Complexity of Resolution of Parametric Systems of Polynomial Equations and Inequations

Guillaume Moroz

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Complexity of Resolution of Parametric Systems of Polynomial Equations and Inequations

Guillaume Moroz

N° 5929

Mai 2006

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--5929--FR+ENG

Complexity of Resolution of Parametric Systems of Polynomial Equations and Inequations

Guillaume Moroz

Thème SYM — Systèmes symboliques
Projet Salsa

Rapport de recherche n° 5929 — Mai 2006 — 26 pages

Abstract: Consider a system of n polynomial equations and r polynomial inequations in n indeterminates of degree bounded by d with coefficients in a polynomial ring of s parameters with rational coefficients of bit-size at most σ. From the real viewpoint, solving such a system often means describing some semi-algebraic sets in the parameter space over which the number of real solutions of the considered parametric system is constant. Following the works of Lazard and Rouillier, this can be done by the computation of a *discriminant variety*. In this report we focus on the case where for a generic specialization of the parameters the system of equations generates a radical zero-dimensional ideal, which is usual in the applications. In this case, we provide a *deterministic* method computing the *minimal* discriminant variety reducing the problem to a problem of elimination. Moreover, we prove that the degree of the computed minimal discriminant variety is bounded by $D := (n+r)d^{(n+1)}$ and that the complexity of our method is $\sigma^{\mathcal{O}(1)}D^{\mathcal{O}(n+s)}$ bit-operations on a deterministic Turing machine.

Key-words: Parametric polynomial system, Discriminant variety, Elimination, Deterministic complexity

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

Complexité de résolution d'un système parametré d'équations et d'inéquations polynomiales

Résumé : On considère un système de n équations polynomiales et r inéquations en n inconnues et s paramètres. Le degré des polynômes considérés est majoré par d et leurs coefficients sont rationels de taille binaire au plus σ. D'un point de vue réel, résoudre un tel système revient souvent à décrire un semi-algébrique de l'espace des paramètres au-dessus duquel le nombre de solutions réels du système parametré considéré est constant. D'après les travaux de Lazard et Rouillier, on peut obtenir ce semi-algébrique par le calcul d'une *variété discriminante*. Dans ce rapport, nous nous restreignons au cas où le systèmes d'équations donnés en entrée est zéro-dimensionel pour une spécialisation générique des paramètres, ce qui correspond à une situation courante dans les applications. Dans ce cas, nous proposons une méthode *déterministe* pour calculer la variété discriminante *minimale* en réduisant le problème à un problème d'élimination. De plus, nous prouvons que le degré de la variété discriminante minimale est majorée par $D := (n+r)d^{(n+1)}$ et que la complexité de notre méthode est de $\sigma^{\mathcal{O}(1)} D^{\mathcal{O}(n+s)}$ opérations binaires sur une machine de Turing.

Mots-clés : Système polynomial parametré, Variété discriminante, Élimination, Complexité déterministe

1 Introduction

The parametric polynomial systems are used in many different fields such as robotics, optimization, geometry problems, and so on. In [26] the authors introduce the notion of discriminant variety which allows them to split the parameter space in open cells where the number of real solutions is constant . Even if it is efficient in a practical point of view, their algorithm is based Gröbner bases computations, whose complexity is not yet well understood. Thus it does not allow us to give a better bound than the worst case's one, which is in exponential space ([19]).

In this article we prove that, under some assumptions, the computation of the minimal discriminant variety of a parametric system is reducible to the FPSPACE problem of general elimination [27]. The proof of the reduction correctness presented here is non trivial. The reduction itself is simple and preserves the sparsity of the input system.

Our input is a system of polynomial equations and inequations of degrees bounded d, which can be written as:

$$\begin{cases} f_1(t,x) = 0 \\ \vdots \\ f_n(t,x) = 0 \end{cases} \text{ and } \begin{cases} g_1(t,x) \neq 0 \\ \vdots \\ g_r(t,x) \neq 0 \end{cases} \quad (t,x) \in \mathbb{C}^s \times \mathbb{C}^n$$

where x are the unknowns and t are the parameters. Moreover, for all specializations in an open ball of the parameters space, the system has a finite number of simple solutions in the unknowns. Such a system will be said *generically simple* (see Definition 4).
We prove that the degree of the minimal discriminant variety of a *generically simple* parametric system is bounded by

$$(n+r)d^{n+1}$$

Our algorithm for *generically simple* parametric systems runs in

$$\sigma^{\mathcal{O}(1)}(n+r)^{\mathcal{O}(n+s)}d^{\mathcal{O}(n(n+s))}$$

bit-operations on a deterministic Turing machine.

When we aim to solve a parametric system, we face two kinds of issues: either we want to describe the solutions in terms of the parameters, or else we want to classify the parameters according to properties of the parametric system's solutions. Different methods have been developped to treat these two problems.

Regarding the first one, many algorithms exist in the literature. Among them we may cite rational parametrizations [30], triangular sets decompositions [33], comprehensive Gröbner bases [34, 22]. We may also mention numerical algorithms such as the Newton-Raphson or the homotopy continuation method [32, 31], which can be used after a specialization of the parameters.

Regarding the second problem on the parameters classification, few algorithm are available, whereas many applications face it, such as parametric optimization ([17]), robot modelling ([11]), geometry problems ([35]) or control theory ([2]) for example. The C.A.D. [10, 7] is the most widespread method. It computes an exhaustive classification, leading to a complexity doubly exponential in the number of unknowns. Some of the algorithms mentioned above ([33, 22]) may also return such kinds of classifications. Especially in [22] the authors compute a complete partition of the parameters space in constructible sets where the vector of multiplicities of the system's solutions is constant. The time complexity of their algorithm is $d^{\mathcal{O}(n^2 s)}$. However, they don't consider inequations and their algorithm is not meant to be implemented. The minimal discriminant variety is included in both of the precedent computations. It describes the maximal open subset of the parameters space where the system's solutions evolve regularly. The computation of this variety is indeed sufficient for a lot of applications.

Our method is a reduction to the general elimination problem. The elimination problem has been widely analysed in the past decades, as it is a key step for quantifier elimination theory (in [23, 28, 4, 3] for example), computation of the dimension of an ideal ([6] among others) or implicitization theory (see [12]). Different techniques and software have been developed. We may mention sparse resultants (see [13] and references therein), linear system reductions (in [6] for example), linear systems parametrized with straight-line programs (see [28, 24]), parametric geometric resolution ([21, 30]) or Gröbner bases (see [9] and [15, 16] for the last improvements).

This article is divided in three parts. In the first one we reduce the problem of computing the minimal discriminant variety to the elimination problem. In the second part, we bound the degree of the minimal discriminant variety. And in the last part we give some examples.

Definition and notation

In the following, we assume that

$$f_1, \cdots, f_n, g_1, \cdots, g_r \in \mathbb{Q}[T_1, \cdots, T_s][X_1, \cdots, X_n]$$

are some polynomials in degrees $d_i = deg(f_i)$ and $d'_j = deg(g_j)$ for $1 \leq i \leq n$ and $1 \leq j \leq r$. We denote by $\mathbb{P}_n$ the projective closure of $\mathbb{C}^n$ and by $\pi : \mathbb{C}^s \times \mathbb{C}^n \to \mathbb{C}^s$ (resp. $\overline{\pi} : \mathbb{C}^s \times \mathbb{P}_n \to \mathbb{C}^s$) the canonical projection onto the parameters space. The exponent h (resp. h_i) of a polynomial or of an ideal denotes its homogenization by the variable X_0 with respect to the variables $X_1, \cdots, X_n$ (resp. its homogenization by the variable X_i with respect to the variables $X_0, \cdots, \hat{X_i}, \cdots, X_n$) . The term *parameters* will refer to the variables $T_1, \cdots, T_s$, while the term *unknowns* will refer to the variables $X_1, \cdots, X_n$.

Finally we use the following notation for the specialization of some variable. For $I \subset \mathbb{Q}[Y_1, \cdots, Y_k, Z]$ and $a \in \mathbb{Q}$, we denote:

$$I_{|Z=a} := (I + \langle Z - a \rangle) \cap \mathbb{Q}[Y_1, \cdots, Y_k]$$

In order to define the notion of discriminant variety according to our assumptions, we introduce the notion of *geometric regularity*.

Definition 1 *Let E be a subset of the parameters space.*
A parametric system S defining a constructible set $\mathcal{C}$ is said to be geometrically regular *over E iff for all open set $\mathcal{U} \subset E$, π restricted to $\pi^{-1}(\mathcal{U}) \cap \mathcal{C}$ is an analytic covering.*

The minimal discriminant variety is now defined as follows.

Definition 2 *[26] A* discriminant variety *of the parametric system S is a variety V in the parameters space such that S is* geometrically regular *over $\mathbb{C}^s \setminus V$.*

Among the discriminant varieties we define the *minimal* one:

Definition 3 *[26] The* minimal discriminant variety *of S is the intersection of all the discriminant varieties of S.*

For the computation of the minimal discriminant variety, we will assume some properties on the input parametric systems we consider.

Definition 4 *Let S be the parametric system defined by:*

$$\left\{\begin{array}{l} f_1(t,x) = 0 \\ \quad\vdots \\ f_n(t,x) = 0 \end{array}\right. \quad \textit{and} \quad \left\{\begin{array}{l} g_1(t,x) \neq 0 \\ \quad\vdots \\ g_r(t,x) \neq 0 \end{array}\right. \qquad (t,x) \in \mathbb{C}^s \times \mathbb{C}^n$$

Denoting $\prod_{j=1}^{r} g_j$ by g_S, assume that the ideal in the polynomial ring over the field of fractions of the parameters

$$I^e = \langle f_1, \cdots, f_n \rangle : g_S^\infty \subset \mathbb{Q}(T_1, \cdots, T_s)[X_1, \cdots, X_n]$$

is radical and 0-dimensional.
Then S is said generically simple.

Remark 1 *Note that the ideal I generated by $f_1, \cdots, f_n \subset \mathbb{Q}[T_1, \cdots, T_s, X_1, \cdots, X_n]$ needs neither to be radical nor equidimensional, although it is sufficient to satisfy the hypotheses.*

Moreover, given a parametric system S defined by $f_1 = 0, \cdots, f_n = 0, g_1 \neq 0, \cdots, g_r \neq 0$, we introduce these two polynomials:
$-\ j_S$ is the determinant of the Jacobian matrix of $f_1, \cdots, f_n$ with respect to the unknowns, of degree denoted by δ
$-\ g_S$ is the product of the g_i for $1 \leq i \leq r$ of degree denoted by δ'
Note that we have $\delta \leq \sum_{i=1}^{n} d_i - n$ and $\delta' = \sum_{j=1}^{r} d'_j$.

Main results

We can now state our main results.

Theorem 1 *Let S be a* generically simple *parametric system.*
Then the total degree of the minimal discriminant variety is bounded by

$$d_1 \cdots d_n(1 + \delta + \delta')$$

Theorem 2 *Let S be a parametric system* generically simple *defined by $f_1 = 0, \cdots, f_n = 0, g_1 \neq 0, \cdots, g_r \neq 0$. Then the union of the varieties defined by the $n+2$ following ideals:*
- R denotes the ring $\mathbb{Q}[T_1, \cdots, T_s]$

$$\left(\left\langle f_1^h, \cdots, f_n^h, ZX_0g_S^h - 1, X_1 - 1\right\rangle \cap R[X_0]\right)_{|X_0=0} \qquad (\mathcal{I}_1)$$
$$\vdots \qquad \vdots$$
$$\left(\left\langle f_1^h, \cdots, f_n^h, ZX_0g_S^h - 1, X_n - 1\right\rangle \cap R[X_0]\right)_{|X_0=0} \qquad (\mathcal{I}_n)$$

$$\left(\langle f_1, \cdots, f_n, g_S - X_{n+1}, ZX_{n+1} - 1\rangle \cap R[X_{n+1}]\right)_{|X_{n+1}=0} \qquad (\mathcal{I}_{n+1})$$

$$\left(\langle f_1, \cdots, f_n, j_S, Zg_S - 1\rangle\right) \cap R \qquad (\mathcal{I}_{n+2})$$

is the minimal discriminant variety of S.

Corollary 1 *A discriminant variety of a* generically simple *parametric system can be computed in:*

$$\sigma^{\mathcal{O}(1)}(d_1 \cdots d_n(\delta + \delta'))^{\mathcal{O}(n+s)}$$

steps on a classical Turing machine. The variable σ denotes the maximal binary size of coefficients of $f_1, \cdots, f_n$ and $g_1, \cdots, g_r$.

Remark 2 *If the system is not* generically simple, *then the the union of the varieties computed is the whole parameter space, which is thus an easy way to check if the initial conditions are verified.*

Remark 3 *Any elimination algorithm may actually be used to compute a discriminant variety, which is welcomed when it comes to an effective computation. Among others, Gröbner bases with a block ordering [15, 16], sparse elimination [13] or straight-line programs [28] may lead to efficient computations.*

Remark 4 *If we allow ourself to use the model of a probabilistic bounded Turing Machine, then at the cost of the sparsity of the system, we may replace the computation of $\mathbf{V}(\mathcal{I}_1), \ldots, \mathbf{V}(\mathcal{I}_n)$ by the computation of the variety of:*

$$\left(\left\langle f_1^h, \cdots, f_n^h, ZX_0g_S^h - 1, \gamma_1X_1 + \cdots + \gamma_nX_n - 1\right\rangle \cap \mathbb{Q}[T_1, \cdots, T_s][X_0]\right)_{|X_0=0}$$

where $(\gamma_1, \ldots, \gamma_n)$ is chosen randomly in $\{0, \ldots, D-1\}^n$ and $D := 3d_1 \cdots d_n$.[1]

[1] The remark 4 and the corollary 1 are proved Section 3

2 Log-space reduction

2.1 Preliminaries

The goal of this section is to show how to reduce the problem of computing the minimal discriminant variety (the *discriminant problem*) to the *elimination problem*. We know that the *elimination problem* is solvable in polynomial space ([27]). Thus via the reduction we prove that the problem of computing the minimal discriminant variety is solvable in polynomial space.

DISCRIMINANT FUNCTION:
- *Input*: $f_1, \cdots, f_n, g_S, j_S \in \mathbb{Q}[T_1, \cdots, T_s, X_1, \cdots, X_n]$
- *Output*: $q_{1,1}, \cdots, q_{t,u_t} \in \mathbb{Q}[T_1, \cdots, T_s]$ such that $\cup_{i=1}^{t} \mathbf{V}(\langle q_{i,1}, \cdots, q_{i,u_i} \rangle)$ is the minimal discriminant variety.

ELIMINATION FUNCTION:
- *Input*: $\begin{cases} p_1, \cdots, p_m \in \mathbb{Q}[T_1, \cdots, T_s][X_1, \cdots, X_n]; \\ T_1, \ldots, T_s \end{cases}$
- *Output*: $q_1, \cdots, q_t \in \mathbb{Q}[T_1, \cdots, T_s]$ such that $\mathbf{V}(\langle q_1, \cdots, q_t \rangle)$ is the variety of the elimination ideal $\langle p_1, \cdots, p_m \rangle \cap \mathbb{Q}[T_1, \cdots, T_s]$.

To achieve the reduction, we will first describe more precisely how the minimal discriminant variety can be decomposed. In [26], the authors show that the minimal discriminant variety of a *generically simple* parametric system S is the union of 3 varieties, denoted respectively by V_{inf}, V_{ineq} and V_{crit}. Let us remind the definitions of these varieties under our assumptions.

Definition 5 *Let S be a* generically simple *parametric system defined by $f_1 = 0, \cdots, f_n = 0$ and $g_1 \neq 0, \cdots, g_r \neq 0$. The varieties V_{inf},V_{ineq} and V_{crit} of the parameters space are respectively defined as follow:*

$V_{inf} = \overline{\pi}(\overline{\mathcal{C}}_S \cap \mathcal{H}_\infty)$
where $\overline{\mathcal{C}}_S$ is the projective closure of the constructible set defined by S, and $\mathcal{H}_\infty = (\mathbb{C}^s \times \mathbb{P}_n) \setminus (\mathbb{C}^s \times \mathbb{C}^n)$ is the hypersurface at the infinity.

$V_{ineq} = \boldsymbol{V}((I_S : g_S^\infty + \langle g_S \rangle) \cap \mathbb{Q}[T_1, \cdots, T_s])$

$V_{crit} = \boldsymbol{V}((I_S : g_S^\infty + \langle j_S \rangle) \cap \mathbb{Q}[T_1, \cdots, T_s])$

Theorem 3 *[26] The* minimal discriminant variety *of a* generically simple *parametric system is the union of V_{inf}, V_{ineq} and V_{crit}.*

Geometrically, this theorem characterizes the different varieties in the parameter space over which the *generically simple* parametric system is not *geometrically regular*. More precisely, the theorem means that over the minimal discriminant variety, three types of irregularity may appear. The first one is the intersections of the system of equations with the Jacobian. The second one is the intersection with the inequations. And the last one is the intersection in the projective space of the the hypersurface at the infinity with the projective closure of the parametric system's zeros.

V_{crit} is already directly the solution of an *elimination problem*. This is the component for which the generic radicality condition is needed. We will now focus on reducing the computation of each of the two varieties V_{inf} and V_{ineq} to the *elimination problem*.

2.2 Reduction of V_{inf} and correctness

Before going further, it should be clear that the computation of V_{inf} can not be handled by the standard projective elimination methods if we want to certify a singly exponential complexity. All of these methods have no good complexity bounds essentially because of the intersection with the particular hypersurface at the infinity as we will see later. However this doesn't prevent us to use results of the projective elimination theory.

Using the algebraic representation of the projection $\overline{\pi}$ of [12], with the notations of the definition 5 we reformulate V_{inf}:

$$V_{inf} \quad = \quad \mathbf{V}\left(\left(\bigcap_{i=1}^{n}(J_S)_{|X_0=0} : X_i^\infty\right) \cap \mathbb{Q}[T_1, \cdots, T_s]\right)$$

where $J_S := (I_S : g_S^\infty)^h$. Note that $\overline{\mathcal{C}}_S = \mathbf{V}(J_S)$.

And using the reformulation of the ideal homogenization of [12], we obtain a formulation of J_S which match explicitly the input of the problem:

$$J_S \quad = \quad \langle f_1^h, \cdots, f_n^h\rangle : {g_S^h}^\infty : X_0^\infty$$

This is however not yet satisfying since this formulation is not trivially reducible to a single elimination problem. The problem here does not come from the saturation by the variables X_i which can be simply handled with the Rabinowitsch trick [29] of adding the new variable Z and the new equation $ZX_i - 1$ to the initial polynomials. Neither is the saturation by g_S a problem since again we may add the equation $Zg_S - 1 = 0$. The complications arise actually from the variable X_0. First we have to saturate by X_0 and then we have to specialize X_0 with 0 to finally eliminate the variables X_i. And it is regrettable since this prevents us to use the usual trick to get rid of the saturation, as we saw in introduction. Moreover we don't want to apply successively two ELIMINATION FUNCTION since it could lead us to an exponential space algorithm.

Fortunately we manage to sort out this problem by proving that for the variety we want to compute, we can commute the specialization of X_0 by 0 and the elimination, which is remarkable since this operation will allow us to use the Rabinowitsch trick to localize by

X_0. Note that the commutation step does not alter the computation only because of the particular structure of V_{inf}.

Proposition 1 *Let S be a parametric system. Then the component V_{inf} of the minimal discriminant variety of S is the union of the varieties defined by the n following ideals for $1 \leq i \leq n$:*

$$\left(\langle f_1^h, \cdots, f_n^h, ZX_0 g_S^h - 1, X_i - 1\rangle \cap R[X_0]\right)_{|X_0=0}$$

Remark 5 *Note that the condition* generically simple *is not needed for the reduction of the computation of V_{inf}. Moreover the proposition remains true even if the number of equations differs from the number of unknowns.*

The proof of this proposition is based on the three following lemmas. The first one gives some basic useful equalities, where h_i denotes the homogenization by the variable X_i with respect to the variables $X_0, \cdots, \hat{X_i}, \cdots, X_n$.

Lemma 1 *[12] Let $J \subset \mathbb{Q}[T_1, \cdots, T_s][X_0, \cdots, X_n]$ be an ideal homogeneous in $X_0, \cdots, X_n$ and p be a polynomial of $\mathbb{Q}[T_1, \cdots, T_s][X_0, \cdots, X_n]$ also homogeneous in $X_0, \cdots, X_n$. Then for all $0 \leq i \leq n$ we have:*

$$(J_{|X_i=1})^{h_i} = J : X_i^\infty$$
$$(J : p^\infty)_{|X_i=1} = J_{|X_i=1} : p_{|X_i=1}^\infty$$
$$J : X_i^\infty \cap \mathbb{Q}[T_1, \cdots, T_s] = J_{|X_i=1} \cap \mathbb{Q}[T_1, \cdots, T_s]$$

and for all $1 \leq i \leq n$:

$$J_{|X_i=1} \cap \mathbb{Q}[T_1, \cdots, T_s][X_0] = (J \cap \mathbb{Q}[T_1, \cdots, T_s][X_0, X_i])_{|X_i=1}$$

Proof: These are classical results that can be recovered from [12]. □

Now comes the first lemma toward the reduction, which proves essentially that the union of the varieties defined by the elimination ideals of the proposition 1 contains V_{inf}.

Lemma 2 *Let J be an ideal of $\mathbb{Q}[T_1, \cdots, T_s][X_0, \cdots, X_n]$ homogeneous in $X_0, \cdots, X_n$. Then, for all $1 \leq i \leq n$ we have:*

$$(J \cap \mathbb{Q}[T_1, \cdots, T_s][X_0, X_i])_{|X_0=0, X_i=1}$$
$$\cap$$
$$(J_{|X_0=0} : X_i^\infty) \cap \mathbb{Q}[T_1, \cdots, T_s]$$

Proof: Let $p \in (J \cap \mathbb{Q}[T_1, \cdots, T_s][X_0, X_i])_{|X_0=0, X_i=1}$. The polynomial p is homogeneous in $X_0, \ldots, X_n$ since it depends only on the variables $T_1, \ldots, T_s$. Thus with the notations of the lemma 1, we have $p \in ((J_{|X_0=0})_{|X_i=1})^{h_i}$. And $J_{|X_0=0}$ being homogeneous in $X_0, \cdots, X_n$, one can apply the first equality of Lemma 1 to deduce $p \in J_{|X_0=0} : X_i^\infty$ which proves the desired result. □

And finally comes the keystone lemma related to the proposition, proving the reciprocal inclusion.

Lemma 3 *Let J be an ideal of $\mathbb{Q}[T_1, \cdots, T_s][X_0, \cdots, X_n]$ homogeneous in $X_0, \cdots, X_n$. Then, for all $1 \leq i \leq n$, we have:*

$$\sqrt{(J \cap \mathbb{Q}[T_1, \cdots, T_s][X_0, X_i])_{|X_0=0, X_i=1}}$$
$$\cup$$
$$\bigcap_{j=1}^{n} (J_{|X_0=0} : X_j^\infty) \cap \mathbb{Q}[T_1, \cdots, T_s]$$

Proof: Let $p \in \bigcap_{j=1}^{n} (J_{|X_0=0} : X_j^\infty) \cap \mathbb{Q}[T_1, \cdots, T_s]$. By definition there exist $q_1, \cdots, q_n \in \mathbb{Q}[T_1, \cdots, T_s][X_0, \cdots, X_n]$ and $k_1, \cdots, k_n \in \mathbb{N}$ such that:

$$\left\{ \begin{array}{rcll} p_1 & := & pX_1^{k_1} + X_0 q_1 & \\ & \vdots & & \in J \\ p_n & := & pX_n^{k_n} + X_0 q_n & \end{array} \right.$$

Since the part of p_i of degree k_i in $X_0, \cdots, X_n$ belongs also to J, we can assume that $p_1, \cdots, p_n$ are homogeneous in $X_0, \cdots, X_n$. Thus, we have in particular:

$$\deg_{X_1, \cdots, X_n}(q_j) < k_j$$

Now we fix a total degree term order $<_X$ on the variables $X_1, \cdots, X_n$. Let K denote the field $\mathbb{Q}(T_1, \cdots, T_s, X_0)$ and consider $p_1, \cdots, p_n$ as polynomials of $K[X_1, \cdots, X_n]$. Denoting by $\mathcal{J}$ the ideal they generate, it follows immediately that

$$G := \{p_1, \cdots, p_n\}$$

form a Gröbner basis of $\mathcal{J}$ with respect to $<_X$ since the p_i have disjoint head terms. Let i be an integer between 1 and n. We first show how to prove the lemma when we have a polynomial of $\mathcal{J}$ such that:

- it is univariate in X_i (1)
- it has all its coefficients in $\mathbb{Q}[T_1, \cdots, T_s, X_0]$ (2)
- its head coefficient is a power of p (3)

Assume for a while that r_i is such a polynomial, d_{X_i} being its degree in X_i. It follows indeed that $r_i \in \mathcal{J}^c$ the contraction ideal of $\mathcal{J}$. And since $p = lcm\{HC(g) | g \in G\}$ we have [5]:

$$\mathcal{J}^c = \langle G \rangle : p^\infty$$

meaning that for some $k \in \mathbb{N}$, $p^k r_i \in \langle G \rangle \subset J$. Finally J is homogeneous so that $\tilde{r_i}$, the part of degree d_{X_i} of $p^k r_i$, belongs to $J \cap \mathbb{Q}[T_1, \cdots, T_s][X_0, X_i]$ and can be written as:

$$\tilde{r_i} = p^l X_i^{d_i} + X_0 q$$

with $l \in \mathbb{N}$ and $q \in \mathbb{Q}[T_1, \cdots, T_s][X_0, X_i]$, which is an equivalent way of writing

$$p \in \sqrt{(J \cap \mathbb{Q}[T_1, \cdots, T_s][X_0, X_i])_{|X_0=0, X_i=1}}$$

It remains us to show the existence of a polynomial satisfying (1),(2) and (3). To carry out this problem, we first notice that $\mathcal{J}$ is zero-dimensional in $K[X_1, \cdots, X_n]$ since the set of the head terms of its Gröbner basis contains a pure power of each variable X_i. So, we may consider the finite dimensional $K-$space vector $\mathcal{A} = K[X_1, \cdots, X_n]/\mathcal{J}$ along with $\mathbf{e}$ the monomial basis of $\mathcal{A}$ induced by G. More precisely, denoting by $\overline{x}$ the class of x in $\mathcal{A}$, we define see $\mathbf{e}$ as the set of $\overline{e_j}$ for $1 \leq j \leq D := \dim(\mathcal{A})$ such that e_j is a term of $K[X_1, \cdots, X_n]$ not multiple of any head term of G. Finally we denote by S the multiplicatively closed set $\{p^k, k \in \mathbb{N}\}$. We will follow a classical method to exhibit a monic univariate polynomial from a zero-dimensional ideal, with coefficients in K. And with results of [5] we ensure that its coefficients are not only in K but rather in the ring $S^{-1}\mathbb{Q}[T_1, \cdots, T_s, X_0] \subset K$.
Let us introduce the classical linear application of multiplication by X_i:

$$\begin{array}{rccc} \Phi_i : & \mathcal{A} & \rightarrow & \mathcal{A} \\ & \overline{q} & \mapsto & \overline{X_i q} \end{array}$$

Then we note M_i the matrix of Φ_i in the base $\mathbf{e}$:

$$M_i = \begin{array}{c} \\ \overline{e_1} \\ \vdots \\ \overline{e_D} \end{array} \begin{array}{c} \begin{array}{ccc} \overline{X_i e_1} & \cdots & \overline{X_i e_D} \end{array} \\ \begin{pmatrix} & & \\ & c_{k,l} & \\ & & \end{pmatrix} \end{array}$$

we notice that the coefficients of M_i come from the reduction of the monomials $X_i e_l$ for $1 \leq l \leq D$ by the Gröbner basis G. And as we can see in [5], this kind of reduction only involves division by the head coefficients of G, such that:

$$\overline{X_i e_l} = c_{1,l}\overline{e_{1,l}} + \cdots + c_{D,l}\overline{e_{D,l}}$$

with $c_{1,l}, \cdots, c_{D,l}$ not only in K but more precisely in the ring $S^{-1}\mathbb{Q}[T_1, \cdots, T_s, X_0] \subset K$ where $S = \{p^k, k \in \mathbb{N}\}$. As a straightforward consequence, if we denote by $\mathcal{P}_i$ the monic characteristic polynomial of M_i in the new variable U, we have $\mathcal{P}_i \in S^{-1}\mathbb{Q}[T_1, \cdots, T_s, X_0][U]$. Besides by the Cayley-Hamilton's theorem, $\mathcal{P}_i$ applied to the variable X_i is the null element of $\mathcal{A}$, meaning that $\mathcal{P}_i(X_i)$ belongs to $\mathcal{J}$ and may be written as:

$$\mathcal{P}_i(X_i) = X_i^D + C_{D-1}X_i^{D-1} + \cdots + C_0$$

with $C_k \in S^{-1}\mathbb{Q}[T_1, \cdots, T_s, X_0]$ for $1 \leq k \leq D-1$. Finally, for some $k' \in \mathbb{N}$ we have

$$r_i := p^{k'}\mathcal{P}_i(X_i) \in \mathcal{J} \cap \mathbb{Q}[T_1, \cdots, T_s, X_0][X_i]$$

which satisfies all the conditions we wanted to achieve the demonstration. □

Finally, a proper combination of the lemmas proves the proposition 1.

2.3 Reduction of V_{ineq} and correctness

As to bound the computation of the variety induced by the inequations

$$V_{ineq} = \mathbf{V}\left((I_S : g_S^\infty + \langle g_S \rangle) \cap \mathbb{Q}[T_1, \cdots, T_s]\right)$$

the direct approach consists first in performing a saturation and then in using the output along with g_S as the input of an elimination algorithm. However this method may not have a single exponential bound on the time complexity in the worst case. Hence both of these algorithms may use a polynomial space in the size of the input, which could finally cost an exponential space if no more care is taken.

In this section we show how to bypass the problem, notably by relaxing the condition on the output and allowing some components of V_{inf} to mix in.

Proposition 2 *Let S be a parametric system. If we denote by $W_{ineq} \subset \mathbb{C}^s$ the variety defined by the following ideal:*

$$(\langle f_1, \cdots, f_n, g_S - X_{n+1}, ZX_{n+1} - 1\rangle \\ \cap \mathbb{Q}[T_1, \cdots, T_s][X_{n+1}])_{|X_{n+1}=0}$$

then the following inclusions chain holds:

$$V_{ineq} \subset W_{ineq} \subset V_{ineq} \cup V_{inf}$$

The first step to prove this proposition is to delay the saturation.

Lemma 4 *Let $p_1, \cdots, p_m, q, r \in \mathbb{Q}[Y_1, \cdots, Y_k]$. Let us fix $<$ a term order and assume that the head monomial of q shares no variable in common with the monomials of $p_1, \cdots, p_m, r$. Then we have the following equality:*

$$\langle p_1, \cdots, p_m\rangle : r^\infty + \langle q\rangle = \langle p_1, \cdots, p_m, q\rangle : r^\infty$$

Proof: The inclusion from left to right is trivial. For the other inclusion, let $p \in \langle p_1, \cdots, p_m, q\rangle : r^\infty$. Denoting by M the head monomial of q with respect to $<$, we obtain by division:

$$p = p' + qt \qquad p', t \in \mathbb{Q}[Y_1, \cdots, Y_k] \tag{1}$$

such that no monomial of p' is multiple of M. It remains to show that p' belongs to $\langle p_1, \cdots, p_m\rangle : r^\infty$ and the proof will be complete. By hypothesis, we know that there exists $l > 0$ and $c_1, \cdots, c_m, c \in \mathbb{Q}[Y_1, \cdots, Y_k]$ such that:

$$r^l p' = c_1 p_1 + \cdots + c_m p_m + cq$$

We divide each of the c_i by q as in (1) and denote by c'_i the remainder of the division. We thus obtain:

$$r^l p' - c'_1 p_1 - \cdots - c'_m p_m = c'q$$

with $c' \in \mathbb{Q}[Y_1, \cdots, Y_k]$. We remark that the polynomial on the left part of the equality has no monomial which is multiple of M, while the head monomial of the right part of the equality is M times the head monomial of c', which means $c' = 0$ and this achieves the proof. □

Corollary 2 *Let $f_1, \cdots, f_n, g$ be some polynomials of $\mathbb{Q}[T_1, \cdots, T_s][X_1, \cdots, X_n]$. Then:*

$$\langle f_1, \cdots, f_n \rangle : g^\infty + \langle g - X_{n+1} \rangle = \langle f_1, \cdots, f_n, g - X_{n+1} \rangle : X_{n+1}^\infty$$

Thanks to this result, we can now reformulate V_{ineq} as being the variety of:

$$\left(\langle f_1, \cdots, f_n, g_S - X_{n+1} \rangle : X_{n+1}^\infty \right)_{|X_{n+1}=0} \cap \mathbb{Q}[T_1, \cdots, T_s]$$

The reduction is not yet complete and we encounter here the same problem we had for the computation of V_{inf}, that is the saturation by X_{n+1} before the specialization of X_{n+1} by 0. This is just fine since the lemmas 1,2 and 3 provide us tools to handle it, even if they do not completely solve the problem yet.

For the first inclusion, we note:

$$I^S := \langle f_1, \cdots, f_n, g_S - X_{n+1} \rangle : X_{n+1}^\infty$$

it follows that the varieties of the proposition 2 rewrite as:

$$\begin{aligned} V_{ineq} &= \mathbf{V}\left(I^S_{|X_{n+1}=0} \cap \mathbb{Q}[T_1, \cdots, T_s] \right) \\ W_{ineq} &= \mathbf{V}\left((I^S \cap \mathbb{Q}[T_1, \cdots, T_s][X_{n+1}])_{|X_{n+1}=0} \right) \end{aligned}$$

and we show easily:

$$(I^S \cap \mathbb{Q}[T_1, \cdots, T_s][X_{n+1}])_{|X_{n+1}=0} \subset I^S_{|X_{n+1}=0} \cap \mathbb{Q}[T_1, \cdots, T_s]$$

which, in term of varieties, proves the first inclusion of the proposition 2.

For the other inclusion we will mainly use the lemma 3. For this, we introduce the homogenization variable X_0, and denote with the exponent h the homogenization by X_0 with respect to $X_0, \cdots, X_{n+1}$. We need also the following classical lemma, which dissociates the affine part from the component at the infinity of a homogeneous ideal.

Lemma 5 *[12] Let $J \in \mathbb{Q}[T_1, \cdots, T_S][X_0, \cdots, X_{n+1}]$ an ideal homogeneous in $X_0, \cdots, X_{n+1}$. Then the following equality holds:*

$$\sqrt{J} = \sqrt{J + \langle X_0 \rangle} \cap \sqrt{J : X_0^\infty}$$

In term of varieties, the equality follows from the observation that $\mathbf{V}(J)$ is the union of $\mathbf{V}(J) \cap \mathcal{H}_\infty$ and $\overline{\mathbf{V}(J) \setminus \mathcal{H}_\infty}$.
We now homogenize I^S by X_0 and we get:

$$W_{ineq} = \mathbf{V}(I^{S^h} \cap \mathbb{Q}[T_1, \cdots, T_s][X_0, X_{n+1}]_{|X_{n+1}=0, X_0=1})$$

Using lemma 3, we get directly:

$$W_{ineq} \subset \mathbf{V}\left(\bigcap_{j=0}^{n} ((I^{S^h})_{|X_{n+1}=0} : X_j^\infty) \cap \mathbb{Q}[T_1, \cdots, T_s]\right)$$

Then we show that $(I^{S^h})_{|X_{n+1}=0}$ contains an ideal which begins to look like what we want:

$$\begin{array}{rcl} I^{S^h} & = & (\langle f_1, \cdots, f_n\rangle : g_S^\infty + \langle g_S - X_{n+1}\rangle)^h \\ (I^{S^h})_{|X_{n+1}=0} & \supset & \left\langle f_1^h, \cdots, f_n^h\right\rangle : {g_S^h}^\infty : X_0^\infty + \left\langle X_0 g_S^h\right\rangle \\ & \supset & J_S + \left\langle X_0 g_S^h\right\rangle \end{array}$$

Then, the lemma 5 allows us to split the ideal $J_S + \left\langle X_0 g_S^h\right\rangle$ in:

$$\sqrt{J_S + \left\langle X_0 g_S^h\right\rangle} = \underbrace{\sqrt{J_S + \left\langle X_0 g_S^h\right\rangle + \langle X_0\rangle}}_{I_1} \cap \underbrace{\sqrt{(J_S + \left\langle X_0 g_S^h\right\rangle) : X_0^\infty}}_{I_2}$$

such that we now have the following inclusion:

$$W_{ineq} \subset \mathbf{V}\left(\bigcap_{j=0}^{n} (I_1 : X_j^\infty) \cap (I_2 : X_j^\infty) \cap \mathbb{Q}[T_1, \cdots, T_s]\right)$$

From there, denoting again $\mathbb{Q}[T_1, \ldots, T_s]$ by R, we remark for $0 \leq j \leq n$:

$$I_1 : X_j^\infty \cap R \quad \supset \quad (J_S)_{|X_0=0} : X_j^\infty \cap R$$

And:

$$\begin{array}{rcl} I_2 : X_j^\infty \cap R & \supset & \left(J_S + \left\langle g_S^h\right\rangle\right) : X_j^\infty : X_0^\infty \cap R \\ & \supset & \left((J_S)_{|X_0=1} + \langle g_S\rangle\right) : X_j^\infty \cap R \\ & \supset & I^S : X_j^\infty \cap R \\ & \supset & I^S \cap R \end{array}$$

Which allows us to conclude with:

$$\begin{array}{l} W_{ineq} \subset \mathbf{V}\left(I^S \cap \bigcap_{j=0}^{n} \left(J_{S|X_0=0}\right) : X_j^\infty) \cap \mathbb{Q}[T_1, \cdots, T_s]\right) \\ \\ \quad \subset V_{ineq} \cup V_{inf} \end{array}$$

This proves the theorem 2.

3 Degree issues

The study of the degree of the minimal discriminant variety relies strongly on the Bezout-Inequality [23, 18]. What we call degree of an ideal I (resp. a variety V) and denote $\deg(I)$ (resp. $\deg(V)$) is the sum of the degrees of the prime ideals associated to $\sqrt{I}$ (resp. the sum of the degrees of the irreducible components of V). With this definition, from [23, 18] we have for $I, J \subset \mathbb{Q}[T_1, \ldots, T_s, X_0, \ldots, X_n]$ and $f \in \mathbb{Q}[T_1, \ldots, T_s, X_0, \ldots, X_n]$:

$$\begin{aligned} \deg(I+J) &\leq \deg(I)\deg(J) \\ \deg(I : f^\infty) &\leq \deg(I) \\ \deg(I \cap \mathbb{Q}[T_1, \ldots, T_s]) &\leq \deg(I) \\ \deg(I) &= \deg(\mathbf{V}(I)) \end{aligned}$$

Degree of V_{inf}

Here we use the prime decomposition of $\sqrt{J_S}$ to bound the degree of V_{inf}. This decomposition will also allow us to prove Remark 4.

First we remind that from proposition 1:

$$V_{inf} = \mathbf{V}\left(\left(\left(\bigcap_{i=1}^{n} J_S : X_i^\infty\right) \cap \mathbb{Q}[T_1, \cdots, T_s, X_0]\right)_{|X_0=0}\right)$$

where $J_S = \left\langle f_1^h, \cdots, f_n^h \right\rangle : {g_S^h}^\infty : X_0^\infty$

Continuing with the properties of the degree we have:

$$\deg(J_S) \leq \deg\left(\left\langle f_1^h, \cdots, f_n^h \right\rangle\right) \leq d_1 \cdots d_n$$

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ be the prime ideals associated to $\sqrt{J_S}$. Then we have:

$$\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_k = \sqrt{J_S}$$

$$\deg(\mathfrak{P}_1) + \cdots + \deg(\mathfrak{P}_k) \leq d_1 \cdots d_n$$

Now let denote by $\lambda_1, \ldots, \lambda_j$ the indices of the prime ideal which do not contain any power of X_i for some $1 \leq i \leq n$. It follows that:

$$\bigcap_{i=1}^{n} \sqrt{J_s : X_i^\infty} = \mathfrak{P}_{\lambda_1} \cap \cdots \cap \mathfrak{P}_{\lambda_j}$$

such that

$$\begin{aligned} \deg(V_{inf}) &= \deg\left(\textstyle\bigcap_{i=1}^{n} \sqrt{J_s : X_i^\infty} \cap \mathbb{Q}[T_1, \cdots, T_s, X_0]_{|X_0=0}\right) \\ &\leq d_1 \cdots d_n \end{aligned}$$

We use the decomposition of $\sqrt{J_S}$ to prove the remark 4.

Proof: (of Remark 4)
We extend Lemma 1, where we replace X_i by a homogeneous linear form in $X_0, \cdots, X_n$, which leads to the following property. If J is an ideal of $\mathbb{Q}[T_1, \cdots, T_s][X_0, \cdots, X_n]$ homogeneous in $X_0, \cdots, X_n$, and $L \in \mathbb{Q}[X_0, \cdots, X_n]$ is a homogeneous linear form in $X_0, \cdots, X_n$, then:

$$J : L^\infty \cap \mathbb{Q}[T_1, \cdots, T_s, X_0] = (J + \langle L - 1 \rangle) \cap \mathbb{Q}[T_1, \cdots, T_s, X_0]$$

From there, we know that the prime ideals which contain a power of X_i for all $1 \leq i \leq n$ contain in fact all the homogeneous linear forms of $\mathbb{Q}[X_0, \cdots, X_n]$. Let denote by E the $\mathbb{Q}$-spacevector of homogeneous linear forms of $\mathbb{Q}[X_0, \cdots, X_n]$. Thus we have for all $L \in E$:

$$\sqrt{J_S : L^\infty} = \bigcap_{i=1}^{j} \mathfrak{P}_{\lambda_i} : L^\infty$$

Let B denote the bounded lattice $\{0, \ldots, D-1\}^n$ of E, where $D = 3d_1 \cdots d_n$. And A be defined by:

$$A := \bigcup_{i=1}^{j} (\mathfrak{P}_{\lambda_i} \cap E)$$

Such that for $L \in B \setminus A$, we have:

$$\textstyle\bigcap_{i=1}^{k} \mathfrak{P}_i : L^\infty = \bigcap_{i=1}^{j} \mathfrak{P}_{\lambda_i}$$

And since each $\mathfrak{P}_{\lambda_i} \cap E$ is a strict linear subspace of E, it follows that A is the union of $j \leq \prod_{i=1}^{n} d_i = \frac{D}{3}$ strict linear subspaces of E . Each $\mathfrak{P}_{\lambda_i} \cap E$ intersects the lattice B in at most D^{n-1} points. Thus the probability of choosing L in $B \cap A$ is $\frac{|B \cap A|}{|B|} \leq \frac{1}{3}$. And for all $L \in B \setminus A$ we have:

$$\begin{aligned}
V_{inf} &= \mathbf{V}\left(\bigcap_{i=1}^{k} \mathfrak{P}_i : L^\infty \cap \mathbb{Q}[T_1, \cdots, T_s, X_0]_{|X_0=0}\right) \\
&= \mathbf{V}\left(\left(\bigcap_{i=1}^{k} \mathfrak{P}_i + \langle L - 1 \rangle\right) \mathbb{Q}[T_1, \cdots, T_s, X_0]_{|X_0=0}\right) \\
&= \mathbf{V}((\langle f_1^h, \cdots, f_n^h, ZX_0 g_S^h - 1, L - 1 \rangle \\
&\qquad \cap \mathbb{Q}[T_1, \cdots, T_s, X_0])_{|X_0=0})
\end{aligned}$$

□

Degree of V_{ineq} and V_{crit}

The degree of the two other components are obtained easily. By definition:

$$\begin{aligned} V_{ineq} &= \mathbf{V}\left((\langle f_1, \cdots, f_n\rangle : g_S^\infty + \langle g_S\rangle) \cap \mathbb{Q}[T_1, \cdots, T_s]\right) \\ V_{crit} &= \mathbf{V}\left((\langle f_1, \cdots, f_n\rangle : g_S^\infty + \langle j_S\rangle)\mathbb{Q}[T_1, \cdots, T_s]\right) \end{aligned}$$

Thus with the properties of the degree, we have respectively:

$$\begin{aligned} \deg(V_{ineq}) &\leq d_1 \cdots d_n \delta' \\ \deg(V_{crit}) &\leq d_1 \cdots d_n \delta \end{aligned}$$

Hence we proved the theorem 1.

Degree of representation of the elimination

To compute the ELIMINATION FUNCTION in a deterministic way, we follow the ideas of [6] which uses the affine effective Nullstellensatz to reduce the problem to a linear algebra system of non homogeneous linear form. One could use the ideas of [28, 20, 21] to perform this elimination, whose complexity bounds rely on the projective effective Nullstellensatz of [25]. However these bounds only hold in a bounded probabilistic Turing machine.

Here we will use the Brownawell's prime power version of Nullstellensatz (see [8]), which is a variant of the affine effective Nullstellensatz:

Theorem 4 *[8] Let $J \subset k[x_0, \cdots, x_n]$ be an ideal generated by m homogeneous polynomial of respective degrees $d_2 \geq \cdots \geq d_m \geq d_1$ and $\mathfrak{M} = \langle x_0, \cdots, x_n\rangle$. Then there are prime ideal $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ containing J and positive integers $e_0, \cdots, e_r$ such that:*

$$\mathfrak{M}^{e_0}\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_\mathfrak{r}{}^{e_r} \subset J, \text{ and}$$

$$e_0 + \sum_{i=1}^{r} e_i \deg(\mathfrak{P}_i) \leq (3/2)^\mu d_1 \cdots d_\mu$$

where $\mu = \min(m, n)$

Using the proposition 3 of [23], we know that if $\mathfrak{P}$ is a prime ideal, then there is $n+1$ polynomials $f_1, \cdots, f_{n+1}$ such that:

$$\mathbf{V}(f_1, \cdots, f_{n+1}) = \mathbf{V}(\mathfrak{P})$$

with $\deg(f_i) \leq \deg(\mathfrak{P})$ for all $1 \leq i \leq n+1$

Thus we deduce the following:

Proposition 3 *Let $I \subset \mathbb{Q}[T_1, \cdots, T_s][X_1, \cdots, X_n]$ generated by $f_1, \cdots, f_m$ indexed such that their degrees satisfy $d_2 \geq \cdots \geq d_m \geq d_1$. Then, with $\mu = \min(m, n)$ we introduce:*

$$F := \left\{ \sum_{i=1}^{m} g_i f_i | \begin{array}{c} g_i \in \mathbb{Q}[T_1, \cdots, T_s][X_1, \cdots, X_n] \\ and \\ \deg(g_i f_i) \leq (3/2)^\mu d_1 \cdots d_\mu \end{array} \right\}$$

Then we have:

$$\mathbf{V}(I \cap \mathbb{Q}[T_1, \cdots, T_s]) = \mathbf{V}(F \cap \mathbb{Q}[T_1, \cdots, T_s])$$

Proof: We homogenize the polynomials $f_1, \cdots, f_m$ by H with respect to $T_1, \cdots, T_s, X_1, \cdots, X_n$, and denote by J the ideal they generate. Then with $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ being prime ideals containing J and verifying the theorem of Brownawell, it follows that the result holds when intersecting J and $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ by $\mathbb{Q}[T_1, \cdots, T_s, H]$. Finally we use the Heintz's proposition reminded above on each $\mathfrak{P}_i$ and specialize H by 1 to conclude. □

Now consider the coefficients of the polynomials $g_1, .., g_m, g$ as unknowns. Assume furthermore that $g_1, \cdots, g_m$ contains all the monomials in $T_1, \cdots, T_s, X_1, \cdots, X_n$ of degree less or equal to $(3/2)^\mu d_1 \cdots d_\mu$, and that g contains the monomials in $T_1, \cdots, T_s$ only. Thus, finding the coefficients satisfying the formula:

$$\sum_{i=1}^{m} g_i f_i - g = 0$$

reduces to the problem of finding null space generators of a matrix of size lower or equal to

$$(m+1)((3/2)^\mu d_1 \cdots d_\mu)^{(n+s)} \times ((3/2)^\mu d_1 \cdots d_\mu)^{(n+s)}$$

Hence the complexity of the corollary 1 follows.

4 Example

We show here an example of minimal discriminant varieties application in our framework. It will allow us to prove that the real parametrization of the Enneper surface matches its real implicit form. In [14] the author solves this problem with a combination `REDLOG`,`QEPCAD` and `QERRC`. Through the process, he has to simplify formulas whose textual representation contains approximatively 500 000 characters. We will see that our framework allows us to use *minimal* discriminant varieties to solve this problem. Notably, this allows us to keep formulas small. The following computations are done with the `Maple` package `DV`, which uses `FGb` to carry out the elimination function. We also use the factorization functions of `Maple` to take the square-free part of the polynomials given in the input, and to simplify the output. Finally `RS` and the `Maple` package `RAG` allows us to treat the discriminant varieties we compute. All these software are available in the Salsa Software Suite [1].

When E and F are two lists of polynomials, T a list of parameters and X a list of unknowns, we denote by

$$\mathbf{DV}(E, F, T, X)$$

the discriminant variety of the parametric system $S : (p = 0)_{p \in E} \wedge (q \neq 0)_{q \in F}$.

4.1 Definition of the Enneper surface

The real Enneper surface $\mathcal{E} \subset \mathbb{R}^3$ has a parametric definition:

$$\mathcal{E} = \left\{ (x(u,v), y(u,v), z(u,v)) \quad | \quad (u,v) \in \mathbb{R}^2 \right\}$$

$$\begin{array}{rcl} x(u,v) & = & 3u + 3uv^2 - u^3 \\ y(u,v) & = & 3v + 3u^2v - v^3 \\ z(u,v) & = & 3u^2 - 3v^2 \end{array}$$

We will also consider the graph of the Enneper surface $\mathcal{E}_g \subset \mathbb{R}^5$ defined as follows:

$$\mathcal{E}_g = \left\{ (x(u,v), y(u,v), z(u,v), u, v) \quad | \quad (u,v) \in \mathbb{R}^2 \right\}$$

Beside, a Gröbner basis computation returns easily its implicit Zarisky closure $\overline{\mathcal{E}}$ [12, 14]:

$$\overline{\mathcal{E}} = \left\{ (x,y,z) \in \mathbb{R}^3 \quad | \quad p(x,y,z) = 0 \right\}$$

$$\begin{array}{rcl} p(x,y,z) & = & -19683x^6 + 59049x^4y^2 - 10935x^4z^3 - 118098x^4z^2 + 59049x^4z - 59049x^2y^4 \\ & & -56862x^2y^2z^3 - 118098x^2y^2z - 1296x^2z^6 - 34992x^2z^5 - 174960x^2z^4 \\ & & +314928x^2z^3 + 19683y^6 - 10935y^4z^3 + 118098y^4z^2 + 59049y^4z + 1296y^2z^6 \\ & & -34992y^2z^5 + 174960y^2z^4 + 314928y^2z^3 + 64z^9 - 10368z^7 + 419904z^5 \end{array}$$

4.2 Discriminant varieties

The main idea to compare $\mathcal{E}_\}$ and $\overline{\mathcal{E}}$ is in a first step to compute the union of their discriminant varieties, V. In a second step we compare $\mathcal{E}_g$ and $\overline{\mathcal{E}}$ on a finite number of well chosen test points outside of V. Finally, the properties of the discriminant variety ensure us that the result of our comparison on these test points holds for every points outside of V.

More precisely, $\mathcal{E}_g$ and $\overline{\mathcal{E}}$ are both algebraic varieties of dimension 2. Thus we choose a common subset of 2 variables, x and y for example, which will be the *parameters* for the two discriminant varieties:

$$\begin{array}{rcl} V_1^{xy} & := & \mathbf{DV}(\ [x - x(u,v), y - y(u,v), z - z(u,v)]\ ,\ [\ ]\ ,\ [x,y]\ ,\ [z,u,v]\ ) \\ V_2^{xy} & := & \mathbf{DV}(\ [p(x,y,z)]\ ,\ [\ ]\ ,\ [x,y]\ ,\ [z]\ ) \end{array}$$

The number of equations equals the number of unknowns in both case and our algorithm returns a non trivial variety for both systems. This ensures us that the two systems are *generically simple*. Here are the results of the computations, which lasted less than 1 second

on a 2.8 GHz Intel Pentium cpu:

$$\begin{aligned} V_1^{xy} = \quad & \mathbf{V}(y^6+60y^4+768y^2-4096+3x^2y^4-312x^2y^2+768x^2+3x^4y^2+60x^4+x^6) \\ & \cup\mathbf{V}(x^6+48x^4+3x^4y^2-336x^2y^2+3x^2y^4+768x^2+4096+768y^2+48y^4+y^6) \end{aligned}$$

$$\begin{aligned} V_2^{xy} = \quad & \mathbf{V}(y^6+60y^4+768y^2-4096+3x^2y^4-312x^2y^2+768x^2+3x^4y^2+60x^4+x^6) \\ & \cup\mathbf{V}(x^6+48x^4+3x^4y^2-336x^2y^2+3x^2y^4+768x^2+4096+768y^2+48y^4+y^6) \\ & \cup\mathbf{V}(x-y)\cup\mathbf{V}(y)\cup\mathbf{V}(x+y)\cup\mathbf{V}(x) \end{aligned}$$

We denote by $\pi_{xy} : \mathbb{R}^3 \to \mathbb{R}^2$ the canonical projection. Then the properties of the discriminant variety ensure us that for each connected component $\mathcal{C}$ of $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$, $(\pi_{xy}^{-1}(\mathcal{C}) \cap \mathcal{E}, \pi_{xy})$ and $(\pi_{xy}^{-1}(\mathcal{C}) \cap \overline{\mathcal{E}}, \pi_{xy})$ are both analytic covering. Moreover, $\mathcal{E} \subset \overline{\mathcal{E}}$. Thus if $\mathcal{C}$ is a connected component of $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$, we get the following property:

$$\exists p \in \mathcal{C}, \pi_{xy}^{-1}(p) \cap \mathcal{E} = \pi_{xy}^{-1}(p) \cap \overline{\mathcal{E}} \iff \forall p \in \mathcal{C}, \pi_{xy}^{-1}(p) \cap \mathcal{E} = \pi_{xy}^{-1}(p) \cap \overline{\mathcal{E}}$$

This allows us to prove that $\mathcal{E}$ and $\overline{\mathcal{E}}$ are equal above $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$: we take one point p in each connected component of $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$, and check that the number of real solutions of $\pi_{xy}^{-1}(p) \cap \mathcal{E}$ and of $\pi_{xy}^{-1}(p) \cap \overline{\mathcal{E}}$ is the same. We use the `RAG` package to get one point in each connected component and `RS` to solve the corresponding zero dimensional real systems. This allows us to prove that

$$\pi_{xy}^{-1}(\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})) \cap \mathcal{E} = \pi_{xy}^{-1}(\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})) \cap \overline{\mathcal{E}}$$

In order to get more information, we repeat this process using respectively the discriminant varieties on the parameter set $\{x, z\}$ and $\{y, z\}$. This leads to the following computations:

$$\begin{aligned} V_1^{xz} &:= \mathbf{DV}(\ [x-x(u,v), y-y(u,v), z-z(u,v)]\ ,\ [\,]\ ,\ [x,z]\ ,\ [y,u,v]\ ) \\ V_2^{xz} &:= \mathbf{DV}(\ [p(x,y,z)]\ ,\ [\,]\ ,\ [x,z]\ ,\ [y]\ ) \end{aligned}$$

and

$$\begin{aligned} V_1^{yz} &:= \mathbf{DV}(\ [x-x(u,v), y-y(u,v), z-z(u,v)]\ ,\ [\,]\ ,\ [y,z]\ ,\ [x,u,v]\ ) \\ V_2^{yz} &:= \mathbf{DV}(\ [p(x,y,z)]\ ,\ [\,]\ ,\ [y,z]\ ,\ [x]\ ) \end{aligned}$$

The result is shown on Figure 1.

Then we compute as above one point in each connected component of the complementary, and this allows us to prove that:

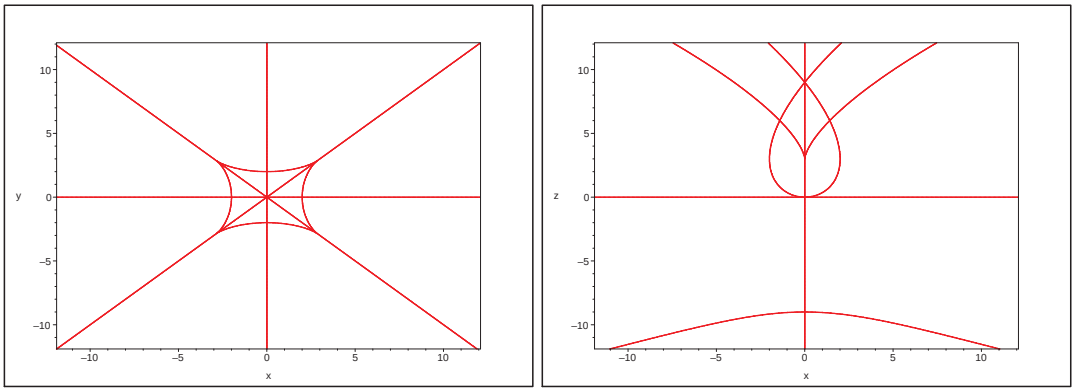
$$\pi_{xz}^{-1}(\mathbb{R}^2 \setminus (V_1^{xz} \cup V_2^{xz})) \cap \mathcal{E} = \pi_{xz}^{-1}(\mathbb{R}^2 \setminus (V_1^{xz} \cup V_2^{xz})) \cap \overline{\mathcal{E}}$$

and

$$\pi_{yz}^{-1}(\mathbb{R}^2 \setminus (V_1^{yz} \cup V_2^{yz})) \cap \mathcal{E} = \pi_{yz}^{-1}(\mathbb{R}^2 \setminus (V_1^{yz} \cup V_2^{yz})) \cap \overline{\mathcal{E}}$$

Using the following notations:

$$\begin{aligned} V^{xy} &:= \pi_{yz}^{-1}(V_1^{xy} \cup V_2^{xy}) \\ V^{xz} &:= \pi_{xz}^{-1}(V_1^{xz} \cup V_2^{xz}) \\ V^{yz} &:= \pi_{yz}^{-1}(V_1^{yz} \cup V_2^{yz}) \end{aligned}$$



$V_1^{xy} \cup V_2^{xy}$ $V_1^{xz} \cup V_2^{xz}$

$V_1^{yz} \cup V_2^{yz}$

Figure 1: The discriminant varieties for the three possible sets of parameters

it remains us to check what happens above each component of

$$V^{xy} \cap V^{xz} \cap V^{yz}$$

An idea is to set apart the linear components from the others. We introduce

$$V_L := \mathbf{V}(x+y) \cup \mathbf{V}(x-y) \cup \mathbf{V}(x) \cup \mathbf{V}(y) \cup \mathbf{V}(z)$$

and denote respectively $V^{xy} \setminus V_L$,$V^{xz} \setminus V_L$ and $V^{yz} \setminus V_L$ by $\widetilde{V^{xy}}$, $\widetilde{V^{xz}}$ and $\widetilde{V^{yz}}$. Using the RAGlib, we verify that

$$\widetilde{V^{xy}} \cap \widetilde{V^{xz}} \cap \widetilde{V^{yz}}$$

has actually no real points.

It remains us to check what happens on each of the 5 linear components of V_L. The intersection of $\mathcal{E}_g$ or $\overline{\mathcal{E}}$ with a linear component P may be seen as a linear substitution of a variable. This operation produces 5 pairs of varieties of dimension 2 (Table 1). To check their equality, we use the same strategy as above and compute the 5 discriminant varieties with 1 parameter,3 unknowns of $K_1, \ldots, K_5$, respectively $V_{K_1}, \ldots, V_{K_5}$, and the 5 discriminant varieties with 1 parameter,1 unknown of $L_1, \ldots, L_5$, respectively $V_{L_1}, \ldots, V_{L_5}$. We check that $K_i = L_i$ for each point by connected component of the complementary of $V_{K_i} \cup V_{L_i}$, in less than 1 second. And at last we intersect again the varieties with their discriminant varieties, which reduces the problem to compare 5 pairs of zero dimensional systems. Thus we check that the equality holds for the finitely many points considered. Finally this allows us to conclude that $\mathcal{E} = \overline{\mathcal{E}}$.

5 Conclusion

We provided a *deterministic* single exponential bit-complexity bound for the computation of the minimal discriminant variety of a *generically simple* parametric system. Note that the complexity of our algorithm relies on the elimination problem's complexity. Thus in a probabilistic bounded Turing machine, the work of [28] for example leads to a polynomial complexity bound in the size of the output. Or if we are only interested in the real solutions, then the use of the single block elimination routine of [4, 3] improves directly the deterministic complexity bound of our method.

The reduction presented in this article is easy to implement in conjunction with a software performing elimination, as those used in [15, 16], [13] or [21] for example.

It would be worth studying the complexity of the computation of the *minimal* discriminant variety when we have more equations than unknowns.

	$\mathcal{E}_g$				
W	$\mathbf{V}(x)$	$\mathbf{V}(y)$	$\mathbf{V}(z)$	$\mathbf{V}(y+x)$	$\mathbf{V}(y-x)$
$\mathcal{E}_g \cap W$	K_1	K_2	K_3	K_4	K_5
System	$\begin{cases} 0-x(u,v) \\ y-y(u,v) \\ z-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ 0-y(u,v) \\ z-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ y-y(u,v) \\ 0-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ -x-y(u,v) \\ z-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ x-y(u,v) \\ z-z(u,v) \end{cases}$
Parameter	z	z	x	x	x
Unknowns	y,u,v	x,u,v	y,u,v	z,u,v	z,u,v
Minimal Discriminant Variety	$V_{K_1} = \mathbf{V}(z) \cup \mathbf{V}(z-3) \cup \mathbf{V}(z-9)$	$V_{K_2} = \mathbf{V}(z) \cup \mathbf{V}(z+3) \cup \mathbf{V}(z+9)$	$V_{K_3} = \mathbf{V}(x) \cup \mathbf{V}(x^2+2)$	$V_{K_4} = V_{K_5} = \mathbf{V}(x+4) \cup \mathbf{V}(x-4) \cup \mathbf{V}(x^2-8) \cup \mathbf{V}(x^2+2)$	

	$\overline{\mathcal{E}}$				
W	$\mathbf{V}(x)$	$\mathbf{V}(y)$	$\mathbf{V}(z)$	$\mathbf{V}(y+x)$	$\mathbf{V}(y-x)$
$\overline{\mathcal{E}} \cap W$	L_1	L_2	L_3	L_4	L_5
System ($sqfr = squarefree$)	$sqfr(p(0,y,z))$	$sqfr(p(x,0,z))$	$sqfr(p(x,y,0))$	$sqfr(p(x,-x,z))$	$sqfr(p(x,x,z))$
Parameter	z	z	x	x	x
Unknown	y	x	y	z	z
Minimal Discriminant Variety	$V_{L_1} = \mathbf{V}(z+9) \cup \mathbf{V}(z) \cup \mathbf{V}(z-3) \cup \mathbf{V}(z-9)$	$V_{L_2} = \mathbf{V}(z-9) \cup \mathbf{V}(z) \cup \mathbf{V}(z-3) \cup \mathbf{V}(z+9)$	$V_{L_3} = \mathbf{V}(x)$	$V_{L_4} = V_{L_5} = \mathbf{V}(x+4) \cup \mathbf{V}(x-4) \cup \mathbf{V}(x^2-8) \cup \mathbf{V}(x)$	

Table 1: Discriminant varieties of the sub varieties

References

[1] SALSA: http://fgbrs.lip6.fr/salsa/software.

[2] Anai, H., Hara, S., and Yokoyama, K. Sum of roots with positive real parts. In *ISSAC'05*, pp. 21–28.

[3] Basu. New results on quantifier elimination over real closed fields and applications to constraint databases. *JACM: Journal of the ACM 46* (1999).

[4] Basu, Pollack, and Roy. On the combinatorial and algebraic complexity of quantifier elimination. *JACM: Journal of the ACM 43* (1996).

[5] Becker, T., and Weispfenning, V. *Gröbner bases*, vol. 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[6] Bernasconi, A., Mayr, E. W., Raab, M., and Mnuk, M. Computing the dimension of a polynomial ideal, May 06 2002.

[7] Brown, C. W., and McCallum, S. On using bi-equational constraints in CAD construction. In *ISSAC* (2005), pp. 76–83.

[8] Brownawell, W. D. A pure power product version of the Hilbert Nullstellensatz. *Michigan Math. J. 45*, 3 (1998), 581–597.

[9] Buchberger, B. A theoretical basis for the reduction of polynomials to canonical forms. *j-SIGSAM 10*, 3 (Aug. 1976), 19–29.

[10] Collins, G. E. *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition*. Springer Verlag, 1975.

[11] Corvez, S., and Rouillier, F. Using computer algebra tools to classify serial manipulators. In *Automated Deduction in Geometry* (2002), pp. 31–43.

[12] Cox, D., Little, J., and O'Shea, D. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer Verlag, 1992.

[13] Cox, D. A., Little, J. B., and O'Shea, D. B. *Using algebraic geometry*, vol. 185 of *Graduate Texts in Mathematics*. Springer-Verlag, 1998.

[14] Dolzmann, A. Solving geometric problems with real quantifier elimination. In *Automated Deduction in Geometry* (1998), vol. 1669 of *Lecture Notes in Computer Science*, pp. 14–29.

[15] Faugère, J. C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *ISSAC 2002* (2002), pp. 75–83.

[16] Faugère, J.-C., and Joux, A. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *Advances in cryptology—CRYPTO 2003*, vol. 2729 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2003, pp. 44–60.

[17] Fotiou, I. A., Rostalski, P., Parrilo, P. A., and Morari, M. Parametric optimization and optimal control using algebraic geometry methods. *International Journal of Control (to appear)*.

[18] Fulton, W. *Intersection theory*, second ed., vol. 2. Springer-Verlag, Berlin, 1998.

[19] Giusti, M. Some effectivity problems in polynomial ideal theory. In *EUROSAM 84*, vol. 174 of *Lecture Notes in Comput. Sci.* 1984, pp. 159–171.

[20] Giusti, M., and Heintz, J. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In *Computational algebraic geometry and commutative algebra*, vol. 34. 1993, pp. 216–256.

[21] Giusti, M., and Schost, É. Solving some overdetermined polynomial systems. In *ISSAC'99*.

[22] Grigoriev, D., and Vorobjov, N. Bounds on numers of vectors of multiplicities for polynomials which are easy to compute. In *ISSAC'00*, pp. 137–146.

[23] Heintz, J. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science 24*, 3 (Aug. 1983), 239–277.

[24] Krick, T., and Pardo, L. M. A computational method for Diophantine approximation. In *Algorithms in algebraic geometry and applications*, vol. 143 of *Progr. Math.* 1996, pp. 193–253.

[25] Lazard, D. Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination. *Bull. Soc. Math. France 105* (1977), 165–190.

[26] Lazard, D., and Rouillier, F. Solving parametric polynomial systems. Tech. rep., INRIA, 2004. Accepted for publication in Journal of Symbolic Computation.

[27] Matera, G., and Turull Torres, J. M. The space complexity of elimination theory: upper bounds. In *Foundations of computational mathematics*. 1997, pp. 267–276.

[28] Puddu, S., and Sabia, J. An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs. *J. Pure Appl. Algebra 129*, 2 (1998), 173–200.

[29] Rabinowitsch, J. L. Zum Hilbertschen Nullstellensatz. *Math. Ann. 102*, 1 (1930), 520.

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

[31] Sommese, A. J., Verschelde, J., and Wampler, C. W. Introduction to numerical algebraic geometry. In *Solving polynomial equations*, vol. 14 of *Algorithms Comput. Math.* 2005, pp. 301–335.

[32] Verschelde, J. Numerical algebraic geometry and symbolic computation. In *ISSAC* (2004), p. 3.

[33] Wang, D. *Elimination methods*. Springer-Verlag, Vienna, 2001.

[34] Weispfenning. Comprehensive grobner bases. *Journal of Symbolic Computation 14* (1992).

[35] Yang, L., and Zeng, Z. An open problem on metric invariants of tetrahedra. In *ISSAC '05*, pp. 362–364.

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

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

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