Computing Parametric Geometric Resolutions

Éric Schost
Laboratoire GAGE, École polytechnique
91128 Palaiseau Cedex, France
schost@gage.polytechnique.fr

October 11, 2002

Abstract

Given a polynomial system of n equations in n unknowns that depends on some parameters, we define the notion of *parametric geometric resolution* as a means to represent some generic solutions in terms of the parameters.

The coefficients of this resolution are rational functions of the parameters; we first show that their degree is bounded by the Bézout number d^n, where d is a bound on the degrees of the input system. Then we present a probabilistic algorithm to compute a parametric resolution. Its complexity is polynomial in the size of the output and in the complexity of evaluation of the input system. The probability of success is controlled by a quantity polynomial in the Bézout number.

We present several applications of this process, notably to computations in the Jacobian of hyperelliptic curves and to questions of real geometry.

AMS Subject classification: 14Q20, 14Y05, 13P99, 68W30.
Keywords: polynomial systems with parameters, complexity, theory of elimination, symbolic Newton operator.

1 Introduction

A variety of real-life problems can be modelized by polynomial systems involving free variables, or *parameters*. Even if a specialization of such a system may be easy to solve, a description of the generic solutions is typically hard to grasp. Still, the motivations for computing a generic description are numerous; we present various examples below. Our goal here is then to present an efficient, ready-to-implement, elimination procedure, adapted to such situations.

An introductory example. We can describe the main features of our approach on a simple example. Consider the following version of a serial robot, inspired by [30]: the robot has two segments of length 1, and is built as follows:

θ_2

(x, y)

θ_1

Figure 1: A simple robot arm

The coordinates (x, y) are thought as parameters, from which we want to recover the angles θ_1, θ_2. For $i = 1, 2$, take $c_i = \cos\theta_i$ and $s_i = \sin\theta_i$. Then these values are related by the following polynomial system:

$$\begin{cases} c_1 + c_2 &= x, \\ s_1 + s_2 &= y, \\ c_1^2 + s_1^2 &= 1, \\ c_2^2 + s_2^2 &= 1. \end{cases}$$

Our goal is to describe the solutions (c_1, s_1, c_2, s_2) in terms of (x, y) by the following kind of representation:

$$s_2^2 - ys_2 + \frac{1}{4}\frac{x^4 + 2x^2y^2 - 4x^2 + y^4}{x^2 + y^2} = 0 \text{ and } \begin{cases} c_1 &= \frac{y}{x}s_2 + \frac{1}{2}\frac{x^2-y^2}{x}, \\ c_2 &= -\frac{y}{x}s_2 + \frac{1}{2}\frac{x^2+y^2}{x}, \\ s_1 &= -s_2 + y. \end{cases}$$

This representation gives a description of the solutions (c_1, s_1, c_2, s_2) for *generic* parameters values (x, y). Indeed, given any value of (x, y) in $\mathbb{R}^2$ that does not cancel the denominators, s_2 becomes the solution of a second-degree equation, with coefficients in $\mathbb{R}$. Then the values of (c_1, s_1, c_2) are given as functions of s_2.

The general case. We now proceed to describe the above process in greater generality. We suppose that we are given a polynomial system $\mathbf{f} = (f_1, \ldots, f_n)$ in $k[P_1, \ldots, P_m, X_1, \ldots, X_n]$, where k is any effective field. The variables $\mathbf{P} = (P_1, \ldots, P_m)$ are thought as parameters, the variables $\mathbf{X} = (X_1, \ldots, X_n)$ as unknowns, and we wish to compute a description of the solutions in terms of the parameters.

We restrict our study to the solutions that do not cancel the Jacobian determinant of the system $\mathbf{f}$ with respect to the variables $\mathbf{X}$. These solutions will be called *simple solutions*.

We then define the notion of *parametric geometric resolution* as a description of these simple solutions by means of primitive element techniques. More precisely, the solutions will be described through the following encoding:

$$Q_u(u) = 0, \quad \begin{cases} Q'_u(u)x_1 &= V_1(u), \\ &\vdots \\ Q'_u(u)x_n &= V_n(u), \end{cases}$$

where

- $x_1, \ldots, x_n$ are the images of $X_1, \ldots, X_n$ in a suitable quotient algebra,
- u is a linear form in $x_1, \ldots, x_n$,
- $Q_u, V_1, \ldots, V_n$ are univariate polynomials whose coefficients are rational functions in $P_1, \ldots, P_m$.

The polynomial Q_u is the *minimal polynomial* of the *primitive element* u. The polynomials $V_1, \ldots, V_n$ are *parametrizations* that give the values of the unknowns $\mathbf{X}$ in terms of the roots of the polynomial Q_u. This generalizes the representation of the solutions given in the introductory example.

We keep in mind that all coefficients of $Q_u, V_1, \ldots, V_n$ are rational functions in the parameters. In the general case, the introduction of the factor $Q'_u(u)$ in the parametrizations will assure good degree properties for these coefficients.

Just as in the example, we also note that this representation gives a description of the *generic* solutions of the parametric system. Indeed, since the coefficients of $Q_u, V_1, \ldots, V_n$ are rational functions, we must avoid the parameter values that cancel one of their denominators.

Fields of application. Before presenting the content of this article, we describe some applications of these techniques. The last two examples cover some situations that are *a priori* non-parametric: yet, they can usefully be brought to our setting, through an appropriate shift of point of view.

- *Specialization.* A parametric resolution describes generic solutions. As such, it can be specialized on an open subset of the parameter space, where the denominators of the coefficients of the polynomials $Q_u, V_1, \ldots, V_n$ do not vanish. This enables to solve generic specializations of the input system $\mathbf{f}$ without further computations, for instance in software environments which do not provide elimination facilities.

We illustrate this possibility in Section 6 by the example of *halving in the Jacobian of a genus 2 curve*: dividing by 2 in a Jacobian amounts to solve a parametric polynomial system, whose parameters are the coordinates of the dividend. A parametric resolution of such a system was used in the genus 2 point-counting record of [23].

- *Real geometry.* As a particular case of parametric system, we may consider systems with infinitesimal coefficients, seeing the infinitesimals as parameters. Solving such systems is a cornerstone of many algorithms in real algebraic geometry [36, 37, 51]. These algorithms often require to study the limits of the solutions when the infinitesimals go to zero, for which a parametric resolution is well-suited.

  As an example, we will show how to compute a family of critical points on deformations of a singular real hypersurface. The computation of such critical points is used as a subroutine in the algorithm of [51], which aims at computing one point on each connected component on a real hypersurface. Our implementation enabled a first comparison between several approaches for this question, applied to a practical interpolation problem in [52].

- *Computing eliminating polynomials.* Finally, many elimination questions can be reduced to our setting, and formulated as the computation of a suitable eliminating form for a polynomial function of the unknowns $X_1, \ldots, X_n$. Such computations are straightforward once a parametric resolution is known.

  This possibility is illustrated by an application coming from invariant theory [7]: the classification of a particular orbit space requires to compute the relation between 3 rational functions of 2 variables. We refer to Section 6 for the treatment of this question using our parametric formalism.

Overview of the article. The goal of this article is threefold. First, we estimate the complexity of a parametric resolution: we give bounds on the degrees of the polynomials that appear in such a representation. Next, we present a probabilistic algorithm for computing a parametric resolution, and estimate in a precise manner its complexity and probability of success. Finally, we present the applications mentioned above in greater detail.

- *Complexity bounds.* The first part of this article is devoted to prove that all coefficients that appear in a parametric resolution have degree bounded by an intrinsic geometric quantity, which itself is bounded by the Bézout number of the input system. This result is the continuity of [53, 27] and notably [34], and improves on the following important aspect.

  The results obtained in the above references require the zero-set of the defining system $\mathbf{f} = (f_1, \ldots, f_n)$ to be in *Noether position* with respect to the variables $P_1, \ldots, P_m$. This condition implies that the number of solutions of all specializations of the system $\mathbf{f}$ is constant, if counted with multiplicities. In particular, this excludes all systems whose parametric resolution comprises *denominators* in the parameters.

Whereas this condition is not a limitation in the context of [53, 27, 34], it is a severe restriction for our situation. First, the validity of this condition is not easily tested for. Furthermore, many applications, for instance all those mentioned in the above paragraphs, do not fit into this setting. Our simple introductory example already gave a hint that the presence of denominators should be expected in many practical cases.

Treating the general case then requires a further geometric study, to control the complexity of the denominators in the coefficients. Correspondingly, if we want to follow the philosophy of elimination used in [27, 34], new algorithmic tools must be used.

- *Algorithms.* We propose an algorithm for a computing a parametric resolution, with complexity polynomial in the size of the output. This algorithm was implemented, and its practical behavior reflects its good theoretical complexity, enabling us to treat otherwise out-of-reach systems. The algorithm is probabilistic, and we have explicit estimates on the probability of success.

  Here is a sketch of the method: the generic solutions will be obtained by successive approximations using a formal Newton operator.

  The underlying paradigm is that solving a polynomial system over the base field k is a well-solved task. Thus, as input, we suppose that we are given a generic point $(p_1, \ldots, p_m)$ in the parameter space, and a description of the solutions of the system $\mathbf{f}$ specialized at $(p_1, \ldots, p_m)$.

  This description has the form

$$q_u(u) = 0, \quad \left\{ \begin{array}{lcl} q'_u(u)x_1 & = & v_1(u), \\ & \vdots & \\ q'_u(u)x_n & = & v_n(u), \end{array} \right.$$

  where $q_u, v_1, \ldots, v_n$ are univariate polynomials with coefficients in k, $x_1, \ldots, x_n$ are the algebraic variables and u is a linear form in $x_1, \ldots, x_n$. Then there exists a parametric resolution composed of polynomials $Q_u, V_1, \ldots, V_n$, such that $q_u, v_1, \ldots, v_n$ are the polynomials $Q_u, V_1, \ldots, V_n$, with coefficients specialized at $(p_1, \ldots, p_m)$.

  Our algorithm consists in lifting the dependency of the polynomials $q_u, v_1, \ldots, v_n$ in the parameters $P_1, \ldots, P_m$; that is, we "unspecialize" the parameters. To this effect, we apply a formal Newton operator to $[q_u, v_1, \ldots, v_n]$. This produces a sequence of polynomials whose coefficients are the successive *power series expansions* of the coefficients of $[Q_u, V_1, \ldots, V_n]$ at $(p_1, \ldots, p_m)$.

  The idea of applying lifting techniques to solve polynomial systems can be traced back to the articles of Trinks [63] and Winkler [66]. It also underlies much of the recent work of the TERA group [27, 26, 25, 28, 34, 35], where the use of the *Straight-Line Program* encoding was the key to algorithms with good complexity.

As in the above references, we suppose that the input system is given by a Straight-Line Program. Our first contribution is then a generalization of the lifting operator of [28]. The computation sequence we propose becomes more lucid, the key point being to extend this operator to a wider class of representations, *triangular representations*.

Then, as in many algorithms relying on lifting techniques, the final step requires to go from a local description to a global one. In our context, this consists in recovering the coefficients of the parametric resolution, which are rational functions, from the knowledge of their power series expansions. This step was not necessary under the stronger hypotheses of [27, 26, 25, 28, 34, 35]; it is now made necessary by the presence of denominators in the coefficients.

To this effect, we propose an algorithm for the rational reconstruction of multivariate rational functions, which reduces to the usual Padé approximants computation in the univariate case. Its complexity is the best known to date for this question.

Summary.

- We define the notion of parametric geometric resolution, as a means to represent the generic solutions of a parametric system. We give bounds for the complexity of a parametric resolution, in a geometric context where previous results did not apply.
- We propose a probabilistic algorithm for computing such a parametric resolution, and work out a precise control of the probabilistic aspects. This algorithm is valid over any effective field, non necessarily perfect, as was often the case [53, 34, 28]. The complexity is polynomial in the size of the output.
- As intermediate results, we give an algorithm for the rational reconstruction of a multivariate rational function. We also extend the Newton operator given in [28] to a larger context, resulting in a simpler presentation of the computations.
- Finally, we demonstrate the use of these results by treating various real-life applications.

Related work. We have already mentioned that this article is in the continuity of the work of the TERA group [27, 26, 25, 28, 35] and notably of [34]. Let us mention other possible approaches.

- *Zero-dimensional solving over a rational function field.* The resolution of the system as a zero-dimensional problem over the rational function field $k(P_1, \ldots, P_m)$ leads to the same output as our algorithm.

  For the resolution of zero-dimensional systems, we mention in particular the algorithm of geometric resolution [27, 26, 25, 28, 35]. Other approaches include the computation of Gröbner bases [9, 21], possibly followed by a Rational Univariate Representation [50]. We also mention the linear algebra methods, using the matrices introduced by Macaulay [44] or generalizations thereof [19, 47, 18].

The complexity of these zero-dimensional solving methods is not always known in terms of operations in the base field, which is here the rational function field $k(P_1, \ldots, P_m)$. Moreover, there is no obvious bound on the degrees of the rational functions that may appear through the computations. Thus it is quite difficult to estimate the complexity of this kind of approach in terms of operations in k, but practice reveals that they are quite costly.

- *Exhaustive descriptions.* A radically different approach to the question of parametric systems is to give an *exhaustive description* of the solutions, describing all possibilities of degeneracy. We mention in particular the techniques of *dynamic evaluation* [16, 29, 14], the *comprehensive Gröbner bases* [65] and the computation of parametric Gröbner bases proposed in [32] and [45].

  Whereas the complexities of the dynamic evaluation method or of Montes' algorithm are not known to us, the approaches of Grigoriev and Vorobjov and of Weispfenning are known to lead to algorithms of complexity of order $d^{O(mn^2)}$, d being a bound on the degree of the input polynomials. A very crude estimation of our complexity result will turn out to be the better bound $d^{O(mn)}$. Still, the reader must keep in mind that the outputs of these algorithms differ from ours.

Acknowledgements. I wish to thank M. Giusti, who advised my PhD. Thesis, from which this work is taken. It is also a pleasure to thank J. Heintz, G. Lecerf, L.-M. Pardo and B. Salvy for many helpful comments.

2 Notations, main results

We now present our results in a more precise fashion. To this effect, we recall and introduce some notations used in the sequel.

The input system. The base field is denoted by k; we will denote by $\overline{k}$ its algebraic closure. We consider a polynomial system $\mathbf{f} = (f_1, \ldots, f_n)$ in $k[P_1, \ldots, P_m, X_1, \ldots, X_n]$, where the indeterminates $\mathbf{P} = (P_1, \ldots, P_m)$ are thought as parameters, or free variables, and $\mathbf{X} = (X_1, \ldots, X_n)$ are thought as algebraic variables.

Given a value $\mathbf{p} = (p_1, \ldots, p_m)$ in $\overline{k}^m$, we will denote by $\mathbf{f}(\mathbf{p}, .)$ the system $\mathbf{f}$ where the indeterminates $\mathbf{P}$ are specialized at $\mathbf{p}$.

For the sake of concision, the field $\overline{k}(P_1, \ldots, P_m)$ will be called $\mathcal{K}$; nevertheless, we will remember that it is a field of rational functions, when geometric arguments or complexity statements are required. For similar concision imperatives, sums such as $\sum u_i x_i$ will always be taken for i in $1, \ldots, n$.

Geometric objects. Let $\mathcal{I}$ be the ideal generated by the polynomials $(f_1, \ldots, f_n)$ in $\overline{k}[P_1, \ldots, P_m, X_1, \ldots, X_n]$. We wish to exclude the locus where the Jacobian determinant $\mathbf{jac}(\mathbf{f}, \mathbf{X})$ vanishes. To this effect, we consider $\mathcal{J} = (\mathcal{I} : \mathbf{jac}(\mathbf{f}, \mathbf{X})^\infty)$ the intersection of the primary components of $\mathcal{I}$ which do not contain a power of $\mathbf{jac}(\mathbf{f}, \mathbf{X})$. The ideal $\mathcal{J}$ can be defined by polynomials with coefficients in k; we suppose that it is not the trivial ideal (1). The corresponding variety $\mathcal{V} = \mathcal{V}(\mathcal{J}) \subset \mathbb{A}^{m+n}(\overline{k})$ is our object of interest.

Let us denote by $\pi : \mathbb{A}^{m+n}(\overline{k}) \to \mathbb{A}^m(\overline{k})$ the canonical projection on the parameter space $\mathbb{A}^m(\overline{k})$. Then Lazard's Lemma (see [8] and [46, Proposition 3.2]) shows the following fact:

Fact 1 *The restriction of π to each irreducible component of $\mathcal{V}(\mathcal{J})$ is a dominant map, not necessarily finite but with generically finite fibers.*

Thus, for a generic value $\mathbf{p}$ in $\mathbb{A}^m(\overline{k})$, the system $\mathbf{f}(\mathbf{p}, .) = 0$ admits finitely many solutions in $\mathcal{V}$, so this situation is actually zero-dimensional over the field $\mathcal{K} = \overline{k}(P_1, \dots, P_m)$.

We denote by $\mathcal{J}_{\mathcal{K}}$ the ideal generated in $\mathcal{K}[X_1, \dots, X_n]$ by the polynomials in $\mathcal{J}$, and by $x_1, \dots, x_n$ the images of $X_1, \dots, X_n$ modulo $\mathcal{J}_{\mathcal{K}}$. Lazard's Lemma implies that $\mathcal{J}$ and $\mathcal{J}_{\mathcal{K}}$ are radical ideals, and the above discussion states that $\mathcal{J}_{\mathcal{K}}$ has dimension zero. We now present our basic way of representing such zero-dimensional objects.

Geometric resolutions. The notion of geometric resolution is defined for zero-dimensional systems in [27, 26, 25, 28, 35]. The definition in a general setting is as follows.

Let $\mathfrak{K}$ be any field, $\mathfrak{J}$ a zero-dimensional ideal of $\mathfrak{K}[X_1, \dots, X_n]$ and x_i the image of X_i modulo $\mathfrak{J}$, for i in $1, \dots, n$. Then a *geometric resolution* of the extension $\mathfrak{K} \to \mathfrak{K}[X_1, \dots, X_n]/\mathfrak{J}$, if it exists, consists in:

- a primitive element $u = \sum u_i x_i$ of $\mathfrak{K} \to \mathfrak{K}[X_1, \dots, X_n]/\mathfrak{J}$,
- its monic minimal polynomial $Q_u \in \mathfrak{K}[\mathcal{U}]$,
- a parametrization of the algebraic variables in terms of the primitive element. Following [4, 50, 28], we use in priority a parametrization of the form $Q_u'(u)x_i = V_i(u)$ in $\mathfrak{K}[X_1, \dots, X_n]/\mathfrak{J}$, where V_i is in $\mathfrak{K}[\mathcal{U}]$, for $i = 1, \dots, n$.

In our particular context, we call *parametric geometric resolution*, or *parametric resolution*, a geometric resolution of the extension $\mathcal{K} \to \mathcal{K}[X_1, \dots, X_n]/\mathcal{J}_{\mathcal{K}}$. Thus, it has coefficients in the rational function field $\mathcal{K}$.

The main results in this paper are the proof of the existence of a primitive element of $\mathcal{K} \to \mathcal{K}[X_1, \dots, X_n]/\mathcal{J}_{\mathcal{K}}$, bounds on the degrees of the expressions that may appear in the corresponding parametric resolution, a study of the locus where its specialization fails, and a probabilistic algorithm to compute such a resolution.

Complexity notations. We will estimate the complexity of the input and the intrinsic complexity of the geometric objects $\mathcal{V}$ and π using the following notations.

- The polynomials $(f_1, \dots, f_n)$ are of degree bounded by d, and given by a Straight-Line Program of size L (see [11] for a definition).

- We call $\deg_\pi$ the generic cardinality of the fibers of the restriction of π to $\mathcal{V}$, that is the generic number of simple solutions of the specialized systems $\mathbf{f}(\mathbf{p},.) = 0$.

  We call $\deg_\mathcal{V}$ the degree of the variety $\mathcal{V}$, using the notion of affine degree given by Heintz in [33].

  Using the Bézout inequality of [33], both $\deg_\pi$ and $\deg_\mathcal{V}$ can be bounded by the Bézout number d^n.

The complexities of our algorithms will be measured using the following notations.

- The notation $f \in O_{\log}(g)$ means that there exists a constant a such that f is in $O(g \log(g)^a)$.

- $\mathcal{M}_u(D)$ denotes the cost of the multiplication of univariate polynomials of degree D, in terms of operations in the base ring. $\mathcal{M}_u(D)$ can be taken in $O(D \log D \log\log D)$, or $O_{\log}(D)$, using the algorithms of Schönhage and Strassen [56] and Schönhage [55].

- $\mathcal{M}_s(D, m)$ denotes the cost of m-variate series multiplication at precision D. This can be taken less than $\mathcal{M}_u((2D+1)^m)$ using Kronecker's substitution, see [39] and [64, ex. 16.16].

  If the base field k has characteristic zero, this complexity is in $O_{\log}\big(\mathcal{M}_u\big(\binom{D+m}{m}\big)\big)$, i.e. *linear* in the size of the series, up to logarithmic factors; see [42].

  We make the assumption that there exists a universal constant $c < 1$ such that $\mathcal{M}_s(D, m) \leq c\mathcal{M}_s(2D, m)$ holds for all D and m.

With these notations, our first result concerns the existence and the complexity of a parametric resolution:

Theorem 1 *Let $u = \sum u_i x_i$ be a primitive element of $\mathcal{K} \to \mathcal{K}[X_1, \ldots, X_n]/\mathcal{J}_\mathcal{K}$ with coefficients in $\overline{k}$, so that the following relations are satisfied in $\mathcal{K}[X_1, \ldots, X_n]/\mathcal{J}_\mathcal{K}$:*

$$Q_u(u) = 0, \quad \left\{ \begin{array}{rcl} Q'_u(u)x_1 & = & V_1(u), \\ & \vdots & \\ Q'_u(u)x_n & = & V_n(u), \end{array} \right.$$

where

- *the polynomials Q_u and $V_1, \ldots, V_n$ are in $\mathcal{K}[\mathcal{U}]$,*

- *the polynomial Q_u is the monic minimal polynomial of u and the polynomials V_i have degree less than Q_u.*

Then the polynomial Q_u has degree $\deg_\pi$.

We recall that $\mathcal{K}$ is $\overline{k}(P_1, \ldots, P_m)$. Then all numerators and the least common multiple of the denominators of all the coefficients of the polynomials $Q_u, V_1, \ldots, V_n$ have degree in $P_1, \ldots, P_m$ at most $\deg_{\mathcal{V}} \leq d^n$.

Furthermore, if the cardinality of k is greater than $d^n(2d^n + nd + 1)$, then there exists a primitive element $u = \sum u_i x_i$ of $\mathcal{K} \to \mathcal{K}[X_1, \ldots, X_n]/\mathcal{J}_{\mathcal{K}}$ with coefficients in k. In this case, the polynomials $Q_u, V_1, \ldots, V_n$ have their coefficients in the subfield $k(P_1, \ldots, P_m)$ of $\mathcal{K}$.

The second theorem is of algorithmic nature. Its complexity statement is notably given in terms of a degree denoted by $\deg_u$. This degree is defined as *the maximum of the degrees of the coefficients that appear in the parametric resolution for a primitive element u*. Using Theorem 1, $\deg_u$ is bounded by $\deg_{\mathcal{V}}$, and thus by d^n.

Theorem 2 *Assume that the cardinality of k is greater than $d^n(2d^n + nd + 1)$. There exists a probabilistic algorithm which computes a parametric resolution for a primitive element $\sum u_i x_i$ with coefficients in k, through the following steps:*

- *the first step consists in computing a geometric resolution of the simple zeros of the specialized system $\mathbf{f}(\mathbf{p}, .) = 0$, where $\mathbf{p} = (p_1, \ldots, p_m)$ is a point in k^m.*
- *the second step is a formal Newton lifting process, which requires*
$$O_{\log}\big((nL + n^4)\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(4\deg_u, m) + nm^2 \deg_\pi \mathcal{M}_u(\deg_u)\mathcal{M}_s(4\deg_u, m-1)\big)$$
operations in k, where $\deg_u$ is the maximum of the degrees in $P_1, \ldots, P_m$ of the numerators and denominators of the coefficients of the polynomials $Q_u, V_1, \ldots, V_n$.

The algorithm chooses $3m - 1$ values in k, including $\mathbf{p} = (p_1, \ldots, p_m)$; if Γ is a subset of k, and these values are chosen in Γ^{3m-1}, then the algorithm succeeds for all choices except at most $110nd^{4n}|\Gamma|^{3m-2}$, for $d \geq 2$ and $n \geq 2$.

We do not give more details on the first step of this algorithm, the resolution of a zero-dimensional system over k, as efficient solutions are already known (see Section 4.1). We concentrate on the lifting step, which is the most expensive.

Since $\deg_u$ is bounded by d^n, the dependence of our complexity in d is of order $d^{O(nm)}$ base field operations.

Theorem 2 shows that the complexity of the lifting step is *polynomial* in the size of the output. More precisely, using the algorithms for fast univariate polynomial and power series arithmetic mentioned above, we obtain the following corollary. The proof is straightforward, using for instance [42, Lemma 3].

Corollary 1 *If k has characteristic zero, then, in terms of operation in k, the complexity of the lifting step is in*

$$O_{\log}\left((nL + n^4 + nm^2)\deg_\pi \binom{4\deg_u + m}{m}\right).$$

The size of the output is within $O\big(n \deg_\pi \binom{\deg_u + m}{m}\big)$ elements in k. Thus, the complexity of the lifting step is at most quartic in the size of the output.

Organization of the paper.

- In Section 3, we prove Theorem 1, and give estimates the degrees of a degeneracy locus, which will help quantify the probability of success of our algorithm.
- Section 4 presents the most important algorithmic tools we use, a new version of a formal Newton operator and a new algorithm for the reconstruction of a multivariate rational function.
- Section 5 presents the main algorithm, with the proof of its complexity and probability of success. This will prove Theorem 2.
- The algorithm is implemented in Magma [2], on the basis of the `Kronecker` package [28, 40]; the applications we treated and the practical behavior of the implementation are presented in Section 6.

3 Degree estimates for the parametric resolution

In this section, we establish the existence of a parametric resolution and prove the bounds on the degree in $P_1, \ldots, P_m$ of its coefficients. We also give a bound on the degree of a hypersurface in the parameter space which contains the points where a parametric resolution cannot be specialized; this result controls the probability of success of the algorithm given in Section 5.

The organization is as follows. Subsection 3.1 establishes some technical algebraic results, that are used in the sequel. In Subsection 3.2, we prove bounds on the complexity of the *minimal polynomial* of a function of $X_1, \ldots, X_n$. We use this result in Subsection 3.3 to give the proof of Theorem 1. Finally, Subsection 3.4 is devoted to the study of the aforementioned degeneracy hypersurface.

Notations. Throughout this section, we use some additional notations. Let us also write again the definitions of the most important objects used up to now.

- The ideal $\mathcal{I} \subset \overline{k}[P_1, \ldots, P_m, X_1, \ldots, X_n]$ is generated by the polynomials $\mathbf{f}$; $\mathcal{J}$ is its saturation with respect to the jacobian determinant of $\mathbf{f}$. The variety $\mathcal{V}$ is the zero-set of $\mathcal{J}$.
- We recall that $\mathcal{K}$ denotes the field $\overline{k}(P_1, \ldots, P_m)$, and $\mathcal{J}_{\mathcal{K}}$ the extension of the ideal $\mathcal{J}$ in $\mathcal{K}[X_1, \ldots, X_n]$. For the sake of shortness, B denotes the finite-dimensional quotient algebra $\mathcal{K}[X_1, \ldots, X_n]/\mathcal{J}_{\mathcal{K}}$.
- We frequently use the notion of *minimal* and *characteristic polynomial* of elements of B, which we now recall. Let then g be in B, and $\mathcal{U}$ a new variable.

  The *minimal polynomial* of g is the monic generator of the ideal $\{P \in \mathcal{K}[\mathcal{U}], P(g) = 0 \text{ in } B\}$. This polynomial is denoted by Q_g; we will write $Q_g = M_g/D_g$, where M_g is primitive in $\overline{k}[P_1, \ldots, P_m][\mathcal{U}]$, and $D_g \in \overline{k}[P_1, \ldots, P_m]$ is its leading coefficient.

The *characteristic polynomial* of g is the characteristic polynomial of the endomorphism of multiplication by g in B. It denoted by χ_g. We will take $\chi_g = \Xi_g/\Theta_g$, where Ξ_g is primitive in $\overline{k}[P_1, \ldots, P_m][\mathcal{U}]$ and $\Theta_g \in \overline{k}[P_1, \ldots, P_m]$ is its leading coefficient.

- If Q is a polynomial or rational function depending on indeterminates $P_1, \ldots, P_m$ and $\mathbf{p} = (p_1, \ldots, p_m)$ is a point in $\overline{k}^m$, we call *specialization* of Q at $\mathbf{p}$ the polynomial Q with all coefficients specialized at $\mathbf{p}$, if possible. It is denoted by $Q(\mathbf{p})$, or $Q(., \mathbf{p})$.

  We extend naturally this denomination to the *specialization* of a parametric resolution at a point $\mathbf{p}$ in $\overline{k}^m$. We obtain a family of polynomials in $\overline{k}[\mathcal{U}]$.

- The notation $\mathbf{u}$ will denote a n-uple $(u_1, \ldots, u_n)$ in $\overline{k}^n$.

  In Subsection 3.4, we introduce some new variables $\lambda_1, \ldots, \lambda_n$. Then, just as above, a notation such as $\Xi(., \mathbf{u})$ denotes a polynomial, here Ξ, where the variables $(\lambda_1, \ldots, \lambda_n)$ are specialized on the values $(u_1, \ldots, u_n)$.

For the sake of simplicity, all complexity results are stated in terms of the Bézout number d^n. More precise results could be obtained using the product of the degrees of the polynomials $f_1, \ldots, f_n$.

3.1 Preliminaries

Since we make no assumption on the field k, some extra care is required concerning the separability of the extensions we consider; this is the object of the following lemma. As a consequence, we deduce the existence of a primitive element for the extension $\mathcal{K} \to B$.

Lemma 1 *The extension $\mathcal{K} \to B$ is a product of separable field extensions, and has degree* $\deg_\pi$.

Proof. Recall that the ideal $\mathcal{J}$ is the defining ideal of the variety $\mathcal{V}$. Let us write the primary decomposition of $\mathcal{J}$ in $\overline{k}[P_1, \ldots, P_m, X_1, \ldots, X_n]$, $\mathcal{J} = \cap_\ell \mathcal{J}_\ell$, where the sum is taken for indices ℓ in some set $\mathcal{L}$. We now use this decomposition to reduce the proof to the prime case.

For each ℓ, let $\mathcal{J}_{\mathcal{K},\ell}$ be the extension of $\mathcal{J}_\ell$ in $\mathcal{K}[X_1, \ldots, X_n] = \overline{k}(P_1, \ldots, P_m)[X_1, \ldots, X_n]$. Since $\mathcal{J}$ is radical, all ideals $\mathcal{J}_\ell$ are prime. Fact 1 states that the restriction of the projection π to each $\mathcal{V}(\mathcal{J}_\ell)$ is dominant, so the ideals $\mathcal{J}_\ell$ contain no element of $\overline{k}[P_1, \ldots, P_m]$. The extended ideals $\mathcal{J}_{\mathcal{K},\ell}$ then remain prime in $\overline{k}(P_1, \ldots, P_m)[X_1, \ldots, X_n]$. From this, we easily deduce the isomorphism

$$\overline{k}(P_1, \ldots, P_m)[X_1, \ldots, X_n]/\mathcal{J}_{\mathcal{K},\ell} \simeq \mathfrak{fr}\left(\overline{k}[P_1, \ldots, P_m, X_1, \ldots, X_n]/\mathcal{J}_\ell\right),$$

where $\mathfrak{fr}(.)$ denotes the fraction field of an integral ring.

Using Fact 1, we also deduce that the extended ideal $\mathcal{J}_\mathcal{K}$ is the intersection of the extended ideals $\mathcal{J}_{\mathcal{K},\ell}$ for ℓ in $\mathcal{L}$, and that any two distinct extended ideals $\mathcal{J}_{\mathcal{K},\ell}$ and $\mathcal{J}_{\mathcal{K},\ell'}$ are coprime. These results yield the following sequence of isomorphisms:

$$
\begin{aligned}
B &= \overline{k}(P_1,\ldots,P_m)[X_1,\ldots,X_n]/\mathcal{J}_{\mathcal{K}} \\
&\simeq \prod_{\ell\in\mathcal{L}} \overline{k}(P_1,\ldots,P_m)[X_1,\ldots,X_n]/\mathcal{J}_{\mathcal{K},\ell} \\
&\simeq \prod_{\ell\in\mathcal{L}} \mathfrak{fr}\left(\overline{k}[P_1,\ldots,P_m,X_1,\ldots,X_n]/\mathcal{J}_\ell\right).
\end{aligned}
$$

By construction, the Jacobian determinant $\mathbf{jac}(\mathbf{f},\mathbf{X})$ is invertible on a dense subset of each zero-set $\mathcal{V}(\mathcal{J}_\ell)$. Then the Jacobian criterion given in [17, Corollary 16.16] states that each of the field extensions

$$\overline{k}(P_1,\ldots,P_m) \to \mathfrak{fr}\left(\overline{k}[P_1,\ldots,P_m,X_1,\ldots,X_n]/\mathcal{J}_\ell\right)$$

is separable (see [46] for a similar statement). Thus the first assertion of the lemma is proved; we now show that the degree of the extension $\mathcal{K}\to B$ is indeed $\deg_\pi$.

Using the separability condition obtained above, Proposition 1 in [33] shows that for each ℓ the degree of the extension

$$\overline{k}(P_1,\ldots,P_m) \to \mathfrak{fr}\left(\overline{k}[P_1,\ldots,P_m,X_1,\ldots,X_n]/\mathcal{J}_\ell\right)$$

is the generic cardinality of the fibers of π restricted to $\mathcal{V}(\mathcal{J}_\ell)$. Thus the sum of their degrees is $\deg_\pi$. This proves the second point of the lemma. ☐

Corollary 2

- *An element in B is primitive for $\mathcal{K}\to B$ if and only if its characteristic polynomial has no multiple root.*
- *There exists a primitive element of the extension $\mathcal{K}\to B$ of the form $\sum u_i x_i$, with coefficients in $\overline{k}$.*

Proof. An element is primitive for $\mathcal{K}\to B$ if and only if its minimal polynomial equals its characteristic polynomial. Separability implies that the minimal polynomial of an element in B has no multiple root, which proves the first assertion.

The second result is folklore, and follows from both facts that $\mathcal{K}\to B$ is a product of separable field extensions, and that $\overline{k}$ is an infinite subfield of $\mathcal{K}$. See for instance the proof of [13, Theorem 2.1.5], which can be transcripted *verbatim* to the present situation. ☐

3.2 Degree of an eliminating polynomial

We now address our first complexity question: we consider the complexity of the minimal polynomial in B of a element $g\in\overline{k}[X_1,\ldots,X_n]$. The following proposition is an extension of [53, Proposition 1]: in our situation, the presence of denominators in the minimal polynomial of the element g deserves special attention.

Proposition 1 *Let g be a polynomial in $\overline{k}[X_1,\ldots,X_n]$. Then the minimal polynomial $Q_g\in\mathcal{K}[\mathcal{U}]$ of the image of g in B can be written M_g/D_g, where*

- *M_g is primitive in $\overline{k}[P_1, \ldots, P_m][\mathcal{U}]$, and $D_g \in \overline{k}[P_1, \ldots, P_m]$ is its leading coefficient;*
- *seen in $\overline{k}[P_1, \ldots, P_m, \mathcal{U}]$, M_g has total degree at most* $\deg_{\mathcal{V}} \deg g$.

If g belongs to $k[X_1, \ldots, X_n]$, then M_g and D_g may be taken with coefficients in k.

Proof. Let φ be the morphism

$$\begin{array}{ccc} \mathcal{V} & \to & \mathbb{A}^{m+1}(\overline{k}) \\ (\mathbf{p}, \mathbf{x}) & \mapsto & (\mathbf{p}, g(\mathbf{x})). \end{array}$$

The closure $\mathcal{W}$ of its image is an hypersurface in $\mathbb{A}^{m+1}(\overline{k})$ of degree at most $\deg_{\mathcal{V}} \deg g$. We will prove that an equation defining this hypersurface yields the minimal polynomial of g in B.

Let thus M_g in $\overline{k}[P_1, \ldots, P_m, \mathcal{U}]$ be a squarefree polynomial of degree at most $\deg_{\mathcal{V}} \deg g$ defining the hypersurface $\mathcal{W}$. We will consider this polynomial in either $\overline{k}[P_1, \ldots, P_m, \mathcal{U}]$ or $\overline{k}[P_1, \ldots, P_m][\mathcal{U}]$; we let $D_g \in \overline{k}[P_1, \ldots, P_m][\mathcal{U}]$ be the leading coefficient of M_g, when M_g is considered univariate in $\mathcal{U}$.

Let $Q_g \in \mathcal{K}[\mathcal{U}]$ be the monic minimal polynomial of the multiplication by g in B. We first notice that the polynomial Q_g can be written M/D, where M and D respectively belong to $\overline{k}[P_1, \ldots, P_m][\mathcal{U}]$ and $\overline{k}[P_1, \ldots, P_m]$, and M is primitive. Then, we prove that $M = M_g$.

- $M_g(g)$ is identically zero on $\mathcal{V} = \mathcal{V}(\mathcal{J})$. Since $\mathcal{J}$ is radical, $M_g(g)$ belongs to $\mathcal{J}$, so $M_g(g)$ is zero in B. This implies that M_g is a multiple of $Q_g = M/D$ in $\mathcal{K}[\mathcal{U}]$, that is, there exists an equality $aM = bM_g$, where a belongs to $\overline{k}[P_1, \ldots, P_m, \mathcal{U}]$ and b belongs to $\overline{k}[P_1, \ldots, P_m]$. Since M is primitive in $\overline{k}[P_1, \ldots, P_m][\mathcal{U}]$, it divides M_g in $\overline{k}[P_1, \ldots, P_m, \mathcal{U}]$.
- Conversely, $M(g)$ belongs to the ideal $\mathcal{J}_{\mathcal{K}} \cap \overline{k}[P_1, \ldots, P_m, X_1, \ldots, X_n]$. Since no prime component of the ideal $\mathcal{J}$ contains an element in $\overline{k}[P_1, \ldots, P_m]$, this intersection is exactly $\mathcal{J}$. Consequently, $M(g)$ belongs to $\mathcal{J}$, so M vanishes on $\mathcal{W}$, that is M_g divides M in $\overline{k}[P_1, \ldots, P_m, \mathcal{U}]$.

This implies that $M = M_g$ up to a factor in $\overline{k}$, so that $Q_g = M/D = M_g/D_g$.

The algebra B is defined by polynomials with coefficients in k, so if g has its coefficients in k then its minimal polynomial Q_g belongs to $k(P_1, \ldots, P_m)[\mathcal{U}]$, i.e. M and D can be taken with coefficients in k. This proves the proposition. $\square$

Remark 1. The proof shows the following fact: for every $\mathbf{p} = (p_1, \ldots, p_m) \in \overline{k}^m$ which does not cancel the denominator D_g, the polynomial $Q_g(\mathbf{p}, \mathcal{U}) \in \overline{k}[\mathcal{U}]$ vanishes on the values taken by g in the fiber $\pi^{-1}(\mathbf{p}) \cap \mathcal{V}$. We use this remark in Subsection 3.4.

3.3 Degree of a parametric resolution

Using well-known techniques [39, 44, 48, 4], we can recover a parametric resolution through the computation of the minimal polynomial of a "generic primitive element" of $\mathcal{K} \to B$; this minimal polynomial is also called a u-resultant [12] or a Chow form [4]. As a consequence, the degree bound obtained in the previous proposition will apply for the whole resolution.

These results are summarized in the following proposition, which gives the first part of Theorem 1.

Proposition 2 *Let $u = \sum u_i x_i$ be a primitive element of $\mathcal{K} \to B$ with coefficients in $\overline{k}$, so that the following relations are satisfied in B:*

$$Q_u(u) = 0, \quad \begin{cases} Q'_u(u)x_1 &= V_1(u), \\ &\vdots \\ Q'_u(u)x_n &= V_n(u), \end{cases}$$

where

- *the polynomials Q_u and $V_1, \ldots, V_n$ are in $\mathcal{K}[\mathcal{U}]$,*
- *the polynomial Q_u is the monic minimal polynomial of u, the polynomials V_i have degree less than Q_u.*

Then Q_u has degree $\deg_\pi$.

We recall that $\mathcal{K}$ is the field $\overline{k}(P_1, \ldots, P_m)$. Then all numerators and the least common multiple of the denominators of all the coefficients of the polynomials $Q_u, V_1, \ldots, V_n$ have degree at most $\deg_{\mathcal{V}}$.

Furthermore, if u has coefficients in k, then the polynomials $Q_u, V_1, \ldots, V_n$ have their coefficients in the subfield $k(P_1, \ldots, P_m)$ of $\mathcal{K}$.

Before proving the proposition, we mention the following useful consequences. Given a primitive element $u = \sum u_i x_i$, the separability of its minimal polynomial Q_u implies that Q'_u is invertible modulo Q_u, so the parametrization introduced in the above proposition makes sense. Inverting Q'_u modulo Q_u, we can write the alternative parametrization, reminiscent of the Shape Lemma [24]:

$$Q_u(u) = 0, \quad \begin{cases} x_1 &= W_1(u), \\ &\vdots \\ x_n &= W_n(u). \end{cases}$$

Both forms of parametrizations will be used in the sequel, so we give them specific names. Formulae similar to those given in Proposition 2 can be found in Kronecker's work [39], hence the following denomination.

Definition 1 *Let $u = \sum u_i x_i$ be a primitive element of $\mathcal{K} \to B$ with coefficients in $\overline{k}$.*

- *We call* Kronecker parametrization *the vector* $\mathcal{R}_u = [Q_u, V_1, \ldots, V_n]$ *defined in Proposition 2.*

- *We call* Shape Lemma parametrization *the vector* $\mathcal{S}_u = [Q_u, W_1, \ldots, W_n]$ *defined above.*

Proposition 2 could be used to give a bound on the degrees of the coefficients in a Shape Lemma parametrization, at best quadratic in the Bézout number, that is, much worse than the bound for the Kronecker form. Practice reflects this point: introducing the normalization Q'_u has the effect to lower the size of the parametrization obtained through the Shape Lemma, as was already noticed in [4, 50].

Remark 2. If $u = \sum u_i x_i$ is a primitive element of $\mathcal{K} \to B$, and if we denote $\mathrm{U} = \sum u_i X_i$, then the equality between radical ideals

$$\mathcal{J}_{\mathcal{K}} = (Q_u(\mathrm{U}), X_1 - W_1(\mathrm{U}), \ldots, X_n - W_n(\mathrm{U}))$$

holds in $\mathcal{K}[X_1, \ldots, X_n]$. This remark is used in the next subsection.

Proof of Proposition 2: introduction of a generic linear form. We deduce Proposition 2 from the study of the minimal (or characteristic) polynomial of a linear combination of the variables $\mathbf{X}$ with generic coefficients. To this effect, we extend the base field, and correspondingly extend the notations. The objects introduced below will be considered again in the next subsection.

Let $(\lambda_1, \ldots, \lambda_n)$ be new indeterminates, which will be used as coefficients of the generic linear form. We denote by k_Λ the field $k(\lambda_1, \ldots, \lambda_n)$ and proceed to extend all previous constructions to this new base field; they will be denoted by a subscript Λ. Since no confusion can occur, we still use the letters $\mathbf{P}, \mathbf{X}$ for indeterminates.

Thus, we denote by $\mathcal{I}_\Lambda$ the ideal generated in $\overline{k_\Lambda}[P_1, \ldots, P_m, X_1, \ldots, X_n]$ by the polynomials $\mathbf{f} = f_1, \ldots, f_n$, and by $\mathcal{J}_\Lambda$ its saturation with respect to the Jacobian determinant $\mathbf{jac}(\mathbf{f}, \mathbf{X})$. The zero-set of $\mathcal{J}_\Lambda$ is denoted by $\mathcal{V}_\Lambda$. It is a routine check that $\mathcal{J}_\Lambda$ is the extension of $\mathcal{J}$ in $\overline{k_\Lambda}[P_1, \ldots, P_m, X_1, \ldots, X_n]$; using the definition of degree from [33], we deduce that the degree of $\mathcal{V}_\Lambda$ equals the degree of $\mathcal{V}$.

We denote by $\mathcal{K}_\Lambda$ the field $\overline{k_\Lambda}(P_1, \ldots, P_m)$, which is the analogous to the field $\mathcal{K}$ used up to now. Similarly, $\mathcal{J}_{\mathcal{K},\Lambda}$ denotes the ideal generated in $\mathcal{K}_\Lambda[X_1, \ldots, X_n]$ by the polynomials in $\mathcal{J}_\Lambda$, B_Λ is the quotient $\mathcal{K}_\Lambda[X_1, \ldots, X_n]/\mathcal{J}_{\mathcal{K},\Lambda}$, and x_i is the image of X_i in B_Λ.

Up to now, the variables $\lambda_1, \ldots, \lambda_n$ have played no active role. We now denote by U_Λ the generic linear form $\sum \lambda_i X_i$, and by $u_\Lambda = \sum \lambda_i x_i$ its image in B_Λ. Given a new indeterminate $\mathcal{U}_\Lambda$, we denote by $\chi_\Lambda \in \mathcal{K}_\Lambda[\mathcal{U}_\Lambda]$ the characteristic polynomial of u_Λ in B_Λ.

The polynomial χ_Λ is the eliminating polynomial for a generic linear form we wanted to introduce. We now present its basic properties, and see how to use it for obtaining a parametric resolution.

Lemma 2 *For any* $\mathbf{u} = (u_1, \ldots, u_n)$ *in* $\overline{k}^n$*, the characteristic polynomial of* $\sum u_i x_i$ *in* B *is the specialization* $\chi_\Lambda(., \mathbf{u})$*.*

Proof. Any $\mathcal{K}$-basis of B is also a $\mathcal{K}_\Lambda$-basis of B_Λ. Consequently, the polynomial χ_Λ is the determinant of $\mathcal{U}_\Lambda \mathbf{I} - \sum \lambda_i \mathbf{M}_{x_i}$, where $\mathbf{M}_{x_i}$ is the matrix of multiplication by x_i in such a basis, and $\mathbf{I}$ is the identity matrix. This proves the lemma. $\square$

Lemma 3 χ_Λ *is an homogeneous polynomial of degree* $\deg_\pi$ *in* $(\mathcal{U}_\Lambda, \lambda_1, \ldots, \lambda_n)$*, monic in* $\mathcal{U}_\Lambda$*. It can be written* $\chi_\Lambda = \Xi_\Lambda / \Theta_\Lambda$*, where* Ξ_Λ *belongs to* $k[P_1, \ldots, P_m, \lambda_1, \ldots, \lambda_n][\mathcal{U}_\Lambda]$*,* Θ_Λ *belongs to* $k[P_1, \ldots, P_m]$*, both polynomials have degree in* $(P_1, \ldots, P_m)$ *bounded by* $\deg_\mathcal{V}$*, and* Θ_Λ *is the leading coefficient of* Ξ_Λ*.*

Proof. The first point is an easy consequence of the proof of the previous lemma, so we concentrate on the second assertion.

By Corollary 2, there exists a primitive element $u = \sum u_i x_i$ of $\mathcal{K} \to B$ with coefficients in $\overline{k}$. Then, also by Corollary 2, its characteristic polynomial χ_u has no multiple root. Using the specialization property of the previous lemma, this shows that the polynomial χ_Λ cannot have multiple roots. Thus it coincides with the minimal polynomial of u_Λ. We can then apply Proposition 1 to the variety $\mathcal{V}_\Lambda$ defined over the field k_Λ to conclude the proof of the lemma. $\square$

Concluding the proof. The polynomial $\chi_\Lambda(\mathrm{U}_\Lambda)$ belongs to the ideal $\mathcal{J}_{\mathcal{K},\Lambda}$, so it can be written $\sum g_j F_j$, where (F_j) are generators of $\mathcal{J}$ in $k[P_1, \ldots, P_m, X_1, \ldots, X_n]$ and (g_j) are polynomials in $\mathcal{K}_\Lambda[X_1, \ldots, X_n]$. Since χ_Λ is a polynomial in $(\lambda_1, \ldots, \lambda_n)$, the polynomials g_j can be taken polynomial in $(\lambda_1, \ldots, \lambda_n)$ too. The derivative of $\chi_\Lambda(\mathrm{U}_\Lambda)$ with respect to λ_i is $\sum \frac{\partial g_j}{\partial \lambda_i} F_j$; it can also be written $\left(\frac{\partial \chi_\Lambda}{\partial \mathcal{U}_\Lambda} X_i + \frac{\partial \chi_\Lambda}{\partial \lambda_i}\right)(\mathrm{U}_\Lambda)$.

Since u is primitive, its minimal polynomial Q_u coincides with its characteristic polynomial χ_u. Lemma 2 then shows that the specialization $(\lambda_1, \ldots, \lambda_n) \leftarrow (u_1, \ldots, u_n)$ in χ_Λ and $\frac{\partial \chi_\Lambda}{\partial \mathcal{U}_\Lambda}$ are Q_u and Q'_u. We take for V_i the specialization of $-\frac{\partial \chi_\Lambda}{\partial \lambda_i}$ and let U be $\sum u_i X_i$. Since the polynomials $\frac{\partial g_j}{\partial \lambda_i}$ are polynomial in the variables $\lambda_1, \ldots, \lambda_n$, the specialization $(\lambda_1, \ldots, \lambda_n) \leftarrow (u_1, \ldots, u_n)$ shows that $\big(Q'_u X_i - V_i\big)(\mathrm{U})$ belongs to $\mathcal{J}_\mathcal{K}$, so vanishes in B.

We have thus obtained a parametrization. Let us prove that is has the announced degree properties. This will conclude the complexity analysis: the conditions given in Proposition 2 obviously impose uniqueness for $V_1, \ldots, V_n$.

First, note that Lemma 3 gives the bound on the degree in $\mathcal{U}_\Lambda$ of χ_Λ and its derivatives.

The polynomial χ_Λ is polynomial in $(\lambda_1, \ldots, \lambda_n)$, so differentiation with respect to λ_i does not alter the degrees of the rational functions in $(P_1, \ldots, P_m)$ that appear. Thus, all numerators in $Q_u, V_1, \ldots, V_n$ have degree at most $\deg_\mathcal{V}$ by Lemma 3. Moreover, all denominators of the coefficients of the polynomials $Q_u, V_1, \ldots, V_n$ divide the denominator of χ_Λ, which is Θ_Λ, so they have degree at most $\deg_\mathcal{V}$ by Lemma 3 again. Thus the complexity analysis is complete.

We conclude the proof by a trivial remark: if the coefficients $(u_1, \ldots, u_n)$ are in the base field k, our construction shows that $Q_u, V_1, \ldots, V_n$ have coefficients in k too. $\square$

3.4 Lucky specializations

A parametric resolution can be specialized on an open subset of the parameter space $\mathbb{A}^m(\overline{k})$, to give a description of the simple solutions of the corresponding specialized system. In this section, we define a universal *discriminant locus* describing the values where the specialization fails, and give a bound on its degree. This bound will be used to control some error probabilities, so it is given in terms of the input data (n, d).

It will be useful to consider both forms of parametrization introduced in the previous subsection, the Kronecker form $\mathcal{R}_u$ and the Shape Lemma form $\mathcal{S}_u$.

Proposition 3 *There exists a non-zero polynomial Δ in $k[P_1, \ldots, P_m, \lambda_1, \ldots, \lambda_n]$ of degree at most $d^n(2d^n + nd + 1)$ in $(P_1, \ldots, P_m)$ and $2d^{2n}$ in $(\lambda_1, \ldots, \lambda_n)$ such that:*

- *for all $\mathbf{p}$ in $\overline{k}^m$ and $\mathbf{u} = (u_1, \ldots, u_n)$ in $\overline{k}^n$, if $\Delta(\mathbf{p}, \mathbf{u})$ is not zero, then $u = \sum u_i x_i$ is a primitive element of $\mathcal{K} \to B$ and $\mathbf{p}$ cancels none of the denominators in either $\mathcal{R}_u$ or $\mathcal{S}_u$. Furthermore, the system $\mathbf{f}(\mathbf{p}, .) = 0$ has $\deg_\pi$ simple solutions, which are described by the specialization of either $\mathcal{R}_u$ or $\mathcal{S}_u$ at $\mathbf{p}$.*

- *for all $\mathbf{p}$ in $\overline{k}^m$, if $\Delta(\mathbf{p}, .)$ is not zero, and $\mathrm{U} = \sum u_i X_i$ is a linear form that induces a primitive element for the extension corresponding to the simple solutions of the specialized system $\mathbf{f}(\mathbf{p}, .) = 0$, then, taking $\mathbf{u} = (u_1, \ldots, u_n)$, $\Delta(\mathbf{p}, \mathbf{u})$ is not zero, so the same conclusion holds.*

Before proving the proposition, we consider its following consequence. If the cardinality of k is greater than $2d^n(2d^n + nd + 1)$, then there exists a value $(\mathbf{p}, \mathbf{u})$ in k^{m+n} which does not cancel Δ. Then the corresponding element $u = \sum u_i x_i$ is a primitive element of $\mathcal{K} \to B$. This concludes the proof of Theorem 1.

Proof of Proposition 3. We consider again the variables $\lambda_1, \ldots, \lambda_n$, and the polynomials χ_Λ, Ξ_Λ and Θ_Λ introduced in the end of the previous subsection, notably Lemma 3.

Let R_Λ be the resultant of Ξ_Λ and Ξ'_Λ, which is a polynomial in $k[P_1, \ldots, P_m, \lambda_1, \ldots, \lambda_n]$. From the proof of Lemma 3, we see that this polynomial is non-zero. The bounds given in Lemma 3 show that R_Λ has degree at most $2 \deg_\pi \deg_\mathcal{V} \le 2d^{2n}$ in $(P_1, \ldots, P_m)$ and $2 \deg_\pi^2 \le 2d^{2n}$ in $(\lambda_1, \ldots, \lambda_n)$. We now show that this polynomial controls the denominators appearing in a parametric resolution, in either Kronecker or Shape Lemma form.

We recall that the characteristic polynomial of an element u in B is written $\chi_u = \Xi_u/\Theta_u$, where Ξ_u is primitive in $\overline{k}[P_1, \ldots, P_m][\mathcal{U}]$ and $\Theta_u \in \overline{k}[P_1, \ldots, P_m]$ is its leading coefficient.

Lemma 4 *For any $\mathbf{u} = (u_1, \ldots, u_n)$ in $\overline{k}^n$, the resultant of Ξ_u and Ξ'_u divides $R_\Lambda(., \mathbf{u})$. If $u = \sum u_i x_i$ is a primitive element of $\mathcal{K} \to B$, the numerator of the discriminant of Q_u divides $R_\Lambda(., \mathbf{u})$.*

Proof. Lemma 2 shows that the characteristic polynomial $\chi_u = \Xi_u/\Theta_u$ is equal to the specialization $\Xi_\Lambda(., \mathbf{u})/\Theta_\Lambda$. Since Ξ_u is primitive, it divides $\Xi_\Lambda(., \mathbf{u})$, the possible factor lying in $\overline{k}[P_1, \ldots, P_m]$. This implies that the resultant of Ξ_u and Ξ'_u divides the resultant of $\Xi_\Lambda(., \mathbf{u})$

and $\Xi_\Lambda(.,\mathbf{u})'$. Since by construction the leading term of Ξ_Λ does not depend on $(\lambda_1,\ldots,\lambda_n)$, this resultant is the specialization $R_\Lambda(.,\mathbf{u})$. This proves the first point.

If u is a primitive element of $\mathcal{K} \to B$, its minimal polynomial Q_u coincides with its characteristic polynomial Ξ_u/Θ_u. The numerator of the discriminant of Q_u then divides the resultant of Ξ_u and Ξ_u', which proves the second point. $\square$

Lemma 5 *Let $\mathbf{u} = (u_1,\ldots,u_n)$ be in $\overline{k}^n$. If $u = \sum u_i x_i$ is a primitive element of $\mathcal{K} \to B$, then all the denominators in $\mathcal{R}_u$ and $\mathcal{S}_u$ divide $\Theta_\Lambda R_\Lambda(.,\mathbf{u})$.*

Proof. The proof of Proposition 2 shows that all denominators appearing in $\mathcal{R}_u$ divide Θ_Λ, which proves the assertion for $\mathcal{R}_u$. Going from the representation $\mathcal{R}_u$ to the representation $\mathcal{S}_u$ requires to invert Q_u' modulo Q_u. The denominators that appear in the inversion divide the numerator of the discriminant of Q_u and Q_u', so they divide $R_\Lambda(.,\mathbf{u})$ by the lemma above. This proves the result. $\square$

Concluding the proof. It remains to exclude the possible degenerate points of $\mathcal{V}$. The Jacobian determinant $\mathbf{jac}(\mathbf{f},\mathbf{X})$ has degree at most nd. The intersection of its zero-set with $\mathcal{V}$ is a variety of degree at most $nd\deg_{\mathcal{V}} \le nd^{n+1}$, whose image by π is contained in an hypersurface of $\mathbb{A}^m(\overline{k})$. Let S by a polynomial in $k[P_1,\ldots,P_m]$ of degree at most nd^{n+1} defining such an hypersurface.

We define Δ as the product $S\Theta_\Lambda R_\Lambda$, which has the requested degree in $(P_1,\ldots,P_m)$ and $(\lambda_1,\ldots,\lambda_n)$. We now prove that Δ fulfills our requirements.

- Let $(\mathbf{p},\mathbf{u})$ be a $(m+n)$-uple in $\overline{k}^{m+n}$ which does not cancel Δ, and u the linear form $\sum u_i x_i$.

  We first briefly describe the fiber $\pi^{-1}(\mathbf{p}) \cap \mathcal{V}$. Since $\mathbf{p}$ does not cancel Δ, the Jacobian determinant of $\mathbf{f}$ vanishes on none of the points in the fiber $\pi^{-1}(\mathbf{p}) \cap \mathcal{V} \subset \mathcal{V}(\mathbf{f})$. Then the Jacobian criterion shows that these points are in finite number. By [33, Proposition 1], this number is at most $\deg_\pi$.

  We now turn to the specialization of the parametric resolution. Lemma 4 shows that the resultant of Ξ_u and Ξ_u', and thus the discriminant of the characteristic polynomial χ_u, cannot be zero, so by Corollary 2, u is a primitive element of $\mathcal{K} \to B$. Lemma 5 then shows that $\mathbf{p}$ cancels none of the denominators in the corresponding resolutions $\mathcal{R}_u$ and $\mathcal{S}_u$.

  Since the numerator of the discriminant of the polynomial $Q_u(\mathbf{p}) \in \overline{k}[\mathcal{U}]$ is not zero, $Q_u(\mathbf{p})$ has $\deg_\pi$ distinct roots. Consequently, the specialization of either $\mathcal{R}_u$ or $\mathcal{S}_u$ at $\mathbf{p}$ describes $\deg_\pi$ distinct points.

  Let f be a polynomial in $\mathcal{J}$. From Remark 2, there exist polynomials $(g_1,\ldots,g_{n+1})$ in $\mathcal{K}[X_1,\ldots,X_n]$ such that $f = \sum g_i(X_i - W_i(\mathrm{U})) + g_{n+1}Q_u(\mathrm{U})$, where $\mathrm{U} = \sum u_i X_i$. The rewriting process introduces no new denominator; since $\mathbf{p}$ cancels none of the denominators in $\mathcal{S}_u$, it cancels none of the denominators in this equality. Consequently, the $\deg_\pi$ points described by the specialization of $\mathcal{S}_u$ at $\mathbf{p}$ cancel the polynomial $f(\mathbf{p}, .)$.

Thus, these points are included in the fiber $\pi^{-1}(\mathbf{p}) \cap \mathcal{V}$. Using the above upper bound on the cardinality of this fiber, we obtain the first part of the proposition.

- Let now $\mathbf{p}$ be in $\overline{k}^m$, and assume that $\Delta(\mathbf{p}, .)$ is not zero. There exists $\mathbf{u}' = (u'_1, \dots, u'_n)$ in $\overline{k}^n$ which does not cancel this polynomial, so the previous point shows that the specialized system $\mathbf{f}(\mathbf{p}, .) = 0$ admits $\deg_\pi$ simple solutions.

  Take now $\mathrm{U} = \sum u_i X_i$ any linear form inducing a primitive element for the extension of $\overline{k}$ generated by the simple solutions of this system. Then U takes $\deg_\pi$ distinct values on these points.

  We denote by $\Xi_\Lambda(\mathbf{p}, \mathbf{u}) \in \overline{k}[\mathcal{U}]$ the polynomial Ξ_Λ whose coefficients are specialized at $(\mathbf{p}, \mathbf{u})$. Since $\Theta_\Lambda(\mathbf{p})$ is not zero, $\Xi_\Lambda(\mathbf{p}, \mathbf{u})$ has full degree $\deg_\pi$ in its leading variable $\mathcal{U}$, so the resultant of $\Xi_\Lambda(\mathbf{p}, \mathbf{u})$ with its derivative is the specialization of the generic resultant R_Λ at $(\mathbf{p}, \mathbf{u})$. Remark 1 shows that $\Xi_u(\mathbf{p})$ vanishes on the $\deg_\pi$ distinct values taken by U, and Lemma 2 shows that it is also the case for $\Xi_\Lambda(\mathbf{p}, \mathbf{u})$. Consequently, the resultant $R_\Lambda(\mathbf{p}, \mathbf{u})$ is not zero. This concludes the proof. $\square$

4 Outlook of the algorithm

Our purpose is now to compute a parametric resolution. To this effect, we propose the following algorithm, reminiscent of both numerical root-finding techniques and Hensel lifting methods.

1. **Initial estimation:** given $\mathbf{p} = (p_1, \dots, p_m)$ in k^m, compute a geometric resolution of the simple roots of the specialized system $\mathbf{f}(\mathbf{p}, .) = 0$.

2. **Approximation:** starting from this specialized solution, approximate the coefficients of the corresponding parametric resolution in a ring of formal power series.

3. **Reconstruction:** recover the coefficients of the parametric resolution from their power series expansion at $(p_1, \dots, p_m)$.

The core of the main algorithm is given in the next section. Here, in the following subsections, we detail our solutions to the three points above: the resolution of the specialized system, a formal Newton operator, and the reconstruction of a rational function from its power series expansion. These parts are largely independent.

It will be useful to recall the following complexity notations:

- $\mathcal{M}_u(D)$ denotes the cost of the multiplication of univariate polynomials of degree D.

- $\mathcal{M}_s(D, m)$ denotes the cost of m-variate series multiplication at precision D.

4.1 Computing the initial resolution

Given a point $\mathbf{p}$ in k^m, the first task is to compute a geometric resolution of the simple solutions of the specialized system $\mathbf{f}(\mathbf{p}, .) = 0$. Such a process will be denoted $\texttt{Resolution}(\mathbf{f}, \mathbf{p})$. In our main algorithm, its output will be denoted $[\mathbf{u}, \mathcal{R}_u^0]$. In this case:

- $\mathbf{u} = (u_1, \ldots, u_n)$ is such that $\sum u_i X_i$ induces a primitive element for the simple solutions of the system $\mathbf{f}(\mathbf{p}, .) = 0$
- $\mathcal{R}_u^0$ is a vector of polynomials $[q_u, v_1, \ldots, v_n]$ in $k[\mathcal{U}]$, forming a geometric resolution for these points.

The superscript 0 in $\mathcal{R}_u^0$ indicates that this resolution is thought as the truncation of a generic resolution at precision 0 around $(p_1, \ldots, p_m)$.

Several tools are available to compute this initial resolution. In the spirit of the present paper, we mention in particular the algorithm of geometric resolution, initially in [26], see also [27, 25]. A simplified and improved version is given in [28], together with the description of its Magma implementation, called `Kronecker` [40].

This algorithm applies in the same model as ours: the input system is given by a Straight-Line Program of size L. Its complexity depends on a geometric quantity attached to the system, called δ, which is at most d^n. With this notation, Theorem 1 in [28] states that the resolution can be computed within $O\big((nL + n^4)\mathcal{M}_u(d\delta)^2\big)$ operations in k. The algorithm is of probabilistic nature, and a probability analysis is done for a similar algorithm in [35].

Let us mention other approaches to this question, which were already presented in the introduction. Popular methods rely on Gröbner bases computations [21, 20], either for a lexicographic ordering, or followed by the computation of a Rational Univariate Representation [50]. Other approaches include the computation of u-resultants by means of linear algebra methods, based on generalizations of Sylvester or Bézout matrices [47, 49].

4.2 Lifting the resolution

Knowing the initial estimate, the successive approximations of the parametric resolution are obtained through a formal Newton approximation process. It consists in computing a sequence of resolutions, whose coefficients are the successive *Taylor series expansions* of the coefficients of the requested parametric resolution. This subsection is devoted to present the details of this Newton lifting operator, and the complexity of an elementary lifting step.

We first present the method in a general setting: we consider the lifting modulo the powers of any ideal of a given coefficient ring. In a second time, we apply this result to our specific problem, where the lifting is done modulo the powers of the maximal ideal of a m-variate power series ring.

Just as the numerical Newton operator doubles the number of digits of accuracy at each step, the formal version doubles the precision of the power series at each step. Thus, the series we compute have successive precisions $1, 2, \ldots, 2^\kappa, \ldots$

Proposition 5 below gives the complexity of the basic step of this operator: using the complexity notations given in the introduction, lifting the Taylor series from precision 2^κ to precision $2^{\kappa+1}$ requires

$$O\big((nL + n^4)\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(2^{\kappa+1}, m)\big)$$

base field operations. In characteristic zero, using fast arithmetic, this complexity is linear, up to logarithmic factors, in the size of the output.

Our use of the formal Newton operator is in the continuity of notably [27, 26, 25, 28, 34, 35]. In particular, a ready-to-implement formal Newton operator was given in the article [28]. Our method generalizes this algorithm to a wider class of representations, *triangular sets representations*. We do not use the full generality of this method here; this is the subject of [59]. Yet, we stress the fact that the presentation of the computations has now become both more general and simpler.

Generalist presentation. We temporarily broaden our framework: we consider a commutative ring with unity $\mathcal{A}$, an ideal $\mathcal{I}$ of $\mathcal{A}$ and some polynomials $\mathbf{F} = (F_1, \ldots, F_N)$ in $\mathcal{A}[X_1, \ldots, X_N]$. We will describe how to approximate some "solutions" of the system $\mathbf{F}$ modulo the powers of $\mathcal{I}$.

To this effect, let $\mathbf{t} = (t_1, \ldots, t_N)$ be polynomials in $\mathcal{A}[X_1, \ldots, X_N]$. We suppose that $\mathbf{t}$ forms what will be called a *triangular set*: for each j, the polynomial t_j is *monic* in X_j, reduced with respect to $(t_{j+1}, \ldots, t_N)$, and depends only on the variables $X_j, \ldots, X_N$.

This triangular set is meant to represent some solutions of the system $\mathbf{F}$ without multiplicities, in the sense that:

- (H1) there exists a $N \times N$ matrix $\mathbf{A}$ with entries in $\mathcal{A}[X_1, \ldots, X_N]$ such that the equality $\mathbf{F} = \mathbf{A}\mathbf{t}$ holds;
- (H2) the Jacobian determinant $\mathbf{jac}(\mathbf{F})$ is invertible in $\mathcal{A}[X_1, \ldots, X_N]/(\mathcal{I}, t_1, \ldots, t_N)$.

For any positive integer κ, we denote $(t_1^\kappa, \ldots, t_N^\kappa)$ the images of the polynomials $(t_1, \ldots, t_N)$ in $\mathcal{A}/\mathcal{I}^{2^\kappa}[X_1, \ldots, X_N]$; these images are the successive approximations of $(t_1, \ldots, t_N)$ we are interested in.

Let κ be a fixed positive integer. We suppose that $(t_1^\kappa, \ldots, t_N^\kappa)$ are known, and propose an algorithm to compute the new approximations $(t_1^{\kappa+1}, \ldots, t_N^{\kappa+1})$ in $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1, \ldots, X_N]$. This algorithm is based on Proposition 4 below; it finally amounts to linear algebra operations in a suitable quotient ring.

As input, we take any triangular set $\mathbf{T}_\kappa = (T_1^\kappa, \ldots, T_N^\kappa)$ of polynomials in $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1, \ldots, X_N]$ such that:

- (H3) $T_j^\kappa = t_j^\kappa$ modulo $\mathcal{I}^{2^\kappa}\,\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1, \ldots, X_N]$, for j in $1, \ldots, N$.

Stating the proper sequence of computations requires some new notations.

- We denote by H_κ the quotient $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1,\ldots,X_N]/(T_1^\kappa,\ldots,T_N^\kappa)$. The canonical image of any $\alpha \in \mathcal{A}[X_1,\ldots,X_N]$ in H_κ is denoted by α_κ; similar notations hold for vector or matrices of polynomials.

- $\mathbf{Jac}(\mathbf{F})$ and $\mathbf{jac}(\mathbf{F})$ respectively denote the jacobian matrix of the system $\mathbf{F}$ and its determinant; $\mathbf{Jac}(\mathbf{t})$ denotes the jacobian matrix of $\mathbf{t}$. Similar notation with subscript κ denotes their images in the matrix algebra over H_κ, and $\mathbf{Jac}(\mathbf{T}_\kappa)$ denotes the jacobian matrix of $\mathbf{T}_\kappa$. The identity matrix is denoted by $\mathbf{I}$. $\mathbf{F}_\kappa$ denotes the reduction of the vector of polynomials $\mathbf{F}$ in H_κ.

- Since $\mathbf{T}_\kappa$ is a triangular set, the quotient H_κ is a free $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}$-module, which admits for a basis the set of monomials

$$\{X_1^{\alpha_1}\ldots X_N^{\alpha_N},\ 0 \le \alpha_j < \deg_{X_j} T_j^\kappa\}.$$

  This canonical basis enables to assign to any element h in H_κ a canonical preimage in $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1,\ldots,X_N]$, denoted by $\widetilde{h}$.

With these notations, the following proposition gives the formula for computing the next approximations $(t_1^{\kappa+1},\ldots,t_N^{\kappa+1})$.

Proposition 4 *The Jacobian matrix* $\mathbf{Jac}(\mathbf{F}_\kappa)$ *is invertible. Let* $\delta_\kappa = (\delta_1^\kappa,\ldots,\delta_N^\kappa)$ *be the product* $\mathbf{Jac}(\mathbf{T}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa$*. Then, for all* j *in* $1,\ldots,N$*, the equality* $t_j^{\kappa+1} = T_j^\kappa + \widetilde{\delta_j^\kappa}$ *holds in* $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1,\ldots,X_N]$.

Proof. The Jacobian determinant $\mathbf{jac}(\mathbf{F})$ is invertible in $\mathcal{A}[X_1,\ldots,X_N]/(\mathcal{I},t_1,\ldots,t_N)$, so by Hensel's Lemma its image is invertible in the quotient $h_\kappa = \mathcal{A}[X_1,\ldots,X_N]/(\mathcal{I}^{2^\kappa},t_1,\ldots,t_N)$. It is straightforward to check that $h_\kappa \simeq H_\kappa/\mathcal{I}^{2^\kappa}H_\kappa$, so another application of Hensel's Lemma shows that $\mathbf{jac}(\mathbf{F})$ is invertible in $H_\kappa/\mathcal{I}^{2^{\kappa+1}}H_\kappa$. We note that $\mathcal{I}^{2^{\kappa+1}}H_\kappa = 0$, so the previous quotient is H_κ. This proves the first point.

The second point is proven through the following explicit computations.

The equality $\mathbf{F} = \mathbf{A}\mathbf{t}$ implies that the Jacobian matrix $\mathbf{Jac}(\mathbf{F})$ is equal to $\mathbf{A}\mathbf{Jac}(\mathbf{t})+\mathbf{B}$, where all entries in the matrix $\mathbf{B}$ belong to the ideal $(t_1,\ldots,t_N)$. The polynomials T_j^κ are chosen such that the images of the polynomials $\mathbf{t}$ in H_κ belong to the ideal $\mathcal{I}^{2^\kappa}H_\kappa$. Consequently, in the relation $\mathbf{Jac}(\mathbf{F}_\kappa) = \mathbf{A}_\kappa\mathbf{Jac}(\mathbf{t}_\kappa) + \mathbf{B}_\kappa$ over H_κ, all entries of $\mathbf{B}_\kappa$ belong to $\mathcal{I}^{2^\kappa}H_\kappa$.

This formula implies that $\mathbf{Jac}(\mathbf{t}_\kappa)$ is invertible over $H_\kappa/\mathcal{I}^{2^\kappa}H_\kappa$ and so, by a new application of Hensel's lemma, over H_κ as well. Consequently, the equality

$$\mathbf{I} = \mathbf{Jac}(\mathbf{t}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{A}_\kappa + \mathbf{Jac}(\mathbf{t}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{B}_\kappa\mathbf{Jac}(\mathbf{t}_\kappa)^{-1}$$

holds, which can be rewritten

$$\mathbf{Jac}(\mathbf{t}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{A}_\kappa = \mathbf{I} + \mathbf{C}_\kappa,$$

where the entries of $\mathbf{C}_\kappa$ belong to $\mathcal{I}^{2^\kappa}H_\kappa$. We then deduce the series of equalities

$$\mathbf{Jac}(\mathbf{t}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa = \mathbf{Jac}(\mathbf{t}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{A}_\kappa\mathbf{t}_\kappa = \mathbf{t}_\kappa + \mathbf{C}_\kappa\mathbf{t}_\kappa = \mathbf{t}_\kappa,$$

since all entries in $\mathbf{t}_\kappa$ and $\mathbf{C}_\kappa$ belong to $\mathcal{I}^{2^\kappa} H_\kappa$, and $\mathcal{I}^{2^{\kappa+1}} H_\kappa = 0$.

In a similar way, the entries in the matrix $\mathbf{Jac}(\mathbf{t}_\kappa)$ differ from the entries in $\mathbf{Jac}(\mathbf{T}_\kappa)$ by elements in $\mathcal{I}^{2^\kappa} H_\kappa$. Since $\mathbf{F}_\kappa$ is in $\mathcal{I}^{2^\kappa} H_\kappa$, this implies the equality over H_κ:

$$\mathbf{Jac}(\mathbf{T}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa = \mathbf{Jac}(\mathbf{t}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa = \mathbf{t}_\kappa. \tag{1}$$

Let δ_κ be the vector $\mathbf{Jac}(\mathbf{T}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa$, computed over H_κ, and $\widetilde{\delta_\kappa}$ the vector of the canonical preimages in $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1, \ldots, X_N]$ of its entries.

Equation (1) means that $\widetilde{\delta_j^\kappa} - t_j^{\kappa+1}$ belongs to $(T_1^\kappa, \ldots, T_N^\kappa)$. Consequently, $\widetilde{\delta_j^\kappa} - t_j^{\kappa+1} + T_j^\kappa$ also belongs to this ideal, and has partial degree in every X_k less than $\deg_{X_k} T_k^\kappa$. Since $(T_1^\kappa, \ldots, T_N^\kappa)$ forms a triangular set, this implies that $\widetilde{\delta_j^\kappa} - t_j^{\kappa+1} + T_j^\kappa$ is zero. This concludes the proof. $\square$

Algorithm `Lift`. The previous proposition is turned into the following procedure `Lift` in a straightforward way; the notations used in this algorithm are the same as in the previous paragraph.

Symbolic Newton lifting

Procedure **Lift**$(\mathbf{F}, \mathbf{T})$
Input: the system $\mathbf{F}$, a triangular set $\mathbf{T} = (T_1^\kappa, \ldots, T_N^\kappa)$, which satisfy hypotheses (H1), (H2) and (H3).
Output: the polynomials $(t_1, \ldots, t_N)$ modulo $\mathcal{I}^{2^{\kappa+1}}$.

\# The computations are done over $\mathcal{A}/\mathcal{I}^{2^{\kappa+1}}[X_1, \ldots, X_N]/(T_1^\kappa, \ldots, T_N^\kappa)$
$\mathbf{Jac}(\mathbf{F}_\kappa) \leftarrow$ `JacobianMatrix`$(\mathbf{F}_\kappa)$;
$\mathbf{Jac}(\mathbf{F}_\kappa)^{-1} \leftarrow$ `Inverse`$(\mathbf{Jac}(\mathbf{F}_\kappa))$;
$\mathbf{Jac}(\mathbf{T}_\kappa) \leftarrow$ `JacobianMatrix`$(\mathbf{T}_\kappa)$;
$\delta_\kappa \leftarrow \mathbf{Jac}(\mathbf{T}_\kappa)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa$;
`return` $(T_1^\kappa + \widetilde{\delta_1^\kappa}, \ldots, T_N^\kappa + \widetilde{\delta_N^\kappa})$;

Application to parametric geometric resolutions. To conclude this subsection, we present the application of this method to our problem of parametric resolutions. The notations are those used in the rest of this paper.

Let $\mathbf{p}$ be a point in k^m, and $u = \sum u_i x_i$ a primitive element of $\mathcal{K} \to \mathcal{K}[X_1, \ldots, X_n]/\mathcal{J}_\mathcal{K}$. We consider the Shape Lemma parametrization $\mathcal{S}_u = [Q_u, W_1, \ldots, W_n]$ defined in Section 3.3 and suppose that $\mathbf{p}$ cancels no denominator in $\mathcal{S}_u$. In this case, we denote by $\mathcal{S}_u^\kappa = [Q_u^\kappa, W_1^\kappa, \ldots, W_n^\kappa]$ the vector $\mathcal{S}_u$, where all coefficients are replaced by their Taylor expansion at $\mathbf{p}$ at precision 2^κ.

The key point is that a resolution under Shape Lemma form is a particular form of triangular set. Then Proposition 4 enables us to compute $\mathcal{S}_u^{\kappa+1}$ from $\mathcal{S}_u^{\kappa}$. The idea is that computing Taylor expansions at $\mathbf{p}$ amounts to compute modulo the powers of the maximal ideal of the m-variate power series ring centered at $\mathbf{p}$.

The proposition below justifies this assertion, and estimates the complexity of the process.

From the proof of this proposition, we deduce that computing the new approximation $\mathcal{S}_u^{\kappa+1}$ amounts to calling the procedure `Lift` defined above, with arguments $(f_1, \ldots, f_n, X_{n+1} - \sum u_i X_i)$ and $(X_1 - W_1^\kappa(X_{n+1}), \ldots, X_n - W_n^\kappa(X_{n+1}), Q_u^\kappa(X_{n+1}))$. We will call $\mathtt{Lift}(\mathbf{f}, \mathcal{S}_u^\kappa, u)$ this process; its output is $\mathcal{S}_u^{\kappa+1}$.

Proposition 5 *Let $u = \sum u_i x_i$ be a primitive element of $\mathcal{K} \to \mathcal{K}[X_1, \ldots, X_n]/\mathcal{J}_\mathcal{K}$ with coefficients in k, and $\mathcal{S}_u = [Q_u, W_1, \ldots, W_n]$ the vector corresponding to the parametrization*

$$Q_u(u) = 0, \quad \begin{cases} x_1 &= W_1(u), \\ & \vdots \\ x_n &= W_n(u). \end{cases}$$

Let $\mathbf{p}$ be a point in k^m which cancels none of the denominators in $\mathcal{S}_u$, such that the points described by the specialization of $\mathcal{S}_u$ at $\mathbf{p}$ do not cancel the Jacobian determinant $\mathbf{jac}(\mathbf{f}, \mathbf{X})$. Given the approximation $\mathcal{S}_u^\kappa$, $\mathcal{S}_u^{\kappa+1}$ can be computed in

$$O\big((nL + n^4)\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(2^{\kappa+1}, m)\big)$$

operations in k.

Proof. We get back to the previous setting by introducing $\mathbf{X} = (X_1, \ldots, X_n, X_{n+1})$, the triangular set $\mathbf{t} = (X_1 - W_1(X_{n+1}), \ldots, X_n - W_n(X_{n+1}), Q_u(X_{n+1}))$ and the equations $\mathbf{F} = (f_1, \ldots, f_n, X_{n+1} - \sum u_i X_i)$. There exists a $(n+1) \times (n+1)$-matrix $\mathbf{A}$ with entries in $k(P_1, \ldots, P_m)[X_1, \ldots, X_n, X_{n+1}]$ such that $\mathbf{F} = \mathbf{A}\mathbf{t}$, where $\mathbf{p}$ cancels none of the denominators in this equality. Let $(P'_1, \ldots, P'_m)$ be new variables, and $\mathcal{A}$ the power series ring $k[[P'_1, \ldots, P'_m]]$. All the entries in the previous matrix equality can be rewritten in terms of $(P'_1, \ldots, P'_m)$, letting $P_j = P'_j + p_j$, for $j = 1, \ldots, m$. None of the new denominators vanishes at zero, so all entries admit Taylor expansion in $\mathcal{A}$.

We apply Proposition 4 with $\mathcal{I} = (P'_1, \ldots, P'_m)$. Using the notation of the previous paragraph, the quotient H_κ is isomorphic to $k[[P'_1, \ldots, P'_m]]/\mathcal{I}^{2^{\kappa+1}}[\mathcal{U}]/Q_u^\kappa$. Since Q_u has degree $\deg_\pi$, and the coefficients are power series in m variables at precision $2^{\kappa+1}$, the cost of an operation in H_κ is $O\big(\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(2^{\kappa+1}, m)\big)$ operations in k.

The cost of the computations lies in the evaluation of the vectors and matrices involved, and in the linear algebra operations. Evaluating the non-zero terms in the matrix $\mathbf{Jac}(\mathbf{T}_\kappa)$ takes $O(n \deg_\pi \mathcal{M}_s(2^{\kappa+1}, m))$ operations in k. Using Baur-Strassen's algorithm [6], evaluating the matrix $\mathbf{Jac}(\mathbf{F}_\kappa)$ and the vector $\mathbf{F}_\kappa$ takes $O(nL)$ operations in the quotient H_κ. All linear algebra takes $O(n^4)$ operations in H_κ, using for instance Leverrier's algorithm [43] for matrix inversion over a ring. All this sums up to $O\big((nL + n^4)\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(2^{\kappa+1}, m)\big)$ operations in k, which proves the proposition. $\square$

4.3 Recovering the coefficients

Referring to the algorithm sketched in the introduction of this section, the last question to answer is how to recover the coefficients of a parametric resolution from their Taylor expansion at some point $\mathbf{p}$. To this effect, we present an algorithm for the reconstruction of a rational function.

The problem can be stated as follows: let D be a positive integer, p and q two polynomials in $k[P_1, \ldots, P_m]$ of degrees at most D such that $q(0) \neq 0$, and r the Taylor expansion of p/q at precision $2D + 1$. Given r as a polynomial of degree $2D$, we want to compute p/q.

In the single variable case, i.e. when $m = 1$, this question is solved using Padé approximants, see [64]. In our general multivariate case, the question can be solved using linear algebra; other solutions based on Gröbner bases computations are presented in [54, 22]. We propose an algorithm with better complexity, which reduces to the usual computation of Padé approximants when $m = 1$.

The algorithm is probabilistic: it requires to choose $m - 1$ values in the base field. We indicate the degree of an hypersurface in $\mathbb{A}^{m-1}(\overline{k})$ that must be avoided to ensure success.

The first paragraph is devoted to present the algorithm. We then estimate the cost of applying it on all the coefficients of a parametric resolution. Due to our approximation process, the origin of the coordinates in the parameter space has moved; to conclude this subsection, we consider the question of restoring the initial coordinates.

4.3.1 Rational reconstruction

The main idea of our algorithm is to get back to an Euclidean situation: we introduce a new variable s, and substitute the variables P_i by $P_i s$ in r. Then we perform a single-variable Padé approximation with main variable s, from which we recover the fraction p/q.

This algorithm uses the following subroutines, where $[P'_2, \ldots, P'_m]$ are new variables.

- `PadeApproximant`$(\widetilde{r})$, where $\widetilde{r}$ is a polynomial of degree $2D$ in $k[[P'_2, \ldots, P'_m]][s]$, with coefficients of precision D.

  The function follows the algorithms given in [64, chapters 5.9 and 11] to compute (D, D) Padé approximant of $\widetilde{r}$. This is done by applying the fast extended monic Euclidean algorithm to $\widetilde{r}$ and s^{2D+1}. The coefficients are power series of fixed precision D; the function raises an error if a division by a series of positive valuation occurs.

- `ConstantCoefficient`$(\overline{q})$, where $\overline{q}$ is in $k[[P'_2, \ldots, P'_m]][s]$.

  The function returns the coefficient of degree 0 of $\overline{q}$, if this coefficient is not zero. Else, it raises an error.

- `Homogenization`$(\widetilde{p}, P_1)$, where $\widetilde{p}$ belongs to $k[P_2, \ldots, P_m][s]$.

  Suppose that for all i the coefficient of s^i in $\widetilde{p}$ has degree at most i. Then, for all i, this function homogenizes the coefficient of s^i in degree i with respect to the variable P_1. If the previous assumption is not satisfied, an error is raised.

Here is our algorithm, which chooses $m-1$ values in the base field. The subsequent proposition shows that the output is correct for a generic choice, gives a bound on the complexity of the process and the probability of success.

Rational reconstruction

Procedure **RationalReconstruction**(r, γ)
Input: r in $k[P_1, \ldots, P_m]$ of degree $2D$, $\gamma = (\gamma_2, \ldots, \gamma_m)$ in k^{m-1}.
Output: a fraction p/q or "Failure".

$\widetilde{r} \leftarrow r(s, P_2 s, \ldots, P_m s)$;
\# We change the coordinates.
$\widetilde{r} \leftarrow \texttt{subs}(P_2 = P_2' + \gamma_2, \ldots, P_m = P_m' + \gamma_m, \widetilde{r})$;
\# The computations are done in $k[[P_2', \ldots, P_m']][s]$
\# with coefficients truncated at precision D.
$\overline{p}, \overline{q} \leftarrow \texttt{PadeApproximant}(\widetilde{r})$;
$\widetilde{p} \leftarrow \overline{p}/\texttt{ConstantCoefficient}(\overline{q})$;
$\widetilde{q} \leftarrow \overline{q}/\texttt{ConstantCoefficient}(\overline{q})$;
\# We change back the coordinates.
$\widetilde{p} \leftarrow \texttt{subs}(P_2' = P_2 - \gamma_2, \ldots, P_m' = P_m - \gamma_m, \widetilde{p})$;
$\widetilde{q} \leftarrow \texttt{subs}(P_2' = P_2 - \gamma_2, \ldots, P_m' = P_m - \gamma_m, \widetilde{q})$;
$\widetilde{P} \leftarrow \texttt{Homogenization}(\widetilde{p}, P_1)$;
$\widetilde{Q} \leftarrow \texttt{Homogenization}(\widetilde{q}, P_1)$;
$\texttt{return subs}(s = 1, \widetilde{P}/\widetilde{Q})$;

Proposition 6 *Suppose that there exist (p, q) of degrees at most D, such that r is the Taylor expansion of p/q at precision $2D+1$. For almost all choices of $(\gamma_2, \ldots, \gamma_m)$, the previous algorithm computes p/q using*

$$O_{\log}\left(\mathcal{M}_u(D)\left(\mathcal{M}_s(D, m-1) + m^2\binom{2D+m-1}{m-1}\right)\right) \subset O_{\log}\left(m^2 \mathcal{M}_u(D)\mathcal{M}_s(2D, m-1)\right)$$

operations in k. The choices of $(\gamma_2, \ldots, \gamma_m)$ that lead to an error belong to an hypersurface of $\mathbb{A}^{m-1}(\overline{k})$ of degree at most $2D(2D+1)^2$.

The proof is divided in several steps. We first show how using the new main variable s reduces the problem to univariate Padé approximant computations over a rational function field. Then we show how to replace rational function computations by power series computations; from this we deduce the complexity and error analysis.

Introduction of a new main variable. Let $\widetilde{R}$ be the substitution $r(P_1 s, \ldots, P_m s)$, for a new variable s. $\widetilde{R}$ belongs to $k(P_1, \ldots, P_m)[s]$ and has degree $2D$; we denote by $(\overline{P}, \overline{Q})$ its (D, D) Padé approximant, computed in $k(P_1, \ldots, P_m)[s]$ by applying the fast Euclidean algorithm to $\widetilde{R}$ and s^{2D+1}.

The polynomials $\big(p(P_1 s, \ldots, P_m s), q(P_1 s, \ldots, P_m s)\big)$ also form a (D, D) Padé approximant of $\widetilde{R}$, so uniqueness shows that they differ of $(\overline{P}, \overline{Q})$ by a factor in $k(P_1, \ldots, P_m)$. Consequently, dividing $\overline{P}$ and $\overline{Q}$ by the constant coefficient of $\overline{Q}$ yields $\widetilde{P} = p(P_1 s, \ldots, P_m s)/q(0)$ and $\widetilde{Q} = q(P_1 s, \ldots, P_m s)/q(0)$, and the substitution $s = 1$ in $\widetilde{P}/\widetilde{Q}$ gives the requested output p/q.

Computing the Padé approximant of $\widetilde{R}$ will not lead to an algorithm with good complexity: the coefficients that appear during the computations are rational functions, with increasing degrees. We now show how to replace these rational functions by power series, and deduce the proof of the proposition.

Dehomogenization. The coefficients that appear in the course of Euclid's algorithm applied to $\widetilde{R}$ and s^{2D+1} are homogeneous rational functions. Thus, if we want to introduce power series, is necessary to dehomogenize these coefficients. We now proceed to do so.

Let $\widetilde{r}$ be $r(s, P_2 s, \ldots, P_m s)$, and $(\overline{p}, \overline{q})$ the output of the Padé approximant computation applied to $\widetilde{r}$. Since the coefficients that occur during Euclid's algorithm applied to $\widetilde{R}$ and s^{2D+1} are homogeneous, $(\overline{p}, \overline{q})$ coincide with the dehomogenization of $(\overline{P}, \overline{Q})$ in the variable P_1.

As above, we define $(\widetilde{p}, \widetilde{q})$ as $(\overline{p}, \overline{q})$ divided by the constant coefficient of $\overline{q}$. Then the previous remarks show that they coincide with the dehomogenization of $(\widetilde{P}, \widetilde{Q})$ in the variable P_1. Since for all i, the coefficients of s^i in $\widetilde{P}$ and $\widetilde{Q}$ are homogeneous of degree i, applying the subroutine `Homogenization`$(., P_1)$ to $\widetilde{p}$ and $\widetilde{q}$ yields $\widetilde{P}$ and $\widetilde{Q}$.

Consequently, it suffices to compute $(\overline{p}, \overline{q})$ then $(\widetilde{p}, \widetilde{q})$ and finally $(\widetilde{P}, \widetilde{Q})$ to solve the problem.

Computation with power series. If none of the denominators occurring during Euclid's algorithm applied to $(\widetilde{r}, s^{2D+1})$ vanishes at zero, all the operations on the coefficients can be done at fixed precision D, replacing the rational functions in $(P_2, \ldots, P_m)$ by their power series expansion at order D.

To get back to this lucky situation, we perform a linear change of variables. Given a value $(\gamma_2, \ldots, \gamma_m)$ in k^{m-1}, we do the computations in the variables $(P'_2, \ldots, P'_m)$, where $P_i = P'_i + \gamma_i$ for $i = 2, \ldots, m$, and get back to the initial variables afterwards.

If A is a polynomial in $k[P_2, \ldots, P_m]$, rewritten A' in the variables $(P'_2, \ldots, P'_m)$, the constant term in $A'(P'_2, \ldots, P'_m)$ is $A(\gamma_2, \ldots, \gamma_m)$. Consequently, the Padé approximant computations can be done at fixed precision in the new variables if $(\gamma_2, \ldots, \gamma_m)$ cancels none of the denominators that appear in the course of Euclid's algorithm applied to $\widetilde{r}$ and s^{2D+1}.

From [10, 64], this is the case if and only if $(\gamma_2, \ldots, \gamma_m)$ cancels none of the non-zero subresultant coefficients associated to $\widetilde{r}$ and s^{2D+1}. These subresultants are minors of the Sylvester matrix associated to $\widetilde{r}$ and s^{2D+1} of sizes $i = 1, 3, \ldots, 4D + 1$, with entries of degrees at most $2D$. Each determinant is a polynomial in $k[P_2, \dots, P_m]$ of degree at most $2Di$, so their product has degree at most $2D(2D+1)^2$. This proves the last point of the proposition.

Complexity. We now estimate the complexity. Since the coefficients are power series in $m-1$ variables at precision D, Euclid's algorithm takes $O_{\log}\big(\mathcal{M}_u(D)\mathcal{M}_s(D, m-1)\big)$ operations in k, see [64, chapter 11].

The changes of variables require the translation by vectors $(\gamma_2, \dots, \gamma_m)$ and $(-\gamma_2, \dots, -\gamma_m)$ on the coefficients of $\widetilde{r}$, $\widetilde{p}$ and $\widetilde{q}$. These polynomials have degree at most $2D$, and their coefficients are polynomials in $(P_2, \dots, P_m)$ of degrees at most $2D$. The following lemma shows that the cost of a translation is $O_{\log}\big(m\mathcal{M}_u(D)\binom{2D+m-2}{m-2}\big)$, so the sum of these costs is in $O_{\log}\big(mD\mathcal{M}_u(D)\binom{2D+m-2}{m-2}\big)$, which is in $O_{\log}\big(m^2\mathcal{M}_u(D)\binom{2D+m-1}{m-1}\big)$.

The proof of the proposition is now almost complete. We only have to establish the following lemma, which we used above. It gives the cost of translating the variables in a multivariate polynomial.

Lemma 6 *Let A a polynomial in $k[P_2, \dots, P_m]$ of degree D, and $(\gamma_2, \dots, \gamma_m)$ a point in k^{m-1}. Then $A(P_2+\gamma_2, \dots, P_m+\gamma_m)$ can be computed in $O_{\log}\big(m\mathcal{M}_u(D)\binom{D+m-2}{m-2}\big)$ operations in k.*

Proof. We move one variable P_i at a time; to keep the notation simple, we describe the case $i = 2$. We consider the polynomial A in $k[P_2][P_3, \dots, P_m]$; then the translation is done by shifting all coefficients.

Using the divide-and-conquer algorithm given in [64, chapter 9.2], shifting a single coefficient requires $O(\mathcal{M}_u(D)\log D)$ operations in k. Since there are at most $\binom{D+m-2}{m-2}$ such coefficients, this sums up to $O(\mathcal{M}_u(D)\log D\binom{D+m-2}{m-2})$ operations in k. Taking all variables P_i into account leads to the announced bound. $\square$

4.3.2 Application to parametric resolutions

The rational reconstruction process will be applied to all the coefficients of a parametric resolution. If $\mathcal{R} = [Q_u, V_1, \dots, V_n]$ is a vector of polynomials in $k[[P_1, \dots, P_m]][\mathcal{U}]$ and γ a point in k^{m-1}, we denote by `RationalReconstruction`$(\mathcal{R}, \gamma)$ the application of the reconstruction process to all the coefficients of the polynomials in $\mathcal{R}$. The output is a boolean value b which indicates success, and, if possible, a sequence of polynomials, where all coefficients are reconstructed.

Due to our Newton approximation scheme, the Taylor expansions will be given at precisions of the form 2^κ. In this short paragraph, we indicate the total cost of the reconstruction under such constraints. Recall that the reconstruction requires to choose $m-1$ values in the base field: we also indicate the degree of a hypersurface of $\mathbb{A}^{m-1}(\overline{k})$ that must be avoided to ensure success.

We suppose that $\mathcal{R}$ corresponds to a parametric resolution in Kronecker form. Then we can suppose that all coefficients in the parametric resolution have for maximal degree an integer denoted by $\deg_u$. Using Theorem 1, $\deg_u$ is bounded by the geometric degree $\deg_{\mathcal{V}}$, itself bounded by the Bézout number d^n. We will also use the hypothesis that the polynomials $[Q_u, V_1, \dots, V_n]$ have degree at most $\deg_\pi \leq d^n$ in their main variable $\mathcal{U}$.

If p/q is a fraction with numerator and denominator of degrees bounded by $\deg_u$, then the first power of 2 that permits reconstruction is the first power of 2 greater than $2\deg_u + 1$. If we denote by $\lceil x \rceil$ the first integer greater than or equal to x, this power is 2^{κ_0}, where $\kappa_0 = \lceil \log_2(2\deg_u + 1) \rceil$. Since $\deg_u \leq d^n$, then $2^{\kappa_0} \leq 4d^n$.

Applying Proposition 6 with $2D = 2^{\kappa_0}$ shows that a single coefficient can be reconstructed if the change of variables γ avoids an hypersurface of degree at most $4d^n(4d^n + 1)^2$, and the reconstruction then takes $O_{\log}(m^2 \mathcal{M}_u(2^{\kappa_0}) \mathcal{M}_s(2^{\kappa_0}, m-1))$ operations in k. Taking all coefficients into account then leads to $O_{\log}\big(nm^2 \deg_\pi \mathcal{M}_u(2^{\kappa_0}) \mathcal{M}_s(2^{\kappa_0}, m-1)\big)$ operations in k.

Since all polynomials in $\mathcal{R}$ have degree in $\mathcal{U}$ at most $\deg_\pi$ and Q_u is monic, there are at most $(n+1)d^n$ rational function to recover, and all of them can be recovered if γ avoids the union of all corresponding hypersurfaces. This union has degree at most $4(n+1)d^{2n}(4d^n + 1)^2$.

Summary. Let us summarize the results we will need in the sequel:

- We assume that the coefficients to reconstruct are rational functions with numerators and denominators of degree at most $\deg_u \leq d^n$.
- The first power of 2 that enables the reconstruction is 2^{κ_0}, with $\kappa_0 = \lceil \log_2(2\deg_u + 1) \rceil$.
- The total cost of the reconstruction is within $O_{\log}\big(nm^2 \deg_\pi \mathcal{M}_u(2^{\kappa_0}) \mathcal{M}_s(2^{\kappa_0}, m-1)\big)$ operations in k.
- The hypersurface of $\mathbb{A}^{m-1}(\overline{k})$ to avoid has degree at most $4(n+1)d^{2n}(4d^n + 1)^2$.

4.3.3 Going back to the initial coordinates

Suppose that the reconstruction of the parametric resolution is successful. Due to our approximation process, the coordinates in the parameter space are centered at some value $(p_1, \dots, p_m)$ in k^m, so we must move back to the initial coordinates. Given a resolution $\mathcal{R} = [Q_u, V_1, \dots, V_n]$ as a vector of polynomials in $k(P_1, \dots, P_m)[\mathcal{U}]$, we introduce a subroutine `RestoreCoordinates`($\mathcal{R}$) devoted to this operation.

Using the same notation as above, we suppose that the coefficients of the polynomials in $\mathcal{R}$ have degree in $P_1, \dots, P_m$ at most $2^{\kappa_0 - 1}$. Lemma 6 shows that the cost necessary to move a single coefficient is $O_{\log}\big(m\mathcal{M}_u(2^{\kappa_0-1})\binom{2^{\kappa_0-1}+m-1}{m-1}\big)$ operations in k. If we suppose that the polynomials in $\mathcal{R}$ have degree at most $\deg_\pi$ in $\mathcal{U}$, then there are $(n+1)\deg_\pi$ coefficients to move. The subroutine `RestoreCoordinates` then induces a total cost of $O_{\log}\big(nm \deg_\pi \mathcal{M}_u(2^{\kappa_0-1})\binom{2^{\kappa_0-1}+m-1}{m-1}\big)$ operations in k.

5 The main algorithm

The main algorithm consists in a loop organized around the Newton approximation process; tests are performed at each pass to decide whether to stop the computation or not.

Before giving the details of the main algorithm, we present the additional subroutine, denoted `StopCriterion`, which decides whether to stop the lifting. In a second time, we give the whole algorithm, and work out its complexity and probability of success. Finally, we mention some possible practical improvements.

We constantly switch between the two forms of parametrization, Kronecker and Shape Lemma: the former has better degree properties, so is well suited for the rational reconstruction, whereas Newton's iterator works using the later representation. In the sequel, we denote `KroneckerParametrization`($\mathcal{S}_u$) a routine which, given a Shape Lemma parametrization, outputs the corresponding Kronecker parametrization, and `ShapeLemmaParametrization`($\mathcal{R}_u$) the converse process.

5.1 The stop criterion

For obvious practical reasons, we do not perform the lifting up to the Bézout bound. Instead, we use a probabilistic test, presented in the subroutine `StopCriterion`: once we have a candidate resolution, the test mainly consists in testing it on a witness point $\mathbf{p}'$; there is a possibility of choosing a bad witness, which will be taken into account in the proof of Proposition 7.

Stop criterion for the lifting process

Procedure **StopCriterion**($\mathcal{R}, \mathbf{f}, \mathbf{p}'$)
Input: a parametric resolution $\mathcal{R} = [Q_u, V_1, \ldots, V_n]$, the system $\mathbf{f}$, $\mathbf{p}'$ in k^m.
Output: a boolean value.

`if`
  $\mathbf{p}'$ cancels none of the denominators in $\mathcal{R}$,
  the specialization of Q_u at $\mathbf{p}'$ is squarefree,
  the points described by the specialization of $\mathcal{R}$ at $\mathbf{p}'$ cancel the system $\mathbf{f}(\mathbf{p}', .)$,
  these points do not cancel the Jacobian determinant of $\mathbf{f}(\mathbf{p}', .)$,
`then return true`
`else return false`

Lemma 7 *Suppose that the polynomials in* $\mathcal{R} = [Q_u, V_1, \ldots, V_n]$ *have degree at most* $\deg_\pi$, *and that their coefficients are rational functions of degree at most* D. *Then the cost of the subroutine* `StopCriterion` *is* $O_{\log}(n \deg_\pi \binom{D+m}{m} + (nL + n^4)\mathcal{M}_u(\deg_\pi))$ *operations in* k.

Proof. All the $(n+1)\deg_\pi$ coefficients of $\mathcal{R}$ have degree at most D in m variables, so their specialization on the point $\mathbf{p}'$ takes less than $(n+1)\deg_\pi \binom{D+m}{m}$ operations in k. Let us denote $[q_u, v_1, \ldots, v_n]$ the specialized resolution, with coefficients in k.

Testing whether the points described by this specialization cancel $\mathbf{f}$ requires to switch to the equivalent Shape Lemma Parametrization $[q_u, w_1, \ldots, w_n]$, with coefficients in k, then to evaluate $\mathbf{f}$ on the elements $[w_1, \ldots, w_n]$ modulo q_u. The first task requires to invert q_u' modulo q_u, hence has cost $O_{\log}(\mathcal{M}_u(\deg_\pi))$, using the fast Euclidean algorithm [64]. The second task takes $O(L\mathcal{M}_u(\deg_\pi))$ additional operations.

Similarly, the Jacobian matrix can be evaluated in nL operations modulo q_u using Baur-Strassen's algorithm [6] and its determinant can be computed in n^4 operations modulo q_u, which adds $O((nL+n^4)\mathcal{M}_u(\deg_\pi))$ operations. Its invertibility can be tested within $O_{\log}(\mathcal{M}_u(\deg_\pi))$ operations. This yields the overall complexity bound. □

5.2 The detailed algorithm

We are now ready to present the main algorithm `ParametricResolution`. It chooses $3m-1$ values in the base field: the coordinates of the points $\mathbf{p}$ and $\mathbf{p}'$, and the change of variables γ used in the rational reconstruction. The following proposition shows that for a generic choice, the output is correct, and quantifies the bad choices. This brings the proof of Theorem 2 restated in the proposition below.

Computing a parametric resolution

Procedure **ParametricResolution**($\mathbf{f}$)
Input: the system $\mathbf{f} = (f_1, \ldots, f_n)$.
Output: a parametric geometric resolution or "Failure".

$\mathbf{p}, \mathbf{p}' \leftarrow$ points in k^m;
$\gamma \leftarrow$ point in k^{m-1};
$\mathbf{u}, \mathcal{R}_u^0 \leftarrow$ `Resolution`$(\mathbf{f}, \mathbf{p})$;
$\mathcal{S}_u^0 \leftarrow$ `ShapeLemmaParametrization`$(\mathcal{R}_u^0)$;
MaxSteps $\leftarrow \lceil \log_2(2d^n+1) \rceil$; $\kappa \leftarrow 0$;
`while` $\kappa \leq$ MaxSteps `do`
  $\mathcal{R}_u^\kappa \leftarrow$ `KroneckerParametrization`$(\mathcal{S}_u^\kappa)$;
  $b, \mathcal{R}_u^\kappa \leftarrow$ `RationalReconstruction`$(\mathcal{R}_u^\kappa, \gamma)$;
  `if` b `then`
    finished $\leftarrow$ `StopCriterion`$(\mathcal{R}_u^\kappa, \mathbf{f}, \mathbf{p}')$;
    `if` finished `then return` `RestoreCoordinates`$(\mathcal{R}_u^\kappa)$;
  `end if`;
  $\mathcal{S}_u^{\kappa+1} \leftarrow$ `Lift`$(\mathbf{f}, \mathcal{S}_u^\kappa, u)$;
  $\kappa \leftarrow \kappa + 1$;
`end while`;
`return` "Failure";

Proposition 7 *Let Γ be a subset of k, and suppose that $(\mathbf{p}, \mathbf{p}', \gamma)$ are chosen in Γ^{3m-1}. If $n \geq 2$ and $d \geq 2$, then the algorithm* `ParametricResolution` *computes a parametric resolution of $\mathcal{K} \to \mathcal{K}[X_1, \ldots, X_n]/\mathcal{J}_{\mathcal{K}}$ for all choices except at most $110nd^{4n}|\Gamma|^{3m-2}$.*

In case of success, the complexity of the lifting step is

$$O_{\log}\big((nL + n^4)\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(4\deg_u, m) + nm^2 \deg_\pi \mathcal{M}_u(\deg_u)\mathcal{M}_s(4\deg_u, m-1)\big)$$

operations in k, where $\deg_u$ is the maximum of the degrees in $P_1, \ldots, P_m$ of the coefficients that appear in the parametric resolution. Else, the algorithm stops after at most $\lceil \log_2(2d^n + 1)\rceil$ lifting steps, and outputs either "Failure" or a wrong answer.

We first show that the algorithm computes the correct answer for generic choices of $(\mathbf{p}, \mathbf{p}', \gamma)$; we return to the quantification of the bad choices in a second time, then estimate the complexity of the process.

Proof of correctness. Let Δ be the polynomial defined in Proposition 3; we assume that the polynomial $\Delta(\mathbf{p}, .)$ is not zero, and let $\mathbf{u}, \mathcal{R}_u^0$ be the output of `Resolution`$(\mathbf{f}, \mathbf{p})$. The second part of Proposition 3 shows that $\Delta(\mathbf{p}, \mathbf{u})$ is not zero, and that $\mathcal{R}_u^0$ is the specialization of a generic resolution $\mathcal{R}_u$ at $\mathbf{p}$.

The points $\mathbf{p}$ and $\mathbf{u}$ satisfy the hypotheses of Proposition 5 so after κ lifting steps, the coefficients of $\mathcal{R}_u$ are known at precision 2^κ. Let $\deg_u$ be the maximum of the degrees in $P_1, \ldots, P_m$ of the coefficients that appear in $\mathcal{R}_u$; Proposition 2 shows that $\deg_u \leq d^n$. We call κ_0 the number of lifting steps necessary before the reconstruction of all the coefficients is possible; the results of Subsection 4.3.2 show that $\kappa_0 \leq \lceil \log_2(2\deg_u + 1)\rceil \leq \lceil \log_2(2d^n + 1)\rceil$.

We now rule out the possibility that, for some $\kappa \leq \kappa_0 - 1$, the rational reconstruction of $\mathcal{R}_u^\kappa \neq \mathcal{R}_u$ is possible and the subroutine `StopCriterion`$(\mathcal{R}_u^\kappa, \mathbf{p}', \mathbf{f})$ outputs `true`; in this case $\mathbf{p}'$ will be called a *bad witness*.

Since $\Delta(\mathbf{p}, \mathbf{u})$ is not zero, the polynomial $\Delta(., \mathbf{u})$ itself is not zero. We suppose that $\mathbf{p}'$ does not cancel this polynomial; the first point in Proposition 3 then implies that the simple solutions of the specialized system $\mathbf{f}(\mathbf{p}', .) = 0$ are described by the specialization of $\mathcal{R}_u$ at $\mathbf{p}'$.

The subroutine `StopCriterion` outputs `true` at step $\kappa \leq \kappa_0 - 1$ if the simple solutions of the system $\mathbf{f}(\mathbf{p}', .) = 0$ are described by the specialization of $\mathcal{R}_u^\kappa$ at $\mathbf{p}'$, i.e. if the specializations of $\mathcal{R}_u$ and $\mathcal{R}_u^\kappa$ coincide at $\mathbf{p}'$. Since $\mathcal{R}_u$ and $\mathcal{R}_u^\kappa$ are different, at least one of their coefficients differs. These coefficients are rational functions of degrees at most d^n and $2^{\kappa-1}$, so the points where their specializations coincide are contained in an hypersurface of $\mathbb{A}^m(\overline{k})$ of degree at most $d^n + 2^{\kappa-1}$.

Taking all $\kappa < \kappa_0$ into consideration shows that the point $\mathbf{p}'$ is a "good witness" if it avoids an hypersurface $\mathbb{A}^m(\overline{k})$ of degree at most $d^n + 0 + d^n + 1 + \cdots + d^n + 2^{(\kappa_0 - 1) - 1} \leq d^n \kappa_0 + 2^{\kappa_0 - 1} \leq d^n(\lceil \log_2(2d^n + 1)\rceil + 2)$. We suppose that this is the case.

The algorithm can then fail only if the reconstruction at step κ_0 fails, so success is assured if the change of variables γ avoids the hypersurface defined in Subsection 4.3.2; this hypersurface has degree at most $4(n + 1)d^{2n}(4d^n + 1)^2$.

Estimation of probabilities. We now return to the assumptions made on $(\mathbf{p}, \mathbf{p}', \gamma)$ and use Zippel-Schwartz' lemma [67, 60] to quantify the choices that assure success. Let Γ be a subset of k, and suppose that the values $(\mathbf{p}, \mathbf{p}', \gamma)$ are chosen in $\Gamma^m \times \Gamma^m \times \Gamma^{m-1}$. Besides, we recall that the polynomial Δ has degree at most $d^n(2d^n + nd + 1)$ in $P_1, \ldots, P_m$.

- There at most $d^n(2d^n + nd + 1)|\Gamma|^{m-1}$ values of $\mathbf{p}$ such that $\Delta(\mathbf{p}, .) = 0$; this discriminates at most $d^n(2d^n + nd + 1)|\Gamma|^{3m-2}$ choices of $(\mathbf{p}, \mathbf{p}', \gamma)$.
- For all remaining values of $\mathbf{p}$, there are at most $4(n+1)d^{2n}(4d^n + 1)^2|\Gamma|^{m-2}$ values of γ which prevent the reconstruction; this represents at most $4(n+1)d^{2n}(4d^n + 1)^2|\Gamma|^{3m-2}$ choices of $(\mathbf{p}, \mathbf{p}', \gamma)$. If $m = 1$, the reconstruction is deterministic, so this possibility of failure is not taken into account.
- For all remaining values of $\mathbf{p}$, for any value of $\mathbf{u}$, there are at most $d^n(2d^n+nd+1)|\Gamma|^{m-1}$ values of $\mathbf{p}'$ such that $\Delta(\mathbf{p}', \mathbf{u}) = 0$; this discriminates at most $d^n(2d^n + nd + 1)|\Gamma|^{3m-2}$ choices of $(\mathbf{p}, \mathbf{p}', \gamma)$.
- Finally, for any value of $\mathbf{p}$ and $\mathbf{u}$, there are at most $d^n(\lceil \log_2(2d^n + 1)\rceil + 2)|\Gamma|^{m-1}$ values of $\mathbf{p}'$ which are bad witnesses. This represents at most $d^n(\lceil \log_2(2d^n + 1)\rceil + 2)|\Gamma|^{3m-2}$ triples $(\mathbf{p}, \mathbf{p}', \gamma)$.

The number of bad choices is thus at most

$$d^n\big(4(n + 1)d^n(4d^n + 1)^2 + 4d^n + 2nd + \lceil \log_2(2d^n + 1)\rceil + 4\big)|\Gamma|^{3m-2}.$$

Using the rough estimates $\log(1 + x) \leq x$ and $nd \leq d^n$ if $d \geq 2$, this quantity is seen to be bounded by

$$d^{2n}\big(4(n + 1)(16d^{2n} + 8d^n + 1) + 12\big)|\Gamma|^{3m-2}.$$

Using $n + 1 \leq 3n/2$ for $n \geq 2$, we bound this number by $nd^{2n}(96d^{2n} + 48d^n + 18)|\Gamma|^{3m-2}$, which itself is bounded by $110nd^{4n}|\Gamma|^{3m-2}$.

Complexity. We finally turn to the complexity of the algorithm, and detail the cost of the last call to each subroutine, in terms of operations in k.

- The last call to `Lift` brings the precision to 2^{κ_0}. Proposition 5 shows that its cost is in $O((nL + n^4)\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(2^{\kappa_0}, m))$.
- The subroutine `KroneckerParametrization` requires to multiply all parametrizations by the derivative of the minimal polynomial Q_u', and to reduce them modulo Q_u. This takes $O(n\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(2^{\kappa_0}, m))$ operations in k.
- We saw in Subsection 4.3.2 that the total cost of the subroutine `RationalReconstruction` is in $O_{\log}\big(nm^2 \deg_\pi \mathcal{M}_u(2^{\kappa_0})\mathcal{M}_s(2^{\kappa_0}, m - 1)\big)$.
- Lemma 7 shows that the complexity of `StopCriterion` is in $O_{\log}\big(n \deg_\pi \binom{2^{\kappa_0-1}+m}{m} + (nL + n^4)\mathcal{M}_u(\deg_\pi)\big)$. In case of success, Subsection 4.3.3 shows that the subroutine `RestoreCoordinates` has complexity $O_{\log}\big(nm \deg_\pi \mathcal{M}_u(2^{\kappa_0-1})\binom{2^{\kappa_0-1}+m-1}{m-1}\big)$.

All these costs sum up to

$$O_{\log}\big((nL+n^4)\mathcal{M}_u(\deg_\pi)\mathcal{M}_s(2^{\kappa_0},m)+nm^2\deg_\pi\mathcal{M}_u(2^{\kappa_0})\mathcal{M}_s(2^{\kappa_0},m-1)\big).$$

Under our assumption that $\mathcal{M}_s(d,m)\leq c\mathcal{M}_s(2d,m)$ for some universal constant $c<1$, the cost of all steps is bounded by $1/(1-c)$ times the cost of the last step. Since $2^{\kappa_0}\leq 4\deg_u$, this yields the overall complexity bound. □

5.3 Practical strategies

This section presents possible improvements of the main algorithm, which have important practical impact.

Modular arithmetic. Most systems we present as applications are defined over the rational field. To avoid the growth of the intermediate coefficients, it is natural to adopt a strategy based on modular computation: the resolution is first computed modulo some prime number $\mathfrak{p}$, then lifted modulo the successive powers $\mathfrak{p}^{2^\kappa}$, and the rational numbers are recovered when their $\mathfrak{p}$-adic approximation is precise enough.

This process is quite similar to the lifting of the parameters presented here, and is used in practice. All necessary algorithmic tools are given in this paper, except the reconstruction of rational numbers, which is a well-solved problem [62, 15, 64]. Still, we do not give more details on this question: such a strategy induces a variety of new possibilities of failure, whose analysis requires to use arithmetic versions of Bézout's theorem and of the Nullstellensatz. This is beyond the scope of this paper; such results may be found in the author's PhD. Thesis [58].

Factorization. Suppose that the minimal polynomial of the specialized system splits into i irreducible factors of degrees $(\deg_\pi^{(1)},\dots,\deg_\pi^{(i)})$, so that this fiber can be described by i geometric resolutions of smaller degree. Even when the generic fiber is irreducible, it is possible to take profit of this factorization: the lifting is done on all smaller resolutions, which are combined before each call to `RationalReconstruction` and `StopCriterion`.

The term $\mathcal{M}_u(\deg_\pi)=\mathcal{M}_u(\sum\deg_\pi^{(i)})$ in the complexity of the lifting step is replaced by $\sum\mathcal{M}_u(\deg_\pi^{(i)})$. This is most important for a naive multiplication algorithm where $\mathcal{M}_u(D)=O(D^2)$, or Karatsuba's method, for which $\mathcal{M}_u(D)=O(D^{1.59})$. The cost of the recombination of all factors is analyzed in [41], and does not modify our complexity bound.

Computing outside a given hypersurface. Suppose that we want the points $\mathcal{V}'\subset\mathcal{V}$ lying outside a given hypersurface $\mathcal{H}\subset\mathbb{A}^{m+n}(\overline{k})$. It suffices to remove the points of $\mathcal{H}$ that intersect the specialized fiber, and perform the lifting on what remains. The correctness of this process requires that the specialization value $\mathbf{p}$ avoids the projection of $\overline{\mathcal{V}}'\cap\mathcal{H}$ on $\mathbb{A}^m(\overline{k})$; taking this possibility into account does not modify the rough upper bound $110nd^{4n}$ in the quantification of the probability of success presented above.

6 Applications

This last section gathers some applications which where the initial motivation for the design of our algorithm. All systems are not displayed for lack of space; the equations are available upon request.

The algorithm is implemented in Magma [2]. The `Kronecker` package developed by G. Lecerf [40] provided many necessary functionalities. We compared our timings with Gröbner Bases computations, for we could easily find a primitive element in each example; we used Magma for these computation, as it allows for such computations on rational function fields.

6.1 Description of the systems

Number of points of a Jacobian. This example, denoted P19 in section 6.2, describes computations that were performed with P. Gaudry and R. Harley for their genus 2 point counting record [23].

More precisely, the framework is the determination of the number of points of the Jacobian of a curve of genus 2 defined over the finite field $k = \mathbb{F}_{\mathfrak{p}}$, where $\mathfrak{p}$ is the first prime greater than 10^{19}. Following Schoof's algorithm for elliptic curves [57], their algorithm is based on explicit computation of divisors of ℓ^i-torsion, for various primes ℓ. This part describes the computations for the case $\ell = 2$.

We have considered a polynomial system with coefficients in $\mathbb{F}_{\mathfrak{p}}$ whose resolution gives some divisors D_{i+1} of 2^{i+1}-torsion from the knowledge of a divisor D_i of 2^i-torsion: this system thus encodes the halving in the Jacobian.

This polynomial system has 4 equations in 6 variables, which split in the 4 coordinates of D_{i+1} plus 2 parameters that are functions of D_i. Given a 2-torsion divisor D_1, the resolution of this system gives a 4-torsion divisor D_2, which is in turn fed to a similar system, and so on. The objective is to go as far as possible, to refine the knowledge of the cardinality.

As i increases, the divisors D_i have their coordinates in extensions of k of increasing degrees, so the resolution of the specialized systems gets harder. It is preferable to compute the parametric resolution for once, then to specialize it when needed.

A priori considerations show that this system has generically 64 solutions, and the resolution of a specialized system shows that they are all simple, so our algorithm applies. Our output is only generically valid, but the specialization values caused no problem. We were thus able to compute divisors up to 256-torsion.

Deformation of singular hypersurfaces. The theoretical background for this problem can be found in the article by F. Rouillier, M.-F. Roy and M. Safey el Din [51] and references therein. These authors address the problem of finding one point in each connected component of a hypersurface $\mathcal{H} = P^{-1}(0) \subset \mathbb{R}^n$. This is achieved by considering the critical points on $\mathcal{H}$ of the function $d_{\mathbf{A}}(\mathbf{M}) = \|\mathbf{AM}\|^2$, for some point $\mathbf{A}$. This is done by computing the (complex) zero-set of the system

$$\big\{P(\mathbf{M}) = 0,\ \ \mathbf{grad}_{\mathbf{M}} P // \mathbf{AM}\big\},$$

where the last condition is expressed by setting $(n-1)$ 2×2 determinants to zero.

We suppose we have a generic enough point $\mathbf{A}$, so this system is zero-dimensional if the hypersurface $\mathcal{H}$ has a finite number of singularities. When $\mathcal{H}$ has an infinite number of singularities, the solution proposed in [51] consists in introducing an infinitesimal ε and studying the critical points on the level sets $P^{-1}(\varepsilon)$. This amounts to solving the system

$$\big\{P(\mathbf{M})=\varepsilon,\ \ \mathbf{grad}_{\mathbf{M}}P//\mathbf{AM}\big\}.$$

We see this system as parametrized by ε; Sard's theorem shows that all solutions of this system are generically simple, so our algorithm can be used to compute a parametric solution. We mention that the final step, described in [51], amounts to studying to limits when $\varepsilon \to 0$ of the points described by the parametric resolution, so as to solve the initial problem.

As an illustration, in [52], with F. Rouillier and M. Safey el Din, we treated some examples taken from the *Birkhoff Interpolation Problem* [31], involving some hypersurfaces in 3 variables (t_2,t_3,t_4), which had not be treated automatically before. In Section 6.2, we consider the two examples

$$\begin{aligned} P_3 = \quad & 3t_3^6+3t_4^6+9t_3^2t_4^4+9t_3^4t_4^2+t_2^2t_4^4+t_2^2t_3^4-t_2^4t_4^2-t_2^4t_3^2+\\ & t_2^6+4t_4^4+4t_3^4+4t_2^4+2t_2^2t_3^2t_4^2+8t_3^2t_4^2-4t_2^2t_4^2-4t_2^2t_3^2,\end{aligned}$$

$$\begin{aligned} P_{10} = \quad & -t_3^6-3-4t_3^4t_4^2+t_2^2t_3^4-4t_2^4t_4^2-t_2^4t_3^2-3t_2^6+t_3^4-9t_2^4-\\ & t_3^2-9t_2^2-4t_4^2+4t_2^2t_3^2t_4^2-2t_2^2t_3^2-8t_2^2t_4^2+4t_3^2t_4^2.\end{aligned}$$

Using a randomly chosen point $\mathbf{A}$ with integer coordinates, we generate two systems called Birkhoff_3 and Birkhoff_{10}.

Computing relations. This system was solved to answer a question of I. Bershenko-Kogan [7]. The initial goal is the determination of the conjugacy classes of $\mathbb{Q}[A,B,C]$ under the action of $\mathrm{GL}_3(\mathbb{Q})$, and notably the study of the orbit of the form $A^n+B^n+C^n$.

This requires to compute the relation R between three rational functions $X/D, Y/D, Z/D$ in two variables P, Q. This relation is an equation of the image of the corresponding rational application, so it is an irreducible polynomial.

We viewed the system the following way: we introduce two parameters x and y, three variables z, P, Q, and the system $(f_1,f_2,f_3)=\big(Dx-X, Dy-Y, Dz-Z\big)$. The relation R is the minimal polynomial of the variable z in $\mathbb{Q}(x,y)\to\mathbb{Q}(x,y)[P,Q,z]/(f_1,f_2,f_3)$. Once we have a parametric resolution, computing this minimal polynomial is easy: a straightforward way to do so is the computation of the squarefree part of a resultant; a more efficient solution is described in [61].

This system is denoted Bershenko is the sequel. Our output was checked in a direct manner: since the relation R must be irreducible, it suffices to evaluate the relation R on the functions $X/D, Y/D, Z/D$, and check that we obtain zero.

The system Hawes. This last example is taken from the database SymbolicData [5] (see also J.-C. Faugère's homepage [1]). Its purpose is to illustrate the behavior of our algorithm with respect to the representation of the input system.

This system has 6 equations plus two inequations in the 8 variables $a, b, c, x, y_1, z_1, y_2, z_2$.

$$
\begin{aligned}
3z_1^2 + y_1^2 + b &= 0,\\
3z_2^2 + y_2^2 + b &= 0,\\
2cy_1 + x + 5y_1^4 + 3ay_1^2 + 2y_1z_1 &= 0,\\
2cy_2 + x + 5y_2^4 + 3ay_2^2 + 2y_2z_2 &= 0,\\
-cy_2^2 + cy_1^2 - xy_2 + xy_1 + z_1^3 + y_1^2z_1 + bz_1 - y_2^5 - ay_2^3 - y_2^2z_2 - z_2^3 - bz_2 + y_1^5 + ay_1^3 &= 0,\\
2(30y_1^3z_1 - y_1^2 + 9ay_1z_1 + 3z_1^2)(-9ay_2^2z_2 + 3xz_2 - 3y_2z_2^2 - 45y_2^4z_2 + y_2^3 - by_2)&\\
-2(30y_2^3z_2 - y_2^2 + 9ay_2z_2 + 3z_2^2)(-9ay_1^2z_1 + 3xz_1 - 3y_1z_1^2 - 45y_1^4z_1 + y_1^3 - by_1)&\\
+6cy_1^2z_1(3xz_2 - 3y_2z_2^2 - 45y_2^4z_2 + y_2^3 - by_2) - 6cy_2^2z_2(3xz_1 - 3y_1z_1^2 - 45y_1^4z_1 + y_1^3 - by_1) &= 0.
\end{aligned}
$$

Thanks to J.-C. Faugère, we know that the original question was "We wish to eliminate x, y_1, z_1, y_2, z_2 from the system ignoring the trivial solutions of $y_1 = y_2$ and $z_1 = z_2$". As in the previous example, this amounts to computing the minimal polynomial with coefficients in $\mathbb{Q}(a, b)$ of c in a suitably-defined quotient algebra. Our solution was described in the previous paragraph; here, we only consider the preliminary task, the computation of a parametric resolution.

The system was initially given under an expanded form, requiring 92 multiplications. An additional work was necessary to recover the original, more compact, formulation given above, with 55 operations. The impact of this reformulation was important on the computation times, as the following tables will show.

6.2 Computation times

We now present the computation times. As the complexity results are stated in terms of arithmetic operations, we first give the times for the resolution over a finite fields, where arithmetic operations have a constant cost; we choose the field $\mathbb{F}_\mathfrak{p}$, $\mathfrak{p} = 10000000000000000051$ being the first prime greater than 10^{19}. In the second table, we present the results of the computations over $\mathbb{Q}$, for which we used the strategy described in Section 5.3.

The computations were done on the machines of the UMS MEDICIS [3], on Compaq Alpha EV6 XP/1000 500 Mhz processors with 640 MB of RAM, using Magma v. 2.6.

Here is the legend for Figures 2 and 3:

- The first four lines give the measure of the input: (n, m, d) and the number of multiplications in the Straight-Line Program giving the system;
- The next two lines give the generic number of solutions ($\deg_\pi$) and the degree in the parameters of the coefficients of the output ($\deg_u$).

Figure 2: Computation over $\mathbb{F}_{10000000000000000051}$

System	P19	Birkhoff_3	Birkhoff_{10}	Bershenko	Hawes
Variables	4	3	3	3	6
Parameters	2	1	1	2	2
Degree	10	6	6	12	9
Multiplications	253	91	80	32	55 (92)
Generic Degree	64	34	136	24	120
Degree of the Coefficients	44	5	19	14	46
Probability of Error	0.01 %	$2.\ 10^{-6}\%$	$2.\ 10^{-6}\%$	3 %	0.26 %
Time	2.6 h.	6 s.	8 m.	1 min.	6 h. (14 h.)
Magma (Gröbner)	∞	11 s.	> 5 h.	10 min.	∞

Figure 3: Computation over $\mathbb{Q}$

System	Birkhoff_3	Birkhoff_{10}	Bershenko	Hawes
Time	15 s.	20 min.	7 min.	15 h. (35 h.)
Magma (Gröbner)	5 min.	∞	∞	∞

- The next line gives the probability of error, if the $3m-1$ values are chosen uniformly in $\mathbb{F}_{10000000000000000051}$. We use the precise evaluation of the probability given in Section 5.
- The last lines in Figure 2 compare the running times of our algorithm with the time taken by Magma's Gröbner engine, on the field $k(P_1, \ldots, P_m)$, for a lexicographic ordering. We have used the factorization method described in Section 5.3.
- The two lines in Figure 3 give the times of the computation over $\mathbb{Q}$.
- In the last column, the figures in parentheses indicate the complexity of evaluation of the developed form of the system, and the corresponding computation times.

Our algorithm behaves very well, and outperforms the Gröbner basis computation proposed by Magma on all these examples. A more extensive list of examples is given in the paper [52] and the author's PhD. Thesis [58], and confirms its good behavior. For the biggest examples, the size of the output becomes the limiting factor: writing down the output of the system Hawes takes more than 20 MB.

The counterpart is a possibility of failure, but the estimates are quite reasonable: there is never more than a few percents of chance that the algorithm fails. When a verification was possible, it never revealed an error.

Finally, the influence of the complexity of evaluation L is predominant for the running time, as the example Hawes clearly shows: (almost) doubling the number of multiplications has the immediate effect of (almost) doubling the computation time. We stress that, as to no surprise, most applications we have met can be formulated in an easy-to-evaluate form, which is to the advantage of our method. Yet, we have observed that the modelization through a Computer Algebra system may spoil such good behavior, since most systems represent polynomials through the list of their coefficients on a monomial basis.

7 Conclusion

In this article, we have studied the geometry of parametric systems, proposed an elimination procedure adapted to such situations, and demonstrated its good practical behavior. Here are some directions for future work.

- As mentioned earlier, when the base field is $\mathbb{Q}$, the first task is to take modular computations into account, and in particular to quantify the new possibilities of degeneracy. This requires to use the arithmetic forms of the geometric results used here; the kind of results we need is given for instance in [38]; the subsequent algorithm is given in the author's PhD. Thesis [58].

- Our algorithm works only for the components were the Jacobian determinant is generically invertible. Recently, G. Lecerf proposed in [41] an extension of the Newton lifting process for multiple components, whose projection on the parameter space is dominant and generically finite. This new tool will enable a extension of our algorithm to the general case.

- Finally, we do not yet make use of the full strength of our Newton operator, which applies for more general representations than those based on primitive elements. A natural generalization of our algorithm is to use an encoding of the output by *triangular sets*. We refer to [59], where these aspects are developed.

References

[1] Jean-Charles Faugère's homepage. http://posso.lip6.fr/ jcf/.

[2] Magma. http://www.maths.usyd.edu.au:8000/u/magma/.

[3] MEDICIS. http://www.medicis.polytechnique.fr/.

[4] Alonso, M. E., Becker, E., Roy, M.-F., and Wörmann, T. Zeros, multiplicities and idempotents for zero-dimensional systems. In *Proceedings of MEGA'94* (1996), vol. 142 of *Progress in Mathematics*, Birkhäuser, pp. 1–15.

[5] Bachmann, O., Dengel, M., Faugère, J.-C., Graebe, H.-G., and Schoenemann, H. The SymbolicData Project. http://symbolicdata.medicis.polytechnique.fr/.

[6] Baur, W., and Strassen, V. The complexity of partial derivatives. *Theoretical Computer Science 22* (1983), 317–330.

[7] Bershenko-Kogan, I. *Inductive approach to Cartan's Moving Frame Method with applications to classical invariant theory.* PhD thesis, University of Minesotta, 2000.

[8] Boulier, F., Lazard, D., Ollivier, F., and Petitot, M. Representation for the radical of a finitely generated differential ideal. In *Proceedings of ISSAC'95* (1995), ACM Press, pp. 158–166.

[9] Buchberger, B. Gröbner bases: An algorithmic method in polynomial ideal theory. In *Multidimensional System Theory.* Reidel, Dordrecht, 1985, pp. 374–383.

[10] Buchberger, B., Collins, G., and Loos, R., Eds. *Computer Algebra.* Springer Verlag, 1982.

[11] Bürgisser, P., Clausen, M., and Shokrollahi, M. A. *Algebraic Complexity Theory.* Springer, 1997.

[12] Canny, J. Some algebraic and geometric problems in PSPACE. In *Proceedings of the 20th ACM Symposium on Theory of Computation* (1988), pp. 460–467.

[13] Cohen, H. *Advanced Topics in computational number theory.* No. 193 in Graduate Texts in Mathematics. Springer-Verlag, 2000.

[14] Dellière, S. *Triangularisation de systèmes constructibles — Application à l'évaluation dynamique.* PhD thesis, Université de Limoges, 1999.

[15] Dixon, J. Exact solution of linear equations using p-adic expansions. *Numerische Mathematik 40* (1982), 137–141.

[16] Duval, D. *Diverses questions relatives au calcul formel avec des nombres algébriques.* PhD thesis, Université scientifique, technologique et médicale de Grenoble, 1987.

[17] Eisenbud, D. *Commutative Algebra with a view toward Algebraic Geometry.* No. 150 in Graduate Texts in Mathematics. Springer, 1996.

[18] Emiris, I., and Mourrain, B. Matrices in elimination theory. *Journal of Symbolic Computation 28*, 1–2 (1999).

[19] Emiris, I., and Rege, A. Monomial bases and polynomial system solving. In *Proceedings of ISSAC'94* (1994), ACM Press, pp. 114–122.

[20] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra 139*, 1–3 (1999), 61–88.

[21] Faugère, J.-C., Gianni, P., Lazard, D., and Mora, T. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation 16*, 4 (1993), 329–344.

[22] Fitzpatrick, P., and Flynn, J. A Gröbner basis technique for Padé approximation. *Journal of Symbolic Computation 13* (1992), 133–138.

[23] Gaudry, P., and Harley, R. Counting points on hyperelliptic curves over finite fields. In *Proceedings of ANTS IV* (2000), no. 1838 in Lecture Notes in Computer Science, pp. 313–332.

[24] Gianni, P., and Mora, T. Algebraic solution of systems of polynomial equations using Gröbner bases. In *Proceedings of AAECC-5* (1989), vol. 356 of *Lecture Notes in Computer Science*, Springer, pp. 247–257.

[25] Giusti, M., Hägele, K., Heintz, J., Morais, J.-E., Montaña, J.-L., and Pardo, L.-M. Lower bounds for Diophantine approximation. In *Proceedings of MEGA'96* (1997), no. 117, 118 in Journal of Pure and Applied Algebra, pp. 277–317.

[26] Giusti, M., Heintz, J., Morais, J.-E., Morgenstern, J., and Pardo, L.-M. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra 124* (1998), 101–146.

[27] Giusti, M., Heintz, J., Morais, J.-E., and Pardo, L.-M. When polynomial equation systems can be solved fast? In *Proceedings of AAECC-11* (1995), vol. 948 of *Lecture Notes in Computer Science*, Springer, pp. 205–231.

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

[29] Gomez-Diaz, T. *Quelques applications de l'évaluation dynamique*. PhD thesis, Université de Limoges, 1994.

[30] Gonzalez-Vega, L. *Computer Algebra in Science and Engineering*. World Scientific Publishing, 1995, ch. Some examples of problem solving by using the symbolic viewpoint when dealing with polynomial systems of equations, pp. 102–116.

[31] Gonzalez-Vega, L. Applying quantifier elimination to the Birkhoff interpolation problem. *Journal of Symbolic Computation 22* (1996), 83–104.

[32] Grigoriev, D., and Vorobjov, N. Bounds on numbers of vectors of multiplicities for polynomials which are easy to compute. In *Proceedings of ISSAC 2000* (2000), ACM Press, pp. 137–145.

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

[34] Heintz, J., Krick, T., Puddu, S., Sabia, J., and Waissbein, A. Deformation techniques for efficient polynomial equation solving. *Journal of Complexity 16*, 1 (2000), 70–109.

[35] Heintz, J., Matera, G., and Waissbein, A. On the time-space complexity of geometric elimination procedures. *Applicable Algebra in Engineering, Communication and Computing 11* (2001), 239–296.

[36] Heintz, J., Roy, M.-F., and Solernó, P. On the complexity of semi-algebraic sets. In *Proc. IFIP 89, San Francisco* (1989), North-Holland, pp. 293–298.

[37] Heintz, J., Roy, M.-F., and Solernó, P. On the theoretical and practical complexity of the existential theory of the reals. *Comput. J. 36*, 5 (1993), 427–431.

[38] Krick, T., Pardo, L. M., and Sombra, M. Sharp estimates for the arithmetic Nullstellensatz. In *Proceedings of EACA'99* (1999).

[39] Kronecker, L. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. reine angew. Math. 92* (1882), 1–122.

[40] Lecerf, G. *Kronecker, a package for Magma for polynomial system solving.* UMS MEDICIS, Laboratoire GAGE, http://kronecker.medicis.polytechnique.fr/, 1999.

[41] Lecerf, G. Quadratic Newton iteration for systems with multiplicity. Manuscript, Laboratoire GAGE, École polytechnique, France, April 2001.

[42] Lecerf, G., and Schost, É.. Fast multivariate power series multiplication in characteristic zero. Manuscript, Laboratoire GAGE, École polytechnique, France, April 2001.

[43] Leverrier, U. J. J. Sur les variations séculaires des éléments elliptiques des sept planètes principales: Mercure, Venus, la terre, Mars, Jupiter, Saturne et Uranus. *Journal de Mathématiques Pures et Appliquées 4* (1840), 220–254.

[44] Macaulay, F. S. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.

[45] Montes, A. A new algorithm for discussing Gröbner bases with parameters. *Journal of Symbolic Computation 33*, 2 (2002), 183–208.

[46] Morrison, S. The differential ideal $[P] : M^\infty$. *Journal of Symbolic Computation 28* (1999), 631–656.

[47] Mourrain, B., and Pan, V. Multivariate polynomials, duality and strucured matrices. *Journal of Complexity 16*, 1 (2000).

[48] Renegar, J. On the computational complexity and geometry of the first-order theory of the reals. Part I. *Journal of Symbolic Computation 13*, 3 (1992), 255–299.

[49] ROJAS, J. Computing complex dimension faster and deterministically. Tech. rep., Department of Mathematics, City University of Hong Kong, 2000.

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

[51] ROUILLIER, F., ROY, M., AND SAFEY EL DIN, M. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *Journal of Complexity 16*, 4 (2000), 716–750.

[52] ROUILLIER, F., SAFEY EL DIN, M., AND SCHOST, É. Solving the Birkhoff interpolation problem via the critical point method : an experimental study. In *Proceedings of ADG 2000* (2001), vol. 2061 of *Lecture Notes in Artificial Intelligence*, Springer-Verlag.

[53] SABIA, J., AND SOLERNÓ, P. Bounds for traces in complete intersections and degrees in the Nullstellensatz. *Applicable Algebra in Engineering Communications and Computing 6* (1996), 353–376.

[54] SAKATA, S. Extension of the Berlekamp-Massey algorithm to n dimensions. *Information and Computation 84* (1990), 207–239.

[55] SCHÖNHAGE, A. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica*, 7 (1977), 395–398.

[56] SCHÖNHAGE, A., AND STRASSEN, V. Schnelle Multiplikation großer Zahlen. *Computing 7* (1971), 281–292.

[57] SCHOOF, R. Elliptic curves over finite fields and the computation of square roots mod *p*. *Mathematics of Computation 44* (1985), 483–494.

[58] SCHOST, É.. *Sur la résolution des systèmes polynomiaux à paramètres.* PhD thesis, École polytechnique, 2000.

[59] SCHOST, É. Degree bounds and lifting techniques for triangular sets. In *Proceedings of ISSAC 2002* (2002).

[60] SCHWARTZ, J. T. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM 27*, 4 (1980), 701–717.

[61] SHOUP, V. Efficient computation of minimal polynomials in algebraic extensions of finite fields. In *Proceedings of ISSAC'99* (1999), ACM Press, pp. 53–58.

[62] THUE, A. Et par andtydninger til en talteoretisk methode. *Christiana 7* (1902).

[63] TRINKS, W. On improving approximate results of Buchberger's algorithm by Newton's method. In *Proceedings of EUROCAL'85* (1985), no. 204 in Lecture Notes in Computer Science, Springer-Verlag, pp. 608–611.

[64] von zur Gathen, J., and Gerhard, J. *Modern computer algebra.* Cambridge University Press, 1999.

[65] Weispfenning, V. Comprehensive Gröbner bases. *Journal of Symbolic Computation 14*, 1 (1992), 1–30.

[66] Winkler, F. A p-adic approach to the computation of Gröbner bases. *Journal of Symbolic Computation 6* (1988), 287–304.

[67] Zippel, R. Probabilistic algorithms for sparse polynomials. In *Proceedings of EUROSAM'79* (1979), no. 72 in Lecture Notes in Computer Science, Springer, pp. 216–226.