Complexity Results for Triangular Sets

Éric Schost

Laboratoire GAGE, École polytechnique, 91128 Palaiseau Cedex, France

Abstract

We study the representation of the solutions of a polynomial system by triangular sets, and concentrate on the positive-dimensional case. We reduce to dimension zero by placing the free variables in the base field, so the solutions can be represented by triangular sets with coefficients in a rational function field.

We give intrinsic-type bounds on the degree of the coefficients in such a triangular set, and on the degree of an associated degeneracy hypersurface. Then we show how to apply lifting techniques in this context, and point out the role played by the evaluation properties of the input system.

Our algorithms are implemented in Magma; we present three applications, relevant to geometry and number theory.

Key words: triangular sets, complexity, symbolic Newton operator

1 Introduction

This article studies the triangular representation of the solutions of a polynomial system. Our first focus is on complexity results and algorithms; we also present a series of applications that were treated with these techniques. To make things clear, let us first display a concrete example of a triangular set.

An example in $\mathbb{Q}[X_1, X_2]$. Consider the polynomial system in $\mathbb{Q}[X_1, X_2]$:

$$F_1 = -X_1^3X_2 + 2X_1^2 - 4X_1X_2^2 + 2X_1X_2 - 2, \quad F_2 = X_1^2X_2 - X_1 + 4X_2^2 - 2X_2.$$

Email address: Eric.Schost@polytechnique.fr (Éric Schost).

It admits the following Gröbner basis for the lexicographic order $X_1 < X_2$:

$$\begin{aligned} T_1 &= X_1^2 - 2, \\ T_2 &= X_2^2 - \tfrac{1}{4} X_1. \end{aligned}$$

Since T_1 is in $\mathbb{Q}[X_1]$ and T_2 in $\mathbb{Q}[X_1, X_2]$, we say that (T_1, T_2) form a *triangular set*. In particular, T_1 describes the projection of the zero-set of (F_1, F_2) on the X_1-axis.

From the field-theoretic point of view, the system (F_1, F_2) generates a prime zero-dimensional ideal, so $\mathbb{Q} \to B := \mathbb{Q}[X_1, X_2]/(F_1, F_2)$ defines a field extension. We let x_1, x_2 be the images of X_1, X_2 in B; then T_1 is the minimal polynomial of x_1 in $\mathbb{Q} \to B$ and T_2, seen in $\mathbb{Q}(x_1)[X_2]$, is the minimal polynomial of x_2 in $\mathbb{Q}(x_1) \to B$.

Generalization and first complexity considerations. Consider now an arbitrary field $\mathfrak{K}$, $\overline{\mathfrak{K}}$ its algebraic closure, and a zero-dimensional variety $\mathfrak{W} \subset \mathbb{A}^n(\overline{\mathfrak{K}})$ defined over $\mathfrak{K}$. For simplicity, we take $\mathfrak{W}$ irreducible over $\mathfrak{K}$; then just as above, the ideal defining $\mathfrak{W}$ admits the following Gröbner basis for the lexicographic order $X_1 < \cdots < X_n$:

$$\begin{aligned} &T_1(X_1), \\ &T_2(X_1, X_2), \\ &\vdots \\ &T_n(X_1, \ldots, X_n), \end{aligned}$$

with T_k in $\mathfrak{K}[X_1, \ldots, X_k]$, and monic in X_k, for $k \leq n$. We will use this as an intuitive definition of a triangular set for the rest of this informal introduction. Note that if $\mathfrak{W}$ is not irreducible, its defining ideal might not have such a triangular family of generators: several triangular sets may be necessary.

For $k \leq n$, the family $T_1, \ldots, T_k$ describes the projection of $\mathfrak{W}$ on the affine subspace of coordinates $X_1, \ldots, X_k$. In particular, as above, T_1 is the minimal polynomial of X_1 modulo the ideal defining $\mathfrak{W}$. This close link between projections and triangular representations is central in what follows.

Let us turn to complexity considerations. The product of the degrees of the polynomials T_k in their "main variable" $\Pi_{k \leq n} \deg_{X_k} T_k$ equals the number of points in $\mathfrak{W}$, and bounds the total degree of each polynomial T_k. Thus, in terms of degrees in the variables $X_1, \ldots, X_n$, there is not much more to say.

New questions arise when the base field $\mathfrak{K}$ is endowed with a "size" function: if $\mathfrak{K}$ is a rational function field, we may consider the degree of its elements;

if $\mathfrak{K}$ is a number field, we can talk about the height of its elements. In this context, it becomes natural to ask how the size of the coefficients in $T_1, \ldots, T_n$ relates to some invariants measuring the "complexity" of the variety $\mathfrak{W}$. In view of the above remarks, a more accurate question is actually, for $k \leq n$, the relation between the size of the coefficients in $T_1, \ldots, T_k$ and the complexity of the projection of $\mathfrak{W}$ on the subspace of coordinates $X_1, \ldots, X_k$.

In this article, we focus on this question in the function field case. Here is the concrete situation from where the question originates.

Polynomial systems with parameters. A variety of problems can be described by polynomial systems involving free variables, or parameters. In such situations, we also often know that there are only finitely many solutions for a generic choice of the parameters.

In other words, we are considering systems that are zero-dimensional over the field of rational functions on some parameter space; triangular sets with rational functions coefficients can then be used to represent their solutions. The following applications motivated this approach; they are detailed in Section 8.

- *Modular equations.* In Gaudry and Schost [2002], we propose a definition of modular equations for hyperelliptic curves, with a view towards point-counting applications. For a given curve, these equations come from the resolution of zero-dimensional polynomial systems, as the minimal polynomial of one of the unknowns. Thus, they can be obtained from a triangular set computation, as in the introductory example.

  An interesting question is that of modular equations for a curve with generic coefficients, which can be precomputed and stored in a database. This was already done in the elliptic case, and is now done for a first hyperelliptic modular equation in the Magma package `CrvHyp`. This naturally raises the question of triangular sets with coefficients in a rational function field.
- *Curves with split Jacobian.* Curves of genus 2 with (2,2)-split Jacobian are of interest in number theory: over $\mathbb{Q}$, torsion, rank and cardinality records are obtained for such curves, see Kulesz [1995, 1999], Howe et al. [2000]. Roughly speaking, these curves are characterized by the presence of elliptic quotients of degree 2 of their Jacobian.

  We studied such curves in Gaudry and Schost [2001], and showed that the elliptic quotients can be read off triangular sets coming from the resolution of a suitable polynomial system. Classification questions require treating this question for curves with generic coefficients, which leads again to the problem of computing triangular sets over a rational function field.
- *Implicitization.* Finally, we will show that the implicit equation of a parametrized surface in $\mathbb{R}^3$ can be obtained using the triangular representation.

Contrary to the above, this question is not *a priori* formalized in terms of a parametric system. Nevertheless, this question actually reduces to the computation of a minimal polynomial over the rational function field $\mathbb{Q}(x_1, x_2)$, which can be done using triangular sets.

These examples share the following property: only a partial information, such as a specific eliminating polynomial, is really wanted. We now see how triangular sets can answer this question with good complexity.

Overview of our results. The above discussion is formalized as follows: we consider a polynomial system $\mathbf{F}$ defined over a field $\mathcal{K}$, depending on m parameters $P_1, \ldots, P_m$ and n unknowns $X_1, \ldots, X_n$. Geometrically speaking, $\mathbf{F}$ defines a variety $\mathcal{W}$ of dimension m in $\mathbb{A}^{m+n}(\overline{\mathcal{K}})$ and generates a zero-dimensional ideal, when extended over the field of rational functions on $\mathbb{A}^m(\overline{\mathcal{K}})$. Then its "generic solutions" can be represented by a family of triangular sets with coefficients in this rational function field.

For this short overview, we assume that the generic solutions are represented by a single triangular set $T_1, \ldots, T_n$. Using additional regularity hypotheses, we will answer the following questions: How do the degrees in this triangular set relate to geometric degrees? How accurately does this triangular set describe the solutions of the parametric system $\mathbf{F}$? How fast can it be computed?

- *Degree bounds.* The coefficients of $T_1, \ldots, T_n$ are rational functions in the free variables $P_1, \ldots, P_m$. We first show that their degrees are bounded by intrinsic geometric degrees, that is, independently of the Bézout number of the system $\mathbf{F}$. Precisely, for $k \leq n$, the coefficients of $T_1, \ldots, T_k$ have degree bounded in terms only of the degree of the projection $\mathcal{W}_k$ of $\mathcal{W}$ on the space of coordinates $P_1, \ldots, P_m, X_1, \ldots, X_k$. The precise bound is of order $(\deg \mathcal{W}_k)^k$.
- *Geometric degree of the degeneracy locus.* A triangular set with coefficients in a rational function field describes generic solutions. Thus, there is an open subset in the parameter space where none of the denominators of these rational functions vanishes, and where their specialization gives a description the solutions of the parametric system $\mathbf{F}$.

  We show that the locus where the specialization fails is contained in an hypersurface whose degree is quadratic in the geometric degree of $\mathcal{W}$. Note the difference with the above degree bounds, which are not polynomial in this degree. The analysis of the probabilistic aspects of our algorithms are based on this result.
- *Algorithms.* Triangular sets are useful for structured problems. For instance, all the above examples can be reduced to the computation of the first k polynomials $T_1, \ldots, T_k$, for some $k \leq n$. We give probabilistic algorithms for computing these polynomials, whose complexity is polynomial in the

size of the output. Using the above upper bound, the complexity actually depends on the degree of the projection $\mathcal{W}_k$ of $\mathcal{W}$ on the space of coordinates $P_1, \ldots, P_m, X_1, \ldots, X_k$, but not on the degree of $\mathcal{W}$ itself.

Note nevertheless that our complexity results comprise an additional factor which is exponential in n, inherent to computations with triangular sets.

Following the series of articles Giusti et al. [1995, 1997, 1998], Heintz et al. [2000], Giusti et al. [2001], Heintz et al. [2001], our algorithms rely on symbolic Newton lifting techniques and the Straight-Line Program representation of polynomials. Their practical behavior matches their good complexity, as they enabled to solve problems that were otherwise out-of-reach.

Comparison with primitive elements techniques. This work is in the continuation of Schost [2003], which focuses on a representation by primitive element techniques, the *geometric resolution*, in a similar context. Caution must be taken when comparing the two approaches. They answer different questions; as such, their complexities cannot be compared directly, since they are stated in terms of different quantities.

We use again the above notation: the geometric object of interest is a variety $\mathcal{W}$ defined by polynomials in $\mathcal{K}[P_1, \ldots, P_m, X_1, \ldots, X_n]$, and for $k \leq n$, $\mathcal{W}_k$ is its projection on the space of coordinates $P_1, \ldots, P_m, X_1, \ldots, X_k$.

The degree bound of the coefficients in a geometric resolution is linear in the degree of $\mathcal{W}$. This is to be compared with the results for the triangular representation, which are not polynomial in this degree. On the other hand, triangular sets take into account the degrees of the successive projections $\mathcal{W}_k$, which cannot be reached using a primitive element. These degrees can be arbitrarily smaller than the degree of $\mathcal{W}$, making the interest of the triangular representation.

Consider now the algorithmic aspect. The algorithm in Schost [2003] computes a parametric geometric resolution with a complexity that depends on the degree of $\mathcal{W}$. The algorithms proposed here compute k polynomials $T_1, \ldots, T_k$, for any given $k \leq n$; their complexity depends on the degree of the corresponding projection $\mathcal{W}_k$ of $\mathcal{W}$ on the space of coordinates $(P_1, \ldots, P_m, X_1, \ldots, X_k)$, but not on the degree of $\mathcal{W}$. Again, this suggests that triangular sets are of interest for problems with a structure, where projections might induce degree drops. We refer to Section 8 for a practical confirmation for several applications.

Related work. In dimension zero, a landmark paper for the triangular representation is Lazard [1992]. Our definition of triangular sets is inspired by

the one given there, as is the treatment of more technical questions such as splitting and combining triangular sets.

In arbitrary dimension, several notions of triangular sets and algorithms exist, see Lazard [1991], Kalkbrener [1991], Maza [1997], Aubry [1999], Dellière [1999], Szanto [1999]. For a comparison of some of these approaches, see Aubry et al. [1999]; we also refer to the detailed survey of Hubert. Our choice to reduce the question to dimension zero over a field of rational functions yields algorithms with good complexity, and easy to implement. Yet, our output is not as strong as for instance that of Lazard [1991], Maza [1997], Dellière [1999]: ours is only generically valid.

Upper bounds on the degrees of the polynomials in a triangular set were given in Gallo and Mishra [1990] and Szanto [1999]; we recall these results in the next section. In particular, the approach of Gallo and Mishra [1990] inspired Theorem 1 below. We also use results from Schost [2003], which follow notably Sabia and Solernó [1996].

Lifting techniques for polynomial systems were introduced in Trinks [1985], Winkler [1988]. They were used again in the series of articles by Giusti, Heintz, Pardo and collaborators, Giusti et al. [1995, 1997, 1998], Heintz et al. [2000], Giusti et al. [2001], Heintz et al. [2001]. The conjoint use of the Straight-Line Program representation led there to algorithms with the best known complexity for primitive element representations. The present work is in the continuation of the above; see also the survey of Pardo [1995] for a historical presentation of the use of Straight-Line Programs in elimination theory. Finally, let us mention the results of Lecerf [2002], which extend lifting techniques to situations with multiplicities.

We note that the article Heintz et al. [2000] precedes Schost [2003] and the present work, and considers similar questions of parametric systems. Nevertheless, we noted in Schost [2003] that the geometric hypotheses made in that article are not satisfied in many "real life" applications, and this is again the case for the applications treated here.

It should be noted that our complexity statements are of an *arithmetic* nature, that is, we only estimate the number of base field operations. When the base field is the rational field, the notion of *binary complexity* will give a better description of the expected computation time. We have not developed this aspect, which requires arithmetic-geometric considerations. We refer to Krick and Pardo [1996], Giusti et al. [1997], Krick et al. [2001] where such ideas are presented.

This work is based on a shorter version published in Schost [2002]. The degree bounds given here are sharper. The whole analysis of the degeneracy locus and the subsequent error probability analyses for the algorithms are new. The

complexity results are now precisely stated in terms of basic polynomial and power series arithmetic.

Acknowledgements. I wish to thank L.M. Pardo for his useful remarks on the first version of this paper.

2 Notation, Main Results

Triangular sets in dimension zero. We first define triangular sets over a ring R. Our definition is directly inspired by that of reduced triangular sets given in Lazard [1992]: a *triangular set* is a family of polynomials $\mathbf{T} = (T_1, \ldots, T_n)$ in $R[X_1, \ldots, X_n]$ such that, for $k \leq n$:

- T_k depends only on $X_1, \ldots, X_k$,
- T_k is monic in X_k,
- T_k has degree in X_j less than the degree in X_j of T_j, for all $j < k$.

Let now $\mathfrak{K}$ be a field, $\overline{\mathfrak{K}}$ its algebraic closure and $\mathfrak{W} \subset \mathbb{A}^n(\overline{\mathfrak{K}})$ a zero-dimensional variety. Recall that $\mathfrak{W}$ is *defined over* $\mathfrak{K}$ if its defining ideal in $\overline{\mathfrak{K}}[X_1, \ldots, X_n]$ is generated by polynomials in $\mathfrak{K}[X_1, \ldots, X_n]$.

In this case, a family $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$ of triangular sets with coefficients in $\mathfrak{K}$ *represents* the points of $\mathfrak{W}$ if the radical ideal defining $\mathfrak{W}$ in $\overline{\mathfrak{K}}[X_1, \ldots, X_n]$ is the intersection of the ideals generated by $\mathbf{T}^1, \ldots, \mathbf{T}^J$, and if for $j \neq j'$, $\mathbf{T}^j$ and $\mathbf{T}^{j'}$ have no common zero.

In this situation, all ideals $(\mathbf{T}^j)$ are radical by the Chinese Remainder Theorem. We then relate the degrees of the polynomials in the family $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$ and the cardinality of $\mathfrak{W}$:

- If $\mathfrak{W}$ is irreducible, the family $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$ is actually reduced to a single triangular set $\mathbf{T} = (T_1, \ldots, T_n)$ and the product $\Pi_{k \leq n} \deg_{X_k} T_k$ is the cardinality of $\mathfrak{W}$. Here, $\deg_{X_k} T_k$ denotes the degree of T_k in the variable X_k.
- If $\mathfrak{W}$ is not irreducible, a family $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$ satisfying our conditions exists but is not unique [Lazard, 1992, Proposition 2 and Remark 1]; now the sum $\sum_{j \leq J} \Pi_{k \leq n} \deg_{X_k} T_k^j$ is the cardinality of $\mathfrak{W}$. Hereafter, note that the superscript in the notation T_k^j does *not* denote a j-th power.

Note that it necessary to work over the algebraically closed field $\overline{\mathfrak{K}}$, or more generally to impose separability conditions, to obtain equalities as above, relating the degrees in the triangular sets $\mathbf{T}$ or $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$ and the number of

points in the variety $\mathfrak{W}$.

The basic geometric setting. We now turn to more geometric considerations. All along this article, we fix a field $\mathcal{K}$, $\overline{\mathcal{K}}$ its algebraic closure, and work in the affine space $\mathbb{A}^{m+n}(\overline{\mathcal{K}})$. We denote by $\mathbf{P} = P_1, \ldots, P_m$ the first m coordinates in $\mathbb{A}^{m+n}(\overline{\mathcal{K}})$ and by $\mathbf{X} = X_1, \ldots, X_n$ the last n coordinates. We use the notion of geometric degree of an arbitrary affine variety (not necessarily irreducible, nor even equidimensional), introduced in Heintz [1983].

In what follows, the affine space $\mathbb{A}^{m+n}(\overline{\mathcal{K}})$ is endowed with two families of projections. For $k \leq n$, we define μ_k and π_k as follows; hereafter, $\mathbf{p}$ denotes a point in $\mathbb{A}^m(\overline{\mathcal{K}})$.

$$\begin{array}{rccc} \mu_k : & \mathbb{A}^{m+n}(\overline{\mathcal{K}}) & \to & \mathbb{A}^{m+k}(\overline{\mathcal{K}}) \\ & (\mathbf{p}, x_1, \ldots, x_n) & \mapsto & (\mathbf{p}, x_1, \ldots, x_k) \end{array} \qquad \begin{array}{rccc} \pi_k : & \mathbb{A}^{m+k}(\overline{\mathcal{K}}) & \to & \mathbb{A}^m(\overline{\mathcal{K}}) \\ & (\mathbf{p}, x_1, \ldots, x_k) & \mapsto & \mathbf{p}. \end{array}$$

Note in particular that π_n maps the whole space $\mathbb{A}^{m+n}(\overline{\mathcal{K}})$ to $\mathbb{A}^m(\overline{\mathcal{K}})$.

The main geometric object is a m-dimensional variety $\mathcal{W} \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$. Our first results are of an intrinsic nature, so we do not need an explicit reference to a defining polynomial system. The assumptions on $\mathcal{W}$ follow the description made in the introduction:

Assumption 1 *Let $\{\mathcal{W}^j\}_{j \leq J}$ denote the irreducible components of $\mathcal{W}$. We assume that for $j \leq J$:*

(1) the image $\pi_n(\mathcal{W}^j)$ is dense in $\mathbb{A}^m(\overline{\mathcal{K}})$.
(2) the extension $\overline{\mathcal{K}}(P_1, \ldots, P_m) \to \overline{\mathcal{K}}(\mathcal{W}^j)$ is separable.

Assumption 1.1 implies that the fibers of the restriction of π_n to each component of $\mathcal{W}$ are generically finite; this justifies treating the first m coordinates as distinguished variables and calling them *parameters*. Assumption 1.2 is of a more technical nature, and will help to avoid many difficulties; it is always satisfied in characteristic zero.

Under Assumption 1, we can define the *generic solutions* of the variety $\mathcal{W}$. Let $\mathcal{J} \subset \overline{\mathcal{K}}[\mathbf{P}, \mathbf{X}]$ be the radical ideal defining $\mathcal{W}$ and $\mathcal{J}_P$ its extension in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$. We call *generic solutions* of $\mathcal{W}$ the roots of $\mathcal{J}_P$, which are in finite number.

We now refer to the previous paragraph, taking $\mathfrak{K} = \overline{\mathcal{K}}(\mathbf{P})$, and for $\mathfrak{W}$ the finite set of generic solutions. Using Assumption 1.2, the ideal $\mathcal{J}_P$ remains radical in $\overline{\mathfrak{K}}[\mathbf{X}]$, so the generic solutions are indeed defined over $\mathfrak{K} = \overline{\mathcal{K}}(\mathbf{P})$. Thus, they can be represented by a family of triangular sets in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$; our

purpose in this article is to study their complexity properties, and provide algorithms to compute with them.

Let us immediately note some particular cases:

- If $\mathcal{W}$ is irreducible, a single triangular set is enough to represent its generic solutions.
- If $\mathcal{W}$ is defined over $\mathcal{K}$, it can be written $\mathcal{W} = \cup_{j \leq J} \mathcal{W}^j$, where for all j, $\mathcal{W}^j$ is defined over $\mathcal{K}$, and the defining ideal of $\mathcal{W}^j$ is prime in $\mathcal{K}[\mathbf{P}, \mathbf{X}]$. Then the generic solutions of each $\mathcal{W}^j$ are represented by a triangular set in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$; the generic solutions of $\mathcal{W}$ are represented by their reunion.

Projections of $\mathcal{W}$. Before presenting the main results, we introduce some notation related to $\mathcal{W}$ and its successive projections. Let k be in $1, \ldots, n$. First of all, we denote by $\mathbf{X}_{\leq k}$ the first k variables $X_1, \ldots, X_k$; if $\mathbf{T}$ is a triangular set, $\mathbf{T}_{\leq k}$ is the sub-family $T_1, \ldots, T_k$.

We denote by $\mathcal{W}_k \subset \mathbb{A}^{m+k}(\overline{\mathcal{K}})$ the closure of $\mu_k(\mathcal{W})$, so in particular $\mathcal{W}_n$ coincides with $\mathcal{W}$. It is a routine check that for all k, $\mathcal{W}_k$ satisfies Assumption 1 as well.

Let $\mathcal{J}_k \subset \overline{\mathcal{K}}[\mathbf{P}, \mathbf{X}_{\leq k}]$ be the ideal defining $\mathcal{W}_k$, and $\mathcal{J}_{P,k}$ its extension in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$. Under Assumption 1.1, $\mathcal{J}_{P,k}$ coincides with $\mathcal{J}_P \cap \overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$. Thus if the generic solutions of $\mathcal{W}$ are defined by a triangular set $\mathbf{T}$, $\mathcal{J}_{P,k}$ is generated by $\mathbf{T}_{\leq k}$.

For $\mathbf{p}$ in $\mathbb{A}^m(\overline{\mathcal{K}})$, we denote by $\mathcal{W}_k(\mathbf{p})$ the fiber $\pi_k^{-1}(\mathbf{p}) \cap \mathcal{W}_k$ and by D_k the generic cardinality of the fibers $\mathcal{W}_k(\mathbf{p})$.

Finally, let B_k be the quotient $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]/\mathcal{J}_{P,k}$; by Assumption 1.2, the extension $\overline{\mathcal{K}}(\mathbf{P}) \to B_k$ is a product of separable field extensions. Using the separability, B_k has dimension D_k, by Proposition 1 in Heintz [1983].

Degree bounds. With this notation, we now present our main results. We assume that the generic solutions of $\mathcal{W}$ are represented by a triangular set $\mathbf{T} = (T_1, \ldots, T_n)$ in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$. In view of the above remarks, this is not a strong limitation: if this assumption is not satisfied, as soon as $\mathcal{W}$ is defined over $\mathcal{K}$, the following upper bounds apply to all the $\mathcal{K}$-defined irreducible components of $\mathcal{W}$.

As mentioned in the preamble, the degree bounds of $\mathbf{T}$ in the $\mathbf{X}$ variables are easily dealt with: for all $k \leq n$, the product $\Pi_{i \leq k} \deg_{X_i} T_i$ is the dimension of B_k over $\overline{\mathcal{K}}(\mathbf{P})$, that is, the generic cardinality D_k of the fibers $\mathcal{W}_k(\mathbf{p})$.

We will thus concentrate on the dependence with respect to the $\mathbf{P}$ variables. For $k \leq n$, the polynomial T_k depends only on the variables $X_1, \ldots, X_k$, and has coefficients in $\mathcal{K}(\mathbf{P}) = \mathcal{K}(P_1, \ldots, P_m)$. It is then natural to relate the degrees of these coefficients to the degree of the projection of $\mathcal{W}$ on the space of coordinates $P_1, \ldots, P_m, X_1, \ldots, X_k$, that is, $\mathcal{W}_k$.

This is the object of our first theorem. In all that follows, we call *degree* of a rational function the maximum of the degrees of its numerator and denominator.

Theorem 1 *Let $\mathcal{W}$ be a variety satisfying Assumption 1, and suppose that the generic solutions of $\mathcal{W}$ are represented by a triangular set $\mathbf{T}$ in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$. For $k \leq n$, all coefficients in T_k have degree bounded by $(2k^2+2)^k(\deg \mathcal{W}_k)^{2k+1}$.*

This result improves those of Gallo and Mishra [1990] and Szanto [1999] for respectively Ritt-Wu's and Kalkbrener's unmixed representations. If $\mathcal{W}$ is given as the zero-set of a system of n equations of degree d, then Gallo-Mishra's bound is $2n(8n)^{2n}d(d+1)^{4n^2}$ and Szanto's is $d^{O(n^2)}$.

With this notation, the Bézout inequality (Theorem 1 in Heintz [1983]) implies that the degree of $\mathcal{W}_k$ is at most d^n for all k. Thus according to Theorem 1, for $k \leq n$, in a worst-case scenario the coefficients in the polynomial T_k have degree bounded by $(2k^2+2)^k d^{2kn+n}$. Hence the estimate is better for low indices k than for higher indices; this contrasts with the previous results, which gave the same bounds for all T_k.

For the worst case $k = n$, our estimates are within the class $d^{2n^2+o(n^2)}$, to be compared with Gallo and Mishra's bound of $d^{4n^2+o(n^2)}$. Any of these bounds are polynomial in d^{n^2}; we do not know if this is sharp.

More importantly, Theorem 1 reveals that the degrees of the coefficients of $\mathbf{T}$ are controlled by the intrinsic geometric quantities $\deg \mathcal{W}_k$, rather than by the degrees of a defining polynomial system. For instance, this indicates a good behavior with respect to decomposition, e.g. into irreducible. Also, these degrees may be bounded *a priori*: in the example presented in Subsection 8.3, the Bézout bound is 1024, but an estimate based on the semantics of the problem gives $\deg \mathcal{W}_k \leq 80$.

Degree of the degeneracy locus. We still assume that the generic solutions of $\mathcal{W}$ are represented by a triangular set $\mathbf{T} = (T_1, \ldots, T_n)$ in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$. Since the coefficients of $\mathbf{T}$ are rational functions, there exists an open subset of the parameter space where they can be specialized, and give a description of the fibers of π_n. Theorem 2 below gives an upper bound on the degree of an hypersurface where this specialization fails.

Theorem 2 *Let $\mathcal{W}$ be a variety satisfying Assumption 1, and suppose that the generic solutions of $\mathcal{W}$ are represented by a triangular set $\mathbf{T}$ in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$. There exists a polynomial $\Delta_{\mathcal{W}} \in \overline{\mathcal{K}}[\mathbf{P}]$ of degree at most $(3n \deg \mathcal{W} + n^2) \deg \mathcal{W}$ such that, if $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ does not cancel $\Delta_{\mathcal{W}}$:*

(1) *$\mathbf{p}$ cancels no denominator in the coefficients of $(T_1, \ldots, T_n)$. We denote by $(t_1, \ldots, t_n) \subset \overline{\mathcal{K}}[\mathbf{X}]$ these polynomials with coefficients specialized at $\mathbf{p}$.*

(2) *$(t_1, \ldots, t_n)$ is a radical ideal. Let $Z_n \subset \mathbb{A}^n(\overline{\mathcal{K}})$ be the zero-set of the polynomials $(t_1, \ldots, t_n)$; then the fiber $\mathcal{W}_n(\mathbf{p})$ is $\{\mathbf{p}\} \times Z_n \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$.*

Just as Theorem 1, this result is of an intrinsic nature, since it depends only on geometric quantities. Nevertheless, in strong contrast with the previous result, these bounds are *polynomial* in the geometric degree of $\mathcal{W}$.

In particular, Theorem 2 shows that the *reunion of the zero-sets* of all denominators of the coefficients of $\mathbf{T}$ is contained in an hypersurface of degree bounded polynomially in terms of the degree of $\mathcal{W}$. Thus, the zero-set of any such denominator has degree bounded by the same quantity. Theorem 1 does not give such a polynomial bound for the *degrees* of the denominators. Were the upper bounds of Theorem 1 to be sharp, this would indicate that these denominators are (high) powers of polynomials of moderate degree.

Algorithms. The above results are purely geometric, and independent of any system of generators. For algorithmic considerations, we now assume that $\mathcal{W}$ is given as the zero-set of a polynomial system $\mathbf{F} = F_1, \ldots, F_n$ in $\mathcal{K}[\mathbf{P}, \mathbf{X}]$. We make the additional assumption that the Jacobian determinant with respect to $\mathbf{X}$ is invertible on a dense subset of $\mathcal{W}$. Then Assumption 1 is satisfied, and we consider the problem of computing triangular sets that represent the generic solutions of $\mathcal{W}$.

The underlying paradigm is that solving a zero-dimensional system over $\mathcal{K}$ by means of triangular sets is a well-solved task. Thus, the basic idea is first to specialize the indeterminates $\mathbf{P}$ in the system $\mathbf{F}$, and solve the corresponding system in the remaining variables $\mathbf{X}$, by means of triangular sets in $\mathcal{K}[\mathbf{X}]$. A lifting process then produces triangular sets with coefficients in a formal power series ring, from which we can recover the required information.

Our first contribution treats the case when $\mathcal{W}$ is irreducible: its generic solutions are then represented by a single triangular set $\mathbf{T} = (T_1, \ldots, T_n)$, and we propose a probabilistic algorithm that computes $T_1, \ldots, T_k$ for any k. If $\mathcal{W}$ is not irreducible, we compute the *minimal polynomial* of X_1 modulo the extended ideal $(F_1, \ldots, F_n)$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$, using similar techniques.

We do not treat the general question of computing a whole family of triangular

sets when $\mathcal{W}$ is not irreducible. From the practical point of view, this might not be a strong restriction: our results cover all the applications that we had to treat.

We use the following complexity notations:

- We suppose that $\mathbf{F}$ is given by a *Straight-Line Program* of size L, and that $F_1, \ldots, F_n$ have degree bounded by d.
- We say that f is in $O_{\log}(g)$ if there exists a constant a such that f is in $O(g \log(g)^a)$ — this is sometimes also expressed by the notation $f \in O^{\tilde{}}(g)$.
- $\mathcal{M}(D)$ denotes the cost of the multiplication of univariate polynomials of degree D, in terms of operations in the base ring. $\mathcal{M}(D)$ can be taken in $O(D \log D \log\log D)$, using the algorithm of Schönhage and Strassen [1971].

  We denote by C_0 a universal constant such that for any ring R, any integer D and any monic polynomial T in $R[X]$ of degree D, all operations $(+, \times)$ in $R[X]/(T)$ can be done in at most $C_0\mathcal{M}(D)$ operations, see Chapter 9 in [von zur Gathen and Gerhard, 1999].

  We assume that there exists constants C_1 and α such that $\mathcal{M}(D)\mathcal{M}(D') \leq C_1\mathcal{M}(DD')\log(DD')^\alpha$ holds for all D, D'. This assumption is satisfied for all commonly used multiplication algorithms.
- $\mathcal{M}_s(D, M)$ denotes the cost of M-variate series multiplication at precision D. This can be taken less than $\mathcal{M}((2D+1)^M)$ using Kronecker's substitution. If the base field has characteristic zero, this complexity becomes linear in the size of the series, up to logarithmic factors; see [Lecerf and Schost, 2003, Theorem 1].

  We assume that there exists a constant $C_2 < 1$ such that $\mathcal{M}_s(D, M) \leq C_2\mathcal{M}_s(2D, M)$ holds for all D and M. This is the case for all commonly used estimates, for instance for the ones mentioned above.

Apart from the above constants, the complexities below are stated in terms of the degrees $\mathfrak{D}_k$ of the rational functions that appear in the output, and the number D_n. This number was defined earlier as the generic cardinality of the fibers $\mathcal{W}_n(\mathbf{p})$; it is thus the generic number of solutions of the parametric system $\mathbf{F}$.

Theorem 3 *Assume that $\mathcal{W}$ is irreducible. Let $\mathbf{p}, \mathbf{p}'$ be in $\mathcal{K}^m$; assume that a description of the zeros of the systems $\mathbf{F}(\mathbf{p}, \mathbf{X})$, $\mathbf{F}(\mathbf{p}', \mathbf{X})$ by triangular sets is known. For $k \leq n$, let $\mathfrak{D}_k$ be the maximum of the degrees of the coefficients of $T_1, \ldots, T_k$. Then $T_1, \ldots, T_k$ can be computed within*

$$O_{\log}\Big((nL+n^3)(C_0C_1)^n\mathcal{M}(D_n)\mathcal{M}_s(4\mathfrak{D}_k, m)+km^2D_n\mathcal{M}(\mathfrak{D}_k)\mathcal{M}_s(4\mathfrak{D}_k, m-1)\Big)$$

operations in $\mathcal{K}$. The algorithm chooses $3m-1$ values in $\mathcal{K}$, including the coordinates of $\mathbf{p}$ and $\mathbf{p}'$. If Γ is a subset of $\mathcal{K}$, and these values are chosen in Γ^{3m-1}, then the algorithm fails for at most $50n(k^2+2)^{3k}d^{6kn+4n}|\Gamma|^{3m-2}$ choices.

Theorem 4 *Let $\mathbf{p}, \mathbf{p}'$ be in $\mathcal{K}^m$; assume that a description of the zeros of the systems $\mathbf{F}(\mathbf{p}, \mathbf{X})$, $\mathbf{F}(\mathbf{p}', \mathbf{X})$ by triangular sets which define prime ideals in $\mathcal{K}[\mathbf{X}]$ is known.*

Let $M_1 \in \overline{\mathcal{K}}(\mathbf{P})[U]$ be the minimal polynomial of X_1 modulo the extended ideal $(F_1, \ldots, F_n)$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$, and $\mathfrak{D}_1$ the maximum of the degrees of its coefficients. Then M_1 can be computed within

$$O_{\log}\Big((nL + n^3)(C_0C_1)^n \mathcal{M}(D_n)\mathcal{M}_s(4\mathfrak{D}_1, m) + m^2 D_n \mathcal{M}(\mathfrak{D}_1)\mathcal{M}_s(4\mathfrak{D}_1, m-1)\Big)$$

operations in $\mathcal{K}$. The algorithm chooses $3m-1$ values in $\mathcal{K}$, including the coordinates of $\mathbf{p}$ and $\mathbf{p}'$. If Γ is a subset of $\mathcal{K}$, and these values are chosen in Γ^{3m-1}, then the algorithm fails for at most $50nd^{4n}|\Gamma|^{3m-2}$ choices.

These complexities are polynomial with respect to the possible number of monomials in the output. The exponential terms $(C_0C_1)^n$ reflect the cost of computing modulo a triangular set with n elements.

Using Theorem 1, the above complexities are bounded in terms only of the degrees of the varieties $\mathcal{W}_k$ (for Theorem 3) and $\mathcal{W}_1$ (for Theorem 4). Triangular sets are thus useful when a partial information is required: they avoid taking the whole degree of the variety $\mathcal{W}$ into account, as would be the case using primitive element techniques.

Finally, note that we could give an alternative formulation for the estimates of probabilities. Referring for instance to Theorem 4, a probability of success greater than $1-\varepsilon$ can be obtained as soon as all random choices are made in a subset Γ of cardinality greater than $50nd^{4n}/\varepsilon$, assuming a uniform probability distribution.

Organization of the paper. Section 3 presents some auxiliary results for a primitive element representation, the geometric resolution, that are used later. In Section 4, we prove Theorem 1. Section 5 gives technical results that are used in Section 6 for proving Theorem 2. Our algorithms are presented in Section 7, and their applications are detailed in Section 8.

3 Geometric Resolutions

Our complexity results rely on another representation of the solutions of a polynomial system, the *geometric resolution*. We introduce this notion in Subsection 3.1. In Subsection 3.2, we present the complexity results that are used later; Subsection 3.3 is devoted to prove one of them.

3.1 Definition

The geometric resolution is a representation of a zero-dimensional variety by means of primitive element techniques. It was introduced under this denomination in Giusti et al. [1995, 1997, 1998, 2001]. See also Gianni and Mora [1989], Alonso et al. [1996], Rouillier [1999] for the use of primitive elements and related techniques for polynomial systems.

We first give the definition in a general setting. Let $\mathfrak{K}$ be any field and $\mathfrak{J}$ a radical zero-dimensional ideal of $\mathfrak{K}[X_1, \ldots, X_N]$. Then a *geometric resolution* of the extension $\mathfrak{K} \to \mathfrak{K}[X_1, \ldots, X_N]/\mathfrak{J}$, if it exists, consists in:

- a primitive element $\mathfrak{U} = \sum_{i=1}^{N} u_i X_i$ of the extension $\mathfrak{K} \to \mathfrak{K}[X_1, \ldots, X_N]/\mathfrak{J}$,
- its monic minimal polynomial $Q \in \mathfrak{K}[U]$,
- a parametrization of the variables X_i in terms of the primitive element.

In the separable case, when Q has no multiple root, it factors over an algebraic closure of $\mathfrak{K}$ as $\Pi(U - \mathfrak{U}(p))$, where p runs over the zero-set of $\mathfrak{J}$.

We use two different kinds of parametrizations for the algebraic variables. The first one takes the form

$$Q'(\mathfrak{U})X_1 = V_1(\mathfrak{U}), \quad \ldots \quad Q'(\mathfrak{U})X_N = V_N(\mathfrak{U});$$

it makes sense as soon as Q' is invertible modulo Q, *i.e.* in the separable case. The second type has the form

$$X_1 = W_1(\mathfrak{U}), \quad \ldots \quad X_N = W_N(\mathfrak{U}).$$

Even if the latter parametrization seems more natural, better complexity bounds are obtained for the former kind, as we will soon see. In any case, the polynomials Q, V_i and W_i have coefficients in the base field $\mathfrak{K}$.

Let us return to our specific problem, and consider again the m-dimensional variety $\mathcal{W} \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$. With the notation of the introduction, we will use geometric resolutions in the following contexts:

- We use the denomination *parametric resolution* when the base field is the rational function field $\overline{\mathcal{K}}(\mathbf{P})$, that is, to describe some generic solutions. We give complexity results for this situation in the next subsection.
- Given $k \leq n$ and a point $\mathbf{p}$ in $\mathbb{A}^m(\overline{\mathcal{K}})$ such that the fiber $\mathcal{W}_k(\mathbf{p})$ is finite, we may consider a *geometric resolution of the points in* $\mathcal{W}_k(\mathbf{p})$. This means that we will consider polynomials $q, w_1, \ldots, w_k$ in $\overline{\mathcal{K}}[U]$, such that q has no multiple root, and such that the $\mathbf{X}$-coordinates of the points in $\mathcal{W}_k(\mathbf{p})$ are defined by $q(\mathfrak{U}) = 0$ and $X_1 = w_1(\mathfrak{U}), \ldots, X_k = w_k(\mathfrak{U})$.

Our first complexity statement concerns the existence and the complexity of a parametric resolution for the varieties $\mathcal{W}_k$ (see Section 2 for the definition); we use it in the next section for proving Theorem 1. It is a slight extension of Proposition 2 in Schost [2003], which itself is inspired by Giusti et al. [1995] and Sabia and Solernó [1996].

Recall that for $k \leq n$, B_k is the quotient algebra $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]/\mathcal{J}_{P,k}$, where $\mathcal{J}_{P,k}$ is the extension of the ideal defining $\mathcal{W}_k$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$; D_k is the dimension of B_k as a $\overline{\mathcal{K}}(\mathbf{P})$-vector space.

Proposition 1 *Let k be in $1, \ldots, n$. There exists $(u_1, \ldots, u_k)$ in $\overline{\mathcal{K}}^k$ such that $\mathfrak{U} = \sum_{i=1}^k u_i X_i$ is a primitive element of B_k. Moreover, for any such primitive element, there exist polynomials $Q_k, V_1, \ldots, V_k$ in $\overline{\mathcal{K}}(\mathbf{P})[U]$ such that:*

- *Q_k has degree D_k and $V_1, \ldots, V_k$ have degree less than D_k.*
- *Q_k is the minimal polynomial of $\mathfrak{U}$ in B_k, and has no multiple root.*
- *The following relations hold in B_k:*

$$Q_k'(\mathfrak{U})X_1 = V_1(\mathfrak{U}), \quad \ldots \quad Q_k'(\mathfrak{U})X_k = V_k(\mathfrak{U}).$$

- *Let $\mathfrak{Q}_k, \mathfrak{V}_1, \ldots, \mathfrak{V}_k$ be the polynomials $Q_k, V_1, \ldots, V_k$ multiplied by the* LCM *of all denominators of their coefficients. Then the total degrees of these polynomials, seen in $\overline{\mathcal{K}}[\mathbf{P}, U]$, are bounded by $\deg \mathcal{W}_k$.*

A parametric resolution describes generic solutions, as it has coefficients in the rational function field $\overline{\mathcal{K}}(\mathbf{P})$; thus it can be specialized on an open subset of the parameter space. The following proposition gives an upper bound on the degree of an hypersurface where the specialization fails. This result is used in Section 6 for proving Theorem 2.

Proposition 2 *Let $\mathfrak{U} = \sum_{i=1}^n u_i X_i$ be a primitive element of B_n, Q_n its minimal polynomial and $W_1, \ldots, W_n$ the polynomials in $\overline{\mathcal{K}}(\mathbf{P})[U]$ of degree less than D_n such that the following relations hold in B_n:*

$$X_1 = W_1(\mathfrak{U}), \quad \ldots \quad X_n = W_n(\mathfrak{U}).$$

There exists a polynomial $\delta_{\mathcal{W}}$ in $\overline{\mathcal{K}}[\mathbf{P}]$ of degree at most $(2nD_n + n^2)\deg \mathcal{W}$ such that, if $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ does not cancel $\delta_{\mathcal{W}}$:

(1) $\mathbf{p}$ cancels no denominator in the coefficients of $Q_n, W_1, \ldots, W_n$. We let $q_n, w_1, \ldots, w_n$ be these polynomials with coefficients specialized at $\mathbf{p}$.
(2) The polynomials $q_n, w_1, \ldots, w_n$ form a geometric resolution for the fiber $\mathcal{W}_n(\mathbf{p})$.
(3) For $k \leq n$, the fiber $\mathcal{W}_k(\mathbf{p})$ has D_k points.

(4) For $k \leq n$, $\mathcal{W}_k(\mathbf{p})$ coincides with the projection $\mu_k(\mathcal{W}_n(\mathbf{p}))$.

The last part of this section is devoted to prove this proposition.

3.3 Proof of Proposition 2

The following proposition is a particular case of Proposition 1 in Schost [2003], which follows Proposition 1 in Sabia and Solernó [1996]. It leads to Corollary 1, which itself gives the proof of Proposition 2.

Proposition 3 *Let k be in $1, \ldots, n$. For $i \leq k$, let φ_i be the map*

$$\begin{aligned} \varphi_i : \quad \mathbb{A}^{m+k}(\overline{\mathcal{K}}) \quad &\to \mathbb{A}^{m+1}(\overline{\mathcal{K}}) \\ (\mathbf{p}, x_1, \ldots, x_k) &\mapsto (\mathbf{p}, x_i), \end{aligned}$$

and let $M_i \in \overline{\mathcal{K}}[\mathbf{P}, U]$ be a squarefree polynomial defining the closure of $\varphi_i(\mathcal{W}_k)$. Consider the polynomial M_i in $\overline{\mathcal{K}}[\mathbf{P}][U]$ and let $N_i \in \overline{\mathcal{K}}[\mathbf{P}]$ be its leading coefficient. Then $G_i = M_i/N_i \in \overline{\mathcal{K}}(\mathbf{P})[U]$ is the monic minimal polynomial of X_i in B_k.

Corollary 1 *Let k in $1, \ldots, n$, $\mathfrak{U} = \sum_{i=1}^{k} u_i X_i$ a primitive element of B_k, Q_k its minimal polynomial and $W_1, \ldots, W_k$ the polynomials in $\overline{\mathcal{K}}(\mathbf{P})[U]$ of degree less than D_k such that the following relations hold in B_k:*

$$X_1 = W_1(\mathfrak{U}), \quad \ldots \quad X_k = W_k(\mathfrak{U}).$$

There exists a polynomial δ_k in $\overline{\mathcal{K}}[\mathbf{P}]$ of degree at most $(2D_k + k)\deg \mathcal{W}_k$ such that, if $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ does not cancel δ_k:

- *$\mathbf{p}$ cancels no denominator in the coefficients of $Q_k, W_1, \ldots, W_k$. We let $q_k, w_1, \ldots, w_k$ be these polynomials with coefficients specialized at $\mathbf{p}$.*
- *The fiber $\mathcal{W}_k(\mathbf{p})$ is finite and has D_k points; $q_k, w_1, \ldots, w_k$ is a geometric resolution for this fiber. In particular, q_k has no multiple root.*

Proof. Let us first exclude the infinite fibers. We use the same notations as in Proposition 3: for $i \leq k$, G_i is the minimal polynomial of X_i in B_k. Then G_i can be written M_i/N_i, where M_i is primitive in $\overline{\mathcal{K}}[\mathbf{P}][U]$, and $N_i \in \overline{\mathcal{K}}[\mathbf{P}]$ is its leading coefficient. Using the previous proposition, N_i has degree at most $\deg \mathcal{W}_k$.

Let $N \in \overline{\mathcal{K}}[\mathbf{P}]$ be the product of all N_i, for $i \leq k$; then N has degree at most $k \deg \mathcal{W}_k$. Corollary 14.6 and the proof of Theorem 14.4 in [Eisenbud, 1996] show that if $\mathbf{p}$ does not cancel N, then the fiber $\mathcal{W}_k(\mathbf{p})$ is finite. Then

by Proposition 1 in Heintz [1983], this fiber has at most D_k points. We now suppose that we are in this situation.

Let f be a polynomial in the ideal $\mathcal{J}_k \subset \overline{\mathcal{K}}[\mathbf{P}, \mathbf{X}_{\leq k}]$ defining $\mathcal{W}_k$. Then f belongs to the extension $\mathcal{J}_{P,k} \subset \overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$ so there exist polynomials $(g_1, \ldots, g_{k+1})$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$ such that $f = \sum_{i=1}^{k} g_i(X_i - W_i(\mathfrak{U})) + g_{n+1}Q_k(\mathfrak{U})$. Let us now suppose that $\mathbf{p}$ cancels no denominator in the coefficients of $Q_k, W_1, \ldots, W_k$. Then $\mathbf{p}$ cancels no denominator in the previous equality. Specializing the variables $\mathbf{P}$ at $\mathbf{p}$ shows that $f(\mathbf{p}, \mathbf{X}_{\leq k})$ is in the ideal $(q_k(\mathfrak{U}), X_1 - w_1(\mathfrak{U}), \ldots, X_k - w_k(\mathfrak{U}))$. Thus the zero-set of these polynomials is contained in the fiber $\mathcal{W}_k(\mathbf{p})$.

Finally, suppose that $\mathbf{p}$ does not cancel the discriminant of Q_k, which is a non-zero polynomial by Proposition 1. Then q_k has D_k distinct roots; since $\mathcal{W}_k(\mathbf{p})$ has cardinality at most D_k, we conclude that $q_k, w_1, \ldots, w_k$ is a geometric resolution for the fiber $\mathcal{W}_k(\mathbf{p})$, as requested.

With the notations of Proposition 1, $\mathbf{p}$ satisfies the last conditions if it does not cancel the determinant δ of the Sylvester matrix associated to $\mathfrak{Q}_k$ and its derivative. We take $\delta_k = N\delta$; the degree estimates of Proposition 1 conclude the proof of the corollary. □

We now conclude the proof of Proposition 2. Let $\delta_{\mathcal{W}}$ be the product of all δ_k, for $k \leq n$. The estimates $D_k \leq D_n$ and $\deg \mathcal{W}_k \leq \deg \mathcal{W}_n$ prove points 1, 2, 3 of the proposition. To prove the last point, we note that the projection $\mu_k(\mathcal{W}_n(\mathbf{p}))$ is contained in $\mathcal{W}_k(\mathbf{p})$ for all $\mathbf{p}$; thus it is enough to exhibit conditions under which their cardinalities coincide.

Let $\mathfrak{U}$ be a linear form $\sum_{i=1}^{n} u_i X_i$ which generates B_n, Q_n its minimal polynomial and $W_1, \ldots, W_n$ the polynomials in $\overline{\mathcal{K}}(\mathbf{P})[U]$ such that the relations $X_1 = W_1(\mathfrak{U}), \ldots, X_n = W_n(\mathfrak{U})$ hold in B_n.

Consider also $k \leq n$, $\mathfrak{U}' = \sum_{i=1}^{k} u'_i X_i$ a linear form which generates B_k and Q_k its minimal polynomial. Then Q_k is the minimal polynomial of $\sum_{i=1}^{k} u'_i W_i$ modulo Q_n and has degree D_k.

Let $\mathbf{p}$ be in $\mathbb{A}^m(\overline{\mathcal{K}})$ and suppose that $\mathbf{p}$ cancels neither δ_k nor δ_n. Then by Corollary 1, $\mathcal{W}_k(\mathbf{p})$ has cardinality D_k. We now prove that the projection $\mu_k(\mathcal{W}_n(\mathbf{p}))$ has cardinality D_k, which will prove Proposition 2. To this effect, we apply Corollary 1 twice.

- Applied for index k, this shows that $\mathbf{p}$ cancels no denominator in the coefficients of Q_k, and that the specialized polynomial q_k has D_k distinct roots.
- For index n, Corollary 1 shows that $\mathbf{p}$ cancels no denominator in the coefficients of $Q_n, W_1, \ldots, W_n$ and the specialized polynomials $q_n, w_1, \ldots, w_n$

form a geometric resolution for the fiber $\mathcal{W}_n(\mathbf{p})$. Let Ξ be the characteristic polynomial of $\sum_{i=1}^{k} u_i' W_i$ modulo Q_n. Then $\mathbf{p}$ cancels no denominator in the coefficients of Ξ; specializing these coefficients at $\mathbf{p}$ yields the characteristic polynomial χ of $\sum_{i=1}^{k} u_i' w_i$ modulo q_n.

We now conclude the proof. Since Q_k is the square-free part of Ξ and q_k has D_k distinct roots, χ has D_k distinct roots. But this number of roots is precisely the cardinality of $\mu_k(\mathcal{W}_n(\mathbf{p}))$, so the proposition is proven. □

4 Degree Bounds: Proof of Theorem 1

In this section, we suppose that the generic solutions of $\mathcal{W}$ are represented by a triangular set $\mathbf{T} = (T_1, \ldots, T_n)$ in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$. For $k \leq n$, recall that $\mathcal{W}_k \subset \mathbb{A}^{m+k}(\overline{\mathcal{K}})$ is the closure of the projection $\mu_k(\mathcal{W})$. We now prove that all coefficients in T_k have degree bounded by $(2k^2+2)^k (\deg \mathcal{W}_k)^{2k+1}$.

The proof goes as follows: we first apply Proposition 1 to $\mathcal{W}_k$, deducing the existence of a suitable parametric resolution. Applying Proposition 4 given below, we obtain Bézout equalities of low degree relating this parametric resolution and the triangular set $(T_1, \ldots, T_k)$. Inspired by [Gallo and Mishra, 1990], we conclude by turning these relations into a linear system for the coefficients of $(T_1, \ldots, T_k)$, from which Theorem 1 follows.

First, we present the Bézout identities we will use. The following proposition is Lemma 5 in Krick et al. [1997]; similar results can be seen in Giusti et al. [1997], originating from Giusti et al. [1995].

Proposition 4 *Let $\mathfrak{K}$ be a field, and let $(F_1, \ldots, F_k)$ be a regular sequence in $\mathfrak{K}[X_1, \ldots, X_k]$. Let d be a bound on the degrees of the polynomials $\mathbf{F}$, and δ the maximum of the degrees of the varieties $\mathcal{V}(F_1, \ldots, F_k)$, for $i = 1, \ldots, k-1$.*

For $i = 0, \ldots, k-1$, let B_k^i be the quotient

$$\mathfrak{K}[X_1, \ldots, X_k]/(F_1, \ldots, F_{k-i}).$$

Assume that the extension $\mathfrak{K}[X_1, \ldots, X_i] \to B_k^i$ is integral and that the jacobian of $(F_1, \ldots, F_{k-i})$ with respect to $(X_{i+1}, \ldots, X_k)$ is a non-zero divisor in B_k^i. Then if H belongs to $(F_1, \ldots, F_k)$, there exists polynomials $(S_1, \ldots, S_k)$ in $\mathfrak{K}[X_1, \ldots, X_k]$ such that

$$H = S_1 F_1 + \cdots + S_k F_k$$

and, for $i = 1, \ldots, k$, $\deg S_i F_i \leq 2k^2 d\delta + \delta \max\{\deg H, d\}$.

With this proposition, we can prove Theorem 1. As before, we denote by $\mathcal{J}_k$ and $\mathcal{J}_{P,k}$ the ideal defining $\mathcal{W}_k$ in $\overline{\mathcal{K}}[\mathbf{P}, \mathbf{X}_{\leq k}]$ and its extension in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$. By Proposition 1, there exist $u_1, \ldots, u_k$ in $\overline{\mathcal{K}}$, and a family of polynomials $Q_k, V_1, \ldots, V_k$ in $\overline{\mathcal{K}}(\mathbf{P})[U]$ such that the ideal $\mathcal{J}_{P,k}$ is generated by

$$(Q_k(\mathfrak{U}), Q_k'(\mathfrak{U})X_k - V_k(\mathfrak{U}), \ldots, Q_k'(\mathfrak{U})X_1 - V_1(\mathfrak{U}))\,,$$

where $\mathfrak{U}$ is the linear form $\sum_{i=1}^{k} u_k X_k$. Without loss of generality, we can assume that the coefficient u_k is not zero. Then, the following family generates the ideal $\mathcal{J}_{P,k}$ as well:

$$\mathcal{R}: \quad (Q_k(\mathfrak{U}), Q_k'(\mathfrak{U})X_{k-1} - V_{k-1}(\mathfrak{U}), \ldots, Q_k'(\mathfrak{U})X_1 - V_1(\mathfrak{U}))\,.$$

We will consider the following families $\mathcal{R}_i$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$, for $0 \leq i \leq k-2$:

$$\mathcal{R}_i: \quad (Q_k(\mathfrak{U}), Q_k'(\mathfrak{U})X_{k-1} - V_{k-1}(\mathfrak{U}), \ldots, Q_k'(\mathfrak{U})X_{i+1} - V_{i+1}(\mathfrak{U}))\,,$$

and $\mathcal{R}_{k-1} = (Q_k(\mathfrak{U}))$. We now check the hypotheses of Proposition 4 for $\mathcal{R}_i$, with $\mathfrak{K} = \overline{\mathcal{K}}(\mathbf{P})$.

- By Proposition 1, Q_k' is invertible modulo Q_k so each equation $Q_k'(\mathfrak{U})X_i - V_i(\mathfrak{U})$ can be written $X_i - W_i(\mathfrak{U})$ modulo $Q_k(\mathfrak{U})$, for some polynomial W_i in $\overline{\mathcal{K}}(\mathbf{P})[U]$. This shows that $\mathcal{R}_i$ is a regular sequence.
- For i in $0, \ldots, k-1$, we define the ring B_k^i as $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]/\mathcal{R}_i$. Since the coefficient u_k is not zero, we deduce that for i in $0, \ldots, k-1$, B_k^i is an integral extension of $\overline{\mathcal{K}}(\mathbf{P})[X_1, \ldots, X_i]$.
- Finally, the jacobian determinant of $\mathcal{R}_i$ with respect to $X_{i+1}, \ldots, X_k$ is a constant multiple of $(k-1-i)$-th power of $Q_k'(\mathfrak{U})$, so it is invertible in B_k^i.

Thus, the hypotheses of Proposition 4 are satisfied; then we need some degree estimates to apply this proposition. Since the variables $\mathbf{P}$ are in the base field $\mathfrak{K} = \overline{\mathcal{K}}(\mathbf{P})$, we estimate all degrees in terms of the variables $\mathbf{X}_{\leq k}$ only. By Proposition 1, the degrees of all polynomials in $\mathcal{R}$ are bounded by $D_k \leq \deg \mathcal{W}_k$. The varieties $\mathcal{V}(\mathcal{R}_i)$ are cylinders built upon zero-dimensional varieties of degree at most $\deg \mathcal{W}_k$ over $\overline{\mathfrak{K}}$, so their degree is at most $\deg \mathcal{W}_k$.

The polynomials in $\mathcal{R}$ are in $\overline{\mathcal{K}}(\mathbf{P})[U]$, but we need equalities involving polynomials in $\overline{\mathcal{K}}[\mathbf{P}][U]$. Let thus $\mathfrak{Q}_k, \mathfrak{V}_1, \ldots, \mathfrak{V}_k$ be the polynomials $Q_k, V_1, \ldots, V_k$ multiplied by the LCM of the denominators of their coefficients. These polynomials satisfy the same properties as $Q_k, V_1, \ldots, V_k$. In particular, for $i \leq k$, there exist $S_{0,i}, \ldots, S_{k-1,i}$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$ such that the following equality holds in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$:

$$T_i = S_{0,i}\mathfrak{Q}_k(\mathfrak{U}) + \sum_{j=1}^{k-1} S_{j,i}\Big(\mathfrak{Q}_k'(\mathfrak{U})X_i - \mathfrak{V}_i(\mathfrak{U})\Big) \tag{1}$$

Let us fix i, and apply Proposition 4. Our conventions on the elements of a triangular set show that the degree of T_i in $\mathbf{X}_{\leq k}$ is at most $\deg \mathcal{W}_k$. Proposition 4 then shows that the degree in $\mathbf{X}_{\leq k}$ of each summand in (1) can be taken at most $2k^2(\deg \mathcal{W}_k)^2 + (\deg \mathcal{W}_k)^2 = (2k^2+1)(\deg \mathcal{W}_k)^2$.

The conclusion is now similar to that of Gallo and Mishra [1990]. Writing $T_i = X_i^{d_i} + R_i$, with $\deg_{X_j} R_j < d_j$ for all $j \leq i$, identity (1) can be rewritten

$$X_i^{d_i} = -R_i + S_{0,i}\mathfrak{Q}_k(\mathfrak{U}) + \sum_{j=1}^{k-1} S_{j,i}\Big(\mathfrak{Q}'_k(\mathfrak{U})X_i - \mathfrak{V}_i(\mathfrak{U})\Big).$$

This can be rewritten as a linear system in the coefficients of $R_i, S_{0,i}, \ldots, S_{k-1,i}$.

Let G be the number of monomials in k variables of degree at most $(2k^2 + 1)(\deg \mathcal{W}_k)^2$, and $G' \leq G$ the number of unknown coefficients in R_i. Then we write the system $\mathbf{Mu} = \mathbf{v}$, where $\mathbf{u}$ is the vector of the $kG + G'$ unknown coefficients of $R_i, S_{0,i}, \ldots, S_{k-1,i}$ and $\mathbf{v}$ is the zero vector, except for one entry equal to 1, corresponding to the coefficient of $X_i^{d_i}$. The matrix $\mathbf{M}$ has G rows and $kG + G'$ columns, and its entries are either the constant 1, or the coefficients of $\mathfrak{Q}_k, \mathfrak{Q}'_k, \mathfrak{V}_1, \ldots, \mathfrak{V}_n$. These are polynomials in $\mathbf{P}$ of degree at most $\deg \mathcal{W}_k$, by Proposition 1.

The coefficients of R_i are uniquely determined, due to our degree constraints for a triangular set. Consequently, by Rouché-Fontené's Theorem, these coefficients can be expressed as quotients of determinants of size at most G, with entries that are polynomials in $\mathbf{P}$ of degree at most $\deg \mathcal{W}_k$. Then their numerators and denominators have degree at most $G \deg \mathcal{W}_k$.

This concludes the proof of Theorem 1: since G is bounded from above by $((2k^2+1)(\deg \mathcal{W}_k)^2+1)^k$, $G \deg \mathcal{W}_k$ is bounded by $(2k^2+2)^k(\deg \mathcal{W}_k)^{2k+1}$. □

5 Preliminaries for Theorem 2

This section is devoted to present intermediate results that are used in Section 6 for proving Theorem 2; they are independent of our general discussion on the variety $\mathcal{W}$ and its generic solutions. In Subsection 5.1, we discuss a notion of *specialization* of a Greatest Common Divisor defined modulo a triangular set in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$. In Subsection 5.2, we define the operations of *splitting* and *recombining* triangular sets, following [Lazard, 1992].

Let $\mathbf{T} = (T_1, \ldots, T_n)$ be a triangular set in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$; we let B be the quotient $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]/\mathbf{T}$ and suppose that B is a field. Thus, the notion of GCD of two polynomials in $B[U]$ is well-defined; we now inspect its specialization properties.

Let thus $\mathbf{p}$ be a point in $\mathbb{A}^m(\overline{\mathcal{K}})$ which cancels no denominator in the coefficients of $\mathbf{T}$. We denote by $\mathbf{t}$ the polynomials $\mathbf{T}$, where all coefficients are specialized at $\mathbf{p}$, and let $\mathfrak{b}$ be the quotient $\overline{\mathcal{K}}[\mathbf{X}]/\mathbf{t}$. We suppose that $\mathbf{t}$ defines a radical ideal, so $\mathfrak{b}$ is the product of fields $\mathfrak{b} \simeq \overline{\mathcal{K}}^D$, for some integer D.

The following proposition exhibits conditions under which the GCD of two polynomials in $B[U]$ specializes well. Since $\mathfrak{b}$ is the product of fields $\overline{\mathcal{K}}^D$, we denote by ψ_ℓ the ℓ-th coordinate map $\mathfrak{b} \to \overline{\mathcal{K}}$, for $\ell \leq D$; it extends to a map $\mathfrak{b}[U] \to \overline{\mathcal{K}}[U]$.

Proposition 5 *Let F, G be polynomials in $B[U]$, with G monic, and $H \in B[U]$ their monic* GCD. *Suppose that $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ cancels no denominator in the coefficients of F, G. Denote by f, g in $\mathfrak{b}[U]$ the polynomials F, G with coefficients specialized at $\mathbf{p}$. Then:*

(1) $\mathbf{p}$ cancels none of the denominators of the coefficients of H; h then denotes the polynomial H with all coefficients specialized at $\mathbf{p}$.
(2) For $\ell \leq D$, the degree of $\gcd(\psi_\ell(f), \psi_\ell(g))$ is at least the degree of H.

Suppose that for $\ell \leq D$, the degree of $\gcd(\psi_\ell(f), \psi_\ell(g))$ is the degree of H. Then:

3. *For $\ell \leq D$, $\psi_\ell(h)$ equals $\gcd(\psi_\ell(f), \psi_\ell(g))$.*
4. *Let Q, R in $B[U]$ be the cofactors for the Bézout equality $QF + RG = H$. Then $\mathbf{p}$ cancels none of the denominators of the coefficients of Q, R. Let q, r in $\mathfrak{b}[U]$ denote these polynomials with coefficients specialized at $\mathbf{p}$. Then for $\ell \leq D$, $\psi_\ell(q), \psi_\ell(r)$ are the cofactors for the Bézout equality of $\psi_\ell(f), \psi_\ell(g)$.*

Proof. We use a classical local-global argument; thus, we suppose without loss of generality that $\mathbf{p} = \mathbf{0}$, and proceed to work in the power series ring $\overline{\mathcal{K}}[[\mathbf{P}]]$ and its fraction field $\overline{\mathcal{K}}((\mathbf{P}))$ instead of the rational function field $\overline{\mathcal{K}}(\mathbf{P})$. We let S denote the reduction modulo the maximal ideal of $\overline{\mathcal{K}}[[\mathbf{P}]]$; S extends to specialization maps $\overline{\mathcal{K}}[[\mathbf{P}]][U] \to \overline{\mathcal{K}}[U]$ and $\overline{\mathcal{K}}[[\mathbf{P}]]^n \to \overline{\mathcal{K}}^n$.

We use below Theorems 6.26 and 6.55 from von zur Gathen and Gerhard [1999] in the ring $\overline{\mathcal{K}}[[\mathbf{P}]][U]$. These results are stated for a prime ideal in an Euclidean base ring, but they extend *verbatim* to the UFD $\overline{\mathcal{K}}[[\mathbf{P}]]$ and its

maximal ideal. We start by proving two auxiliary results.

Lifting the coordinate functions. Let $\mathbf{x}^1, \ldots, \mathbf{x}^D$ be the D distinct roots of $\mathbf{t}$ in $\overline{\mathcal{K}}^n$. Then for $\ell \leq D$, the polynomials $\psi_\ell(f), \psi_\ell(g)$ are obtained by specializing $\mathbf{P}$ at $\mathbf{0}$ and $\mathbf{X}$ at $\mathbf{x}^\ell$ in F, G. Using the points $\mathbf{x}^\ell$, we proceed to lift the splitting of $\mathfrak{b}$ into a splitting of B.

By assumption, none of the denominators in $\mathbf{T}$ vanishes at zero, so we denote by $\overline{\mathbf{T}}$ the image of these polynomials in $\overline{\mathcal{K}}[[\mathbf{P}]][\mathbf{X}]$. Since $\mathfrak{b}$ is a product of field extensions and $\overline{\mathcal{K}}$ is algebraically closed, we deduce that the jacobian determinant of $\mathbf{t}$ is invertible in $\mathfrak{b}$, so Hensel's Lemma applies. We obtain the existence of $\mathbf{X}^1, \ldots, \mathbf{X}^D$ in $\overline{\mathcal{K}}[[\mathbf{P}]]^n$ that cancel $\overline{\mathbf{T}}$, and such that $S(\mathbf{X}^\ell) = \mathbf{x}^\ell$ for $\ell \leq D$.

Enumeration shows that these are all the roots of $\overline{\mathbf{T}}$ in an algebraic closure of $\overline{\mathcal{K}}((\mathbf{P}))$, thus $\overline{\mathcal{K}}((\mathbf{P}))[\mathbf{X}]/\overline{\mathbf{T}}$ is the product of D copies of $\overline{\mathcal{K}}((\mathbf{P}))$. For $\ell \leq D$, let Ψ_ℓ be the field embedding $B \to \overline{\mathcal{K}}((\mathbf{P}))$ that maps $(\mathbf{X} \mod \mathbf{T})$ to $\mathbf{X}^\ell$. It extends to a map $B[U] \to \overline{\mathcal{K}}((\mathbf{P}))[U]$.

An interpolation result. Let z be in B. Let us suppose that all values $\Psi_\ell(z)$ are in the subring $\overline{\mathcal{K}}[[\mathbf{P}]]$ of $\overline{\mathcal{K}}((\mathbf{P}))$. We now prove that no coefficient of z on the canonical basis of B vanishes at zero; this result is used twice below.

The coefficients of z are obtained as follows. We denote by $\mathbf{z} = [z_1, \ldots, z_D]^t$ the column vector of the coordinates of z in the canonical basis, and $\Psi(z)$ the column vector $[\Psi_1(z), \ldots, \Psi_D(z)]$. Then these vectors are related by the relation $\mathbf{V}\mathbf{z} = \Psi(z)$, where we now describe the matrix $\mathbf{V}$.

The matrix $\mathbf{V}$ is a generalized Vandermonde Matrix associated to $\mathbf{X}^1, \ldots, \mathbf{X}^D$, see Mourrain and Ruatta [2002]. Its entries are the values taken by $\mathbf{X}^1, \ldots, \mathbf{X}^D$ on all monomials of the canonical basis; thus its determinant is in $\overline{\mathcal{K}}[[\mathbf{P}]]$. Since the entries of $\Psi(z)$ are in $\overline{\mathcal{K}}[[\mathbf{P}]]$, it is enough to prove that the constant term of $\det(\mathbf{V})$ is non zero to conclude. This term is the determinant of the analogous Vandermonde matrix associated to the points $\mathbf{x}^1, \ldots, \mathbf{x}^D$ in $\overline{\mathcal{K}}^n$. But by Proposition 4.6 in Mourrain and Ruatta [2002], this determinant is not zero, *q.e.d.*

Concluding the proof. For $\ell \leq D$, $\Psi_\ell(H)$ is $\gcd(\Psi_\ell(F), \Psi_\ell(G))$, since Ψ_ℓ embeds B into $\overline{\mathcal{K}}((\mathbf{P}))$. Our assumptions on F, G show that $\Psi_\ell(F)$ and $\Psi_\ell(G)$ are in the subring $\overline{\mathcal{K}}[[\mathbf{P}]][U]$ of $\overline{\mathcal{K}}((\mathbf{P}))[U]$, thus so is their monic GCD. Using the above interpolation result, this proves the first statement of the proposition.

By construction, $S(\Psi_\ell(F)) = \psi_\ell(f)$ and $S(\Psi_\ell(G)) = \psi_\ell(g)$. Since $\Psi_\ell(G)$ is monic, Theorem 6.26 in von zur Gathen and Gerhard [1999] shows that the degree of $\gcd(\psi_\ell(f), \psi_\ell(g))$ is at least the degree of $\gcd(\Psi_\ell(F), \Psi_\ell(G)) = \deg H$. This proves the second statement.

We suppose now that $\gcd(\psi_\ell(f), \psi_\ell(g))$ has degree d for all ℓ. Using again Theorem 6.26 in von zur Gathen and Gerhard [1999], we see that $\gcd(\psi_\ell(f), \psi_\ell(g))$ is the specialization $S(\Psi_\ell(H))$. Since none of the coefficients of H vanishes at zero, this can be obtained by first letting $\mathbf{P} = \mathbf{0}$ in H, then evaluating at $\mathbf{x}^\ell$. This is our third statement.

Finally, for $\ell \leq D$, the equality $\Psi_\ell(Q)\Psi_\ell(F)+\Psi_\ell(R)\Psi_\ell(G) = \Psi_\ell(H)$ holds. Using our assumption on the degree of $\gcd(\psi_\ell(f), \psi_\ell(g))$, Theorem 6.55 in von zur Gathen and Gerhard [1999] shows that $\Psi_\ell(Q), \Psi_\ell(R)$ are in $\overline{\mathcal{K}}[[\mathbf{P}]][U]$, and that their images by S are the cofactors for the Bézout equality of $\psi_\ell(f), \psi_\ell(g)$. Applying again the above interpolation result concludes the proof. □

5.2 Splitting and Combining Triangular Sets

Our second, and last, intermediate result presents the basic ways of splitting and combining triangular sets. The first paragraph closely follows [Lazard, 1992], and we give it again for completeness. In a second time, as a corollary of Proposition 5, we show how to *specialize* the process of combining two triangular sets; this result is used in Subsection 6.3. In the sequel, superscripts *do not* indicate powers.

The general case. Let $\mathfrak{K}$ be a field, $\mathbf{X} = X_1, \ldots, X_n$ and $\mathbf{T}$ a triangular set in $\mathfrak{K}[\mathbf{X}]$. Let us fix $k \leq n$ and suppose that $B_k = \mathfrak{K}[\mathbf{X}_{\leq k}]/\mathbf{T}_{\leq k}$ is a field. We now define the *splitting* of $\mathbf{T}$ as a family of triangular sets $\mathbf{T}^1, \ldots, \mathbf{T}^J$ in $\mathfrak{K}[\mathbf{X}]$; it is denoted by $\mathtt{Split}(\mathbf{T})$.

Let us write $T_{k+1} = \Pi_{j=1}^J T_{k+1,j}$ the factorization of T_{k+1} into irreducibles in the polynomial ring $B_k[X_{k+1}]$ (with repetitions allowed). We can then define $\mathbf{T}^j$, for $j \leq J$. For $i \leq k$, we take $T_i^j = T_i$. For index $k+1$, we take $T_{k+1}^j = T_{k+1,j}$. For $i > k+1$, we define T_i^j as T_i with coefficients reduced modulo $T_{k+1,j}$.

In the converse direction, let $\mathbf{T}^1$ and $\mathbf{T}^2$ be two triangular sets in $\mathfrak{K}[\mathbf{X}]$, and suppose that there exists $k \leq n$ such that:

- $\mathbf{T}^1_{\leq k} = \mathbf{T}^2_{\leq k}$ and $B_k = \mathfrak{K}[\mathbf{X}_{\leq k}]/\mathbf{T}^1_{\leq k}$ is a field;
- T^1_{k+1} and T^2_{k+1} are coprime in $B_k[X_{k+1}]$;
- for $i > k+1$, T_i^1 and T_i^2 have the same degree in the variable X_i (recall that they are monic in X_i by definition).

Then we say that $\mathbf{T}^1$ and $\mathbf{T}^2$ can be *combined*. We define their combination, the triangular set $\mathbf{T}$, as follows: $T_i = T_i^1 = T_i^2$ for $i \leq k$ and $T_{k+1} = T_{k+1}^1 T_{k+1}^2$. For $i > k+1$, we now define T_i using an explicit form of the Chinese Remainder Theorem.

Let us consider T_i^1 and T_i^2 as multivariate polynomials in $X_{k+2}, \ldots, X_n$ with coefficients in $B_k[X_{k+1}]$. With this point of view, let M be any monomial in $X_{k+2}, \ldots, X_n$ and c_1 and c_2 its coefficients in respectively T_i^1 and T_i^2. Let U_1, U_2 be the Bézout coefficients, so that $U_1 T_{k+1}^1 + U_2 T_{k+1}^2 = 1$. Then we define $c(M) = c_2 U_1 T_{k+1}^1 + c_1 U_2 T_{k+1}^2$ and T_i is the sum of the terms $c(M)M$, taken for all monomials M.

Under the above assumptions, $\mathbf{T}$ is a triangular set: for $i > k+1$, the polynomials T_i^1 and T_i^2 have the same degree in X_i and are monic in X_i, so that T_i is monic in X_i as well (for $i \leq k+1$, this is obviously also the case). The ideal generated by $\mathbf{T}$ is the sum of those defined by $\mathbf{T}^1$ and $\mathbf{T}^2$; splitting $\mathbf{T}$ gives back $\mathbf{T}^1$ and $\mathbf{T}^2$.

Application to parametric situations. We now consider the particular case $\mathfrak{K} = \overline{\mathcal{K}}(\mathbf{P})$. Let $\mathbf{T}^1, \mathbf{T}^2$ be triangular sets in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$ and suppose that $\mathbf{T}^1, \mathbf{T}^2$ can be combined, for some $k \leq n$. Let $\mathbf{T}$ be their combination, as defined above. Let $\mathbf{p}$ be in $\mathbb{A}^m(\overline{\mathcal{K}})$, which cancels no denominator in the coefficients of $\mathbf{T}^1, \mathbf{T}^2$, and denote $\mathbf{t}^1, \mathbf{t}^2$ these triangular sets with coefficients specialized at $\mathbf{p}$.

The next proposition shows how the recombination can be *specialized* at the point $\mathbf{p}$; we will use it in Subsection 6.3. The proof is a direct consequence of point 4 in Proposition 5, and the definition of $\mathbf{T}$ given in the previous paragraph.

Proposition 6 *Assume that the triangular sets $\mathbf{t}^1_{\leq k+1}$ and $\mathbf{t}^2_{\leq k+1}$ define radical ideals in $\overline{\mathcal{K}}[\mathbf{X}_{\leq k+1}]$ with no common solution. Then $\mathbf{p}$ cancels none of the denominators of the coefficients of $\mathbf{T}$. If $\mathbf{t}$ denotes the triangular set $\mathbf{T}$ with all coefficients specialized at $\mathbf{p}$, then $\mathbf{t}$ generates the sum of the ideals generated by $\mathbf{t}^1, \mathbf{t}^2$, so in particular it generates a radical ideal.*

6 Specialization Properties: Proof of Theorem 2

We now return to our original complexity questions: we consider again the variety $\mathcal{W}$, that satisfies Assumption 1, and suppose that its generic solutions are represented by a triangular set $\mathbf{T} = (T_1, \ldots, T_n)$. We now consider bounding the degree of a degeneracy hypersurface associated to $\mathbf{T}$:

There exists a polynomial $\Delta_{\mathcal{W}} \in \overline{\mathcal{K}}[\mathbf{P}]$ *of degree at most* $(3n \deg \mathcal{W} + n^2) \deg \mathcal{W}$ *such that, if* $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ *does not cancel* $\Delta_{\mathcal{W}}$*:*

(1) $\mathbf{p}$ *cancels no denominator in the coefficients of* $(T_1, \ldots, T_n)$*. We denote by* $(t_1, \ldots, t_n)$ *these polynomials with coefficients specialized at* $\mathbf{p}$*.*
(2) $(t_1, \ldots, t_n)$ *is a radical ideal. Let* $Z_n \subset \mathbb{A}^n(\overline{\mathcal{K}})$ *be the zero-set of the polynomials* $(t_1, \ldots, t_n)$*; then* $\mathcal{W}_n(\mathbf{p})$ *equals* $\{\mathbf{p}\} \times Z_n \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$*.*

The proof consists in specializing all steps of a conversion algorithm from a geometric resolution to a triangular set. In Subsection 6.1, we give such an algorithm, which computes the triangular set $\mathbf{T}$ from a parametric resolution associated to $\mathcal{W}$. The algorithm works over the base field $\overline{\mathcal{K}}(\mathbf{P})$, and applies when $\mathcal{W}$ is irreducible. In Subsection 6.2, we show how to specialize all steps of this algorithm at a point $\mathbf{p}$ in $\mathbb{A}^m(\overline{\mathcal{K}})$, under suitable geometric conditions. In Subsection 6.3, we drop the irreducibility assumption and quantify the geometric conditions, giving the proof of Theorem 2.

6.1 A Conversion Algorithm

Let $\mathcal{J}$ the ideal defining $\mathcal{W}$, and $\mathcal{J}_P$ its extension in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$. By assumption, $\mathcal{J}_P$ is generated by the triangular set $\mathbf{T}$. Let B_n be the quotient $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]/\mathbf{T}$. As described in Section 2, for $k \leq n$, we define the quotient B_k as $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]/\mathbf{T}_{\leq k}$ and denote by D_k its dimension. We suppose that $\mathcal{W}$ is irreducible, so the field extensions $\overline{\mathcal{K}}(\mathbf{P}) \to B_n$ is separable, by Assumption 1, thus so are all intermediate extensions.

Propositions 1 and 2 show that $\overline{\mathcal{K}}(\mathbf{P}) \to B_n$ admits the parametric resolution $Q(\mathfrak{U}) = 0$ and $X_1 = W_1(\mathfrak{U}), \ldots, X_n = W_n(\mathfrak{U})$, where $\mathfrak{U}$ is a linear combination of the variables $\mathbf{X}$; we now show how to compute the triangular set $\mathbf{T}$ starting from $Q, W_1, \ldots, W_n$. Consider the following sequence:

(1) **Initialization**: let $A_0 = \overline{\mathcal{K}}(\mathbf{P})$, $R_0 = Q$, $S_0 = 0$.
(2) **Loop**: for k in $1, \ldots, n$ do
- Let $S_k = \text{MinimalPolynomial}(W_k)$ in $A_{k-1}[U]/R_{k-1}(U)$.
- Let $A_k = A_{k-1}[X_k]/S_k(X_k)$, and x_k the image of X_k in A_k.
- Let $R_k = \gcd(x_k - W_k(U), R_{k-1}(U))$ in $A_k[U]$.

Proposition 7 shows that this algorithm computes the polynomials T_k. Actually, we must take into account the polynomials R_k as well; for consistency we also take $T_0 = 0$ and $B_0 = \overline{\mathcal{K}}(\mathbf{P})$.

Proposition 7 *For* $k = 0, \ldots, n$*, the following holds:*

(1) $S_k = T_k$*, so that* A_k *coincides with the quotient* B_k *defined above.*

(2) R_k is the minimal polynomial of $\mathfrak{U}$ over the subfield B_k of B_n, so $B_n = B_k[U]/R_k(U)$.

PROOF. Let us denote by $\mathcal{P}_k$ the above assertions. Their validity for $k = 0$ is immediate. For $k = 1, \ldots, n$, we prove that $\mathcal{P}_{k-1}$ implies $\mathcal{P}_k$. This is an immediate consequence of the following lemma.

Lemma 1 *Let $A \to B$ be a separable field extension, such that $B = A[U]/R$, with R irreducible, and denote by u the image of U in B. Let W be in $A[U]$, $x = W(u)$ in B and P the minimal polynomial of x over A. Let $C = A[X]/P$ be the subfield $A(x) \subset B$. Then the minimal polynomial of u over C is the* GCD *of $R(U)$ and $W(U) - x$ in $C[U]$.*

PROOF. Let $S \in C[U]$ be the minimal polynomial of u over C. Since $R(u) = 0$, S divides R. Similarly, since $x = W(u)$, S divides $W - x$, so S divides the GCD of $(R, W - x)$ in $C[U]$. To conclude, it is enough to show that S and $\gcd(R, W-x)$ have the same degree. From the field inclusions $A \to C \to B$, we deduce that the degree of S is $\deg R/\deg P$. Let us prove that $\gcd(R, W - x)$ has degree $\deg R/\deg P$ too.

Let χ be the characteristic polynomial of W in B; since P is irreducible, χ is a power of P. We consider an algebraic closure $\overline{A}$ of A and write the factorizations in $\overline{A}[U]$:

$$R = \prod_{k=1}^{\deg R} (U - u_k), \quad \chi = \prod_{k=1}^{\deg R} (X - W(u_k)), \quad P = \prod_{j=1}^{\deg P} (X - w_j).$$

Then all w_j are distinct since B is separable, so for j in $1, \ldots, \deg P$, there are precisely $\deg R/\deg P$ roots u_k of R such that $W(u_k) = w_j$. Let now $\overline{C}$ be the quotient $\overline{A}[X]/P$. Then $\overline{C}$ is not a field, but a product of fields $\Pi_{j=1}^{\deg P} C_j$. All C_j are isomorphic to $\overline{A}$, and the image of X in C_j is w_j.

Let us embed $C = A[X]/P$ into one of these fields, for instance C_1. Then the GCD of R and $W - x$ has the same degree when it is considered in $C[U]$ or $C_1[U]$, and we conclude the proof by estimating its degree in $C_1[U]$. Indeed, the degree of $\gcd(R, W-x)$ in $C_1[U]$ is the number of roots u_k of R, such that $W(u_k) = w_1$. By the remarks above, this number is $\deg R/\deg P$. □

We can then prove Proposition 7. Assuming $\mathcal{P}_{k-1}$, we see that A_{k-1} is the subfield $B_{k-1} = \overline{\mathcal{K}}(\mathbf{P})(x_1, \ldots, x_{k-1})$, and that B_n is $B_{k-1}[U]/R_{k-1}(U)$. Thus the minimal polynomial of W_k in $B_{k-1}[U]/R_{k-1}(U)$ is indeed T_k; this prove point 1 for $\mathcal{P}_k$. Applying the above lemma concludes the proof, taking $B_{k-1} \to B_k \to B_n$ for the fields $A \to C \to B$ mentioned in the lemma. □

Let $\mathbf{p}$ be in $\mathbb{A}^m(\overline{\mathcal{K}})$. We now prove that each step of the previous algorithm can be specialized at $\mathbf{p}$: under suitable geometric conditions, none of the denominators that appear vanishes at $\mathbf{p}$, and specializing the variables $\mathbf{P}$ at $\mathbf{p}$ gives the requested output. We refer to Section 2 for the definition of the notation used here, notably of the projections μ_k.

Proposition 8 *Assume that $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ is such that:*

(1) $\mathbf{p}$ cancels no denominator in the coefficients of $Q, W_1, \ldots, W_n$. We denote by $q, w_1, \ldots, w_n$ the polynomials of $\overline{\mathcal{K}}[U]$ obtained by specializing all coefficients in $Q, W_1, \ldots, W_n$ at $\mathbf{p}$.
(2) For $k \leq n$, the fiber $\mathcal{W}_k(\mathbf{p})$ has D_k points.
(3) The polynomials $q, w_1, \ldots, w_n$ form a geometric resolution for the fiber $\mathcal{W}_n(\mathbf{p})$.
(4) For $k \leq n$, $\mathcal{W}_k(\mathbf{p})$ coincides with the projection $\mu_k(\mathcal{W}_n(\mathbf{p}))$.

Then $\mathbf{p}$ cancels no denominator in $(T_1, \ldots, T_n)$. Denote by $(t_1, \ldots, t_n)$ the polynomials $(T_1, \ldots, T_n)$ with coefficients specialized at $\mathbf{p}$. Then $(t_1, \ldots, t_n)$ is a radical ideal. Let $Z_n \subset \mathbb{A}^n(\overline{\mathcal{K}})$ be the zero-set of $(t_1, \ldots, t_n)$; then $\mathcal{W}_n(\mathbf{p})$ equals $\{\mathbf{p}\} \times Z_n$.

Proof. Let us first recall how the polynomials $\mathbf{T} = (T_1, \ldots, T_n)$ are obtained. Let $B_0 = \overline{\mathcal{K}}(\mathbf{P})$ and $R_0 = Q$. Then, using Proposition 7, for $k \leq n$, T_k, B_k, R_k are defined as follows:

- T_k is the minimal polynomial of W_k in $B_{k-1}[U]/R_{k-1}(U)$;
- B_k is the quotient field $B_{k-1}[X_k]/T_k(X_k)$;
- R_k is the GCD of $x_k - W_k(U)$ and $R_{k-1}(U)$ in $B_k[U]$.

We now prove that each step of this algorithm can be specialized at $\mathbf{p}$, in a suitable sense: for k in $1, \ldots, n$, all coefficients in $T_1, \ldots, T_k, R_k$ will be specialized at $\mathbf{p}$, which will define a quotient $\mathfrak{b}_k$ analogous to B_k. The quotient $\mathfrak{b}_k$ will not be a field; hence, some care is needed as to giving a precise meaning to notions such as minimal polynomial or GCD over $\mathfrak{b}_k$.

More precisely, we prove the following properties by induction. Properties $\mathfrak{A}_n$ and $\mathfrak{B}_n$ are enough to prove the proposition, but we actually need to handle the last property to make the recursion work. In the sequel, superscripts *do not* indicate powers.

$\mathfrak{A}_k$ **:** $\mathbf{p}$ cancels no denominator in the coefficients of $T_1, \ldots, T_k$; then $t_1, \ldots, t_k$ denote these polynomials with coefficients specialized at $\mathbf{p}$.
$\mathfrak{B}_k$ **:** The ideal $(t_1, \ldots, t_k)$ of $\overline{\mathcal{K}}[\mathbf{X}_{\leq k}]$ is radical. Let $Z_k \subset \mathbb{A}^k(\overline{\mathcal{K}})$ be its zero-

set; then $\mathcal{W}_k(\mathbf{p})$ coincides with $\{\mathbf{p}\} \times Z_k$.

We let $\mathfrak{b}_k$ be the quotient $\overline{\mathcal{K}}[\mathbf{X}_{\leq k}]/(t_1, \ldots, t_k)$. Then $\mathfrak{b}_k$ is the product of D_k copies of $\overline{\mathcal{K}}$, by Hypothesis 2. For $j \leq D_k$, we denote by ϕ_j the j-th coordinate function $\mathfrak{b}_k \to \overline{\mathcal{K}}$. This function maps $X_1, \ldots, X_k$ to some values $x_1^{(j)}, \ldots, x_k^{(j)}$, and we denote by $p_k^{(j)}$ the point of $\mathcal{W}_k(\mathbf{p})$ with coordinates $(\mathbf{p}, x_1^{(j)}, \ldots, x_k^{(j)})$. The map ϕ_j also extends to a map between polynomial rings $\mathfrak{b}_k[U] \to \overline{\mathcal{K}}[U]$.

$\mathfrak{C}_k$ **:** $\mathbf{p}$ cancels no denominator in the coefficients of R_k. We let $r_k \in \mathfrak{b}_k[U]$ denote this polynomial with coefficients specialized at $\mathbf{p}$, and for $j \leq D_k$, let $r_{k,j}$ be $\phi_j(r_k)$ in $\overline{\mathcal{K}}[U]$. Then $r_{k,j}$ is $\Pi(U - \mathfrak{U}(p))$, the product being taken on all points p in $\mathcal{W}_n(\mathbf{p})$ such that $\mu_k(p) = p_k^{(j)}$.

The validity for $k = 0$ is obvious; we now suppose that $\mathfrak{A}_{k-1}, \mathfrak{B}_{k-1}, \mathfrak{C}_{k-1}$ are satisfied, and prove their validity at step k. By assumption, we come equipped with a quotient $\mathfrak{b}_{k-1} = \overline{\mathcal{K}}[\mathbf{X}_{\leq k-1}]/(t_1, \ldots, t_{k-1})$, which is a product of D_{k-1} copies of $\overline{\mathcal{K}}$. For $j \leq D_{k-1}$, we denote by ϕ_j the j-th coordinate map $\mathfrak{b}_{k-1} \to \overline{\mathcal{K}}$ and its extension $\mathfrak{b}_{k-1}[U] \to \overline{\mathcal{K}}[U]$.

Proof of $\mathfrak{A}_k$. Let χ be the characteristic polynomial of W_k in the quotient $B_{k-1}[U]/R_{k-1}(U)$. Our hypotheses show that $\mathbf{p}$ cancels no denominator in the coefficients of χ. Since χ is a power of the minimal polynomial T_k of W_k, $\mathbf{p}$ cancels no denominator in the coefficients of T_k. This proves $\mathfrak{A}_k$; we let $t_k \in \mathfrak{b}_{k-1}[U]$ be the polynomial T_k with all coefficients specialized at $\mathbf{p}$.

Proof of $\mathfrak{B}_k$. By definition, R_{k-1} divides $T_k(W_k)$ in $B_{k-1}[U]$. Let $S \in B_{k-1}[U]$ be the quotient, satisfying the equality $T_k(W_k) = R_{k-1}S$. Then $\mathbf{p}$ cancels no denominator in the coefficients of S, and we let s be S with coefficients specialized at $\mathbf{p}$. Then the equality $t_k(w_k) = r_{k-1}s$ holds in $\mathfrak{b}_{k-1}[U]$. For $j \leq D_{k-1}$, let $t_{k,j}, w_{k,j}, s_j$ in $\overline{\mathcal{K}}[U]$ be the images of t_k, w_k, s by ϕ_j. The relation $t_{k,j}(w_{k,j}) = r_{k-1,j}s_j$ shows that all roots of $r_{k-1,j}$ cancel $t_{k,j}(w_{k,j})$.

Let $Z_k \subset \mathbb{A}^k(\overline{\mathcal{K}})$ be the zero-set of $(t_1, \ldots, t_k)$. We first prove that $\{\mathbf{p}\} \times Z_k$ contains the fiber $\mathcal{W}_k(\mathbf{p})$. Let $p_k = (\mathbf{p}, x_1, \ldots, x_k)$ be a point in $\mathcal{W}_k(\mathbf{p})$; we thus want to prove that $(t_1, \ldots, t_k)$ vanish at $(x_1, \ldots, x_k)$.

By Hypothesis 4, there exist p in $\mathcal{W}_n(\mathbf{p})$ such that $\mu_k(p) = p_k$. Since $\mu_{k-1}(p)$ is in $\mathcal{W}_{k-1}(\mathbf{p})$, there exists $j \leq D_{k-1}$ such that $(x_1, \ldots, x_{k-1}) = (x_1^{(j)}, \ldots, x_{k-1}^{(j)})$. In particular, $(x_1, \ldots, x_{k-1})$ cancel $(t_1, \ldots, t_{k-1})$. By Hypothesis 3, $w_k\,(\mathfrak{U}(p))$ equals x_k. Then by property $\mathfrak{C}_{k-1}$, $r_{k-1,j}$ vanishes at $\mathfrak{U}(p)$, so by the above discussion, $t_{k,j}$ vanishes at x_k. Thus $\{\mathbf{p}\} \times Z_k$ contains $\mathcal{W}_k(\mathbf{p})$.

We finally prove that these sets coincide. For $j \leq k$, t_j has the same degree as T_j, so the quotient $\overline{\mathcal{K}}[\mathbf{X}_{\leq k}]/(t_1, \ldots, t_k)$ has the same dimension as the quotient

$\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]/(T_1,\ldots,T_k)$. This dimension is D_k, so it equals the cardinality of $\mathcal{W}_k(\mathbf{p})$ by Hypothesis 2. We deduce that $\{\mathbf{p}\}\times Z_k$ equals $\mathcal{W}_k(\mathbf{p})$ and $(t_1,\ldots,t_k)$ is radical. This proves $\mathfrak{B}_k$.

Setting up the new quotient. Let $\mathfrak{b}_k$ be the quotient

$$\mathfrak{b}_k = \overline{\mathcal{K}}[X_1,\ldots,X_k]/(t_1,\ldots,t_k) = \mathfrak{b}_{k-1}[X_k]/t_k \simeq \overline{\mathcal{K}}^{D_k}.$$

For $\ell \leq D_k$, let us denote by ψ_ℓ the ℓ-th coordinate function $\mathfrak{b}_k \to \overline{\mathcal{K}}$. This function maps $X_1,\ldots,X_k$ to some values $x_1^{(\ell)},\ldots,x_k^{(\ell)}$, such that the coordinates of the corresponding point in $\mathcal{W}_k(\mathbf{p})$ are $(\mathbf{p}, x_1^{(\ell)},\ldots,x_k^{(\ell)})$. It extends to a map $\mathfrak{b}_k[U] \to \overline{\mathcal{K}}[U]$. From now on we consider the polynomial r_{k-1} in $\mathfrak{b}_k[U]$, and its images $r_{k-1,\ell} = \psi_\ell(r_{k-1})$ in $\overline{\mathcal{K}}[U]$. Similar notations hold for w_k and $w_{k,\ell}$.

Proof of $\mathfrak{C}_k$. We now turn to the last step, the specialization of the GCD computation. Let $\ell \leq D_k$ and $(\mathbf{p}, x_1^{(\ell)},\ldots,x_k^{(\ell)})$ the coordinates of the corresponding point in $\mathcal{W}_k(\mathbf{p})$. The definition of r_{k-1} shows that $r_{k-1,\ell}$ factors as the product $\Pi(U-\mathfrak{U}(p))$, taken on all points in $\mathcal{W}_n(\mathbf{p})$ whose first coordinates are $(\mathbf{p}, x_1^{(\ell)},\ldots,x_{k-1}^{(\ell)})$. Let $r_{k,\ell}$ be the GCD of $w_{k,\ell}(U) - x_k^{(\ell)}$ and $r_{k-1,\ell}(U)$. Then $r_{k,\ell}$ is the product $\Pi(U-\mathfrak{U}(p))$, taken on all points p in $\mathcal{W}_n(\mathbf{p})$ such that $\mu_k(p) = (\mathbf{p}, x_1^{(\ell)},\ldots,x_k^{(\ell)})$.

We apply Proposition 5, that describes the specialization properties of GCD's. The first part of the proposition shows that for all ℓ, the degree of $r_{k,\ell}$ is at least the degree of R_k. We now proceed to prove that these degrees are actually equal.

Using the above characterization, the product of the polynomials $r_{k,\ell}$ for $\ell \leq D_k$ is $\Pi(U-\mathfrak{U}(p))$, taken on all points in $\mathcal{W}_n(\mathbf{p})$. By hypothesis 2, it has degree D_n. On the other hand, since there are D_k polynomials $r_{k,\ell}$, their product has degree at least $D_k \deg R_k$ by the previous reasoning, with equality if and only if they all have degree $\deg R_k$. But the definition of D_k and R_k shows that $D_k \deg R_k = D_n$. Thus all polynomials $r_{k,\ell}$ necessarily have degree $\deg R_k$.

We can then apply the first and third points of Proposition 5: $\mathbf{p}$ cancels no denominator in R_k; if r_k denotes this polynomial with all coefficients specialized at $\mathbf{p}$, then $\psi_\ell(r_k) = r_{k,\ell}$. This is precisely the content of assertion $\mathfrak{C}_k$. □

Up to now, we assumed that $\mathcal{W}$ was irreducible. We now drop this assumption, and prove Theorem 2:

There exists a polynomial $\Delta_{\mathcal{W}} \in \overline{\mathcal{K}}[\mathbf{P}]$ *of degree at most* $(3n \deg \mathcal{W} + n^2) \deg \mathcal{W}$ *such that, if* $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ *does not cancel* $\Delta_{\mathcal{W}}$*:*

(1) $\mathbf{p}$ *cancels no denominator in the coefficients of* $(T_1, \ldots, T_n)$*. We denote by* $(t_1, \ldots, t_n)$ *these polynomials with coefficients specialized at* $\mathbf{p}$*.*
(2) $(t_1, \ldots, t_n)$ *is a radical ideal. Let* $Z_n \subset \mathbb{A}^n(\overline{\mathcal{K}})$ *be the zero-set of the polynomials* $(t_1, \ldots, t_n)$*; then* $\mathcal{W}_n(\mathbf{p})$ *equals* $\{\mathbf{p}\} \times Z_n \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$*.*

The proof relies on Proposition 9 below. The fact that $\mathcal{W}$ is not irreducible anymore requires further work, and the introduction of new objects associated to $\mathcal{W}$ and its irreducible components.

- Recall that the generic solutions of $\mathcal{W}$ are represented by the triangular set $\mathbf{T}$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$.
- We write $\mathcal{W} = \cup_{j \leq J} \mathcal{W}^j$, where $\mathcal{W}^j$ is irreducible, and for $j \leq J$, let $\mathbf{T}^j$ be the triangular set in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$ that represents the generic solutions of $\mathcal{W}^j$.
- For $k \leq n$ and $j \leq J$, we denote by $\mathcal{W}_k^j$ the closure of $\mu_k(\mathcal{W}_k)$. Not all $\mathcal{W}_k^j$ may be distinct; we let $J_k \leq J$ be the number of distinct varieties among them. We suppose without loss of generality that $\mathcal{W}_k^1, \ldots, \mathcal{W}_k^{J_k}$ are a system of representatives of the distinct varieties among $\mathcal{W}_k^1, \ldots, \mathcal{W}_k^J$.
- For $\mathbf{p}$ in $\mathbb{A}^m(\overline{\mathcal{K}})$ and $j \leq J$, we define $\mathcal{W}_k^j(\mathbf{p})$ as the fiber $\pi_k^{-1}(\mathbf{p}) \cap \mathcal{W}_k^j$.

Proposition 9 *Assume that* $\mathbf{p} \in \mathbb{A}^m(\overline{\mathcal{K}})$ *is such that:*

(1) For $k \leq n$*, and* $j, j' \leq J_k$ *with* $j \neq j'$*,* $\mathcal{W}_k^j(\mathbf{p}) \cap \mathcal{W}_k^{j'}(\mathbf{p})$ *is empty.*
(2) $\mathbf{p}$ *satisfies the assumptions of Proposition 8 for all varieties* $\mathcal{W}^j$*,* $j \leq J$*.*

Then $\mathbf{p}$ *cancels no denominator in the coefficients of* $(T_1, \ldots, T_n)$*. Denote by* $(t_1, \ldots, t_n)$ *these polynomials with coefficients specialized at* $\mathbf{p}$*. Then the ideal* $(t_1, \ldots, t_n)$ *is a radical ideal. If* $Z_n \subset \mathbb{A}^n(\overline{\mathcal{K}})$ *denotes its zero-set,* $\mathcal{W}_n(\mathbf{p})$ *equals* $\{\mathbf{p}\} \times Z_n$*.*

Before proving the proposition, we deduce the proof of Theorem 2; this simply amounts to quantify all conditions given in the proposition.

- For $k \leq n$ and $j, j' \leq J_k$, with $j \neq j'$, Hypothesis 1 is satisfied if $\mathbf{p}$ avoids a hypersurface of degree at most $\deg \mathcal{W}_k^j \deg \mathcal{W}_k^{j'}$. Taking all k, j, j' into account, we bound the sum of these degrees by $n(\deg \mathcal{W})^2$.
- For $j \leq J$, using Propositions 2 and 8, Hypothesis 2 is satisfied when $\mathbf{p}$ avoids a hypersurface of degree at most $(2n \deg \mathcal{W}^j + n^2) \deg \mathcal{W}^j$. The sum

of these degrees is bounded by $(2n \deg \mathcal{W} + n^2) \deg \mathcal{W}$.

This concludes the proof of Theorem 2. Thus, we can concentrate on proving Proposition 9 above. We use the notions of splitting and combining triangular sets, introduced in Subsection 5.2.

Starting from $\mathbf{T}$, the following process computes the family $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$. Let $\mathcal{F}_0$ be $\{\mathbf{T}\}$. For $k = 1, \ldots, n$, we define inductively the families of triangular sets $\mathcal{F}_k$ as follows: $\mathcal{F}_k$ is the reunion of the families $\mathtt{Split}(\mathbf{S})$, for $\mathbf{S}$ in $\mathcal{F}_{k-1}$. Note that at step k, the splitting is done by factoring the k-th polynomial of each triangular set in $\mathbf{S}$. Then the following property is straightforward to prove for $k \leq n$:

$\mathcal{F}_k$ has precisely J_k elements, which we denote by $\mathbf{T}^{1,k}, \ldots, \mathbf{T}^{J_k,k}$. Besides, up to reordering, we can assume that for $j \leq J_k$, the generic solutions of $\mathcal{W}_k^j$ are represented by the ideal generated by $\mathbf{T}_{\leq k}^{j,k}$ in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}_{\leq k}]$.

The idea for proving Proposition 9 is to go all the way back from $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$ to $\mathbf{T}$, since Proposition 8 will enable to specialize the coefficients of all polynomials in $\{\mathbf{T}^1, \ldots, \mathbf{T}^J\}$. To this effect, we prove the following properties by decreasing induction on k. Note that properties $\mathfrak{A}_0$ and $\mathfrak{B}_0$ do prove Proposition 9.

$\mathfrak{A}_k$ **:** For $j \leq J_k$, $\mathbf{p}$ cancels no denominator in the coefficients of the polynomials in $\mathbf{T}^{j,k}$. We let $\mathbf{t}^{j,k}$ be the polynomials in $\mathbf{T}^{j,k}$ with coefficients specialized at $\mathbf{p}$.

$\mathfrak{B}_k$ **:** Let Z_k^j be the zero-set of $\mathbf{t}^{j,k}$ in $\mathbb{A}^n(\overline{\mathcal{K}})$ and Z_k their reunion for $j = 1, \ldots, J_k$. Then $\mathcal{W}_n(\mathbf{p})$ is $\{\mathbf{p}\} \times Z_k \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$.

$\mathfrak{C}_k$ **:** For $j \neq j'$, the ideals generated by $\mathbf{t}_{\leq k}^{j,k}$ and $\mathbf{t}_{\leq k}^{j',k}$ in $\overline{\mathcal{K}}[\mathbf{X}_{\leq k}]$ are radical and have no common zero.

Let us first take $k = n$. By Hypothesis 2, we can apply Proposition 8 to the varieties $\mathcal{W}_j$, $j \leq J$, obtaining properties $\mathfrak{A}_n$ and $\mathfrak{B}_n$. Property $\mathfrak{C}_n$ is then a consequence of Hypothesis 1. Thus, the induction is initiated; let us now assume that $\mathfrak{A}_{k+1}$, $\mathfrak{B}_{k+1}$ and $\mathfrak{C}_{k+1}$ hold, and study step k.

Consider $j \leq J_k$, and the triangular set $\mathbf{T}^{j,k}$ in $\mathcal{F}_k$. By definition, the result of $\mathtt{Split}(\mathbf{T}^{j,k})$ is a family of triangular sets that all belong to $\mathcal{F}_{k+1}$. Without loss of generality, we assume that these are $\mathbf{T}^{1,k+1}, \ldots, \mathbf{T}^{N,k+1}$, for some integer N. Then $\mathbf{T}^{j,k}$ is obtained by successively recombining $\mathbf{T}^{1,k+1}, \ldots, \mathbf{T}^{N,k+1}$ using the Chinese Remainder Theorem, see Subsection 5.2.

By assumption $\mathfrak{A}_{k+1}$, $\mathbf{p}$ cancels no denominator in $\mathbf{T}^{1,k+1}, \ldots, \mathbf{T}^{N,k+1}$; we denote $\mathbf{t}^{1,k+1}, \ldots, \mathbf{t}^{N,k+1}$ these triangular sets with coefficients specialized at $\mathbf{p}$. Let us first consider the recombination of $\mathbf{t}^{1,k+1}$ and $\mathbf{t}^{2,k+1}$. We have $\mathbf{t}_{\leq k}^{1,k+1} = \mathbf{t}_{\leq k}^{2,k+1}$ and by assumption $\mathfrak{C}_{k+1}$, $\mathbf{t}_{\leq k+1}^{1,k+1}$ and $\mathbf{t}_{\leq k+1}^{2,k+1}$ generate radical ideals with

no common zero in $\overline{\mathcal{K}}[\mathbf{X}_{\leq k+1}]$. Thus we can apply Proposition 6 to recombine them.

Iterating this argument, we see that $\mathbf{p}$ cancels no denominator in $\mathbf{T}^{j,k}$, and denote by $\mathbf{t}^{j,k}$ its specialization. Then $\mathbf{t}^{j,k}$ defines a radical ideal, which is the sum of those generated by $\mathbf{t}^{1,k+1}, \ldots, \mathbf{t}^{N,k+1}$.

Taking all j into account, we deduce $\mathfrak{A}_k$ and $\mathfrak{B}_k$. Let us prove $\mathfrak{C}_k$; for simplicity, we show that $\mathbf{t}^{1,k}_{\leq k}$ and $\mathbf{t}^{2,k}_{\leq k}$ are coprime in $\overline{\mathcal{K}}[\mathbf{X}_{\leq k}]$. We know that $\mathbf{T}^{1,k}_{\leq k}$ defines the generic solutions of $\mathcal{W}^1_k$. Since $\mathbf{t}^{1,k}_{\leq k}$ is the specialization of $\mathbf{T}^{1,k}_{\leq k}$ at $\mathbf{p}$, it describes the fiber $\mathcal{W}^1_k(\mathbf{p})$. The similar reasoning holds for $\mathcal{W}^2_k$, so the conclusion follows from Hypothesis 1. □

7 Lifting Techniques

We have now proven our various degree estimates, and turn to algorithmic considerations. Thus, we have to be more specific on the definition of the geometric objects: the input is now a polynomial system $\mathbf{F} = F_1, \ldots, F_n$ in $\mathcal{K}[\mathbf{P}, \mathbf{X}]$. For complexity statements, we suppose that $\mathbf{F}$ is given by a Straight-Line Program of size L, and that d is a bound on the degrees of the polynomials $\mathbf{F}$.

Let $\mathcal{W} \subset \mathbb{A}^{m+n}(\overline{\mathcal{K}})$ be the zero-set of $\mathbf{F}$. We assume that the jacobian determinant of $\mathbf{F}$ with respect to $\mathbf{X}$ is invertible on a dense subset of $\mathcal{W}$. Then Lazard's lemma (see [Boulier et al., 1995, Lemma 2] and [Morrison, 1999, Proposition 3.2]) implies that $\mathcal{W}$ satisfies Assumption 1. Thus its generic solutions are represented by a family of triangular sets; in this section, we present some algorithms for computing with these triangular sets.

We first treat the case when $\mathcal{W}$ is irreducible; then its generic solutions are represented by a single triangular set $\mathbf{T}$ in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$. Theorem 3 below gives an algorithm for computing this triangular set by lifting techniques. See the introduction for the genesis of such ideas.

Recall that $\mathcal{M}(D)$ denotes the complexity of univariate polynomial multiplication in degree D over any ring and $\mathcal{M}_s(D, M)$ the complexity of M-variate power series multiplications truncated in total degree D. The constants C_0, C_1 are defined in the introduction; D_n is the generic number of solutions of the systems $\mathbf{F}(\mathbf{p}, \mathbf{X})$, for $\mathbf{p}$ in $\mathbb{A}^m(\overline{\mathcal{K}})$.

Assume that $\mathcal{W}$ is irreducible. Let $\mathbf{p}, \mathbf{p}'$ be in $\mathcal{K}^m$; assume that a description of the zeros of the systems $\mathbf{F}(\mathbf{p}, \mathbf{X})$, $\mathbf{F}(\mathbf{p}', \mathbf{X})$ by triangular sets is available. For $k \leq n$, let $\mathfrak{D}_k$ be the maximum of the degrees of the coefficients of $T_1, \ldots, T_k$.

Then $T_1, \ldots, T_k$ can be computed within

$$O_{\log}\Big((nL+n^3)(C_0C_1)^n\mathcal{M}(D_n)\mathcal{M}_s(4\mathfrak{D}_k,m)+km^2D_n\mathcal{M}(\mathfrak{D}_k)\mathcal{M}_s(4\mathfrak{D}_k,m-1)\Big)$$

operations in $\mathcal{K}$. The algorithm chooses $3m-1$ values in $\mathcal{K}$, including the coordinates of $\mathbf{p}$ and $\mathbf{p}'$. If Γ is any subset of $\mathcal{K}$, and these values are chosen in Γ^{3m-1}, then the algorithm fails for at most $50n(k^2+2)^{3k}d^{6kn+4n}|\Gamma|^{3m-2}$ choices.

In the general case, we show to recover an eliminating polynomial for the variable X_1 using these techniques. Precisely, let $\mathcal{J}$ be the ideal $(F_1, \ldots, F_n)$, $\mathcal{J}_P$ its extension in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$ and B the quotient $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]/\mathcal{J}_P$. Then Theorem 4 addresses the question of computing the minimal polynomial M_1 of X_1 in B.

Let $\mathbf{p}, \mathbf{p}'$ be in $\mathcal{K}^m$; assume that a description of the zeros of the systems $\mathbf{F}(\mathbf{p}, \mathbf{X})$, $\mathbf{F}(\mathbf{p}', \mathbf{X})$ by triangular sets which define prime ideals in $\mathcal{K}[\mathbf{X}]$ is known. Let $\mathfrak{D}_1$ be the maximum of the degrees of the coefficients of M_1. Then M_1 can be computed within

$$O_{\log}\Big((nL+n^3)(C_0C_1)^n\mathcal{M}(D_n)\mathcal{M}_s(4\mathfrak{D}_1,m)+m^2D_n\mathcal{M}(\mathfrak{D}_1)\mathcal{M}_s(4\mathfrak{D}_1,m-1)\Big)$$

operations in $\mathcal{K}$. The algorithm chooses $3m-1$ values in $\mathcal{K}$, including the coordinates of $\mathbf{p}$ and $\mathbf{p}'$. If Γ is a subset of $\mathcal{K}$, and these values are chosen in Γ^{3m-1}, then the algorithm fails for at most $50nd^{4n}|\Gamma|^{3m-2}$ choices.

This section is organized as follows. Some basic algorithms are described in Subsection 7.1. In Subsection 7.2, we treat the irreducible case; the minimal polynomial computation is addressed in Subsection 7.3.

7.1 Sketch of the Algorithms and Additional Subroutines

The algorithms underlying Theorems 3 and 4 can be sketched as follows:

(1) Choose a generic value $\mathbf{p}$ in $\mathcal{K}^m$ and compute a family of triangular sets that represent the solutions of the specialized system $\mathbf{F}(\mathbf{p}, \mathbf{X})$.
(2) Apply a lifting process, to compute triangular sets with coefficients in the power series ring centered at $\mathbf{p}$.
(3) When the precision of the power series is high enough, use a rational reconstruction process to recover triangular sets with coefficients in $\mathcal{K}(\mathbf{P})$.

We now give more details on some of these points: the computation of a triangular set in $\mathcal{K}[\mathbf{X}]$, the complexity of an operation $(+, \times)$ modulo a triangular set, and the complexity of the rational reconstruction of a rational function.

Initial resolution. The first task is to compute a family of triangular sets $\mathbf{r}^1, \ldots, \mathbf{r}^Q$ in $\mathcal{K}[\mathbf{X}]$ that represent the solutions of the specialized system $\mathbf{F}(\mathbf{p}, \mathbf{X})$. In Subsection 7.3.2, we also ask that all triangular sets $\mathbf{r}^1, \ldots, \mathbf{r}^Q$ define prime ideals in $\mathcal{K}[\mathbf{X}]$.

This routine is called $\texttt{Solve}(\mathbf{F}, \mathbf{p})$. To this effect, we may use zero-dimensional solving procedures of Lazard [1992], Dellière [1999], Aubry et al. [1999] ... Since the complexities of such algorithms are not well known, *we do not take the cost of this phase into account* in the complexity estimates. Note that the cost of the lifting phase is predominant in practice.

Computing modulo a triangular set. Let $\mathbf{T} = (T_1, \ldots, T_n)$ be a triangular set with coefficients in a ring R. The quotient $B := R[\mathbf{X}]/\mathbf{T}$ is built as the succession of n monogeneous extensions of R. We use this point of view to estimate the complexity of an operation in B.

With the notation of Section 2, all operations $(+, \times)$ modulo a single polynomial of degree D require at most $C_0\mathcal{M}(D)$ base ring operations. We deduce that for any triangular set $\mathbf{T} = (T_1, \ldots, T_n)$ in $R[X_1, \ldots, X_n]$, the operations $(+, \times)$ can be done modulo $\mathbf{T}$ in at most $C_0^n \Pi_{k \leq n} \mathcal{M}\left(\deg_{X_k} T_k\right)$ operations in R. See also [Langemyr, 1990] for similar considerations.

Rational reconstruction. In the end of the lifting process, we need to recover some rational functions in $\mathcal{K}(\mathbf{P}) = \mathcal{K}(P_1, \ldots, P_m)$ from their power series expansion. We now present our solution to deal with this question.

If r is a power series in $\mathcal{K}[[P_1, \ldots, P_m]]$ of precision $2D + 1$, we look for a rational function p/q, with $q(0) \neq 0$ and p, q of degree at most D, of which r is the power series expansion. Finding such a rational function, if it exists, amounts to solve a linear system for the coefficients of p and q. When $m = 1$, a faster solution exists, based on Padé approximant computations. In [Schost, 2003, Proposition 6], we introduced a probabilistic extension of this algorithm:

Proposition 10 *Suppose that there exist (p, q) of degrees at most D, such that r is the Taylor expansion of p/q at precision $2D+1$, and $q(0) \neq 0$. We can compute p/q by a probabilistic algorithm within $O_{\log}\left(m^2\mathcal{M}(D)\mathcal{M}_s(2D, m-1)\right)$ operations in $\mathcal{K}$. The algorithm chooses $m-1$ values in $\mathcal{K}$. The choices that lead to an error belong to an hypersurface of $\mathbb{A}^{m-1}(\overline{\mathcal{K}})$ of degree at most $2D(2D+1)^2$.*

In this subsection, *we assume that $\mathcal{W}$ is irreducible*, so its generic solutions are represented by a triangular set $\mathbf{T} = (T_1, \ldots, T_n)$. For fixed $k \leq n$, we now show how to compute $(T_1, \ldots, T_k)$ by lifting techniques. We first present the elementary lifting step; then we give the full algorithm. The complexity and probability analyses will prove Theorem 3.

7.2.1 The Basic Lifting Step

Let $\mathbf{p}$ be a point in the parameter space $\mathcal{K}^m$, such that:

H_1 : The jacobian determinant of $\mathbf{F}(\mathbf{p}, \mathbf{X})$ with respect to $\mathbf{X}$ is invertible on all solutions of the system $\mathbf{F}(\mathbf{p}, \mathbf{X})$.
H_2 : $\mathbf{p}$ does not cancel the polynomial $\Delta_{\mathcal{W}}$ defined in Theorem 2.

Up to a change of variables, we can assume that $\mathbf{p} = \mathbf{0}$. Let A be the m-variate power series ring $\mathcal{K}[[\mathbf{P}]]$ and $\mathfrak{m}$ its maximal ideal. Using Theorem 2, hypothesis H_2 shows that all coefficients in $\mathbf{T}$ admit power series expansions in A; for $\kappa \geq 0$, we denote by $\mathbf{T} \mod \mathfrak{m}^{2^\kappa}$ the triangular set obtained by reducing all coefficients of $\mathbf{T}$ modulo $\mathfrak{m}^{2^\kappa}$.

In this paragraph, we show how to compute the sequence $\mathbf{T} \mod \mathfrak{m}^{2^\kappa}$. The initial value is $\mathbf{t} = \mathbf{T} \mod \mathfrak{m}$, which we assume to know.

By definition of $\mathbf{T}$, there exists a $n \times n$ matrix $\mathbf{A}$ with entries in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$ such that $\mathbf{F} = \mathbf{AT}$, where $\mathbf{T}$ is seen as the column-vector $[T_1, \ldots, T_n]^t$, and $\mathbf{F}$ as $[F_1, \ldots, F_n]^t$. Since all polynomials in $\mathbf{T}$ are monic in their main variable, all denominators in the entries of $\mathbf{A}$ admit power series expansions in A. Thus, we can now consider $\mathbf{F}, \mathbf{T}, \mathbf{A}$ with entries in $A[\mathbf{X}]$. Using Theorem 2, we then rephrase hypotheses H_1 and H_2 as follows:

H'_1 : The jacobian determinant of $\mathbf{F}$ with respect to $\mathbf{X}$ is invertible in $\mathcal{K}[\mathbf{X}]/\mathbf{t}$.
H'_2 : There exists a $n \times n$ matrix $\mathbf{A}$ with entries in $A[\mathbf{X}]$ such that the equality $\mathbf{F} = \mathbf{AT}$ holds.

Our main result is the following proposition. We denote $\texttt{Lift}(\mathbf{T}, \mathbf{F})$ the subroutine which performs the underlying computations.

Proposition 11 *Suppose that hypotheses H'_1 and H'_2 hold for the triangular set $\mathbf{T}$. Let $\kappa > 0$, and suppose that $\mathbf{T} \mod \mathfrak{m}^{2^\kappa}$ is known. Then $\mathbf{T} \mod \mathfrak{m}^{2^{\kappa+1}}$ can be computed within*

$$O\left((nL + n^3)C_0^n \mathcal{M}_s(2^{\kappa+1}, m)\Pi_{k \leq n}\mathcal{M}\left(\deg_{X_k} T_k\right)\right)$$

base field operations.

PROOF. The proof follows from an explicit formula given in Schost [2003]. Stating this result requires some new notation.

- Let $A_\kappa = A/\mathfrak{m}^{2^{\kappa+1}}$ and $\tau = (\tau_1, \ldots, \tau_n)$ be a triangular set in $A_\kappa[\mathbf{X}]$ such that $\tau = \mathbf{T} \mod \mathfrak{m}^{2^\kappa}$. We denote by Q_κ the quotient $A_\kappa[\mathbf{X}]/(\tau_1, \ldots, \tau_n)$.
- Let $\mathbf{F}_\kappa$ be the image of $\mathbf{F}$ in $Q_\kappa[\mathbf{X}]$, $\mathbf{Jac}(\tau)$ and $\mathbf{Jac}(\mathbf{F}_\kappa)$ the jacobian matrices of τ and $\mathbf{F}$ computed in the matrix algebra over Q_κ.

In [Schost, 2003, Proposition 4], we prove the following points. First, $\mathbf{Jac}(\mathbf{F}_\kappa)$ is invertible in the matrix algebra over Q_κ. Let $\delta = (\delta_1, \ldots, \delta_n)$ be the product $\mathbf{Jac}(\tau)\mathbf{Jac}(\mathbf{F}_\kappa)^{-1}\mathbf{F}_\kappa$ and $\widetilde{\delta}$ its canonical preimage in $A_\kappa[\mathbf{X}]$. In this situation, $\mathbf{T} \mod \mathfrak{m}^{2^{\kappa+1}}$ is given by $\tau + \widetilde{\delta}$ in $A_\kappa[\mathbf{X}]$.

We now complete the complexity analysis. From the previous subsection, the operations $(+, \times)$ in Q_κ require $C_0^n \Pi_{k \leq n} \mathcal{M}\left(\deg_{X_k} T_k\right)$ operations in A_κ. All operations in A_κ require $\mathcal{M}_s(2^{\kappa+1}, m)$ base field operations, so the operations $(+, \times)$ in Q_κ take $C_0^n \mathcal{M}_s(2^{\kappa+1}, m) \Pi_{k \leq n} \mathcal{M}\left(\deg_{X_k} T_k\right)$ operations in $\mathcal{K}$.

Let us now estimate how many operations in Q_κ are necessary. Algorithm `Lift` requires to compute $\mathbf{F}_\kappa$, $\mathbf{Jac}(\mathbf{F}_\kappa)$ and $\mathbf{Jac}(\tau)$, to invert $\mathbf{Jac}(\mathbf{F}_\kappa)$ and matrix-vector multiplications. Computing $\mathbf{F}_\kappa$ and $\mathbf{Jac}(\mathbf{F}_\kappa)$ amounts to evaluate the system $\mathbf{F}$ and its jacobian in Q_κ. Using the algorithm of Baur and Strassen [1983], this takes $O(nL)$ operations in Q_κ, where L is the complexity of evaluation of the system $\mathbf{F}$.

The inverse of $\mathbf{Jac}(\mathbf{F}_\kappa)$ is computed by induction on κ by Hensel's Lemma. Thus the only inversion is done for $\kappa = 0$, and can be done in $\mathcal{K}[\mathbf{X}]/\mathbf{t}$, according to Proposition 11: all other inverses are obtained by matrix multiplication over Q_κ and take $O(n^3)$ operations in Q_κ. The other costs are negligible before the previous quantities, concluding the complexity analysis. □

7.2.2 Main Algorithm

The main algorithm follows the lines given in Subsection 7.1. We choose a generic point $\mathbf{p}$ in $\mathcal{K}^m$, so the specialization of $\mathbf{T}$ at $\mathbf{p}$ gives a description of the solutions of the system $\mathbf{F}(\mathbf{p}, \mathbf{X})$. We require that `Solve`$(\mathbf{F}, \mathbf{p})$ outputs a single triangular set $\mathbf{r}$, which is thus the specialization of $\mathbf{T}$ at $\mathbf{p}$. Then, we apply the above lifting process to $\mathbf{r}$. We use an additional subroutine denoted `Stop`, which is described below.

Computing a triangular set by lifting techniques
Input: The system $\mathbf{F}$, $\mathbf{p}, \mathbf{p}'$ in $\mathcal{K}^m$
Output: The polynomials $T_1, \ldots, T_k$.
$\mathbf{r} \leftarrow$ `Solve`$(\mathbf{F}, \mathbf{p})$
$\mathbf{r}' \leftarrow$ `Solve`$(\mathbf{F}, \mathbf{p}')$
`while not(Finished) do`
  $\mathbf{r} \leftarrow$ `Lift`$(\mathbf{r}, \mathbf{F})$
  `Finished`,$T_1, \ldots, T_k \leftarrow$ `Stop`$(\mathbf{r}, \mathbf{r}')$
`end while`
`return` $T_1, \ldots, T_k$

The subroutine `Stop` first tries to compute a rational reconstruction of all the coefficients in $r_1, \ldots, r_k$, yielding polynomials $R_1, \ldots, R_k$. Even if the reconstruction is possible, it might not coincide with $T_1, \ldots, T_k$, if we have stopped the lifting too early. Thus we use a witness value $\mathbf{p}'$: we compute a description $\mathbf{r}' = r'_1, \ldots, r'_n$ of the solutions of the system $\mathbf{F}(\mathbf{p}', \mathbf{X})$. `Stop` tests if the specialization of $R_1, \ldots, R_k$ at $\mathbf{p}'$ is $r'_1, \ldots, r'_k$. If the reconstruction is possible and the test is passed, `Stop` outputs `true` and $R_1, \ldots, R_k$; else it returns `false`.

Complexity analysis. Let $\mathfrak{D}_k$ be the maximal degree in $\mathbf{P}$ of the coefficients in $T_1, \ldots, T_k$. Then the lifting must be run to precision 2^{p+1}, with $p = \lceil \log_2(\mathfrak{D}_k) \rceil$, so that $2^{p+1} \leq 4\mathfrak{D}_k$. From Proposition 11, the cost of the last lifting step is within $O\left((nL + n^3) C_0^n \mathcal{M}_s(4\mathfrak{D}_k, m) \Pi_{k \leq n} \mathcal{M}\left(\deg_{X_k} T_k\right)\right)$ operations in $\mathcal{K}$. We now use our assumptions on the functions $\mathcal{M}$ and $\mathcal{M}_s$ to deduce a simpler estimate on the total cost.

- Since the inequality $\mathcal{M}(D)\mathcal{M}(D') \leq C_1 \mathcal{M}(DD') \log(DD')^\alpha$ holds for all D, D', $\Pi_{k \leq n} \mathcal{M}\left(\deg_{X_k} T_k\right)$ is bounded by $C_1^n \mathcal{M}(\Pi_{k \leq n} \deg_{X_k} T_k)$, up to logarithmic factors.
- Since there exists $C_2 < 1$ such that $\mathcal{M}_s(D, M) \leq C_2 \mathcal{M}_s(2D, M)$ holds for all D, M, the whole cost of the lifting is equivalent to the cost of the last step.

Recall that $\Pi_{k \leq n} \deg_{X_k} T_k$ coincides with the generic degree D_n; then using the above remarks, the whole cost of the lifting phase is seen to be within $O_{\log}\left((nL + n^3)(C_0 C_1)^n \mathcal{M}(D_n) \mathcal{M}_s(4\mathfrak{D}_k, m)\right)$.

It remains to study the cost of the rational reconstruction. There are at most kD_n coefficients to reconstruct. From Proposition 10, each reconstruction costs $O_{\log}\left(m^2 \mathcal{M}(\mathfrak{D}_k) \mathcal{M}_s(4\mathfrak{D}_k, m-1)\right)$ operations in $\mathcal{K}$; this concludes the complexity analysis.

Probability analysis. The algorithm chooses $3m-1$ values in the base field: the $2m$ coordinates of the points $\mathbf{p}$ and $\mathbf{p}'$, and $m-1$ values γ for the rational reconstruction. Suppose that these values are chosen in the box Γ^{3m-1}, where Γ is a given subset of $\mathcal{K}$. We now estimate the number of choices that lead to success, using Zippel-Schwartz' Lemma from Zippel [1979] and Schwartz [1980].

Recall that this lemma states that given any subset Γ of $\mathcal{K}$, the number of zeros of a ℓ-variate polynomial of degree D in $\Gamma^\ell \subset \mathcal{K}^\ell$ is at most $D|\Gamma|^{\ell-1}$.

- Let us first suppose that the point $\mathbf{p}$ does not cancel the polynomial $\Delta_{\mathcal{W}}$ from Theorem 2, and that the jacobian determinant of $\mathbf{F}$ is invertible everywhere on the fiber above $\mathbf{p}$. Then by Proposition 11, the lifting can be initiated.

  By Theorem 2 and Zippel-Schwartz's Lemma, the first condition excludes at most $(3n(\deg \mathcal{W})^2 + n^2 \deg \mathcal{W})|\Gamma|^{m-1}$ values of $\mathbf{p}$, which give rise to $(3n(\deg \mathcal{W})^2 + n^2 \deg \mathcal{W})|\Gamma|^{3m-2}$ points in Γ^{3m-1}. Similarly, the second condition excludes at most $nd \deg \mathcal{W}|\Gamma|^{3m-2}$ points, since the intersection of $\mathcal{W}$ with the zero-set of the jacobian determinant has degree at most $nd \deg \mathcal{W}$.

- We suppose that $\mathbf{p}'$ does not cancel the polynomial $\Delta_{\mathcal{W}}$, so $\mathbf{r}'$ is the specialization of $\mathbf{T}$ at $\mathbf{p}'$. As above, this excludes at most $(3n(\deg \mathcal{W})^2 + n^2 \deg \mathcal{W})|\Gamma|^{3m-2}$ points.

- We then exclude the possibility that the lifting stops too early. This is the case if for some $\kappa < \lceil \log_2(\mathfrak{D}_k) \rceil$, the reconstruction of all rational functions in $\mathbf{r}$ is possible, yielding a triangular set $\mathbf{R} \neq \mathbf{T}$, whose specialization at $\mathbf{p}'$ nevertheless coincides with $\mathbf{r}'$.

  Let us fix $\mathbf{p}$. Then the coefficients of $\mathbf{T}$ and $\mathbf{R}$ are rational functions of degrees at most $\mathfrak{D}_k$ and $2^{\kappa-1}$, so the points $\mathbf{p}'$ where their specializations coincide are contained in an hypersurface of $\mathbb{A}^m(\overline{\mathcal{K}})$ of degree at most $\mathfrak{D}_k + 2^{\kappa-1}$.

  Taking all possible $\kappa < \lceil \log_2(\mathfrak{D}_k) \rceil$ into consideration shows that for fixed $\mathbf{p}$, $\mathbf{p}'$ must avoid an hypersurface in $\mathbb{A}^m(\overline{\mathcal{K}})$ of degree at most $\mathfrak{D}_k(\lceil \log_2(2\mathfrak{D}_k + 1) \rceil + 2)$, which excludes $\mathfrak{D}_k(\lceil \log_2(2\mathfrak{D}_k + 1) \rceil + 2)|\Gamma|^{m-1}$ values of $\mathbf{p}'$. Letting $\mathbf{p}$ and γ vary, this removes at most $\mathfrak{D}_k(\lceil \log_2(2\mathfrak{D}_k + 1) \rceil + 2)|\Gamma|^{3m-2}$ points in Γ^{3m-1}.

- The algorithm can now only fail at the last rational reconstruction. Let us fix $\mathbf{p}$. By Proposition 10, each rational reconstruction requires to choose $m-1$ values outside of an hypersurface of degree at most $4\mathfrak{D}_k(2\mathfrak{D}_k + 1)^2$. Since there are at most kD_n such reconstructions to perform, this discriminates at most $4kD_n\mathfrak{D}_k(2\mathfrak{D}_k + 1)^2|\Gamma|^{m-2}$ values of γ. Letting $\mathbf{p}$ and γ vary, this removes at most $4kD_n\mathfrak{D}_k(2\mathfrak{D}_k + 1)^2|\Gamma|^{3m-2}$ points in Γ^{3m-1}.

We sum all these estimates, and use the inequalities $D_n \leq \deg \mathcal{W} \leq d^n$ and $\mathfrak{D}_k \leq (2k^2+2)^k d^{2kn+n}$ from Theorem 1. After some rewriting and simplifying, we see that the above restrictions discriminate at most $50n^3(k^2+2)^{3k}d^{6kn+4n}|\Gamma|^{3m-2}$ points in Γ^{3m-1}. This concludes the probability analysis of Theorem 3.

7.3 Computing a Minimal Polynomial

We now drop the irreducibility assumption made above. Recall that we denote by $\mathcal{J}$ the ideal $(F_1, \ldots, F_n)$ and by $\mathcal{J}_P$ its extension in $\overline{\mathcal{K}}(\mathbf{P})[\mathbf{X}]$. Let $M_1 \in \mathcal{K}(\mathbf{P})[U]$ be the minimal polynomial of X_1 modulo $\mathcal{J}_P$. In this subsection, we show how to compute M_1 by lifting techniques, thus proving Theorem 4.

We first relate this minimal polynomial to triangular sets. Write the decomposition of $\mathcal{W} = \cup_{j \leq J} \mathcal{W}^j$, corresponding to the prime decomposition of $\mathcal{J}$ in $\mathcal{K}[\mathbf{P}, \mathbf{X}]$ and let $\mathbf{T}^j$ be the triangular set that describes the generic solutions of $\mathcal{W}^j$, for $j \leq J$. The first polynomials $T_1^1, \ldots, T_1^J$ may not be all distinct; without loss of generality, we assume that $T_1^1, \ldots, T_1^K$ are representatives of the distinct polynomials among them, for some $K \leq J$.

By construction, $\mathbf{T}^1, \ldots, \mathbf{T}^K$ define prime ideals in $\mathcal{K}(\mathbf{P})[\mathbf{X}]$, so $T_1^1, \ldots, T_1^K$ are irreducible in $\mathcal{K}(\mathbf{P})[X_1]$. Since they are pairwise distinct, they are pairwise coprime in both $\mathcal{K}(\mathbf{P})[X_1]$ and $\overline{\mathcal{K}}(\mathbf{P})[X_1]$. We deduce that their product is M_1.

Our lifting process does not yield directly the triangular sets $\mathbf{T}^j$. Indeed, the input is a resolution of a specialization of $\mathbf{F}$: its irreducible components may not be the traces of those of $\mathcal{W}$, since specialization may induce additional factorizations. Thus, we first address the question of lifting in presence of factorization, and deduce the proof of Theorem 4 in a second time.

7.3.1 Factorized Lifting

We fix some $j \leq J$ and let $\mathbf{T}^j$ be the triangular set which describes the generic solutions of $\mathcal{W}^j$. Let $\mathbf{p}$ be a point in $\mathcal{K}^m$ such that:

$\mathbf{H}_1$: $\mathbf{p}$ does not cancel the polynomial $\Delta_{\mathcal{W}^j}$ from Theorem 2.
$\mathbf{H}_2$: The jacobian determinant of $\mathbf{F}(\mathbf{p}, \mathbf{X})$ with respect to $\mathbf{X}$ is invertible on all solutions of the system $\mathbf{F}(\mathbf{p}, \mathbf{X})$.

For simplicity, we drop the superscript in $\mathbf{T}^j$, writing $\mathbf{T}$ instead. We assume without loss of generality that $\mathbf{p} = \mathbf{0}$ and let $\mathbf{t}$ be the specialization of $\mathbf{T}$ at $\mathbf{0}$. The following proposition shows that the lifting techniques apply to any *factor* of $\mathbf{t}$, which is required to prove Theorem 4. We use the notation

of Subsection 7.2.1, writing A for the power series ring $\mathcal{K}[[\mathbf{P}]]$ and $\mathfrak{m}$ for its maximal ideal.

Proposition 12 *Let* $\mathbf{r}$ *be a triangular set in* $\mathcal{K}[\mathbf{X}]$ *such that the ideal generated by* $\mathbf{r}$ *contains* $\mathbf{t}$. *Then there exists a triangular set* $\mathbf{R}$ *in* $A[\mathbf{X}]$ *such that the specialization* $\mathbf{R} \mod \mathfrak{m}$ *is* $\mathbf{r}$, *and the ideal generated by* $\mathbf{R}$ *contains* $\mathbf{T}$. *The approximations* $\mathbf{R} \mod \mathfrak{m}^{2^\kappa}$ *can be computed with the complexity given in Proposition 11.*

Proof. We first deduce the last statement from the existence of the triangular set $\mathbf{R}$. Indeed, suppose that $\mathbf{R}$ is such that $\mathbf{R} \mod \mathfrak{m} = \mathbf{r}$, and $\mathbf{T} = \mathbf{B}\mathbf{R}$ for some matrix $\mathbf{B}$. Since Hypotheses H_1' and H_2' hold for $\mathbf{T}$, these equalities show that they hold for $\mathbf{R}$ too, so Proposition 11 applies, as requested. Thus, we concentrate on proving the existence of the triangular set $\mathbf{R}$, and begin by treating a particular case.

A particular case. Let us first suppose that there exists $k \leq n$ such that the following holds. Let B denote $A[\mathbf{X}_{\leq k-1}]/\mathbf{T}_{\leq k-1}$ and $\mathfrak{n}$ the ideal of B induced by $\mathfrak{m}+(T_1, \ldots, T_{k-1})$. Thus, the quotient $B/\mathfrak{n}$ is $\mathcal{K}[\mathbf{X}_{\leq k-1}]/\mathbf{t}_{\leq k-1}$. Our assumption is:

- $\mathbf{r}_{\leq k-1} = \mathbf{t}_{\leq k-1}$;
- there exists a polynomial q_k in $B/\mathfrak{n}\,[X_k]$ such that $t_k = q_k r_k$ holds in $B/\mathfrak{n}\,[X_k]$;
- for j in $k+1, \ldots, n$, we see t_j as a polynomial in the variables $X_{k+1}, \ldots, X_j$ with coefficients in $B/\mathfrak{n}\,[X_k]$, and assume that r_j is obtained by reducing all these coefficients modulo r_k.

Since A is complete with respect to the $\mathfrak{m}$-adic topology, B is complete with respect to the $\mathfrak{n}$-adic topology. Hypotheses H_1' and H_2' imply that the derivative of t_k with respect to X_k is invertible in $B/\mathfrak{n}\,[X_k]/(t_k)$. Hensel's Lemma then shows that there exists Q_k and R_k in B such that $T_k = Q_k R_k$ holds in $B[X_k]$ and $r_k = R_k \mod \mathfrak{n}$. The polynomial R_k is defined in $B[X_k]$, but we may identify it to its canonical preimage in $A[X_1, \ldots, X_k] \subset A[X_1, \ldots, X_n]$.

For $j < k$, we define $R_j = T_j$. For $j > k$, we define R_j as follows. We see T_j as polynomial in the variables $X_{k+1}, \ldots, X_j$ with coefficients in $B[X_k]$, and define R_j by reducing all these coefficients modulo R_k. As such, this polynomial is a multivariate polynomial in $X_{k+1}, \ldots, X_j$ with coefficients in $A[X_1, \ldots, X_k]$ modulo $T_1, \ldots, T_{k-1}, R_k$, but as above, we may identify it with its canonical preimages in $A[X_1, \ldots, X_n]$. Through this identification, $\mathbf{r} = \mathbf{R} \mod \mathfrak{m}$.

We then prove the existence of a matrix $\mathbf{B}$ such that the equality $\mathbf{T} = \mathbf{B}\mathbf{R}$ holds, by successively constructing its lines.

- For $j < k$, we have $T_j = R_j$, so we take a line composed only of 0's, with 1 at entry j.
- Let us now take $j = k$. The equality $T_k = Q_k R_k$ in $B[X_k]$ can be rewritten in $A[X_1, \ldots, X_k]$ as $T_k = Q_k R_k + S_k$, where S_k is in the ideal $(T_1, \ldots, T_{k-1}) = (R_1, \ldots, R_{k-1})$. This enables to define the k-th line of $\mathbf{B}$.
- Finally, we take $j > k$. Then R_j is such that $R_j = T_j$ with all coefficients reduced modulo R_k in $B[X_k]$. Thus, $T_j = R_j + s_j$, where s_j is in the ideal generated by R_k in $B[X_k, \ldots, X_j]$. From the definition of B, this can be rewritten as $T_j = R_j + S_j$ in $A[X_1, \ldots, X_j]$, where S_j is in the ideal $(T_1, \ldots, T_{k-1}, R_k) = (R_1, \ldots, R_k)$.

This enables to complete the definition of $\mathbf{B}$, from which the proposition follows.

The general case. Let k be the least integer such that $r_k \neq t_k$; if $\mathbf{r} = \mathbf{t}$, we take $k = n + 1$. We prove by induction on k that if $\mathbf{T}$ satisfies hypotheses H'_1, H'_2, and $\mathbf{t} = \mathbf{T} \mod \mathfrak{m}$ belongs to the ideal generated by $\mathbf{r}$, then there exists a triangular set $\mathbf{R}$ such that $\mathbf{r} = \mathbf{R} \mod \mathfrak{m}$, and a $n \times n$ matrix $\mathbf{B}$ with entries in $A[\mathbf{X}]$ such that $\mathbf{T} = \mathbf{BR}$. We call this property $\mathcal{P}_k$; $\mathcal{P}_{n+1}$ is obvious, so we suppose that $k \leq n$ and that $\mathcal{P}$ is proved for $k + 1, \ldots, n + 1$.

Since t_k is in the ideal generated by $\mathbf{r}$, we deduce that r_k divides t_k in the polynomials ring over $\mathcal{K}[\mathbf{X}_{\leq k-1}]/\mathbf{t}_{\leq k-1}$. We then define a triangular set $\mathbf{s}$ in $\mathcal{K}[\mathbf{X}]$ as follows. We take $s_1, \ldots, s_k = r_1, \ldots, r_k$, and for $j > k$ we define s_j as t_j with all coefficient reduced modulo s_k. Thus $\mathbf{T}$ and $\mathbf{s}$ satisfy the hypotheses of the previous paragraphs, which enables to define a triangular set $\mathbf{S}$ and a matrix $\mathbf{B}$ such that $\mathbf{T} = \mathbf{BS}$ and $\mathbf{s} = \mathbf{S} \mod \mathfrak{m}$.

The triangular set $\mathbf{S}$ satisfies hypotheses H'_1 and H'_2. For $j > k$, $s_j - t_j$ is in the ideal generated by $\mathbf{r}$. Since t_j is in this ideal, s_j is in this ideal too. Consequently, we can apply our induction argument on $\mathbf{S}$ and $\mathbf{r}$, since now $\mathbf{s}$ and $\mathbf{r}$ coincide at least up to index k. This shows the existence of a triangular set $\mathbf{R}$ and a matrix $\mathbf{B}'$ such that $\mathbf{S} = \mathbf{B}'\mathbf{R}$, and $\mathbf{R} \mod \mathfrak{m} = \mathbf{r}$. Thus, $\mathbf{T} = \mathbf{BB}'\mathbf{R}$. This shows $\mathcal{P}_k$, which proves the proposition. □

7.3.2 Main Algorithm

The main algorithm follows again the lines given Subsection 7.1; we start by choosing a generic enough point in the parameter space. Precisely, we let $\mathbf{p}$ be a point in $\mathcal{K}^m$ such that:

$\mathbf{H}_1$: $\mathbf{p}$ does not cancel the polynomial $\delta_{\mathcal{W}}$ from Proposition 2.
$\mathbf{H}_2$: $\mathbf{p}$ cancels none of the polynomials $\Delta_{\mathcal{W}^j}$ from Theorem 2.

H_3 : the jacobian determinant of $\mathbf{F}$ with respect to $\mathbf{X}$ is invertible on all solutions of the system $\mathbf{F}(\mathbf{p}, \mathbf{X})$.

From these hypotheses, we deduce that $\mathbf{T}^1, \ldots, \mathbf{T}^J$ can be specialized at $\mathbf{p}$, and that the specializations $\mathbf{t}^1, \ldots, \mathbf{t}^J$ describe the solutions of $\mathbf{F}(\mathbf{p}, \mathbf{X})$. Unfortunately, there is no guarantee that the routine $\texttt{Solve}(\mathbf{F}, \mathbf{p})$ will precisely compute these specializations, since undesired factorizations may occur. We now show how to bypass this difficulty.

Let $\mathbf{r}^1, \ldots, \mathbf{r}^Q$ triangular sets that describe the solutions of $\mathbf{F}(\mathbf{p}, \mathbf{X})$, and define prime ideals in $\mathcal{K}[\mathbf{X}]$. Then for all i, there exists j such that $\mathbf{t}^j$ is in the ideal defined by $\mathbf{r}^i$. Using hypotheses H_2 and H_3, Proposition 12 shows that the lifting process can be applied to $\mathbf{r}^i$, yielding a triangular set $\mathbf{R}^i$ in $\mathcal{K}[[\mathbf{P}]][\mathbf{X}]$. The following proposition shows that these are enough to compute the polynomial M_1.

Proposition 13 *Reorder $\mathbf{r}^1, \ldots, \mathbf{r}^Q$ so that $r_1^1, \ldots, r_1^q$ are representatives of the distinct polynomials among $r_1^1, \ldots, r_1^Q$, for some $q \leq Q$. Then $\Pi_{i \leq q} R_1^i = M_1$ in $\mathcal{K}[[\mathbf{P}]][X_1]$.*

Proof. We first show that $R_1^1, \ldots, R_1^Q$ are irreducible in $\mathcal{K}[[\mathbf{P}]][X_1]$. Suppose that $R_1^i = GH$ in $\mathcal{K}[[\mathbf{P}]][X_1]$. Since R_1^i is monic, we may suppose that G and H are monic. Then $r_1^i = (G \mod \mathfrak{m})(H \mod \mathfrak{m})$. Since r_1^i is irreducible, it follows that for instance $G \mod \mathfrak{m}$ is a unit. Since G is monic, G is the constant 1, so R_1^i is irreducible.

The polynomials $R_1^1, \ldots, R_1^q$ are all pairwise distinct, hence pairwise coprime, since they are irreducible. Since each of them divides one of the polynomials T_1^j, each of them divides M_1. Thus $\Pi_{i \leq q} R_1^i$ divides M_1. The degree of $\Pi_{i \leq q} R_1^i$ is the degree of $\Pi_{i \leq q} r_1^i$, *i.e.* the cardinality of $\mu_1(\mathcal{W}_n(\mathbf{p}))$. Using hypothesis H_1 and Proposition 2, we see that it coincides with the generic degree D_1, that is, the degree of M_1. Thus, $\Pi_{i \leq q} R_1^i = M_1$. □

This is the basis of the following algorithm. The subroutine `Stop` computes the product of all polynomials r_1^i, and if possible, a rational reconstruction of all coefficients of the product. This gives a polynomial M, on which we apply a probabilistic check: as before, we test whether M specializes on the minimal polynomial of X_1 for a randomly chosen witness $\mathbf{p}'$. As in the previous subsection, this routine is denoted by `Stop`; the computation of minimal polynomial of X_1 for the specialization value $\mathbf{p}'$ is denoted by $\texttt{MinimalPolynomial}(\mathbf{F}, \mathbf{p}')$.

Computing a minimal polynomial

Input: The system $\mathbf{F}$, two points $\mathbf{p}, \mathbf{p}'$
Output: The minimal polynomial M_1.

$\mathbf{r}^1, \ldots, \mathbf{r}^q \leftarrow$ `Solve`$(\mathbf{F}, \mathbf{p})$
$m' \leftarrow$ `MinimalPolynomial`$(\mathbf{F}, \mathbf{p}')$
`while not(Finished) do`
  `for` i `in` $1, \ldots, q$ `do`
    $\mathbf{r}^i \leftarrow$ `Lift`$(\mathbf{r}^i, \mathbf{F})$
  `Finished`,$M_1 \leftarrow$ `Stop`$(\mathbf{r}^1, \ldots, \mathbf{r}^q, m')$
`end while`
`return` M_1

The complexity and probability analyses strictly follow those of Subsection 7.2. The only notable differences are that we now take hypotheses H_1, H_2 and H_3 into account, and that the coefficients of M_1 are of degree bounded by d^n, according to Proposition 3. We leave the details of the computation to the reader.

8 Applications

To conclude this article, we present three applications of our algorithms, coming from geometry, number theory and cryptography.

The algorithms are implemented in Magma. They outperformed the built-in functions on all these examples, so we rather focus on comparing times with the approach through primitive element techniques presented in Schost [2003]. This confirms the advantage of triangular techniques for problems such as presented here, where only a partial information is required.

For all these examples, the probabilistic aspect was not a problem. When verification was possible, it never revealed an error. Further, in many situations, problem-specific arguments can show that the output is correct once it is computed.

All computations were done on a Compaq XP/1000 EV6 from the MEDICIS resource center, see `http://www.medicis.polytechnique.fr/`.

Let $\varphi_i = N_i/D_i\,(i = 1, 2, 3)$ be a triple of rational functions in $\mathbb{Q}(X_1, X_2)$. Take $D = \mathrm{lcm}(D_1, D_2, D_3)$ and let φ be the map

$$\begin{aligned} \varphi \ : \mathbb{R}^2 - V(D) &\to \qquad\quad \mathbb{R}^3 \\ \mathbf{x} \qquad &\mapsto (\varphi_1(\mathbf{x}), \varphi_2(\mathbf{x}), \varphi_3(\mathbf{x}))\,. \end{aligned}$$

We suppose that φ is not degenerate, in the sense that its image has dimension 2 as a constructible set. Then the problem of *implicitization* consists in computing an equation M defining the closure $\mathcal{V}$ of the image of φ. This question has attracted a lot of attention, notably because of its relevance for Computer Aided Geometric Design, see Cox [2001], d'Andréa [2001], Ruatta [2002], Busé et al. [2002], Busé and Jouanolou [2002] and references therein.

Many of these solutions are based on suitable resultant formulas. We here propose a solution that inherits the good complexity of the above algorithms, applies in all generality and is quite practical. We note the obvious generalization to n-space; nevertheless we stick to dimension 2 for simplicity.

Consider the polynomial system

$$\mathbf{F} = \{D_i(X_1, X_2)Y_i - N_i(X_1, X_2)\ (i = 1, 2, 3), \quad D(X_1, X_2)Z - 1\}$$

in $\mathbb{Q}[Y_1, Y_2, Y_3, X_1, X_2, Z]$, let $\mathcal{W} \subset \mathbb{A}^6(\mathbb{C})$ be its zero-set and $\mathcal{V}$ the projection of $\mathcal{W}$ on the subspace of coordinates Y_1, Y_2, Y_3. What we are looking for is an equation defining the closure of $\mathcal{V}$.

Without loss of generality, we suppose that the projection of $\mathcal{V}$ is dense in the space $\mathbb{A}^2(\mathbb{C})$ of coordinates Y_1, Y_2; then Sard's Theorem shows that the Jacobian determinant of $\mathbf{F}$ with respect to Y_3, X_1, X_2, Z is invertible on all points of $\mathcal{W}$ above some open subset of $\mathbb{A}^2(\mathbb{C})$. Since $\mathcal{W}$ is irreducible, this Jacobian determinant is thus invertible on a dense subset of $\mathcal{W}$, so we can apply the previous results.

Let us see the equation M in $\mathbb{Q}[Y_1, Y_2][Y_3]$. By Proposition 3, the minimal polynomial of Y_3 modulo the ideal generated by $\mathbf{F}$ in $\mathbb{C}(Y_1, Y_2)[Y_3, X_1, X_2, Z]$ is M, divided by its leading coefficient. Thus, we can apply Theorem 4 and use the underlying algorithm to compute M.

From the practical viewpoint, the additional variable Z introduced for applying Rabinovicz' trick burdens the computation. Referring to the proof of Proposition 11, the special shape of the system $\mathbf{F}$ shows that the lifting phase

can be done using only the system

$$\widetilde{\mathbf{F}} = \{D_i(X_1, X_2)Y_i - N_i(X_1, X_2) \ (i = 1, 2, 3)\}$$

in $\mathbb{Q}[Y_1, Y_2, Y_3, X_1, X_2]$. This reflects the local nature of lifting techniques.

We illustrate the method on an example from invariant theory [Bershenko-Kogan, 2000], with

$$\begin{aligned}
\varphi_1 &= \frac{1}{3}\frac{X_1X_2^2 + X_2^2 + X_2 + X_1^2X_2 - 6X_1X_2 + X_1 + X_1^2}{X_1X_2},\\
\varphi_2 &= -\frac{1}{9}\frac{(X_2 - 1 + X_1)(-X_2 - 1 + X_1)(-X_2 + 1 + X_1)}{X_1X_2},\\
\varphi_3 &= \frac{1}{36}\frac{(X_1+1)^2(X_2+1)^2(P(X_1) + P(X_2) + X_1X_2^3 - X_1^2X_2^2 + X_2X_1^3)^2}{X_1^2X_2^2(X_1 + X_2 + 1)^4}
\end{aligned}$$

and $P(X) = X + 2X^2 + X^3$. In Schost [2003], we treated this example using a minimal polynomial computation modulo a parametric geometric resolution, that is, primitive element techniques; this took 7 minutes. The time now drops to 20 seconds using triangular sets.

8.2 Genus 2 Curves with (2,2)-split Jacobian

Genus 2 curves with Jacobian (2,2)-isogeneous to a product of elliptic curves appear frequently in number theory: rank and torsion records are obtained for such curves, see Kulesz [1995, 1999], Howe et al. [2000]. In Gaudry and Schost [2001], we give an explicit classification of such situations, using the algorithms presented here. We now describe part of the necessary computations.

Isomorphism classes of genus 2 (resp. elliptic) curves are classified by their Igusa invariants j_1, j_2, j_3 (resp. by their j-invariant). There exists a polynomial $T(J_1, J_2, J_3)$ such that a genus 2 curve has (2,2)-split Jacobian if and only if its Igusa invariants cancel T; then the j-invariants of the underlying elliptic curves are the roots of a polynomial of degree 2, whose coefficients are rational functions of j_1, j_2, j_3. We are thus looking for this polynomial, together with the polynomial T.

A genus 2 curve with (2,2)-split Jacobian admits the equation

$$y^2 = x^6 + ax^4 + bx^2 + 1;$$

its Igusa invariants are then rational functions $J_1(a, b), J_2(a, b), J_3(a, b)$. The

underlying elliptic curves are isomorphic to the curves

$$y^2 = x^3 + ax^2 + bx + 1;$$

their j-invariant is a rational function $J(a, b)$. Let thus $\mathbf{F}$ be the system obtained in $\mathbb{Q}[j_1, j_2, j_3, j, a, b, Z]$ after canceling denominators in

$$\{j - J(a, b), j_1 - J_1(a, b), j_2 - J_2(a, b), j_3 - J_3(a, b)\}$$

and removing the zero-set of the denominators of J, J_1, J_2, J_3 by using Rabinovicz' trick with the variable Z. Just as in the previous subsection, we note that the lifting can done without using the variable Z.

We take j_1, j_2 for parameters, and work in $\mathbb{Q}(j_1, j_2)[j_3, j, a, b, Z]$ modulo the ideal generated by $\mathbf{F}$. This ideal is prime of dimension zero, so its solutions are represented by a triangular set in $\mathbb{Q}(j_1, j_2)[j_3, j, a, b, Z]$. The first polynomial $T_1 \in \mathbb{Q}(j_1, j_2)[j_3]$ is the relation T mentioned above, which was already known to Mestre [1990]. As requested, the second polynomial $T_2 \in \mathbb{Q}(j_1, j_2)[j_3, j]$ gives j in terms of j_1, j_2, j_3 when the denominators of its coefficients do not vanish.

We use the algorithm of Subsection 7.2. The polynomial T_1 is computed in 22 seconds, and T_1, T_2 in 140 seconds. As a comparison, using the algorithm of Schost [2003], computing a representation by primitive element requires more than 400 seconds. This illustrates again the interest of the "triangular" approach, when only a partial information is wanted.

8.3 Modular Equations

In Gaudry and Schost [2002], *modular equations* for hyperelliptic curves are defined. Over a finite base field, they aim at simplifying the problem of point-counting in the Jacobian of such curves, a question of first importance for hyperelliptic cryptosystems, see Gaudry [2000].

In fixed genus, modular equations are univariate polynomials indexed by a prime ℓ. Given a hyperelliptic curve C and a prime ℓ, the ℓ-th modular equation partly describes the structure of the ℓ-torsion divisors in the Jacobian of C; its factorization pattern gives information on the cardinality of the Jacobian of C modulo ℓ.

The ℓ-torsion divisors form a finite group G_ℓ, and are solutions of an algebraic system, in suitable coordinates. Introducing a well-chosen function t_ℓ on G_ℓ, the modular equation becomes the minimal polynomial Ξ_ℓ of t_ℓ modulo G_ℓ.

Computing Ξ_ℓ for a generic curve is done using the algorithm of Subsection 7.3.

We treated the 3-torsion in genus 2; the corresponding system has 3 equations in 3 unknowns X_1, X_2, X_3 and 3 parameters P_1, P_2, P_3 which parameterize curves of genus 2. The output $\Xi_3 \in \mathbb{Q}(P_1, P_2, P_3)[T]$ is computed within 4.5 hours; for comparison, it takes more than 20 hours to compute a representation by a primitive element. The polynomial Ξ_3 is now used within Magma's hyperelliptic curves package `CrvHyp`.

References

M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities and idempotents for zero-dimensional systems. In *Proceedings of MEGA'94*, volume 143 of *Progress in Mathematics*, pages 1–15. Birkhäuser, 1996.

P. Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université Paris VI, 1999.

P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28(1,2):45–124, 1999.

W. Baur and V. Strassen. The complexity of partial derivatives. *Theoretical Computer Science*, 22:317–330, 1983.

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

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

L. Busé, D. Cox, and C. d'Andréa. Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points. Preprint math.AG/0205251, 2002.

L. Busé and J.-P. Jouanolou. On the closed image of a rational map and the implicitization problem. Preprint math.AG/0210096, 2002.

D. Cox. Equations of parametric curves and surfaces via syzygies. *Contemporary Mathematics*, 286:1–20, 2001.

C. d'Andréa. Resultants and moving surfaces. *Journal of Symbolic Computation*, 31(5):585–602, 2001.

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

D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, 1996.

G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Proceedings of MEGA'90*, volume 94 of *Progress in Mathematics*, pages 119–142. Birkhäuser, 1990.

P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie.* PhD thesis, École polytechnique, 2000.

P. Gaudry and É. Schost. On the invariants of the quotients of the Jacobian of a curve of genus 2. In *Proceedings of AAECC-14*, volume 2227 of *Lecture*

Notes in Computer Science, pages 373–386. Springer, 2001.

P. Gaudry and É. Schost. Modular equations for hyperelliptic curves. Manuscript, École polytechnique, France, 2002.

P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Gröbner bases. In *Proceedings of AAECC-5*, volume 356 of *Lecture Notes in Computer Science*, pages 247–257. Springer, 1989.

M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower bounds for Diophantine approximation. *Journal of Pure and Applied Algebra*, 117,118:277–317, 1997.

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

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

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

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

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

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

E. Howe, F. Leprévost, and B. Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Mathematicum*, 12:315–364, 2000.

É. Hubert. Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems. In *Symbolic and Numerical Scientific Computations*. Springer. To appear.

M. Kalkbrener. *Three contributions to elimination theory.* PhD thesis, Kepler University, Linz, 1991.

T. Krick and L. M. Pardo. A computational method for Diophantine approximation. In *Proceedings of MEGA'94*, volume 143 of *Progress in Mathematics*, pages 193–254. Birkhäuser, 1996.

T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. Journal*, 109:521–598, 2001.

T. Krick, J. Sabia, and P. Solernó. On intrinsic bounds in the Nullstellensatz. *Applicable Algebra in Engineering, Communication and Computing*, 8:125–134, 1997.

L. Kulesz. Courbes algébriques de genre 2 possédant de nombreux points rationnels. *C. R. Acad. Sci. Paris*, 321:91–94, 1995.

L. Kulesz. Application de la méthode de Dem'janenko-Manin à certaines familles de courbes de genre 2 et 3. *Journal of Number Theory*, 76:130–146,

1999.

L. Langemyr. Algorithms for a multiple algebraic extension. In *Proceedings of MEGA'90*, volume 94 of *Progress in Mathematics*, pages 235–248. Birkhäuser, 1990.

D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Applied Mathematics*, 33:147–160, 1991.

D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13(2):117–133, 1992.

G. Lecerf. Quadratic Newton iteration for systems with multiplicity. *Foundations of Computational Mathematics*, 2:247–293, 2002.

G. Lecerf and É. Schost. Fast multivariate power series multiplication in characteristic zero. *SADIO Electronic Journal on Informatics and Operations Research.*, 2003. To appear.

M. Moreno Maza. *Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques*. PhD thesis, Université Paris VI, 1997.

J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Proceedings of MEGA'90*, volume 94 of *Progress in Mathematics*, pages 313–334. Birkhäuser, 1990.

S. Morrison. The differential ideal $[P] : M^\infty$. *Journal of Symbolic Computation*, 28(4/5):631–656, 1999.

B. Mourrain and O. Ruatta. Relation between roots and coefficients, interpolation and application to system solving. *Journal of Symbolic Computation*, 33(5):679–699, 2002.

L. M. Pardo. How lower and upper complexity bounds meet in elimination theory. In *Proceedings of AAECC-11*, volume 948 of *Lecture Notes in Computer Science*, pages 33–69. Springer, 1995.

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

O. Ruatta. *Dualité algébrique, structures et applications*. PhD thesis, École doctorale Mathématiques et Informatique de Marseille, 2002.

J. Sabia and P. Solernó. Bounds for traces in complete intersections and degrees in the Nullstellensatz. *Applicable Algebra in Engineering, Communication and Computing*, 6:353–376, 1996.

A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7:281–292, 1971.

É. Schost. Degree bounds and lifting techniques for triangular sets. In *Proceedings of ISSAC 02*, pages 238–245. ACM Press, 2002.

É. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13:349–393, 2003.

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

A. Szanto. *Computation with polynomial systems*. PhD thesis, Cornell University, 1999.

W. Trinks. On improving approximate results of Buchberger's algorithm by Newton's method. In *Proceedings of EUROCAL'85*, volume 204 of *Lecture Notes in Computer Science*, pages 608–611. Springer-Verlag, 1985.

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

F. Winkler. A p-adic approach to the computation of Gröbner bases. *Journal of Symbolic Computation*, 6(2/3):287–304, 1988.

R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of EUROSAM'79*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979.