

Polynomial equation solving by lifting procedures for ramified fibers

A.Bompadre ^{a,1}G.Matera ^{b,c,*}R.Wachenchauzer ^dA.Waissbein ^{a,2}

^a*Departamento de Matemáticas, Facultad de Ciencias y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I (1428) Buenos Aires, Argentina.*

^b*Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, Campus Universitario, José M. Gutiérrez 1150 (1613) Los Polvorines, Buenos Aires, Argentina.*

^c*Member of the CONICET, Argentina.*

^d*Departamento de Computación, Facultad de Ingeniería, Universidad de Buenos Aires, Av. Paseo Colón 850 (1063) Buenos Aires, Argentina.*

Abstract

Let be given a parametric polynomial equation system which represents a generically-unramified family of zero-dimensional algebraic varieties. We exhibit an efficient algorithm which computes a complete description of the solution set of an arbitrary parameter instance from a complete description of the infinitesimal structure of a particular ramified parameter instance of our family. This generalizes in the case of space curves previous methods of Heintz *et al.* and Schost, which require the given parameter instance to be unramified. We illustrate our method solving particular polynomial equation systems by deformation techniques.

Key words: Efficient polynomial equation solving, ramified fibers of dominant mappings, Puiseux expansions of space curves, Newton-Hensel lifting.

* Corresponding author.

Email addresses: `abompadr@mit.edu` (A.Bompadre), `gmatera@ungs.edu.ar` (G.Matera), `rosita@mara.fi.uba.ar` (R.Wachenchauzer), `awaissbe@dm.uba.ar` (A.Waissbein).

¹ *Present address:* MIT Operations Research Center, 77, Massachusetts Avenue Building E40-130 Cambridge, MA 02139 USA.

² Research was partially supported by the following Argentinian and German grants : UBACyT X198, PIP CONICET 2461, BMBF-SETCIP AL/PA/01-EIII/02, UNGS 30/3005 and beca de posgrado interno CONICET. Some of the results presented here were first announced at the *Workshop Argentino de Informática Teórica*, WAIT'01, held in September 2001 (see [12]).

1 Introduction

Algorithmic multivariate polynomial system solving is a central theme of computational algebraic geometry, which arises in connection with numerous scientific and technical problems (see e.g. [21], [62]). In order to solve polynomial equation systems, several symbolic and numeric algorithms have been proposed. Unfortunately, typical symbolic elimination methods based on rewriting techniques (see e.g. [19], [20]) have superexponential complexity, which makes them infeasible for realistically sized problems. On the other hand, in the case of typical numeric (iterative) techniques (see e.g. [55]), it is not easy to obtain good initial guesses for the solutions of the system under consideration.

In order to circumvent these difficulties different attempts were made, from the symbolic and the numeric point of view, to solve polynomial equation systems by means of deformation techniques based on a perturbation of the original system and a subsequent path-following method (see e.g. [18], [6], [29], [1], [42], [10]). A common drawback of these methods is the fact that they typically introduce spurious solutions which may be computationally expensive to identify and eliminate in order to obtain the actual solutions.

In the series of papers [31], [52], [30], [28] and [32], a new symbolic elimination algorithm was introduced. This algorithm is based on a flat deformation of a certain morphism of affine varieties, which was isolated and refined in [39] (see also [58]). More precisely, let V be a \mathbb{Q} -definable equidimensional affine variety of dimension m , and let be given a generically unramified, finite morphism $\pi : V \rightarrow \mathbb{C}^m$. Then, given a complete description of a particular unramified fiber $\pi^{-1}(y_0)$, [39] exhibits an algorithm which computes a complete description of an arbitrary fiber $\pi^{-1}(y)$ using a global version of the Newton–Hensel lifting.

This deformation technique may be used in order to solve particular polynomial equation systems. A typical application of this method is the following (see e.g. [39], [38], [53]): suppose that we are given a sparse polynomial equation system which defines a zero-dimensional affine variety. Suppose further that a suitable replacement of some of the coefficients of the original polynomials by indeterminates gives a generically unramified family of zero-dimensional affine varieties, with underlying finite morphism. Then, if there exists a particular unramified fiber which is easy to solve, it is possible to solve the original system by using the algorithm of [39].

Our main objective here is to extend the “catalogue” of polynomial equation systems which may be treated using this deformation technique. For this purpose, we are going to exhibit an algorithm which, given a generically unramified family of zero-dimensional affine varieties, represented by a dominant (not necessarily finite) morphism $\pi : V \rightarrow \mathbb{C}^m$, and the infinitesimal struc-

ture of a particular (eventually *ramified*) fiber $\pi^{-1}(y_0)$, computes a complete description of any fiber $\pi^{-1}(y)$.

In view of the main outcome of the articles [40] and [33], namely the conclusion that the elimination techniques of [30] and [28] can be efficiently reduced to the case of algebraic curves (i.e. affine equidimensional algebraic subvarieties of dimension 1 of \mathbb{C}^{n+1}), in this article we shall limit ourselves to this case.

Let $V \subset \mathbb{C}^{n+1}$ be a \mathbb{Q} -definable algebraic space curve, and let us assume that the morphism $\pi : V \rightarrow \mathbb{C}$ induced by the canonical projection in the first coordinate is dominant and generically unramified. Let $\pi^{-1}(\varepsilon_0)$ be a finite and ramified fiber. Suppose further that we are given the infinitesimal structure of $\pi^{-1}(\varepsilon_0)$, i.e. the set of singular parts of the Puiseux expansions of the branches of V lying above ε_0 (see Section 2.2). Then we exhibit an algorithm which computes a complete description of an arbitrary fiber $\pi^{-1}(\varepsilon)$ (see Section 4).

Our algorithmic method is essentially based on a new variant of the global Newton–Hensel procedure of [30] and [28] which is described in Section 3. Its time–space complexity is roughly $O(\delta D^\alpha)$, where δ is the degree of V , D is the degree of π and $\alpha = 1$ in several important cases. Then our algorithm extends and improves the procedures in [39] and [58]. Furthermore, our algorithm treats all the branches of V lying above ε_0 separately, improving thus the refinements of [39, Section 3].

Finally, in Section 5 we illustrate our method on a few examples, where the deformation technique of [39] cannot be applied. We solve Pham–Brieskorn systems, examples provided by discretization problems of partial differential equations and generalized Reimer systems.

2 Preliminaries

In this section we fix the notation and terminology used throughout this paper. In Section 2.1 we introduce the terminology about projections and the notion of geometric solution of an affine variety. In Section 2.2 we introduce terminology about space curves, extending the usual terminology of Puiseux expansions of plane curves (see e.g. [64]) and rational Puiseux expansions (see e.g. [23], [65]). Finally, in Section 2.3 we fix our computational model.

2.1 Geometric solutions

We use standard notions and notations of commutative algebra and algebraic geometry, which can be found in e.g. [24], [48], [60], [45].

For a given algebraically closed field k and $m \in \mathbb{N}$, we denote by $\mathbb{A}^m(k)$ the m -dimensional affine space k^m equipped with its Zariski topology over k . In particular, we shall use the notation $\mathbb{A}^m := \mathbb{A}^m(\mathbb{C})$. Let us fix $n \in \mathbb{N}$. Points in \mathbb{A}^{n+1} shall be denoted either by (ε, x) , with $\varepsilon \in \mathbb{C}$ and $x \in \mathbb{C}^n$, or by $(\varepsilon, x_1, \dots, x_n)$ with $\varepsilon, x_1, \dots, x_n \in \mathbb{C}$.

Let $\mathcal{E}, X_1, \dots, X_n$ be indeterminates over \mathbb{Q} , let $X := (X_1, \dots, X_n)$, and let $\mathbb{Q}[\mathcal{E}, X] := \mathbb{Q}[\mathcal{E}, X_1, \dots, X_n]$ be the ring of polynomials in the variables \mathcal{E}, X with coefficients in \mathbb{Q} . Let F_1, \dots, F_n be polynomials in $\mathbb{Q}[\mathcal{E}, X]$ which form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$ and generate a radical ideal in $\mathbb{Q}[\mathcal{E}, X]$. Then

$$V := \{(\varepsilon, x) \in \mathbb{A}^{n+1} : F_1(\varepsilon, x) = 0, \dots, F_n(\varepsilon, x) = 0\},$$

is an equidimensional affine variety of dimension $\dim V = 1$. The coordinate ring $\mathbb{Q}[V]$ and the ring of rational functions $\mathbb{Q}(V)$ of V are defined as the quotient ring $\mathbb{Q}[\mathcal{E}, X]/(F_1, \dots, F_n)$ and its total ring of fractions respectively.

Let $\pi : V \rightarrow \mathbb{A}^1$ be the morphism induced by the restriction to V of the canonical projection in the first coordinate $\pi(\varepsilon, x) := \varepsilon$. Let $V = \mathcal{C}_1 \cup \dots \cup \mathcal{C}_s$ be the decomposition of V into irreducible components. Suppose that $\pi|_{\mathcal{C}_i}$ is dominant for $1 \leq i \leq s$. We define the degree of π as the number $D := \sum_{i=1}^s [\mathbb{Q}(\mathcal{C}_i) : \mathbb{Q}(\mathcal{E})]$, where $[\mathbb{Q}(\mathcal{C}_i) : \mathbb{Q}(\mathcal{E})]$ denotes the degree of the (finite) field extension $\mathbb{Q}(\mathcal{E}) \hookrightarrow \mathbb{Q}(\mathcal{C}_i)$ for $1 \leq i \leq s$.

We assume that π is *generically unramified*, i.e. the fiber $\pi^{-1}(\varepsilon)$ consists of exactly D points for a generic value $\varepsilon \in \mathbb{A}^1$. This implies that the Jacobian determinant $J_F := \det(\partial F_i / \partial X_j)_{1 \leq i, j \leq n}$ is not a zero divisor in $\mathbb{Q}[V]$.

Let U be a nonzero linear form of $\mathbb{Q}[X]$ and let u be the element of $\mathbb{Q}[V]$ induced by U . Let $\pi_u : V \rightarrow \mathbb{A}^2$ be the morphism defined by $\pi_u(\varepsilon, x) := (\varepsilon, u(x))$. By a standard argument we conclude that the Zariski closure $\overline{\pi_u(V)}$ of the image of V under π_u is a \mathbb{Q} -definable hypersurface of \mathbb{A}^2 . Let Z be an indeterminate over \mathbb{Q} . Then there exists a unique (up to scaling by nonzero elements of \mathbb{Q}) minimal equation $M_u \in \mathbb{Q}[\mathcal{E}, Z]$ defining $\overline{\pi_u(V)}$. From the Bézout inequality (see e.g. [36], [26]) we deduce the estimate $\deg M_u \leq \deg V$. On the other hand, we have the estimate $\deg_Z M_u \leq D$. Let $m_u \in \mathbb{Q}(\mathcal{E})[Z]$ denote the (unique) monic multiple of M_u with $\deg_Z m_u = \deg_Z M_u$. We call m_u the *projection polynomial* of u in V .

We define the *Projection Problem* as follows: given F_1, \dots, F_n and the linear form $U \in \mathbb{Q}[X]$, find the projection polynomial m_u .

It is well-known that there exists a non-empty Zariski open set $\mathcal{U} \subset \mathbb{A}^n$ such that for any linear form $U := \lambda_1 X_1 + \dots + \lambda_n X_n$ with $(\lambda_1, \dots, \lambda_n) \in \mathcal{U}$ we have $\deg_Z m_u = D$. Any linear form satisfying this condition is called *generic*. Let us observe that for any generic linear form $U \in \mathbb{Q}[X]$, the induced coordinate

function u is a *primitive element* of the \mathbb{Q} -algebra extension $\mathbb{Q}(\mathcal{E}) \hookrightarrow \mathbb{Q}(V)$, whose minimal polynomial over $\mathbb{Q}(\mathcal{E})$ equals m_u .

Let $U \in \mathbb{Q}[X]$ be a generic linear form. Using a suitable variant of the so-called Shape Lemma (see e.g. [56], [33]), the computation of the projection m_u can be easily extended to a symbolic solution of V in the following sense (see e.g. [30], [28], [33]). A *geometric solution* of the affine variety V consists of:

- a generic linear form $U \in \mathbb{Q}[X]$,
- the projection polynomial $m_u \in \mathbb{Q}(\mathcal{E})[Z]$.
- elements v_1, \dots, v_n of $\mathbb{Q}(\mathcal{E})[Z]$ such that $\frac{\partial m_u}{\partial Z} X_i \equiv v_i \pmod{\mathbb{Q}(\mathcal{E}) \otimes \mathbb{Q}[V]}$ and $\deg_Z v_i < D$ hold for $1 \leq i \leq n$.

This notion of geometric solution has a long history, going back at least to [44] (see also [47], [67]). One might consider [18] and [27] as early references where this notion was implicitly used in modern symbolic computation.

2.2 Space Curves

We maintain the notations and assumptions introduced in Section 2.1. Let T be an indeterminate over \mathbb{Q} . A *parameterization* of the curve V is a non-constant vector $(\tilde{\mathcal{E}}, \tilde{X})$ of elements of the field of Laurent series $\overline{\mathbb{Q}}((T))$, with $\tilde{X} := (\tilde{X}_1, \dots, \tilde{X}_n) \in \overline{\mathbb{Q}}((T))^n$, such that $F_1(\tilde{\mathcal{E}}, \tilde{X}) = 0, \dots, F_n(\tilde{\mathcal{E}}, \tilde{X}) = 0$ holds in $\overline{\mathbb{Q}}((T))$. A parameterization $(\tilde{\mathcal{E}}, \tilde{X})$ is called *irreducible* if there does not exist an integer $k > 1$ for which $(\tilde{\mathcal{E}}, \tilde{X}) \in \overline{\mathbb{Q}}((T^k))^{n+1}$ holds. The *coefficient field* of a parameterization $(\tilde{\mathcal{E}}, \tilde{X})$ of V is the field extension of \mathbb{Q} generated by the coefficients of the series $\tilde{\mathcal{E}}, \tilde{X}_1, \dots, \tilde{X}_n$.

We define the *order* $o_T(\varphi)$ of $\varphi \in \overline{\mathbb{Q}}((T))$ as the least power of T appearing with a nonzero coefficient in φ . Two parameterizations $(\tilde{\mathcal{E}}, \tilde{X})$ and $(\tilde{\mathcal{E}}', \tilde{X}')$ are called *equivalent* if there exists a power series $\varphi \in \mathbb{C}[[T]]$ of order 1 such that $\tilde{\mathcal{E}}(T) = \tilde{\mathcal{E}}'(\varphi(T))$, $\tilde{X}_1(T) = \tilde{X}'_1(\varphi(T))$, \dots , $\tilde{X}_n(T) = \tilde{X}'_n(\varphi(T))$ holds in $\overline{\mathbb{Q}}((T))$. A *branch* \mathcal{C} of the curve V is defined as the equivalence class of an irreducible parameterization of V . We say that a branch \mathcal{C} lies above a point $\varepsilon \in \mathbb{A}^1$ if there exists a parameterization $(\tilde{\mathcal{E}}, \tilde{X})$ in the equivalence class that defines the branch \mathcal{C} with $\tilde{\mathcal{E}} \in \overline{\mathbb{Q}}[[T]]$ and $\tilde{\mathcal{E}}(0) = \varepsilon$.

In what follows we shall consider the branches of V lying above 0. It is well-known that if 0 is an unramified value of the morphism $\pi : V \rightarrow \mathbb{A}^1$ of Section 2.1, then all the branches of V lying above 0 have a parameterization of the form (T, \tilde{X}) with $\tilde{X} \in \mathbb{Q}[[T]]^n$. Furthermore, efficient algorithms considering the projection problem in this case are known (see e.g. [39], [58]). In this article we shall suppose that the fiber $\pi^{-1}(0)$ is finite and (scheme-theoretically)

ramified, i.e. the condition $\#(\pi^{-1}(0)) < D$ holds.

Now we explain how the parameterizations of the branches of V lying above 0 can be represented by means of Puiseux series in \mathcal{E} . Let $\overline{\mathbb{Q}}(\mathcal{E})^* := \cup_{q \geq 0} \overline{\mathbb{Q}}(\mathcal{E}^{1/q})$ denote the field of Puiseux series in the variable \mathcal{E} over $\overline{\mathbb{Q}}$. It is well-known that $\overline{\mathbb{Q}}(\mathcal{E})^*$ is an algebraically closed field. In fact, it is the algebraic closure of $\mathbb{Q}(\mathcal{E})$ (see e.g. [64]).

Let us consider F_1, \dots, F_n as elements of the polynomial ring $\overline{\mathbb{Q}}(\mathcal{E})^*[X]$. Since the \mathbb{Q} -algebra extension $\mathbb{Q}(\mathcal{E}) \hookrightarrow \mathbb{Q}(V)$ is finitely generated, it follows that the affine variety $\{\bar{x} \in \mathbb{A}^n(\overline{\mathbb{Q}}(\mathcal{E})^*) : F_1(\bar{x}) = 0, \dots, F_n(\bar{x}) = 0\}$ has dimension zero. Therefore, under our hypotheses there exist $D := \deg \pi$ distinct n -tuples $x^{(\ell)} := (x_1^{(\ell)}, \dots, x_n^{(\ell)}) \in (\overline{\mathbb{Q}}(\mathcal{E})^*)^n$ of Puiseux series which are solutions of the system defined by F_1, \dots, F_n over $\overline{\mathbb{Q}}(\mathcal{E})^*$, i.e. such that the following equalities hold in $\overline{\mathbb{Q}}(\mathcal{E})^*$ for $1 \leq \ell \leq D$:

$$F_1(\mathcal{E}, x^{(\ell)}) = 0, \dots, F_n(\mathcal{E}, x^{(\ell)}) = 0. \quad (1)$$

For $1 \leq \ell \leq D$, let us write $x^{(\ell)} := (x_1^{(\ell)}, \dots, x_n^{(\ell)})$ and $x_i^{(\ell)} := \sum_{m \geq m_\ell} a_{i,m}^{(\ell)} \cdot \mathcal{E}^{\frac{m}{e_\ell}}$ ($1 \leq i \leq n$), with $e_\ell \in \mathbb{N}$, $m_\ell \in \mathbb{Z}$ and $a_{i,m}^{(\ell)} \in \overline{\mathbb{Q}}$. Without loss of generality we may assume for $1 \leq \ell \leq D$ that e_ℓ has no common factors with the greatest common divisor of the set of m 's for which $a_{i,m}^{(\ell)} \neq 0$ holds. The number e_ℓ is called the *ramification index* of the series $x^{(\ell)}$. Let us remark that for $1 \leq \ell \leq D$ the coefficient field generated by all the coordinates of $x^{(\ell)}$ is a finite extension of \mathbb{Q} (see e.g. [23]). Its degree f_ℓ is called the *residual degree* of $x^{(\ell)}$.

Following [23] (see also [65]), a set of non-equivalent parameterizations

$$\{(\tilde{\mathcal{E}}^{(1)}, \tilde{X}^{(1)}), \dots, (\tilde{\mathcal{E}}^{(\hat{g})}, \tilde{X}^{(\hat{g})})\} \subset \overline{\mathbb{Q}}((T))^{n+1} \quad (2)$$

containing a complete set of representatives of the branches of V lying above 0 is called a *system of rational Puiseux expansions* (of the branches of V lying above 0) if it is invariant under the action of the Galois group of the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$ and $\tilde{\mathcal{E}}^{(\ell)} = \lambda_\ell T^{e_\ell}$, with $e_\ell \in \mathbb{N}$ and $\lambda_\ell \in \overline{\mathbb{Q}} \setminus \{0\}$ for $1 \leq \ell \leq \hat{g}$. Let g be the number of orbits defined on the set (2) under the action of the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ and suppose that we have chosen the numbering in (2) such that the first g elements represent different orbits.

Let us observe that from a given system of rational Puiseux expansions we may easily obtain the system of classical Puiseux expansions of the branches of V lying above 0, i.e. the complete set of solutions of (1). Indeed, let

$$\left\{(\tilde{\mathcal{E}}^{(\ell)}, \tilde{X}^{(\ell)}) := \left(\lambda_\ell T^{e_\ell}, \sum_{m \geq m_\ell} a_{1,m}^{(\ell)} T^m, \dots, \sum_{m \geq m_\ell} a_{n,m}^{(\ell)} T^m\right) : 1 \leq \ell \leq g\right\} \quad (3)$$

be a system of rational Puiseux expansions of V , and let $\xi_\ell, \lambda_\ell^{-1/e_\ell} \in \overline{\mathbb{Q}}$ denote

a primitive e_ℓ -th root of 1 and an e_ℓ -th root λ_ℓ^{-1} for $1 \leq \ell \leq g$. Then the classical Puiseux expansions of the branches of V lying above 0 are given by

$$\left\{ \widetilde{X}^{(\ell)}(\xi_\ell^j \lambda_\ell^{-1/e_\ell} \mathcal{E}^{1/e_\ell}) : 1 \leq \ell \leq g, 1 \leq j \leq e_\ell \right\}.$$

Observe that the ramification index of the expansion $\widetilde{X}^{(\ell)}(\xi_\ell^j \lambda_\ell^{-1/e_\ell} \mathcal{E}^{1/e_\ell})$ is e_ℓ . Let R denote the least integer such that the partial expansion vectors $\sum_{m=m_\ell}^R a_m^{(\ell)} T^m := \sum_{m=m_\ell}^R (a_{1,m}^{(\ell)}, \dots, a_{n,m}^{(\ell)}) T^m$ are pairwise distinct for $1 \leq \ell \leq D$. Let us remark that a combination of [58, Proposition 1] and [23, Lemma 2] yields the estimate $R - m_\ell \leq 2(e_\ell f_\ell)^2$. The integer R is called the *regularity index* of the system (3). For $1 \leq \ell \leq g$, the partial expansion $\sum_{m=m_\ell}^R a_m^{(\ell)} T^m$ is called the *singular part* of $\widetilde{X}^{(\ell)}$.

2.3 Computational model

Our model of computation is based on the concept of *arithmetic-boolean circuits* (also called *arithmetic networks*) and *computation trees* (see e.g. [63] or [15]). An arithmetic-boolean circuit over $\mathbb{Q}[\mathcal{E}, X]$ is a directed acyclic graph (*dag* for short) whose nodes are labeled either by an element of $\mathbb{Q} \cup \{\mathcal{E}, X_1, \dots, X_n\}$, or by an arithmetic operation or a selection (pointing to other nodes) subject to a previous equal-to-zero decision. On the *dag* associated to a given arithmetic-boolean circuit β we may play a pebble game (see [14], [57]). A pebble game is a strategy of evaluation of β which converts β into a sequential algorithm (called computation tree) and associates to β natural time and space measures. Space is defined as the maximum number arithmetic registers used at any moment of the game, and time is defined as the total number of arithmetic operations and selections performed during the game. A computation tree without selections is called a *straight-line program* (see e.g. [61], [37], [15]). In the sequel, we shall tacitly assume that our arithmetic-boolean circuits and computation trees in $\mathbb{Q}[\mathcal{E}, X]$ contain only *non-essential* divisions, i.e. only divisions by nonzero elements of \mathbb{Q} .

3 Lifting procedures for ramified fibers

With notations and assumptions as in Section 2.1, let $\{(\widetilde{\mathcal{E}}^{(\ell)}, \widetilde{X}^{(\ell)}) : 1 \leq \ell \leq g\}$ be a set of parameterizations which induces a system of rational Puiseux expansions of the branches of V lying above 0 by the action of the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$. For $1 \leq \ell \leq g$, let $e_\ell, f_\ell \in \mathbb{N}$ denote the ramification index and the

residual degree of the Puiseux expansions associated to the parameterization

$$(\tilde{\mathcal{E}}^{(\ell)}, \tilde{X}^{(\ell)}) := \left(\lambda_\ell T^{e_\ell}, \sum_{m \geq m_\ell} a_m^{(\ell)} T^m \right), \quad (4)$$

with $a_m^{(\ell)} \in \overline{\mathbb{Q}}^n$ for $1 \leq \ell \leq g$, $m \geq m_\ell$. We have $\sum_{\ell=1}^g e_\ell f_\ell = D$ [23]. Let $R \in \mathbb{Z}$ be the regularity index of the system of rational Puiseux expansions (4). Let us recall the estimate $R - m_\ell \leq 2(e_\ell f_\ell)^2$ on the size of the singular parts of the parameterizations in (4) (see Section 2.2).

Let T, Y_1, \dots, Y_n be indeterminates over $\overline{\mathbb{Q}}$ and write $Y := (Y_1, \dots, Y_n)$. Let $K^{(\ell)} := \mathbb{Q}(\{\lambda_\ell, a_{m,1}^{(\ell)}, \dots, a_{m,n}^{(\ell)} : m \geq m_\ell\})$ be the coefficient field of the parameterization $(\tilde{\mathcal{E}}^{(\ell)}, \tilde{X}^{(\ell)})$. Denote by $\sigma_1^{(\ell)}, \dots, \sigma_{f_\ell}^{(\ell)}$ the morphisms of the Galois group of the field extension $\mathbb{Q} \hookrightarrow K^{(\ell)}$. For any $(\ell, j, k) \in \mathbb{N}^3$ with $1 \leq \ell \leq g$, $1 \leq j \leq n$ and $1 \leq k \leq f_\ell$, let us define $G_j^{(\ell,k)} \in \overline{\mathbb{Q}}[T, Y]$ by:

$$G_j^{(\ell,k)} := T^{\alpha_{j,\ell}} F_j \left(\sigma_k^{(\ell)}(\lambda_\ell) T^{e_\ell}, \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)}) T^m + Y T^R \right), \quad (5)$$

where $\alpha_{j,\ell} \in \mathbb{Z}$ is chosen such that the order of T in $G_j^{(\ell,k)}$ equals zero.

Our algorithmic methods are based on a deformation technique which allows us to compute an arbitrary fiber of the morphism $\pi : V \rightarrow \mathbb{A}^1$ by “lifting” the fiber $\pi^{-1}(0)$. In order to perform this process of lifting, we would like to use a global Newton–Hensel procedure as in [30], [28] (see also [39], [58]). Unfortunately, this is no longer possible because the essential hypothesis on the unramifiedness of the fiber $\pi^{-1}(0)$ is missed.

In order to circumvent this difficulty, one might try to proceed as in the plane curve case and consider the ideal $\mathcal{I}^{(\ell,k)}$ of $\overline{\mathbb{Q}}[T, Y]$ generated by the polynomials $G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)}$ for $1 \leq \ell \leq g$ and $1 \leq k \leq f_\ell$. Let $V^{(\ell,k)}$ be the affine subvariety of \mathbb{A}^{n+1} defined by $\mathcal{I}^{(\ell,k)}$, and let $\pi^{(\ell,k)} : V^{(\ell,k)} \rightarrow \mathbb{A}^1$ be the morphism defined by $\pi^{(\ell,k)}(t, x) := t$. Unlike the plane curve case, $G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)}$ are not necessarily smooth at $T = 0$, unless a suitable flatness condition is satisfied (compare [6], [3] and [4]). In Section 3.2 we exhibit a flatness condition which assures that the points of the fiber $(\pi^{(\ell,k)})^{-1}(0)$ are $(G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)})$ -smooth. Then in Section 3.3 we describe a variant of the global Newton–Hensel procedure of [30] and [28] specifically adapted to our situation. Finally, in Section 3.4 we show that this flatness condition is also necessary to assure smoothness.

Let us observe that the main results of this section, namely Theorems 5 and 7 below, depend on the infinitesimal structure of the fiber $\pi^{-1}(0)$, and hence can be (slightly) generalized to the case where F_1, \dots, F_n form a regular sequence

of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and generate a radical ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$. Nevertheless, for the sake of clarity we are not going to prove this generalization.

3.1 Properties of the ideal $\mathcal{I}^{(\ell,k)}$

Let us fix integers ℓ, k with $1 \leq \ell \leq g$ and $1 \leq k \leq f_\ell$. In order to exhibit our flatness condition we first need to establish some properties of the ideal $\mathcal{I}^{(\ell,k)}$.

Let $\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]$ denote the (extended) ideal generated by $\mathcal{I}^{(\ell,k)}$ in $\overline{\mathbb{Q}}(T)^*[Y]$. In order to describe the zero set of $\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]$ in $\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$, for any pair (ℓ, k) let $\mathcal{L}_{\ell,k}$ be the set of pairs (ℓ', k') for which there exists a vector of Puiseux series associated to the (ℓ', k') -th parameterization which agrees up to order R with another one associated to the (ℓ, k) -th parameterization, i.e.

$$\mathcal{L}_{\ell,k} := \left\{ (\ell', k'); e_\ell = e_{\ell'}, m_\ell = m_{\ell'}, \left(\exists \lambda_\ell^{-1/e_\ell} \right) \left(\exists \lambda_{\ell'}^{-1/e_{\ell'}} \right) \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)}) \sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m T^m = \sum_{m=m_{\ell'}}^{R-1} \sigma_{k'}^{(\ell')} (a_m^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m T^m \right\}. \quad (6)$$

The sets $\mathcal{L}_{\ell,k}$ form a partition of the set of pairs $\cup_{1 \leq \ell \leq g} \{\ell\} \times \{1, \dots, f_\ell\}$.

Lemma 1 *The extended ideal $\mathcal{I}^{(\ell,k)}\overline{\mathbb{Q}}(T)^*[Y]$ defines a zero-dimensional subvariety $\tilde{V}^{(\ell,k)}$ of $\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$. Furthermore, we have*

$$\tilde{V}^{(\ell,k)} \cap \overline{\mathbb{Q}}[T]^n = \left\{ \sum_{m \geq R} \sigma_{k'}^{(\ell')} (a_m^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m \sigma_k^{(\ell)} (\lambda_\ell^{\frac{1}{e_\ell}})^m T^{m-R}; (\ell', k') \in \mathcal{L}_{\ell,k} \right\}. \quad (7)$$

PROOF.— From the definition of $G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)}$ and the parameterization $(\tilde{\mathcal{E}}^{(\ell)}, \tilde{X}^{(\ell)})$, it follows that the vector of power series $\sum_{m \geq R} \sigma_k^{(\ell)}(a_m^{(\ell)}) T^{m-R}$ is a point of $\tilde{V}^{(\ell,k)} \subset \mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$. On the other hand, we observe that any point of $\tilde{V}^{(\ell,k)}$ induces univocally a finite set of points $\bar{x} \in \mathbb{A}^n(\overline{\mathbb{Q}}(\mathcal{E})^*)$ such that $F_j(\mathcal{E}, \bar{x}) = 0$ holds in $\overline{\mathbb{Q}}(\mathcal{E})^*$ for $1 \leq j \leq n$. Since $\{x \in \mathbb{A}^n(\overline{\mathbb{Q}}(\mathcal{E})^*) : F_1(\bar{x}) = 0, \dots, F_n(\bar{x}) = 0\}$ has dimension zero (see Subsection 2.2), it follows that $\tilde{V}^{(\ell,k)}$ must also have dimension zero.

Now we show identity (7). Let $\widehat{V}^{(\ell,k)}$ be the right-hand side of identity (7):

$$\widehat{V}^{(\ell,k)} := \left\{ \sum_{m \geq R} \sigma_{k'}^{(\ell')} (a_m^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m \sigma_k^{(\ell)} (\lambda_\ell^{\frac{1}{e_\ell}})^m T^{m-R}; (\ell', k') \in \mathcal{L}_{\ell,k} \right\}.$$

It is easy to see that $\widehat{V}^{(\ell,k)} \subset \tilde{V}^{(k,\ell)}$ holds. On the other hand, we observe that

any point $\sum_{m \geq 0} b_m T^m \in \tilde{V}^{(\ell, k)} \cap \overline{\mathbb{Q}}[[T]]^n$ induces a unique parameterization

$$\varphi := \left(\sigma_k^{(\ell)}(\lambda_\ell) T^{e_\ell}, \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)}) T^m + \sum_{m \geq R} b_{m-R} T^m \right)$$

of a branch of V lying above 0, and hence a vector of Puiseux series

$$\bar{x} := \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)}) \sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m \mathcal{E}^{\frac{m}{e_\ell}} + \sum_{m \geq R} b_{m-R} \sigma_k^{(\ell)}(\lambda_\ell^{-\frac{1}{e_\ell}})^m \mathcal{E}^{\frac{m}{e_\ell}}$$

satisfying $F_j(\mathcal{E}, \bar{x}) = 0$ for $j = 1, \dots, n$. Then there exists (ℓ_0, k_0) such that $\bar{x} = \sum_{m \geq m_{\ell_0}} \sigma_{k_0}^{(\ell_0)}(a_m^{(\ell_0)}) \sigma_{k_0}^{(\ell_0)}(\lambda_{\ell_0}^{-1})^{m/e_{\ell_0}} \mathcal{E}^{m/e_{\ell_0}}$. This shows that (ℓ_0, k_0) belongs to $\mathcal{L}_{\ell, k}$ and $\varphi = \left(\sigma_k^{(\ell)}(\lambda_\ell) T^{e_\ell}, \sum_{m \geq m_\ell} \sigma_{k_0}^{(\ell_0)}(a_m^{(\ell_0)}) \sigma_{k_0}^{(\ell_0)}(\lambda_{\ell_0}^{-1/e_{\ell_0}})^m \sigma_k^{(\ell)}(\lambda_\ell^{1/e_\ell})^m T^m \right)$ holds. Then $\sum_{m \geq R} b_m T^{m-R} = \sum_{m \geq R} \sigma_{k_0}^{(\ell_0)}(a_m^{(\ell_0)}) \sigma_{k_0}^{(\ell_0)}(\lambda_{\ell_0}^{-1/e_{\ell_0}})^m \sigma_k^{(\ell)}(\lambda_\ell^{1/e_\ell})^m T^{m-R}$, which shows identity (7). \blacksquare

Let us observe that $G_1^{(\ell, k)}, \dots, G_n^{(\ell, k)}$ are obtained from F_1, \dots, F_n by applying the mapping $\Psi_R^{(\ell, k)} : \overline{\mathbb{Q}}[\mathcal{E}, X] \rightarrow \overline{\mathbb{Q}}[T, Y]$ defined by

$$\Psi_R^{(\ell, k)}(F(\mathcal{E}, X)) := T^{\alpha_F} F\left(\sigma_k^{(\ell)}(\lambda_\ell) T^{e_\ell}, \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)}) T^m + Y T^R\right),$$

where $\alpha_F \in \mathbb{Z}$ is chosen such that the order of T in $\Psi_R^{(\ell, k)}(F)$ is zero. In order to “invert” the mapping $\Psi_R^{(\ell, k)}$, up to a power of \mathcal{E} , we introduce the following morphism $\Phi_R^{(\ell, k)} : \overline{\mathbb{Q}}(T)[Y] \rightarrow \overline{\mathbb{Q}}(\mathcal{E})[X]$ of $\overline{\mathbb{Q}}$ -algebras:

$$\Phi_R^{(\ell, k)}(F(T, Y)) := F\left(\mathcal{E}, \mathcal{E}^{-R} \left(X - \sum_{m=m_\ell}^{R-1} \sigma_k^{(\ell)}(a_m^{(\ell)}) \mathcal{E}^m\right)\right).$$

We have $\mathcal{E}^{\alpha_F} \Phi_R^{(\ell, k)}(\Psi_R^{(\ell, k)}(F)) = F(\sigma_k^{(\ell)}(\lambda_\ell) \mathcal{E}^{e_\ell}, X)$ for any $F \in \overline{\mathbb{Q}}[\mathcal{E}, X]$.

Lemma 2 $G_1^{(\ell, k)}, \dots, G_n^{(\ell, k)}$ form a regular sequence of $\overline{\mathbb{Q}}[T, Y]$.

PROOF.— Arguing by contradiction, assume that $G_1^{(\ell, k)}, \dots, G_n^{(\ell, k)}$ do not form a regular sequence. Then there exists $j \geq 2$ such that $G_j^{(\ell, k)}$ is a zero divisor of $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell, k)}$, i.e. there exist $\tilde{H}, \tilde{P}_1, \dots, \tilde{P}_{j-1} \in \overline{\mathbb{Q}}[T, Y]$ such that

$$\tilde{H} \Psi_R^{(\ell, k)}(F_j) = \tilde{H} G_j^{(\ell, k)} = \sum_{i=1}^{j-1} \tilde{P}_i G_i^{(\ell, k)} = \sum_{i=1}^{j-1} \tilde{P}_i \Psi_R^{(\ell, k)}(F_i) \quad (8)$$

holds in $\overline{\mathbb{Q}}[T, Y]$. Applying the morphism $\Phi_R^{(\ell, k)}$ to the left and right-hand side members of identity (8) and multiplying by a suitable power of \mathcal{E} , we deduce

that there exist $H, P_1, \dots, P_{j-1} \in \overline{\mathbb{Q}}[\mathcal{E}, X]$ such that

$$HF_j(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X) = \sum_{i=1}^{j-1} P_i F_i(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X) \quad (9)$$

holds in $\overline{\mathbb{Q}}[\mathcal{E}, X]$. Identity (9) may be rewritten in the following way:

$$\sum_{h=0}^{e_\ell-1} \mathcal{E}^h H_h F_j(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X) = \sum_{h=0}^{e_\ell-1} \mathcal{E}^h \sum_{i=1}^{j-1} P_{i,h} F_i(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X), \quad (10)$$

with $H_h, P_{1,h}, \dots, P_{j-1,h} \in \overline{\mathbb{Q}}[\mathcal{E}^{e_\ell}, X]$ for $0 \leq h \leq e_\ell - 1$. Then identity (10) holds if and only if the following identity

$$H_h F_j(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X) = \sum_{i=1}^{j-1} P_{i,h} F_i(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X)$$

holds in $\overline{\mathbb{Q}}[\mathcal{E}, X]$ for $0 \leq h \leq e_\ell - 1$. This implies that F_j is a zero divisor of the $\overline{\mathbb{Q}}$ -algebra $\overline{\mathbb{Q}}[\mathcal{E}, X]/(F_1, \dots, F_{j-1})$, which contradicts our hypotheses. \blacksquare

Let us remark that Lemma 2 shows in particular that the ring $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell,k)}$ is Cohen–Macaulay.

From now on we fix the notations: $J_F := \det\left(\frac{\partial F_i}{\partial X_j}\right)_{1 \leq i, j \leq n}$, $J_G := \det\left(\frac{\partial G_i^{(\ell,k)}}{\partial Y_j}\right)_{1 \leq i, j \leq n}$.

Lemma 3 *The ideal $\mathcal{I}^{(\ell,k)}$ is a radical ideal of $\overline{\mathbb{Q}}[T, Y]$.*

PROOF.— Since by hypothesis the morphism π is generically unramified, the Jacobian determinant J_F is not a zero divisor of $\overline{\mathbb{Q}}[\mathcal{E}, X]/(F_1, \dots, F_n)$. We claim that the Jacobian determinant J_G is not a zero divisor of $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell,k)}$.

Suppose that there exist polynomials $\widetilde{H}, \widetilde{P}_1, \dots, \widetilde{P}_n \in \overline{\mathbb{Q}}[T, Y]$ such that

$$\widetilde{H} J_G = \sum_{i=1}^n \widetilde{P}_i G_i^{(\ell,k)} \quad (11)$$

holds in $\overline{\mathbb{Q}}[T, Y]$. Observe that $J_F(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X) = \mathcal{E}^\alpha \Phi_R^{(\ell,k)}(J_G)$ holds for a suitable $\alpha \in \mathbb{Z}$. Arguing as in the proof of Lemma 2 we conclude that there exist polynomials $H_h, P_{i,h} \in \overline{\mathbb{Q}}[\mathcal{E}^{e_\ell}, X]$ for $0 \leq h \leq e_\ell - 1$ and $1 \leq i \leq n$ such that identity (11) holds if and only if the identity

$$H_h J_F(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X) = \sum_{i=1}^n P_i F_i(\sigma_k^{(\ell)}(\lambda_\ell)\mathcal{E}^{e_\ell}, X)$$

holds in $\overline{\mathbb{Q}}[\mathcal{E}^{e_\ell}, X]$ for $0 \leq h \leq e_\ell - 1$. We conclude that J_F is a zero divisor of $\overline{\mathbb{Q}}[\mathcal{E}, X]/(F_1, \dots, F_n)$, contradicting thus the hypothesis on the generic unramifiedness of π . We conclude that J_G is not a zero divisor of $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell, k)}$. This implies that the ideal generated by the $n \times n$ minors of the Jacobian matrix of $G_1^{(\ell, k)}, \dots, G_n^{(\ell, k)}$ with respect to T, Y_1, \dots, Y_n has codimension at least 1 in $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell, k)}$. Since $\overline{\mathbb{Q}}[T, Y]/\mathcal{I}^{(\ell, k)}$ is a Cohen–Macaulay ring, from [24, Theorem 18.15] we conclude that $\mathcal{I}^{(\ell, k)}$ is radical. ■

3.2 The unramifiedness of the morphism $\pi^{(\ell, k)}$ at $T = 0$

In what follows, we shall use the following terminology: For a given polynomial $G \in \overline{\mathbb{Q}}[T, Y] := \overline{\mathbb{Q}}[T, Y_1, \dots, Y_n]$, let us write $G(T, Y) = T^\alpha g(Y) + \widehat{G}$, where g is a nonzero polynomial of $\overline{\mathbb{Q}}[Y]$ and $\widehat{G} \in \overline{\mathbb{Q}}[T, Y]$ has at least $\alpha + 1$ order in T . The polynomial $g(Y)$ is called the *initial form* of G and is denoted $in(G)$.

Let us fix $\ell, k \in \mathbb{N}$ with $1 \leq \ell \leq g$ and $1 \leq k \leq e_\ell$. We are going to show that the morphism $\pi^{(\ell, k)} : V^{(\ell, k)} \rightarrow \mathbb{A}^1$ defined by $\pi^{(\ell, k)}(t, y) := t$ is unramified at every point of the fiber $(\pi^{(\ell, k)})^{-1}(0)$. For this purpose, we are going to prove that for any point $b \in (\pi^{(\ell, k)})^{-1}(0)$ there exists a unique holomorphic branch of the curve $V^{(\ell, k)}$ passing through b , and $b \in (\pi^{(\ell, k)})^{-1}(0)$ has multiplicity 1 in this branch. This is equivalent to showing that the zero-dimensional affine variety defined by the (initial) ideal $in(\mathcal{I}^{(\ell, k)}) \subset \overline{\mathbb{Q}}[Y]$ generated by the set $\{in(F) : F \in \mathcal{I}^{(\ell, k)}\}$ has as many points as the number of holomorphic branches of $V^{(\ell, k)}$ passing through points of $(\pi^{(\ell, k)})^{-1}(0)$, namely $\#(\widetilde{V}^{(\ell, k)} \cap \overline{\mathbb{Q}}[T]^n)$ with the notations of Lemma 1. This is the content of our next result.

Proposition 4 *Let $W^{(\ell, k)}$ denote the affine subvariety of \mathbb{A}^n defined by the ideal $in(\mathcal{I}^{(\ell, k)})$. Then the following identity holds in \mathbb{A}^n :*

$$W^{(\ell, k)} = \{\sigma_{k'}^{(\ell')} (a_R^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)} (\lambda_\ell^{\frac{1}{e_\ell}})^R : (\ell', k') \in \mathcal{L}_{\ell, k}\}.$$

PROOF.— Let $\widehat{W}^{(\ell, k)} := \{\sigma_{k'}^{(\ell')} (a_R^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)} (\lambda_\ell^{\frac{1}{e_\ell}})^R : (\ell', k') \in \mathcal{L}_{\ell, k}\}$. We want to show that $W^{(\ell, k)} = \widehat{W}^{(\ell, k)}$ holds.

We first prove the inclusion $W^{(\ell, k)} \supset \widehat{W}^{(\ell, k)}$. Let $b \in \widehat{W}^{(\ell, k)}$ and let $F \in \mathcal{I}^{(\ell, k)}$. Then there exists $(\ell', k') \in \mathcal{L}_{\ell, k}$ such that $b = \sigma_{k'}^{(\ell')} (a_R^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-1/e_{\ell'}})^R \sigma_k^{(\ell)} (\lambda_\ell^{1/e_\ell})^R$ holds. Let us write $F = T^\alpha in(F) + \widehat{F}$, with $in(F) \in \overline{\mathbb{Q}}[Y] \setminus \{0\}$ and $\widehat{F} \in \overline{\mathbb{Q}}[T, Y]$

of order at least $\alpha + 1$ in T . From Lemma 1 we have

$$\begin{aligned} 0 &= F\left(T, \sum_{m \geq R} \sigma_{k'}^{(\ell')} (a_m^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m \sigma_k^{(\ell)} (\lambda_{\ell}^{\frac{1}{e_{\ell}}})^m T^{m-R}\right) \\ &= T^{\alpha} \text{in}(F) \left(\sigma_{k'}^{(\ell')} (a_R^{(\ell')}) \sigma_{k'}^{(\ell')} (\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)} (\lambda_{\ell}^{\frac{1}{e_{\ell}}})^R \right) + T^{\alpha+1} \widehat{f}(T) \\ &= T^{\alpha} \text{in}(F)(b) + T^{\alpha+1} \widehat{f}(T), \end{aligned}$$

with $\widehat{f} \in \overline{\mathbb{Q}}[[T]]$. Then $\text{in}(F)(b) = 0$, which shows the inclusion $W^{(\ell,k)} \supset \widehat{W}^{(\ell,k)}$.

In order to prove the converse inclusion, let $U \in \mathbb{Q}[X]$ be a generic linear form, i.e. a linear form whose projection polynomial $m_u \in \mathbb{Q}(\mathcal{E})[Z]$ has degree D (see Section 2.1). For $1 \leq i \leq D$, let $U^{(i)}$ be the element of $\mathbb{Q}(\mathcal{E})^*$ defined by $U^{(i)} := U(x^{(i)})$, where $\{x^{(1)}, \dots, x^{(D)}\}$ denote the classical Puiseux expansions of the branches of V lying above 0. Let u be the rational function induced by U in $\mathbb{Q}(V)$. Observe that $\prod_{i=1}^D (Z - U^{(i)})$ annihilates u in the zero-dimensional $\overline{\mathbb{Q}}(\mathcal{E})^*$ -algebra $\overline{\mathbb{Q}}(\mathcal{E})^* \otimes \mathbb{Q}(V)$. Taking into account that $\prod_{i=1}^D (Z - U^{(i)})$ belongs to $\mathbb{Q}(\mathcal{E})[Z]$ (see [23]) and has degree D in Z , we conclude that $m_u = \prod_{i=1}^D (Z - U^{(i)})$ holds. This shows that $U^{(j)} \neq U^{(k)}$ for $1 \leq j < k \leq D$ and we have the following expression for $m_u(Z)$ in $\overline{\mathbb{Q}}(\mathcal{E})^*[Z]$ (compare [23]):

$$m_u(\mathcal{E}, Z) = \prod_{\ell=1}^g \prod_{k=1}^{f_{\ell}} \prod_{j=1}^{e_{\ell}} \left(Z - \sum_{m \geq m_{\ell}} U \left(\sigma_k^{(\ell)} (a_m^{(\ell)}) \right) \sigma_k^{(\ell)} (\lambda_{\ell}^{-\frac{1}{e_{\ell}}})^m \xi_{\ell}^{jm} \mathcal{E}^{\frac{m}{e_{\ell}}} \right),$$

where $\sigma_1^{(\ell)}, \dots, \sigma_{f_{\ell}}^{(\ell)}$ range over all the morphisms of the Galois group of the field extension $\mathbb{Q} \hookrightarrow K^{(\ell)}$ and $\lambda_{\ell}^{-1/e_{\ell}}, \xi_{\ell}$ denote an e_{ℓ} -th root of λ_{ℓ}^{-1} and a primitive e_{ℓ} -th root of 1. From [23, Theorem 2], we deduce that, for $1 \leq \ell \leq g$,

$$m_u^{(\ell)} := \prod_{k=1}^{f_{\ell}} m_u^{(\ell,k)} := \prod_{k=1}^{f_{\ell}} \left(\prod_{j=1}^{e_{\ell}} \left(Z - \sum_{m \geq m_{\ell}} U \left(\sigma_k^{(\ell)} (a_m^{(\ell)}) \right) \sigma_k^{(\ell)} (\lambda_{\ell}^{-\frac{1}{e_{\ell}}})^m \xi_{\ell}^{jm} \mathcal{E}^{\frac{m}{e_{\ell}}} \right) \right) \quad (12)$$

is an irreducible polynomial of $\mathbb{Q}((\mathcal{E}))[[Z]]$, and, for $1 \leq k \leq f_{\ell}$, $m_u^{(\ell,k)}$ is an irreducible element of $\overline{\mathbb{Q}}((\mathcal{E}))[[Z]]$ satisfying

$$m_u^{(\ell,k)} \left(\sigma_k^{(\ell)} (\lambda_{\ell}) T^{e_{\ell}}, Z \right) = \prod_{j=1}^{e_{\ell}} \left(Z - \sum_{m \geq m_{\ell}} U \left(\sigma_k^{(\ell)} (a_m^{(\ell)}) \right) (\xi_{\ell}^j T)^m \right). \quad (13)$$

For $1 \leq \ell \leq g$ and $1 \leq k \leq f_{\ell}$, let us consider the morphism of $\overline{\mathbb{Q}}$ -algebras

$$\begin{aligned} \widetilde{\Psi}_R^{(\ell,k)} : \overline{\mathbb{Q}}((\mathcal{E}))[[X]] &\longrightarrow \overline{\mathbb{Q}}((T))[[Y]] \\ F(\mathcal{E}, X) &\longmapsto F \left(\sigma_k^{(\ell)} (\lambda_{\ell}) T^{e_{\ell}}, \sum_{m=m_{\ell}}^{R-1} \sigma_k^{(\ell)} (a_m^{(\ell)}) T^m + Y T^R \right). \end{aligned}$$

Let us fix ℓ', k' with $1 \leq \ell' \leq g$ and $1 \leq k' \leq e_{\ell}$. Applying the morphism

$\tilde{\Psi}_R^{(\ell,k)}$ to the polynomial $m_u^{(\ell',k')}(\mathcal{E}, U(X))$, from identity (12) we obtain:

$$\begin{aligned} \tilde{\Psi}_R^{(\ell,k)}\left(m_u^{(\ell',k')}(\mathcal{E}, U(X))\right) &= \prod_{j=1}^{e_{\ell'}} \left(\sum_{m=m_{\ell}}^{R-1} U\left(\sigma_k^{(\ell)}(a_m^{(\ell)})\right) T^m + U(Y) T^R - \right. \\ &\quad \left. - \sum_{m \geq m_{\ell}} U\left(\sigma_{k'}^{(\ell')}(a_m^{(\ell')})\right) \sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^m \sigma_k^{(\ell)}(\lambda_{\ell}^{\frac{1}{e_{\ell}}})^m \xi_{\ell}^{jm} T^{\frac{me_{\ell}}{e_{\ell'}}} \right). \end{aligned}$$

This identity shows that all the factors of $\tilde{\Psi}_R^{(\ell,k)}\left(m_u^{(\ell',k')}(\mathcal{E}, U(X))\right)$ have order at most R and the coefficient of the least nonzero power of T arising in the Laurent series $\tilde{\Psi}_R^{(\ell,k)}\left(m_u^{(\ell',k')}(\mathcal{E}, U(X))\right) \in \overline{\mathbb{Q}}[Y]((T))$ is

- either of the form $\alpha U(Y - \sigma_{k'}^{(\ell')}(a_R^{(\ell')}) \sigma_{k'}^{(\ell')}(\lambda_{\ell'}^{-\frac{1}{e_{\ell'}}})^R \sigma_k^{(\ell)}(\lambda_{\ell}^{-\frac{1}{e_{\ell}}})^R)$ with $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, in case that $(\ell', k') \in \mathcal{L}_{\ell,k}$ holds,
- or a nonzero constant $\alpha \in \overline{\mathbb{Q}}$ otherwise.

We deduce that the coefficients of the least nonzero power of T arising in the following elements of $\overline{\mathbb{Q}}[Y]((T))$:

$$\tilde{\Psi}_R^{(\ell,k)}\left(\prod_{(\ell',k') \in \mathcal{L}_{\ell,k}} m_u^{(\ell',k')}(\mathcal{E}, U(X))\right), \quad \tilde{\Psi}_R^{(\ell,k)}\left(\prod_{(\ell',k') \notin \mathcal{L}_{\ell,k}} m_u^{(\ell',k')}(\mathcal{E}, U(X))\right),$$

are of the form $\alpha \prod_{b \in \widehat{W}^{(\ell,k)}} U_1(Y - b) \in \overline{\mathbb{Q}}[Y]$ with $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, and a constant $\tilde{\alpha} \in \overline{\mathbb{Q}} \setminus \{0\}$ respectively. We conclude that the following identity holds:

$$\text{in}\left(\Psi_R^{(\ell,k)}\left(m_u(\mathcal{E}, U(X))\right)\right) = \alpha \prod_{b \in \widehat{W}^{(\ell,k)}} U(Y - b). \quad (14)$$

Since $m_u(\mathcal{E}, U(X)) \in \mathcal{I}(V)$, we conclude that there exists $\alpha \in \mathbb{Z}$ such that $T^\alpha \Psi_R^{(\ell,k)}\left(m_u(\mathcal{E}, U(X))\right) \in \mathcal{I}^{(\ell,k)}$. Then $\text{in}\left(\Psi_R^{(\ell,k)}\left(m_u(\mathcal{E}, U(X))\right)\right) \in \text{in}(\mathcal{I}^{(\ell,k)})$.

Now, let U_1, \dots, U_n be \mathbb{Q} -linearly independent generic linear forms. Repeating the previous arguments with U_1, \dots, U_n , from identity (14) we conclude that $W^{(\ell,k)}$ is a zero-dimensional subvariety of \mathbb{A}^n . Furthermore, we have

$$\deg \widehat{W}^{(\ell,k)} \leq \deg W^{(\ell,k)} \leq \deg \left(\prod_{b \in \widehat{W}^{(\ell,k)}} U_1(Y - b) \right) = \#(\widehat{W}^{(\ell,k)}).$$

This shows that $\#(\widehat{W}^{(\ell,k)}) = \#(W^{(\ell,k)})$. Therefore, taking into account the inclusion $\widehat{W}^{(\ell,k)} \subset W^{(\ell,k)}$, we see that $W^{(\ell,k)} = \widehat{W}^{(\ell,k)}$ holds. \blacksquare

Now we exhibit a flatness condition which assures that any point of the fiber $(\pi^{(\ell,k)})^{-1}(0)$ is $(G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)})$ -smooth. For this purpose, we introduce the notion of standard basis (see [20]). A set $\{G_1, \dots, G_s\} \subset \overline{\mathbb{Q}}[T, Y] := \overline{\mathbb{Q}}[T, Y_1, \dots, Y_n]$ is called a *standard basis* (of the ideal I they generate) if the ideal $(\text{in}(G_1), \dots, \text{in}(G_s))$ generated by the initial forms of G_1, \dots, G_s in $\overline{\mathbb{Q}}[Y]$

agrees with the ideal $\text{in}(I) := (\text{in}(G) : G \in I)$ generated by the initial forms of all the polynomials $G \in I$.

Theorem 5 *Let notations and assumptions be as above. Suppose further that $G_1^{(\ell,k)}(T, Y), \dots, G_n^{(\ell,k)}(T, Y)$ form a standard basis of the ideal $\mathcal{I}^{(\ell,k)}$. Then the Jacobian determinant J_G does not vanish at any point of $(\pi^{(\ell,k)})^{-1}(0)$.*

PROOF.— Since $G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)}$ form a standard basis of $\mathcal{I}^{(\ell,k)}$ we see that

$$\begin{aligned} (\pi^{(\ell,k)})^{-1}(0) &= \{0\} \times V(G_1^{(\ell,k)}(0, Y), \dots, G_n^{(\ell,k)}(0, Y)) = \\ &= \{0\} \times V(\text{in}(G_1^{(\ell,k)}), \dots, \text{in}(G_n^{(\ell,k)})) = \{0\} \times W^{(\ell,k)} \end{aligned}$$

holds. From Proposition 4 we see that for any $b \in W^{(\ell,k)}$ there exists a unique vector of power series $\varphi \in \overline{\mathbb{Q}}[[T]]$ such that $\varphi(0) = b$ and $G_i^{(\ell,k)}(T, \varphi) = 0$ hold for $1 \leq i \leq n$. Then [3, Lemma 3] shows that $Y = b$ has multiplicity 1 as a zero of the ideal generated by $G_1^{(\ell,k)}(0, Y), \dots, G_n^{(\ell,k)}(0, Y)$. Therefore, J_G does not vanish at any point $(0, y) \in (\pi^{(\ell,k)})^{-1}(0)$. ■

3.3 A global Newton–Hensel lifting

As expressed in the introduction, our purpose is to solve (in the sense of Subsection 2.1) certain specific polynomial equation systems by means of deformations. Applying a suitable variant of the so-called Shape Lemma (see [43], [56], [33]), polynomial equation solving can be efficiently reduced to the problem of computing generic linear projections. In our context, this problem can be stated as follows:

Lifting of a projection: given a set $\{(\tilde{\mathcal{E}}^{(1)}, \tilde{X}^{(1)}), \dots, (\tilde{\mathcal{E}}^{(g)}, \tilde{X}^{(g)})\}$ of parameterizations of V , whose orbits under the action of the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ form a system of rational Puiseux expansions of the branches of the curve V lying above 0, and a generic linear form $U \in \mathbb{Q}[X]$, compute the projection polynomial $m_u \in \mathbb{Q}(\mathcal{E})[Z]$.

Let us fix ℓ with $1 \leq \ell \leq g$ and let S_1, S_2 be indeterminates over \mathbb{Q} . Let $q^{(\ell)}$ be a monic irreducible polynomial of $\mathbb{Q}[S_1]$ of degree $f_\ell = [K^{(\ell)} : \mathbb{Q}]$ such that there exists a \mathbb{Q} -isomorphism of fields $\Upsilon_\ell : \mathbb{Q}[S_1]/(q^{(\ell)}(S_1)) \rightarrow K^{(\ell)}$. For any $m \geq m_\ell$ and $1 \leq j \leq n$, let $f^{(\ell)}, f_{m,j}^{(\ell)}$ be the (unique) polynomials of $\mathbb{Q}[S_1]$ of degree at most $f_\ell - 1$, such that $\Upsilon_\ell(f^{(\ell)}) := \lambda_\ell^{-1}$ and $\Upsilon_\ell(f_{m,j}^{(\ell)}) := a_{m,j}^{(\ell)}$. Finally, let $p^{(\ell)} \in \mathbb{Q}[S_1, S_2]$ be the polynomial $p^{(\ell)} := S_2^{e_\ell} - f^{(\ell)}(S_1)$, and let

$$W^{(\ell)} := \{(s_1, s_2) \in \mathbb{A}^2 : p^{(\ell)}(s_1, s_2) = 0, q^{(\ell)}(s_1) = 0\}. \quad (15)$$

It is easy to see that $W^{(\ell)}$ is a zero-dimensional variety of degree $\deg W^{(\ell)} = e_\ell f_\ell$. [23] shows that the field $K^{(\ell)}$ is the field extension of \mathbb{Q} generated by the coefficients $a_{j,m}^{(\ell)}$ for $1 \leq j \leq n$ and $m_\ell \leq m < R$. In particular, $K^{(\ell)}$ is the minimal field extension of \mathbb{Q} containing the coefficients of the singular parts of the given set of rational Puiseux expansions.

For $\kappa \geq R$, let $u^{(\kappa,\ell)} := \sum_{m=m_\ell}^{\kappa} U(f_m^{(\ell)}(S_1))(S_2 T)^m \in \mathbb{Q}(S_1, S_2, T)$ and let $\chi_{u^{(\kappa,\ell)}} \in \mathbb{Q}(T)[Z]$ denote the characteristic polynomial of the projection $\pi_{u^{(\kappa,\ell)}}^{(\ell)} : \mathbb{A} \times W^{(\ell)} \rightarrow \mathbb{A}^2$ defined by $\pi_{u^{(\kappa,\ell)}}^{(\ell)}(t, s_1, s_2) := (t, u^{(\kappa,\ell)}(t, s_1, s_2))$. We have

$$\chi_{u^{(\kappa,\ell)}} = \prod_{k=1}^{f_\ell} \prod_{j=1}^{e_\ell} \left(Z - \sum_{m=m_\ell}^{\kappa} U(\sigma_k^{(\ell)}(a_m^{(\ell)})) \left(\xi_\ell^j \sigma_k^{(\ell)} (\lambda_\ell^{-\frac{1}{e_\ell}} T) \right)^m \right). \quad (16)$$

Observe that if the norm in the field extension $K^{(\ell)}(\sigma_k^{(\ell)}(\lambda_\ell^{-1/e_\ell} T))/\mathbb{Q}(T^{e_\ell})$ is extended to polynomials, then $\chi_{u^{(\kappa,\ell)}}$ is the norm of $Z - \sum_{m=m_\ell}^{\kappa} U(a_m^{(\ell)}) \lambda_\ell^{-1/e_\ell} T^m$. This shows that $\chi_{u^{(\kappa,\ell)}}$ is an element of $\mathbb{Q}(T^{e_\ell})[Z]$.

Before continuing, we introduce the following terminology: for $G, \tilde{G} \in \overline{\mathbb{Q}}((\mathcal{E}))$ and any $s \in \mathbb{Z}$, we say that \tilde{G} approximates G with precision s in $\overline{\mathbb{Q}}((\mathcal{E}))$ if the Laurent series $G - \tilde{G}$ has order at least $s + 1$ in \mathcal{E} . We shall use the notation $G \equiv \tilde{G} \pmod{(\mathcal{E}^{s+1})}$. Furthermore, if G, \tilde{G} are two elements of a polynomial ring $\overline{\mathbb{Q}}((\mathcal{E}))[Z]$, we say that \tilde{G} approximates G with precision s if every coefficient $\tilde{a} \in \overline{\mathbb{Q}}((\mathcal{E}))$ of \tilde{G} approximates the corresponding coefficient $a \in \overline{\mathbb{Q}}((\mathcal{E}))$ of G with precision s (in the sense of the previous definition).

From identities (12) and (16) we easily deduce that the congruence relation

$$m_u^{(\ell)}(T^{e_\ell}, Z) \equiv \chi_{u^{(\kappa,\ell)}}(T, Z) \pmod{(T^{\kappa - \delta_0 m_\ell e_\ell f_\ell + 1})} \quad (17)$$

holds in $\mathbb{Q}((T))[Z]$, with $\delta_0 := -1$ for $m_\ell < 0$ and $\delta_0 := 0$ otherwise. Taking into account that $\chi_{u^{(\kappa,\ell)}}(T, Z)$ is an element of $\mathbb{Q}(T^{e_\ell})[Z]$, replacing T^{e_ℓ} by \mathcal{E} in (17) we obtain the following result:

Lemma 6 *For any $\kappa \geq R$, $\chi_{u^{(\kappa,\ell)}}(\mathcal{E}^{1/e_\ell}, Z) \in \mathbb{Q}(\mathcal{E})[Z]$ approximates the polynomial $m_u^{(\ell)}(\mathcal{E}, Z) \in \mathbb{Q}((\mathcal{E}))[Z]$ with precision $\lfloor \frac{\kappa - \delta_0 m_\ell e_\ell f_\ell}{e_\ell} \rfloor$ in $\mathbb{Q}((\mathcal{E}))[Z]$.*

Now we state our version of the global Newton–Hensel lifting.

Theorem 7 *Let hypotheses be as in Theorem 5. Let be given $\kappa \geq 0$. For $1 \leq j \leq n$, let $G_j^{(\ell)}$ be the following element of $\mathbb{Q}[S_1, S_2, S_2^{-1}, T, Y]$:*

$$G_j^{(\ell)}(S_1, S_2, T, Y) := T^{\alpha_{j\ell}} F_j \left(T^{e_\ell}, \sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(S_1)(S_2 T)^m + Y T^R \right).$$

Let $N_{G^{(\ell)}}$ be the Newton–Hensel operator associated to $G_1^{(\ell)}, \dots, G_n^{(\ell)}$, namely

$$N_{G^{(\ell)}}(Y) := Y - \left(\frac{\partial G_i^{(\ell)}}{\partial Y_j} \right)_{1 \leq i, j \leq n}^{-1} \cdot (G_1^{(\ell)}, \dots, G_n^{(\ell)})^t, \quad (18)$$

where t denotes transposition, and let $N_{G^{(\ell)}}^\kappa$ denote the κ -th fold iteration of $N_{G^{(\ell)}}$. Finally, let

$$\tilde{u}^{(\kappa, \ell)} := U \left(\sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(S_1)(S_2 T)^m + N_{G^{(\ell)}}^\kappa(S_1, S_2, T, f_R^{(\ell)}(S_1)S_2^R)T^R \right)$$

and let $\chi_{\tilde{u}^{(\ell, k)}} \in \overline{\mathbb{Q}}(T)[Z]$ be its characteristic polynomial. Then $\chi_{\tilde{u}^{(\ell, k)}}(\mathcal{E}^{1/e_\ell}, Z)$ approximates the polynomial $m_u^{(\ell)}$ with precision $\lfloor \frac{R-1-\delta_0 m_\ell e_\ell f_\ell + 2^\kappa}{e_\ell} \rfloor$ in $\mathbb{Q}((\mathcal{E}))[Z]$.

PROOF.— Let (s_1, s_2) be a point of the variety $W^{(\ell)}$. Then there exists a (unique) pair (k, j) with $1 \leq k \leq f_\ell$ and $1 \leq j \leq e_\ell$, such that $f^{(\ell)}(s_1) = \sigma_k^{(\ell)}(\lambda_\ell^{-1})$, $s_2 = \xi_\ell^j \sigma_k^{(\ell)}(\lambda_\ell^{-1/e_\ell})$ and $f_m^{(\ell)}(s_1) = \sigma_k^{(\ell)}(a_m^{(\ell)})$ hold for $m_\ell \leq m \leq R$. This implies that the following identity holds in $\overline{\mathbb{Q}}[T, Y]$ for $1 \leq i \leq n$:

$$G_i^{(\ell)}(s_1, s_2, T, Y) = s_2^{\alpha_{j\ell}} G_i^{(\ell, k)}(s_2 T, s_2^{-R} Y). \quad (19)$$

Let us observe that $s_2^R \sigma_k^{(\ell)}(a_R^{(\ell)}) \in \mathbb{A}^n$ belongs to the affine variety defined by $G_1^{(\ell)}(s_1, s_2, 0, Y), \dots, G_n^{(\ell)}(s_1, s_2, 0, Y)$. Furthermore, from Theorem 5 and identity (19) we conclude that $J_{G^{(\ell)}}(T, Y) := \det(\partial G_i^{(\ell)} / \partial Y_j)_{1 \leq i, j \leq n}(s_1, s_2, T, Y)$ does not vanish at $(0, s_2^R \sigma_k^{(\ell)}(a_R^{(\ell)})) \in \mathbb{A}^{n+1}$, and hence $J_{G^{(\ell)}}(T, s_2^R \sigma_k^{(\ell)}(a_R^{(\ell)}))$ is a unit in the local ring $(\overline{\mathbb{Q}}[[T]], (T))$.

From Hensel’s Lemma (see e.g. [24]) in the version of [39] we deduce that the following congruence relation holds in $\overline{\mathbb{Q}}[[T]]^n$:

$$N_{G^{(\ell)}}^\kappa(s_1, s_2, T, \sigma_k^{(\ell)}(a_R^{(\ell)})s_2^R) \equiv \sum_{m \geq R} \sigma_k^{(\ell)}(a_m^{(\ell)})s_2^m T^{m-R} \pmod{(T^{2^\kappa})}.$$

Therefore, we obtain

$$\begin{aligned} U \left(\sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(s_1)(s_2 T)^m + N_{G^{(\ell)}}(s_1, s_2, T, \sigma_k^{(\ell)}(a_R^{(\ell)})s_2^R)T^R \right) &\equiv \\ &\equiv U \left(\sum_{m \geq m_\ell} \sigma_k^{(\ell)}(a_m^{(\ell)})(s_2 T)^m \right) \pmod{(T^{R+2^\kappa})}, \end{aligned}$$

which implies $\tilde{u}^{(\kappa, \ell)}(s_1, s_2, T) \equiv u^{(R-1+2^\kappa, \ell)}(s_1, s_2, T) \pmod{(T^{R+2^\kappa})}$.

Lemma 6 shows that $\chi_{u^{(R-1+2^\kappa, \ell)}}(\mathcal{E}^{1/e_\ell}, Z)$ approximates $m_u^{(\ell)}$ in $\mathbb{Q}((\mathcal{E}))[Z]$ with precision $\lfloor \frac{R-1-\delta_0 m_\ell e_\ell f_\ell + 2^\kappa}{e_\ell} \rfloor$. Therefore, $\chi_{\tilde{u}^{(\kappa, \ell)}}(\mathcal{E}^{1/e_\ell}, Z)$ also approximates $m_u^{(\ell)}$ in $\mathbb{Q}((\mathcal{E}))[Z]$ with precision $\lfloor \frac{R-1-\delta_0 m_\ell e_\ell f_\ell + 2^\kappa}{e_\ell} \rfloor$. This proves the theorem. \blacksquare

3.4 Unramifiedness and flatness conditions

All the hypotheses of Theorems 5 and 7 are fairly “geometric” in nature, and hence reasonable assumptions from our point of view (compare [39]), except perhaps for the standard basis requirement. Nevertheless, this is not an arbitrary “algebraic” requirement, as shown by the following result:

Lemma 8 *Let notations and assumptions be as in Lemmas 1, 2 and 3. Suppose that the morphism $\pi^{(\ell,k)}$ is unramified at $T = 0$. Then $G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)}$ form a standard basis of the ideal $\mathcal{I}^{(\ell,k)}$.*

PROOF.— Let $x \in \mathbb{A}^{n+1}$ be a point of the fiber $(\pi^{(\ell,k)})^{-1}(0)$. Let $(\mathcal{O}_{V^{(\ell,k)},x}, \mathfrak{m}_x)$ denote the local ring of the point x on the variety $V^{(\ell,k)}$ and let $(\mathcal{O}_{\mathbb{A}^1,0}, \mathfrak{m}_0)$ denote the local ring of 0 on \mathbb{A}^1 . Since $\pi^{(\ell,k)}$ is unramified at $T = 0$, we have

$$\mathfrak{m}_x = (\pi^{(\ell,k)})^*(\mathfrak{m}_0) \quad (20)$$

for any $x \in (\pi^{(\ell,k)})^{-1}(0)$, where $(\pi^{(\ell,k)})^*$ denotes the local homomorphism $(\pi^{(\ell,k)})^* : \mathcal{O}_{\mathbb{A}^1,0} \rightarrow \mathcal{O}_{V^{(\ell,k)},x}$ induced by the morphism $\pi^{(\ell,k)}$.

Identity (20) implies that the morphism $d_x \pi^{(\ell,k)} : T_{V^{(\ell,k)},x} \rightarrow T_{\mathbb{A}^1,0}$ of tangent spaces is injective [22]. We deduce that the dimension $\dim(T_{V^{(\ell,k)},x})$ of the tangent space $T_{V^{(\ell,k)},x}$ of $V^{(\ell,k)}$ at x is at most 1. Taking into account that $V^{(\ell,k)}$ is an equidimensional variety of dimension 1 (Lemma 2), we conclude that $\dim(T_{V^{(\ell,k)},x}) = 1$. Therefore, x is a smooth point of $V^{(\ell,k)}$.

Identity (20) shows that the quotient ring $\mathcal{O}_{V^{(\ell,k)},x}/(\pi^{(\ell,k)})^*(\mathfrak{m}_0)$ is a zero-dimensional $\overline{\mathbb{Q}}$ -algebra. Let us observe that $\mathcal{O}_{V^{(\ell,k)},x}$ is a Cohen–Macaulay ring (because it is a localization of a Cohen–Macaulay ring), the local ring $\mathcal{O}_{\mathbb{A}^1,0}$ is a regular ring and the identity

$$\dim \mathcal{O}_{V^{(\ell,k)},x} = \dim \mathcal{O}_{\mathbb{A}^1,0} + \dim \mathcal{O}_{V^{(\ell,k)},x}/(\pi^{(\ell,k)})^*(\mathfrak{m}_0)$$

holds. Then applying [48, Theorem 23.1] we conclude that the local homomorphism

$$(\pi^{(\ell,k)})^* : \mathcal{O}_{\mathbb{A}^1,0} \rightarrow \mathcal{O}_{V^{(\ell,k)},x} \quad (21)$$

induced by $\pi^{(\ell,k)}$ is flat.

We observe that the localization $\overline{\mathbb{Q}}[V^{(\ell,k)}]_{\mathfrak{m}_0}$ is a semilocal ring, whose maximal ideals correspond to the maximal ideals \mathfrak{m}_x induced by the points x of $(\pi^{(\ell,k)})^{-1}(0)$. Therefore, since the morphism of (21) is flat for any point $x \in (\pi^{(\ell,k)})^{-1}(0)$, applying [48, Theorem 7.1] we conclude that

$$(\pi^{(\ell,k)})^* : \overline{\mathbb{Q}}[\mathbb{A}^1]_{\mathfrak{m}_0} \rightarrow \overline{\mathbb{Q}}[V^{(\ell,k)}]_{\mathfrak{m}_0}$$

is flat, i.e. $\pi^{(\ell,k)}$ is flat at $T = 0$. Therefore, from [5, Part I, Proposition 3.1] (see also [6]) it follows that any syzygy $(h_1, \dots, h_n) \in \overline{\mathbb{Q}}[Y]^n$ of the polynomials $G_1^{(\ell,k)}(0, Y), \dots, G_n^{(\ell,k)}(0, Y)$ “lifts” to a syzygy $(H_1, \dots, H_n) \in \overline{\mathbb{Q}}[T, Y]^n$ of $G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)}$, i.e. for $1 \leq i \leq n$ the identity $H_i(0, Y) = h_i(Y)$ holds.

Now we adapt the contents of e.g. [49] to our setting. For $F \in \overline{\mathbb{Q}}[T, Y]$, let $o_T(F)$ denote the highest power of T dividing F . We claim that any polynomial $G \in \mathcal{I}^{(\ell,k)}$ has a representation

$$G = \sum_{i=1}^n H_i G_i^{(\ell,k)} \quad (22)$$

with order $o_T(H_i) \geq o_T(G)$ for $1 \leq i \leq n$. Let $G \in \mathcal{I}^{(\ell,k)}$ be a polynomial with a representation $G = \sum_{i=1}^n H_i G_i^{(\ell,k)}$. Let $\alpha := \min\{o_T(H_i) : 1 \leq i \leq n\}$, and suppose that $\alpha < o_T(G)$ holds. Let \mathcal{J} be the set of indices i for which $\alpha = o_T(H_i)$ holds. Then the identity

$$\sum_{i \in \mathcal{J}} (T^{-\alpha} H_i)(0, Y) G_i^{(\ell,k)}(0, Y) = 0$$

shows that $(h_1, \dots, h_n) \in \overline{\mathbb{Q}}[Y]^n$, with $h_i := (T^{-\alpha} H_i)(0, Y)$ if $i \in \mathcal{J}$ and $h_i := 0$ otherwise, is a syzygy of $G_1^{(\ell,k)}(0, Y), \dots, G_n^{(\ell,k)}(0, Y)$. Then there exists a lifting $(\widetilde{H}_1, \dots, \widetilde{H}_n) \in \overline{\mathbb{Q}}[T, Y]^n$ of the syzygy (h_1, \dots, h_n) , and we have:

$$G = \sum_{i=1}^n (H_i - T^\alpha \widetilde{H}_i) G_i^{(\ell,k)},$$

with $o_T(H_i - T^\alpha \widetilde{H}_i) > \alpha$ for $1 \leq i \leq n$. Repeating this argument at most $o_T(G)$ times, we conclude the validity of our claim.

Finally, let $G \in \mathcal{I}^{(\ell,k)}$. Then we have a representation of G as in (22), with order $o_T(H_i) \geq o_T(G)$ for $1 \leq i \leq n$. Let \mathcal{J} be the (nonempty) set of indices i for which $o_T(G) = o_T(H_i)$ holds. Then we have

$$\begin{aligned} in(G) &= (T^{-o_T(G)} G)(0, Y) = \sum_{i \in \mathcal{J}} (T^{-o_T(G)} H_i)(0, Y) \cdot G_i^{(\ell,k)}(0, Y) \\ &= \sum_{i \in \mathcal{J}} (T^{-o_T(G)} H_i)(0, Y) \cdot in(G_i^{(\ell,k)}). \end{aligned}$$

This shows that $G_1^{(\ell,k)}, \dots, G_n^{(\ell,k)}$ form a standard basis of the ideal $\mathcal{I}^{(\ell,k)}$. ■

4 Algorithms and complexity estimates

Let notations and assumptions be as in Section 2.1. Let $\delta := \deg V$ denote the degree of the variety V , and let $D := \deg \pi$ denote the degree of the morphism $\pi : V \rightarrow \mathbb{A}^1$. Suppose that we are given a straight–line program β computing F_1, \dots, F_n with space \mathcal{S} and time \mathcal{T} .

Let S_1, S_2 be indeterminates over \mathbb{Q} . With the notations of Section 3.3, for $1 \leq \ell \leq g$ and $m_\ell \leq m \leq R$, let $q^{(\ell)}, f^{(\ell)}, f_{m,1}^{(\ell)}, \dots, f_{m,n}^{(\ell)} \in \mathbb{Q}[S_1]$ and $p^{(\ell)} \in \mathbb{Q}[S_1, S_2]$ be polynomials defining the system of rational Puiseux expansions of the branches of V lying above 0 of Section 3.3. In particular, we have the estimates $\deg(q^{(\ell)}) = f_\ell$, $\deg(f^{(\ell)}) < f_\ell$ and $\deg(f_{m,i}^{(\ell)}) < f_\ell$ for $1 \leq i \leq n$, and the singular parts of the (classical) Puiseux expansions of the branches of V lying over 0 are given by

$$\bigcup_{\ell=1}^g \left\{ \left(T^{e_\ell}, \sum_{m=m_\ell}^R f_m^{(\ell)}(s_1) s_2^m T^m \right); p^{(\ell)}(s_1, s_2) = q^{(\ell)}(s_1) = 0 \right\}, \quad (23)$$

where $f_m^{(\ell)} := (f_{m,1}^{(\ell)}, \dots, f_{m,n}^{(\ell)}) \in \mathbb{Q}[S_1]^n$. Let $U \in \mathbb{Q}[X]$ a generic linear form, i.e. a linear form whose projection polynomial $m_u \in \mathbb{Q}(\mathcal{E})[Z]$ satisfies $\deg_Z m_u = D$. Then identity (12) of Section 3 shows that m_u has the following factorization into irreducible factors in $\mathbb{Q}((\mathcal{E}))[Z]$:

$$m_u = \prod_{\ell=1}^g m_u^{(\ell)} := \prod_{\ell=1}^g \left(\prod_{k=1}^{f_\ell} \prod_{j=1}^{e_\ell} \left(Z - \sum_{m \geq m_\ell} U(\sigma_k^{(\ell)}(a_m^{(\ell)})) \sigma_k^{(\ell)} (\lambda_\ell^{-\frac{1}{e_\ell}})^m \xi_\ell^{jm} \mathcal{E}^{\frac{m}{e_\ell}} \right) \right). \quad (24)$$

In this section we exhibit an algorithm which has as input the straight–line program β and the dense representation of $p^{(\ell)}, q^{(\ell)}, f^{(\ell)}, f_{m,1}^{(\ell)}, \dots, f_{m,n}^{(\ell)}$ for $1 \leq \ell \leq g$ and $m_\ell \leq m \leq R$ and computes a geometric solution of V .

Let us fix ℓ with $1 \leq \ell \leq g$. The critical part of our algorithm is a procedure which computes a suitable approximation $\hat{m}_u^{(\ell)} \in \mathbb{Q}(\mathcal{E})[Z]$ of the polynomial $m_u^{(\ell)} \in \mathbb{Q}((\mathcal{E}))[Z]$. This procedure applies our variant of the global Newton–Hensel lifting of [30] and [28], based on Theorem 7. For this purpose, we shall deal with the variety $W^{(\ell)}$ of (15), namely

$$W^{(\ell)} := \{(s_1, s_2) \in \mathbb{A}^2 : q^{(\ell)}(s_1) = 0, p^{(\ell)}(s_1, s_2) = 0\}.$$

From the fact that $\deg W^{(\ell)} = e_\ell f_\ell$ holds, we easily conclude that S_2 is a primitive element of the \mathbb{Q} –algebra extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[W^{(\ell)}]$. Therefore, we have a geometric solution of $W^{(\ell)}$ of the form

$$W^{(\ell)} = \{(s_1, s_2) \in \mathbb{A}^2 : m_{S_2}^{(\ell)}(s_2) = 0, s_1 \frac{\partial m_{S_2}^{(\ell)}}{\partial Z}(s_2) - v^{(\ell)}(s_2) = 0\}, \quad (25)$$

where $m_{S_2}^{(\ell)} \in \mathbb{Q}[Z]$ is the minimal polynomial of S_2 in the extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[W^{(\ell)}]$ and $v^{(\ell)} \in \mathbb{Q}[Z]$ satisfies $\deg v^{(\ell)} < \deg W^{(\ell)}$.

In the sequel, time-complexity estimates will be given using the standard “soft-Oh” notation O^\sim , which does not take into account polylogarithmic terms.

Lemma 9 *There exists a computation tree computing the geometric solution (25) of $W^{(\ell)}$ with space $O(e_\ell f_\ell^2)$ and time $O^\sim(e_\ell f_\ell^2)$.*

PROOF.— Let us suppose first $f_\ell = 1$. Then we may assume without loss of generality $q^{(\ell)} = S_1$. Furthermore, we have $f^{(\ell)} \in \mathbb{Q} \setminus \{0\}$ and $p^{(\ell)} = S_2^{e_\ell} - f^{(\ell)}$. Therefore, $m_{S_2}^{(\ell)} = p^{(\ell)} = Z^{e_\ell} - f^{(\ell)}$ and $v^{(\ell)} = 0$ yield in fact the geometric solution of $W^{(\ell)}$ we are looking for (and we have nothing to compute).

Now suppose that $f_\ell > 1$ holds. Let us introduce a new indeterminate Λ , and let us consider the linear form $\mathcal{L} := \Lambda S_1 + S_2 \in \mathbb{Q}[\Lambda][S_1, S_2]$. It is easy to see that \mathcal{L} is a primitive element of the integral ring extension $\mathbb{Q}[\Lambda] \hookrightarrow \mathbb{Q}[\Lambda] \otimes \mathbb{Q}[W^{(\ell)}]$, with minimal equation

$$m_{\mathcal{L}}^{(\ell)}(Z) = \text{Res}_{S_1}(q^{(\ell)}(S_1), p^{(\ell)}(S_1, Z - \Lambda S_1)), \quad (26)$$

where $\text{Res}_{S_1}(f, g)$ denotes the resultant of f and g with respect to S_1 . Following an idea originally due to [44] (see also [47, II.21], [54], [2], [56], [33]), we have a congruence relation:

$$m_{\mathcal{L}}^{(\ell)}(Z) = m_{S_2}^{(\ell)}(Z) + \Lambda \left(S_1 \frac{\partial m_{S_2}^{(\ell)}}{\partial Z}(Z) + \tilde{v}^{(\ell)}(Z) \right) \pmod{\Lambda^2},$$

with $\tilde{v}^{(\ell)} \in \mathbb{Q}[Z]$, $\deg \tilde{v}^{(\ell)} < e_\ell f_\ell$ and $S_1(\partial m_{S_2}^{(\ell)}/\partial Z)(S_2) + \tilde{v}^{(\ell)}(S_2) \in I(W^{(\ell)})$. Then $m_{S_2}^{(\ell)}$ and $v^{(\ell)} := -\tilde{v}^{(\ell)}$ can be obtained from the resultant of the right-hand side of identity (26) modulo Λ^2 . Using interpolation in the variable Z , this computation can be performed with space $O(e_\ell f_\ell^2)$ and time $O^\sim(e_\ell f_\ell^2)$. ■

Our variant of the global Newton–Hensel lifting requires the R -th “initial approximation” of $m_u^{(\ell)}$ given by the following expression (compare with (24)):

$$\tilde{m}_u^{(\ell)}(T^{e_\ell}, Z) := \prod_{k=1}^{f_\ell} \prod_{j=1}^{e_\ell} \left(Z - \sum_{m=m_\ell}^R U(\sigma_k^{(\ell)}(a_m^{(\ell)})) \sigma_k^{(\ell)} (\lambda_\ell^{-\frac{1}{e_\ell}})^m \zeta_\ell^{jm} T^m \right). \quad (27)$$

Lemma 10 *There exists a computation tree which takes as input the polynomials $p^{(\ell)}, q^{(\ell)}, f^{(\ell)}, f_{m,i}^{(\ell)}$ ($1 \leq k \leq n$), $m_{S_2}^{(\ell)}, v^{(\ell)}$, which define the ℓ -th expansion of the given system of rational Puiseux expansions of V and form the geometric solution (25) of $W^{(\ell)}$, and computes the dense representation of $\tilde{m}_u^{(\ell)}$ with space $O(R_\ell e_\ell f_\ell)$ and time $O^\sim(R_\ell e_\ell^2 f_\ell^2)$, where $R_\ell := (R - m_\ell) e_\ell f_\ell + 1$.*

PROOF.— From the definition of $\widetilde{m}_u^{(\ell)}$ and the variety $W^{(\ell)}$ we easily see that $T^{-m_\ell e_\ell f_\ell} \widetilde{m}_u^{(\ell)}(T^{e_\ell}, T^{m_\ell} Z)$ equals the characteristic polynomial $\chi_{\widetilde{u}}$ of the polynomial $\widetilde{u}(T, S_1, S_2) := \sum_{m=m_\ell}^R U(f_m^{(\ell)}(S_1)) S_2^m T^{m-m_\ell}$ in the \mathbb{Q} -algebra $\mathbb{Q}[T] \otimes \mathbb{Q}[W^{(\ell)}] \cong \mathbb{Q}[\mathbb{A}^1 \times W^{(\ell)}]$. Let us observe that S_2 is a primitive element of the extension $\mathbb{Q}[T] \hookrightarrow \mathbb{Q}[\mathbb{A}^1 \times W^{(\ell)}]$ and the input polynomials $m_{S_2}^{(\ell)}, v^{(\ell)}$ also yield a geometric solution of the variety $\mathbb{A}^1 \times W^{(\ell)}$.

In order to compute the dense representation of $\chi_{\widetilde{u}}$ we use a straightforward adaptation of the algorithm of [40, Lemma 3]. Let $M \in \mathbb{Q}^{(e_\ell f_\ell) \times (e_\ell f_\ell)}$ be the companion matrix of the polynomial $m_{S_2}^{(\ell)}$. Then the characteristic polynomial of the matrix $N := \widetilde{u}(T, v^{(\ell)}(M), M)$ equals the characteristic polynomial $\chi_{\widetilde{u}}$.

Let us suppose first that $R = m_\ell$ holds. Then $\chi_{\widetilde{u}}$ is a pseudo-homogeneous polynomial whose coefficients can be computed using [40, Lemma 3] with space $O(e_\ell f_\ell)$ and time $O(e_\ell^2 f_\ell^2)$. On the other hand, if $R \neq m_\ell$, taking into account that the algorithm manipulates polynomials in T of degree at most $(R - m_\ell)e_\ell f_\ell$, and the fact that the polynomial $m_{S_2}^{(\ell)}(Z)$ does not depend on the variable T , we conclude that the procedure underlying [40, Lemma 3] can be executed using space $O((R - m_\ell)e_\ell^2 f_\ell^2)$ and time $O((R - m_\ell)e_\ell^3 f_\ell^3)$. In conclusion, we see that the procedure takes in both cases space $O((R - m_\ell)e_\ell f_\ell + 1)e_\ell f_\ell$ and time $O(((R - m_\ell)e_\ell f_\ell + 1)e_\ell^2 f_\ell^2)$. Finally, taking into account that the dense representation of $\widetilde{m}_u^{(\ell)}$ can be immediately obtained from that of $\chi_{\widetilde{u}}$ finishes the proof of the lemma. \blacksquare

Now we can describe the algorithm computing an arbitrary approximation in $\mathbb{Q}(\mathcal{E})[Z]$ of the polynomial $m_u^{(\ell)} \in \mathbb{Q}((\mathcal{E}))[[Z]]$. This algorithm applies our variant of the global Newton–Hensel lifting (Theorem 7), combined with an adaptation of the procedure of [33, Proposition 7]. For this purpose, following Theorem 7, let Y_1, \dots, Y_n be indeterminates over \mathbb{Q} , let $Y := (Y_1, \dots, Y_n)$, and let us define $G_1^{(\ell)}, \dots, G_n^{(\ell)} \in \mathbb{Q}[S_1, S_2^{-1}, S_2, T, Y]$ by:

$$G_j^{(\ell)} := T^{\alpha_{j\ell}} F_j \left(T^{e_\ell}, \sum_{m=m_\ell}^{R-1} f_m^{(\ell)}(S_1) (S_2 T)^m + Y T^R \right). \quad (28)$$

Proposition 11 *Let us fix $\kappa > 0$. Then there exists a computation tree which takes as input the polynomials $p^{(\ell)}, q^{(\ell)}, f^{(\ell)}, f_{m,i}^{(\ell)}$ ($1 \leq k \leq n$), $m_{S_2}^{(\ell)}, v^{(\ell)}$, which define the ℓ -th parameterization of the given system of rational Puiseux expansions of V and form the geometric solution (25) of $W^{(\ell)}$, and computes an approximation $\hat{m}_u^{(\ell)} \in \mathbb{Q}(\mathcal{E})[[Z]]$ of $m_u^{(\ell)}$ in $\mathbb{Q}((\mathcal{E}))[[Z]]$ with precision $\lceil \frac{R+\kappa}{e_\ell} \rceil + 1$ and parameterizations of Y_1, \dots, Y_n in terms of the linear form U up to order $\lceil \frac{R+\kappa}{e_\ell} \rceil + 1$, with space and time*

$$O\left(n e_\ell f_\ell (\mathcal{S}_\ell (\kappa + \delta_0 m_\ell e_\ell f_\ell) + R_\ell)\right) \text{ and } O\left(n e_\ell f_\ell (\mathcal{I}_\ell + n^4) (\kappa + \delta_0 m_\ell e_\ell f_\ell + (R_\ell - 1) e_\ell f_\ell)\right)$$

respectively, where $R_\ell := (R - m_\ell)e_\ell f_\ell + 1$, $\delta_0 := -1$ for $m_\ell < 0$ and $\delta_0 := 0$ otherwise, and $\mathcal{S}_\ell, \mathcal{T}_\ell$ denote the space and time complexity required for the evaluation of the polynomials $G_1^{(\ell)}, \dots, G_n^{(\ell)}$.

PROOF.— Theorem 5 shows that the Newton operator $N_{G^{(\ell)}}$ of (18) is well defined at $f_R^{(\ell)}(s_1)s_2^R$ for any $(s_1, s_2) \in W^{(\ell)}$. Then Theorem 7 shows that from the $\tau := \lceil \log_2(\kappa + \delta_0 m_\ell e_\ell f_\ell + 1) \rceil$ -fold iteration of the Newton operator $N_{G^{(\ell)}}$ we obtain a rational function $\hat{m}_u \in \mathbb{Q}(\mathcal{E})[Z]$ which approximates $m_u^{(\ell)}$ in $\mathbb{Q}(\mathcal{E})$ with precision $\lfloor \frac{R+\kappa}{e_\ell} \rfloor$.

In order to compute $\hat{m}_u(T^{e_\ell}, Z)$ we use an adaptation of the procedure of [33, Proposition 7]: we start with the initial approximation provided by the polynomial $\tilde{m}_u^{(\ell)}$ of (27) and parameterizations of X_1, \dots, X_n in terms of the linear form U up to order $R+1$, i.e. elements $\tilde{v}_1^{(\ell)}, \dots, \tilde{v}_n^{(\ell)}$ of $\mathbb{Q}(\mathcal{E})[Z]$ such that $\frac{\partial \tilde{m}_u^{(\ell)}}{\partial Z}(T^{e_\ell}, U)X_i \equiv \tilde{v}_i^{(\ell)}(T^{e_\ell}, U) \pmod{(T^{R+1}, m_u^{(\ell)}(T^{e_\ell}, U))}$. Then we perform τ steps of the global Newton–Hensel lifting of [33, Proposition 7] applied to the polynomials $G_1^{(\ell)}, \dots, G_n^{(\ell)}$.

Applying Lemma 10 we obtain the polynomial $\tilde{m}_u^{(\ell)}$ of (27) with space $O(R_\ell e_\ell f_\ell)$ and time $O(R_\ell e_\ell^2 f_\ell^2)$. Combining Lemma 10 and the formulae of e.g. [2], [56] or [33] as in the proof of Lemma 9 we obtain the parameterizations of X_1, \dots, X_n in terms of U up to order $R+1$ with space $O(nR_\ell e_\ell f_\ell)$ and time $O(nR_\ell e_\ell^2 f_\ell^2)$.

Now, applying [33, Proposition 7] we obtain an approximation of $m_u^{(\ell)}$ with precision $R + \kappa + 1$ in $\mathbb{Q}(\mathcal{E})[Z]$ and parameterizations of X_1, \dots, X_n in terms of U up to order $R + \kappa + 1$ with space and time

$$O\left(n e_\ell f_\ell (\mathcal{S}_\ell(\kappa + \delta_0 m_\ell e_\ell f_\ell) + R_\ell)\right) \text{ and } O\left(n e_\ell f_\ell (\mathcal{T}_\ell + n^4)(\kappa + \delta_0 m_\ell e_\ell f_\ell + R_\ell)\right),$$

respectively. Since $m_u^{(\ell)}(T^{e_\ell}, Z)$ and the parameterizations of X_1, \dots, X_n in terms of U are elements of $\mathbb{Q}(\mathcal{E})[Z]$, replacing T^{e_ℓ} by \mathcal{E} we obtain $\hat{m}_u^{(\ell)}$ and the parameterizations of X_1, \dots, X_n in terms of U up to order $\lfloor \frac{R+\kappa}{e_\ell} \rfloor + 1$. Adding the complexity of each step of our procedure the proposition follows. ■

Now we state the main result of this section:

Theorem 12 *There exists a computation tree in $\mathbb{Q}[\mathcal{E}, X]$ which takes as input the straight–line program β defining the polynomials F_1, \dots, F_n and the given system of rational Puiseux expansions and computes a geometric solution of V with space and time*

$$O\left(n \delta \sum_{\ell=1}^g e_\ell^2 f_\ell (\mathcal{S}_\ell(\delta_0 m_\ell e_\ell f_\ell + 1) + R_\ell)\right) \text{ and } O\left(\sum_{\ell=1}^g n e_\ell^2 f_\ell (\mathcal{T}_\ell + n^4)(\delta + \delta_0 m_\ell e_\ell f_\ell + (R_\ell - 1)f_\ell)\right)$$

respectively, where $R_\ell := (R - m_\ell)e_\ell f_\ell + 1$, $\delta_0 := -1$ for $m_\ell < 0$ and $\delta_0 := 0$ otherwise, and $\mathcal{S}_\ell, \mathcal{T}_\ell$ denote the space and time complexity required for the evaluation of the polynomials $G_1^{(\ell)}, \dots, G_n^{(\ell)}$ of (28). Furthermore, for any $\rho \geq 2$, such a computation tree can be randomly constructed with a probability of success of at least $1 - \frac{1}{2\rho} \geq \frac{3}{4}$.

PROOF.— Let $U \in \mathbb{Q}[X]$ be a generic linear form. Let us fix $\rho \geq 2$. Using the Zippel–Schwartz test (see [59], [68]), we conclude that the coefficients of U can be randomly chosen in the set $\{1, \dots, 4\rho n D^2\}$ with a probability of success of at least $1 - \frac{1}{2\rho} \geq \frac{3}{4}$, where $D := \deg \pi$.

Let $\delta := \deg V$. Applying Proposition 11 for $1 \leq \ell \leq g$ with $\kappa := 3e_\ell \delta - R$, we obtain elements $\hat{m}_u^{(\ell)}, \hat{v}_1^{(\ell)}, \dots, \hat{v}_n^{(\ell)}$ ($1 \leq \ell \leq g$) of $\mathbb{Q}(\mathcal{E})[Z]$ such that:

- (1) $\hat{m}_u^{(\ell)}(\mathcal{E}, Z) \equiv m_u^{(\ell)}(\mathcal{E}, Z)$ modulo $(\mathcal{E}^{3\delta+1})$,
- (2) $\frac{\partial \hat{m}_u^{(\ell)}}{\partial Z}(\mathcal{E}, U)X_i \equiv \hat{v}_i^{(\ell)}(\mathcal{E}, U)$ modulo $(\mathcal{E}^{3\delta+1}, m_u^{(\ell)}(\mathcal{E}, U))$,
- (3) $\deg_Z \hat{m}_u^{(\ell)} \leq e_\ell f_\ell$ and $\deg_Z \hat{v}_i^{(\ell)} \leq e_\ell f_\ell - 1$ for $1 \leq i \leq n$.

These polynomials can be computed with space and time

$$O\left(n\delta \sum_{\ell=1}^g e_\ell^2 f_\ell (\mathcal{S}_\ell(\delta_0 m_\ell f_\ell + 1) + R_\ell)\right) \text{ and } O\left(\sum_{\ell=1}^g n e_\ell^2 f_\ell (\mathcal{T}_\ell + n^4)(\delta + \delta_0 m_\ell f_\ell + (R_\ell - 1)f_\ell)\right).$$

Let v_1, \dots, v_n be the elements of $\mathbb{Q}(\mathcal{E})[Z]$ parameterizing X_1, \dots, X_n in terms of the linear form U in V , i.e. satisfying $\frac{\partial m_u}{\partial Z}(\mathcal{E}, U)X_i \equiv v_i(\mathcal{E}, U) \pmod{I(V)}$ for $1 \leq i \leq n$. From [58, Proposition 1] we see that the orders $o_{\mathcal{E}}(m_u), o_{\mathcal{E}}(v_1), \dots, o_{\mathcal{E}}(v_n)$ are bounded from below by $-\delta$. Combining this observation with properties (1), (2), (3) we conclude that the following congruence relations hold in $\mathbb{Q}(\mathcal{E})[Z]$:

$$\begin{aligned} \check{m}_u &:= \prod_{\ell=1}^g \hat{m}_u^{(\ell)} \equiv m_u \pmod{(\mathcal{E}^{2\delta+1})}, \\ \check{v}_i &:= \sum_{1 \leq \ell \leq g} \left(\prod_{\ell' \neq \ell} \hat{m}_u^{(\ell')} \right) \hat{v}_i^{(\ell)} \equiv v_i \pmod{(\mathcal{E}^{2\delta+1})}. \end{aligned}$$

Using fast procedures for multiplication and Chinese Remainder Theorem (see e.g. [9]), we compute the polynomials $\check{m}_u, \check{v}_1, \dots, \check{v}_n$ using space $O(n\delta D)$ and time $O(n\delta D)$.

Taking into account the estimates

$$\begin{aligned} \deg_Z m_u &= D, \quad \deg_Z v_i \leq D - 1, \quad (1 \leq i \leq n), \\ \deg_{\mathcal{E}} m_u &\leq \delta, \quad \deg_{\mathcal{E}} v_i \leq \delta \quad (1 \leq i \leq n), \end{aligned}$$

(see [58]), we conclude that m_u, v_1, \dots, v_n can be computed from the truncated Laurent series $\check{m}_u, \check{v}_1, \dots, \check{v}_n$ using Padé approximants. More precisely,

by interpolation in the variable Z we reduce the computation of the polynomials m_u, v_1, \dots, v_n to at most $(n+1)D$ problems of Padé approximation of degree at most δ . Thus, using a fast algorithm for computing Padé approximations (see e.g. [9]), we conclude that the polynomials m_u, v_1, \dots, v_n can be computed using space $O(n\delta D)$ and time $O(n\delta D)$. Adding the space and time complexity of each step of our procedure we deduce the complexity estimate of the statement of Theorem 12. ■

Let us make here a few remarks concerning the hypotheses and complexity estimates of Theorem 12. First we observe that the parameters S_ℓ and T_ℓ can be estimated by $O(\mathcal{S}+n)$ and $O(\mathcal{T}+nR_\ell)$ respectively, where \mathcal{S} and \mathcal{T} are the space and time complexity of the straight-line program computing F_1, \dots, F_n . Then we have the worst-case estimates $O(n^2\mathcal{S}\delta D^4)$ and $O(n^4\mathcal{T}\delta D^4)$ for the space and time complexity of the procedure underlying Theorem 12. Nevertheless, these estimates can be improved in several important cases, such as that with $R = m_\ell$ and $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})} \hookrightarrow \mathbb{Q}[V]_{(\mathcal{E})}$ an integral extension. In this case we have the estimates $O((\mathcal{S}+n)n\delta D e)$ and $O((\mathcal{T}+n^4)n\delta D e)$ respectively, with $e := \max\{e_\ell : 1 \leq \ell \leq g\}$ (see Subsections 5.3 and 5.4).

Theorem 12 generalizes the results of [39] and [58] in the unidimensional case. More precisely, in case that the “known” π -fiber is unramified, our space and time complexity estimates are $O((n+\mathcal{S})n\delta D)$ and $O((n^4+\mathcal{T})D\delta)$, which improve the estimates of [39] and have the same asymptotic behaviour as those of [58].

The algorithm underlying Theorem 12 proceeds by computing a suitable approximation of the factors $m_u^{(\ell)}$ of the minimal polynomial $m_u = \prod_{1 \leq \ell \leq g} m_u^{(\ell)}$ of the linear form U . Observe that for $1 \leq \ell \leq g$ the polynomial $m_u^{(\ell)}$ is an irreducible polynomial of $\mathbb{Q}((\mathcal{E}))[Z]$ (see Section 3). In this sense, this algorithm constitutes an improvement of the refinements described in Section 3 of [39] (based on the factorization of the polynomial m_u in $\mathbb{Q}[\mathcal{E}, Z]$).

The singular parts (23) can be efficiently computed from the input polynomials F_1, \dots, F_n and a geometric solution of an *unramified* fiber of the morphism π , by a suitable combination of the following algorithmic tools:

- A Newton polygon algorithm for computing the singular parts of a system of rational Puiseux expansions as in [23] or [66].
- A projection procedure for unramified fibers as in [58].

The asymptotic space and time complexity of such a procedure is roughly $O(D^4 + \varrho^2)$ and $O(D^8 + \varrho^2)$ respectively, where ϱ denotes the geometric degree of the system F_1, \dots, F_n (in the sense of [28]). Observe that the estimates $D \leq \delta \leq \varrho$ hold. Nevertheless, as we are only interested in particular cases where the singular parts can be immediately generated (see Subsections 5.3 and 5.4), we are not going to use this procedure.

5 Examples

In this section we apply our algorithmic method in order to compute a geometric solution of certain zero-dimensional polynomial equation systems. In Section 5.1 we treat the case of Pham–Brieskorn systems. In Section 5.2 we treat a family of systems which arise from a semidiscretization of certain parabolic differential equations with nonlinear source terms and nonlinear boundary conditions. Finally, in Section 5.4 we treat a generalization of Reimer systems, which we called generalized Reimer systems.

In all the above cases, we “deform” the polynomial equation system under consideration to a one-dimensional polynomial equation system satisfying the hypotheses of Theorem 7. Then the algorithm underlying the proof of Theorem 12 yields an efficient procedure to compute a geometric solution of the original zero-dimensional polynomial equation system.

5.1 Pham–Brieskorn systems

Let us fix $n, d \in \mathbb{N}$. Let $g_1, \dots, g_n \in \mathbb{Q}[X] := \mathbb{Q}[X_1, \dots, X_n]$ satisfy $\deg(g_i) < d$ and $g_i(0, \dots, 0) \neq 0$ for $1 \leq i \leq n$. Let us define $f_1, \dots, f_n \in \mathbb{Q}[X]$ by:

$$f_1 := X_1^d - g_1, \dots, f_n := X_n^d - g_n. \quad (29)$$

A system of this form is called a *Pham–Brieskorn system* (see e.g. [34], [35], [11], [53]). It is easy to see that f_1, \dots, f_n form a regular sequence of $\mathbb{Q}[X]$ and generate a radical ideal of $\mathbb{Q}[X]$. Therefore, f_1, \dots, f_n define a zero-dimensional affine subvariety \tilde{V} of \mathbb{A}^n . Our aim is to compute a geometric solution of this variety \tilde{V} .

Let \mathcal{E} be an indeterminate over \mathbb{Q} and define $F_1, \dots, F_n \in \mathbb{Q}[\mathcal{E}, X]$ by:

$$F_1 := X_1^d - \mathcal{E}g_1, \dots, F_n := X_n^d - \mathcal{E}g_n. \quad (30)$$

Let V be the affine subvariety of \mathbb{A}^{n+1} defined by the polynomials F_1, \dots, F_n , and let $\pi : V \rightarrow \mathbb{A}^1$ be the morphism defined by $\pi(\varepsilon, x) = \varepsilon$. We observe that $\pi^{-1}(1) = \{1\} \times \tilde{V}$ and $\pi^{-1}(0) = \{0\} \subset \mathbb{A}^{n+1}$ hold.

In Section 5.3 we exhibit an algorithm which computes a geometric solution of the variety V . Furthermore, specializing the polynomials of $\mathbb{Q}[\mathcal{E}, X]$ which constitute this geometric solution into the value $\mathcal{E} = 1$ we shall obtain a geometric solution of \tilde{V} .

5.2 Systems coming from a semidiscretization of certain parabolic differential equations

In this section we consider a family of polynomial equation systems which arises in the analysis of the stationary solutions of a numerical approximation, obtained by a semidiscretization in space, of certain parabolic differential equations with nonlinear source terms and nonlinear boundary conditions (see e.g. [13], [25]).

Let us fix $n, d \in \mathbb{N}$ with $d \geq 2$. Let T be an indeterminate over \mathbb{Q} , and let $g, h \in \mathbb{Q}[T] \setminus \{0\}$ satisfy $\deg(g) < d$ and $\deg(h) = d$. Let us write $h = aT^d + h_1(T)$ with $a \neq 0$ and $\deg(h_1) < d$. Let f_1, \dots, f_n be the polynomials of $\mathbb{Q}[X] := \mathbb{Q}[X_1, \dots, X_n]$ defined in the following way:

$$\begin{aligned} f_1 &:= 2(n-1)^2(X_2^d - X_1^d) - g(X_1), \\ f_i &:= (n-1)^2(X_{i+1}^d - 2X_i^d + X_{i-1}^d) - g(X_i), \quad (2 \leq i \leq n-1) \\ f_n &:= 2(n-1)^2(X_{n-1}^d - X_n^d) + 2(n-1)h(X_n) - g(X_n). \end{aligned} \quad (31)$$

An important case of study is that of the stationary solutions of the porous medium equation with nonlinear source terms and nonlinear boundary condition (see e.g. [41], [17]). Typical discretizations of this problem lead for example to instances of system (31) with $h := T^d$ and $g := T$ (see e.g. [25]).

Let \tilde{V} be the affine subvariety of \mathbb{A}^n defined by the polynomials f_1, \dots, f_n . Our aim is to exhibit an efficient algorithm which computes a geometric solution of the variety \tilde{V} . For this purpose, let $f := (f_1, \dots, f_n)$, $e_n := (0, \dots, 0, 1) \in \mathbb{Q}^n$, $G := (g(X_1), \dots, g(X_n))$, and $X^d := (X_1^d, \dots, X_n^d)$. Let $A \in \mathbb{Q}^{n \times n}$ be the following nonsingular tridiagonal matrix:

$$A := (n-1)^2 \begin{pmatrix} -2 & 2 & & & & \\ & 1 & -2 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & -2 & 1 \\ & & & & 2 & -2 + \frac{2a}{n-1} \end{pmatrix}.$$

Then the polynomials f_1, \dots, f_n can be expressed as:

$$f^t = A \cdot (X^d)^t + 2(n-1)h_1(X_n)e_n^t - G^t, \quad (32)$$

where t denotes transposition.

In order to solve the system defined by the polynomials in (32), we introduce

a new indeterminate \mathcal{E} and consider the following polynomials of $\mathbb{Q}[\mathcal{E}, X]$:

$$(\tilde{F}_1, \dots, \tilde{F}_n)^t := A \cdot (X^d)^t + \mathcal{E} \left(2(n-1)h_1(X_n)e_n^t - G^t \right) - 2(n-1)\mathcal{E}(1-\mathcal{E})e_n^t. \quad (33)$$

Let V be the affine subvariety of \mathbb{A}^{n+1} defined by the polynomials $\tilde{F}_1, \dots, \tilde{F}_n$ and let $\pi : V \rightarrow \mathbb{A}^1$ the morphism defined by $\pi(\varepsilon, x) = \varepsilon$. We observe that $\pi^{-1}(1) = \{1\} \times \tilde{V}$ and $\pi^{-1}(0) = \{0\} \subset \mathbb{A}^{n+1}$. Since the matrix A is nonsingular, multiplying both sides of (33) by A^{-1} we obtain the following polynomials, whose zero set also defines the variety V :

$$(F_1, \dots, F_n)^t := (X^d)^t + \mathcal{E}A^{-1} \left(2(n-1)h_1(X_n)e_n^t - G^t \right) - \mathcal{E}(\mathcal{E}-1)v^t, \quad (34)$$

where $v := \frac{n-1}{2a}(1, \dots, 1)$. In Section 5.3 we exhibit an algorithm computing a geometric solution of the variety V . By specializing the polynomials of $\mathbb{Q}[\mathcal{E}, X]$ which constitute this geometric solution into the value $\mathcal{E} = 1$ we shall obtain a geometric solution of our input variety \tilde{V} .

5.3 A common approach to both examples

In this section we describe an algorithm which finds a geometric solution of the variety defined by any system of the form (30) and (34). Then, we shall specialize the polynomials of $\mathbb{Q}[\mathcal{E}, X]$ which form such geometric solution into the value $\mathcal{E} = 1$ in order to obtain a geometric solution of the variety defined by the corresponding system of the form (29) and (31).

Let us fix $n, d \in \mathbb{N}$. For $1 \leq i \leq n$, let $H_i \in \mathbb{Q}[\mathcal{E}, X]$ satisfy $\deg H_i \leq d-1$ and $\alpha_i := H_i(0, 0) \neq 0$. Suppose further that we are given a straight-line program computing the polynomials H_1, \dots, H_n using space \mathcal{S} and time \mathcal{T} .

For $1 \leq i \leq n$, let us define $F_i \in \mathbb{Q}[\mathcal{E}, X]$ by the following expression:

$$F_i := X_i^d - \mathcal{E}H_i(\mathcal{E}, X). \quad (35)$$

Let \mathcal{I} be the ideal of $\mathbb{Q}[\mathcal{E}, X]$ generated by F_1, \dots, F_n and let V be the affine subvariety of \mathbb{A}^{n+1} defined by \mathcal{I} . Let $\pi : V \rightarrow \mathbb{A}^1$ denote the restriction to V of the canonical projection onto the first coordinate. Our purpose is to compute a geometric solution of $\{1\} \times \tilde{V} := \pi^{-1}(1)$.

It is easy to see that any system of the form (30) and (34) is a particular instance of a system of the form (35). In order to apply our algorithmic method, we first show in Lemmas 13 and 14 below that the polynomials F_1, \dots, F_n of (35) form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$, the ideal $\mathcal{I} \subset \mathbb{Q}[\mathcal{E}, X]$ they generate is radical, and the morphism π is finite and generically unramified.

Lemma 13 *The polynomials F_1, \dots, F_n form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$ and the morphism π is finite.*

PROOF.— From Buchberger’s first criterion (see e.g. [7]), we conclude that for $1 \leq i \leq n$ the polynomials F_1, \dots, F_i form a Gröbner basis of the ideal they generate with respect to the graded lexicographical order induced by the ordering $X_1 > \dots > X_n > \mathcal{E}$. This implies that the affine variety of \mathbb{A}^{n+1} defined by F_1, \dots, F_i has codimension i for $1 \leq i \leq n$. Then F_1, \dots, F_n form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$.

Furthermore, we observe that the leading monomial of F_i under this order is X_i^d for $1 \leq i \leq n$. Therefore, the set $\{X_1^{i_1} \cdots X_n^{i_n} : 0 \leq i_1, \dots, i_n < d\}$ is a basis as $\mathbb{Q}[\mathcal{E}]$ -module of $\mathbb{Q}[\mathcal{E}, X]/\mathcal{I}$. This proves that π is a finite morphism. ■

For $1 \leq i \leq n$, let $G_i \in \mathbb{Q}[\mathcal{E}, X]$ be the following polynomial:

$$G_i(\mathcal{E}, X) := \mathcal{E}^{-d} F_i(\mathcal{E}^d, \mathcal{E}X).$$

Let $\widetilde{W} \subset \mathbb{A}^{n+1}$ be the affine variety defined by G_1, \dots, G_n , and let $\tilde{\pi} : \widetilde{W} \rightarrow \mathbb{A}^1$ be the morphism induced by the canonical projection onto the first coordinate. We claim the morphism $\tilde{\pi}$ is generically unramified.

Let us observe that for $\varepsilon \neq 0$ we have $\#(\tilde{\pi}^{-1}(\varepsilon)) = \#(\pi^{-1}(\varepsilon^d))$. Therefore, from the fact that the morphism π is finite we easily conclude that $\tilde{\pi}$ is dominant and $\dim \widetilde{W} \geq 1$ holds. Furthermore, from the fact that $\mathbb{Q}(V)$ is a zero-dimensional $\mathbb{Q}(\mathcal{E})$ -algebra, we deduce that $\mathbb{Q}(\widetilde{W})$ is also a zero-dimensional $\mathbb{Q}(\mathcal{E})$ -algebra. This shows that \widetilde{W} is a one-dimensional variety.

Let us fix $\varepsilon \in \mathbb{A}^1$. Taking into account that $\deg_X G_i(\varepsilon, X) = d$ for $1 \leq i \leq n$, from the Bézout inequality (see [36], [26]) we deduce that $\deg \tilde{\pi}^{-1}(\varepsilon) \leq d^n$ holds. On the other hand, for $1 \leq i \leq n$ we have $G_i(0, X) = X_i^d - \alpha_i$, where $\alpha_i = H_i(0, 0) \neq 0$. This implies that $\tilde{\pi}^{-1}(0)$ has cardinality d^n . We conclude that any generic fiber $\tilde{\pi}^{-1}(\varepsilon)$ has cardinality d^n .

Lemma 14 *\mathcal{I} is a radical ideal and the morphism π is generically unramified.*

PROOF.— For a generic choice $\varepsilon \in \mathbb{A}^1$, we have $\#(\tilde{\pi}^{-1}(\varepsilon)) = \#(\pi^{-1}(\varepsilon^d)) = d^n$. This implies that there exists a fiber $\pi^{-1}(\varepsilon)$ of cardinality d^n . On the other hand, applying the Bézout inequality (see [36], [26]) we see that $\#(\pi^{-1}(\varepsilon)) \leq d^n$ holds for any $\varepsilon \in \mathbb{A}^1$. We conclude that $\#(\pi^{-1}(\varepsilon)) = d^n$ holds for any generic choice of the value $\varepsilon \in \mathbb{A}^1$.

Let ε be a generic element of \mathbb{A}^1 . Then $\dim_{\mathbb{C}} \mathbb{C}[X]/(F_1(\varepsilon, X), \dots, F_n(\varepsilon, X)) = d^n = \deg \pi^{-1}(\varepsilon)$. This implies (see e.g. [20, Corollary 2.6]) that $\pi^{-1}(\varepsilon)$ is a smooth variety and the polynomials $F_1(\varepsilon, X), \dots, F_n(\varepsilon, X)$ generate a rad-

ical ideal of $\mathbb{C}[X]$. In particular, we have that the Jacobian determinant $J_F(\varepsilon, X) := \det(\partial F_i / \partial X_j)_{1 \leq i, j \leq n}(\varepsilon, X)$ does not vanish on any point $x \in \mathbb{A}^n$ with $(\varepsilon, x) \in \pi^{-1}(\varepsilon)$. Thus, $J_F(\mathcal{E}, X)$ is not a zero divisor of $\mathbb{Q}[\mathcal{E}, X]/\mathcal{I}$ and π is generically unramified. Finally, since F_1, \dots, F_n form a regular sequence of $\mathbb{Q}[\mathcal{E}, X]$, from [24, Theorem 18.15] we deduce that the ideal \mathcal{I} is radical. ■

Let us observe that the origin $0 \in \mathbb{A}^{n+1}$ is the only point of $\pi^{-1}(0)$. Therefore, there are $\deg(\pi) = d^n$ branches of the curve V passing through $0 \in \mathbb{A}^{n+1}$.

For $F \in \mathbb{Q}[\mathcal{E}, X]$, let us write $F(\mathcal{E}^d, \mathcal{E}X) = \mathcal{E}^\alpha f(X) + O(\mathcal{E}^{\alpha+1})$, with $f \neq 0$. We define the initial term of F with respect to the weight $(d, 1, \dots, 1)$ as the polynomial $in_d(F) := f$. Let $in_d(\mathcal{I}) \subset \mathbb{Q}[X]$ be the ideal generated by the set $\{in_d(F) : F \in \mathcal{I}\}$ and let $W \subset \mathbb{A}^n$ be the affine variety defined by $in_d(\mathcal{I})$.

Lemma 15 $W = V(X_1^d - \alpha_1, \dots, X_n^d - \alpha_n)$ and G_1, \dots, G_n form a standard basis.

PROOF.— Let us observe that the set $\{in_d(F) : F \in \mathcal{I}\}$ is contained in the set of initial terms (in the sense of Section 3) of the polynomials of the ideal (G_1, \dots, G_n) . Let $F \in (G_1, \dots, G_n)$, and let us write $F = \mathcal{E}^\alpha \tilde{F}(\mathcal{E}, X)$, with $\alpha \geq 0$ and $\tilde{F}(0, X) \neq 0$. Since \mathcal{E} is not a zero divisor of the \mathbb{Q} -algebra $\mathbb{Q}[\mathcal{E}, X]/(G_1, \dots, G_n)$, we conclude that $\tilde{F} \in (G_1, \dots, G_n)$ holds. Then

$$in_d(\tilde{F}) = \tilde{F}(0, X) \in (G_1(0, X), \dots, G_n(0, X)) = (X_1^d - \alpha_1, \dots, X_n^d - \alpha_n),$$

which implies that $in_d(\mathcal{I}) \subset (X_1^d - \alpha_1, \dots, X_n^d - \alpha_n)$ holds and G_1, \dots, G_n form a standard basis. On the other hand,

$$(X_1^d - \alpha_1, \dots, X_n^d - \alpha_n) = (in_d(F_1), \dots, in_d(F_n)) \subset in_d(\mathcal{I}),$$

from which the statement of Lemma 15 follows. ■

Since there are d^n branches of V lying above 0 and $\deg W = d^n$, we conclude that the system of (classical) Puiseux expansions of the branches of the curve V lying above 0 has regularity index 1, and the singular parts of its expansions are represented by the points of W .

Lemmas 14 and 15 show that the polynomials of (35) satisfy the hypotheses of Theorems 7 and 12. In order to apply the algorithm underlying Theorem 12 to our input system, we first need an explicit description of the set of singular parts of a system of rational Puiseux expansions of the branches of V lying above 0. For this purpose, we observe that the set of singular parts is given by

$$\{(T^d, \xi^{j_1} \alpha_1^{1/d} T, \dots, \xi^{j_n} \alpha_n^{1/d} T); 0 \leq j_1, \dots, j_n < d\} \subset \overline{\mathbb{Q}}[T]^{n+1},$$

where $\xi \in \overline{\mathbb{Q}}$ is a primitive d -th root of 1 and $\alpha_1^{1/d}, \dots, \alpha_n^{1/d} \in \overline{\mathbb{Q}}$ are d -th roots of $\alpha_1, \dots, \alpha_n$ respectively. Replacing T by $\alpha_1^{-1/d}T$ we obtain the following system of rational Puiseux expansions of the branches of V lying above 0:

$$\{(\alpha_1^{-1}T^d, T, \xi^{j_2}\beta_2^{1/d}T, \dots, \xi^{j_n}\beta_n^{1/d}T); 0 \leq j_2, \dots, j_n < d\} \subset \overline{\mathbb{Q}}[T]^{n+1},$$

where $\beta_2^{1/d}, \dots, \beta_n^{1/d} \in \overline{\mathbb{Q}}$ are d -th roots of $\beta_2 := \alpha_1^{-1}\alpha_2, \dots, \beta_n := \alpha_1^{-1}\alpha_n$ respectively. With the notations of Section 2.2, we have $g=1, e_1=d, f_1=d^{n-1}$.

Let Y_2, \dots, Y_n be new indeterminates over \mathbb{Q} . Let

$$W_0 := \{(\xi^{j_2}\beta_2^{1/d}, \dots, \xi^{j_n}\beta_n^{1/d}); 0 \leq j_2, \dots, j_n < d\} = V(Y_2^d - \beta_2, \dots, Y_n^d - \beta_n).$$

Then we see that a geometric solution of the variety W_0 yields the polynomials $q^{(1)}, f_2^{(1)}, \dots, f_n^{(1)}$ required for the application of the algorithm of Theorem 12.

Let $U := \gamma_2 Y_2 + \dots + \gamma_n Y_n$ be a linear form of $\mathbb{Q}[Y_2, \dots, Y_n]$ inducing a primitive element of the \mathbb{Q} -algebra extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[W_0]$. Let us fix $\rho \geq 2$. Using the Zippel–Schwartz test (see [59], [68]), we conclude that the coefficients of U can be randomly chosen in the set $\{1, \dots, 4\rho nd^{2n-2}\}$ with a probability of success of at least $1 - \frac{1}{2\rho} \geq \frac{3}{4}$.

We now describe an algorithm computing a geometric solution of W_0 . Let $m_2, \dots, m_n \in \mathbb{Q}[Z]$ be the sequence of polynomials defined recursively by:

$$m_2 := Z^d - \beta_2, \quad m_i := \text{Res}_{\tilde{Z}}(\gamma_i^{-d}(Z - \tilde{Z})^d - \beta_i, m_{i-1}(\tilde{Z})) \quad \text{for } 3 \leq i \leq n.$$

Then the polynomial m_n equals (up to scaling by a nonzero element of \mathbb{Q}) the minimal polynomial $q^{(1)} \in \mathbb{Q}[Z]$ of the coordinate function induced by U in the \mathbb{Q} -algebra extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[W]$. Combining fast algorithms for the computation of univariate resultants (see e.g. [46]) and univariate interpolation (see e.g. [9]) as in e.g. [33], we conclude that $q^{(1)}$ can be computed in space $O(d^{2n-2})$ and time $O^\sim(d^{2n-2})$. Combining this algorithm and the formulae of e.g. [2] or [56] as in the proof of Lemma 9, we obtain a geometric solution of W_0 with space $O(nd^{2n-2})$ and time $O^\sim(d^{2n-2})$. Finally, applying Theorem 12 we obtain the following result:

Theorem 16 *There exists a computation tree computing a geometric solution of the variety V with space $O(n\mathcal{S}d^{2n})$ and time $O^\sim(\mathcal{T}d^{2n})$.*

The geometric solution provided by Theorem 16 consists of a randomly chosen linear form $U \in \mathbb{Q}[X]$ and polynomials $m_u, v_1, \dots, v_n \in \mathbb{Q}[\mathcal{E}, Z]$. Suppose that the U is also a primitive element of the original variety $\{1\} \times \tilde{V} = V \cap (\{1\} \times \mathbb{A}^n)$. Specializing m_u, v_1, \dots, v_n into the value $\mathcal{E} = 1$, we obtain polynomials $m_u(1, Z), v_1(1, Z), \dots, v_n(1, Z)$ of $\mathbb{Q}[X]$ defining a (eventually non-reduced) Shape–Lemma–like representation of \tilde{V} . Therefore, computing a square-free

representation of $m_u(1, Z)$, and cleaning the multiple factors of the polynomial $m_u(1, Z)$ out of $v_1(1, Z), \dots, v_n(1, Z)$ we obtain a geometric solution of \tilde{V} with the same complexity estimate (see [33] for details).

This result improves the $O(3^n d^{2n})$ time-complexity estimate of [50]. Let us also mention the results of [51], where the authors announce an $O(d^{2n})$ time-complexity estimate for approximating one root of a Pham system. Comparing our result with the $O(\mathcal{T} d^{2n-1})$ time-complexity estimate provided by the application of the algorithm of [33] to this case, we see that the performance of [33] is better. Nevertheless, let us observe that the leading term d^{2n} of our time-complexity estimate can be expressed as $\delta \deg_{\mathcal{E}} m_u$ and we are dealing in this case with an “ill-conditioned” system, for which the worst case estimates $\delta = d^n$ and $\deg_{\mathcal{E}} m_u = d^n$ hold. If the input system satisfies $\deg_{\mathcal{E}} m_u \ll d^n$, then the performance of [33] does not change, whereas in our time-complexity estimate the d^{2n} factor reduces accordingly. Furthermore, if $\deg_{\mathcal{E}} m_u = 1$, we achieve the lower bound d^n of this factor (see [16]).

5.4 Reimer Systems

In this section we consider another family of examples called (generalized) Reimer systems (compare [8]). Let us fix $n \in \mathbb{N}$, and let us define $f_1, \dots, f_n \in \mathbb{Q}[X] := \mathbb{Q}[X_1, \dots, X_n]$ in the following way:

$$f_i := \alpha_i + \sum_{j=1}^n a_{i,j} X_j^{i+1}, \quad (36)$$

where $a_{i,j}, \alpha_i$ ($1 \leq i, j \leq n$) are *generic* elements of \mathbb{Q} (see Lemma 17 below) with $\alpha_i, a_{i,i} \neq 0$ for $1 \leq i \leq n$. Let \tilde{V} be affine subvariety of \mathbb{A}^n defined by f_1, \dots, f_n . Our purpose is to compute a geometric solution of \tilde{V} .

Our next result shows that \tilde{V} has dimension zero and degree $(n+1)!$.

Lemma 17 *Let $U := (U_{i,j})_{1 \leq i,j \leq n}$ be a matrix of indeterminates and let H_1, \dots, H_n be the elements of $\mathbb{Q}[U, X]$ defined in the following way:*

$$H_i := \alpha_i + \sum_{j=1}^n U_{i,j} X_j^{i+1}.$$

Then there exists a non-empty Zariski open set $\mathcal{U} \subset \mathbb{A}^{n^2}$ with the following property: for any $u \in \mathcal{U}$, the affine subvariety of \mathbb{A}^n defined by the polynomials $H_1(u, X), \dots, H_n(u, X)$ has dimension 0 and degree $(n+1)!$.

PROOF.— Let Z be the affine variety of \mathbb{A}^{n^2+n} defined by H_1, \dots, H_n and let $\pi_U : Z \rightarrow \mathbb{A}^{n^2}$ the morphism defined by $\pi(u, x) = u$. Let \wp be the prime

ideal of $\mathbb{Q}[U]$ generated by the set $\{U_{i,j}; 1 \leq i, j \leq n, i \neq j\}$. We claim that H_1, \dots, H_n form a regular sequence of $\mathbb{Q}[U]_{\wp}[X]$.

In order to prove this claim, following [38], we define a “triangular” sequence $(R_j^{(i)})_{1 \leq i \leq n, i+1 \leq j \leq n} \subset \mathbb{Q}[U, X]$ in the following way:

- $R_j^{(1)} := \text{Res}_{X_1}(H_1, H_j)$ for $j = 2, \dots, n$.
- $R_j^{(i)} := \text{Res}_{X_i}(R_i^{(i-1)}, R_j^{(i-1)})$ for $2 \leq i \leq n-1$ and $i+1 \leq j \leq n$.

From elementary properties of the resultant we see that $R_i^{(i-1)}$ is a nonzero element of $\mathbb{Q}[U, X_i, \dots, X_n] \cap (H_1, \dots, H_i)$, with $\deg_X R_i^{(i-1)} = \deg_{X_i} R_i^{(i-1)}$. Furthermore, a recursive argument shows that the coefficient of the highest power of X_i occurring in $R_i^{(i-1)}$ does not belong to the prime ideal \wp . We conclude that H_1, \dots, H_i define an ideal of $\mathbb{Q}[U]_{\wp}[X]$ of Krull dimension $n-i$. This implies that H_1, \dots, H_n form a regular sequence of $\mathbb{Q}[U]_{\wp}[X]$.

Furthermore, the polynomial $R_n^{(n-1)}$ gives an integral dependence equation for the coordinate class of X_n in the ring $\mathbb{Q}[U]_{\wp}[X_1, \dots, X_n]/(H_1, \dots, H_n)$ over the ring $\mathbb{Q}[U]_{\wp}$. Then a recursive argument with the polynomials $R_i^{(i-1)}$ for $1 \leq i \leq n$ shows that

$$\mathbb{Q}[U]_{\wp} \hookrightarrow \mathbb{Q}[U]_{\wp}[X_1, \dots, X_n]/(H_1, \dots, H_n) \quad (37)$$

is an integral \mathbb{Q} -algebra extension.

We conclude that there exists a Zariski neighborhood $\tilde{\mathcal{U}} \subset \mathbb{A}^{n^2}$ of $V(\wp)$ such that $\pi_U|_{Z \cap (\tilde{\mathcal{U}} \times \mathbb{A}^n)} : Z \cap (\tilde{\mathcal{U}} \times \mathbb{A}^n) \rightarrow \tilde{\mathcal{U}}$ is a finite morphism and $Z \cap (\tilde{\mathcal{U}} \times \mathbb{A}^n)$ is an equidimensional variety of dimension n^2 . This shows that for any choice of $u \in \tilde{\mathcal{U}}$ the variety $Z \cap \{U = u\} = \pi_U^{-1}(u)$ has dimension 0.

Now we show that the existence of the Zariski open set $\mathcal{U} \subset \tilde{\mathcal{U}}$ of the statement of the lemma. First, we observe that the Bézout inequality (see [36], [26]) implies $\deg(\pi_U^{-1}(u)) \leq d^n$ for any $u \in \tilde{\mathcal{U}}$. On the other hand, for any nonsingular diagonal matrix $u^{(0)} \in \tilde{\mathcal{U}}$ we have $\deg(\pi_U^{-1}(u^{(0)})) = (n+1)!$. We conclude that there exists a non-empty Zariski open set $\mathcal{U} \subset \tilde{\mathcal{U}}$ such that $\deg(\pi_U^{-1}(u)) = (n+1)!$ holds for any $u \in \mathcal{U}$. ■

Let us observe that for any $u \in \mathcal{U}$ we have that $\mathbb{C}[X]/(H_1(u, X), \dots, H_n(u, X))$ is a finite-dimensional \mathbb{C} -vector space of dimension at most $(n+1)!$. On the other hand, we have $\#(\pi_U^{-1}(u)) = (n+1)!$. We conclude that the polynomials $H_1(u, X), \dots, H_n(u, X)$ generate a radical zero-dimensional ideal of $\mathbb{C}[X]$, and hence the Jacobian determinant $J_H(u, X) := \det(\partial H_i / \partial X_j)_{1 \leq i, j \leq n}(u, X)$ does not vanish on any point x with $(u, x) \in \pi_U^{-1}(u)$. This implies that J_H does not vanish on any point of $Z \cap (\mathcal{U} \times \mathbb{A}^n)$.

In order to solve a system of the form (36) with $a := (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{U}$, let us introduce an indeterminate \mathcal{E} over \mathbb{Q} and the following elements of $\mathbb{Q}[\mathcal{E}, X]$:

$$F_i := \alpha_i \mathcal{E}^{i+1} + a_{i,i} X_i^{i+1} + \sum_{\substack{1 \leq j \leq n \\ j \neq i}} a_{i,j} \mathcal{E} X_j^{i+1} \quad (1 \leq i \leq n). \quad (38)$$

Let V the affine subvariety of \mathbb{A}^{n+1} defined by F_1, \dots, F_n and let $\pi : V \rightarrow \mathbb{A}^1$ be the morphism defined by $\pi(\varepsilon, x) := \varepsilon$. We have $\pi^{-1}(1) = \{1\} \times \tilde{V}$ and $\pi^{-1}(0) = \{0\} \subset \mathbb{A}^{n+1}$. We are going to show that F_1, \dots, F_n form a regular sequence of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and generate a radical ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$, and the morphism π is dominant and generically unramified.

For this purpose, let us define $G_1, \dots, G_n \in \mathbb{Q}[\mathcal{E}, X]$ in the following way:

$$G_i := \mathcal{E}^{-(i+1)} F_i(\mathcal{E}, \mathcal{E}X) = \alpha_i + \sum_{j=1}^n g_{i,j} X_j^{i+1},$$

where $g_{i,j} := a_{i,j} \mathcal{E}$ for $i \neq j$ and $g_{i,i} := a_{i,i}$. Let \tilde{W} be the affine subvariety of \mathbb{A}^{n+1} defined by G_1, \dots, G_n , and let $\tilde{\pi} : \tilde{W} \rightarrow \mathbb{A}^1$ be the morphism defined by $\tilde{\pi}(\varepsilon, x) = \varepsilon$. Observe that $g(1) \in \mathcal{U}$ holds, where $\mathcal{U} \subset \mathbb{A}^{n^2}$ is the Zariski open set of the statement of Lemma 17. Therefore, for a generic choice $\varepsilon \in \mathbb{A}^1$, we have $g(\varepsilon) \in \mathcal{U}$. Taking into account the remarks after the proof of Lemma 17, we conclude that $\tilde{\pi}$ is dominant and generically unramified.

Finally, since $\#(\tilde{\pi}^{-1}(\varepsilon)) = \#(\pi^{-1}(\varepsilon))$ holds for any $\varepsilon \neq 0$, we deduce the following result:

Lemma 18 *The morphism π is dominant and generically unramified.*

On the other hand, we have the following result:

Lemma 19 *F_1, \dots, F_n form a regular sequence in $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and generate a radical ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$.*

PROOF.— For $1 \leq i \leq n$, let $\hat{F}_i \in [\mathcal{E}, X_0, \dots, X_n]$ denote the homogenization of the polynomial F_i with respect to the variables X . We have $\hat{F}_i \equiv a_{i,i} X_i^{i+1} \pmod{(\mathcal{E})}$. Following [38], we define the following “triangular” sequence $(\hat{R}_j^{(i)})_{1 \leq i \leq n, i+1 \leq j \leq n}$ of $\mathbb{Q}[\mathcal{E}, X]$:

- $\hat{R}_j^{(1)} := \text{Res}_{X_1}(\hat{F}_1, \hat{F}_j)$ for $j = 2, \dots, n$.
- $\hat{R}_j^{(i)} := \text{Res}_{X_i}(\hat{R}_i^{(i-1)}, \hat{R}_j^{(i-1)})$ for $2 \leq i \leq n-1$ and $i+1 \leq j \leq n$.

From the elementary properties of the resultant we deduce that $\hat{R}_j^{(i)}$ is an homogeneous polynomial of $(\hat{F}_1, \dots, \hat{F}_j) \cap \mathbb{Q}[\mathcal{E}, X_0, X_{i+1}, \dots, X_n]$. Furthermore,

taking into account the congruence relation $\widehat{F}_i \equiv a_{i,i}X_i^{i+1} \pmod{(\mathcal{E})}$, a simple recursive argument shows that $\widehat{R}_i^{(i-1)} \equiv c_i X_i^{m_i} \pmod{(\mathcal{E})}$ holds for suitable $c_i \in \mathbb{Q} \setminus \{0\}$ and $m_i \in \mathbb{N}$. This shows that the coefficient of $X_i^{m_i}$ in $\widehat{R}_i^{(i-1)}$ does not belong to the prime ideal $(\mathcal{E}) \subset \mathbb{Q}[\mathcal{E}]$. Specializing the variable X_0 into the value $X_0 = 1$, with a similar argument as in the proof of Lemma 17 we conclude that F_1, \dots, F_n form a regular sequence of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ and

$$\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})} \hookrightarrow \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]/(F_1, \dots, F_n)$$

is an integral \mathbb{Q} -algebra extension.

Finally, since F_1, \dots, F_n form a regular sequence of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$, and the morphism π is generically unramified, applying [24, Theorem 18.15] as in Lemma 14 we conclude that the ideal generated by F_1, \dots, F_n in $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ is radical. ■

Let us observe that the origin $0 \in \mathbb{A}^{n+1}$ is the only point of $\pi^{-1}(0)$. Therefore, there are $\deg(\pi) = (n+1)!$ branches of V passing through $0 \in \mathbb{C}^{n+1}$.

For any $F \in \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$, let us write $F(\mathcal{E}, \mathcal{E}X) = \mathcal{E}^\alpha \widetilde{F}(\mathcal{E}, X)$ with $\widetilde{F} \in \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X] \setminus (\mathcal{E})\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$. We define the initial term of F with respect to the weight $(1, \dots, 1)$ as $in_1(F) := \widetilde{F}(0, X)$. Let \mathcal{I} be the ideal of $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$ generated by F_1, \dots, F_n , and let $in_1(\mathcal{I}) \subset \mathbb{Q}[X]$ be the ideal generated by the set $\{in_1(F) : F \in \mathcal{I}\}$. Let $W := V(in_1(\mathcal{I})) \subset \mathbb{A}^n$.

Lemma 20 $W = V(a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n)$ and G_1, \dots, G_n form a standard basis in $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$.

PROOF.— Let us observe that the set $\{in_1(F) : F \in \mathcal{I}\}$ is contained in the set of initial terms (in the sense of Section 3) of the polynomials of the ideal $(G_1, \dots, G_n) \subset \mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]$. Let $F \in (G_1, \dots, G_n)$ and write $F = \mathcal{E}^\alpha \widetilde{F}(\mathcal{E}, X)$, with $\alpha \geq 0$ and $\widetilde{F}(0, X) \neq 0$. Since \mathcal{E} is not a zero divisor of the \mathbb{Q} -algebra $\mathbb{Q}[\mathcal{E}]_{(\mathcal{E})}[X]/(G_1, \dots, G_n)$, we conclude that $\widetilde{F} \in (G_1, \dots, G_n)$ holds. Then

$$in_1(\widetilde{F}) = \widetilde{F}(0, X) \in (G_1(0, X), \dots, G_n(0, X)) = (a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n),$$

which implies that $in_1(\mathcal{I}) \subset (a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n)$ holds and G_1, \dots, G_n form a standard basis. On the other hand, we have the inclusion

$$(a_{1,1}X_1^2 - \alpha_1, \dots, a_{n,n}X_n^{n+1} - \alpha_n) = (in_1(F_1), \dots, in_1(F_n)) \subset in_1(\mathcal{I}),$$

from which the lemma follows. ■

Since there are $(n+1)!$ branches of V lying above 0 and $\deg W = (n+1)!$, we conclude that the system of (classical) Puiseux expansions of the branches of

the curve V lying above 0 has regularity index 1, and the singular parts of its expansions are represented by the points of W .

Lemmas 18, 19 and 20 show that the polynomials F_1, \dots, F_n of (38) satisfy all the hypotheses of Theorems 7 and 12 (see the remark right before Section 3.1). In order to apply the algorithm underlying Theorem 12 we need a description of the singular parts of the branches of V lying above 0. A similar argument as in Section 5.3 shows that, with the notations of Section 2.2, $g = 1$, $e_1 = 1$ and $f_1 = (n + 1)!$ in this case. Hence, we have that a geometric solution of the variety W yields the polynomials $q^{(1)}, f_1^{(1)}, \dots, f_n^{(1)}$ required for the application of Theorem 12. Such a geometric solution can be obtained in space $O(n(n + 1)!^2)$ and time $O((n + 1)!^2)$, using a similar algorithm to that of Section 5.3. Finally, applying Theorem 12 we obtain the following result:

Theorem 21 *There exists a straight-line program computing a geometric solution of the variety V with space $O(n(n + 1)!^2)$ and time $O((n + 1)!^2)$.*

In order to obtain a geometric solution of the variety $\{1\} \times \tilde{V} = \pi^{-1}(1)$ from the geometric solution of V provided by Theorem 21, we proceed in a similar way as in Section 5.3 (see the remarks after Theorem 16).

Acknowledgments: The authors wish to thank Joos Heintz for his helpful remarks. They are specially grateful to the anonymous referees for many suggestions which helped to significantly improve the presentation of the results of this paper. G. Matera and R. Wachenchauzer thank the Departamento de Computación, Universidad Favaloro, where they did part of this work.

References

- [1] E. Allgower, K. Georg, Numerical continuation methods: An Introduction, Springer Series in Comput. Mathematics 13, Heidelberg, 1990.
- [2] M. Alonso, E. Becker, M.-F. Roy, T. Wörmann, Zeroes, multiplicities and idempotents for zerodimensional systems, in: Proceedings of MEGA'94, Progress in Math. 142, Birkhäuser, Basel, 1996, pp. 1–15.
- [3] M. Alonso, G. Niesi, T. Mora, M. Raimondo, Local parametrizations of space curves at singular points, in: Computer Graphics and Mathematics, Springer Eurographic Seminar Series, Berlin Heidelberg New York, 1991, pp. 61–90.
- [4] M. Alonso, G. Niesi, T. Mora, M. Raimondo, An algorithm for computing analytic branches of space curves at singular points, in: Proceedings 1992 Int. Workshop on Math. Mechanization, Int. Academic Pub., 1992, pp. 135–166.
- [5] M. Artin, Lectures on deformation of singularities, Tata Inst. Fund. Res., 1976.

- [6] D. Bayer, D. Mumford, What can be computed in algebraic geometry? in: D. Eisenbud, L. Robbiano (Eds.), *Computational Algebraic Geometry and Commutative Algebra*, Symp. Math. XXXIV, Cambridge U. P., 1993, pp. 1–49.
- [7] T. Becker, V. Weispfenning, *Gröbner bases. A computational approach to commutative algebra*, Springer GTM 141, Berlin Heidelberg New York, 1993.
- [8] D. Bini, B. Mourrain, Polynomial test suite, <http://www-sop.inria.fr/saga>.
- [9] D. Bini, V. Pan, *Polynomial and matrix computations*, Birkhäuser, 1994.
- [10] L. Blum, F. Cucker, M. Shub, S. Smale, *Complexity and Real Computation*, Springer, New York Berlin Heidelberg, 1998.
- [11] A. Bompadre, Un problema de eliminación geométrica en sistemas de Pham–Brieskorn, Master’s thesis, Fac. Cs. Exactas y Nat., Univ. Buenos Aires, 2000.
- [12] A. Bompadre, G. Matera, R. Wachenchauzer, A. Weissbein, Lifting procedures for ramified fibers and polynomial equation solving, in: M. Frías, J. Heintz (Eds.), *Proc. Workshop Argentino de Informática Teórica, WAIT’01*, Buenos Aires, September 2001, vol. 30 *Anales JAIIO*, Buenos Aires, 2001, pp. 13–31.
- [13] J.F. Bonder, J. Rossi, Blow-up vs. spurious steady solutions, *Proceedings of the American Mathematical Society* 129 (1) (2001) 139–144.
- [14] A. Borodin, Time space tradeoffs (getting closer to the barriers?), in: 4th International Symposium on Algorithms and Computation, ISAAC ’93, Hong Kong, December 1993, Springer LNCS 762, pp. 209–220, 1993.
- [15] P. Bürgisser, M. Clausen, M. Shokrollahi, *Algebraic Complexity Theory*, Springer Grund. Math. Wiss. 315, Berlin Heidelberg New York, 1997.
- [16] D. Castro, M. Giusti, J. Heintz, G. Matera, L.M. Pardo, The hardness of polynomial equation solving, to appear in *Found. Comput. Mathematics*, 2003.
- [17] M. Chipot, M. Fila, P. Quittner, Stationary solutions, blow up and convergence to stationary solutions for semilinear parabolic equations with nonlinear boundary conditions, *Acta Math. Univ. Comenianae* 60 (1) (1991) 35–103.
- [18] A. Chistov, D. Grigoriev, Subexponential time solving systems of algebraic equations I, II, LOMI preprints E-9-83, E-10-83, Steklov Inst., Leningrad, 1983.
- [19] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms: An introduction to computational algebraic geometry and commutative algebra*, Springer UTM, Berlin Heidelberg New York, 1992.
- [20] D. Cox, J. Little, D. O’Shea, *Using algebraic geometry*, Springer GTM 185, Berlin Heidelberg New York, 1998.
- [21] D. Cox, B. Sturmfels, *Applications of computational algebraic geometry*, vol. 53 *Proc. Symp. Applied Math.*, AMS, Providence, Rhode Island, 1998.
- [22] V. Danilov, Algebraic varieties and schemes, in: I. Shafarevich (Ed.), *Algebraic geometry I*, vol. 23 of *Enc. Math. Sciences*, Springer, 1994, pp. 167–297.

- [23] D. Duval, Rational Puiseux expansions, *Compositio Math.* 70 (1989) 119–154.
- [24] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer GTM 150, Berlin Heidelberg New York, 1995.
- [25] R. Ferreira, P. Groisman, J. Rossi, Numerical blow-up for a nonlinear problem with a nonlinear boundary condition, *Mathematical models and methods in applied sciences* 12 (4) (2002) 461–484.
- [26] W. Fulton, *Intersection Theory*, Springer, Berlin Heidelberg New York, 1984.
- [27] P. Gianni, T. Mora, Algebraic solution of systems of polynomial equations using Gröbner bases, in: L. Huguet, A. Poli (Eds.), *Proc. AAEECC-5*, Menorca, Spain, June 1987, Springer LNCS 356, 1989, pp. 247–257.
- [28] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, L.M. Pardo, Lower bounds for Diophantine approximation, *J. Pure Appl. Algebra* 117,118 (1997) 277–317.
- [29] M. Giusti, J. Heintz, La détermination des points isolés et de la dimension d’une variété algébrique peut se faire en temps polynomial, in: D. Eisenbud, L. Robbiano (Eds.), *Computational Algebraic Geometry and Commutative Algebra*, *Symp. Mat. XXXIV*, Cambridge Univ. Press, 1993, pp. 216–256.
- [30] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight-line programs in geometric elimination theory, *J. Pure Appl. Algebra* 124 (1998) 101–146.
- [31] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo, When polynomial equation systems can be solved fast?, in: G. Cohen, M. Giusti, T. Mora (Eds.), *Proc. AAEECC-11*, Springer LNCS 948, 1995, pp. 205–231.
- [32] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo, Le rôle des structures de données dans les problèmes d’élimination, *C. R. Acad. Sci. Paris* 325 (1997) 1223–1228.
- [33] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, *J. Complexity* 17 (1) (2001) 154–211.
- [34] M. Gonzalez-Lopez, L. Gonzalez-Vega, Newton identities in the multivariate case: Pham systems, in: B. Buchberger et al. (Eds.), *Gröbner bases and applications*, London Math. SLNS 251, Cambridge U. Press, 1998, pp. 351–366.
- [35] L. Gonzalez-Vega, A special quantifier elimination algorithm for Pham systems, in: C. Detzell et al. (Eds.), *Real algebraic geometry and ordered structures*, vol. 253 of *Contemporary Mathematics*, AMS, Providence, RI, 1998, pp. 115–366.
- [36] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, *Theoretical Computer Science* 24 (3) (1983) 239–277.
- [37] J. Heintz, On the computational complexity of polynomials and bilinear mappings. A survey, in: L. Huguet, A. Poli (Eds.), *Proc. AAEECC-5*, Menorca, Spain, June 1987, Springer LNCS 356, 1989, pp. 269–300.

- [38] J. Heintz, G. Jerónimo, J. Sabia, J. San Martín, P. Solernó, On the multihomogeneous Bézout theorem, manuscript Univ. Buenos Aires, 2002.
- [39] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving, *J. Complexity* 16 (1) (2000) 70–109.
- [40] J. Heintz, G. Matera, A. Waissbein, On the time–space complexity of geometric elimination procedures, *Appl. Alg. Eng. Comm. Comp.* 11 (4) (2001) 239–296.
- [41] D. Henry, *Geometric theory of semilinear parabolic equations*, Springer LNM 840, Berlin Heidelberg, 1981.
- [42] B. Huber, B. Sturmfels, A polyhedral method for solving sparse polynomial systems, *Mathematics of Computation* 64 (112) (1995) 1541–1555.
- [43] T. Krick, L.M. Pardo, A computational method for Diophantine approximation, in: L. González-Vega, T. Recio (Eds.), *Algorithms in Algebraic Geometry and Applications*, Progress in Math. 143, Birkhäuser, Basel, 1996, pp. 193–254.
- [44] L. Kronecker, Grundzüge einer arithmetischen Theorie de algebraischen Grössen, *J. reine angew. Math.* 92 (1882) 1–122.
- [45] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston, 1985.
- [46] T. Lickteig, M.-F. Roy, Cauchy index computation, *Calcolo* 33 (1997) 337–351.
- [47] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press, 1916.
- [48] H. Matsumura, *Commutative Ring Theory*, Cambridge Univ. Press, 1986.
- [49] T. Mora, G. Pfister, C. Traverso, An introduction to the tangent cone algorithm, in: C. Hoffmann (Ed.), *Issues in robotics and non-linear geometry*, vol. 6 of *Adv. in Computing Research*, JAI Press, Greenwich Conn., 1992, pp. 199–270.
- [50] B. Mourrain, V. Pan, Solving special polynomial systems by using structural matrices and algebraic residues, in: F. Cucker, M. Shub (Eds.), *Proc. FOCM'97*, Springer, Berlin Heidelberg New York, 1997, pp. 287–304.
- [51] B. Mourrain, V. Pan, Multivariate polynomials, duality and structured matrices, *J. Complexity* 16 (1) (2000) 110–180.
- [52] L.M. Pardo, How lower and upper complexity bounds meet in elimination theory, in: G. Cohen, M. Giusti, T. Mora (Eds.), *Proc. AAEECC–11*, Springer LNCS 948, Berlin Heidelberg New York, 1995, pp. 33–69.
- [53] L.M. Pardo, J. San Martín, Deformation techniques to solve generalized Pham systems, manuscript Universidad de Cantabria, 2002.
- [54] J. Renegar, On the computational complexity and geometry of the first order theory of the reals I, II, III, *J. Symb. Comput.* 13 (3) (1992) 255–352.
- [55] W. Rheinboldt, *Methods for solving systems of nonlinear equations*, vol. 70 of *CBMS–NSF Regional Conf. Series in Appl. Math.*, SIAM, Philadelphia, 1998.

- [56] F. Rouillier, Solving zero-dimensional systems through rational univariate representation, *Appl. Alg. Eng. Comm. Comp.* 9 (5) (1997) 433–461.
- [57] J. Savage, *Models of Computation. Exploring the Power of Computing*, Addison Wesley, Reading, Massachusetts, 1998.
- [58] E. Schost, Computing parametric geometric resolutions, *Appl. Alg. Eng. Comm. Comp.* 13 (2003) 349–393.
- [59] J. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, *Journal of the ACM* 27 (4) (1980) 701–717.
- [60] I. Shafarevich, *Basic Algebraic Geometry: Varieties in Projective Space*, Springer, Berlin Heidelberg New York, 1994.
- [61] V. Strassen, Algebraic complexity theory, In: van Leeuwen, J. (Ed.), *Handbook of Theor. Computer Science*, Ch. 11, Elsevier, Amsterdam, 1990, pp. 634–671.
- [62] B. Sturmfels, *Solving Systems of Polynomial Equations*, CBMS Regional Conference Series in Mathematics, AMS, Providence, RI. 2002.
- [63] J. von zur Gathen, Parallel arithmetic computations: A survey, in: B.R.J. Gruska, J. Wiedermann (Eds.), *Proc. 12th Symp. MFCS*, Bratislava, Czechoslovakia, 1986, Springer LNCS 233, 1986, pp. 93–112.
- [64] R. Walker, *Algebraic Curves*, Dover Publications Inc., New York, 1950.
- [65] P. Walsh, On the complexity of rational Puiseux expansions, *Pacific Journal of Mathematics* 188 (2) (1999) 369–387.
- [66] P. Walsh, A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function, *Math. Comp.* 69 (231) (2000) 1167–1182.
- [67] O. Zariski, *Algebraic surfaces*, Springer, Berlin Heidelberg New York, 1995.
- [68] R. Zippel, Probabilistic algorithms for sparse polynomials, in: *Proc. EUROSAM'79*, Marseille 1979, Springer LNCS 72, 1979, pp. 216–226.