt* Π_U*.*

Proof. If $I = \langle f_1, \ldots, f_{n-\delta} \rangle$, then $\boldsymbol{V}(I)$ has no irreducible component of dimension $< \delta$ so that, $W_{\mathrm{sd}} = \emptyset$. It follows from Proposition 16 that, reusing the notations of the proof of Corollary 17, we only have to prove that $\Pi_U(\boldsymbol{V}(Q'')) \subset W_\infty$ to conclude.

Thus, let us consider $Q = Q'_i$ with $\dim(Q) < \delta, \mathcal{P} = \sqrt{Q}$ and denote by $\mathbb{Q}[U, X]_{\mathcal{P}}$ the localization of $\mathbb{Q}[U, X]$ at $\mathcal{P}$. The ideals $I\mathbb{Q}[U, X]$ and $I\mathbb{Q}[U, X]_{\mathcal{P}}$ are generated by $n - \delta$ elements and so the height of their isolated primary components are $\leq n - \delta$ according to the general form Krull's principal ideal theorem ([16]).

If the height of $I\mathbb{Q}[U, X]_{\mathcal{P}}$ is $< n - \delta$, then $I\mathbb{Q}[U, X]$ has a primary component of height $< n - \delta$ (and thus of dimension $> \delta$ since $\mathbb{Q}[U, X]$ is a Cohen-Macaulay ring) contained in $\mathcal{P}$, which shows that $\boldsymbol{V}(\Pi_U(Q)) \subset W_\infty$.

Suppose now that the height of$I\mathbb{Q}[U, X]_{\mathcal{P}}$ is $n - \delta$. Since $I\mathbb{Q}[U, X]_{\mathcal{P}}$ is generated by $n - \delta$ elements (the images of the f_i in $\mathbb{Q}[U, X]_{\mathcal{P}}$), and since $\mathbb{Q}[U, X]_{\mathcal{P}}$ is a local ring, these elements forms a regular sequence (Theorem 17.4 in [16]). The ring $Q[U, X]_{\mathcal{P}}$ being Cohen-Macaulay, the ideal $I\mathbb{Q}[U, X]_{\mathcal{P}}$ is then pure equidimensional (it does not have any primary component of height $\neq n - \delta$) and consequently, $I\mathbb{Q}[U, X]$ has no primary component of height $\neq n - \delta$ contained in $\mathcal{P}$, which is impossible since $Q \subset \mathcal{P}$ has dimension $< \delta$ (and so its height is $> n - \delta$ since $\mathbb{Q}[U, X]$ is Cohen-Macaulay). □

According to Corollary 17 and Corollary 18 a key filter is the test on the dimension of $\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]))$. If it is less than δ, on can replace W_c (resp. W_{sing}) by $\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])$ (resp. $\boldsymbol{V}((I \cap \mathbb{Q}[U]) + \mathrm{Jac}_U^{d-\delta}(I \cap \mathbb{Q}[U])))$ in many cases (most cases in regard of systems coming from applications), otherwise, one will need to compute the radical of I (or at least to replace some primary components by their radical). The goal of the function CRITICAL detailed in section 7, is to compute $\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])$, which is compulsory for getting its dimension, to compute eventually $\boldsymbol{V}((I \cap \mathbb{Q}[U]) + \mathrm{Jac}_U^{d-\delta}(I \cap \mathbb{Q}[U]))$ and to return a comprehensive information (for example "need to compute the radical") to keep track, in the remaining computations, of the detected properties (for example, if $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]))) < \delta)$, according to Corollary 17, apart some possible missing points of W_{sd} one has a large discriminant variety if W_∞ and $W_{\mathcal{F}}$ are already known). The specifications of the CRITICAL algorithm are the following :

Algorithm CRITICAL

- **Input** : $\mathcal{E}, G, G_\Pi, \delta, U, X$ as in Algorithm PREPROCESSING
- **Output** : G_c, G_{sing} and *Property* such that
  - G_c and G_{sing} are reduced Gröbner bases for $<_U$
  - if *Property=Minimal*, then $W_D = W_\infty \cup \boldsymbol{V}(\langle G_c\rangle) \cup \boldsymbol{V}(\langle G_{\mathrm{sing}}\rangle) \cup W_{\mathcal{F}}$ is the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U (Corollary 18).
  - if *Property=PartialLarge*, then $W_\infty \cup W_{\mathrm{sd}} \cup \boldsymbol{V}(\langle G_c\rangle) \cup \boldsymbol{V}(\langle G_{\mathrm{sing}}\rangle) \cup W_{\mathcal{F}}$ has dimension $< \delta$ and is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U (Corollary 17).
  - if *Property=NeedRadical*, then $W_\infty \cup W_{\mathrm{sd}} \cup \boldsymbol{V}(\langle G_c\rangle) \cup \boldsymbol{V}(\langle G_{\mathrm{sing}}\rangle) \cup W_{\mathcal{F}}$ is not a discriminant variety of $\mathcal{C}$ w.r.t. Π_U (if $I = \langle G\rangle$, $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]))) \geq \delta$).

3.3 The CORE algorithm

From Algorithms PREPROCESSING and PROPERNESSDEFECTS one knows how to compute W_∞ and $W_{\mathcal{F}}$. Let us explore how to drive the remaining computations from the output of Algorithm CRITICAL. If I denotes any ideal such that $\boldsymbol{V}(I) = \bar{\mathcal{C}}$, then :

- [A] if $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) < \delta$ (if *Property* $\neq$ *NeedRadical*) two case occur
  - [1] if *Property=Minimal*, say if $\#\mathcal{E} = n - \delta$ (or if I is generated by $n - \delta$ polynomials), one has $W_{\mathrm{sd}} = \emptyset$ and Algorithm CRITICAL computes W_c and W_{sing} (Corollary 18).

- ◦ [2] if *Property* $\neq$ *Minimal*, say if $\#\mathcal{E} \neq n - \delta$ (or if I is not known to be generated by $n-\delta$ polynomials), then Algorithm CRITICAL computes W_c and W_{sing}, may be part of W_{sd} and also some possible extraneous components of dimension $<\delta$ (Corollary 17). Depending on the use :
  - [a] the missing points from W_{sd} may not play any role in the studied application and we can stop the computations;
  - [b] the computation of a discriminant variety is required and then one needs to compute W_{sd};
  - [c] the computation of a minimal discriminant variety is required and then one needs to remove some embedded primary components, (Corollary 17) : one will perform again thees tests and computations; if the process comes back to [A-2-c], one then will also need to compute also W_{sd}.

- [B] if dim $(\boldsymbol{V}((I + \text{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) \geq \delta$ (if *Property* = *NeedRadical*), say if dim $(\boldsymbol{V}((I + \text{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U])) = \delta$, one needs to replace the primary components $Q_i \subset I$, $i = 1 \ldots i_1$ by their radical and perform again these tests and computations.

The situations [A-1] and [A-2-a] cover most systems coming from applications and do not require to perform any decomposition of I. Since these cases can be detected or checked dynamically, our general strategy consists in betting that we are in one of these situations. This requires in particular extraneous informations from the user (especially for the case [A-2-a]). We thus decompose the general algorithm into two algorithms. The first one, named CORE (detailed in section 7) runs straightforwardly Algorithms PREPROCESSING, PROPERNESSDEFECTS and CRITICAL. It does not depends on the extraneous informations given by the user and has the following specifications :

Algorithm CORE

- **Input** : $\mathcal{E}, \mathcal{F}, U, X$
- **Output** : $G, G_\Pi, G_{D,1}, \ldots, G_{D,k}$ and *Property* such that
  - ◦ G is a reduced Gröbner basis for $<_{U,X}$ where $<_U$ and $<_X$ are Degree Reverse Lexicographic orderings;
  - ◦ $(G_{D,i})_{i=1\ldots k}$ and I_Π are Gröbner bases for $<_U$;
  - ◦ if *Property*=*Minimal*, then $\cup_{i=1}^k \boldsymbol{V}(\langle G_{D,i}\rangle)$ is the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U;
  - ◦ if *Property*=*PartialLarge*, then $W_{\text{sd}} \cup_{i=1}^k \boldsymbol{V}(\langle G_{D,i}\rangle)$ is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U, which has the same components of dimension δ, if any, as the minimal one;
  - ◦ if *Property*=*NeedRadical*, then $W_{\text{sd}} \cup W_c \cup W_{\text{sing}} \cup_{i=1}^k \boldsymbol{V}(\langle G_{D,i}\rangle)$ is the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U.

In short, the algorithm CORE fully solves the problem when in situations [A-1] and [A-2-a] and it returns a comprehensive message (*Property*=*PartialLarge* or *Property*=*NeedRadical*) otherwise. Also, the general algorithm will first run the CORE Algorithm and, when necessary (situations [A-2-b], [A-2-c] of [B]), will decompose I and follow the computations. One important remark is that some part of the discriminant variety are definitively known in any case : this is always the case for $W_\infty \cup W_{\mathcal{F}}$, and sometimes the case for $W_\infty \cup W_{\mathcal{F}} \cup W_c \cup W_{\text{sing}}$ (note that W_{sd} always miss when *Property* $\neq$ *Minimal*).

3.4 The general algorithm

In this section, we describe a general algorithm which computes a discriminant variety in any case. The global strategy consists in running first the CORE algorithm described in the previous section and, in case of failure (which may not happens for almost all the problems coming from applications), depending on the message returned (*Property*) and on the end-user query (a minimal discriminant variety may be required, the components of small dimension may be ignored, etc.) the proposed solution may (at least partially) decompose I to follow the computations.

The situations where Algorithm CORE may fail are fully specified by Corollary 17 and Corollary 18. In order to follow the computations, one needs to compute the radical of some primary components (those of dimension δ which do not contain any polynomial of $\mathbb{Q}[U]$) and/or the projection of the components of dimension $<\delta$. This can obviously be done using classical algorithms such as those described in [4] (primary decomposition and/or computation of the radical of an ideal) but also by lazy strategies such as decompositions into regular and separable triangular sets [1].

Most existing algorithms for computing decompositions can be optimized in our case. For example, the knowledge of an ideal defining W_∞ can easily be exploited to optimize algorithm [11] (performing differently the saturations), the computation of the Jacobian criterion in CORE could also be reused in Algorithms like [9]. We do not detail such optimization in the present contribution, but better point out the extraneous work required when decomposing the problem. In order to keep simple descriptions, we suppose that the decomposition process is able to compute equidimensional and radical irredundant decompositions (it is not useful to have such a full decomposition according to Corollary 17 and Corollary 18).

Definition 19. *Given an ideal I, a* radical equidimensional decomposition *of I is a finite set of radical equidimensional ideals $Q_i, i=1,\ldots,m$ such that $\sqrt{I}=\bigcap_{i=1}^m I_i$. The decomposition is* irredundant *if none of the I_i is contained in an associated prime of another I_i, or equivalently if none of the $\boldsymbol{V}(I_i)$ contents any component of another $\boldsymbol{V}(I_i)$.*

We describe now how the minimal discriminant variety may be computed from a radical equidimensional decomposition.

Proposition 20. *Using Notation 1, let $\sqrt{\langle\mathcal{E}\rangle}=\bigcap_{i=1}^m I_i$ be a radical equidimensional decomposition of $\langle\mathcal{E}\rangle$. Then $\bigcap_{i=1}^m (I_i\colon(\prod_{i=1}^l f_i)^\infty)$ is a radical equidimensional decomposition of $\langle\mathcal{E}\rangle\colon(\prod_{i=1}^l f_i)^\infty$. If the former is irredundant, the same becomes true for the latter, after removing the components which are equals to the full ring.*

In other words, it is equivalent to decompose $\langle\mathcal{E}\rangle$ or the ideal I which is produced by Algorithm PREPROCESSING

Proof. This is an immediate consequence of the standard properties of the saturation of ideals, which commutes with intersections and radical computation. □

Proposition 21. *Using the notations of Algorithm* PREPROCESSING*, let $\bigcap_{i=1}^m I_i$ be a radical equidimensional decomposition of I. We suppose that it is irredundant in dimension δ, which means that the I_i of dimension δ does not share any irreducible component. We denote by $I_\Pi^{(i)}$, $W_{\mathcal{F}}^{(i)}$, ... the objects (ideals and varieties, not Gröbner bases) associated to I_i as introduced in the specifications of Algorithms* PREPROCESSING, PROPERNESSDEFECTS, CRITICAL *and* CORE. *We have*

- $\sqrt{I_\Pi}=\bigcap_{i=1}^m I_\Pi^{(i)}$ *and* $\overline{\Pi_U(\boldsymbol{V}(I))}=\boldsymbol{V}(I_\Pi)=\bigcup_{i=1}^m \boldsymbol{V}(I_\Pi^{(i)})$;
- $\sqrt{I_{\mathcal{F}}}=\bigcap_{i=1}^m \sqrt{I_{\mathcal{F}}^{(i)}}$ *and* $W_{\mathcal{F}}=\boldsymbol{V}(I_{\mathcal{F}})=\bigcup_{i=1}^m W_{\mathcal{F}}^{(i)}$;
- $W_\infty=\bigcup_{i=1}^m W_\infty^{(i)}$ *and* $W_\infty^{(i)}=\boldsymbol{V}(I_\Pi^{(i)})$ *if and only if* $\dim(I_i)>\dim(I_\Pi^{(i)})$;
- W_{sd} *is included in the union of those of the* $\boldsymbol{V}(I_\Pi^{(i)})$ *such that* $\dim(I_i)<\delta$*; the inclusion becomes an equality if the decomposition is irredundant.*
- *Let* $J\subset\{1,\ldots,m\}$ *be the set of indexes* i *such that* $\dim(I_i)=\dim(I_\Pi^{(i)})=\delta$. *Then* $W_c=W'\cup\bigcup_{i\in J}\boldsymbol{V}((I_i+\mathrm{Jac}_X^{n-\delta}(I_i))\cap\mathbb{Q}[U])\cup\bigcup_{i,j\in J,i\neq j}\boldsymbol{V}((I_i+I_j)\cap\mathbb{Q}[U])$ *where* $W'\subset W_\infty\cup W_{\mathrm{sd}}$.

- *If $\delta < d$ then* $W_{\mathrm{sing}} = W'' \cup \bigcup_{i \in J} \boldsymbol{V}(I_{\Pi}^{(i)} \cup \mathrm{Jac}_U^{d-\delta}(I_{\Pi}^{(i)})) \cup \bigcup_{i,j \in J, i \neq j} \boldsymbol{V}(K_{i,j})$ *where* $W'' \subset W_{\infty} \cup W_{\mathrm{sd}}$ *and* $K_{i,j}$ *is the intersection of the radical equidimensional components of dimension* $< \delta$ *of* $I_{\Pi}^{(i)} + I_{\Pi}^{(j)}$.

Proof. As $I_{\Pi}^{(i)} = I_i \cap \mathbb{Q}[U]$, the first item is an immediate consequence of the commutativity of the intersection. Similarly, $I_{\mathcal{F}}^{(i)} = (I_i + \mathcal{F}) \cap \mathbb{Q}[U]$ and the second item results from the identity $\sqrt{I+K} \bigcap \sqrt{J+K} = \sqrt{(I \cap J) + K}$.

The first part of the third item results immediately from the definitions. If $W_{\infty} = \boldsymbol{V}(I_{\Pi}^{(i)})$, then almost all fibers of the projection have a positive dimension, which implies the inequality for the dimensions. Conversely, the inequality implies that one of the irreducible components of $\boldsymbol{V}(I_i)$ has a dimension higher than that of $I_{\Pi}^{(i)}$; by equidimensionality, this is true for all the components, and implies that for almost any point of any component of $\boldsymbol{V}(I_{\Pi}^{(i)})$ the fiber of the projection is infinite, and thus that this component is included in $W_{\infty}^{(i)}$.

The assertions concerning W_{sd} result immediately from the definitions.

For W_c and W_{sing}, we can ignore the points which belong to $\Pi_U(\boldsymbol{V}(I_i))$ for $i \notin J$, since they belong to $W_{\infty} \cup W_{\mathrm{sd}}$. If a point belongs to one unique $\boldsymbol{V}(I_i)$, $i \in J$, it is critical "at large" (could be a singular point) for Π_U if and only if it belongs to $\boldsymbol{V}(I_i + \mathrm{Jac}_U^{n-\delta}(I_i))$. If a point belongs to several $\boldsymbol{V}(I_i)$, it belongs to the singular locus of $\boldsymbol{V}(I)$, which proves the assertion concerning W_c.

Finally, a point which does not belong to $W_{\infty} \cup W_{\mathrm{sd}}$ belongs to the singular locus of $\overline{\Pi_U(\boldsymbol{V}(I))}$, either if it is a singular point of some $\boldsymbol{V}(I_{\Pi}^{(i)})$, or if it belongs to two different irreducible components of $\overline{\Pi_U(\boldsymbol{V}(I))}$. If these components belong to the same $\boldsymbol{V}(I_{\Pi}^{(i)})$, the point belongs to the singular locus of $\boldsymbol{V}(I_{\Pi}^{(i)})$; thus we may suppose that it belongs to $\boldsymbol{V}(I_{\Pi}^{(i)})$ and $\boldsymbol{V}(I_{\Pi}^{(j)})$ with $j \neq i$; we may also suppose that it is not contained in any common component of $\boldsymbol{V}(I_{\Pi}^{(i)})$ and $\boldsymbol{V}(I_{\Pi}^{(j)})$ (if it was the case, the point would belong to the singular of both $\boldsymbol{V}(I_{\Pi}^{(i)})$ and $\boldsymbol{V}(I_{\Pi}^{(j)})$). Consequently, it does not belong to the union of the components of dimension δ of $\boldsymbol{V}(I_{\Pi}^{(i)} + I_{\Pi}^{(j)})$ and therefore belongs to $\boldsymbol{V}(K_{i,j})$. Conversely, it is immediate that the points of $\boldsymbol{V}(K_{i,j})$ belong to the singular locus of $\overline{\Pi_U(\boldsymbol{V}(I))}$. □

Proposition 21 allows to complete the algorithm to compute the discriminant variety. For this purpose we call DECOMPOSE a procedure which computes a radical equidimensional decomposition of an ideal. As irredundancy removal is costly and not always implemented in practice, we make a case distinction depending on the irredundancy of the output of DECOMPOSE. However we suppose that the output of DECOMPOSE is irredundant in dimension δ, condition which is not very costly to satisfy, if triangular sets are used to decompose. We suppose also that the ideals output by DECOMPOSE are represented by Gröbner bases, but, for being shorter, we describe the operations done on this output as ideal operations. The specifications of the global algorithm (detailed in section 7) are the following :

Algorithm DISCRVAR

- **Input:**
  - $\mathcal{E}, \mathcal{F}, U, X$ as in the preceding algorithms
  - *Request*, which may be set to *NeedMinimal* if a minimal discriminant variety is requested, *NeedSmallDim* if a discriminant variety is requested and *Partial* if one allows W_{sd} to be incomplete.
- **Output:** $I_{D,1}, \ldots, I_{D,k}$, *Property* such that
  - $G_{D,i}, i = 1, \ldots, k$ are Gröbner bases for $<_{U,X}$
  - if *Request* = *Minimal,* then one wants that $\bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i} \rangle)$ should be the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U.
  - if *Request* = *Large*, then $\bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i} \rangle)$ has to be a (non necessarily minimal) discriminant variety of $\mathcal{C}$ w.r.t. Π_U;

- if *Request* $=$ *PartialLarge*, then it suffices that $W_{\mathrm{sd}} \cup \bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U.
- *Property* may take the same values as *Request*, indicating possibly that a stronger result than asked has been obtained (for example the user may ask for a non minimal discriminant variety but receive the minimal one).

4 The real case

In this section, we focus on the study of $\mathcal{S} = \{x \in \mathbb{R}^n,\ p_1(x) = 0, \ldots, p_s(x) = 0,\ f_1(x) > 0, \ldots f_l(x) > 0\}$, deriving the results obtained for the related complex problem ($\mathcal{C} = \{x \in \mathbb{C}^n \quad , \quad p_1(x) = 0, \ldots, p_s(x) = 0,\ f_1(x) \neq 0, \ldots f_l(x) \neq 0\}$).

A first remark is that there does not exist, in general, a minimal discriminant variety for $\mathcal{S}$ (take for example $\mathcal{S} = \{(u, x) \in \mathbb{R}^2,\ u\,x - 1 = 0,\ u > 0\}$) : an equivalent object would necessarily been a semi-algebraic set, not an algebraic set. Also, we do not pretend to give a full set of definitions but better show how to use discriminant (complex) varieties in the real case.

Proposition 22. *Let $W \subset \mathbb{C}^d$ be a discriminant variety of $\mathcal{C}$ wrt Π_U. If $W \neq \overline{\Pi_U(\mathcal{C})}$, the number of points of $\mathcal{S}$ is constant over any connected open set $\mathcal{U} \subset \left(\overline{\Pi_{\mathcal{U}}(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$.*

Proof. If $\mathcal{U} \subset \mathbb{R}^d$ is any connected subset such that $\mathcal{U} \cap W = \emptyset$, as $(\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}$ then either $\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C} \cap \mathbb{R}^n = \emptyset$ or $(\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C} \cap \mathbb{R}^n, \Pi_U)$ is an analytic covering of $\mathcal{U}$. In particular, the number of real roots of $\mathcal{S}$ or of $\mathcal{S}'$ is always constant over $\mathcal{U}$. □

Definition 2 can not be straightforwardly generalized in the real case ($W \cap \mathbb{R}^d$ is not a discriminant variety of $\mathcal{S}$ wrt Π_U) : one may, for example, have $W_\infty = \overline{\Pi_U(\mathcal{C})}$ while $\phi_u(\mathcal{C}) \cap \mathbb{R}^{n-\delta}$ is finite for almost all $u \in \cap\ (\Pi_U(\mathcal{C}) \setminus W) \cap \mathbb{R}^d$. This is the case if there are complex irreducible components of dimension $> \delta$ without any real point. We distinguish 3 cases :

- [A] $W = \overline{\Pi_U(\mathcal{C})}$; This means that $\forall u \in \Pi_U(\mathcal{C})$, $\phi_u(\mathcal{C})$ is not a finite set of points, but one can not conclude for $\mathcal{C} \cap \mathbb{R}^n$ or $\mathcal{S}$. In particular, W is not a (real) discriminant variety of $\mathcal{S}$ according to Definition 2.
- [B] $W \subsetneqq \overline{\Pi_U(\mathcal{C})}$;
  - [I] if $\exists u \in \left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$ such that $\phi_u(\mathcal{S}) \neq \emptyset$, then almost all points $(u, x) \in \mathcal{S}$ verify $\Pi_U((u, x)) \in \left(\overline{\Pi_{\mathcal{U}}(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$ so that $W \cap \mathbb{R}^d$ can be viewed as a (real) discriminant variety of $\mathcal{S}$ according to Proposition 22.
  - [II] if $\forall u \in \left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$, $\phi_u(\mathcal{S}) = \emptyset$ then $\mathcal{S} \subset \left(\Pi_U^{-1}(W) \cap \mathcal{C} \cap \mathbb{R}^n\right)$ and one can study $\mathcal{S}$ as a subset of $\mathcal{C} \cap \Pi_U^{-1}(W)$ (instead of $\mathcal{C}$). A main remark is that either $\dim(\mathcal{C}) < \dim(\mathcal{C} \cap \Pi_U^{-1}(W))$ (always the case when $\delta = d$) or the number of irreducible components of $\bar{\mathcal{C}}$ is less than the number of irreducible components of $\overline{\mathcal{C} \cap \Pi_U^{-1}(W)}$, so that $\mathcal{C} \cap \Pi_U^{-1}(W)$ is "smaller" than $\mathcal{C}$.

Note that the condition $\exists u \in \left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$ (or $\forall u \in \left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$, $\phi_u(\mathcal{S}) = \emptyset$) can be tested in practice by taking one sample point u in each connected component of $\left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$ (performing an open CAD such as in [7] or using one of the algorithms from [3]) and by solving the zero-dimensional system $\phi_u(\mathcal{S})$ (using for example Algorithm [20]).

The main problem to be solved is the case [A] : If $W = \overline{\Pi_U(\mathcal{C})}$, one first needs to decide if $\phi_u(\mathcal{S})$ is a finite set of points for almost all $u \in \phi_u(\mathcal{S})$ (otherwise, $W \cap \mathbb{R}^d$ is a discriminant variety of $\mathcal{S}$ wrt Π_U). Suppose that $W = \overline{\Pi_U(\mathcal{C})}$, and let $Y \subset [U, X]$ be a subset of transcendental variables for I with $\boldsymbol{V}(I) = \bar{\mathcal{C}}$ and set $Y' = [U, X] \setminus Y$ (Y can be computed from a Gröbner basis of I [8]). According to the results from the above sections, replacing U by Y and X by Y' and setting $d' = \#Y$, we have :

- $\overline{\Pi_Y(\mathcal{C})} = \mathbb{R}^{d'}$;

- $\dim(\mathcal{C}) = \dim(\Pi_Y(\mathcal{C})) = d' > \delta$
- any discriminant variety W' of $\mathcal{C}$ wrt Π_Y has dimension $< d'$.

Again, two situation may occur :

- if $\exists y \in \mathbb{R}^{d'} \setminus \left(W' \cap \mathbb{R}^{d'}\right)$ such that $\phi_y(\mathcal{S}) \neq \emptyset$ then $\dim(\mathcal{S}) = \dim(\mathcal{C})$ and thus, for almost all $u \in \Pi_U(\mathcal{C}) \cap \mathbb{R}^d$, $\phi_u(\mathcal{S})$ is not a finite set of points.
- if $\forall y \in \mathbb{R}^{d'} \setminus \left(W' \cap \mathbb{R}^{d'}\right)$, $\phi_y(\mathcal{S}) = \emptyset$, then then $\mathcal{S} \subset \left(\Pi_Y^{-1}(W') \cap \mathcal{C} \cap \mathbb{R}^n\right)$ and one can study $\mathcal{S}$ as a subset of $\mathcal{C} \cap \Pi_Y^{-1}(W')$ (instead of $\mathcal{C}$), noticing that $\dim(\mathcal{C}) < \dim(\mathcal{C} \cap \Pi_Y^{-1}(W'))$.

This shows the following result :

Corollary 23. *There exist an algorithm which computes a constructible set $\mathcal{C}' \subset \mathcal{C}$ such that $\mathcal{S} \subset \mathcal{C}'$ and if W' denotes the discriminant variety of $\mathcal{C}'$ wrt Π_U then $W^{'} \cap \mathbb{R}^d$ is a discriminant variety of $\mathcal{S}$.*

A possible algorithm - REALDISCRVAR - (Corollary 23) is described in section 7. It is specified as follows

Algorithm REALDISCRVAR

- **Input:**
  - $\mathcal{E}, \mathcal{F}, U, X$ as in the preceding algorithms.
  - *Request*, which may be set to *NeedMinimal* if a minimal discriminant variety is requested, *NeedSmallDim* if a discriminant variety is requested and *Partial* if one allows W_{sd} to be incomplete;
  - SAMPLEPOINTS(Eq,Ineq,k) a functions which computes at least one point in each connected component of the semialgebraic set of $\mathbb{R}^k$ $\{g = 0,\ g \in \text{Eq},\ f > 0,\ f \in \text{Ineq}\}$.
- **Ouput:** $G_{D,1}, \ldots, G_{D,k}$, *Property* such that
  - $G_{D,i}, i = 1, \ldots, k$ are Gröbner bases for $<_{U,X}$
  - if *Request* = *DiscrVar*, then one wants that $\bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ is a discriminant variety of $\mathcal{S}$ w.r.t. Π_U.
  - if *Request* = *Large*, then $\bigcup_{i=1}^{k} \boldsymbol{V}(G_{D,i})$ has to be a (non necessarily minimal) discriminant variety of $\mathcal{S}$ w.r.t. Π_U;
  - if *Request* = *PartialLarge*, then it suffices that $W_{\text{sd}} \cup \bigcup_{i=1}^{k} \boldsymbol{V}(I_{D,i})$ is a discriminant variety of $\mathcal{S}$ w.r.t. Π_U.

One practical difference between the real and complex cases is that one needs, in the real case, to characterize all the connected components of $\overline{\Pi_U(\mathcal{S})} \setminus \left(W' \cap \mathbb{R}^{d'}\right)$, say at least computing one point in each, for computing a discriminant variety : this can be performed using some algorithms from [3] or simply using a Cylindrical Algebraic Decomposition [5] (we will see in the next section how to optimize the use of the CAD in our context). Note that however, such a computation is required for solving the initial problem in most cases (for example counting the number of solutions wrt the parameters).

5 Using discriminant varieties - Examples

This section is devoted to the practical use of discriminant varieties. We focus on the real case which is more simple to illustrate. We revisit some applications already solved by ad-hoc computations. The goal is to illustrate, on non-trivial and practical examples, how to solve efficiently some problems dealing with parametric systems, by using our algorithms as black-boxes. We have chosen difficult problems, but not too difficult, in order that the proposed solutions can easily be reproduced by the reader. In both applications we present, the goal is to compute the number of real roots of a parametric system wrt the parameters values.

5.1 Using discriminant varieties for counting the number of roots

For simplicity, we suppose that the constructible set $\mathcal{C}'$ from Corollary 23 is equal to $\mathcal{C}$ so that if W is a discriminant variety of $\mathcal{C}$, then $W \cap \mathbb{R}^d$ is a discriminant variety of $\mathcal{S}$ (which is the case in most situations). We denote by $\mathcal{U}_1$, ...$\mathcal{U}_k$ the connected components of $\left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$.

If $u_1, \ldots, u_k$ are sample points such that $u_i \in \mathcal{U}_i$ then $\bigcup_{i=1}^k \Pi_U^{-1}(u_i)$ intersects each connected component of $\mathcal{S} \cap \mathbb{R}^n$ in a finite number of points. Moreover, if $\mathcal{U}$ is a small neighborhood of u_i, then $\Pi_U^{-1}(u_i) \cap \mathcal{S}$ defines exactly one point in each connected component of $\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{S}$. Thus, by computing one point on each $\mathcal{U}_i$, one can get the number of real points of $\mathcal{S}$ or $\mathcal{C}$ over any point of $\mathcal{U}_i$, which is constant on $\mathcal{U}_i$. The number of real or complex solutions of $\mathcal{S}$ for parameters' values which do not belong to $W \cap \mathbb{R}^d$ depends only on the connected component $\mathcal{U}_i$ and is a computable well defined function of the index i.

In the real case, obtaining the sample points u_1, ..., u_k consists in computing one point on each connected component of $\left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$, which may be got with a good theoretical complexity by the algorithms described in [3]. In practice, the end-user often wants to compute the number of real roots of the system as a function of the parameters. Computing at least one point on each $\mathcal{U}_i$ is not enough for this: one needs also, at least, an algorithm to test if two points are in the same connected component, or hopefully a comprehensive description of the connected components.

Basically, the CAD algorithm [5] computes a cylindrical decomposition of the ambient space in cells such that the polynomials of a given set have a constant sign on each cell. A straightforward method would then consist in computing a CAD of $\mathbb{C}^d$, adapted to the polynomials whose zeroes sets are $\overline{\Pi_U(\mathcal{C})}$ and W (which are explicitly known after the computation of a discriminant variety); it is easy to detect which cells are included in $\left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$ by testing the values of the polynomials at the sample points. If we enlarge W by the cells of dimension $< \delta$ contained in $\overline{\Pi_U(\mathcal{C})}$, we obtain again a discriminant variety such that the corresponding $\mathcal{U}_i$ are the cells of dimension δ contained in $\left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$.

In practice, we directly compute the cells of dimension δ contained in $\left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$ using the strategy proposed in [7] (Open CAD) : compared with a standard CAD, the most costly operations (the computations with real algebraic numbers) can then be avoided in the lifting step (this is immediate if $d = \delta$; in the other case, one may compute a discriminant variety of $\left(\overline{\Pi_U(\mathcal{C})} \cap \mathbb{R}^d\right) \setminus \left(W \cap \mathbb{R}^d\right)$ w.r.t. a projection on $\mathbb{R}^\delta$ and reduce the problem to the computation of an open CAD of $\mathbb{R}^\delta$ [7]) and the number of polynomials to be computed in the projection step is exponentially less than in the classical process (there is no need to compute the subresultants coefficients).

One finally gets a partition of $\overline{\Pi_U(\mathcal{C})}$ consisting in W (possibly extended) and a collection of cells of dimension δ supplied by sample points on them. Given these sample points, one has then to plug the corresponding parameter's values in the initial system and to solve the corresponding zero-dimensional problems using [20] or [21].

Remark 24. Such a process describes only *generic* solutions (outside a discriminant variety). Note that however, the non generic solutions lies on $\mathcal{S} = \mathcal{S} \cap \Pi_U^{-1}(W)$ (or $\mathcal{C} = \mathcal{C} \cap \Pi_U^{-1}(W)$ in the complex case) which theoretically can be solved using the same process. We do not study in detail such a recursive use of our algorithms in the present contribution, since getting the full description of the parameter's space is not required in general in the applications and also since it requires a lot of additional optimizations/tricks to be efficient in practice.

5.2 Cuspidal manipulators

We revisit here an ad-hoc computation done in [7]. An extension of this problem (one variable more) can be found in [6]. The goal was to compute a classification of 3-revolute-jointed manipulators based on the cuspidal behavior. This ability to change posture without meeting a singularity is equivalent to the existence of a point in the workspace, such that a polynomial of degree four depending on the parameters of the manipulator and on the Cartesian coordinates of the effector has a triple root.

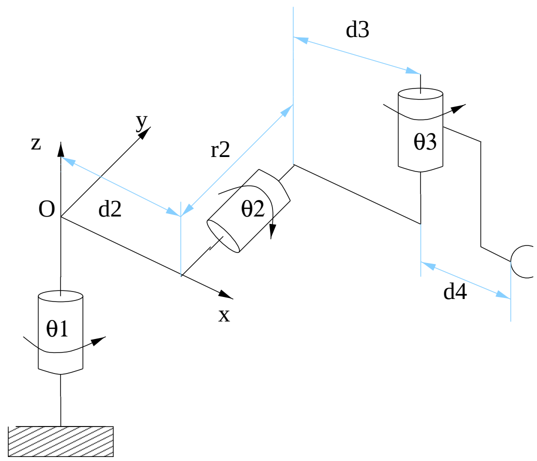

Figure 1.

The system that characterizes the cuspidal robots depends on 3 parameters d_4, d_3 and r_2 which are the design parameters (supposed to be positive). It is given by:

$$P(t) = a\,t^4 + b\,t^3 + c\,t^2 + d\,t + e = 0, \frac{\partial P}{\partial t} = 0, \frac{\partial^2 P}{\partial t^2} = 0, d_4 > 0, d_3 > 0, r_2 > 0$$

with $\left\{\begin{array}{l} a = m_5 - m_2 + m_0 \\ b = -2m_3 + 2m_1 \\ c = -2m_5 + 4m_4 + 2m_0 \\ d = 2m_3 + 2m_1 \\ e = m_5 + m_2 + m_0 \end{array}\right.$, and $\left\{\begin{array}{l} m_0 = -r^2 + r_2^2 + \frac{(R+1-L)^2}{4} \\ m_1 = 2r_2 d_4 + (L - R - 1) d_4 r_2 \\ m_2 = (L - R - 1) d_4 d_3 \\ m_3 = 2 r_2 d_3 d_4^2 \\ m_4 = d_4^2 (r_2^2 + 1) \\ m_5 = d_4^2 d_3^2 \\ r^2 = x^2 + y^2 \\ R = r^2 + z^2 \\ L = d_4^2 + d_3^2 + r_2^2 \end{array}\right.$

In [7], the authors used a particular change of variables and a ad-hoc method based on decompositions into triangular sets to compute a discriminant variety. The final decomposition of the parameter's space was obtained using an open Cylindrical Algebraic Decomposition ([7]). Let us show how the method proposed in this article allows to solve automatically the problem. The example is interesting since the equidimensional decomposition of $\mathcal{E}$ is very difficult to compute in practice.

We take $\mathcal{E} = \{P, \frac{\partial P}{\partial t}, \frac{\partial^2 P}{\partial t^2}\}$, $\mathcal{F} = \{d_4, d_3, r_2\}$, $U = [d_4, d_3, r_2]$ and $X = [t, z, r]$. The system has dimension 4 but the only component of dimension 4 is embedded in $\boldsymbol{V}(d_4) \subset W_{\mathcal{F}}$ to that the Algorithm PREPROCESSING does not perform any localization and its output is :

- $\delta = 3$;
- I is the Gröbner basis of $\mathcal{E}$ for $<_{U,X}$;
- $I_\Pi = \{\}$;
- $I_{\mathcal{F}} = \{d4\} \cup \{d3\} \cup \{r2\}$;

As in most situations, W_∞ is easy to compute. On this example, the result Algorithm PROPERNESSDEFECTS returns :

- $I_4^\infty = \{1\}, I_5^\infty = \{r_2 d_4 - d_3 r_2 + r_2^3 d_4\}, I_6^\infty = \{1\}$

Since $< \mathcal{E} > + \operatorname{Jac}_X^{n-d}(\mathcal{E})$ has dimension $< d$ and since the system has 3 equations and depends on 3 parameters, then $W_D = \cup_{i=4\ldots 6} \boldsymbol{V}(I_i^\infty) \cup \boldsymbol{V}((< \mathcal{E} > + \operatorname{Jac}_X^{n-d}(\mathcal{E})) \cap \mathbb{Q}[U])$. The output of Algorithm CRITICAL is :

- *Property=Minimal*
- $I_{\text{sing}} = \{\}$
- $I_{\text{crit}} = \{ -d_4^2 + r_2^2 + d_3^2,\ d_4^2 r_2^6 - d_4^4 r_2^4 + 2d_4^2 r_2^4 + 3d_4^2 d_3^2 r_2^4 - 2d_4^4 r_2^2 + d_4^2 r_2^2 - 2d_4^4 d_3^2 r_2^2 + 3d_4^2 d_3^4 r_2^2 - d_3^2 r_2^2 - d_4^4 d_3^4 + d_4^2 d_3^2 + d_4^2 d_3^6 - 2d_4^2 d_3^4 - d_4^4 + 2d_4^4 d_3^2,\ r_2^8 + 2d_3^2 r_2^6 + 2r_2^6 - 2d_4^2 r_2^6 + d_4^4 r_2^4 - 4d_4^2 r_2^4 - 2d_3^2 r_2^4 - 2d_4^2 d_3^2 r_2^4 + r_2^4 + d_3^4 r_2^4 - 2d_4^2 r_2^2 + 2d_4^4 r_2^2 + 2d_4^2 d_3^2 r_2^2 + d_4^4,\ d_3^2 r_2^2 - d_4^2 + 2d_4^2 d_3 + d_3^2 - d_4^2 d_3^2 - 2d_3^3 + d_3^4,\ d_3^2 r_2^2 - d_4^2 - 2d_4^2 d_3 + d_3^2 - d_4^2 d_3^2 + 2d_3^3 + d_3^4 \}$

Also, even if we apply directly the algorithm DISCRVAR with the request *Minimal*, no decomposition will be computed and only two Gröbner bases computations for a block ordering $<_{U,X}$ are needed (I and I_{crit}). Removing the polynomials that have no real roots, our algorithm gives exactly the same result as the one obtained in [7]. As in [7], one can easily terminate the computations by using an open CAD and some tools for computing the real roots of a zero-dimensional system. The projection of the discriminant variety on the subspace (d_3, r_2) (obtained after the first CAD projection step) appears in following figure.

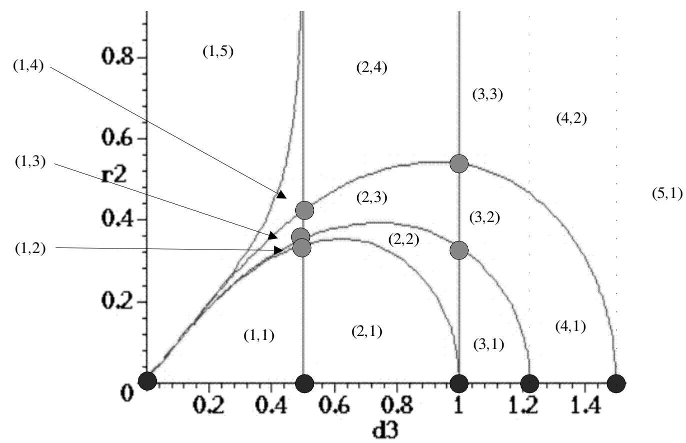

Figure 2. Partition of the parameters'space (d_3, r_2)

Over each open cell, there are exactly six sheets on the discriminant variety, and the following table gives the number of solutions found at a sample point in each of the cells delimited by these sheets (by solving the corresponding zero-dimensional systems):

$(d_3, r_2) \setminus d_4$	1	2	3	4	5	6	7
(1,1)	0	0	4	4	2	0	0
(1,2)	0	4	4	4	2	0	0
(1,3)	0	4	4	4	2	0	0
(1,4)	0	4	4	2	2	0	0
(1,5)	0	4	4	2	0	0	0
(2,1)	0	0	4	4	2	2	0
(2,2)	0	4	4	4	2	2	0
(2,3)	0	4	4	4	2	2	0
(2,4)	0	4	4	2	2	2	0
(3,1)	0	4	4	4	2	2	4
(3,2)	0	4	4	4	2	2	4
(3,3)	0	4	4	2	2	2	4
(4,1)	0	4	4	4	2	2	4
(4,2)	0	4	4	2	2	2	4
(5,1)	0	4	4	2	2	2	4

We may consider that the problem is completely solved, even if no precise information is known for parameter's values that belongs to the discriminant variety: it will anyway be impossible to construct, in practice, a robot whose parameters belong to a strict closed subset of the parameter's space.

5.3 Equi-Cevaline points on triangles

The problem proposed in [29] has been already solved by the authors of this paper, partially by "hand". In their article, they asked for a general solver able to produce the same kind of results. In [14], one of us gave a complete answer and showed how to design a solver able to produce automatically the solution. In this section we show that our algorithm fits the requirements of such a solver.

The goal is to study the points of $\mathbb{R}^3$ where three lines passing through one point P and one vertex of a triangle intersects the triangle in three segments of same length. In the following system, the parameters a, b, c represent the lengths of the sides of a triangle $A\ B\ C$, l is the common length of the intersections and x, y, z are the homogeneous barycentric coordinates of P:

$$\begin{aligned}
&p_1{:}=(c^2-l^2)y^2+(b^2-l^2)z^2+(b^2+c^2-a^2-2\,l^2)y\,z=0;\\
&p_2{:}=(a^2-l^2)z^2+(c^2-l^2)x^2+(c^2+a^2-b^2-2\,l^2)z\,x=0;\\
&p_3{:}=(b^2-l^2)x^2+(a^2-l^2)y^2+(a^2+b^2-c^2-2\,l^2)x\,y=0;\\
&f_1{:}=x+y+z-1=0;
\end{aligned}$$

After substituting x by $1-y-z$, and according to the notations introduced in the present paper, we take $\mathcal{E}=\{p_1,\,p_2,\,p_3\}$, $\mathcal{F}=\{a,\,b,\,c,\,a+b-c,\,b+c-a,\,c+a-b\}$ (the conditions asserting that the triangle exists), $X=[y,z,l]$ and $U=[a,b,c]$. In [14], the author defines in fact a discriminant variety constituted by conditions of degeneracy (degenerated triangles) and 10 polynomials. As for the previous application, there is no need to localize by $\mathcal{F}$, $W_{\mathcal{F}}$ is clearly defined by $\mathcal{F}$, and W_{sing} and W_{sd} are empty. Thus it only remains to compute W_∞ and W_c. Our algorithm computes easily $W_\infty=\boldsymbol{V}(a\,b\,c(a+c-b)(a+c+b)(b+a-c)(a-b-c))$, which corresponds exactly to the degenerated situations (degenerated triangles) listed by the authors in [29] and [14]. W_c is then the union of the zero sets of the following polynomials:

$\{a-b, a+b, a-c, a+c, c+b, c-b, (1/5)\,c^4-(2/5)\,a^2c^2+a^4-(2/5)\,b^2c^2-(2/5)\,a^2b^2+(1/5)\,b^4, -(5/3)\,c^4+(2/3)\,a^2c^2+a^4+(2/3)\,b^2c^2-2\,a^2b^2+b^4, c^4-a^2c^2+a^4-b^2c^2-a^2b^2+b^4, 5\,c^4-2\,a^2c^2+a^4-2\,b^2c^2-2\,a^2b^2+b^4, c^4-2\,a^2c^2+a^4-2\,b^2c^2-2\,a^2b^2+5\,b^4, c^4-2\,a^2c^2+a^4+(2/3)\,b^2c^2+(2/3)\,a^2b^2-(5/3)\,b^4, -(3/5)\,c^4-(2/5)\,a^2c^2+a^4+(6/5)\,b^2c^2-(2/5)a^2b^2-(3/5)\,b^4\}$.

By removing the polynomials that have no real roots in the first quadrant, we obtain the same 10 polynomials as in [14]. In other words, our algorithm is an automatic method for solving the problem.

6 Conclusion

In this article, we proposed some tools for computing the discriminant variety of a basic constructible set $\mathcal{C}$ (w.r.t. a given projection) and for describing the sub-manifolds of its complementary in the Zariski closure of the image of $\mathcal{C}$. We shown that this object is optimal and easy to compute in most cases. We also demonstrate its efficiency in terms of computation times (cuspidal manipulators) but also in terms of quality of the output (Equi-Cevaline points on triangles).

There are several directions in which this work needs to be improved.

First of all, the discriminant variety is computed as a union of several varieties. It appears that this output is usually strongly redundant: W_∞ is produced as a union of $n-\delta$ components, while it is frequently equal to the one which corresponds to the lowest variable; the components of $\mathcal{C}$ of dimension $>\delta$ are included in both W_c and W_∞ (and also, very frequently, in $W_{\mathcal{F}}$); if $d>\delta$, W_c and W_{sing} share a big component, frequently equal to W_c. It would save a lot of computation time if one could avoid the computations needed to produce redundant components and to recognize their redundancy. Also W_c and especially W_{sing} are costly to compute because of the high degree of the Jacobian determinants, which would make interesting any method avoiding the Jacobian criterion or decreasing the cost of its computation. Therefore we need other ways to compute a discriminant variety, which produce a better decomposition as output. A first result in this direction appears in [?].

In the same way, it appears that the discriminant variety of $\Pi_U^{-1}(W_D)\cap\mathcal{C}$ may be needed, and that its computation may take strongly advantage of the computation done for W_D. This needs to be made more explicit.

Another direction should be to estimate the complexity of our algorithm. We already know, since the object which is computed is optimal and several algorithms compute a discriminant variety, that the degree of the discriminant variety is simply exponential in the number of variables (see [13] for example). Computing a precise bound would give precious informations on the complexity of solving parametric systems. We also know that the running time of our algorithm is simply exponential in the number of variables when using the Gröbner engine proposed in [13]. A challenge would be to prove that we would get a better or at least more precise bound by using [10] as Gröbner engine.

Finally, we have to extend the class of problems which may be solved by computing discriminant variety. For example, by choosing conveniently the set of U-variables and applying recursively our algorithm to $\mathcal{C}\cap\Pi_U^{-1}(W_D)$, one may obtain a decomposition of $\mathcal{C}$ into smooth equidimensional semi-algebraic sets. By refining this decomposition one may deduce a cell decomposition of $\mathcal{C}$ (decomposition in semi-algebraic sets isomorphic to some $\mathbb{R}^i$). The knowledge of the neighborhood relation between these cells would imply a complete description of the topology of $\mathcal{C}$. In our opinion one of the main challenges of our field would be to design an algorithm to do this, which, together, would be practically efficient and have a good complexity (i.e. simply exponential in the number of variables). We are yet far from this objective for several reasons, notably because of the use of the CAD which makes the computation doubly exponential in the dimension d of $\mathcal{C}$ (note however that the CAD alone would induce a much higher complexity, doubly exponential in n).

We already addressed the problem of computing equi-dimensional and radical decompositions for solving the general case. For example, in the case of constructible sets whose projection on the parameter's space is dense, we never need to compute a full decomposition but simply the radical of the primary components of dimension δ of the studied ideal whose intersection with $\mathbb{Q}[U]$ have dimension δ and the intersection with $\mathbb{Q}[U]$ of the primary components of dimension $<\delta$. One can thus easily optimize existing classical algorithms which compute primary decomposition for this specific purpose but getting an efficient decomposition designed for our purpose is still a challenge.

Bibliography

[1] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28:105–124, 1999.

[2] P. Aubry, F. Rouillier, and M. Safey. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[3] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computations in Mathematics*. Springer-Verlag, 2003.

[4] T. Becker and V. Weispfenning. *Groebner bases: a computational approach to commutative algebra*. Graduate Texts in Mathematics: readings in mathematics. Springer, 1993.

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

[6] S. Corvez. *Etude de systèmes polynomiaux : contributions à la classification d'une famille de manipulateurs et au calculs des intersections de courbes A-splines*. PhD thesis, Université de Rennes 1, 2005.

[7] S. Corvez and F. Rouillier. Using computer algebra tools to classify serial manipulators. In F. Winkler, editor, *Automated Deduction in Geometry*, volume 2930 of *Lecture Notes in Artificial Intelligence*, pages 31–43. Springer, 2003.

[8] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms an introduction to computational algebraic geometry and commutative algebra*. Undergraduate texts in mathematics. Springer-Verlag New York-Berlin-Paris, 1992.

[9] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 110:207–235, 1992.

[10] Jean-Charles Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero f_5. In *International Symposium on Symbolic and Algebraic Computation Symposium - ISSAC 2002, Villeneuve d'Ascq, France*, 2002.

[11] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2):149–168, 1988.

[12] M. Giusti, G. Lecerf, and B. Salvy. A gröbner free alternative for solving polynomial systems. *Journal of Complexity*, 17(1):154–211, 2001.

[13] D. Grigoriev and N. Vorobjov. Bounds on numbers of vectors of multiplicities for polynomials which are easy to compute. In *ISSAC: Proceedings of the ACM SIGSAM International Symposium on Symbolic and Algebraic Computation*, 2000.

[14] D. Lazard. On the specification for solvers of polynomial systems. In *5th Asian Symposium on Computers Mathematics -ASCM 2001*, volume 9 of *Lecture Notes Series in Computing*, pages 66–75. World Scientific, 2001.

[15] Daniel Lazard. Computing with parameterized varieties. In *submitted to Algebraic Geometry and Geometric Modeling*, 2005.

[16] H. Matsumura. *Commutative Theory Ring*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge, second edition edition, 1989. Translated from Japaneese by M. Reid.

[17] A. Montes. Improving dispgb algorithm using the discriminant ideal. *to appear in A3L issue of the Jour. Symb. Comp.*, 2005.

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

[19] D. Mumford. The red book of varieties ans schemes. *Lecture Notes in Mathematics*, 1358, 1988.

[20] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Journal of Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[21] F. Rouillier. On the rational univariate representation. In *International Conference on Polynomial System Solving*, pages 75–79, 2004.

[22] Mohab Safey El Din and Eric Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In J.R. Sendra, editor, *International Symposium on Symbolic and Algebraic Computation 2003 - ISSAC'2003, Philadelphie, USA*, pages 224–231. ACM Press, aug 2003.

[23] Mohab Safey El Din and Eric Schost. Properness defects of projection functions and computation of at least one point in each connected component of a real algebraic set. *Journal of Discrete and Computational Geometry*, sep 2004.

[24] E. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):349 – 393, 2003.

[25] P. Trébuchet. *Vers une résolution stable et rapide des équations algébriques*. PhD thesis, Université Pierre et Marie Curie, 2002.

[26] D. Wang. *Elimination Methods*. Springer-Verlag,Wien New York, 2001.

[27] V. Weispfenning. Comprehensive gröbner bases. *Journal of Symbolic Computation*, 14:1–29, 1992.

[28] V. Weispfenning. *Solving parametric polynomial equations and inequalities by symbolic algorithms*. World Scientific, 1995.

[29] L. Yang and Z. Zeng. Equi-cevaline points on triangles. In World Scientific, editor, *Proceedings of he Fourth Asian Symposium*, Computer Mathematics, pages 130–137, 2000.

7 Algorithms

Algorithm PREPROCESSING

- **Input** : $\mathcal{E}, \mathcal{F}, U, X$
- **Output** : δ and $G, G_\Pi, G_\mathcal{F}$ such that
  - G is a reduced Gröbner basis for $<_{U,X}$ such that $\mathcal{C} \cap \Pi_U^{-1}(\overline{\Pi_U(\mathcal{C})} \setminus W_\mathcal{F}) = \boldsymbol{V}(\langle G \rangle) \cap \Pi_U^{-1}(\overline{\Pi_U(\mathcal{C})} \setminus W_\mathcal{F})$;
  - G_Π, $G_\mathcal{F}$ are reduced Gröbner bases for $<_U$ such that $\boldsymbol{V}(\langle G_\Pi \rangle) = \overline{\Pi_U(\mathcal{C})}$ and $\boldsymbol{V}(\langle G_\mathcal{F} \rangle) = W_\mathcal{F}$;
- **Begin**
  - **Compute** $G_\mathcal{E}$ the reduced Gröbner basis of $\mathcal{E}$ for $<_{U,X}$
  - **Deduce** $G_{\mathcal{E},U} = G_\mathcal{E} \cap \mathbb{Q}[U]$
  - **Compute** $d_{\mathcal{E},U}$, the dimension of $G_{\mathcal{E},U}$
  - **Compute** $G_{\mathcal{E}\cap\mathcal{F}}$, the reduced Gröbner basis of $\mathcal{E} \cup \{ \prod_{i=1}^s f_i\}$ for $<_{U,X}$
  - **if** $(G_{\mathcal{E}\cap\mathcal{F}} = G_\mathcal{E})$ **then return** $(\delta = -1,\ G = \{1\},\ G_\Pi = \{1\},\ G_\mathcal{F} = \{1\})$
  - **else**
    - **Deduce** $G_{\mathcal{E}\cap\mathcal{F},U} = G_{\mathcal{E}\cap\mathcal{F}} \cap \mathbb{Q}[U]$
    - **Compute** $d_{\mathcal{E}\cap\mathcal{F},U}$, the dimension of $G_{\mathcal{E}\cap\mathcal{F},U}$
    - **if** $(d_{\mathcal{E},U} = d_{\mathcal{E}\cap\mathcal{F},U})$ **then**
      - **Compute** $G_{\mathcal{E},T\mathcal{F}}$, the reduced Gröbner basis of $\mathcal{E} \cup \{T(\prod_{i=1}^l f_i) - 1\}$ for $<_{T,(U,X)}$
      - **Deduce** $G_{\mathcal{E},\mathcal{F}} = G_{\mathcal{E},T\mathcal{F}} \cap \mathbb{Q}[X, U]$
      - **return**(PREPROCESSING$(G_{\mathcal{E},\mathcal{F}}, \mathcal{F}, U, X)$)
    - **else return**($\delta = d_{\mathcal{E},U},\ G = G_\mathcal{E},\ G_\Pi = G_{\mathcal{E},U},\ G_\mathcal{F} = G_{\mathcal{E}\cap\mathcal{F},U}$)
- **End**

Algorithm PROPERNESSDEFECTS

- **Input** : $G_{U,X}$,U,X where $G_{U,X}$ a reduced Gröbner basis w.r.t $<_{U,X}$ where $<_U$ and $<_X$ are Degree Reverse Lexicographic orderings;
- **Output** : $G_i^\infty, i = d+1...n$ such that
  - G_i^∞ is a Gröbner basis for $<_U$
  - $W_\infty = \cup_{i=0}^{n-d} \boldsymbol{V}(G_i^\infty)$
- **Begin**
  - **Set** $G_i^\infty = G_{U,X} \cap \mathbb{Q}[U]$ for $i = d+1, ..., n$
  - **for** $g \in G_{U,X}$
    - **if** $\exists i \in [d+1...n]$ and $\exists k \in \mathbb{N}^\star$ such that $\mathrm{LM}_{<_X}(g) = X_i^k$ **then** $G_i^\infty = G_i^\infty \cup \{\mathrm{LC}_{<_X}(g)\}$
  - **return** $(G_i^\infty, d+1 = 1, ..., n)$
- **End**

Algorithm CRITICAL

- **Input** : $\mathcal{E}, G, G_\Pi, \delta, U, X$ as in Algorithm PREPROCESSING
- **Output** : G_c, G_{sing} and *Property* such that
  - G_c and G_{sing} are reduced Gröbner bases for $<_U$
  - if *Property*=*Minimal*, then $W_D = W_\infty \cup \boldsymbol{V}(\langle G_c\rangle) \cup \boldsymbol{V}(\langle G_{\mathrm{sing}}\rangle) \cup W_{\mathcal{F}}$ is the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U (Corollary 18).
  - if *Property*=*PartialLarge*, then $W_\infty \cup W_{\mathrm{sd}} \cup \boldsymbol{V}(\langle G_c\rangle) \cup \boldsymbol{V}(\langle G_{\mathrm{sing}}\rangle) \cup W_{\mathcal{F}}$ has dimension $< \delta$ and is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U (Corollary 17).
  - if *Property*=*NeedRadical*, then $W_\infty \cup W_{\mathrm{sd}} \cup \boldsymbol{V}(\langle G_c\rangle) \cup \boldsymbol{V}(\langle G_{\mathrm{sing}}\rangle) \cup W_{\mathcal{F}}$ is not a discriminant variety of $\mathcal{C}$ w.r.t. Π_U (if $I = \langle G\rangle$, $\dim(\boldsymbol{V}((I + \mathrm{Jac}_X^{n-\delta}(I)) \cap \mathbb{Q}[U]))) \geq \delta$).

- **Begin**
  - **Compute** G_{jac}, the reduced Gröbner basis of $(\langle G\rangle \cup \{\mathrm{Jac}_X^{n-\delta}(\mathcal{E})\})$ w.r.t. $<_{U,X}$
  - **Deduce** $G_c = G_{\mathrm{jac}} \cap \mathbb{Q}[U]$
    - if $\delta < d$ compute G_{sing}, the reduced Gröbner basis of $(\langle G_\Pi\rangle \cup \{\mathrm{Jac}_U^{d-\delta}(G_\Pi)\})$ w.r.t. $<_U$
    - else set $G_{\mathrm{sing}} = \{1\}$
  - **If** $\dim(\langle G_c\rangle) < \delta$ **then**
    - **if** $n - \delta = \sharp\mathcal{E}$ **then return**$(G_c, G_{\mathrm{sing}},$ *Minimal*$)$

  - **else return**$(G_c,\, G_{\rm sing},\, \mathit{PartialLarge})$

- **else return**$(G_c, G_{\rm sing}, \mathit{NeedRadical})$

- **End**

Algorithm CORE

- **Input** : $\mathcal{E}, \mathcal{F}, U, X$
- **Output** : $G, G_\Pi, G_{D,1}, \ldots, G_{D,k}$ and *Property* such that
  - G is a reduced Gröbner basis for $<_{U,X}$ where $<_U$ and $<_X$ are Degree Reverse Lexicographic orderings;
  - $(G_{D,i})_{i=1\ldots k}$ and I_Π are Gröbner bases for $<_U$;
  - if *Property*=*Minimal*, then $\cup_{i=1}^k \boldsymbol{V}(\langle G_{D,i}\rangle)$ is the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U;
  - if *Property*=*PartialLarge*, then $W_{\rm sd} \cup_{i=1}^k \boldsymbol{V}(\langle G_{D,i}\rangle)$ is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U, which has the same components of dimension δ, if any, as the minimal one;
  - if *Property*=*NeedRadical*, then $W_{\rm sd} \cup W_c \cup W_{\rm sing} \cup_{i=1}^k \boldsymbol{V}(\langle G_{D,i}\rangle)$ is the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U.
- **Begin**
  - $\delta, G, G_\Pi, G_{\mathcal{F}}$=PREPROCESSING$(\mathcal{E}, \mathcal{F}, U, X)$
  - **if** $(G_\Pi = \{1\})$ **then return**$(G, G_\Pi, \delta, 1, G_\Pi, \mathit{Minimal})$
  - $(G_i^\infty)_{i=1\ldots n-d}$=PROPERNESSDEFECTS$(G, U, X)$
  - **if** $G_i^\infty = G_\Pi$ for some i in $\{1, \ldots, n-d\}$ **then return**$(G, G_\Pi, \delta, 1, G_\Pi, \mathit{Minimal})$
  - $G_c, G_{\rm sing}, \mathit{Property}$=CRITICAL$(\mathcal{E}, G, G_\Pi, \delta, U, X)$
  - *if Property*=*NeedRadical*, **then**

    return$(G, G_\Pi, \delta, n-d+1, G_{\mathcal{F}}, (G_i^\infty)_{i=1\ldots n-d}, \mathit{Property})$
  - **else return**$(G, G_\Pi, \delta, n-d+3, I_{\mathcal{F}}, (G_i^\infty)_{i=1\ldots n-d}, G_c, G_{\rm sing}, \mathit{Property})$
- **End**

Algorithm DiscrVar

- **Input:**
  - $\mathcal{E}, \mathcal{F}, U, X$ as in the preceding algorithms
  - *Request*, which may be set to *NeedMinimal* if a minimal discriminant variety is requested, *NeedSmallDim* if a discriminant variety is requested and *Partial* if one allows W_{sd} to be incomplete.
- **Output:** $I_{D,1}, \ldots, I_{D,k}$, *Property* such that
  - $G_{D,i}, i = 1, \ldots, k$ are Gröbner bases for $<_{U,X}$
  - if *Request* = *Minimal,* then one wants that $\bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ should be the minimal discriminant variety of $\mathcal{C}$ w.r.t. Π_U.
  - if *Request* = *Large*, then $\bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ has to be a (non necessarily minimal) discriminant variety of $\mathcal{C}$ w.r.t. Π_U;
  - if *Request* = *PartialLarge*, then it suffices that $W_{\text{sd}} \cup \bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U.
  - *Property* may take the same values as *Request*, indicating possibly that a stronger result than asked has been obtained (for example the user may ask for a non minimal discriminant variety but receive the minimal one).

Begin

- $G, G_\Pi, \delta, k, (G_{D,i})_{i=1,\ldots,k}$, *Property*=CORE$(\mathcal{E}, U, X)$
- **if** *Property* = *Minimal* or *Request* = *Property* **then return** $((G_{D,i})_{i=1,\ldots,k}$, *Property*)
- $(G_i)_{i=1,\ldots,m} =$ DECOMPOSE(G)
- **if** *Property* = *PartialLarge* and *Request* = *Large* **then**
  - $G_D = \{G_{D,i}, i = 1, \ldots, k\}$
  - **for** $i = 1, \ldots, m$ **do if** $\dim(G_i) < \delta$ **then**
    - $G_\Pi^{(i)} = G_i \cap \mathbb{Q}[U]$
    - **if** $\dim(G_\Pi^{(i)}) = \dim(G_i)$ **then** $G_D = G_D \cup \{G_\Pi^{(i)}\}$
  - **return**$(I_D$, *Large*)
- $I_D = \{G_{D,i}, i = 1, \ldots, n - d + 1\}$ *(at this stage we have* $\boldsymbol{V}(G_D) = W_\infty \cup W_{\mathcal{F}}$*)*
- **for** $i = 1, \ldots, m$ **do if** $\dim(G_i) \leqslant \delta$ **then**
  - $G_\Pi^{(i)} = G_i \cap \mathbb{Q}[U]$
  - **if** $\dim(G_\Pi^{(i)}) = \dim(G_i) < \delta$ **then** $G_D = G_D \cup \{G_\Pi^{(i)}\}$
  - **if** $\dim(G_\Pi^{(i)}) = \dim(G_i) = \delta$ **then** $G_D = G_D \cup \{$ CRITICAL$(G_i, G_i, G_\Pi^{(i)}, \delta, U, X)\}$
- **for** $i = 1, \ldots, m$ **do for** $j = i + 1, \ldots, m$ **do**
  - **if** $\delta = \dim(G_i) = \dim(G_j) = \dim(G_\Pi^{(i)}) = \dim(G_\Pi^{(j)})$ **then**
    - $G_D = G_D \cup \{(G_i + G_j) \cap \mathbb{Q}[U]\}$
    - **if** $\delta < d$ **and** $G_\Pi^{(i)} \neq G_\Pi^{(j)}$ **then**
      - $(K_{i'})_{i'=1,\ldots,m'} =$ DECOMPOSE $(G_\Pi^{(i)} + G_\Pi^{(j)})$
      - **for** $i' = 1, \ldots, m'$ **do if** $\dim(K_{i'}) < \delta$ **then** $G_D = G_D \cup \{K_{i'}\}$
- **if** DECOMPOSE provides a certified irredundant output
  - **then** *Property* = *Minimal*
  - **else** *Property* = *Large*
- **return**$(G_D$, *Property*)

End

Algorithm RealDiscrVar

- **Input:**
  - $\mathcal{E}, \mathcal{F}, U, X$ as in the preceding algorithms.
  - *Request*, which may be set to *NeedMinimal* if a minimal discriminant variety is requested, *NeedSmallDim* if a discriminant variety is requested and *Partial* if one allows W_{sd} to be incomplete;
  - SamplePoints(Eq,Ineq,k) a functions which computes at least one point in each connected component of the semialgebraic set of $\mathbb{R}^k$ $\{g = 0,\ g \in \mathrm{Eq},\ f > 0,\ f \in \mathrm{Ineq}\}$.
- **Ouput:** $G_{D,1}, \ldots, G_{D,k}$, *Property* such that
  - $G_{D,i}, i = 1, \ldots, k$ are Gröbner bases for $<_{U,X}$
  - if *Request* = *DiscrVar,* then one wants that $\bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ is a discriminant variety of $\mathcal{S}$ w.r.t. Π_U.
  - if *Request* = *Large*, then $\bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ has to be a (non necessarilly minimal) discriminant variety of $\mathcal{S}$ w.r.t. Π_U;
  - if *Request* = *PartialLarge*, then it suffices that $W_{\mathrm{sd}} \cup \bigcup_{i=1}^{k} \boldsymbol{V}(\langle G_{D,i}\rangle)$ is a discriminant variety of $\mathcal{S}$ w.r.t. Π_U.

Begin

- $\delta, G, G_\Pi, G_{\mathcal{F}}$=PreProcessing($\mathcal{E}, \mathcal{F}, U, X$)
- **if** ($G_\Pi = \{1\}$) **then return**(G,G_Π,δ,1,G_Π,*DiscrVar*)
- $(G_i^\infty)_{i=1\ldots n-d}$=PropernessDefects($G$,$U$,$X$)
- **if** $G_i^\infty = G_\Pi$ for some i in $\{1, \ldots, n-d\}$ **then**
  - Compute $Y \subset [U, X]$ a maximal subset of transcendental variables for $I = \langle G\rangle$;
  - $G'_\Pi, G'_{D,1}, \ldots, G'_{D,k}$, *Property*=DiscrVar($G, G_{\mathcal{F}}, Y, [U, X] \setminus Y$, *Large*)
  - if SamplePoints($G'_\Pi \cup_{i=1}^{k} G'_{D,i}, \mathcal{F}, \#Y) \neq \emptyset$ then **return**(I_Π)
  - else **return**(RealDiscrVar($G \cup_{i=1}^{k} G_{D,i}, \mathcal{F}, U, X$))

End