January 2018

On the Extended Hensel Construction and its Application to the Computation of Real Limit Points

Masoud Ataei Jaliseh
The University of Western Ontario

Supervisor
Marc Moreno Maza
The University of Western Ontario

Graduate Program in Computer Science

A thesis submitted in partial fulfillment of the requirements for the degree in Master of Science

Abstract

The Extended Hensel Construction (EHC) is a procedure which, for an input bivariate polynomial with complex coefficients, can serve the same purpose as the Newton-Puiseux algorithm. We show that the EHC requires only linear algebra and univariate polynomial arithmetic. We deduce complexity estimates and report on a software implementation together with experimental results. This work is motivated and illustrated by two applications. The first one is the computation of real branches of space curves. The second one is the computation of limits of real multivariate rational function. For the latter, we present an algorithm for determining the existence of the limit of a real multivariate rational function q at a given point p which is an isolated zero of the denominator of q. When the limit exists, the algorithm computes it, without making any assumptions on the number of variables.

Keywords: Computer Algebra, Extended Hensel Construction, Limits of multivariate rational functions.

Co-Authorship Statement

This thesis gathers results from a publication co-authored with Parisa Alvandi and Marc Moreno Maza, and a preprint co-authored with Parisa Alvandi, Mahsa Kazemi and Marc Moreno Maza. The latter (see Chapters 6 and 8) extends a paper published by my three colleagues in the proceedings of ISSAC 2016. The former (see Chapters 2, 3, 4, 5 and 8) is a follow-up paper in the proceedings of ISSAC 2017.

Acknowledgements

I would like to thank my supervisor Professor Marc Moreno Maza for the opportunity to pursue this research and for many interesting and valuable discussions in completion of this work. I am also very grateful to my colleagues and friends, including Dr. Parisa Alvandi, Dr Mahsa Kazemi, Dr. Armin Jamshidpey and Dr. Robert Moir for their great help with the exposition in this thesis and all members of ORCCA lab for creating a friendly working environment.

Also, I would like to thank Western University and the department of Computer Science for providing financial support in completion of my Master degree. I would also like to thank Ms. Janice Wiersma for her kind help with various administrative tasks related to my graduate studies at Western.

I would like to thank my examiners, Professors Lucian Ilie, Rob Corless, David Jeffrey and Robert Webber, for accepting to be in my thesis examination committee.

And last but not least, I would like to thank my wife Mahshad and my parents for their support and patience during my studies.

Contents

Introduction

The *Extended Hensel Construction* (EHC) is an algorithm which is used for factorizing univariate polynomials with power series coefficients. It was proposed in [SK99] by T. Sasaki and F. Kako. Their goal was to provide a practically more efficient alternative to the classical Newton-Puiseux method for univariate power series coefficients. In the same paper, Sasaki and Kako proposed an extension of the EHC to power series coefficients in more than one variable. Figure 0.1 illustrates our implementation of the EHC in the PowerSeries library, available at `www.regularchains.org`.

```
> alias(T = RootOf(_Z^2 + y)):
> P := PowerSeries([y, z]):
  U := UnivariatePolynomialOverPowerSeries([y, z], x):
  poly := y*x^3 + (-2*y + z + 1)*x + y:
  U:-ExtendedHenselConstruction(poly, [0, 0], 3);
```

$$\left[\left[x = \frac{-T + T\,y - \frac{1}{2}\,T\,z + \frac{1}{2}\,y^2}{y}\right], \left[x = \frac{T - T\,y + \frac{1}{2}\,T\,z + \frac{1}{2}\,y^2}{y}\right], [x = -y]\right]$$

Figure 0.1: EHC applied to a trivariate polynomial.

The work of Sasaki and Kako was further extended by their students, see the papers [IS07, SI16,Iwa03,Ina05,SY98]. See also the works of S. Abhyankar [Abh89] and T.-C. Kuo [Kuo89]. The EHC relies on the so-called *Yun-Moses polynomials* originally introduced in [MY73], studied in [Tsu09], and called *Lagrange interpolation polynomials* in [SK99]. The definition of those polynomials suggests to compute them by applying the Extended Euclidean Algorithm (EEA) over a field of multivariate rational functions. In practice, this is a computational bottleneck. In [SI16], Sasaki and D. Inaba suggest to use Gröbner bases instead and report on favourable experimental results.

In this paper, we propose a new method for computing the Yun-Moses polynomials using Wronskian matrices. For an input bivariate polynomial $F(X, Y)$ with coefficients in a field $\mathbb{K}$ and total degree d, we show that the Yun-Moses polynomials (needed when applying the EHC to $F(X, Y)$) can be computed within $O(d^3\,\mathrm{M}(d))$ operations in $\mathbb{K}$, where $n \longmapsto \mathrm{M}(n)$ is a (polynomial) multiplication time [GG03]. In addition, we exhibit a new strategy for performing the lifting steps so that the k-th lifting step of the EHC applied to $F(X, Y)$ can be computed within $O(k\,d\,\mathrm{M}(d)^2)$ operations in $\mathbb{K}$ (instead of $O(k^2\,d\,\mathrm{M}(d)^2)$ in a direct approach) or within $O(k\,d\,\mathrm{M}(d))$ operations in the algebraic closure of $\mathbb{K}$. These enhancements of the EHC are described in Chapters 3 to 4, and supported by the experimentation reported in Chapter 8.

In [KT78], H.T. Kung and J.F. Traub present a complexity analysis for the Newton-Puiseux method over the field $\mathbb{C}$ of complex numbers. They show that the first k iterations of Newton-Puiseux on an input bivariate polynomial of degree d requires $O(d\,k\,\mathrm{M}(k))$ operations in $\mathbb{C}$ using a *linear lifting scheme* (Theorem 5.2 in [KT78]) and $O(d\,\mathrm{M}(k))$ operations in $\mathbb{C}$ using a

quadratic lifting scheme (Corollary 5.1 in [KT78]). This latter estimate is improved in [CC86] by D. V. Chudnovsky and G. V. Chudnovsky, yielding $O(d\,k)$ operations in $\mathbb{C}$. When the base field $\mathbb{K}$ is finite, state of the art algorithms are presented by A. Poteaux and M. Rybowicz in [PR15].

In both [KT78] and [CC86], the estimated cost is for computing a *single branch*. Thus, for computing all branches, the costs of the linear and quadratic lifting schemes of [KT78] become respectively $O(d^2\,k\,\mathrm{M}(k))$ and $O(d^2\,\mathrm{M}(k))$ operations in $\mathbb{C}$. The EHC currently uses a linear lifting scheme and, with the enhancements proposed in this paper, it computes all the branches, for the first k operations, within $O(k^2\,d\,\mathrm{M}(d))$ operations in $\mathbb{C}$. The experimentation reported in Chapter 8 show that, for problems of practical interest, an EHC implementation can outperform counterparts based on the linear and quadratic lifting schemes of [KT78]. Since we implemented both Kung and Traub's algorithm and our enhanced EHC, let us go further in comparing their algebraic complexity. All the above mentioned algorithms need to factor a univariate polynomial over $\mathbb{C}$. This is the Newton polynomial of $F(X, Y)$ in the case of the EHC and the polynomial $F(X, 0)$ for the algorithm of Kung and Traub. If both polynomials split into linear factors over $\mathbb{K}$, where $\mathbb{K}$ is $\mathbb{Q}$ or an algebraic extension of $\mathbb{Q}$, and putting aside the cost of factoring those polynomials (which can be regarded as similar), the total cost, counting operations in $\mathbb{C}$, of factoring $F(X, Y)$ into linear factors in X over $\mathbb{C}(\langle Y^* \rangle)$, computing k terms in each branch, is $O(d^3\mathrm{M}(d) + k^2\,d\,\mathrm{M}(d))$ for the EHC and $O(d^2\,k\,\mathrm{M}(k))$ (resp. $O(d^2\,\mathrm{M}(k))$) the algorithm of Kung and Traub using a linear (resp. quadratic) lifting scheme.

In practice, the EHC has the advantage that its computation flow has a simpler structure and offers opportunities for efficient implementation. This observation is based on our experience with both approaches through a series of papers [ACM13, AMSV15, AKM16]. Indeed, in addition to polynomial factorization, the EHC can be applied to the computation of limits of multivariate rational functions [AKM16] and tangent cones [AMSV15]. Both types of computation rely on the computation of real limit points, which are discussed in Chapter 5. With respect to our ISSAC 2017 article [AAM17] this latter Chapter is substantially expanded and provides proofs and detailed algorithms.

In [ACM13], an algorithm is proposed for computing the non-trivial limit points of the quasi-component $W(T)$ of a regular chain $T \subset \mathbb{Q}[X_1, \ldots, X_n]$. Those points form the set $\overline{W(T)} \setminus W(T)$, where $\overline{W(T)}$ is the Zariski closure of $W(T)$.

In Chapter 5, we use the EHC for computing the non-trivial limit points of the *real* quasi-component of T. To be precise, letting $W_{\mathbb{R}}(T) := Z_{\mathbb{R}}(T) \setminus Z_{\mathbb{R}}(h_T)$, we are interested in the set $\overline{W_{\mathbb{R}}(T)} \setminus W_{\mathbb{R}}(T)$, where $\overline{W_{\mathbb{R}}(T)}$ is the closure of $W_{\mathbb{R}}(T)$ in $\mathbb{R}^n$ endowed with the Euclidean topology. Unfortunately, it is not true that the non-trivial limit points of $W_{\mathbb{R}}(T)$ are the non-trivial limit points of $W(T)$ with real coordinates. Figure 0.2 yields a counter-example, which illustrates how the factorization produced by the EHC helps computing the limit points of both $W(T)$ (complex case) and $W_{\mathbb{R}}(T)$ (real case).

As mentioned above, computing the non-trivial limit points of real quasi-components can be used to determine tangent cones and limits of multivariate rational functions. We dedicate Chapters 6 and 7 to this latter question, extending the work initiated in the ISSAC 2016 article [AKM16].

Prior to our work, two papers had revitalized the search for such general procedures determining the limits, when they exist, of real multivariate rational functions. In [XZ14] S.J. Xiao and G.X. Zeng propose a first algorithm that, given a multivariate rational function

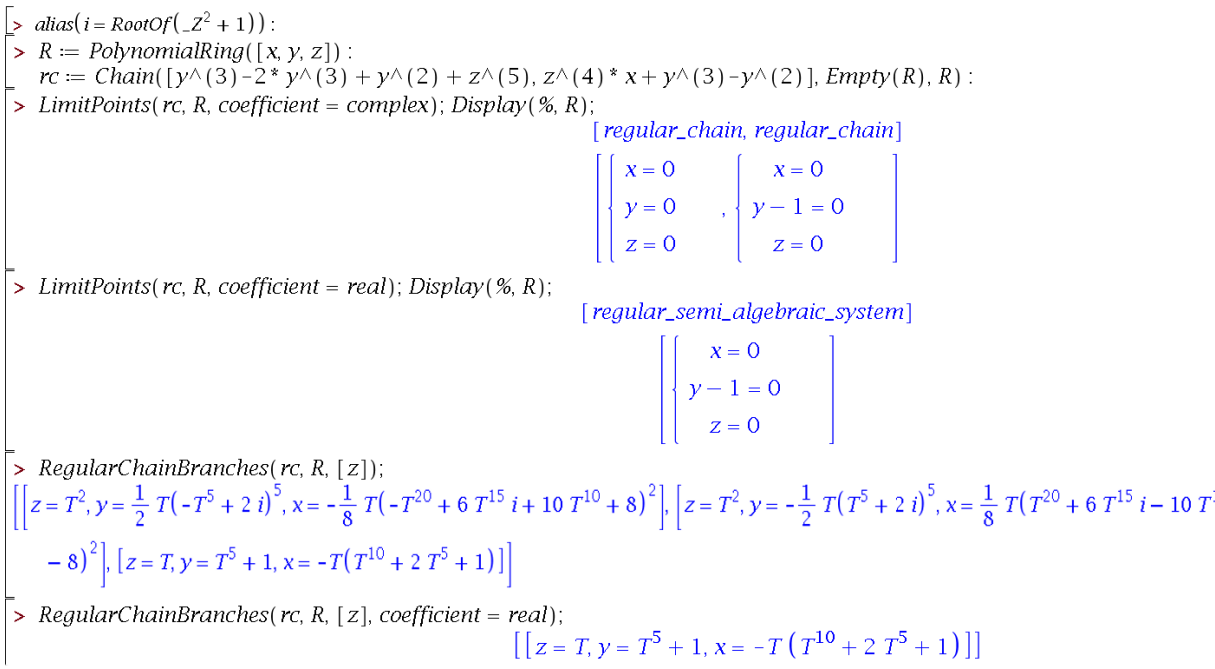

Figure 0.2: Computational of limit points: complex and real cases.

$q \in \mathbb{Q}(X_1, \ldots, X_n)$, decides whether $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q$ is zero or not. The "not-case" includes the situation where $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q$ does not exist as well as the case where it exists but it is not zero. Their algorithm is based on the observation that the posed question can be phrased as a quantifier elimination problem, that the authors solve using triangular decomposition of algebraic systems, rational univariate representation as well as adjoining infinitesimal elements to the base field. A second algorithm reduces the question of deciding whether $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q$ exists or not (and computing it, when it exists) to calling the first algorithm.

In [CMV13], C. Cadavid, S. Molina and J.D. Vélez propose an algorithm, now available in MAPLE as the `limit/multi` command, for determining the existence and possible value of limits of the form $\lim_{(x,y)\to(0,0)} q$, where q is a bivariate rational function, and such that $(0, 0)$ is an isolated zero of the real algebraic set defined by the denominator of q. In a follow-up preprint [VHC17], J.D. Vélez, P. Hernández and C. Cadavid extend the method of [CMV13] to rational functions in three variables, still assuming that the origin is an isolated zero of the denominator. Both papers [CMV13] and [VHC17] rely on the key observation that, for determining the existence and possible value of limits of the form $\lim_{(x,y)\to(0,0)} q$ and $\lim_{(x,y,z)\to(0,0,0)} q$, it is sufficient to study *limits along a real algebraic set* $\chi(q)$, that is, limits of the form $\lim_{(x,y)\to(0,0),(x,y)\in\chi(q)} q$ and $\lim_{(x,y,z)\to(0,0,0),(x,y,z)\in\chi(q)} q$. This latter notion is defined in Chapter 6 of the present thesis. In the three-variable case, the method of [VHC17] requires to compute the singular locus of $\chi(q)$ and the irreducible components of the algebraic set over $\mathbb{C}$ associated with $\chi(q)$.

The method of S.J. Xiao and G.X. Zeng [XZ14] has the advantage of not making any assumptions on the number of variables nor the zero set of the denominator. Meanwhile, the

works of C. Cadavid, S. Molina, J.D. Vélez and P. Hernández avoid the use of infinitesimal elements and rely on a deeper geometrical insight, through a notion of *discriminant variety*, see Notation 2. Unfortunately, the recourse to singular loci and irreducible decomposition is a limitation in view of an implementation.

In Chapter 7, we propose an algorithm for determining the existence and possible value of $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q$, for an arbitrary number n of variables. As in [CMV13] and [VHC17], we assume that the origin is an isolated zero of the denominator of the rational function q. However, we avoid the computation of singular loci and decompositions into irreducible components of the real and complex algebraic sets involved in the method of [VHC17]. Instead, we take advantage of the theory of regular chains and the RealTriangularize algorithm [CDM$^+$13b, CDM$^+$13a] for decomposing semi-algebraic systems. The experimental results reported in Chapter 8 suggest that our algorithm can solve more problems than the algorithm of S.J. Xiao and G.X. Zeng, in particular when the number n of variables increases.

Broadly speaking, Lemma 9 says the following. Consider a regular semi-algebraic system $R := [Q, T, P_>]$ in $\mathbb{R}^n$ (see Definition 1) where T is a regular chain such that the origin $\underline{o}$ of $\mathbb{R}^n$ is in the closure (w.r.t. Euclidean topology) of the zero set $Z_\mathbb{R}(R)$ of R in $\mathbb{R}^n$. Let d be the dimension of $Z_\mathbb{R}(R)$ with $1 \leq d < n$. Let $\mathcal{M}$ be the $(n - d + 1) \times n$ matrix whose first row is the vector $(X_1, \ldots, X_n)$ and the other rows are the gradients ∇t_j, for $j = d + 1, \ldots, n$, with $T = \{t_{d+1}, \ldots, t_n\}$. Then, there exists a non-empty set $O \subset D^*_\rho \cap Z_\mathbb{R}(S)$, which is open relatively to $Z_\mathbb{R}(S)$ and which satisfies $\underline{o} \in \overline{O}$ (that is, the origin is in the closure of O) such that $\mathcal{M}$ is full rank at any point of O. To be even broader, this result says that there exists $r > 0$ such that the intersection of $D^*_r \cap Z_\mathbb{R}(S)$ (where D^*_r is the punctured ball of radius r and centered at the origin) and any sphere (or ellipsoid) centered at the origin is either empty or has dimension less than d. This result allows us to take advantage if the method of Lagrange multipliers.

Chapter 1

Preliminaries

The algorithms in Chapter 7 rely essentially on the technique of Lagrange multipliers, see Section 1.1. The applicability of this technique is based on theoretical results gathered in Chapter 6 The key arguments come from the theories of regular chain, see Section 1.2, topology, see Section 1.3, parametric polynomial systems, see Section 1.4, and regular semi-algebraic systems, see Section 1.5. We also recall the notion of Puiseux series in Section 1.6 and refer to the book of G. Fischer [Fis01] for details.

1.1 Lagrange multipliers

The following review is based on [Vap]. Let n, m be positive integers. Let Ω be an open set of $\mathbb{R}^n$, let $f, g_1, \ldots, g_m : \Omega \to \mathbb{R}$ be C^1 functions, let $b = (b_1, \ldots, b_m) \in \mathbb{R}^m$ and let x^* be a point of Ω. Define $\Sigma_b := \{y \in \mathbb{R}^n \ : \ g_1(y) = b_1, \ldots, g_m(y) = b_m\}$. The point $x^\star$ is called a *local conditional extremal point of f under the constraints $g_1 = b_1, \ldots, g_m = b_m$*, whenever there exists a neighbourhood U of $x^\star$ such that $f(x)$ takes an extremal value (maximum or minimum) at $x = x^*$ on $\Sigma_b \cap U$. When this holds, the gradients $\nabla f(x^\star), \nabla g_1(x^\star), \ldots, \nabla g_m(x^\star)$ are linearly dependent. The above theorem is, in fact, usually stated when $m < n$ holds and $\nabla g_1(x^\star), \ldots, \nabla g_m(x^\star)$ are linearly independent, i.e. when $g(x^\star)$ is a regular value of the function $g = (g_1, \ldots, g_m)$ (at least if we restrict g to some neighbourhood V of $x^\star$). Then, the necessary condition of the theorem can be translated into the identity

$$\nabla f(x^\star) = \lambda_1^\star \nabla g_1(x^\star) + \ldots + \lambda_m^\star \nabla g_m(x^\star), \tag{1.1}$$

for some real numbers $\lambda_1^\star, \ldots, \lambda_m^\star$ called *Lagrange multipliers*. Observe that, if we define the *Lagrange function*

$$F(x, \lambda) = f(x) + \sum_{i=1}^{m} \lambda_i (b_i - g_i(x)), \tag{1.2}$$

then the conditions (1.1) and $x^\star \in \Sigma_b$, for some neighbourhood U of $x^\star$ are equivalent to the fact that $(x^\star, \lambda^\star)$ is a critical point of F.

1.2 Regular chain theory

This section is a brief summary of concepts and algorithms for which details can be found in [CM12]. Throughout this paper, $\mathbb{K}$ is a field of characteristic 0 and $\overline{\mathbb{K}}$ is its algebraic closure. We say that $\mathbb{K}$ is an *algebraic number field* if it is a finite degree field extension of the field $\mathbb{Q}$ of rational numbers. Here degree refers to the dimension of $\mathbb{K}$ as a vector space over $\mathbb{Q}$. Let $\mathbb{K}[\underline{X}]$ be the polynomial ring over $\mathbb{K}$ and with ordered variables $\underline{X} = X_1 < \cdots < X_n$. Let $p \in \mathbb{K}[\underline{X}]$. Assume that $p \notin \mathbb{K}$. Denote by $\mathrm{mvar}(p)$, $\mathrm{init}(p)$, and $\mathrm{mdeg}(p)$ respectively the greatest variable appearing in p (called the *main variable* of p), the leading coefficient of p w.r.t. $\mathrm{mvar}(p)$ (called the *initial* of p), and the degree of p w.r.t. $\mathrm{mvar}(p)$ (called the *main degree* of p); denote by $\mathrm{discrim}(p)$ the discriminant of p w.r.t. $\mathrm{mvar}(p)$. For $F \subset \mathbb{K}[\underline{X}]$, we denote by $\langle F \rangle$ and $V(F)$ the ideal generated by F in $\mathbb{K}[\underline{X}]$ and the algebraic set of $\overline{\mathbb{K}}^n$ consisting of the common roots of the polynomials of F.

Triangular set. Let $T \subset \mathbb{K}[\underline{X}]$ be a *triangular set*, that is, a set of non-constant polynomials with pairwise distinct main variables. Denote by $\mathrm{mvar}(T)$ the set of main variables of the polynomials in T. A variable $v \in \underline{X}$ is called *algebraic* w.r.t. T if $v \in \mathrm{mvar}(T)$, otherwise it is said *free* w.r.t. T. If no confusion is possible, we shall always denote by $\underline{U} = U_1, \ldots, U_d$ and $\underline{Y} = Y_1, \ldots, Y_m$ the free variables and the main variables of T, respectively. We let $d = 0$ whenever T has no free variables. For $v \in \mathrm{mvar}(T)$, we denote by T_v and T_v^- the polynomial $f \in T$ with $\mathrm{mvar}(f) = v$ and the polynomials $f \in T$ with $\mathrm{mvar}(f) < v$, respectively. Let h_T be the product of the initials of the polynomials in T. We denote by $\mathrm{sat}(T)$ the *saturated ideal* of T: if T is the empty triangular set, then $\mathrm{sat}(T)$ is defined as the trivial ideal $\langle 0 \rangle$, otherwise it is the ideal $\langle T \rangle : h_T^\infty$. The *quasi-component* $W(T)$ of T is defined as $V(T) \setminus V(h_T)$. The Zariski closure of $W(T)$ in $\overline{\mathbb{K}}^n$, denoted by $\overline{W(T)}$, is the intersection of all algebraic sets $V \subseteq \overline{\mathbb{K}}^n$ such that $W(T) \subseteq V$ holds; moreover we have $\overline{W(T)} = V(\mathrm{sat}(T))$. For $f \in \mathbb{K}[\underline{X}]$, we denote by $\mathrm{res}(f, T)$ the *iterated resultant* of f w.r.t. T, that is, f itself, if f is constant, or $\mathrm{res}(\mathrm{res}(f, T_v, v), T_v^-)$ if $v \in \mathrm{mvar}(T)$ and $v = \mathrm{mvar}(f)$ hold, or $\mathrm{res}(f, T_v^-)$ otherwise.

Regular chain. A triangular set $T \subset \mathbb{K}[\underline{X}]$ is a *regular chain* if either T is empty, or letting v be the largest variable occurring in T, the set T_v^- is a regular chain, and the initial of T_v is regular (that is, neither zero nor zero divisor) modulo $\mathrm{sat}(T_v^-)$. Let $H \subset \mathbb{K}[\underline{X}]$. The pair $[T, H]$ is a *regular system* if each polynomial in H is regular modulo $\mathrm{sat}(T)$. If H consists of a single polynomial h, then we also write $[T, h]$, for short, instead of $[T, H]$. The *dimension* of T is the dimension of its saturated ideal. A regular chain T, or a regular system $[T, H]$, is *square-free* if for all $t \in T$, the polynomial $\mathrm{der}(t)$ is regular w.r.t. $\mathrm{sat}(T)$, where $\mathrm{der}(t) = \frac{\partial t}{\partial v}$ and $v = \mathrm{mvar}(t)$. By $[T, H_{\neq}]$, we denote the algebraic system consisting of the equations $f = 0$ for all $f \in T$ and the inequations $h \neq 0$ for $h \in H \cup \{h_T\}$.

Triangular decomposition. Let $F \subset \mathbb{K}[\underline{X}]$. Regular chains $T_1, \ldots, T_e$ of $\mathbb{K}[\underline{X}]$ form a *triangular decomposition* of $V(F)$ in the sense of Kalkbrener (resp. Wu and Lazard) whenever we have $V(F) = \cup_{i=1}^e \overline{W(T_i)}$ (resp. $V(F) = \cup_{i=1}^e W(T_i)$). We denote by $\mathrm{Triangularize}$ an algorithm, such as the one of [CM12], computing a Kalkbrener triangular decomposition.

Regularization. Let $p \in \mathbb{K}[\underline{X}]$ and $T \subset \mathbb{K}[\underline{X}]$ be a regular chain. The function call $\mathrm{Regularize}(p, T)$ computes a set of regular chains $\{T_1, \ldots, T_e\}$ such that: (1) for each $i = 1, \ldots, e$, either $p \in \mathrm{sat}(T_i)$ holds or p is regular w.r.t. $\mathrm{sat}(T_i)$; (2) we have $\overline{W(T)} = \overline{W(T_1)} \cup \cdots \cup \overline{W(T_e)}$, and $\mathrm{mvar}(T) = \mathrm{mvar}(T_i)$ holds for each $i = 1, \ldots, e$.

Good specialization. Let $[T, H]$ be a square-free regular system of $\mathbb{K}[\underline{X}]$. Recall that $\underline{Y}$ and $\underline{U} = U_1, \ldots, U_d$ stand respectively for $\mathrm{mvar}(T)$ and $\underline{X} \setminus \underline{Y}$. Let $a = (a_1, \ldots, a_d)$ be a point of $\overline{\mathbb{K}}^d$. We say that $[T, H]$ *specializes well* at a if: (i) for each $t \in T$ the polynomial $\mathrm{init}(t)$ is not zero modulo the ideal $\langle U_1 - a_1, \ldots, U_d - a_d \rangle$; (ii) the image of $[T, H]$ modulo $\langle U_1 - a_1, \ldots, U_d - a_d \rangle$ is a square-free regular system.

Border polynomial [YHX01]. Let $[T, H]$ be a square-free regular system of $\mathbb{K}[\underline{X}]$. Let bp be the primitive and square free part of the product of all $\mathrm{res}(\mathrm{der}(t), T)$ $\mathrm{res}(h, T)$ for $h \in H$ and $t \in T$. We call bp the *border polynomial* of $[T, H]$. Proposition 1 follows from the specialization property of sub-resultants and states a fundamental property of border polynomials.

Proposition 1. *The system* $[T, H]$ *specializes well at* $a \in \overline{\mathbb{K}}^d$ *if and only if the border polynomial* $bp(a) \neq 0$.

1.3 Topology

Limit points. Let (X, τ) be a topological space. A point $p \in X$ is a *limit* of a sequence $(x_n, n \in \mathbb{N})$ of points of X if, for every neighborhood U of p, there exists an N such that, for every $n \geq N$, we have $x_n \in U$; when this holds we write $\lim_{n \to \infty} x_n = p$. If X is a Hausdorff space then limits of sequences are unique, when they exist. Let $S \subseteq X$ be a subset. A point $p \in X$ is a *limit point* of S if every neighborhood of p contains at least one point of S different from p itself. Equivalently, p is a limit point of S if it is in the closure of $S \setminus \{p\}$. In addition, the closure of S is equal to the union of S and the set of its limit points. If the space X is sequential, and in particular if X is a metric space, the point p is a limit point of S if and only if there exists a sequence $(x_n, n \in \mathbb{N})$ of points of $S \setminus \{p\}$ with p as limit. In practice, the "interesting" limit points of S are those which do not belong to S. For this reason, we call such limit points *non-trivial* and we denote by $\lim(S)$ the set of non-trivial limit points of S.

Relation between Zariski topology and the Euclidean topology. When $\mathbb{K} = \mathbb{C}$, the affine space $\mathbb{A}^s$ of dimension n over $\mathbb{C}$ is endowed with both Zariski topology and the Euclidean topology. The basic open sets of the Euclidean topology are the balls while the basic open sets of Zariski topology are the complements of hypersurfaces. A Zariski closed (resp. open) set is closed (resp. open) in the Euclidean topology on $\mathbb{A}^s$. The following properties emphasize the fact that Zariski topology is coarser than the Euclidean topology: every nonempty Euclidean open set is Zariski dense and every nonempty Zariski open set is dense in the Euclidean topology on $\mathbb{A}^s$. However, the closures of a constructible set in Zariski topology and the Euclidean topology are equal. More formally, we have the following (Corollary 1 in I.10 of [Mum99]) key result. Let $V \subseteq \mathbb{A}^s$ be an irreducible affine variety and $U \subseteq V$ be open in the Zariski topology induced on V. Then, the closure of U in Zariski topology and the closure of U in the Euclidean topology are both equal to V.

1.4 Parametric polynomial systems

The following is based on [LR07] and [MXX12]. In the sequel of this section, the field $\mathbb{K}$ is either $\mathbb{R}$ or $\mathbb{C}$. Let $f_1, \ldots, f_s, p_1, \ldots, p_r \in \mathbb{Q}[\underline{X}]$, with, as before $\underline{X} = X_1 < \cdots < X_n$. Consider

the constructible set $C = \{x \in \mathbb{C}^n : f_1(x) = \cdots = f_s(x) = 0, p_1(x) \neq 0, \ldots, p_r(x) \neq 0\}$ and the semi-algebraic set $\mathcal{S} = \{x \in \mathbb{R}^n : f_1(x) = \cdots = f_s(x) = 0, p_1(x) > 0, \ldots, p_r(x) > 0\}$. Let $1 \leq d < n$. We view the variables $X_1, \ldots, X_d$ as *parameters* and we rename them as $\underline{U} = U_1, \ldots, U_d$. We denote by $\Pi_{\underline{U}}$ the canonical projection on the parameter space.

Discriminant variety in the complex case. Let δ be the dimension of $\overline{\Pi_{\underline{U}}(C)} = \overline{\Pi_{\underline{U}}(\overline{C})}$. An algebraic set $W \subset \mathbb{C}^d$ is a *discriminant variety* of C w.r.t. $\Pi_{\underline{U}}$ if the following four conditions hold:

1. $W \subseteq \overline{\Pi_{\underline{U}}(C)}$ holds,
2. $W = \overline{\Pi_{\underline{U}}(C)}$ holds if and only if $\Pi_{\underline{U}}^{-1}(u) \cap C$ is infinite for almost all $u \in \overline{\Pi_{\underline{U}}(C)}$,
3. the connected components $\mathcal{U}_1, \ldots, \mathcal{U}_k$ of $\overline{\Pi_{\underline{U}}(C)} \setminus W$ are analytic sub-manifolds of dimension δ, and
4. for all $1 \leq i \leq k$, the pair $(\Pi_{\underline{U}}^{-1}(\mathcal{U}_i), \Pi_{\underline{U}})$ is an analytic covering of $\mathcal{U}_i$.

This latter condition implies that there exists finitely many disjoint connected subsets $C_1, \ldots, C_{i_k}$ of $\mathbb{C}^n$ such that their union equals $\Pi_{\underline{U}}^{-1}(\mathcal{U}_i) \cap C$ and $\Pi_{\underline{U}}$ is a local diffeomorphism from C_j onto $\mathcal{U}_i$, for $1 \leq j \leq i_k$ and $1 \leq i \leq k$. Moreover, W contains the union of the critical values of the restriction of $\Pi_{\underline{U}}$ to the regular locus of C, as well as the projection of the singular locus of C.

Proposition 2 (Theorem 4, [MXX12])**.** *Let $[T, H]$ be a square-free regular system of $\mathbb{K}[\underline{X}]$ and bp its border polynomial. Then, the zero set of bp in $\mathbb{K}^d$ is the $\subseteq$-minimal discriminant variety of $[T, H_{\neq}]$ regarded as a parametric polynomial system, for which the parameters are the free variables of T.*

The real case. In practice, studying the parametric semi-algebraic system $\mathcal{S}$ can be done by

1. computing a discriminant variety W of the parametric constructible set C, and
2. applying the following proposition.

Proposition 3 (Corollary 1, [LR07])**.** *Assume that $W \neq \overline{\Pi_{\underline{U}}(C)}$ holds. Then, $(\overline{\Pi_{\underline{U}}(C)} \setminus W) \cap \mathbb{R}^d$ has finitely many connected components, $\mathcal{U}_1, \ldots, \mathcal{U}_e$, which are real analytic manifolds. Moreover, for each $i = 1, \ldots, e$, the number of points of $\mathcal{S}$ over $\mathcal{U}_i$ is constant, and if $\Pi_{\underline{U}}^{-1}(\mathcal{U}_i) \cap \mathcal{S}$ is not empty, then $(\Pi_{\underline{U}}^{-1}(\mathcal{U}_i) \cap \mathcal{S}, \Pi_{\underline{U}})$ is a real analytic covering of $\mathcal{U}_i$.*

1.5 Triangular decomposition of semi-algebraic sets

In this section, we recall that any semi-algebraic system decomposes into finitely many *regular semi-algebraic systems* (see Definition 1 for this term). For coherency with our software implementation, we assume the base field $\mathbb{K}$ of our polynomial coefficients is $\mathbb{Q}$ instead of $\mathbb{R}$. See [CDM+13a] for details. Nevertheless, one can easily reduce the case where $\mathbb{K}$ is a real algebraic extension of $\mathbb{Q}$ to the case $\mathbb{K} = \mathbb{Q}$ by encoding this extension with a *regular semi-algebraic system* given by polynomials with coefficients in $\mathbb{Q}$.

Semi-algebraic system. Let us consider four finite polynomial subsets $F = \{f_1, \ldots, f_s\}$, $N = \{n_1, \ldots, n_t\}$, $P = \{p_1, \ldots, p_r\}$ and $H = \{h_1, \ldots, h_\ell\}$ of $\mathbb{Q}[\underline{X}]$, where, as before, $\underline{X}$ stands for n ordered variables $X_1 < \cdots < X_n$. Let $N_{\geq}$ denote the set of the inequalities $\{n_1 \geq$

$0, \ldots, n_t \geq 0\}$. Let $P_>$ denote the set of the inequalities $\{p_1 > 0, \ldots, p_r > 0\}$. Let $H_{\neq}$ denote the set of inequations $\{h_1 \neq 0, \ldots, h_\ell \neq 0\}$. We will denote by $[F, P_>]$ the *basic semi-algebraic system* $\{f_1 = 0, \ldots, f_s = 0, p_1 > 0, \ldots, p_r > 0\}$ and by $S := [F, N_\geq, P_>, H_{\neq}]$ the semi-algebraic system (SAS) which is the conjunction of the following conditions: $f_1 = 0, \ldots, f_s = 0$, $n_1 \geq 0, \ldots, n_t \geq 0$, $p_1 > 0, \ldots, p_r > 0$ and $h_1 \neq 0, \ldots, h_\ell \neq 0$. The semi-algebraic set consisting of the zeros of S in $\mathbb{R}^n$ is denoted by $Z_\mathbb{R}(S)$ while the constructible set consisting of the zeros of $[F, N_\geq]$ in $\mathbb{C}^n$ is denoted by $Z_\mathbb{C}([F, N_\geq])$; if $N_\geq$ is empty we simply write $V(F)$ instead of $Z_\mathbb{C}([F, N_\geq])$. For an algebraic set $W \subseteq \mathbb{C}^n$, we denote by $W \cap \mathbb{R}^n$ the subset of $\mathbb{R}^n$ consisting of the points of W with real coordinates.

Definition 1. *Let $T \subset \mathbb{Q}[\underline{X}]$ be a square-free regular chain. As before, let $\underline{U} = U_1, \ldots, U_d$ and $\underline{Y} = Y_1, \ldots, Y_{n-d}$ designate respectively the variables of $\underline{X}$ that are free w.r.t. T, and those that are algebraic w.r.t. T. With $P \subset \mathbb{Q}[\underline{X}]$ as above, assume that each polynomial in P is regular w.r.t.* sat(T). *Let Q be a quantifier-free formula over $\mathbb{Q}[\underline{X}]$ involving only the $\underline{U}$ variables. Let O be the semi-algebraic subset of $\mathbb{R}^d$ defined by Q. We say that $R := [Q, T, P_>]$ is a* regular semi-algebraic system *if either $d = 0$ and the semi-algebraic system $[T, P_>]$ admits real solutions, or $d > 0$ and the following conditions hold:*

(i) O is a non-empty open subset in $\mathbb{R}^d$,

(ii) the regular system $[T, P]$ specializes well at every point a of O,

(iii) at each point a of O, the specialized system $[T(a), P(a)_>]$ admits real solutions.

The zero set *of R, denoted by $Z_\mathbb{R}(R)$, is the set of points $(a, \zeta) \in \mathbb{R}^d \times \mathbb{R}^{n-d}$ such that $Q(a)$ holds, and $t(a, \zeta) = 0$, $p(a, \zeta) > 0$ both hold for all $t \in T$ and all $p \in P$.*

Remark 1. *Using the notations of Definition 1, let $R = [Q, T, P_>]$ be a regular semi-algebraic system. Since O is open, each connected component C of O in $\mathbb{R}^d$ is locally homeomorphic to the hyper-cube $(0, 1)^d$. From Property (ii), the zero set $Z_\mathbb{R}(R)$ consists of disjoint graphs of continuous semi-algebraic functions defined on each such C. Moreover, from Property (iii), there is at least one such graph. For these reasons, the regular semi-algebraic system R can be understood as a parameterization of the set $Z_\mathbb{R}(R)$. Clearly, the dimension of $Z_\mathbb{R}(R)$ is d.*

Moreover, from Property (ii), together with Proposition 1 and Proposition 3, we deduce that for every connected component C of O, $(\Pi_{\underline{U}}^{-1}(C) \cap Z_\mathbb{R}(R), \Pi_{\underline{U}})$ is a real analytic covering of C. This implies that, at each point a of O, the Jacobian matrix of $T(a)$ is full rank.

Proposition 4. *As above, let $S := [F, N_\geq, P_>, H_{\neq}]$ be a semi-algebraic system. Then, there exists a finite family of regular semi-algebraic systems $R_1, \ldots, R_e$ such that $Z_\mathbb{R}(S)$ equals the union of $Z_\mathbb{R}(R_1), \ldots, Z_\mathbb{R}(R_e)$. We call $R_1, \ldots, R_e$ a* triangular decomposition *of S and we denote by* RealTriangularize *an algorithm computing such a decomposition.*

Remark 2. *Expanding Remark 1, recall that we have observed that the dimension of $Z_\mathbb{R}(R)$ is d. In practice, this number is immediately deduced from the number of polynomials in the regular chain T. Indeed, we have $d = n - \#(T)$, where $\#(T)$ denotes the number of elements of T.*

An important feature of the RealTriangularize *algorithm [CDM+13a] is the fact that triangular decompositions of semi-algebraic sets can be computed incrementally. Indeed, this algorithm relies on a procedure, called* Intersect, *such that, for a given semi-algebraic constraint (that is, either a polynomial equation, or a polynomial inequality) C, the function call*

Intersect(R, C) *returns regular semi-algebraic systems* $R_1, \ldots, R_e$ *such that* $Z_{\mathbb{R}}(R) \cap Z_{\mathbb{R}}(C)$ *equals the union of* $Z_{\mathbb{R}}(R_1), \ldots, Z_{\mathbb{R}}(R_e)$.

The algorithms of Section 7 use another important procedure: for a regular semi-algebraic system R, one needs to check whether the origin $\underline{o}$ *of* $\mathbb{R}^n$ *belongs or not to the closure of* $Z_{\mathbb{R}}(R)$ *in the Euclidean topology. The fact that the closure of* $Z_{\mathbb{R}}(R)$ *is a semi-algebraic set can be proved by constructing this set from other semi-algebraic sets by means if set-theoretic operations, as well as projection. Algorithms for those latter operations are described in [CDM*$^+$*13a] and [CDM*$^+$*13b]; this leads naturally to an algorithm for deciding whether or not* $\underline{o}$ *belongs to the closure of* $Z_{\mathbb{R}}(R)$.

1.6 Puiseux series

This section is devoted to concepts and notations related to Puiseux series, taken from [Fis01]. Let $\mathbb{K}$ be an algebraic number field and $\overline{\mathbb{K}}$ its algebraic closure. We denote by $\mathbb{K}[[X_1, \ldots, X_n]]$ and $\mathbb{K}\langle X_1, \ldots, X_n\rangle$ the respective rings of formal power series and convergent power series in $X_1, \ldots, X_n$ with coefficients in $\mathbb{K}$. When $n = 1$, we write U instead of X_1. Thus $\mathbb{K}[[U]]$ and $\mathbb{K}\langle U\rangle$ are the rings of formal and convergent univariate power series in U and coefficients in $\mathbb{K}$.

Puiseux series. We denote by $\mathbb{K}[[U^*]] = \bigcup_{\ell=1}^{\infty} \mathbb{K}[[U^{\frac{1}{\ell}}]]$ the ring of *formal Puiseux series*. Hence, given $\varphi \in \mathbb{K}[[U^*]]$, there exists $\ell \in \mathbb{N}_{>0}$ such that $\varphi \in \mathbb{K}[[U^{\frac{1}{\ell}}]]$ holds. Thus, we can write $\varphi = \sum_{m=0}^{\infty} a_m U^{\frac{m}{\ell}}$, for some $a_0, \ldots, a_m, \ldots \in \mathbb{K}$. We denote by $\mathbb{K}((U^*))$ the quotient field of $\mathbb{K}[[U^*]]$. Let $\varphi \in \mathbb{K}[[U^*]]$ and $\ell \in \mathbb{N}$ such that $\varphi = f(U^{\frac{1}{\ell}})$ holds for some $f \in \mathbb{K}[[U]]$. We say that the Puiseux series φ is *convergent* if we have $f \in \mathbb{K}\langle U\rangle$. Convergent Puiseux series form an integral domain denoted by $\mathbb{K}\langle U^*\rangle$; its quotient field is denoted by $\mathbb{K}(\langle U^*\rangle)$. We recall Puiseux's theorem: if $\mathbb{K}$ is an algebraically closed field of characteristic zero, the field $\mathbb{K}((U^*))$ of formal Puiseux series over $\mathbb{K}$ is the algebraic closure of the field of formal Laurent series over $\mathbb{K}$; moreover, if $\mathbb{K} = \mathbb{C}$, then the field $\mathbb{C}(\langle Y^*\rangle)$ of convergent Puiseux series over $\mathbb{C}$ is algebraically closed as well.

Puiseux parameterization. Let $f \in \mathbb{K}\langle X_1\rangle[X_2]$ be of positive degree d in X_2. A *Puiseux parametrization* of f is a pair $(\psi(U), \varphi(U))$ of elements of $\overline{\mathbb{K}}\langle U\rangle$ for some new variable U, such that

1. $\psi(U) = U^{\varsigma}$, for some $\varsigma \in \mathbb{N}_{>0}$;
2. $f(\psi(U), \varphi(U)) = 0$ holds in $\overline{\mathbb{K}}\langle U\rangle$, and
3. there is no integer $\ell > 1$ such that both $\psi(U)$ and $\varphi(U)$ are in $\overline{\mathbb{K}}\langle U^{\ell}\rangle$.

The index ς is called the *ramification index* of the parametrization $(U^{\varsigma}, \varphi(U))$. Assume that f is *general* in X_2 of order $k \geq 1$, that is, $f(0, X_2) \neq 0$ and the minimum degree of a term in $f(0, X_2)$ is k. Then, Puiseux's theorem guarantees that f admits Puiseux parameterizations and Newton-Puiseux's algorithm computes them. Assume further that f is monic in X_2. Then, there exist $\varphi_1, \ldots, \varphi_d \in \mathbb{K}\langle U\rangle$ such that we have $f(U^d, X_2) = (X_2 - \varphi_1(U)) \cdots (X_2 - \varphi_d(U))$.

Chapter 2

Extended Hensel construction

This chapter is somehow detailed review of the EHC, which is required to understand the results of the subsequent chapters Most of the proofs are omitted, though, and we refer to [SK99].

Notation 1. *Let $\mathbb{K}$ be an algebraic number field and $\overline{\mathbb{K}}$ its algebraic closure. Let $F(X,Y) \in \mathbb{K}[X,Y]$ be a bivariate polynomial with complex number coefficients. We assume that F is monic and square-free as a univariate polynomial in X; we denote by d its partial degree w.r.t. X. We assume that F has at least two terms and that $F(X,0) = X^d$ holds. We explain in Remark 4 how to reduce to this latter hypothesis. For $f_1, \ldots, f_m$ in some polynomial ring, we denote by $\langle f_1, \ldots, f_m \rangle$ the ideal that $f_1, \ldots, f_m$ generate in that ring.*

Newton line. We plot each non-zero term $c\,X^{e_x}Y^{e_y}$ of $F(X,Y)$ to the point of coordinates (e_x, e_y) in the Euclidean plane equipped with Cartesian coordinates. We call *Newton Line* the straight line L passing through the point $(d,0)$ and another point, such that no other points lie below L. The equation of L is $e_x/d + e_y/\delta = 1$ for some $\delta \in \mathbb{Q}$. We define $\widehat{\delta}, \widehat{d} \in \mathbb{Z}^{>0}$ such that $\widehat{\delta}/\widehat{d} = \delta/d$ and $\gcd(\widehat{\delta}, \widehat{d}) = 1$ both hold.

Newton polynomial. The sum of all the terms of $F(X,Y)$ which are plotted on the Newton line of F is called the *Newton polynomial* of F. We denote it by $F^{(0)}$. Observe that the Newton polynomial is a homogeneous polynomial in $(X, Y^{\delta/d})$. Let $\zeta_1, \ldots, \zeta_r \in \overline{\mathbb{K}}$ be the distinct roots of $F^{(0)}(X,1)$, for some $r \geq 2$. Note that the case where $F^{(0)}$ has only one distinct root is covered by Remark 5. Hence we have $\zeta_i \neq \zeta_j$ for all $1 \leq i < j \leq r$ and there exist positive integers $m_1 \leq m_2 \leq \cdots \leq m_r$ such that, using the homogeneity of $F^{(0)}(X,Y)$, we have

$$F^{(0)}(X,Y) = (X - \zeta_1 Y^{\delta/d})^{m_1} \cdots (X - \zeta_r Y^{\delta/d})^{m_r}.$$

The *initial factors* of $F^{(0)}(X,Y)$ are $G_i^{(0)}(X,Y) := (X - \zeta_i Y^{\delta/d})^{m_i}$, for $1 \leq i \leq r$. For simplicity, we put $\widehat{Y} = Y^{\widehat{\delta}/\widehat{d}}$.

The purpose of the EHC, as stated in Algorithm 1, is to factorize $F(X,Y)$ as $F(X,Y) = G_1(X,Y) \cdots G_r(X,Y)$, with $G_i(X,Y) \in \overline{\mathbb{K}}(\langle Y^* \rangle)[X]$ and $\deg_X(G_i) = m_i$, for $1 \leq i \leq r$. Thus, the EHC factorizes $F(X,Y)$ over $\overline{\mathbb{K}}(\langle Y^* \rangle)$, thus over $\mathbb{C}(\langle Y^* \rangle)$. However, $\deg_X(G_i) = 1$ may not hold for some i. Nevertheless, as shown in Section 2.1, factorizing $F(X,Y)$ into linear factors is achieved by repeated applications of the EHC. Lemma 1 and Theorem 1 are the fundamental results of the EHC.

Lemma 1 (Yun-Moses polynomials)**.** *Let $\widehat{G}_i(X,\widehat{Y}) \in \mathbb{C}\langle\widehat{Y}\rangle[X]$, for $i = 1,\ldots,r$ with $r \geq 2$, be homogeneous polynomials in $(X,\widehat{Y})$ such that $\gcd(\widehat{G}_i,\widehat{G}_j) = 1$ for any $i \neq j$. Let $d = \deg_X\left(\widehat{G}_1\cdots\widehat{G}_r\right)$ and $\deg_X(\widehat{G}_i) = m_i$, for $i = 1,\ldots,r$. Then, for each $\ell \in \{0,\ldots,d-1\}$, there exists a unique set of polynomials $\{W_i^{(\ell)}(X,\widehat{Y}) \in \mathbb{C}\langle\widehat{Y}\rangle[X] \mid i = 1,\ldots,r\}$ satisfying*

$$W_1^{(\ell)}\left(\left(\widehat{G}_1\cdots\widehat{G}_r\right)/\widehat{G}_1\right) + \cdots + W_r^{(\ell)}\left(\left(\widehat{G}_1\cdots\widehat{G}_r\right)/\widehat{G}_r\right) = X^\ell\widehat{Y}^{d-\ell},$$

where $\deg_X(W_i^{(\ell)}(X,\widehat{Y})) < \deg_X(\widehat{G}_i(X,\widehat{Y}))$, $i = 1,\ldots,r$. The polynomials $W_i^{(0)},\ldots,W_i^{(d-1)}$ for $1 \leq i \leq r$ are homogeneous in $(X,\widehat{Y})$ of degree m_i. We call Yun-Moses polynomials *the elements of $\{W_i^{(\ell)} \mid (\ell,i) \in \{0,\ldots,d-1\}\times\{1,\ldots,r\}\}$.*

Proof. We shall first prove that there exists only one set of polynomials $\{W_i^{(\ell)}(x,1) \mid i = 1,\ldots,r\}$ satisfying the condition in the above lemma, when $\widehat{Y} = 1$. Using the extended Euclidean algorithm, one can compute $A_1,\ldots,A_r \in \mathbb{C}[X]$ such that $A_1\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_1} + \cdots + A_r\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_r} = 1$. If we multiply both sides of the above equality by X^ℓ, then we have

$$A_1X^\ell\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_1} + \cdots + A_rX^\ell\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_r} = X^\ell. \tag{2.1}$$

For each $i = 1,\ldots,r-1$, let $Q_i, R_i \in \mathbb{C}[X]$ such that $A_iX^\ell = Q_i\widehat{G}_i + R_i$ and $\deg_X(R_i) < \deg_X(\widehat{G}_i)$. Thus the last equality can be re-written as:

$$R_1\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_1} + \cdots + R_{r-1}\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_{r-1}} + (A_rX^\ell + \sum_{i=1}^{r-1}Q_i\widehat{G}_r)\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_r} = X^\ell.$$

Observe that we have $\deg_X(R_i\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_i}) < d$ for $i = 1,\ldots,r-1$, $\deg_X(\frac{\widehat{G}_1\cdots\widehat{G}_r}{\widehat{G}_r}) = d - m_r$, and also $\ell < d$. Combined with relation 2.1, we obtain

$$\deg_X(A_rX^\ell + \sum_{i=1}^{r-1}Q_i\widehat{G}_r) < m_r = \deg_X(\widehat{G}_r).$$

Hence, we set $W_i^{(\ell)}(X,1) = R_i$, for $i = 1,\ldots,r-1$ and $W_r^{(\ell)}(X,1) = A_rX^\ell + \sum_{i=1}^{r-1}Q_i\widehat{G}_r$. Since

$$\deg_X\left(W_i^{(\ell)}(X,1)\left(\widehat{G_1}\cdots\widehat{G_r}\right)/\widehat{G}_i\right) < d,$$

we can homogenize in degree d both $W_i^{(\ell)}(X,1)$ and $\widehat{G_i}(X,1)$, for $i = 1,\ldots,r$, using $\widehat{Y}$ as homogenization variable. This homogenization process defines each $W_i^{(\ell)}(X,\widehat{Y})$ uniquely. Moreover, we have $\deg_X(W_i^{(\ell)}(X,\widehat{Y})) < \deg_X(\widehat{G_i})$. □

Theorem 1 (Extended Hensel Construction)**.** *Let F be as in Notation 1 and let $F^{(0)}(X,Y)$ be the Newton polynomial of $F(X,Y)$. We denote by $G_1^{(0)}(X,Y)$, …, $G_r^{(0)}(X,Y)$ the initial factors of $F^{(0)}(X,Y)$. Hence we have*

$$F^{(0)}(X,Y) = G_1^{(0)}(X,Y)\cdots G_r^{(0)}(X,Y),$$

where $G_i^{(0)}(X,Y) = (X - \zeta_i Y^{\widehat{\delta}/\widehat{d}})^{m_i}$ *for* $i = 1, \ldots, r$ *and* $\zeta_i \in \mathbb{C}$*. We define the ideal*

$$S_k = \langle X^d Y^{(k+0)/\widehat{d}}, X^{d-1} Y^{(k+\widehat{\delta})/\widehat{d}}, \ldots, X^0 Y^{(k+d\widehat{\delta})/\widehat{d}} \rangle, \tag{2.2}$$

for $k = 1, 2, \ldots$*. Then, for all integer* $k > 0$*, we can construct* $G_i^{(k)}(X,Y) \in \mathbb{C}\langle Y^{1/\widehat{d}} \rangle[X]$*, for* $i = 1, \ldots, r$*, satisfying*

$$F(X,Y) = G_1^{(k)}(X,Y) \cdots G_r^{(k)}(X,Y) \mod S_{k+1}, \tag{2.3}$$

and $G_i^{(k)}(X,Y) \equiv G_i^{(0)}(X,Y) \mod S_1$*, for all* $i = 1, \ldots, r$*.*

Proof. See Theorem 1 in [SK99]. The proof is constructive and by induction on k. **Base case:** Since $F(X,Y) \equiv F^{(0)}(X,Y) \mod S_1$, the theorem is valid for $k = 0$. **Inductive step:** Let the theorem be valid up to the $(k-1)$-th construction. We write:

$$G_i^{(k-1)} = G_i^{(0)}(X,Y) + \Delta G_i^{(1)}(X,Y) + \cdots + \Delta G_i^{(k-1)}(X,Y),$$

such that $G_i^{(k')}(X,Y) \in S_{k'}$, and $\deg_X(\Delta G_i^{(k')}(X,Y)) < \deg_X(G_i^{(0)}(X,Y)) = m_i$ for $k' = 1, \ldots, k-1$. These latter properties are part of the induction hypothesis. Now define

$$\Delta F^{(k)}(X,Y) := F(X,Y) - G_1^{(k-1)} \cdots G_r^{(k-1)} \mod S_{k+1}.$$

It follows from the induction hypotheses that $\Delta F^{(k)}(X,Y) \in S_k$ holds. Thus, we can write

$$\Delta F^{(k)}(X,Y) = f_{d-1}^{(k)} X^{d-1} Y^{\widehat{\delta}/\widehat{d}} + \cdots + f_0^{(k)} X^0 Y^{d\widehat{\delta}/\widehat{d}} \tag{2.4}$$

where $f_\ell^{(k)} = c_\ell^{(k)} Y^{k/\widehat{d}}$ and $c_\ell^{(k)} \in \mathbb{C}$ for $\ell = 0, \ldots, d-1$. We construct $G_i^{(k)}(X,Y)$, and thus $\Delta G_1^{(k)}, \ldots, \Delta G_r^{(k)}$, such that we have:

$$G_i^{(k)}(X,Y) = G_i^{(k-1)}(X,Y) + \Delta G_i^{(k)}(X,Y),$$

and $\Delta G_i^{(k)}(X,Y) \equiv 0 \mod S_k$. Then we have:

$$\begin{aligned} F(X,Y) &\equiv \textstyle\prod_{i=1}^r \left(G_i^{(k-1)} + \Delta G_i^{(k)} \right) \mod S_{k+1} \\ &\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} \tfrac{F^{(0)}}{G_1^{(0)}} + \cdots + \Delta G_r^{(k)} \tfrac{F^{(0)}}{G_r^{(0)}} \\ &\quad + \underbrace{\text{other terms}}_{\text{containing } \Delta G_i^{(k)}(X,Y) \Delta G_j^{(k)}(X,Y)} \mod S_{k+1} \\ &\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} \tfrac{F^{(0)}}{G_r^{(0)}} + \cdots + \Delta G_r^{(k)} \tfrac{F^{(0)}}{G_r^{(0)}} \\ &\qquad \mod S_{k+1}. \end{aligned}$$

Indeed, we have $\Delta G_i^{(k)}(X,Y) \Delta G_j^{(k')}(X,Y) \equiv 0 \mod S_{k+1}$ for $k, k' \geq 0$, from the induction hypotheses and the relation $S_k S_{k'} = S_{k+k'}$. Therefore, we have

$$\Delta F^{(k)} \equiv \Delta G_1^{(k)} \frac{F^{(0)}}{G_1^{(0)}} + \cdots + \Delta G_r^{(k)} \frac{F^{(0)}}{G_r^{(0)}} \mod S_{k+1}. \tag{2.5}$$

If in Lemma 1, we let $\widehat{G}_i(X,\widehat{Y}) = G_i^{(0)}(X,\widehat{Y})$, combining Equations (2.4) and (2.5), one can solve for $\Delta G_1^{(k)},\ldots,\Delta G_r^{(k)}$

$$\begin{aligned}\sum_{i=1}^r \Delta G_i^{(k)} \frac{F^{(0)}}{G_i^{(0)}} &= \sum_{\ell=0}^{d-1} f_\ell^{(k)} X^\ell \widehat{Y}^{d-\ell}\\ &= \sum_{\ell=0}^{d-1} f_\ell^{(k)} \left(\sum_{i=1}^r W_i^{(\ell)} \frac{F^{(0)}}{G_i^{(0)}}\right)\\ &= \sum_{i=1}^r \left(\sum_{\ell=0}^{d-1} f_\ell^{(k)} W_i^{(\ell)}\right) \frac{F^{(0)}}{G_i^{(0)}}.\end{aligned}$$

Since $\deg_X(f_\ell^{(k)} W_i^{(\ell)}) < \deg_X(G_i^{(0)})$ and $\deg_X(\Delta G_i^{(k)}(X,Y)) < \deg_X(G_i^{(0)})$ both hold for $i = 1,\ldots,r$, we deduce $\Delta G_i^{(k)}(X,Y) = \sum_{\ell=0}^{d-1} W_i^{(\ell)}(X,Y) f_\ell^{(k)}(Y)$, for $i = 1,\ldots,r$. □

Remark 3. *Theorem 1 still holds if $G_1^{(0)}(X,Y),\ldots,G_r^{(0)}(X,Y)$ just satisfy the same properties as $\widehat{G}_1(X,\widehat{Y}),\ldots,\widehat{G}_r(X,\widehat{Y})$ of Lemma 1.*

Remark 4. *Write $F(X,0) = X^d + a_1X^{e_1} + \cdots + a_mX^{e_m} + a_{m+1}$. If the polynomial F doesn't satisfy the assumption $F(X,0) = X^d$, we apply to $F(X,Y)$ the change of variables $(X,Y) := (W/Y^{1/d},Y)$ and factor out $1/Y$. We obtain a polynomial $\overline{F}(W,Y)$ satisfying $\overline{F}(W,0) = W^d$. After applying the EHC to $\overline{F}$, we multiply each computed factor by $1/Y^{1/d}$ and revert the change of variables.*

Remark 5. *Assume the Newton polynomial factorizes to $F^{(0)} = (X - aY)^d$ for some $a \in \mathbb{K}$. Since $d \geq 2$, we split $F^{(0)}$ into at least two factors, as follows. Let $Y = 1$ and apply the change of variables $X := W - a/d$, called the* Shreedharacharya-Tschirnhaus *trick in Lemma 1.8 of [MC13]. After homogenizing back, we obtain a polynomial $\overline{F}(W,Y)$ whose Newton polynomial splits into at least two co-prime factors. Applying the EHC to $\overline{F}(W,Y)$ produces at least two factors.*

Algorithm 1 Extended Hensel Construction on a given F as in Notation 1 and a positive integer k

procedure EHC_LIFT(F, k)
  Compute the Newton polynomial $F^{(0)}$ and $\widehat{\delta}, \widehat{d}$;
  Compute $F^{(0)} = G_1^{(0)} \cdots G_r^{(0)}$, see Remark 3
  if $r = 1$ **then**
    Apply the change of variable in Remark 5
  end if
  Compute the Yun-Moses polynomial $W_i^{(\ell)}$ for $i = 1, \cdots, r$ and $\ell = 0, \cdots, d-1$; (see Section 3)
  for $j = 1, \ldots, k$ **do**
    Compute $\Delta F^{(j)}(X, Y) := F(X, Y) - \prod_{i=1}^{r} G_i^{(j-1)} \mod \bar{S}_{j+1}$ (see Section 4 as well as Page 13 of [SK99]);
    Compute $\Delta G_i^{(j)} = \sum_{\ell=0}^{m-1} W_i^{(\ell)} f_\ell^{(j)}$, for $i = 1, \cdots, r$;
    Let $G_i^{(j)} = G_i^{(j-1)} + \Delta G_i^{(j)}$ for $i = 1, \cdots, r$;
  end for
  Reverse the change of variable, if any;
  return $G_1^{(k)}, \ldots, G_r^{(k)}$;
end procedure

2.1 Complete factorization in $\mathbb{C}(\langle Y^* \rangle)[X]$

To separate all the branches of the curve $F(X, Y) = 0$ around the origin, one should use a sufficient accuracy (that is, degree in Y) for the lifted factors. Theorem 4.5 in [HS83] suggests a minimum accuracy of $B := 2\, deg_X(F)\, deg_Y(F)$.

After applying EHC_Lift(F, k) with $k = \widehat{d}B - \widehat{\delta}$, which is the number of iteration needed for accuracy B, one needs to re-apply the EHC on each lifted factor of multiplicity greater than 1. For each additional call, with a lifted factor $G := G_i^{(k)}(X, Y)$, the value of k is set to $\widehat{d}B' - \widehat{\delta}$, where $B' := 2\, deg_X(G)\, deg_Y(G)$. Moreover, for each lifted factor $G_i^{(k)}(X, Y)$, with the notations of Theorem 1, we apply the change of coordinates $X = X - \zeta_i Y$. See [SK99] for details. This process generates a tree of calls to the EHC. Obviously, one needs to do at most d calls in total.

One may wonder what is the maximum total number of lifting steps along a branch of that tree. One can easily verify that, after completing the factorization of F in $\mathbb{C}(\langle Y^* \rangle)[X]$ into linear factors, this maximum is given by $\widehat{d}B - \widehat{\delta}$.

Chapter 3

On the Yun-Moses polynomials

We use the notations of Chapter 2, including the proof of Theorem 1. Define $\widetilde{Y} = Y^{1/\widehat{d}}$. In this section, we take advantage of the fact each Yun-Moses polynomial is a rational function in X, Y, whose denominator is just a power of Y.

Lemma 2. *We have* $\Delta F^{(k)} \in \mathbb{K}[X, \widetilde{Y}]$, *for all* $k = 1, 2, \ldots$.

Proof. From the Extended Hensel Construction, it is known that $\Delta F^{(k)} \equiv F - G_1^{(k-1)} \cdots G_r^{(k-1)} \mod S_{k+1}$, where $G_i^{(k-1)} = G_i^{(0)} + \Delta G_i^{(1)} + \cdots + \Delta G_i^{(k-1)}$. And we have

$$\Delta F^{(k)}(X, \widetilde{Y}) = f_{d-1}^{(k)} X^{d-1} \widetilde{Y}^{\widehat{\delta}} + \cdots + f_0^{(k)} X^0 \widetilde{Y}^{d\widehat{\delta}}$$

where $f_\ell^{(k)} = c_\ell^{(k)} \widetilde{Y}^k$ with $c_\ell^{(k)} \in \mathbb{C}$ for $\ell = 0, \ldots, d-1$. The goal is to prove $c_\ell^{(k)} \in \mathbb{K}$ and we prove it by induction. For $k = 1$, $\Delta F^{(1)} \equiv F - F^{(0)} \mod S_2$. Since $F, F^{(0)} \in \mathbb{K}[X, Y]$, we have $\Delta F^{(1)} \in \mathbb{K}[X, \widetilde{Y}]$. Now assume $\Delta F^{(k-1)} \in \mathbb{K}[X, \widetilde{Y}]$, thus $G_1^{(k-2)} \cdots G_r^{(k-2)} = F - \Delta F^{(k-1)} \in \mathbb{K}[X, \widetilde{Y}]$. We want to prove $\Delta F^{(k)} \in \mathbb{K}[X, \widetilde{Y}]$. In modulo S_{k+1}, we have

$$\begin{aligned} \Delta F^{(k)} &\equiv F - G_1^{(k-1)} \cdots G_r^{(k-1)} \\ &\equiv F - (G_1^{(k-2)} + \Delta G_1^{(k-1)}) \cdots (G_r^{(k-2)} + \Delta G_r^{(k-1)}) \\ &\equiv F - (G_1^{(k-2)} \cdots G_r^{(k-2)} + \textstyle\sum_{i=1}^r \Delta G_i^{(k-1)} \frac{F^{(0)}}{G_i^{(0)}}). \end{aligned}$$

The last equivalence is valid, due to $\Delta G_i^{(k-1)} \Delta G_j^{(k-1)} \equiv 0 \mod S_{k+1}$ and

$$(G_1^{(k-1)} \cdots G_r^{(k-1)})/G_i^{(k-1)} \equiv (G_1^{(0)} \cdots G_r^{(0)})/G_i^{(0)} \mod S_{k+1}.$$

On the other hand, $\Delta G_i^{(k-1)} = \sum_{\ell=0}^{d-1} W_i^{(\ell)} f_\ell^{(k-1)}$. So, we have

$$\begin{aligned} \textstyle\sum_{i=1}^r \Delta G_i^{(k-1)} \frac{F^{(0)}}{G_i^{(0)}} &= \textstyle\sum_{i=1}^r \sum_{\ell=0}^{d-1} W_i^{(\ell)} f_\ell^{(k-1)} \frac{F^{(0)}}{G_i^{(0)}} \\ &= \textstyle\sum_{\ell=0}^{d-1} f_\ell^{(k-1)} \sum_{i=1}^r W_i^{(\ell)} \frac{F^{(0)}}{G_i^{(0)}} \\ &= \textstyle\sum_{\ell=0}^{d-1} f_\ell^{(k-1)} X^d \widetilde{Y}^{\widehat{\delta}(d-\ell)}, \end{aligned}$$

therefore, modulo S_{k+1}, we have

$$\begin{aligned}\Delta F^{(k)} &\equiv F - (G_1^{(k-1)} \cdots G_r^{(k-1)} + \textstyle\sum_{\ell=0}^{d-1} f_\ell^{(k-1)} X^d \widetilde{Y}^{\widehat{\delta}(d-\ell)}) \\ &\equiv F - (G_1^{(k-1)} \cdots G_r^{(k-1)} + \textstyle\sum_{\ell=0}^{d-1} c_\ell^{(k-1)} X^d \widetilde{Y}^{(k-1)\widehat{\delta}(d-\ell)}).\end{aligned}$$

By induction assumption for $k-1$, we have $c_\ell^{(k-1)} \in \mathbb{K}$ and $G_1^{(k-1)} \cdots G_r^{(k-1)} \in \mathbb{K}[X, \widetilde{Y}]$, therefore, $\Delta F^{(k)} \in \mathbb{K}[X, \widetilde{Y}]$. □

From Lemma 1, the Yun-Moses polynomials associated with the initial factors $G_1^{(0)}, \ldots, G_r^{(0)}$ of $F^{(0)}$ satisfy

$$\sum_{i=1}^{r} W_i^{(\ell)} \frac{F^{(0)}}{G_i^{(0)}} = X^\ell \widehat{Y}^{d-\ell} \text{ for } \ell = 0, \cdots d-1, \tag{3.1}$$

where $\widehat{Y} = Y^{\widehat{\delta}/\widehat{d}}$ with $G_i^{(0)} = (X - \zeta_i \widehat{Y})^{m_i}$ where ζ_i is a root of $F^{(0)}(X, 1)$ and m_i is its multiplicity. Also, we have $\deg_X(W_i^{(\ell)}) < m_i$, thus, we write $W_i^{(\ell)} = \sum_{j=0}^{m_i-1} w_{i,j}^{(\ell)}(\widehat{Y}) X^j$ for any ℓ. Let us fix λ in $\{1, \ldots, r\}$. Define the column vector $\mathcal{X}_\lambda^\ell = [w_{\lambda,j}^{(\ell)}]$. The goal is to find $\mathcal{X}_\lambda^\ell$, what we shall do by solving a system of linear equations. Now for $\mu = 0, 1, \ldots, m_\lambda - 1$, we take the μ-th derivative of each side in Equation (3.1) and let $X = \zeta_\lambda \widehat{Y}$ in those derivatives. In other words, we have

$$\frac{\partial^\mu}{\partial X^\mu}\left(\sum_{i=1}^{r} W_i^{(\ell)} \frac{F^{(0)}}{G_i^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}} = \frac{\partial^\mu}{\partial X^\mu}(X^\ell \widehat{Y}^{d-\ell})|_{X=\zeta_\lambda \widehat{Y}}.$$

On the left-hand side of the above equality, after evaluating at $X = \zeta_\lambda \widehat{Y}$, all terms of the sum become zero, except the λ-th term. Therefore, we have

$$\frac{\partial^\mu}{\partial X^\mu}\left(W_\lambda^{(\ell)} \frac{F^{(0)}}{G_\lambda^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}} = \frac{\partial^\mu}{\partial X^\mu}(X^\ell \widehat{Y}^{d-\ell})|_{X=\zeta_\lambda \widehat{Y}}.$$

Also we have $W_\lambda^{(\ell)} = \sum_{j=0}^{m_\lambda-1} w_{\lambda,j}(\widehat{Y}) X^j$, thus, we have

$$\sum_{j=0}^{m_\lambda-1} \frac{\partial^\mu}{\partial X^\mu}\left(X^j \frac{F^{(0)}}{G_\lambda^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}} w_{\lambda,j}^{(\ell)} = \frac{\partial^\mu}{\partial X^\mu}(X^\ell \widehat{Y}^{d-\ell})\Big|_{X=\zeta_\lambda \widehat{Y}}. \tag{3.2}$$

On the other hand, we know that

$$\frac{\partial^\mu}{\partial X^\mu}\left(\frac{F^{(0)}}{G_\lambda^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}} = \frac{1}{m_\lambda!} \frac{\partial^{\mu+m_\lambda}}{\partial X^{\mu+m_\lambda}}(F^{(0)})\Big|_{X=\zeta_\lambda \widehat{Y}}.$$

Since $F^{(0)} \in \mathbb{K}[X, \widehat{Y}]$, we have $\frac{\partial^\mu}{\partial X^\mu}\left(\frac{F^{(0)}}{G_\lambda^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}} \in \mathbb{K}(\zeta_\lambda)[\widehat{Y}]$. So, Equation (3.2) is a system of linear equations $\mathcal{W}_\lambda \mathcal{X}_\lambda^{(\ell)} = \mathcal{B}_\lambda^{(\ell)}$ in $\mathbb{K}(\zeta_\lambda)[\widehat{Y}]$ (also see [SK99]) with coefficient matrix

$$\mathcal{W}_\lambda = [\alpha_{j,\mu}] \text{ with } \alpha_{j,\mu} = \frac{\partial^\mu}{\partial X^\mu}\left(X^j \frac{F^{(0)}}{G_\lambda^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}}, \tag{3.3}$$

unknown vector $\mathcal{X}_\lambda^\ell = [w_{\lambda,j}^{(\ell)}]$ and constant vector

$$\mathcal{B}_\lambda^{(\ell)} = [\beta_\mu] \text{ with } \beta_\mu = \frac{\partial^\mu}{\partial X^\mu}(X^\ell \widehat{Y}^{d-\ell})|_{X=\zeta_\lambda \widehat{Y}} \tag{3.4}$$

for $j, \mu = 0, 1, \ldots, m_\lambda - 1$. The matrix $\mathcal{W}_\lambda$ is a Wronskian matrix. It is known that a Wronskian matrix is invertible whenever the functions in the first row are analytic and linearly independent, see [Boc00]. In our case, the functions $\left(X^j \frac{F^{(0)}}{G_\lambda^{(0)}}\right)|_{X=\zeta_\lambda \widehat{Y}}$, for $j = 0, 1, \ldots, m_\lambda - 1$, are, indeed, linearly independent polynomials in $\mathbb{K}(\zeta_\lambda)[\widehat{Y}]$, therefore, the Wronskian matrix $\mathcal{W}_\lambda$ is invertible.

Now let us find the inverse of $\mathcal{W}_\lambda$. For simplicity of notations, let $f := \left(\frac{F^{(0)}}{G_\lambda^{(0)}}\right)|_{X=\zeta_\lambda \widehat{Y}}$ and $f^{(\mu)} := \left(\frac{\partial^\mu}{\partial X^\mu}\frac{F^{(0)}}{G_\lambda^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}}$ for $\mu = 1, \ldots, m_\lambda - 1$.

Proposition 5. *The inverse of $\mathcal{W}_\lambda$ is $\mathcal{W}_\lambda^{-1} = M_2 M_1$ where M_1 and M_2 are square matrices of order m_λ, defined as follows. The matrix M_1 writes $M_1 = M_{1(m_\lambda-1)} \cdots M_{11} M_{10}$ such that, for $j = 0, \cdots, m_\lambda - 1$, we have*

$$M_{1j} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \frac{1}{j!f} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \binom{j+1}{j}\frac{-f'}{f} & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \binom{m_\lambda-1}{j}\frac{-f^{(m_\lambda-1-j)}}{f} & 0 & \cdots & 1 \end{bmatrix}.$$

Hence, the matrix M_{1j} differs from the identity matrix only in its $(j+1)$-th column. The matrix M_2 is an upper triangular matrix given by $M_2 = [\gamma_{j,k}]$ with $\gamma_{j,k} = (-1)^{j+k}\binom{k}{k-j}\zeta_\lambda^{k-j}\widehat{Y}^{k-j}$ if $j \le k$ and $\gamma_{j,k} = 0$ if $j > k$, for $j, k \in \{0, 1, \ldots, m_\lambda - 1\}$.

Proof. To prove $\mathcal{W}_\lambda^{-1} = M_2 M_1$, it is enough to show that $M_2^{-1} = M_1 \mathcal{W}_\lambda$ holds, where M_2^{-1} is given by the next claim.

Claim: M_2^{-1} is upper triangular with $\binom{k}{k-j}\zeta_\lambda^{k-j}\widehat{Y}^{k-j}$ as $(j,k)-$entry.

Proof of the claim: Let A be the upper triangular matrix with $\binom{k}{k-j}T^{k-j}$ as $(j,k)-$entry where T is a new variable. We show that $A|_{T=\zeta_\lambda \widehat{Y}} \cdot M_2 = I$ where I is the identity matrix of order m_λ. Let us look at the dot product of the $(j+1)$-th row of A and the $(k+1)$-th column of M_2 where $k \ge j$. This dot product is:

$$\sum_{l=0}^{k-j}(-1)^{k+j+l}\binom{k}{k-j-l}T^l\binom{j+l}{l}\zeta_\lambda^{k-j-l}\widehat{Y}^{k-j-l}.$$

The above quantity is also equal to each side of Equation (3.5):

$$\binom{k}{j}\sum_{l=0}^{k-j}(-1)^{k+j+l}\binom{k-j}{l}T^l\zeta_\lambda^{k-j-l}\widehat{Y}^{k-j-l} = \binom{k}{j}(T-\zeta_\lambda\widehat{Y})^{k-j}. \tag{3.5}$$

So for $k = j$, the right hand side of Equation (3.5) equals 1, and when $k \neq j$ (i.e. $k > j$), by evaluating $T = \zeta_\lambda \widehat{Y}$, it is 0. Hence, we have $A|_{T=\zeta_\lambda \widehat{Y}} \cdot M_2 = I$ and $M_2^{-1} = A|_{T=\zeta_\lambda \widehat{Y}}$, proving the claim.

Now, it is enough to show that $M_2^{-1} = M_1 \cdot \mathcal{W}_\lambda$ holds. Observe that M_{1j} is the product of some elementary matrices (which are obtained by applying one elementary row operation on the identity matrix, like the above matrices). Let $N_{j-1} := M_{1(j-1)} \cdots M_{10} \mathcal{W}_\lambda$. By multiplying M_{1j} by N_{j-1}, we are factoring out f from the $(j+1)$-th row and adding $-\binom{k}{j} f^{(k)}$ multiple of the $(j+1)$-th row to the $(j+k)$-th row for $k = 2, \ldots, m_\lambda - j - 1$. Therefore, the factor f will be removed from the $(j+1)$-th row. Furthermore, the term with highest derivative will also be removed from all rows after the $(j+1)$-th one. Hence, $M_{1(m_\lambda - 1)} \cdots M_{10} \mathcal{W}_\lambda$ is an upper triangular matrix such that every entry in the upper triangle is given by multiplying the term with lowest derivative of f by $1/(j! f)$. Since the $(j+1, k+1)-$entry of $\mathcal{W}_\lambda$ is $\frac{\partial^j}{\partial X^j}\left(X^k \frac{F^{(0)}}{G_\lambda^{(0)}}\right)$ at $X = \zeta_\lambda \widehat{Y}$, the $(j+1, k+1)-$entry of $M_{1(m_\lambda-1)} \cdots M_{10} \mathcal{W}_\lambda$ is

$$\frac{1}{j! f} \frac{k!}{(k-j)!} \zeta_\lambda^{k-j} \widehat{Y}^{k-j} f = \binom{k}{k-j} \zeta_\lambda^{k-j} \widehat{Y}^{k-j},$$

which is exactly M_2^{-1}. This completes the proof. □

Lemma 1 yields the following for Yun-Moses polynomials.

Corollary 1. *If $F(X, Y) \in \mathbb{K}[X, Y]$, then $W_\lambda^{(\ell)} \in \mathbb{K}(\zeta_\lambda)\langle \widehat{Y} \rangle[X]$, where ζ_λ is the root of the initial factor of $F^{(0)}$ corresponding to $W_\lambda^{(\ell)}$,*

Proof. From Lemma 1, we have $W_\lambda^\ell \in \mathbb{C}\langle \widehat{Y} \rangle[X]$. Thus, it is enough to show that the coefficients of W_λ^ℓ are from $\mathbb{K}(\zeta_\lambda)$. First, observe that $F^{(0)}$ and $G_\lambda^{(0)}$ are two homogeneous polynomials of degrees $\sum_j m_j$ and m_λ in $\mathbb{K}[X, \widehat{Y}]$ and $\mathbb{K}(\zeta_\lambda)[X, \widehat{Y}]$, respectively. For any $\mu = 0, 1, \ldots, m_\lambda - 1$, we have

$$\frac{\partial^\mu}{\partial X^\mu}\left(\frac{F^{(0)}}{G_\lambda^{(0)}}\right)\Big|_{X=\zeta_\lambda \widehat{Y}} \in \mathbb{K}(\zeta_\lambda)[\widehat{Y}].$$

Hence, the coefficients of all entries of $\mathcal{W}_\lambda^{-1}$, defined in Proposition 5, live in $\mathbb{K}(\zeta_\lambda)$. Also, observe that the coefficients of all entries in matrix $\mathcal{B}_\lambda^{(\ell)}$ defined in (3.4) live in the same field $\mathbb{K}(\zeta_\lambda)$, therefore, $w_{\lambda,j} \in \mathbb{K}(\zeta_\lambda)\langle Y \rangle$, for all $j = 0, 1, \ldots, m_\lambda - 1$. Hence $W_\lambda^{(\ell)} \in \mathbb{K}(\zeta_\lambda)\langle Y \rangle[X]$. □

3.1 Computing the polynomials W_λ

In this section, we discuss how we compute the Yun-Moses polynomials W_λ. We regard each W_λ as a univariate polynomial in X, so we need to compute the coefficients of X^j for $j = 0, 1, \ldots, m_\lambda - 1$, which are univariate polynomials in $\widehat{Y} = Y^{\widehat{\delta}/\widehat{d}}$. Therefore, we need to compute the inverse of the Wronskian matrix $\mathcal{W}_\lambda$ by computing $M_{10}, M_{11}, \ldots, M_{1(m_\lambda-1)}$ and M_2 at $X = \zeta_\lambda \widehat{Y}$. Since $\frac{F^{(0)}}{G_\lambda^{(0)}}(X, \widehat{Y})$ is a homogeneous polynomial, then f, as defined before Proposition 5,

is just a term in $\widehat{Y}$. Therefore, all entries of $\mathcal{W}_\lambda^{-1}$ are just terms in $\widehat{Y}$; so to compute $\mathcal{W}_\lambda^{-1} = M_2 M_{10} \cdots M_{1(m_\lambda-1)}$, we just need to do arithmetic on the coefficients of $\widehat{Y}$ and keep track of the degree of $\widehat{Y}$ in each entry. We can observe that the degree of $\widehat{Y}$ in the $(j,k)-$entry of $\mathcal{W}_\lambda^{-1}$ is $m_\lambda - d - j + k$ (see Section 3.2). On the other hand, the degree of $\widehat{Y}$ in the j-th entry of $\mathcal{B}_\lambda^{(\ell)}$ is $d - j$ (see Section 3.2). Hence, computing the product $\mathcal{W}_\lambda^{-1} = M_2 M_{10} \cdots M_{1(m_\lambda-1)}$ can be done as if those matrices had coefficients in $\mathbb{K}(\zeta_\lambda)$ rather than $\mathbb{K}(\zeta_\lambda)[\widehat{Y}]$.

3.2 Complexity analysis

Let $f := F^{(0)}(X, \widehat{Y})/(X - \zeta_\lambda \widehat{Y})^{m_\lambda}$, where ζ_λ is a root of $F^{(0)}(X, 1)$, and let d_f be the degree of f w.r.t. X. So $d_f = d - m_\lambda$. We use the notations of Proposition 5. After evaluation at $X = \zeta_\lambda \widehat{Y}$, in all entries of M_1 below the main diagonal, the degree of the denominator of the $(j,k)-$entry is $(j-k+1)d_f$, the degree of the numerator is $(j-k)(d_f-1)$ for $j, k = 1, \ldots, m_\lambda$, with $j \geq k$. Thus, in the $(j,k)-$entry, the degree of $\widehat{Y}$ is $-(d - m_\lambda + j - k)$. In M_2, the degree of $\widehat{Y}$ on the $(j,k)-$entry is $k - j$ for $j, k = 1, \ldots, m_\lambda$ with $k \geq j$. Hence, the $\widehat{Y}$-degree in the $(j,k)-$entry of $\mathcal{W}_\lambda^{-1}$ is $2m_\lambda - d + k - j$.

Recall that $n \longmapsto \mathrm{M}(n)$ denotes a (polynomial) multiplication time [GG03]. In particular, $\mathrm{M}(n)$ is an upper bound for the number of operations in $\mathbb{K}(\zeta_\lambda)$ required for multiplying two univariate polynomials in $\mathbb{K}(\zeta_\lambda)$ with degree less than n. Let $\mathrm{A}(n)$ be an upper bound for the number of operations in $\mathbb{K}$ required by one addition or multiplication in a simple algebraic extension of $\mathbb{K}$ of degree n. We have: $\mathrm{A}(n) \in O(\mathrm{M}(n))$. Observe that the cost of evaluating f and its derivatives up to $f^{(m_\lambda-1)}$ is negligible. Let C_1 be the cost of constructing the matrices $M_{10}, M_{11}, \ldots, M_{1(m_\lambda-1)}$ and M_2. Assuming that $1/\zeta_\lambda$ and all involved binomial coefficients are precomputed, we have: $C_1 = \left(\frac{(m_\lambda-1)m_\lambda}{2} + \sum_{j=0}^{m_\lambda-1} m_\lambda - j\right) A(d)$. The cost C_2 of multiplying $M_{10}, M_{11}, \ldots, M_{1(m_\lambda-1)}$ and M_2 is:

$$C_2 = \left(\sum_{j=1}^{m_\lambda-1} (m_\lambda - j)(2j-1) + m_\lambda \sum_{j=1}^{m_\lambda} 2(j-1) - 2 \sum_{k=1}^{m_\lambda} \sum_{j=1}^{k} j \right) A(d).$$

To understand where the factor $A(d)$ comes from, one should note that, if $F^{(0)}(X, 1)$ does not split into linear factors over $\mathbb{K}$, it is sufficient to work with its irreducible factors over $\mathbb{K}$, see Remark 3. Therefore, the cost C_{YM} of computing the Yun-Moses polynomials $W_\lambda^{(\ell)}$, for $\ell \in \{0, \ldots, d-1\}$, is given by $C_{\mathrm{YM}} = C_1 + C_2 = O(m_\lambda^3 \mathrm{M}(d))$. This leads us to:

Theorem 2. *One can compute all the Yun-Moses polynomials $W_i^{(\ell)}$ ($0 \leq \ell \leq d-1$, $1 \leq i \leq r$), within $O(d^3\,\mathrm{M}(d))$ operations in $\mathbb{K}$.*

Proof. For constructing the matrices $M_{10}, M_{11}, \ldots, M_{1(m_\lambda-1)}$, we need, respectively, $m_\lambda, m_\lambda - 1, \ldots, 1$ arithmetic calculations and therefore, $\left(\frac{(m_\lambda-1)m_\lambda}{2}\right) A(d)$ as the total cost. Also for M_2, since it is an upper triangular matrix, it needs $\sum_{j=0}^{m_\lambda-1} m_\lambda - j$ arithmetic computations. Thus the total cost for constructing the matrices $M_{10}, M_{11}, \ldots, M_{1(m_\lambda-1)}$, and M_2 is

$$C_1 = \left(\frac{(m_\lambda - 1)m_\lambda}{2} + \sum_{j=0}^{m_\lambda-1} m_\lambda - j \right) A(d).$$

M_1, row j \ M_2, col k	1	2	$\cdots$	k	$\cdots$	m_λ
1	$2\,m_\lambda$	$2\,(m_\lambda-1)$	$\cdots$	$2\,(m_\lambda-k-1)$	$\cdots$	2
2	$2\,(m_\lambda-1)$	$2\,(m_\lambda-1)$	$\cdots$	$2\,(m_\lambda-k-2)$	$\cdots$	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
j	$2\,(m_\lambda-j+1)$	$2\,(m_\lambda-j+1)$	$\cdots$	$2\,(m_\lambda-k-j)$	$\cdots$	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
m_λ	2	2	$\cdots$	2	$\cdots$	2

Table 3.1: Calculation of the total number of multiplications and additions for multiplying each row of M_1 by each column of M_2.

Due to the sparsity of the matrices $M_{10}, M_{11}, \ldots, M_{1(m_\lambda-1)}$, computing $M_1 = M_{10}M_{11}\ldots M_{1(m_\lambda-1)}$ requires $\sum_{j=1}^{m_\lambda-1}(m_\lambda-j)(2j-1)$ multiplications and additions in $\mathbb{K}$.

Next, we multiply M_2 and M_1. As we know, the matrices M_2 and M_1 are, respectively, upper and lower triangular matrices. The number of multiplications and additions for multiplying each row of M_2 by each column of M_1 is listed in Table 3.1. Thus the total number of the arithmetic computations for computing M_2M_1 is

$$\left(m_\lambda\sum_{j=1}^{m_\lambda}2(j-1)-2\sum_{k=1}^{m_\lambda}\sum_{j=1}^{k}j\right)A(d).$$

Thus the total cost of arithmetic computations for building

$$M_1 = M_{10}M_{11}\cdots M_{1(m_\lambda-1)}$$

and multiplying M_2 and M_1 is

$$C_2=\left(\sum_{j=1}^{m_\lambda-1}(m_\lambda-j)(2j-1)+m_\lambda\sum_{j=1}^{m_\lambda}2(j-1)-2\sum_{k=1}^{m_\lambda}\sum_{j=1}^{k}j\right)A(d).$$

Thus the cost of computing Yun-Moses polynomials $W_\lambda^{(\ell)}$, for $\ell=0,\ldots,d-1$, is $O(m_\lambda^3 M(d))$. Thus the total cost for computing all the Yun-Moses polynomials $W_i^{(}\ell)$, for $\ell=0,\ldots,d-1$, and for $i=1,\ldots,r$, is $O(d^3\,\mathrm{M}(d))$. □

Chapter 4

Lifting the factors

We turn our attention to the lifting of the factors during the EHC, Lines 8-12 in Algorithm 1. A naive implementation of that step would make the running-time of the i-iteration growing quadratically with i. Adapting and enhancing an idea of L. Bernardin in [Ber98], we make this running-time in $O(i)$ instead of $O(i^2)$.

Let $\tilde{Y} = Y^{1/\widehat{d}}$. Let Δ_i^k be such that $\Delta G_i^{(k)} = \Delta_i^k \tilde{Y}^k$ and define $\Delta_i^0 = G_i^{(0)}$. Therefore, Δ_i^k, for $k > 0$, is homogeneous with respect to $(X, \widehat{Y})$ of degree m_i and we can write $G_i^{(k)} = \Delta_i^0 + \Delta_i^1 \tilde{Y} + \Delta_i^2 \tilde{Y}^2 + \cdots + \Delta_i^k \tilde{Y}^k$. While Bernardin in [Ber98] discusses his "recycling" strategy for univariate polynomials with constant coefficients, we enhance his idea for the bivariate polynomials $G_i^{(k)}$.

For $j = 2, \ldots, r$ and $k \geq 1$, we let P_j^k be a degree k univariate polynomial in $\tilde{Y}$ satisfying $P_j^k \equiv G_1^{(k-1)} \cdots G_j^{(k-1)} \mod S_{k+1}$. So, initially, we have $P_j^1 \equiv G_1^{(0)} \cdots G_j^{(0)} \mod S_2$, for $j = 2, \ldots, r$. For $j = 2$ and $k > 1$ we have

$$\begin{aligned} P_2^k &\equiv G_1^{(k-1)} G_2^{(k-1)} \mod S_{k+1}, \text{ so} \\ P_2^k &= \Delta_1^0 \Delta_2^0 + \left(\Delta_1^0 \Delta_2^1 + \Delta_2^0 \Delta_1^1\right) \tilde{Y} + \cdots \\ &\quad + \left(\Delta_1^0 \Delta_2^{k-1} + \cdots + \Delta_2^0 \Delta_1^{k-1}\right) \tilde{Y}^{k-1} \\ &\quad + \left(\Delta_1^1 \Delta_2^{k-1} + \cdots + \Delta_2^1 \Delta_1^{k-1}\right) \tilde{Y}^k. \end{aligned}$$

For the next iteration, that is from k to $k+1$, we have:

$$\begin{aligned} P_2^{k+1} &\equiv G_1^{(k)} G_2^{(k)} \mod S_{k+2}, \text{ so} \\ P_2^{k+1} &= \Delta_1^0 \Delta_2^0 + \left(\Delta_1^0 \Delta_2^1 + \Delta_2^0 \Delta_1^1\right) \tilde{Y} + \cdots \\ &\quad + \left(\Delta_1^0 \Delta_2^{k-1} + \cdots + \Delta_2^0 \Delta_1^{k-1}\right) \tilde{Y}^{k-1} \\ &\quad + \left(\Delta_1^0 \Delta_2^k + \cdots + \Delta_2^0 \Delta_1^k\right) \tilde{Y}^k \\ &\quad + \left(\Delta_1^1 \Delta_2^k + \cdots + \Delta_2^1 \Delta_1^k\right) \tilde{Y}^{k+1}. \end{aligned}$$

If we assume that P_2^k has been computed and stored at the previous iteration, then it is enough to compute $\Delta_1^0 \Delta_2^k$, $\Delta_2^0 \Delta_1^k$ and $\Delta_1^1 \Delta_2^k + \cdots + \Delta_2^1 \Delta_1^k$ in the current iteration in order to deduce P_2^{k+1},

with the following recursive formula:

$$P_2^{k+1} = P_2^k + (\Delta_1^0\Delta_2^k + \Delta_1^k\Delta_2^0)\tilde{Y}^k + (\Delta_1^1\Delta_2^k + \cdots + \Delta_1^k\Delta_2^1)\tilde{Y}^{k+1}.$$

Now for $j = 3, \ldots, r$, define

$$\begin{aligned} P_j^k &\equiv P_{j-1}^k G_j^{(k-1)} \quad \bmod S_{k+1}, \text{ so} \\ P_j^k &= p_{j-1}^{k,0}\Delta_j^0 + \left(p_{j-1}^{k,1}\Delta_j^0 + p_{j-1}^{k,0}\Delta_j^1\right)\tilde{Y} + \cdots \\ &\quad + \left(p_{j-1}^{k,0}\Delta_j^{k-1} + \cdots + p_{j-1}^{k,k-1}\Delta_j^0\right)\tilde{Y}^{k-1} \\ &\quad + \left(p_{j-1}^{k,1}\Delta_j^{k-1} + \cdots + p_{j-1}^{k,k}\Delta_j^0\right)\tilde{Y}^k, \end{aligned}$$

where $P_{j-1}^k = p_{j-1}^{k,0} + p_{j-1}^{k,1}\tilde{Y} + \cdots + p_{j-1}^{k,k}\tilde{Y}^k$. Hence, we deduce:

$$\begin{aligned} P_j^{k+1} &= P_{j-1}^{k+1} G_j^{(k)} \quad \bmod S_{k+2}, \text{ so} \\ P_j^{k+1} &= p_{j-1}^{k+1,0}\Delta_j^0 + \left(p_{j-1}^{k+1,1}\Delta_j^0 + p_{j-1}^{k+1,0}\Delta_j^1\right)\tilde{Y} + \cdots \\ &\quad + \left(p_{j-1}^{k+1,0}\Delta_j^{k-1} + \cdots + p_{j-1}^{k+1,k-1}\Delta_j^0\right)\tilde{Y}^{k-1} \\ &\quad + \left(p_{j-1}^{k+1,0}\Delta_j^{k} + \cdots + p_{j-1}^{k+1,k}\Delta_j^0\right)\tilde{Y}^{k} \\ &\quad + \left(p_{j-1}^{k+1,1}\Delta_j^{k} + \cdots + p_{j-1}^{k+1,k+1}\Delta_j^0\right)\tilde{Y}^{k+1}. \end{aligned}$$

If we assume that P_j^k and P_{j-1}^k have been computed and stored at the previous iteration, then we can recycle some of the terms of P_j^k and P_{j-1}^k in support of the calculation of P_j^{k+1}. However, there are definitely new terms in P_j^{k+1} that we need to compute in the current iteration, namely $p_{j-1}^{k+1,0}\Delta_j^k$ and $p_{j-1}^{k+1,1}\Delta_j^k + \cdots + p_{j-1}^{k+1,k+1}\Delta_j^0$.

Observe that $p_{j-1}^{k+1,i} = p_{j-1}^{k,i}$ holds for $i = 0, 1, \ldots, k-1$, while $p_{j-1}^{k+1,k} = p_{j-1}^{k,k} + q_j^{k+1}$ holds, where q_j^{k+1} is recursively given by

$$q_j^{k+1} = p_{j-1}^{k+1,0}\Delta_j^k + q_{j-1}^{k+1}\Delta_j^0 \text{ with } q_2^{k+1} = \Delta_2^k\Delta_1^0 + \Delta_2^0\Delta_1^k. \tag{4.1}$$

Now observe that we have

$$\begin{aligned} p_j^{k+1,k} &= p_{j-1}^{k+1,0}\Delta_j^k + \cdots + p_{j-1}^{k+1,k}\Delta_j^0 \\ &= p_{j-1}^{k+1,0}\Delta_j^k + p_{j-1}^{k,1}\Delta_j^{k-1} + \cdots + p_{j-1}^{k,k-1}\Delta_j^1 \\ &\qquad + (p_{j-1}^{k,k} + q_j^{k+1})\Delta_j^0 \\ &= p_{j-1}^{k+1,0}\Delta_j^k + p_j^{k,k} + q_{j-1}^{k+1}\Delta_j^0 = p_j^{k,k} + q_j^{k+1}. \end{aligned}$$

Therefore, we can write

$$P_j^{k+1} = P_j^k + q_j^{k+1}\tilde{Y}^k + \left(p_{j-1}^{k+1,1}\Delta_j^k + \cdots + p_{j-1}^{k+1,k+1}\Delta_j^0\right)\tilde{Y}^{k+1}. \tag{4.2}$$

Note: the term q_j^{k+1} is missing in the formula at the top of the left column on p. 3 of [Ber98].

4.1 Complexity analysis

It follows from Equation (4.2) that each P_j^ℓ, for $0 \leq \ell \leq k+1$, is derived from $P_j^{\ell-1}$ and P_{j-1}^ℓ *in a Pascal Triangle fashion*. More precisely, letting $\ell = k+1$, if P_j^k and P_{j-1}^{k+1} are known, computing P_j^{k+1} requires 2 multiplications for computing q_j^{k+1} (see Equations (4.1) and (4.2)) and k multiplications for the new terms (see Equation(4.2)). Every product involves a polynomial of degree m_j and a polynomial of degree $m_1 + \cdots + m_{j-1}$. Also, all P_j^ℓ for $j = 1, \ldots, r$ and $\ell = 1, \ldots, k$ need to be computed before computing P_r^{k+1}. Let C_{lift} be the cost of computing P_r^{k+1}. We have: $C_{\text{lift}} = \sum_{l=2}^{r}(k+2)\mathrm{M}(\max(m_1 + \cdots + m_{l-1}, m_l))\mathrm{A}(d)$. This leads us to the following result.

Theorem 3. *The k-th iteration of Step 9 in the Algorithm 1 runs in $O(k\, d\mathrm{M}(d)^2)$ operations in $\mathbb{K}$.*

Chapter 5

Real limit points

Let $T \subset \mathbb{Q}[X_1, \ldots, X_n]$ be a one-dimensional regular chain; we denote by U its free variable. In [ACM13], an algorithm is proposed for computing the non-trivial limit points of the quasi-component $W(T)$, that is, the set $\overline{W(T)} \setminus W(T)$ (where $\overline{W(T)}$ is the Zariski closure of $W(T)$). In Algorithm 4 of [AKM16], a similar, but different, computation is needed. In this case, we need the non-trivial limit points of $W_{\mathbb{R}}(T) := Z_{\mathbb{R}}(T) \setminus Z_{\mathbb{R}}(h_T)$, that is, the set $\overline{W_{\mathbb{R}}(T)} \setminus W_{\mathbb{R}}(T)$, where $\overline{W_{\mathbb{R}}(T)}$ is the closure of $W_{\mathbb{R}}(T)$ in $\mathbb{R}^n$ endowed with the Euclidean topology. Unfortunately, it is not true that the non-trivial limit points of $W_{\mathbb{R}}(T)$ are the non-trivial limit points of $W(T)$ with real coordinates, as shown by the example of Figure 0.2 However, the algorithm of [ACM13], which is based on Puiseux series, can be adapted in order to compute the non-trivial limit points of $W_{\mathbb{R}}(T)$. This adaptation is explained hereafter. The LimitPoints command of the RegularChains library in MAPLE handles both cases, $W(T)$ and $W_{\mathbb{R}}(T)$. The *Puiseux parametrizations* of the regular chain T in Definition 2 (see also [ACM13], Definition 2) encode all the branches of $V(\mathrm{sat}(T))$ when the free variable U approaches zero. It is proved in [ACM13] that the non-trivial limit points of $W(T)$ around $U = 0$ are obtained by letting U to be zero in all the Puiseux parametrizations of T.

Definition 2. *Let $T := \{t_1, \ldots, t_{n-1}\} \subset \mathbb{Q}[X_1 < \cdots < X_n]$ be a one-dimensional regular chain whose free variable is X_1 and such that $X_1 = 0$ is a root of the product h_T of the initials of T. Let $\chi = (\chi_2(U), \ldots, \chi_n(U))$ be a vector of $\mathbb{C}((U^*))^{n-1}$ and let $\varsigma_1 = 1$. We assume that, for all $2 \leq j \leq n$, there exists a non-negative integer ς_j such that $(U^{\varsigma_j}, \chi_j(U))$ is a Puiseux parametrization of the univariate polynomial $t_{j-1}(U^{\varsigma_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j)$ around $U = 0$, where the minimum exponent of U in $\chi_j(U)$ is non-negative. Let $\varsigma := \mathrm{lcm}(\varsigma_2, \ldots, \varsigma_n)$ and $\phi_j = \chi_j(U^{\frac{\varsigma}{\varsigma_j}})$. Then $(U^{\varsigma}, \phi_2, \ldots, \phi_n)$ is called a* Puiseux parametrization *of T around $U = 0$.*

Example 1. *Let $T := \{t_1, t_2\} \subseteq \mathbb{Q}[X_1 < X_2 < X_3]$ be a regular chain where $t_1 := X_2^4 - 2\,X_2^3 + X_2^2 + X_1^5$ and $t_2 := X_1^4\,X_3 + X_2^3 - X_2^2$. We note that the product of the initials of T is $h_T := X_1^4$. We would like to compute the Puiseux parametrizations of the regular chain T around $X_1 = 0$. Using the* ExtendedHenselConstruction *command of our library* PowerSeries

[1], *one can compute the Puiseux parametrizations of* t_1 *around* $X_1 = 0$ *and obtain:*

$$\begin{aligned}
\Phi_1 &:= \left(X_1 = U^2, X_2 = 1 + \sqrt{-1}\,U^5 + U^{10} + O(U^{15})\right),\\
\Phi_2 &:= \left(X_1 = U^2, X_2 = 1 - \sqrt{-1}\,U^5 + U^{10} + O(U^{15})\right),\\
\Phi_3 &:= \left(X_1 = U^2, X_2 = \sqrt{-1}\,U^5 - U^{10} + O(U^{15})\right),\\
\Phi_4 &:= \left(X_1 = U^2, X_2 = -\sqrt{-1}\,U^5 - U^{10} + O(U^{15})\right).
\end{aligned} \tag{5.1}$$

The big-oh notation is used above to indicate at which degree the displayed power series are truncated.

Now by substituting Φ_1 *into* t_2*, we obtain* $t_{21} := U^8\,X_3 + (1 + \sqrt{-1}\,U^5 + U^{10})^3 - (1 + \sqrt{-1}\,U^5 + U^{10})^2$*. Next, we compute Puiseux parametrizations of* t_{21} *around* $U = 0$ *and obtain:*

$$\left(U = U, X_3 = -\frac{\sqrt{-1}}{U^4} + U^2 - 3\,\sqrt{-1}\,U^7 + O(U^8)\right).$$

Since there is a negative exponent of U *appearing in the above Puiseux parametrization of* t_{21}*, this parametrization would not result in a Puiseux parametrization for the regular chain* T*. By repeating the same process with* Φ_2*, one obtains a Puiseux parametrization in which negative exponents of* U *appear as well. However, the scenario is different when substituting* Φ_3 *into* t_2*. Indeed, this substitution yields* $t_{23} := U^8\,X_3 + (\sqrt{-1}\,U^5 - U^{10})^3 - (\sqrt{-1}\,U^5 - U^{10})^2$*, whose Puiseux parametrization around* $U = 0$ *is*

$$X_3 = -U^2\left(-U^{20} + 3\,\sqrt{-1}\,U^{15} + 2\,U^{10} + \sqrt{-1}\,U^5 + 1 + O(U^{25})\right).$$

Since there is no negative exponents of U *in the latter Puiseux parametrization, we deduce the following Puiseux parametrization of the regular chain* T*:*

$$\begin{aligned}
\Phi_{2,3} := (&X_1 = U^2, X_2 = \sqrt{-1}\,U^5 - U^{10} + O(U^{15}),\\
&X_3 = U^{22} - 3\,\sqrt{-1}\,U^{17} - 2\,U^{12} - \sqrt{-1}\,U^7 - U^2 + O(U^{27}))
\end{aligned}$$

Proceeding similarly with Φ_4*, one obtains the second Puiseux parametrization of* T*:*

$$\begin{aligned}
\Phi_{2,4} := (&X_1 = U^2, X_2 = -\sqrt{-1}\,U^5 - U^{10} + O(U^{15}),\\
&X_3 = U^{22} + 3\,\sqrt{-1}\,U^{17} - 2\,U^{12} + \sqrt{-1}\,U^7 - U^2 + O(U^{27}))
\end{aligned}$$

In both Puiseux parametrizations of regular chain T*, the ramification index is* $\varsigma = \mathrm{lcm}(2, 1) = 2$*.*

Remark 6. *Definition 2 implies each Puiseux parametrization* $(U^\varsigma, \phi_2, \ldots, \phi_n)$ *of* T *belongs to* $\mathbb{C}\langle U\rangle^n$*. Hence, those Puiseux parametrizations of* T *that escape to infinity when* U *approaches zero do not result in any limit points of* $W(T)$*.*

Definition 3. *Using the notations of Definition 2, the Puiseux parametrization* $(U^\varsigma, \phi_2, \ldots, \phi_n)$ *is called a real Puiseux parametrization of* T *if* $\phi_i \in \mathbb{R}\langle U\rangle$*, for* $i = 2, \ldots, n$*.*

[1] This library is freely available from `www.regularchains.org`

Example 2. *Let T be again the regular chain in Example 1 with Puiseux parametrizations $\Phi_{2,3}, \Phi_{2,4}$ at $U = 0$. Then by substituting $U = 0$ in $\Phi_{2,3}, \Phi_{2,4}$, we obtain one non-trivial limit point for $W(T)$, namely $\{(X_1 = 0, X_2 = 0, X_3 = 0)\}$, for which its coordinates are real. However, none of the branches of the space curve defined by $W(T)$ is real. Hence, $W_{\mathbb{R}}(T)$ has no non-trivial limit points!*

Thus, for computing the non-trivial limit points of $Z_{\mathbb{R}}(T)$, one needs to compute the real Puiseux parametrizations of $Z_{\mathbb{R}}(T)$ when its free variable approaches zero. To do so, it is enough to have a method for detecting the real Puiseux expansions of a single polynomial. As it is explained in [CMV13], when T only contains one (bivariate) polynomial, one way of separating the real Puiseux expansions from the complex ones is to detect for which initial factors of the method of computing the Puiseux expansions, complex coefficients will appear in the computations. However, no method is proposed for general cases when T has more than one polynomial. In Section 5.1, we propose Algorithm 2 for computing real Puiseux parametrizations of regular chains of dimension one.

5.1 Real branches of bivariate polynomials

Proposition 6. *Let $\mathbb{K}$ be an algebraic number field and $f(U, Y) \in \mathbb{K}\langle U\rangle[Y]$ be square-free, monic w.r.t Y, and of degree $s > 0$ in Y. Then, for each $\ell = 1, \ldots, s$, one can compute a positive integer σ_ℓ as well as algebraic numbers $\Theta_\ell^1, \ldots, \Theta_\ell^{\sigma_\ell}$ over $\mathbb{K}$ such that*

1. *for $i = 1, \ldots, \sigma_\ell$, the algebraic number Θ_ℓ^i has a minimal polynomial of the form $h_\ell^i(Y) \in \mathbb{K}(\Theta_\ell^1, \ldots, \Theta_\ell^{i-1})[Y]$,*
2. *$f(U, Y)$ factorizes as $(Y-\chi_1(U)) \cdots (Y-\chi_s(U))$ where $\chi_\ell(U) \in \mathbb{K}(\Theta_\ell^1, \ldots, \Theta_\ell^{\sigma_\ell})((U^*))$.*

Proof. Based on Theorem 1, the existence of expansions $\chi_1(U), \ldots, \chi_s(U)$ is guaranteed.

To prove this proposition, we should show that there exist algebraic numbers $\Theta_\ell^1, \ldots, \Theta_\ell^{\sigma_\ell}$ over $\mathbb{K}$ such that $\chi_\ell(U) \in \mathbb{K}(\Theta_\ell^1, \ldots, \Theta_\ell^{\sigma_\ell})((U^*))$, for $\ell = 1, \ldots, s$.

Let $f_0 := F(U, Y)$. Then based on Theorem 1, there are $f_1, \ldots, f_{\sigma_\ell} \in \mathbb{C}((U^*))[Y]$ such that $f_i \in EHC(f_{i-1})$, for $i = 1, \ldots, \sigma_\ell$, and $f_{\sigma_\ell} = Y - \chi_\ell(U)$.

Based on Lemma 2 and Corollary 1, there is at most one algebraic number Θ_ℓ^1 with minimal polynomial $h_\ell^1(Y) \in \mathbb{K}[Y]$ (which is, indeed, computed by substituting $U = 1$ in Newton polynomial of f_0) such that $\mathbb{K}_1 := \mathbb{K}(\Theta_\ell^1)$ and $f_1 \in \mathbb{K}_1((U^*))[Y]$. Since EHC is applied recursively on polynomials f_i, thus there are algebraic numbers Θ_ℓ^i with minimal polynomials $h_\ell^i(Y) \in \mathbb{K}_{i-1}[Y]$, where $\mathbb{K}_i := \mathbb{K}_{i-1}(\Theta_\ell^i)$ and $f_i \in \mathbb{K}_i((U^*))[Y]$, for $i = 2, \ldots, \sigma_\ell$. Therefore, $f_{\sigma_\ell} \in \mathbb{K}_{\sigma_\ell}((U^*))[Y]$ and consequently, $\chi_\ell(Y) \in \mathbb{K}_{\sigma_\ell}((U^*)) = \mathbb{K}(\Theta_\ell^1, \ldots, \Theta_\ell^{\sigma_\ell})((U^*))$.

Note that EHC sometimes does a change of coordinates on the input polynomial, but this change of coordinates is within the coefficient ring of its input polynomial. Thus it does not introduce any new algebraic number. □

Proposition 6 follows from the *extended Hensel construction*. In fact, Proposition 6 gives a characterization of all the Puiseux expansions of polynomial f. This proposition shows that there is a finite extension of $\mathbb{K}$ for which $f(U, Y)$ can be written as $(Y-\chi_1(U)) \cdots (Y-\chi_s(U))$, and therefore all the coefficients of the Puiseux expansions of f are determined. Especially,

when $\mathbb{K} = \mathbb{Q}$, then determining whether or not $\chi_\ell(U)$ is a real Puiseux expansion is equivalent to the fact that each Θ_ℓ^{i-1} is a real algebraic number over $\mathbb{Q}(\Theta_\ell^1, \ldots, \Theta_\ell^{i-1})$, for $i = 1, \ldots, \sigma_\ell$.

Furthermore, based on the construction of $h_\ell^i(Y)$, all of the solutions of polynomials $h_\ell^i(Y)$ will appear in some of Puiseux expansions of $f(U, Y)$, while not all such solutions are real algebraic numbers. Therefore, it is required to encode each solution of $h_\ell^i(Y)$, including Θ_ℓ^{i-1}, "uniquely", to distinguish all solutions from each other.

Let $h(Y) \in \mathbb{K}[Y]$ be an irreducible and monic polynomial with degree s. Let also $\frac{\mathbb{K}[X_1,\ldots,X_n]}{\langle F\rangle}$ be the residue class ring of $\mathbb{K}[X_1, \ldots, X_n]$ with respect to F, where $F \subset \mathbb{K}[X_1, \ldots, X_n]$.

Remark 7. *To construct the splitting field $\mathbb{L}$ of $h(Y)$ and compute the factorization of $h(Y)$ into linear factors over $\mathbb{L}$, one can proceeds as follows.*

1. *Initialize $i := 1$, $X_i := Y$, $\mathbb{L} := \mathbb{K}$, $R_0 := \{\}$, $\mathcal{P} := \{\}$ and $\mathcal{F} := \{h(Y)\}$; the set $\mathcal{F}$ is assumed to maintain a list of univariate polynomials in Y_i irreducible over $\mathcal{L}$ and of degree at least two,*
2. *While $\mathcal{F}$ is not empty do*
   (a) *pick a polynomial $f(X_i) \in \mathcal{F}$ over $\mathbb{L}$,*
   (b) *let α_i be a root of $f(X_i)$ (in the algebraic closure of $\mathbb{K}$),*
   (c) *replace $\mathbb{L}$ by $\mathbb{L}(\alpha_i)$, that is, by adjoining α_i to $\mathbb{L}$,*
   (d) *replace T by $R_i := R_{i-1} \cup \{r_i(X_1, \ldots, X_i)\}$, where the multivariate $r_i(X_1, \ldots, X_i)$ is obtained from $f(X_i)$ after replacing the algebraic numbers $\alpha_1, \ldots, \alpha_{i-1}$ with the variables $X_1, \ldots, X_{i-1}$,*
   (e) *factor $f(X_i)$ into irreducible factors over $\mathbb{L}$, then add the obtained factors of degree 1 (resp. greater than 1) to $\mathcal{P}$ (resp. $\mathcal{F}$); when adding a factor to $\mathcal{P}$ replace X_i with Y;when adding a factor to $\mathcal{F}$, replace X_i with X_{i+1} and $\alpha_1, \ldots, \alpha_{i-1}, \alpha_i$ with $X_1, \ldots, X_{i-1}, X_i$,*
   (f) *if $\mathcal{F}$ is not empty then $i := i + 1$.*
3. *Let $s' := i$.*

At the end of this procedure, the set $R_{s'}$ is a regular chain in the polynomial ring $\mathbb{K}[X_1, \ldots, X_{s'}]$ generating a maximal ideal such that $\mathbb{K}[X_1, \ldots, X_{s'}]/\langle R_{s'}\rangle$ is isomorphic to the splitting field $\mathbb{K}(p)$ of $h(Y)$. Furthermore,

$$\mathbb{K}[Y] \subset \frac{\mathbb{K}[X_1]}{\langle R_1\rangle}[Y] \subset \cdots \subset \frac{\mathbb{K}[X_1, \ldots, X_{s'}]}{\langle R_{s'}\rangle}[Y].$$

Remark 8. *Let $R_1 := \{h(X_1)\}$. Then, there exists a positive integer $s' \leq s$ and zero-dimensional regular chains $R_i \subset \mathbb{K}[X_1, \ldots, X_{i-1}]$, for $i = 2, \ldots, s'$ such that $\mathbb{K}[Y] \subset \frac{\mathbb{K}[X_1]}{\langle R_1\rangle}[Y] \subset \cdots \subset \frac{\mathbb{K}[X_1,\ldots,X_{s'}]}{\langle R_{s'}\rangle}[Y]$, where $h(Y)$ admits at least one linear factor over $\frac{\mathbb{K}[X_1,\ldots,X_i]}{\langle R_i\rangle}[Y]$, for each i; furthermore, $\frac{\mathbb{K}[X_1,\ldots,X_{s'}]}{\langle R_{s'}\rangle}[Y]$ is the splitting field of $h(Y)$. This remark is derived from [LM83] and [Tra76].*

Using regular chains $R_1, \ldots, R_{s'}$ in Remark 8, one can encode all the solutions of polynomial $h(Y)$, "uniquely". It is worth mentioning that the Split command of the PolynomialTools package in MAPLE computes the regular chains $R_1, \ldots, R_{s'}$, implicitly.

Example 3. *Suppose $h(Y) := Y^3 + Y^2 + 3$. Using the* Split *command in* MAPLE*, one obtains $R_1 := \{X_1^3 + X_1^2 + 3\}$ and $R_2 := R_1 \cup \{X_2^2 + (1 + X_1)\, X_2 + X_1^2 + X_1\}$, for which $\frac{\mathbb{Q}[X_1,X_2]}{\langle R_2\rangle}[Y]$ is the*

Algorithm 2 Real Puiseux expansions of f when $U \to 0$

procedure REALPUISEUXEXPANSIONS($f(U, Y), U = 0$)
  $\mathcal{B}$:= Puiseux expansions of $f(U, Y)$ at $U = 0$;
  $\mathcal{R} := \{\}$;
  for $\chi(U) \in \mathcal{B}$ **do**
    let $\chi(U) \in \mathbb{K}((U^*))(\Theta^1, \ldots, \Theta^\sigma)$;
    let $R^i_{j_i} \subset \mathbb{K}[X_{i,1}, \ldots, X_{i,j_i}]$ be the zero-dimensional regular chain encoding the algebraic number Θ^i
    let C be a regular chain encoding the field $\mathbb{K}$
    $\mathcal{F} := C \cup R^1_{j_1} \cup \cdots \cup R^\sigma_{j_\sigma}$;
    if RealTriangularize($\mathcal{F}$) $\neq \emptyset$ **then**
      $\mathcal{R} := \mathcal{R} \cup \{\chi(U)\}$;
    end if
  end for
  return $\mathcal{R}$;
end procedure

splitting field of $h(Y)$. Using the command RealTriangularize *of the* RegularChains *library, we can check that $Z_{\mathbb{R}}(R_1)$ contains one real solution, while the set $Z_{\mathbb{R}}(R_2)$ does not have any real solutions.*

Definition 4. *Let Θ be a root of $h(Y)$. Let also j be the smallest integer for which $\Theta \in \frac{\mathbb{K}[X_1,\ldots,X_j]}{\langle R_j \rangle}$, then R_j is called the encoding regular chain corresponding to Θ.*

In fact, the initial problem of determining whether Θ is a real algebraic number over $\mathbb{K}$ is equivalent to check whether or not $Z_{\mathbb{R}}(R_j)$ has a real solution or not over $\mathbb{K}$. Furthermore, $\mathbb{K}$ must be a real extension of $\mathbb{Q}$. To make sure that a polynomial system has real solutions, one can use $RealTriangularize$ command of the $RegularChains$ Library in Maple. In fact, the command $RealTriangularize$ computes the real solutions of the polynomial system defined by F, where $F \subset \mathbb{Q}[X_1, \ldots, X_n]$. Thus, for checking whether or not Θ is a real algebraic number over $\mathbb{K}$, using $RealTriangularize$, more considerations are required due to the constraint imposed by the coefficient ring. To remove this constraint, since $\mathbb{K}$ is an algebraic extension of $\mathbb{Q}$, thus one can compute a zero-dimensional regular chain $C \subset \mathbb{Q}[Y_1, \ldots, Y_m]$ (for some m) such that $\frac{\mathbb{Q}[Y_1,\ldots,Y_m]}{\langle C \rangle}$ is isomorphic to $\mathbb{K}$. This means that one can apply $RealTriangularize$ on the system defined by $C \cup R_j \subset \mathbb{Q}[Y_1, \ldots, Y_m, X_1, \ldots, X_j]$; if this system has any real solutions, then we deduce that Θ is a real algebraic number over $\mathbb{K}$.

Algorithm 2 implements the above idea to distinguish real Puiseux expansions of bivariate polynomial f at $U = 0$. This algorithm, first, computes all of the Puiseux expansions of the polynomial f at $U = 0$ and then determines which one is a real expansion for f. Based on Proposition 6, each Puiseux expansion $\chi(U)$ of f belongs to $\mathbb{K}((U^*))(\Theta^1, \ldots, \Theta^\sigma)$ for some $\Theta^1, \ldots, \Theta^\sigma$. Let C be the regular chain encoding the number field $\mathbb{K}$ and $\mathcal{R}^i_{j_i} \subset \mathbb{K}[X_{i,1}, \ldots, X_{i,j_i}]$ the zero-dimensional regular chain encoding the algebraic number Θ^i. Then if the polynomial system defined by $C \cup R^1_{j_1} \cup \cdots \cup R^\sigma_{j_\sigma}$ has any real solutions, then we deduce that $\chi(U)$ is a real Puiseux expansion of f.

5.2 Real branches of space curves

Proposition 7. *With the notations of Definition 2, let* $(U^{\varsigma}, \phi_2, \ldots, \phi_n)$ *be a Puiseux parametrization of the regular chain* T *around* $U = 0$*. Then, for each* $j = 2, \ldots, n$*, one can compute algebraic numbers* $\Theta_j^1, \ldots, \Theta_j^{\sigma_j}$ *over* $\mathbb{K}_{j-1}$ *such that* $\phi_j(U) \in \mathbb{K}_j[U]$*, where* $\mathbb{K}_1 := \mathbb{Q}$ *and* $\mathbb{K}_j := \mathbb{K}_{j-1}(\Theta_j^1, \ldots, \Theta_j^{\sigma_j})$ *for some non-negative integer* σ_j*.*

Proof. To prove this proposition, it is enough to prove that $\chi_j(U) \in \mathbb{K}_j[U]$, for $j = 2, \ldots, n$. We prove this by induction on j. For $j = 2$, $(U^{\varsigma}, \chi_2(U))$ is a Puiseux parametrization of the bivariate polynomial $t_1(U, X_2)$ around $U = 0$. Since $t_1(U, X_2) \in \mathbb{Q}[U, X_2]$, thus according to Proposition 6, there exist algebraic numbers $\Theta_2^1, \ldots, \Theta_2^{\sigma_2}$ over $\mathbb{Q}$ such that $\chi_2(U) \in \mathbb{Q}(\Theta_2^1, \ldots, \Theta_2^{\sigma_2})$. Suppose $\chi_{j-1}(U) \in \mathbb{K}_{j-1}[U]$. Thus, $\chi_j(U)$ is a Puiseux expansion of bivariate polynomial

$$t_{j-1}(U^{\varsigma_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j)$$

which, in turn, belongs to $\mathbb{K}_{j-1}[U, X_j]$ by induction hypothesis step. Based on Proposition 6, there exists algebraic numbers $\Theta_j^1, \ldots, \Theta_j^{\sigma_j}$ over $\mathbb{K}_{j-1}$ such that $\chi_i(U) \in \mathbb{K}_{j-1}(\Theta_j^1, \ldots, \Theta_j^{\sigma_j})[U]$. Now if we let $\mathbb{K}_j := \mathbb{K}_{j-1}(\Theta_j^1, \ldots, \Theta_j^{\sigma_j})$, this completes the proof. □

Proposition 8. *Following up on Proposition 7, the Puiseux parametrization* $(U^{\varsigma}, \phi_2(U), \ldots, \phi_n(U))$ *is a real Puiseux parametrization of* T *if and only if* $\mathbb{K}_n$ *is a real extension of* $\mathbb{Q}$*.*

Proof. The correctness of the relation $\mathbb{K}_1 := \mathbb{Q} \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_n$ is trivial based on the constructive proof of Proposition 7. Thus for determining whether or not the Puiseux parametrization $(U^{\varsigma}, \phi_2, \ldots, \phi_n)$ is real, it is enough to check if $\mathbb{K}_n$ is a real extension over $\mathbb{Q}$. □

Algorithm 3 Real Puiseux parametrizations of T when $U \to 0$

procedure REALREGULARCHAINBRANCHES($T, U = 0$)
  $\mathcal{R} := \{\}$;
  $\varsigma_1 = 1$
  for j **from** 2 **to** n **do**
    $\mathcal{R}_j := \{\}$;
    for $(\chi_2(U), \ldots, \chi_{j-1}(U)) \in \mathcal{R}$ **do**
      $\mathcal{B} :=$ *RealPuiseuxExpansions*$(t_{j-1}(U^{\varsigma_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j), 0)$
      $\varsigma_j =$ *RamificationIndex*$(t_{j-1}(U^{\varsigma_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j), 0)$
      if $\mathcal{B} \neq \emptyset$ **then**
        let $\mathcal{B} := \{\chi_j^1(U), \ldots, \chi_j^{\ell_j}(U)\}$
        $\mathcal{R}_j := \mathcal{R}_j \cup \left\{\left(\chi_2(U), \ldots, \chi_{j-1}(U), \chi_j^1(U)\right), \ldots, \left(\chi_2(U), \ldots, \chi_{j-1}(U), \chi_j^{\ell_j}(U)\right)\right\}$
      end if
    end for
    $\mathcal{R} := \mathcal{R}_j$
  end for
  return $\mathcal{R}$;
end procedure

Algorithm 3 computes the real Puiseux parametrizations corresponding to regular chain T. Based on Definition 2, for computing the Puiseux parametrizations of T, one needs to compute the Puiseux parametrizations $(U^{s_j}, \chi_j(U))$ of the bivariate polynomial

$$t_{j-1}(U^{s_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j),$$

for $j = 2, \ldots, n$. If any of such parametrization has complex coefficients, then it would not result in a real Puiseux parametrization for regular chain T. Thus, we should only consider the real Puiseux parametrizations of bivariate polynomials $t_{j-1}(U^{s_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j)$. To do so, in Algorithm 3 at line 7, we call Algorithm 2 for computing the real Puiseux expansions of bivariate polynomials to filter out the expansions that would not contribute in building a real Puiseux parametrization for regular chain T.

Based on Definition 2, for computing the Puiseux parametrizations of T, one needs to compute the Puiseux parametrizations $(U^{s_j}, \chi_j(U))$ of the bivariate polynomial

$$t_{j-1}(U^{s_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j),$$

for $j = 2, \ldots, n$. If any of such parametrization has complex coefficients, then it would not result in a real Puiseux parametrization for regular chain T. Thus, we should only consider the real Puiseux parametrizations of bivariate polynomials $t_{j-1}(U^{s_{j-1}}, \chi_2(U), \ldots, \chi_{j-1}(U), X_j)$. To do so, one needs to use Algorithm 2, successively.

Chapter 6

Regular semi-algebraic systems and limits of real rational functions

Fix a real number $\rho > 0$ and let D^*_ρ be the punctured ball

$$D^*_\rho \;=\; \{(x_1, \ldots, x_n) \in \mathbb{R}^n \;\mid\; 0 < \sqrt{x_1^2 + \cdots + x_n^2} < \rho\}.$$

Let $q : \mathbb{R}^n \longrightarrow \mathbb{R}$ be a rational function defined on D^*_ρ.

Notation 2. *Let $\chi(q)$ be the subset of $\mathbb{R}^n$ (regarded as affine space) where the gradient $\nabla_{x_1,\ldots,x_n} q$ of q at $(x_1, \ldots, x_n)$ and the vector $(x_1, \ldots, x_n)$ of $\mathbb{R}^n$ (regarded as vector space) are co-linear. For $n = 2$, writing (x, y) for (x_1, x_2), we have*

$$\chi(q) \;=\; \{(x, y) \in \mathbb{R}^2 \;\mid\; y\frac{\partial q}{\partial x} - x\frac{\partial q}{\partial y} = 0\}.$$

In higher dimension, using McCoy theorem, the real algebraic set $\chi(q)$ is the vanishing locus of all 2-by-2 minors of the 2-by-n matrix where rows are $\nabla_{x_1,\ldots,x_n} q$ and $(x_1, \ldots, x_n)$.

Definition 5. *Let S be a semi-algebraic set of dimension at least 1 and such that the origin of $\mathbb{R}^n$ belongs to the closure $\overline{Z_{\mathbb{R}}(S)}$ of $Z_{\mathbb{R}}(S)$ in the Euclidean topology. Let $L \in \mathbb{R}$. We say that, when $(x_1, \ldots, x_n) \in \mathbb{R}^n$ approaches the origin along S, the limit of the rational function $q(x_1, \ldots, x_n)$ exists and equals L, whenever for all $\varepsilon > 0$, there exists $0 < \delta$ such that for all $(x_1, \ldots, x_n) \in S \cap D^*_\delta$ the inequality $|q(x_1, \ldots, x_n) - L| < \varepsilon$ holds. When this holds, we write*

$$\lim_{\substack{(x_1, \ldots, x_n) \to (0, \ldots, 0) \\ (x_1, \ldots, x_n) \in S}} q(x_1, \ldots, x_n) = L$$

Lemma 3 is a direct generalization of Proposition 1 in [CMV13] (bivariate case) and Lemma 7 is a less direct generalization of one of the properties established in Proposition 5 of [VHC17] (trivariate case).

Lemma 8 and Lemma 9 are the core results supporting Algorithm 7 (see Section 7) when dealing with rational functions with an arbitrary number of variables. These results are new and, thus, have no counterparts either in [CMV13,VHC17] or in our ISSAC 2016 paper [AKM16].

We provide proofs for those results since they are essential for understanding the algorithms presented in Section 7. Meanwhile, Lemma 4 follows from Lemma 3 and elementary reasoning about limits; hence we omit its proof.

Lemma 3. *For all $L \in \mathbb{R}$ the following two assertions are equivalent:*

(*i*) $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q(x_1,\ldots,x_n)$ *exists and equals L,*

(*ii*) $\lim_{\substack{(x_1,\ldots,x_n)\to(0,\ldots,0)\\(x_1,\ldots,x_n)\in\chi(q)}} q(x_1,\ldots,x_n)$ *exists and equals L.*

Proof. Clearly the first assertion implies the second one. Next, we assume that the second one holds and we prove that the first one holds as well. Hence, we assume that for all $\varepsilon > 0$, there exists $0 < \delta < \rho$ such that for all $(x_1,\ldots,x_n) \in \chi(q) \cap D^*_\delta$ the inequality $|q(x_1,\ldots,x_n) - L| < \varepsilon$ holds. We fix $\varepsilon > 0$. For every $r > 0$, we define $C_r = \{(x_1,\ldots,x_n) \in \mathbb{R}^n \mid \sqrt{x_1^2 + \cdots + x_n^2} = r\}$. For all $0 < r < \rho$, we choose $t_1(r)$ (resp. $t_2(r)$) minimizing (resp. maximizing) q on C_r. Applying the method of Lagrange multipliers, we have $t_1(r), t_2(r) \in \chi(q)$, for all $0 < r < \rho$. Observe that for all $(x_1,\ldots,x_n) \in \mathbb{R}^n$, with $r := \sqrt{x_1^2 + \cdots + x_n^2} < \rho$, we have $q(t_1(r)) - L \leq q(x_1,\ldots,x_n) - L \leq q(t_2(r)) - L$. From the assumption and the definitions of $t_1(r), t_2(r)$, there exists $0 < \delta < \rho$ such that, for all $r < \delta$, we have $-\varepsilon < q(t_1(r)) - L$ and $q(t_2(r)) - L < \varepsilon$. Therefore, there exists $0 < \delta < \rho$ such that for all $(x_1,\ldots,x_n) \in D^*_\delta$ the inequality $|q(x_1,\ldots,x_n) - L| < \varepsilon$ holds. □

Lemma 4. *Let $R_1,\ldots,R_e$ be regular semi-algebraic systems forming a triangular decomposition of $\chi(q)$ in the sense of Proposition 4. Then, for all $L \in \mathbb{R}$ the following two assertions are equivalent:*

(*i*) $\lim_{\substack{(x_1,\ldots,x_n)\to(0,\ldots,0)\\(x_1,\ldots,x_n)\in\chi(q)}} q(x_1,\ldots,x_n)$ *exists and equals L.*

(*ii*) *for all $i \in \{1,\ldots,e\}$ such that $Z_{\mathbb{R}}(R_i)$ has dimension at least 1 and the origin belongs to $\overline{Z_{\mathbb{R}}(R_i)}$, we have* $\lim_{\substack{(x_1,\ldots,x_n)\to(0,\ldots,0)\\(x_1,\ldots,x_n)\in Z_{\mathbb{R}}(R_i)}} q(x_1,\ldots,x_n)$ *exists and equals L.*

Lemma 5. *Assume $n \geq 3$. Let $S = [Q, T, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1,\ldots,X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension d with $n > d \geq 1$. Then the number of d-dimensional semi-algebraic sets which are the intersection of $Z_{\mathbb{R}}(S)$ and a sphere (or an ellipsoid) centred at the origin is finite.*

Proof. Assume by contradiction there are infinitely many of such d-dimensional semi-algebraic sets $W_1, W_2, \ldots, W_i, \ldots$ which are intersection of $Z_{\mathbb{R}}(S)$ and a sphere (or an ellipsoid) centred at the origin. Consider the sequence $V_1 := W_1$, $V_2 := W_2 \setminus W_1$, …, $V_i := W_i \setminus (V_1 \cup \cdots \cup V_{i-1})$, …. Observe that the semi-algebraic sets V_i are disjoint (by construction) and d-dimensional (by the nature of spheres and ellipsoids). It follows from Theorem 5.21 in [BPR06] that if a semi-algebraic set X contains all V_i's, the set X must have dimension at least $d+1$. However, all V_i's are contained in $Z_{\mathbb{R}}(S)$ which has dimension d. A contradiction. □

Lemma 6. *Let $h \in \mathbb{R}[X_1,\ldots,X_n]$ be of positive degree in X_n. Assume that there exists a real number λ such that $\nabla h(p) = \lambda p$ holds for all p in a neighbourhood V_0 of the origin in $\mathbb{R}^n$. Let also $U_0 \subset \mathbb{R}^{n-1}$ be a neighbourhood of the origin in $\mathbb{R}^{n-1}$ such that the standard projection of V_0 onto $(X_1,\ldots,X_{n-1})$ contains U_0. Assume the leading coefficient c of h in X_n and the discriminant Δ of h in X_n vanish nowhere on U_0. Then, there exists a smooth function $u : U_0 \longrightarrow \mathbb{R}$ for which*

$$h(x_1,\ldots,x_{n-1},u(x_1,\ldots,x_{n-1})) = 0 \tag{6.1}$$

holds, for all $(x_1,\ldots,x_{n-1}) \in U_0$. Moreover, the graph of every smooth function $u : U_0 \longrightarrow \mathbb{R}$ satisfying Relation (6.1) is contained in a sphere centred at the origin.

Proof. We view h as a parametric polynomial in X_n with $X_1, \ldots, X_{n-1}$ as parameters. Since the leading coefficient c of h in X_n and the discriminant Δ of h in X_n vanish nowhere on U_0, it follows from Section 1.4 that the intersection of U_0 and the discriminant variety of h is empty. Therefore, there exists a smooth analytic function $u : U_0 \longrightarrow \mathbb{R}$ such that Equation (6.1) holds for all $(x_1, \ldots, x_{n-1}) \in U_0$. Let u be such a function and define

$$W = \{(x_1, \ldots, x_{n-1}, x_n) \mid x_1, \ldots, x_{n-1} \in U_0 \text{ and } x_n = u(x_1, \ldots, x_{n-1})\}.$$

Thus, the set W is the graph of u. For any $t \in W$, the normal vector of W at t is given by

$$n(t) = \frac{(-\partial u/\partial X_1, \ldots, -\partial u/\partial X_{n-1}, 1)}{\sqrt{(\partial u/\partial X_1)^2 + \cdots + (\partial u/\partial X_{n-1})^2 + 1}}.$$

Using Equation (6.1) and the hypothesis on ∇h, elementary calculations yield

$$n(t) = \frac{(x_1, \ldots, x_{n-1}, u(x_1, \ldots, x_{n-1}))}{\sqrt{x_1^2 + \cdots + x_{n-1}^2 + u^2(x_1, \ldots, x_{n-1})}}$$

which results in the following equalities:

$$\begin{cases} \frac{X_i}{\sqrt{X_1^2+\cdots+X_{n-1}^2+u^2(X_1,\ldots,X_{n-1})}} = -\frac{\partial u/\partial X_i}{\sqrt{(\partial u/\partial X_1)^2+\cdots+(\partial u/\partial X_{n-1})^2+1}} \quad , \quad i = 1, \ldots, n-1 \\ \frac{u(X_1,\ldots,X_{n-1})}{\sqrt{X_1^2+\cdots+X_{n-1}^2+u^2(X_1,\ldots,X_{n-1})}} = \frac{1}{\sqrt{(\partial u/\partial X_1)^2+\cdots+(\partial u/\partial X_{n-1})^2+1}} \end{cases} \tag{6.2}$$

The last equality in Relation (6.2) implies that we have:

$$u(X_1, \ldots, X_{n-1}) = \frac{\sqrt{X_1^2 + \cdots + X_{n-1}^2 + u^2(X_1, \ldots, X_{n-1})}}{\sqrt{(\partial u/\partial X_1)^2 + \cdots + (\partial u/\partial X_{n-1})^2 + 1}}.$$

Consequently, we obtain the following system of PDEs:

$$\left\{ u(X_1, \ldots, X_{n-1})\, \partial u/\partial X_i = -X_i \quad , \text{ for } i = 1, \ldots, n-1. \right. \tag{6.3}$$

Now for $i = 1$, we integrate both sides of Equation (6.3) with respect to X_1. There exists a differentiable function $F_2(X_2, \ldots, X_{n-1})$ such that we have:

$$\frac{u^2(X_1, \ldots, X_{n-1})}{2} = \frac{-X_1^2}{2} + F_2(X_2, \ldots, X_{n-1}). \tag{6.4}$$

Now by taking the derivative of both sides of Equation (6.4) with respect to X_2, we have

$$u\, \partial u/\partial X_2 = \partial F_2/\partial X_2.$$

After substitution of the latter equality in the equation $u\, \partial u/\partial X_2 = -X_2$, there exists a differentiable function $F_3(X_3, \ldots, X_{n-1})$ such that we have:

$$\frac{-X_2^2}{2} = F_2(X_2, \ldots, X_{n-1}) + F_3(X_3, \ldots, X_{n-1}).$$

By continuing in the same manner, we have

$$\frac{-X_{i-1}^2}{2} = F_{i-1}(X_{i-1}, \ldots, X_{n-1}) + F_i(X_i, \ldots, X_{n-1}),$$

for $i = 2, 3, \ldots, n-2$. But for $i = n-1$, we have $u\,\partial u/\partial X_{n-1} = \partial F_{n-1}/\partial X_{n-1}$. After substitution of the latter equality in $u\,\partial u/\partial X_{n-1} = -X_{n-1}$, there exists a constant C such that we have:

$$\frac{-X_{n-1}^2}{2} = F_{n-1}(X_{n-1}) + C.$$

Therefore. we have

$$\frac{u^2(X_1, \ldots, X_{n-1})}{2} = -\frac{X_1^2}{2} - \cdots - \frac{X_{n-1}^2}{2} + C.$$

Let $\alpha = (\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$ be a point of W. Since $u(\alpha_1, \ldots, \alpha_{n-1}) = \alpha_n$ holds, we have $C = 1/2(\alpha_1^2 + \cdots + \alpha_n^2)$. We deduce:

$$u(X_1, \ldots, X_{n-1}) = \sqrt{r^2 - X_1^2 - \cdots - X_{n-1}^2},$$

where we define $r^2 := \alpha_1^2 + \cdots + \alpha_n^2$. Finally, we conclude that W is a neighbourhood of $p \in D_\rho^*$ contained in a sphere centred at the origin. □

Lemma 7. *Assume $n \geq 3$. Let $S = [Q, \{t_n\}, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_\mathbb{R}(S)$ has dimension $d := n - 1$, and the closure $\overline{Z_\mathbb{R}(S)}$ contains the origin. W.l.o.g. we assume that* $\mathrm{mvar}(t_n) = X_n$ *holds. Let $\mathcal{M}$ be the $2 \times n$ matrix with the vector $(X_1, \ldots, X_n)$ as first row and the gradient vector $\nabla t_n = \left(\frac{\partial t_n}{\partial X_1} \cdots \frac{\partial t_n}{\partial X_n}\right)$ as second row. Then, there exists a non-empty set $O \subset D_\rho^* \cap Z_\mathbb{R}(S)$, which is open relatively to $Z_\mathbb{R}(S)$, such that $\mathcal{M}$ is full rank at any point of O, and the origin is in the closure of O.*

Proof. We shall first prove the following claim.

Claim: Assume that there exists r such that $0 < r < \rho$ holds and $\mathcal{M}$ is not full rank at any point of $D_r^* \cap Z_\mathbb{R}(S)$. Then, there exists r' such that $0 < r' < r$ holds and $S_{r'}$, the r'-radius sphere centred at the origin, intercepts $Z_\mathbb{R}(S)$ on a semi-algebraic set of dimension $n - 1$.

Proof of the Claim: Since the origin is in the closure of $Z_\mathbb{R}(S)$, we know that $D_r^* \cap Z_\mathbb{R}(S)$ is not empty. W.l.o.g. we can assume that $Z_\mathbb{R}(S) \subseteq D_r^*$ holds. Indeed, if this was not the case, we could decompose $D_r^* \cap Z_\mathbb{R}(S)$ into finitely many regular semi-algebraic systems and reason with each of those which has the origin of $\mathbb{R}^n$ in the topological closure (w.r.t. Euclidean topology) of its zero set. The standard projection of $Z_\mathbb{R}(S)$ onto $(X_1, \ldots, X_{n-1})$ is an open set U_0 of $\mathbb{R}^{n-1}$. We apply Lemma 6 with $h := t_n$ and $V_0 := Z_\mathbb{R}(S)$. The conclusion of the claim follows.

Lemma 5 conclude: W.l.o.g. we can assume that $Z_\mathbb{R}(S)$ does not intercept sphere centred at the origin on semi-algebraic sets W_i of dimension $n - 1$ for $i = 1, 2, \ldots, m$ for some $m \geq 0$. Indeed, if this was the case, we can remove all such W_i from $Z_\mathbb{R}(S)$ (since such W_i doesn't have the origin of $\mathbb{R}^n$ in its topological closure) and keep reasoning with each component of $Z_\mathbb{R}(S) \setminus \cup_{i=1}^m W_i$ which contains the origin of $\mathbb{R}^n$ in its topological closure.

As a consequence of the above claims, for every r such that $0 < r < \rho$ holds, there exists a point p of $D_r^* \cap Z_\mathbb{R}(S)$ at which $\mathcal{M}$ is full rank. Therefore, for all $r > 0$ small enough, the

set $D_r^* \cap Z_{\mathbb{R}}(S)$ contains a point p_r, as well as a neighbourhood N_r of p_r (due to the full rank characterization in terms of minors) such that N_r is open relatively to $Z_{\mathbb{R}}(S)$ and $\mathcal{M}$ is full rank at any point of N_r. Taking the union of those neighbourhoods N_r finally yields the conclusion of the lemma. □

Lemma 9 extends Lemma 7 from a regular semi-algebraic system of dimension $n-1$ to a regular semi-algebraic system of arbitrary dimension. But, before stating and proving Lemma 9, let us look, with Lemma 8, to the case of a regular semi-algebraic system of dimension $n-2$.

Lemma 8. *Assume that $n \geq 3$ holds. Let $S = [Q, \{t_n, t_{n-1}\}, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension $n-2$, and the closure $\overline{Z_{\mathbb{R}}(S)}$ contains the origin. Note that $\{t_n, t_{n-1}\}$ is a regular chain and without loss of generality, we can assume that* $\mathrm{mvar}(t_n) = X_n$ *and* $\mathrm{mvar}(t_{n-1}) = X_{n-1}$ *holds. Consider the matrix*

$$\mathcal{M} = \begin{bmatrix} X_1 & X_2 & X_3 & \cdots & X_n \\ \frac{\partial t_n}{\partial X_1} & \frac{\partial t_n}{\partial X_2} & \frac{\partial t_n}{\partial X_3} & \cdots & \frac{\partial t_n}{\partial X_n} \\ \frac{\partial t_{n-1}}{\partial X_1} & \frac{\partial t_{n-1}}{\partial X_2} & \frac{\partial t_{n-1}}{\partial X_3} & \cdots & \frac{\partial t_{n-1}}{\partial X_n} \end{bmatrix}.$$

Then, there exists a non-empty set $O \subset D_\rho^* \cap Z_{\mathbb{R}}(S)$, which is open relatively to $Z_{\mathbb{R}}(S)$ and which satisfies $\underline{o} \in \overline{O}$ (that is, the origin is in the closure of O) such that $\mathcal{M}$ is full rank at any point of O.

Proof. The proof consists of two main steps. The first one uses a PDE argument and borrows ideas from the proof of Lemma 6 The second step uses a topological argument and follows the proof of Lemma 7.

Let O be an open set in $Z_{\mathbb{R}}(S)$ with $\underline{o} \in \overline{O}$. We view t_n (resp. t_{n-1}) as a parametric polynomial in X_n (resp. X_{n-1}) with $X_1, \ldots, X_{n-1}$ (resp. $X_1, \ldots, X_{n-2}$) as parameters. Let also $U_0 \subset \mathbb{R}^{n-1}$ be a neighbourhood of the origin in $\mathbb{R}^{n-1}$ and $V_0 \subset \mathbb{R}^{n-2}$ be a neighbourhood of the origin in $\mathbb{R}^{n-2}$ such that the standard projection of O onto $(X_1, \ldots, X_{n-1})$ contains U_0 and the standard projection of O onto $(X_1, \ldots, X_{n-2})$ contains V_0.

Since the leading coefficient and discriminant of t_n (resp. t_{n-1}) vanish nowhere on U_0 (resp. V_0), it follows from Section 1.4 that the intersection of U_0 (resp. V_0) and the discriminant variety of t_n (resp. t_{n-1}) is empty. Therefore, there exist smooth analytic functions $u(X_1, \ldots, X_{n-1}) : U_0 \to \mathbb{R}$ and $v(X_1, \ldots, X_{n-2}) : V_0 \to \mathbb{R}$ such that we have:

$$t_n(X_1, \ldots, X_{n-2}, v, u) = 0 \text{ and } t_{n-1}(X_1, \ldots, X_{n-2}, v) = 0.$$

Now assume that the above matrix M is not full rank at any point of O. Therefore all minors of M are zero in O. Let us look at the $n-2$ minors m_i, where m_i is the determinant of sub-matrix of M obtained with the i-th column and last two columns for $i = 1, \ldots, (n-2)$. From $m_i = 0$, we derive the following:

$$X_n u_v v_{X_i} + X_{n-1} v_{X_i} + X_n u_{X_i} + X_i = 0 \tag{6.5}$$

for $i = 1, \ldots, (n-2)$. Observe that we have $\int (u_v v_{X_i} + u_{X_i}) dX_i = u + c_0$ and $\int v_{X_i} dX_i = v + c_1$. Now for $i = 1$, we integrate of the first equation (that is, for $i = 1$) from 6.5 with respect to X_1. It follows that there exists a differentiable function $F_1(X_2, \ldots, X_{n-2})$ such that we have

$$X_n u + X_{n-1} v + \frac{X_1^2}{2} + F_1(X_2, \ldots, X_{n-2}) = 0.$$

Now by taking derivative with respect to X_2 and substituting in the second equation (that is, for $i = 2$) in 6.5, we have $\frac{\partial}{\partial X_2} F_1(X_2, \ldots, X_{n-2}) = X_2$. Then, there exists a differentiable function $F_2(X_3, \ldots, X_{n-2})$ such that $F_1(X_2, \ldots, X_{n-2}) = \frac{X_2^2}{2} + F_2(X_3, \ldots, X_{n-2})$. Hence, we have:

$$X_n u + X_{n-1} v + \frac{X_1^2}{2} + \frac{X_2^2}{2} + F_2(X_3, \ldots, X_{n-2}) = 0$$

Continuing in this manner, we have, for some differentiable function $F_{n-3}(X_{n-2})$,

$$X_n u + X_{n-1} v + \frac{X_1^2}{2} + \ldots + \frac{X_{n-3}^2}{2} + F_{n-3}(X_{n-2}) = 0.$$

By taking derivative with respect to X_{n-2} and substituting in the last equation (that is, for $i = n-2$) in 6.5, we have $\frac{\partial}{\partial X_{n-2}} F_{n-3}(X_{n-2}) = X_{n-2}$. Therefore, $F_{n-3}(X_{n-2}) = \frac{X_{n-2}^2}{2} + c$ for some constant number c. Hence, we have:

$$X_n u + X_{n-1} v + \frac{X_1^2}{2} + \frac{X_2^2}{2} + \ldots + \frac{X_{n-2}^2}{2} + c = 0. \tag{6.6}$$

Using definition of u and v, we have $X_n = u(X_1, \ldots, X_{n-2}, X_{n-1})$ and $X_{n-1} = v(X_1, \ldots, X_{n-2})$, therefore the graph of equation 6.6 is an ellipsoid centred at the origin.

Now, we proceed with the second step of the proof and follow the proof of Lemma 7. We start with a claim.

Claim: Assume that there exists r such that $0 < r < \rho$ holds and $\mathcal{M}$ is not full rank at any point of $D_r^* \cap Z_{\mathbb{R}}(S)$. Then, there exists r' such that $0 < r' < r$ holds and $E_{r'}$, the ellipsoid as in equation 6.6 for $c = -r'^2$ (centred at the origin), intercepts $Z_{\mathbb{R}}(S)$ on a semi-algebraic set of dimension $n - 2$.

Proof of the Claim: Since the origin is in the closure of $Z_{\mathbb{R}}(S)$, we know that $D_r^* \cap Z_{\mathbb{R}}(S)$ is not empty. W.l.o.g. we can assume that $Z_{\mathbb{R}}(S) \subseteq D_r^*$ holds. Indeed, if this was not the case, we could decompose $D_r^* \cap Z_{\mathbb{R}}(S)$ into finitely many regular semi-algebraic systems and reason with each of those which has the origin of $\mathbb{R}^n$ in the topological closure (w.r.t. Euclidean topology) of its zero set. The standard projection of $Z_{\mathbb{R}}(S)$ onto $(X_1, \ldots, X_{n-1})$ is an open set U_0 of $\mathbb{R}^{n-1}$ and the standard projection of $Z_{\mathbb{R}}(S)$ onto $(X_1, \ldots, X_{n-2})$ is an open set V_0 of $\mathbb{R}^{n-1}$. We apply argument before this claim on t_n and t_{n-1} for $O := Z_{\mathbb{R}}(S)$. The conclusion of the claim follows.

Now we use Lemma 5. W.l.o.g. we can assume that $Z_{\mathbb{R}}(S)$ does not intercept an ellipsoid centred at the origin on semi-algebraic sets W_k's of dimension $d-1$ where $k = 1, \ldots, m$. Indeed, if this was the case, then we could remove all such W_k from $Z_{\mathbb{R}}(S)$ (since such W_k doesn't have the origin of $\mathbb{R}^n$ in its topological closure) and keep reasoning with each component of $Z_{\mathbb{R}}(S) \setminus \cup_{k=1}^m W_i$ which contains the origin of $\mathbb{R}^n$ in its topological closure.

As a consequence of the above claims, for every r such that $0 < r < \rho$ holds, there exists a point p of $D_r^* \cap Z_{\mathbb{R}}(S)$ at which $\mathcal{M}$ is full rank. Therefore, for all $r > 0$ small enough, the set $D_r^* \cap Z_{\mathbb{R}}(S)$ contains a point p_r, as well as a neighbourhood N_r of p_r (due to the full rank characterization in terms of minors) such that N_r is open relatively to $Z_{\mathbb{R}}(S)$ and $\mathcal{M}$ is full rank at any point of N_r. Taking the union of those neighbourhoods N_r finally yields the conclusion of the lemma. □

Lemma 9 extends Lemma 8 from a regular semi-algebraic system of dimension $n - 2$ to a regular semi-algebraic system of arbitrary dimension. The proof techniques are similar.

Lemma 9. *Assume that $n \geq 3$ holds. Let $S = [Q, T, P_>]$ be a regular semi-algebraic system of $\mathbb{Q}[X_1, \ldots, X_n]$ such that $Z_{\mathbb{R}}(S)$ has dimension d, with $n > d \geq 2$, and the closure $\overline{Z_{\mathbb{R}}(S)}$ contains the origin. W.l.o.g. we can assume that the polynomials $t_{d+1}, \ldots, t_n$ forming the regular chain T have main variables $X_{d+1}, \ldots, X_n$. Let $\mathcal{M}$ be the $(n-d+1) \times n$ matrix whose first row is the vector $(X_1, \ldots, X_n)$ and, for $j = d+1, \ldots, n$, whose $(j-d+1)$-th row is the gradient vector*

$$\nabla t_j = \left(\frac{\partial t_j}{\partial X_1} \ \cdots \ \frac{\partial t_j}{\partial X_n} \right)$$

where t_j is the polynomial of T with $\mathrm{mvar}(t_j) = X_j$. Then, there exists a non-empty set $O \subset D^*_\rho \cap Z_{\mathbb{R}}(S)$, which is open relatively to $Z_{\mathbb{R}}(S)$ and which satisfies $\underline{o} \in \overline{O}$ (that is, the origin is in the closure of O) such that $\mathcal{M}$ is full rank at any point of O.

Proof. Let O an open set in $Z_{\mathbb{R}}(S)$ with $\underline{o} \in \overline{O}$. We view t_ι for $\iota = n-d+1, \ldots, n$ as a parametric polynomial in X_ι with $X_1, \ldots, X_{\iota-1}$ as parameters. Let also $V_\iota \subset \mathbb{R}^{\iota-1}$ be a neighbourhood of the origin in $\mathbb{R}^{\iota-1}$ such that the standard projection of O onto $(X_1, \ldots, X_{\iota-1})$ contains V_ι.

Since the leading coefficient and discriminant of t_i vanish nowhere on V_i, it follows from Section 1.4 that the intersection of V_i and the discriminant variety of t_i is empty. Therefore, there exist smooth analytic functions

$$u_{n-d+1}(X_1, \ldots, X_{n-d+1}) : O \to \mathbb{R}, \ \ldots, \ u_n(X_1, \ldots, X_{n-1}) : O \to \mathbb{R}$$

such that

$$t_n(X_1, \ldots, X_{n-d}, u_{n-d+1}, \ldots, u_n) = 0, \cdots, t_{n-d+1}(X_1, \ldots, X_{n-d}, u_{n-d+1}) = 0.$$

Let m_i for $i = 1, \ldots, n-d$ be the minor of M obtained with columns $i, n-d+1, n-d+2, \ldots, n$ and let m_{ij} be the minor of the sub-matrix corresponding to minor m_i obtained by removing j-th column for $j = 1, \ldots, d+1$ and the last row. So

$$m_i = \det \begin{bmatrix} X_i & X_{n-d+1} & X_{n-d+2} & \ldots & X_n \\ (u_n)_{X_i} & (u_n)_{X_{n-d+1}} & (u_n)_{X_{n-d+2}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+1})_{X_i} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

$$m_{i1} = \det \begin{bmatrix} X_{n-d+1} & X_{n-d+2} & X_{n-d+3} & \ldots & X_n \\ (u_n)_{X_{n-d+1}} & (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+1})_{X_{n-d+1}} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

$$m_{i2} = \det \begin{bmatrix} X_i & X_{n-d+2} & X_{n-d+3} & \ldots & X_n \\ (u_n)_{X_i} & (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+1})_{X_i} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

Note: in the expansion of m_i, all m_{ij}, for $j = 3, \ldots, d+1$, will appear with coefficient zero. So among all m_{ij}'s, we are just interested in m_{i1} and m_{i2}.

Assume the matrix M is not full rank at any point of O. Then, all minors of M (given by the Mc Coy theorem [McC42]) are zero, especially m_i's for $i = 1, 2, \ldots, n-d$. This implies we have the following system of partial differential equations:

$$\begin{cases} m_{11}\frac{\partial}{\partial X_1}u_{n-d+1} + m_{12} = 0 \\ m_{21}\frac{\partial}{\partial X_2}u_{n-d+1} + m_{22} = 0 \\ \quad\vdots \\ m_{(n-d)1}\frac{\partial}{\partial X_{n-d}}u_{n-d+1} + m_{(n-d)2} = 0 \end{cases} \tag{6.7}$$

Claim: $X_n u_n + X_{n-1}u_{n-1} + \ldots + X_{n-d+1}u_{n-d+1} + \frac{X_{n-d}^2}{2} + \frac{X_{n-d-1}^2}{2} + \ldots + + \frac{X_1^2}{2} + c = 0$ is implied by System 6.7.

Proof of the claim: We can expand the i-th differential equation, for $i = 1, \ldots, n-d$, in System 6.7 as:

$$(m_{i11}\frac{\partial u_{n-d+2}}{\partial X_{n-d+1}} + m_{i12})\frac{\partial u_{n-d+1}}{\partial X_i} + m_{i21}\frac{\partial u_{n-d+2}}{\partial X_i} + m_{i22} = 0 \tag{6.8}$$

where

$$m_{i11} = \det\begin{bmatrix} X_{n-d+2} & X_{n-d+3} & X_{n-d+4} & \ldots & X_n \\ (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_{n-d+2}} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

$$m_{i12} = \det\begin{bmatrix} X_{n-d+1} & X_{n-d+3} & X_{n-d+4} & \ldots & X_n \\ (u_n)_{X_{n-d+1}} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_{n-d+1}} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

$$m_{i21} = \det\begin{bmatrix} X_{n-d+2} & X_{n-d+3} & X_{n-d+4} & \ldots & X_n \\ (u_n)_{X_{n-d+2}} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_{n-d+2}} & -1 & 0 & \ldots & 0 \end{bmatrix}$$

$$m_{i22} = \det\begin{bmatrix} X_i & X_{n-d+3} & X_{n-d+4} & \ldots & X_n \\ (u_n)_{X_i} & (u_n)_{X_{n-d+3}} & (u_n)_{X_{n-d+4}} & \ldots & -1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (u_{n-d+3})_{X_i} & -1 & 0 & \ldots & 0 \end{bmatrix}.$$

Observe $m_{i11} = m_{i21}$. So we can rewrite Equation 6.8 as

$$m_{i11}\frac{\partial u_{n-d+2}}{\partial X_{n-d+1}}\frac{\partial u_{n-d+1}}{\partial X_i} + m_{i12}\frac{\partial u_{n-d+1}}{\partial X_i} + m_{i11}\frac{\partial u_{n-d+2}}{\partial X_i} + m_{i22} = 0 \tag{6.9}$$

Continuing the same approach on Equation 6.9, one can observe that the coefficient of X_k, for $k = n-d+1, \ldots, n$, is U_{ik} a function of partial derivatives of u_j, for $j = n-d+1, \ldots, n$, such

that an anti-derivative of U_{ik} with respect to X_i is the function u_k. Therefore, Equation 6.9 can be rewritten as

$$X_n U_{in} + X_{n-1} U_{i(n-1)} + \ldots + X_{n-d+1} U_{i(n-d+1)} + X_i = 0. \tag{6.10}$$

Now for $i = 1$, take integral of Equation 6.10 with respect to X_1. Then there exists a differentiable function $F_1(X_2, \ldots, X_{n-d})$ such that we have:

$$X_n u_n + X_{n-1} u_{n-1} + \ldots + X_{n-d+1} u_{n-d+1} + \frac{X_1^2}{2} + F_1(X_2, \ldots, X_{n-d}) = 0. \tag{6.11}$$

By taking derivative of Equation 6.11 with respect to X_2 and substituting into Equation 6.10 for $i = 2$, we have $F_1(X_2, \ldots, X_{n-d}) = X_2$. Then there exists a differentiable function $F_2(X_3, \ldots, X_{n-d})$ such that $F_1 = \frac{X_2^2}{2} + F_2$. Therefore

$$X_n u_n + X_{n-1} u_{n-1} + \ldots + X_{n-d+1} u_{n-d+1} + \frac{X_1^2}{2} + \frac{X_2^2}{2} + F_2(X_3, \ldots, X_{n-d}) = 0. \tag{6.12}$$

Continuing the same approach, there exists a constant c such that

$$X_n u_n + X_{n-1} u_{n-1} + \ldots + X_{n-d+1} u_{n-d+1} + \frac{X_1^2}{2} + \frac{X_2^2}{2} + \ldots + \frac{X_{n-d}^2}{2} + c = 0. \tag{6.13}$$

This proves the claim.

Using the definitions of the analytic functions $u_n, \ldots, u_{n-d+1}$, the claim implies that the semi-algebraic set $Z_{\mathbb{R}}(S)$ contains parts of disjoint ellipsoids centred at the origin.

Now, we proceed as in the second step of the proof of Lemma 8. We start with a claim.

Claim: Assume that there exists r such that $0 < r < \rho$ holds and $\mathcal{M}$ is not full rank at any point of $D_r^* \cap Z_{\mathbb{R}}(S)$. Then, there exists r' such that $0 < r' < r$ holds and $E_{r'}$, the ellipsoid as in Equation 6.13 for $c = -r'^2$ (centred at the origin), intercepts $Z_{\mathbb{R}}(S)$ on a semi-algebraic set of dimension d.

Proof of the Claim: Since the origin is in the closure of $Z_{\mathbb{R}}(S)$, we know that $D_r^* \cap Z_{\mathbb{R}}(S)$ is not empty. W.l.o.g. we can assume that $Z_{\mathbb{R}}(S) \subseteq D_r^*$ holds. Indeed, if this was not the case, we could decompose $D_r^* \cap Z_{\mathbb{R}}(S)$ into finitely many regular semi-algebraic systems and reason with each of those which has the origin of $\mathbb{R}^n$ in the topological closure (w.r.t. Euclidean topology) of its zero set. The standard projection of $Z_{\mathbb{R}}(S)$ onto $(X_1, \ldots, X_{\iota-1})$, for $\iota = n - d + 1, \ldots n$, is an open set V_ι of $\mathbb{R}^{\iota-1}$. We apply argument before this claim on t_ι for $O := Z_{\mathbb{R}}(S)$. The conclusion of the claim follows.

Now we use Lemma 5. W.l.o.g. we can assume that $Z_{\mathbb{R}}(S)$ does not intercept an ellipsoid centred at the origin on semi-algebraic sets W_k's of dimension $d-1$ where $k = 1, \ldots, m$. Indeed, if this was the case, then we could remove all such W_k from $Z_{\mathbb{R}}(S)$ (since such W_k doesn't have the origin of $\mathbb{R}^n$ in its topological closure) and keep reasoning with each component of $Z_{\mathbb{R}}(S) \setminus \cup_{k=1}^m W_i$ which contains the origin of $\mathbb{R}^n$ in its topological closure.

As a consequence of the above claims, for every r such that $0 < r < \rho$ holds, there exists a point p of $D_r^* \cap Z_{\mathbb{R}}(S)$ at which $\mathcal{M}$ is full rank. Therefore, for all $r > 0$ small enough, the set $D_r^* \cap Z_{\mathbb{R}}(S)$ contains a point p_r, as well as a neighbourhood N_r of p_r (due to the full rank characterization in terms of minors) such that N_r is open relatively to $Z_{\mathbb{R}}(S)$ and $\mathcal{M}$ is full rank

at any point of N_r. Taking the union of those neighbourhoods N_r finally yields the conclusion of the lemma. □

We conclude this section by presenting an optimization trick for computing the limit of the fraction of polynomials f and g at the origin. This optimization is stated in Lemma 10 below and is taken from Proposition 2.2 of [XZ14]. For this reason, we refer to it as the *Chinese limit trick*.

Lemma 10 (Chinese limit trick)**.** *Let f and g be two non-zero polynomials in $\mathbb{R}[X_1, \ldots, X_n]$. Assume that $\lim_{x \to o} \frac{f(x)}{g(x)}$ exists. Then, using the lexicographic monomial order induced by $X_1 < \cdots < X_n$, the trailing monomial of f is not lower than the trailing monomial of g.*

Lemma 10 implies that if the trailing monomial of f is lower than the trailing monomial of g with respect to any lexicographic variable ordering over $X_1, \ldots, X_n$, then it is guaranteed that $\lim_{x \to \underline{o}} \frac{f(x)}{g(x)}$ does not exist. Note that Lemma 10 is true, whether the origin is an isolated zero of the denominator or not.

Chapter 7

Computing limits of multivariate rational functions

We describe in this chapter our procedure for determining the existence and the possible value of limits of the form $\lim_{(x_1,\ldots,x_n)\to(0,\ldots,0)} q(x_1,\ldots,x_n)$. Following the notations of Section 6, recall that q is a rational function in the n ordered variables $X_1 < \cdots < X_n$ and with rational number coefficients.

Our procedure extends to an arbitrary n the algorithm proposed in [CMV13] for $n = 2$. Hence, as in that paper, we assume that the origin is an isolated zero of the denominator of q. The pseudo-code for our procedure is stated in Algorithms 4, 7, 5 and 6.

Algorithm 4 Limit of rational function $q \in \mathbb{Q}(X_1,\ldots,X_n)$ at origin

procedure LIMIT(q)
  $\mathcal{A} :=$ Minors($\begin{bmatrix} X_1 & \cdots & X_n \\ \frac{\partial q}{\partial X_1} & \cdots & \frac{\partial q}{\partial X_n} \end{bmatrix}$);
  $\mathcal{D} :=$ RealTriangularize($\mathcal{A}$);
  $\mathcal{L} := \emptyset$;
  for $S \in \mathcal{D}$ **do**
    if $\underline{o} \in \overline{Z_{\mathbb{R}}(S)}$ and $\dim(Z_{\mathbb{R}}(S)) > 0$ **then**
      $\mathcal{L} := \mathcal{L} \cup \{LimitInner(q, S)\}$;
    end if
  end for
  return $\mathcal{L}$;
end procedure

Proposition 9. *Algorithm 4 terminates and returns finitely many pairs $(L_1, S_1), \ldots, (L_e, S_e)$ where each of $L_1, \ldots, L_e$ is either a real number, or the flag* no_limit*, and $S_1, \ldots, S_e$ are all regular semi-algebraic systems such that each of the sets $Z_{\mathbb{R}}(S_1), \ldots, Z_{\mathbb{R}}(S_e)$ has dimension one and contains the origin in its closure. Moreover, if $L_i \in \mathbb{R}$, then L_i is the limit of q at the origin along the $Z_{\mathbb{R}}(S_i)$ for all $i = 1, \ldots, e$. In addition, the rational function q admits a finite limit at the origin if and only if $L_1, \ldots, L_e$ are all real numbers and equal; if this holds, then this common value is the limit of q at the origin.*

Proof. Algorithm 4 applies Lemma 3 as follows. At Line (2), it computes the real algebraic set $\chi(q)$ defined in Notation 2 and at Line (3) it computes a triangular decomposition $\mathcal{D}$ of $\chi(q)$ as defined in Proposition 4. Following Lemma 4, each regular semi-algebraic system $S \in \mathcal{D}$ which is zero-dimensional, or such that the origin is not contained in the closure of $Z_{\mathbb{R}}(S)$, is discarded at Line (6). For every other regular semi-algebraic system (RSAS) S, one runs $\mathrm{L}imitinner(q, S)$ at Line (7), that is, one makes a call to Algorithm 7.

Algorithm 7 is the core routine. It first checks whether $Z_{\mathbb{R}}(S)$ has dimension one or not. If $\dim(Z_{\mathbb{R}}(S)) = 1$ holds, one runs $\mathrm{LimitAlongCurve}(q, S)$, that is, Algorithm 6. Applying Algorithm 7 with RSASs of dimension one can be seen as the *base case* of that recursive routine while the rest of that routine reduces computation with RSASs of dimension higher than one to this base case.

This reduction is performed by repeated applications of the Lagrange multipliers trick, as in the proof of Lemma 3. It follows from Lemma 8 that there exists a minor $m \in \mathrm{M}inors(\mathcal{M})$ (where $\mathcal{M}$ is defined at Line (6) of Algorithm 7) such that we have $Z_{\mathbb{R}}(S) \not\subseteq Z_{\mathbb{R}}(m)$. Note that we know that the Jacobian of T (that is, the matrix formed with the ∇t, for $t \in T$) is full rank. This follows from Proposition 3 and explains why we do not need to compute any singular loci.

Once such a minor $m \in \mathrm{M}inors(\mathcal{M})$ is found, we compute $Z_{\mathbb{R}}(S) \cap Z_{\mathbb{R}}(\{m \neq 0\})$ using the Intersect command defined in Remark 2; this is done at Line (12). The resulting triangular decomposition consists of RSASs with the same dimension as S. The goal of Line (13) is to remove any RSAS S' such that $\overline{Z_{\mathbb{R}}(S')}$ does not contain the origin; see also Remark 2 for that test.

At Lines (16) to (19), we prepare for applying the Lagrange multipliers trick: since $\nabla_{(X_1,\ldots,X_n)} q$ is proportional to $(X_1, \ldots, X_n)$ along $\chi(q)$ we cannot re-use the family of circles C_r as in the proof of Lemma 3; instead, we use a family of ellipsoids, given by E_r; this idea was introduced in [VHC15]. In particular, at Line (16), we determine values for the coefficients $A_1, \ldots, A_n$ of the polynomial E_r such that at least one minor of $\mathcal{M}'$ is not zero. This task is delegated to Algorithm 5: in practice, choosing $A_1, \ldots, A_n$ all positive at random works; if this would not work, we would determine $A_1, \ldots, A_n$ by solving a polynomial system.

The for-loop located between Lines (21) and (43) runs until we find a minor m' of the matrix $\mathcal{M}'$ (where $\mathcal{M}'$ is defined at Line (18) of Algorithm 7) such that the dimension of $Z_{\mathbb{R}}(S) \cap Z_{\mathbb{R}}(\{m' = 0\})$ is less than that of $Z_{\mathbb{R}}(S)$. This search is expected to be *successful* because the non-linear programs consisting of minimizing/maximizing $q(x_1, \ldots, x_n)$ under the constraints $(x_1, \ldots, x_n) \in Z_{\mathbb{R}}(S) \cap \{E_r = 0\}$ have solutions, necessarily. However, this search depends on the minor m, as well. In fact, what the previous non-linear optimization argument guarantees is the existence of a pair of minors (m, m') such that $\mathcal{M}$ is full rank for $m \neq 0$ while $\mathcal{M}'$ is not full rank for $m' = 0$. For this reason, for certain m, the search for m', or the recursive call at Line (30), may fail. Such a situation leads the algorithm to try the next m from $\mathrm{M}inors(\mathcal{M})$. It follows that Algorithm 7 must implement a *backtracking* mechanism.

This backtracking feature is achieved by endowing the algorithm with a *state machine*. Note that at Lines (7), (20), (32), (40), (45), and (50) a variable called state is assigned in order to record the *new* state of the algorithm. Observe that, if the variable state never receives the value backtrack during the execution of Algorithm 7, then only the first minor $m \in \mathrm{M}inors(\mathcal{M})$ and the first minor $m' \in \mathrm{M}inors(\mathcal{M}')$ are considered by the algorithm.

Observe that, during one iteration of the for-loop located between Lines (21) and (43), if the variable L receives the value backtrack , or the variable $\mathcal{I}$ remains empty, then this iteration

failed to find a minor m'; as a consequence either this for-loop goes for another iteration, or, if all iterations have been executed, the variable state will receive the value backtrack implying that the current value of the minor m cannot lead to find a minor m' with the desired properties.

Finally, observe that the execution of the for-loop located between Lines (8) and (54) terminates either with state reaching the value found_second_minor (implying that a pair of minors (m, m') with the desired properties has been found) or with state having the value backtrack (implying that no such pair was found).

It follows from the above discussion that Algorithm 7 always terminates and so does Algorithm 4. Moreover, as mentioned above, since the non-linear programs consisting of minimizing/maximizing q under the constraints $(x_1, \ldots, x_n) \in Z_{\mathbb{R}}(S) \cap \{E_r = 0\}$ necessarily have solutions (where q and S are the input of Algorithm 7), the calls that Algorithm 4 makes to Algorithm 7 ultimately produces an answer of the form $(L_1, S_1), \ldots, (L_e, S_e)$ with the desired properties. □

Algorithm 5 Ellipsoid in $\mathbb{R}^n$ randomly generated

1: **procedure** RANDOMELLIPSOID(n)
2: **repeat**
3: choose $A_1, \ldots, A_n, r$ randomly with $r > 0$;
4: let $E_r := \sum_{i=1}^{n} A_i X_i^2 - r^2$;
5: $\mathcal{S} := \begin{bmatrix} \frac{\partial E_r}{\partial X_1} & \cdots & \frac{\partial E_r}{\partial X_n} \\ X_1 & \cdots & X_n \end{bmatrix}$;
6: **until** $\mathcal{S}$ has at least one non-zero minor
7: **return** $(A_1, \ldots, A_n, r)$;
8: **end procedure**

Algorithm 6 Limit of the rational function $q \in \mathbb{Q}(X_1, \ldots, X_n)$ at the origin along the real curve C given by the RSAS $[Q, T, P_>]$

1: **procedure** LIMITALONGCURVE(q, C)
2: Let f, g be the numerator and denominator of q;
3: Let $R := \{gX_{n+1} - f\} \cup T$ with X_{n+1} a new variable; ▷ R is a regular chain for $X_1 < \cdots < X_{n+1}$;
4: Compute the limit points of $Z_{\mathbb{R}}(R) \setminus Z_{\mathbb{R}}(h_R)$ in $\mathbb{R}^n$ for the Euclidean topology; see Section 5;
5: If x_{n+1} escapes to infinity when $(x_1, \ldots, x_n)$ approaches the origin along one branch of $Z_{\mathbb{R}}(R)$, then return no_limit;
6: If there is only one such limit point $(x_1, \ldots, x_n, x_{n+1})$ with $x_1 = \cdots = x_n = 0$, then x_{n+1} is the desired limit of q;
7: Otherwise return no_limit since q has no limit along C at the origin;
8: **end procedure**

Algorithm 7 Limit of the rational function $q \in \mathbb{Q}(X_1, \ldots, X_n)$ at the origin along the zero set of the regular semi-algebraic system S (Part 1)

procedure LIMITINNER(q, S)
  if $\dim(Z_{\mathbb{R}}(S)) = 1$ **then**
    return (LimitAlongCurve(q, S), S);
  end if
  let $[Q, T, P_>] := S$;
  $\mathcal{M} := \begin{bmatrix} X_1 & \cdots & X_n \\ \nabla t, t \in T & & \end{bmatrix}$;
  state := search_first_minor;
  for $m \in \mathrm{Minors}(\mathcal{M})$ **do**
    if $Z_{\mathbb{R}}(S) \subseteq Z_{\mathbb{R}}(m)$ **then next**;
    end if
    $\mathcal{J} := \emptyset$;
    for $S' \in \mathrm{Intersect}(S, \{m \neq 0\})$ **do**
      if $\underline{o} \notin \overline{Z_{\mathbb{R}}(S')}$ or $\dim(Z_{\mathbb{R}}(S')) = 0$ **then**
        next;
      end if
      $(A_1, \ldots, A_n, r) := \mathrm{RandomEllipsoid}(n)$;
      let $E_r := \sum_{i=1}^{n} A_i X_i^2 - r^2$;
      $\mathcal{M}' := \begin{bmatrix} \frac{\partial E_r}{\partial X_1} & \cdots & \frac{\partial E_r}{\partial X_n} \\ X_1 & \cdots & X_n \\ \nabla t, t \in T & & \end{bmatrix}$;
      let $[Q', T', P_>{}'] := S'$;

Algorithm 4 Limit of the rational function $q \in \mathbb{Q}(X_1, \ldots, X_n)$ at the origin along the zero set of the regular semi-algebraic system S (Part 2)

```
20:             state := search_second_minor;
21:             for m' ∈ Minors(M') do
22:                 if res(m', T') = 0 then
23:                     next;
24:                 end if
25:                 I := ∅;
26:                 for C ∈ Intersect(S', m' = 0) do
27:                     if o ∉ closure(Z_R(C)) or dim(Z_R(C)) = 0 then
28:                         next;
29:                     end if
30:                     L := LimitInner(q, C);
31:                     if L = backtrack then
32:                         state := backtrack;
33:                         break;
34:                     else
35:                         I := I ∪ {L};
36:                     end if
37:                 end for
38:                 if I ≠ ∅ and state ≠ backtrack then
39:                     J := J ∪ I;
40:                     state := found_second_minor;
41:                     break;
42:                 end if
43:             end for
44:             if state ≠ found_second_minor then
45:                 state := backtrack;
46:                 break;
47:             end if
48:         end for
49:         if state ≠ backtrack then
50:             state := found_first_minor;
51:             break;
52:         end if
53:     end for
54:     if state = found_first_minor then
55:         return J;
56:     else
57:         return backtrack;
58:     end if
59: end procedure
```

We conclude this section with two examples illustrating Algorithm 4.

Example 4. *Let $q \in \mathbb{Q}(x, y, z, w)$ be the rational function defined by $q(x, y, z, w) = \frac{z\,w+x^2+y^2}{x^2+y^2+z^2+w^2}$. We aim at computing $\lim_{(x,y,z,w)\to(0,0,0,0)} q$. A first step of the procedure consists in calculating the real algebraic set $\chi(q)$ such that our limit problem reduces to compute*

$$\lim_{(x,y,z,w)\to(0,0,0,0),(x,y,z,w)\in\chi(q)} q.$$

The set $\chi(q)$, defined in Notation 2, is obtained by the method of Lagrange multipliers, see Section 1.1 and the proof of Lemma 3. The RealTriangularize *algorithm yields the following decomposition: $\chi(q) = Z_{\mathbb{R}}(R_1) \cup Z_{\mathbb{R}}(R_2) \cup Z_{\mathbb{R}}(R_3) \cup Z_{\mathbb{R}}(R_4)$, where R_1, R_2, R_3, R_4 are respectively given by the* regular semi-algebraic systems *(see Section 1.5 for this term):*

$$\left\{ \begin{array}{l} x = 0 \\ y = 0 \\ z = 0 \\ w = 0 \end{array} \right. , \left\{ \begin{array}{l} z = 0 \\ w = 0 \end{array} \right. , \left\{ \begin{array}{l} x = 0 \\ y = 0 \\ z + w = 0 \end{array} \right. \text{ and } \left\{ \begin{array}{l} x = 0 \\ y = 0 \\ z - w = 0 \end{array} \right. .$$

For our purpose of limit computation, only R_2, R_3, R_4 are interesting, since they define either a curve or a surface passing through the origin, whereas R_1 is simply the origin.

Computing the limit of q along each of the curves $Z_{\mathbb{R}}(R_3)$ and $Z_{\mathbb{R}}(R_4)$ is achieved by a specific procedure presented in Section 5, based on Puiseux series. This procedure extends to the real case a technique presented in [ACM13] for the complex case. On this particular example, evaluating $q(x, y, z, w)$ at $Z_{\mathbb{R}}(R_3)$ and $Z_{\mathbb{R}}(R_4)$, immediately yields the value of the limit in each case, which are $-\frac{1}{2}$ and $\frac{1}{2}$, respectively.

Now we focus on R_2 which consists simply of a regular chain, namely $T := \{t_1, t_2\}$ with $t_1 = z$ and $t_2 = w$. In order to compute the limit of $q(x, y, z, w)$ along $Z_{\mathbb{R}}(R_2)$, we apply again the method of Lagrange multipliers. More precisely, we wish to optimize $q(x, y, z, w)$ along $t_1(x, y, z, w) = t_2(x, y, z, w) = 0$ intercepted with a family of ellipsoids $E_r(x, y, z, w) = 0$ with $E_r := A_1\,x^2 + A_2\,y^2 + A_3 z^2 + A_4\,w^2 - r^2$, where A_1, A_2, A_3, A_4 are positive values to be determined.

By definition of $\chi(q)$, the gradient $\nabla_{x,y,z,w} q$ is proportional to (x, y, z, w) along $\chi(q)$. Hence, in order to apply the Lagrange multipliers method, we need to check that the vectors $\nabla_{x,y,z,w} t_1$, $\nabla_{x,y,z,w} t_2$ and (x, y, z, w) are linearly independent almost everywhere on $Z_{\mathbb{R}}(R_2)$. By considering the following Jacobian matrix

$$\left[\begin{array}{cccc} x & y & z & w \\ \frac{\partial t_1}{\partial x} & \frac{\partial t_1}{\partial y} & \frac{\partial t_1}{\partial z} & \frac{\partial t_1}{\partial w} \\ \frac{\partial t_2}{\partial x} & \frac{\partial t_2}{\partial y} & \frac{\partial t_2}{\partial z} & \frac{\partial t_2}{\partial w} \end{array} \right] = \left[\begin{array}{cccc} x & y & z & w \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right]$$

we see that the vectors $\nabla_{x,y,z,w} t_1$, $\nabla_{x,y,z,w} t_2$ and (x, y, z, w) are linearly independent as long as $x \neq 0$ or $y \neq 0$ holds. We choose to impose the constraint $y \neq 0$; using the incremental version of RealTriangularize*, we compute the intersection $Z_{\mathbb{R}}(R_2) \cap \{y \neq 0\}$ and obtain $Z_{\mathbb{R}}(R_5)$ where $R_5 := \{z = 0, w = 0, y \neq 0\}$. Now we choose $(A_1, A_2, A_3, A_4) = (3, 1, 2, 3)$ such that*

$$\left[\begin{array}{cccc} A_1 x & A_2 y & A_3 z & A_4 w \\ x & y & z & w \end{array} \right]$$

is full rank. We are ready to apply the method of Lagrange multipliers, considering the following matrix

$$\begin{bmatrix} A_1 x & A_2 y & A_3 z & A_4 w \\ x & y & z & w \\ \frac{\partial t_1}{\partial x} & \frac{\partial t_1}{\partial y} & \frac{\partial t_1}{\partial z} & \frac{\partial t_1}{\partial w} \\ \frac{\partial t_2}{\partial x} & \frac{\partial t_2}{\partial y} & \frac{\partial t_2}{\partial z} & \frac{\partial t_2}{\partial w} \end{bmatrix} = \begin{bmatrix} 3x & 1y & 2z & 3w \\ x & y & z & w \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

which has a single non-zero minor, namely $m = 4xy$. *Using again the incremental version of* RealTriangularize, *we compute* $Z_{\mathbb{R}}(R_5) \cap Z_{\mathbb{R}}(m = 0)$ *and obtain* $Z_{\mathbb{R}}(R_6)$, *where* $R_6 := \{x = 0, z = 0, w = 0, y \neq 0\}$. *We are now in dimension one. Using the procedure of Section 5 (or, on this particular example, using substitution and elementary calculations) yields* 1 *as the limit along* $Z_{\mathbb{R}}(R_6)$.

Putting everything together, we have three different values for the limit of $q(x, y, z, w)$ *along the three curves* $Z_{\mathbb{R}}(R_3)$, $Z_{\mathbb{R}}(R_4)$ *and* $Z_{\mathbb{R}}(R_6)$. *The corresponding values are* $-\frac{1}{2}, \frac{1}{2}, 1$, *which shows that the limit of* q *at the origin does not exist.*

Example 5. *Let* $q \in \mathbb{Q}(x, y, z)$ *be the rational function defined by* $q(x, y, z) = \frac{x^2 y z^2}{x^4 + z^4 + y^4}$. *Here again, we aim at computing* $\lim_{(x,y,z)\to(0,0,0)} q$. RealTriangularize *produces the following decomposition of the real algebraic set* $\chi(q)$: $\chi(q) = Z_{\mathbb{R}}(R_1) \cup Z_{\mathbb{R}}(R_2) \cup Z_{\mathbb{R}}(R_3) \cup Z_{\mathbb{R}}(R_4)$, *where* R_1, R_2, R_3, R_4 *are respectively given by the regular semi-algebraic systems:*

$$\left\{ x = 0 \right. , \left\{ z = 0 \right. , \left\{ \begin{array}{l} x^2 - z^2 = 0 \\ y^6 + 3\, y^4\, z^2 - 2\, z^6 = 0 \\ z \neq 0 \end{array} \right. \text{and} \left\{ \begin{array}{l} x = 0 \\ y = 0 \\ z = 0 \end{array} \right. .$$

The system R_4 *can be discarded and the system* R_3 *has dimension one, hence the limit of* q *along* $Z_{\mathbb{R}}(R_3)$ *is handled by the procedure of Section 5, which yields* 0.

We focus on R_1 *and* R_2. *Similarly to the previous example, we consider the non-linear program consisting of optimizing* $q(x, y, z)$ *subject to* $(x, y, z) \in Z_{\mathbb{R}}(R_1)$ *(resp.* $(x, y, z) \in Z_{\mathbb{R}}(R_2)$*) and* $E_r(x, y, z) = 0$ *with* $E_r := A_1\, x^2 + A_2\, y^2 + A_3 z^2 - r^2$, *where* A_1, A_2, A_3 *are positive values to be determined.*

Let $T := \{t_1\} = \{x\}$ *be the regular chain part of* R_1. *Recall that* $\nabla_{x,y,z} q$ *is proportional to* (x, y, z) *along* $\chi(q)$. *Hence, we first determine when the following matrix*

$$\begin{bmatrix} x & y & z \\ \frac{\partial t_1}{\partial x} & \frac{\partial t_1}{\partial y} & \frac{\partial t_1}{\partial z} \end{bmatrix} = \begin{bmatrix} x & y & z \\ 1 & 0 & 0 \end{bmatrix}$$

is full rank. The set of its 2-by-2 minors is $\{y, z, 0\}$*; hence this matrix is full rank whenever* $y \neq 0$ *or* $z \neq 0$ *holds. Since* $Z_{\mathbb{R}}(R_1) \not\subseteq Z_{\mathbb{R}}(y)$ *holds, we impose the constraint* $y \neq 0$ *and compute* $Z_{\mathbb{R}}(R_1) \cap \{y \neq 0\}$ *yielding* $Z_{\mathbb{R}}(R_5)$ *with* $R_5 := \{x = 0, y \neq 0\}$. *Next, we let* $(A_1, A_2, A_3) = (9, 10, 2)$ *such that*

$$\begin{bmatrix} A_1 x & A_2 y & A_3 z \\ x & y & z \end{bmatrix}$$

has at least one non-zero minor. Putting the three gradient vectors together, we form the following matrix

$$\begin{bmatrix} A_1 x & A_2 y & A_3 z \\ x & y & z \\ \frac{\partial t_1}{\partial x} & \frac{\partial t_1}{\partial y} & \frac{\partial t_1}{\partial z} \end{bmatrix} = \begin{bmatrix} 9x & 10y & 2z \\ x & y & z \\ 1 & 0 & 0 \end{bmatrix}.$$

Its determinant is $8\,y\,z$ *and we compute* $Z_{\mathbb{R}}(R_5) \cap \{y\,z = 0\}$ *yielding* $Z_{\mathbb{R}}(R_6)$ *with* $R_6 := \{x = 0, z = 0, y \neq 0\}$. *The regular semi-algebraic system* R_6 *represents a space curve and the procedure of Section 5 computes the limit of* q *at the origin along* $Z_{\mathbb{R}}(R_6)$, *yielding* 0. *We proceed similarly with* R_2. *In this case, the non-linear programming trick yields the following space curve* $\{y = 0, z = 0, x \neq 0\}$ *along which the limit of* q *at the origin is also* 0. *Finally, the limit of* q *at origin exists and is equal to* 0.

Chapter 8

Experimentation

In this chapter, we present experimental results for the algorithms proposed in this paper and provide empirical comparison with related works. In Section 8.1, we compare different implementations of the EHC with the method of Kung and Traub, using both their linear and quadratic lifting schemes. Section 8.2 is devoted to an experimental comparison of various MAPLE implementations for computing limits of multivariate rational functions. All these experimental results were obtained on an Ubuntu desktop (1.6GHz Intel(R) Xeon(R) CPU, 48GB.).

8.1 Comparing the method of Kung and Traub with the EHC

Table 8.1 gathers running times for comparing the EHC and Kung-Traub's method for $k = 10$ and $k = 20$, where k is as in introduction. The columns KT Lin and KT Quad correspond to linear and quadratic lifting methods of Kung and Traub, respectively. Thus, for the EHC, which is based on a linear lifting, as well as for KT Lin, $k = 10$ and $k = 20$ means 10 and 20 iterations of the "main loop". For KT Quad, $k = 10$ and $k = 20$ means 4 and 5 iterations of the "main loop".

Each test-example has a number and can be found in the archive posted at the web page `wwww.regularchains.org/papers/Benchmark-ISSAC-2017.zip`. The column MD gives the degree of the main variable in the input polynomial. The columns KT10 and KT20 correspond to $k = 10$ and $k = 20$. The sub-columns EHC10 and EHC20 under EHCWM, give the timings for our enhanced EHC, described in this paper, that is, based on Sections 3 and 4. The sub-column EHC10, under EHCEEA, gives the timings for an implementation of the original EHC method as described in [SK99]. The sub-columns YM1 and YM2 show the timings for computing the Yun-Moses polynomials corresponding to EHC10, respectively for EHCWM and EHCEEA.

In Table 8.1, the three most significant digits of the timings are recorded and ∞ means the computations exceeded either the time limit of 3600sec, or the memory limit of 48Gb.

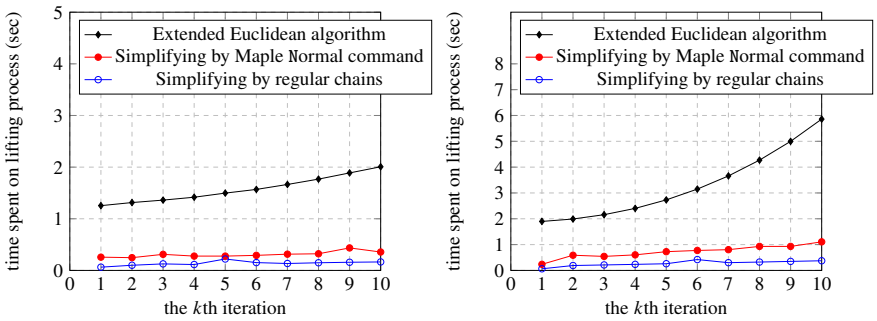

Figure 8.1: For each k on the x-axis, these plots show the time spent for lifting the factors of EHC, from step $k-1$ to step k see Lines 8-12 in Algorithm 1: (1) the black curve corresponds to the original EHC [SK99]; (2) The red curve corresponds to the implementation of EHC with the optimization tricks presented in this paper, when the simplifications of algebraic numbers are done with the Normal command of MAPLE, and (3) the blue curve is the timing of EHC with the optimization tricks when the simplifications of algebraic numbers are done with the RegularChains library.

Ex	MD	KT Lin		KT Quad		EHCWM			EHCEEA	
		KT10	KT20	KT10	KT20	EHC10	YM1	EHC20	EHC10	YM2
1	5	2.22	18.6	4.93	4.91	0.48	0.22	0.73	0.90	0.21
7	4	5.60	65.8	0.56	0.58	0.22	0.14	0.23	0.34	0.13
8	4	14.9	230	1.25	1.25	0.23	0.13	0.28	0.36	0.12
9	3	5.53	114	1.51	1.56	0.30	0.11	0.39	0.88	0.10
10	3	2.71	42.0	0.28	0.63	0.16	0.08	0.20	0.32	0.12
11	3	0.46	2.34	0.21	0.21	0.16	0.08	0.17	0.26	0.12
12	3	0.50	6.86	0.28	0.32	0.16	0.08	0.18	0.30	0.12
13	4	0.86	10.9	0.50	0.48	0.26	0.15	0.28	0.46	0.24
14	4	3.21	34.8	0.69	0.71	0.26	0.15	0.34	0.52	0.24
15	6	27.6	535	4.85	4.85	0.64	0.42	0.82	2.05	1.08
16	7	45.6	836	8.45	9.91	0.64	0.43	0.92	2.33	1.74
17	7	145	∞	23.4	23.2	0.78	0.43	3.37	4.12	1.77
19	4	0.14	0.16	0.16	0.14	0.39	0.26	0.45	0.51	0.15
20	4	2.79	7.98	0.77	0.82	0.26	0.15	0.29	0.50	0.24
21	4	8.58	143	1.96	1.93	0.23	0.12	0.31	0.47	0.16
24	5	2.90	24.8	1.11	1.11	0.26	0.15	0.35	0.49	0.17
25	7	1.83	9.45	0.90	1.00	0.46	0.31	0.50	0.73	0.42
26	8	2.35	12.3	3.09	3.29	0.66	0.53	0.74	2.18	1.80
27	8	60.8	2876	23.1	27.1	0.77	0.53	1.20	2.31	1.28
28	9	215	∞	73.8	123	1.88	1.03	2.11	7.03	4.92
30	17	∞	∞	∞	∞	39.8	6.70	41.3	53.8	16.5
31	32	∞	∞	∞	∞	599	24.9	∞	∞	∞
32	33	∞	∞	∞	∞	224	25.0	∞	∞	∞

Table 8.1: Comparing EHC versus Kung-Traub's method for $k = 10$ and $k = 20$. The columns KT Lin and KT Quad correspond to linear and quadratic lifting methods of Kung and Traub, respectively. The sub-columns EHC10 and EHC20 under EHCWM, give the timings for our enhanced EHC and the sub-column EHC10, under EHCEEA, gives the timings for an implementation of the original EHC method as described in [SK99]. (timings are in seconds)

Figure 8.1 focuses on the performance of the optimization tricks applied on the lifting process of EHC as explained in Section 4, for two different bivariate polynomials. Note that square-root scaling has been used for the y-axis. The EHC algorithm, as well as Kung-Traub's method, are implemented in Maple and they are integrated into PowerSeries library. The libraries RegularChains and PowerSeries are available at `www.regularchains.org`.

8.2 Computing limits of multivariate rational functions

This section is devoted to an experimental comparison of various MAPLE implementation for computing limits of multivariate rational functions: MAPLE's built-in command `limit`, the `TestLimit` command presented in [XZ14] and our implementation of the algorithm of Section 7 within the RationalFunctionLimit command of the `RegularChains` library. In Tables 8.2 and 8.3, the abbreviations LM, TL, and RFL stand for `limit`, `TestLimit`, and `RationalFunctionLimit` commands. Further, NV, TD and LV represent the number of variables, the maximum total degree between numerator and denominator, and the value of the limit, respectively. The timings in columns LM, TL, RFL are in seconds.

We used more than 50 test-examples[1] where the denominators of rational functions are defined by sum of squares of variables. A representative subset of these examples is provided in Table 8.2.

For bivariate rational functions (examples 1-5), both LM and TL run faster than RFL, except on Example 2. Recall that LM applies to bivariate rational functions only.

Out of the 25 examples in 3 variables or more, TL and RFL solve respectively 9 and 23 examples within the prescribed resource limits of 48 GB of memory and 1800 sec of CPU time. Moreover, out of those 25 examples, TL fails on 8 of them due to a division-by-zero error. For the 17 examples in 3 variables or more, for which TL does not hit such an error, RFL runs faster than TL on 8 examples.

Taking into account the 30 examples: (1) TL and RFL solve respectively 13 and 28 examples, (2) for the 21 examples for which TL does not hit an error, RFL runs faster than TL 8 times, and (3) for the 13 examples for which TL computes the answer, TL is faster than RFL on 11 times. Note that when the limit exists RFL outperforms TL. Meanwhile, when the limit value is undefined and TL does not hit an error most of the time, and TL is faster than RFL.

The comparison of RFL against TL and LM reported in Table 8.3 is based on test-examples where the denominator is not a sum of squares (including Motzkin, Choi and Lam polynomials). In such cases, TL is the fastest command.

Table 8.4 demonstrates the time consumptions for computing real and complex limit points corresponding to the regular chains of dimension one in the triangular decomposition of the polynomial systems in the first column. The second and third columns are respectively, the time spent for computing the number of real limit points. The fourth and fifth columns are respectively, the time spent for computing and the number of complex limit points. The command for computing real and complex limit points of regular chains is called LimitPoints and it is part of R*egularChains* library of Maple.

[1]The list of the examples and the timings corresponding to Table 8.2 can be found at `www.regularchains.org/RationalLimit/RationalFunctionLimit.zip` and `www.regularchains.org/RationalLimit/Report`, respectively.

Ex	NV	TD	LM	TL	RFL	LV	Chinese limit trick
1	2	4	0.076	0.112	0.769	-1	X
2	2	4	0.081	wrong answer	0.771	-1	X
3	2	2	0.022	0.002	0.584	undefined	X
4	2	4	0.116	0.002	1.113	undefined	X
5	2	4	0.063	0.113	0.782	-1	X
6	3	5	NA	0.611	2.559	0	X
7	3	8	NA	∞	∞	NA	X
8	3	18	NA	8.904	0.618	0	X
9	3	18	NA	0.601	0.617	0	X
10	4	4	NA	0.002	3.381	undefined	X
11	4	2	NA	0.002	0.580	undefined	X
12	4	4	NA	0.002	3.336	undefined	X
13	4	5	NA	∞	14.233	0	X
14	4	21	NA	∞	2.531	0	X
15	4	6	NA	∞	3.432	0	X
16	5	19	NA	∞	1.482	0	X
17	5	4	NA	3.343	4.675	0	X
18	6	6	NA	Error	3.372	0	X
19	6	6	NA	Error	3.908	undefined	X
20	6	18	NA	Error	2.014	undefined	X
21	6	10	NA	∞	150.706	0	X
22	6	10	NA	∞	165.471	0	X
23	6	6	NA	Error	44.038	0	X
24	7	6	NA	0.019	0.019	undefined	✓
25	8	5	NA	∞	30.378	0	X
26	8	9	NA	Error	173.229	0	X
27	9	4	NA	0.005	8.931	undefined	X
28	9	10	NA	Error	∞	NA	X
29	9	5	NA	Error	12.293	0	X
30	10	10	NA	Error	84.954	0	X

Table 8.2: Comparisons between three different commands for computing the limit of real multivairate rational functions: limit, TestLimit, and RationalFunctionLimit. Here, the denominator is a sum of squares of variables.

In Tables 8.2 and 8.3, ∞ means the computations exceeded either the time limit of 1800 sec, or the memory limit of 48Gb.

Ex	NV	TD	LM	TL	RFL	LV	Chinese limit trick
32	2	10	1.157	0.002	∞	undefined	X
33	2	16	5.530	0.002	∞	undefined	X
66	3	6	NA	0.002	0.030	undefined	✓
67	3	8	NA	0.002	∞	undefined	X
68	3	6	0.055	0.002	0.033	undefined	✓
69	3	8	0.050	0.002	0.033	undefined	✓
70	4	4	NA	0.003	∞	undefined	X
71	4	6	NA	0.003	∞	undefined	X

Table 8.3: Comparisons between three different commands for computing the limit of real multivairate rational functions: limit, TestLimit, and RationalFunctionLimit. Here, non-negative polynomials proposed by Motzkin, Choi and Lam have been used in the denominators.

Sys	RealLimit	#LM	ComplexLimit	#LM
Liu-Lorenz	777.300	4	1708.829	9
MontesS3	0.015	0	0.015	0
Neural	1.538	3	2.368	3
cox-issac07	0.438	0	0.575	1

Table 8.4: Complex limit points vs real limit points

As in [CMV13] and [VHC15], we assume that the origin is an isolated zero of the denominator. However, relaxing this assumption is work in progress thanks to RealTriangularize and the ideas proposed in [LR07].

In Chapter 5, we have presented an algorithm for determining the real branches of a space curve about one of its points. This is a core routine for computing limits of real multivariate rational functions as well as for addressing topological questions like whether a point belongs to the closure of a CAD cell. To this end, we revisited the extended Hensel construction and established properties of the Yun-Moses polynomials.

Bibliography

[AAM17] P. Alvandi, M. Ataei, and M. Moreno Maza. On the extended Hensel construction and its application to the computation of limit points. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany, July 25-28, 2017*, pages 13–20, 2017.

[Abh89] S. S. Abhyankar. Irreducibility criterion for germs of analytic functions of two complex variables. *Advances in Mathematics*, 74(2):190 – 257, 1989.

[ACM13] P. Alvandi, C. Chen, and M. Moreno Maza. Computing the limit points of the quasi-component of a regular chain in dimension one. In *Proc. of CASC*, volume 8136, pages 30–45, 2013.

[AKM16] P. Alvandi, M. Kazemi, and M. Moreno Maza. Computing limits of real multivariate rational functions. In *ISSAC*, pages 39–46, 2016.

[AMSV15] P. Alvandi, M. Moreno Maza, É. Schost, and P. Vrbik. A standard basis free algorithm for computing the tangent cones of a space curve. In *Proc. of CASC*, pages 45–60, 2015.

[Ber98] L. Bernardin. On bivariate Hensel and its parallelization. In *ISSAC*, pages 96–100, 1998.

[Boc00] M. Bocher. The theory of linear dependence. *Annals of Mathematics, Second Series*, 2(1/4):81–96, 1900.

[BPR06] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry (Algorithms and Computation in Mathematics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[CC86] D. V. Chudnovsky and G. V. Chudnovsky. On expansion of algebraic functions in power and Puiseux series, I. *J. Complexity*, 2(4):271–294, 1986.

[CDM+13a] C. Chen, J. H. Davenport, J. P. May, M. Moreno Maza, B. Xia, and R. Xiao. Triangular decomposition of semi-algebraic systems. *J. Symb. Comput.*, 49:3–26, 2013.

[CDM+13b] C. Chen, J. H. Davenport, M. Moreno Maza, B. Xia, and R. Xiao. Computing with semi-algebraic sets: Relaxation techniques and effective boundaries. *J. Symb. Comput.*, 52:72–96, 2013.

[CM12] C. Chen and M. Moreno Maza. Algorithms for computing triangular decomposition of polynomial systems. *J. Symb. Comput.*, 47(6):610–642, 2012.

[CMV13] C. Cadavid, S. Molina, and J. D. Vélez. Limits of quotients of bivariate real analytic functions. *J. Symb. Comput.*, 50:197–207, 2013.

[Fis01] G. Fischer. *Plane Algebraic Curves*. AMS, 2001.

[GG03] J. V. Z. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2 edition, 2003.

[HS83] D. L. Hilliker and E. G. Straus. Determination of bounds for the solutions to those binary Diophantine equations that satisfy the hypotheses of Runge's theorem. *Trans. AMS*, 280(2):637–657, 1983.

[Ina05] D. Inaba. Factorization of multivariate polynomials by extended Hensel construction. *SIGSAM Bull.*, 39(1):2–14, 2005.

[IS07] D. Inaba and T. Sasaki. A numerical study of extended Hensel series. In *SNC*, pages 103–109, 2007.

[Iwa03] M. Iwami. Analytic factorization of the multivariate polynomial. *Proc. of CASC'03*, pages 213–225, 2003.

[KT78] H. T. Kung and J. F. Traub. All algebraic functions can be computed fast. *J. ACM*, 25(2):245–260, 1978.

[Kuo89] T. Kuo. Generalized Newton-Puiseux theory and Hensel's lemma in $\mathbb{C}[x, y]$. *Canad. J. Math.*, 41:1101–1116, 1989.

[LM83] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. In *STOC*, pages 140–151, 1983.

[LR07] D. Lazard and F. Rouillier. Solving parametric polynomial systems. *J. Symb. Comput.*, 42(6):636–667, 2007.

[MC13] B. Mannaa and T. Coquand. Dynamic Newton-Puiseux theorem. *J. Logic & Analysis*, 5, 2013.

[McC42] N. H. McCoy. Remarks on divisors of zero. *The American Mathematical Monthly*, 49(5):286–295, 1942.

[Mum99] D. Mumford. *The Red Book of Varieties and Schemes*. Springer-Verlag, 2nd edition, 1999.

[MXX12] M. Moreno Maza, B. Xia, and R. Xiao. On solving parametric polynomial systems. *Mathematics in Computer Science*, 6(4):457–473, 2012.

[MY73] J. Moses and D.Y.Y. Yun. The EZ-GCD algorithm. In *Proc. ACM National Conference*, pages 159–166, 1973.

[PR15] A. Poteaux and M. Rybowicz. Improving complexity bounds for the computation of Puiseux series over finite fields. In *Proc. of ACM on ISSAC*, pages 299–306, 2015.

[SI16] T. Sasaki and D. Inaba. Enhancing the extended Hensel construction by using Gröbner bases. In *CASC*, volume 9890, pages 457–472, 2016.

[SK99] T. Sasaki and F. Kako. Solving multivariate algebraic equation by Hensel construction. *Japan J. Indust. and Appl. Math.*, 1999.

[SY98] T. Sasaki and S. Yamaguchi. An analysis of cancellation error in multivariate Hensel construction with floating-point number arithmetic. In *ISSAC*, pages 1–8, 1998.

[Tra76] B. M. Trager. Algebraic factoring and rational function integration. In *SYMSAC*, pages 219–226, 1976.

[Tsu09] K. Tsuji. An improved EZ-GCD algorithm for multivariate polynomials. *J. Symb. Comput.*, 44(1):99–110, 2009.

[Vap] I. B. Vapnyarskii. *Encyclopedia of Mathematics*, chapter Lagrange multipliers. Springer.

[VHC15] J. D. Vélez, J. P. Hernández, and C. A. Cadavid. Limits of quotients of real polynomial functions of three variables. *ArXiv e-prints*, May 2015.

[VHC17] J. D. Velez, J. P. Hernandez, and C. A. Cadavid. Limits of quotients of polynomial functions in three variables. *ACM Commun. Comput. Algebra*, 51(2):42–56, October 2017.

[XZ14] S.J. Xiao and G.X. Zeng. Determination of the limits for multivariate rational functions. *Science China Mathematics*, 57(2):397–416, 2014.

[YHX01] L. Yang, X. R. Hou, and B. Xia. A complete algorithm for automated discovering of a class of inequality-type theorems. *Science in China, Series F*, 44(1):33–49, 2001.

Curriculum Vitae

Name: Masoud Ataei Jaliseh

Education

University of Western Ontario
London, ON
2016 - 2017 M.Sc. in Computer Science

University of Western Ontario
London, ON
2011 - 2015 Ph.D. in Mathematics

Institute for Advanced Studies in Basic Sciences (IASBS)
Zanjan, Iran
2009–2011 MSc in Mathematics

Related Work Experience: Teaching Assistant
The University of Western Ontario
2016 - 2017

Publications:

- Parisa Alvandi, Masoud Ataei, Mahsa Kazemi and Marc Moreno Maza, *On the Extended Hensel Construction and its Application to the Computation of Real Limit Points* (submitted to Journal of Symbolic Computation).
- Parisa Alvandi, Masoud Ataei and Marc Moreno Maza, *On the extended Hensel construction and its application to the computation of limit points* Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation. ACM, 2017.
- Masoud Ataei, Ján Mináč and Nguyễn Duy Tân, *Description of Galois unipotent extensions* Journal of Algebra 471 (2017): 193-219.
- Masoud Ataei, *A new good Galois tower of function fields over finite fields* (In Progress).