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

Parisa Alvandi
University of Western Ontario
palvandi@uwo.ca

Masoud Ataei
University of Western Ontario
mataeija@uwo.ca

Marc Moreno Maza
University of Western Ontario
moreno@csd.uwo.ca

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, and, for the multivariate case, can be seen as an effective variant of Jung-Abhyankar Theorem. 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 the computation of real branches of space curves.

CCS CONCEPTS

• **Computing methodologies** → **Symbolic and algebraic manipulation**; *Symbolic and algebraic manipulation*; Algebraic algorithms;

KEYWORDS

Extended Hensel Construction; Wronskian matrices; real branches of space curves; limit points of constructible sets

```
> 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);
```

$$\left[\left[x = \frac{-\mathrm{RootOf}(\_Z^2 + y) + \mathrm{RootOf}(\_Z^2 + y)\, y - \frac{1}{2}\,\mathrm{RootOf}(\_Z^2 + y)\, z + \frac{1}{2}\, y^2}{y}\right],\right.$$
$$\left[x = \frac{\mathrm{RootOf}(\_Z^2 + y) - \mathrm{RootOf}(\_Z^2 + y)\, y + \frac{1}{2}\,\mathrm{RootOf}(\_Z^2 + y)\, z + \frac{1}{2}\, y^2}{y}\right],$$
$$\left.[x = -y]\right]$$

Figure 1: EHC applied to a trivariate polynomial.

1 INTRODUCTION

The *Extended Hensel Construction* (EHC) is an algorithm which is used for factorizing univariate polynomials with power series coefficients. It was proposed in [22] 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 1 illustrates our implementation of the EHC in the `PowerSeries` library, available at www.regularchains.org.

The work of Sasaki and Kako was further extended by their students, see the papers [11–13, 21, 23]. See also the works of S. Abhyankar [1] and T.-C. Kuo [15]. The EHC relies on the so-called *Yun-Moses polynomials* originally introduced in [18], studied in [25], and called *Lagrange interpolation polynomials* in [22]. 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 [21], Sasaki and D. Inaba suggest to use Gröbner bases instead.

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 $O(d^3\,\mathsf{M}(d))$ operations in $\mathbb{K}$, where $n \longmapsto \mathsf{M}(n)$ is a (polynomial) multiplication time [9]. 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 $O(k\,d\,\mathsf{M}(d)^2)$ operations in $\mathbb{K}$ (instead of $O(k^2\,d\,\mathsf{M}(d)^2)$ in a direct approach) or within $O(k\,d\,\mathsf{M}(d))$ operations in the algebraic closure of $\mathbb{K}$. These enhancements of the EHC are described in Sections 3 to 4, and supported by the experimentation reported in Section 6.

In [14], 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 $O(d\,k\,\mathsf{M}(k))$ operations in $\mathbb{C}$ using a *linear lifting scheme* (Theorem 5.2 in [14]) and $O(d\,\mathsf{M}(k))$ operations in $\mathbb{C}$ using a *quadratic lifting scheme* (Corollary 5.1 in [14]). This latter estimate is improved in [7] 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 [19].

In both [14] and [7], the estimated cost is for computing a *single branch*. Thus, for computing all branches, the costs of the linear and quadratic lifting schemes of [14] become respectively $O(d^2\,k\,\mathsf{M}(k))$ and $O(d^2\,\mathsf{M}(k))$ 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 $O(k^2\,d\,\mathsf{M}(d))$ operations in $\mathbb{C}$. The experimentation reported in Section 6 show that, for problems of practical interest, an EHC implementation can outperform counterparts based on the linear and quadratic lifting schemes of [14]. 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

ISSAC '17, July 25-28, 2017, Kaiserslautern, Germany

ACM ISBN 978-1-4503-5064-8/17/07…$15.00
https://doi.org/10.1145/3087604.3087658

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 $O(d^3\mathsf{M}(d) + k^2\, d\, \mathsf{M}(d))$ for the EHC and $O(d^2\, k\, \mathsf{M}(k))$ (resp. $O(d^2\, \mathsf{M}(k))$) the algorithm of Kung and Traub using a linear (resp. quadratic) lifting scheme.

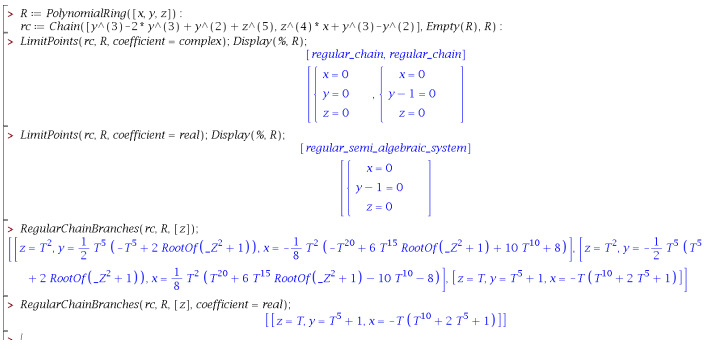

Figure 2: Computational of limit points: complex and real cases.

In addition to polynomial factorization, the EHC can be applied to the computation of limits of multivariate rational functions [3] and tangent cones [4]. In [2], an algorithm is proposed for computing the non-trivial limit points of the quasi-component $W(T)$ of a regular chain $T \subset \mathbb{Q}[X_1,\ldots,X_n]$. In this paper, 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 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) $W_{\mathbb{R}}(T)$ (real case). Section 5 is devoted to this question.

2 EXTENDED HENSEL CONSTRUCTION

The purpose of this paper requires a somehow detailed review of the EHC. Most of the proofs are omitted, though, and we refer to [22]. We also recall the notion of Puiseux series and refer to the book of G. Fischer [8] for this topic.

Notation 1. *Let $F(X,Y) \in \mathbb{C}[X,Y]$ 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 2 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 (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 $\hat{\delta},\hat{d} \in \mathbb{Z}^{>0}$ such that $\hat{\delta}/\hat{d} = \delta/d$ and $\gcd(\hat{\delta},\hat{d}) = 1$ 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 Newton's polynomial is a homogeneous polynomial in $(X, Y^{\delta/d})$. Let $\zeta_1,\ldots,\zeta_r \in \mathbb{C}$ be the distinct roots of $F^{(0)}(X,1)$, for some $r \geq 2$. 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 $\hat{Y} = Y^{\hat{\delta}/\hat{d}}$.

Puiseux series. Let $\mathbb{K}$ be an algebraic number field and $\overline{\mathbb{K}}$ its algebraic closure. We denote by $\mathbb{K}[[Y]]$ and $\mathbb{K}\langle Y\rangle$ the respective rings of formal power series and convergent power series in Y with coefficients in $\mathbb{K}$. We denote by $\mathbb{K}[[Y^*]] = \bigcup_{\ell=1}^{\infty} \mathbb{K}[[Y^{\frac{1}{\ell}}]]$ the ring of *formal Puiseux series*. Hence, given $\varphi \in \mathbb{K}[[Y^*]]$, there exists $\ell \in \mathbb{N}_{>0}$ such that $\varphi \in \mathbb{K}[[Y^{\frac{1}{\ell}}]]$ holds and we can write $\varphi = \sum_{m=0}^{\infty} a_m Y^{\frac{m}{\ell}}$, for some $a_0,\ldots,a_m,\ldots \in \mathbb{K}$. We denote by $\mathbb{K}((Y^*))$ the quotient field of $\mathbb{K}[[Y^*]]$. Let $\varphi \in \mathbb{K}[[Y^*]]$ and $\ell \in \mathbb{N}$ such that $\varphi = f(Y^{\frac{1}{\ell}})$ holds for some $f \in \mathbb{K}[[Y]]$. We say that the Puiseux series φ is *convergent* if we have $f \in \mathbb{K}\langle Y\rangle$. The ring of convergent Puiseux series is denoted by $\mathbb{K}\langle Y^*\rangle$ and its quotient field by $\mathbb{K}(\langle Y^*\rangle)$. We recall Puiseux's theorem: if $\mathbb{K}$ is an algebraically closed field of characteristic zero, the field $\mathbb{K}((Y^*))$ 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.

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 $G_i(X,Y) \in \mathbb{C}(\langle Y^*\rangle)[X]$ and $\deg_X(G_i) = m_i$, for $1 \leq i \leq r$. Thus, the EHC factorizes $F(X,Y)$ over $\mathbb{C}(\langle Y^*\rangle)$. However, $\deg_X(G_i) = 1$ may not hold for some i. Nevertheless, as shown hereafter 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. While we include a proof of Theorem 1 in order to develop the results of Section 4 we refer to [22] for a proof of Lemma 1.

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

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

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

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 $G_1^{(0)}(X,Y),\ldots,G_r^{(0)}(X,Y)$ the initial factors of $F^{(0)}(X,Y)$. Hence we have $G_i^{(0)}(X,Y) = (X-\zeta_i Y^{\hat{\delta}/\hat{d}})^{m_i}$ for $i=1,\ldots,r$ and $\zeta_i \in \mathbb{C}$. We define the ideal*

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

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

$$F(X,Y) = G_1^{(k)}(X,Y)\cdots G_r^{(k)}(X,Y) \mod S_{k+1}, \quad (2)$$

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

Proof. 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

$$\Delta F^{(k)}(X,Y) = f_{d-1}^{(k)} X^{d-1} Y^{\hat{\delta}/\hat{d}} + \cdots + f_0^{(k)} X^0 Y^{d\hat{\delta}/\hat{d}} \quad (3)$$

where $f_\ell^{(k)} = c_\ell^{(k)} Y^{k/\hat{d}}$ 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: $\Delta G_i^{(k)}(X,Y) \equiv 0 \mod S_k$. Then we have:

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

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

$$\Delta F^{(k)} \equiv \Delta G_1^{(k)}\frac{F^{(0)}}{G_1^{(0)}} + \cdots + \Delta G_r^{(k)}\frac{F^{(0)}}{G_r^{(0)}} \mod S_{k+1}. \quad (4)$$

If in Lemma 1, we let $\hat{G}_i(X,\hat{Y}) = G_i^{(0)}(X,\hat{Y})$, combining Equations (3) and (4), one can solve for $\Delta G_1^{(k)},\ldots,\Delta G_r^{(k)}$

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

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

Remark 2. *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 3. *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 [17]. 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

1: **procedure** EHC_Lift(F,k)
2: Compute the Newton polynomial $F^{(0)}$ and $\hat{\delta},\hat{d}$;
3: Compute $F^{(0)} = G_1^{(0)}\cdots G_r^{(0)}$, see Remark 1
4: **if** $r=1$ **then**
5: Apply the change of variable in Remark 3
6: **end if**
7: Compute the Yun-Moses polynomial $W_i^{(\ell)}$ for $i=1,\cdots,r$ and $\ell=0,\cdots,d-1$; (see Section 3)
8: **for** $j=1,\ldots,k$ **do**
9: 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 [22]);
10: Compute $\Delta G_i^{(j)} = \sum_{\ell=0}^{m-1} W_i^{(\ell)} f_\ell^{(j)}$, for $i=1,\cdots,r$;
11: Let $G_i^{(j)} = G_i^{(j-1)} + \Delta G_i^{(j)}$ for $i=1,\cdots,r$;
12: **end for**
13: Reverse the change of variable, if any;
14: **return** $G_1^{(k)},\ldots,G_r^{(k)}$;
15: **end procedure**

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 [10] suggests a minimum accuracy of $B := 2\,deg_X(F)\,deg_Y(F)$.

After applying EHC_Lift(F,k) with $k = \hat{d}B - \hat{\delta}$, 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 $\hat{d}B' - \hat{\delta}$, 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 [22] for details. This process generates a tree of calls to the EHC. Obviously, one needs to do at most d calls in total.

3 ON THE YUN-MOSES POLYNOMIALS

We use the notations of Section 2, including the proof of Theorem 1. Define $\tilde{Y} = Y^{1/\hat{d}}$.

LEMMA 2. *We have $\Delta F^{(k)} \in \mathbb{K}[X, \tilde{Y}]$, 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

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

where $f_\ell^{(k)} = c_\ell^{(k)} \tilde{Y}^k$ 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 $\Delta F^{(1)} \in \mathbb{K}[X, \tilde{Y}]$. Now assume $\Delta F^{(k-1)} \in \mathbb{K}[X, \tilde{Y}]$, thus $G_1^{(k-2)} \cdots G_r^{(k-2)} = F - \Delta F^{(k-1)} \in \mathbb{K}[X, \tilde{Y}]$. We want to prove $\Delta F^{(k)} \in \mathbb{K}[X, \tilde{Y}]$. In modulo S_{k+1}, we have

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

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

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

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

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

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

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

$$\sum_{i=1}^r W_i^{(\ell)} \frac{F^{(0)}}{G_i^{(0)}} = X^\ell \hat{Y}^{d-\ell} \text{ for } \ell = 0, \cdots d-1, \tag{5}$$

where $\hat{Y} = Y^{\hat{\delta}/\hat{d}}$ with $G_i^{(0)} = (X - \zeta_i \hat{Y})^{m_i}$ 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 $W_i^{(\ell)} = \sum_{j=0}^{m_i-1} w_{i,j}^{(\ell)}(\hat{Y}) X^j$ 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 (5) and let $X = \zeta_\lambda \hat{Y}$ in those derivatives. In other words, we have

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

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

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

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

$$\sum_{j=0}^{m_\lambda - 1} \frac{\partial^\mu}{\partial X^\mu} \left(X^j \frac{F^{(0)}}{G_\lambda^{(0)}} \right) \Big|_{X = \zeta_\lambda \hat{Y}} w_{\lambda,j}^{(\ell)} = \frac{\partial^\mu}{\partial X^\mu} (X^\ell \hat{Y}^{d-\ell}) \Big|_{X = \zeta_\lambda \hat{Y}}. \tag{6}$$

On the other hand, $\frac{\partial^\mu}{\partial X^\mu} \left(\frac{F^{(0)}}{G_\lambda^{(0)}} \right) \Big|_{X = \zeta_\lambda \hat{Y}} = \frac{1}{m_\lambda!} \frac{\partial^{\mu + m_\lambda}}{\partial X^{\mu + m_\lambda}} (F^{(0)}) \Big|_{X = \zeta_\lambda \hat{Y}}$. Since $F^{(0)} \in \mathbb{K}[X, \hat{Y}]$, we have $\frac{\partial^\mu}{\partial X^\mu} \left(\frac{F^{(0)}}{G_\lambda^{(0)}} \right) \Big|_{X = \zeta_\lambda \hat{Y}} \in \mathbb{K}(\zeta_\lambda)[\hat{Y}]$. So, Equation (6) is a system of linear equations $\mathcal{W}_\lambda \mathcal{X}_\lambda^{(\ell)} = \mathcal{B}_\lambda^{(\ell)}$ in $\mathbb{K}(\zeta_\lambda)[\hat{Y}]$ (also see [22]) with coefficient matrix

$$\mathcal{W}_\lambda = [\alpha_{j,\mu}] \text{ with } \alpha_{j,\mu} = \frac{\partial^\mu}{\partial X^\mu} \left(X^j \frac{F^{(0)}}{G_\lambda^{(0)}} \right) \Big|_{X = \zeta_\lambda \hat{Y}}, \tag{7}$$

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

$$\mathcal{B}_\lambda^{(\ell)} = [\beta_\mu] \text{ with } \beta_\mu = \frac{\partial^\mu}{\partial X^\mu} (X^\ell \hat{Y}^{d-\ell}) |_{X = \zeta_\lambda \hat{Y}} \tag{8}$$

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 [6]. In our case, the functions $\left(X^j \frac{F^{(0)}}{G_\lambda^{(0)}} \right) |_{X = \zeta_\lambda \hat{Y}}$, for $j = 0, 1, \ldots, m_\lambda - 1$, are, indeed, linearly independent polynomials in $\mathbb{K}(\zeta_\lambda)[\hat{Y}]$, therefore, the Wronskian matrix $\mathcal{W}_\lambda$ is invertible. Now let us find the inverse of $\mathcal{W}_\lambda$. Let $f := \left(\frac{F^{(0)}}{G_\lambda^{(0)}} \right) |_{X = \zeta_\lambda \hat{Y}} \in$ and $f^{(\mu)} := \left(\frac{\partial^\mu}{\partial X^\mu} \frac{F^{(0)}}{G_\lambda^{(0)}} \right) \Big|_{X = \zeta_\lambda \hat{Y}}$ for $\mu = 1, \ldots, m_\lambda - 1$.

PROPOSITION 1. *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 $M_2 = [\gamma_{j,k}]$ with $\gamma_{j,k} = (-1)^{j+k}\binom{k}{k-j}\zeta_\lambda^{k-j}\hat{Y}^{k-j}$ 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 $\binom{k}{k-j}\zeta_\lambda^{k-j}\hat{Y}^{k-j}$ 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 $A|_{T=\zeta_\lambda\hat{Y}} \cdot M_2 = I$ 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:

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

The above quantity is also equal to each side of Equation (9):

$$\binom{k}{j}\sum_{l=0}^{k-j}(-1)^{k+j+l}\binom{k-j}{l}T^l\zeta_\lambda^{k-j-l}\hat{Y}^{k-j-l} = \binom{k}{j}(T-\zeta_\lambda\hat{Y})^{k-j}. \quad (9)$$

So for $k = j$, the right hand side of Equation (9) equals 1, and when $k \ne j$ (i.e. $k > j$), by evaluating $T = \zeta_\lambda\hat{Y}$, it is 0. Hence, we have $A|_{T=\zeta_\lambda\hat{Y}} \cdot M_2 = I$ and $M_2^{-1} = A|_{T=\zeta_\lambda\hat{Y}}$, 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 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 $X = \zeta_\lambda\hat{Y}$, the $(j+1,k+1)-$entry of $M_{1(m_\lambda-1)}\cdots M_{10}\mathcal{W}_\lambda$ is

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

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

Proof. From Lemma 1, we have $W_\lambda^\ell \in \mathbb{C}\langle\hat{Y}\rangle[X]$. 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 $\mathbb{K}[X,\hat{Y}]$ and $\mathbb{K}(\zeta_\lambda)[X,\hat{Y}]$, respectively. For any $\mu = 0,1,\ldots,m_\lambda - 1$, we have

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

Hence, the coefficients of all entries of $\mathcal{W}_\lambda^{-1}$, defined in Proposition 1, live in $\mathbb{K}(\zeta_\lambda)$. Also, observe that the coefficients of all entries in matrix $\mathcal{B}_\lambda^{(\ell)}$ defined in (8) 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 $W_\lambda^{(\ell)} \in \mathbb{K}(\zeta_\lambda)\langle Y\rangle[X]$. □

We discuss how we compute the Yun-Moses polynomials W_λ. We regard 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 $\hat{Y} = Y^{\hat{\delta}/\hat{d}}$. Therefore, we 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 $X = \zeta_\lambda\hat{Y}$. Since $\frac{F^{(0)}}{G_\lambda^{(0)}}(X,\hat{Y})$ is a homogeneous polynomial, then f, as defined before Proposition 1, is just a term in $\hat{Y}$. Therefore, all entries of $\mathcal{W}_\lambda^{-1}$ are just terms in $\hat{Y}$; 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 $\hat{Y}$ and keep track of the degree of $\hat{Y}$ in each entry.

Let $f := F^{(0)}(X,\hat{Y})/(X-\zeta_\lambda\hat{Y})^{m_\lambda}$, 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 1. After evaluation at $X = \zeta_\lambda\hat{Y}$, 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 $j \ge k$. In M_2, the degree of $\hat{Y}$ on the $(j,k)-$entry is $k-j$ for $j,k = 1,\ldots,m_\lambda$ with $k \ge j$. Hence, the $\hat{Y}$-degree in the $(j,k)-$entry of $\mathcal{W}_\lambda^{-1}$ is $2m_\lambda - d + k - j$.

Let $\mathsf{A}(n)$ 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: $\mathsf{A}(n) \in O(\mathsf{M}(n))$. 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 1. Therefore, the cost C_{YM} of computing the Yun-Moses polynomials $W_\lambda^{(\ell)}$, for $\ell \in \{0,\ldots,d-1\}$, is given by $C_{\mathrm{YM}} = C_1 + C_2 = O(m_\lambda^3\,\mathsf{M}(d))$. This leads us to:

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

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 [5], we make this running-time in $\Theta(i)$ instead of $\Theta(i^2)$.

Let $\tilde{Y} = Y^{1/\hat{d}}$. 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 $(X, \hat{Y})$ 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 [5] 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

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

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

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

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

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

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:

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

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

$$q_j^{k+1} = p_{j-1}^{k+1,0}\Delta_j^k + q_{j-1}^{k+1}\Delta_j^0 \text{ with } q_2^{k+1} = \Delta_2^k\Delta_1^0 + \Delta_2^0\Delta_1^k. \quad (10)$$

Now observe that we have

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

Therefore, we can write

$$P_j^{k+1} = P_j^k + q_j^{k+1}\tilde{Y}^k + \left(p_{j-1}^{k+1,1}\Delta_j^k + \cdots + p_{j-1}^{k+1,k+1}\Delta_j^0\right)\tilde{Y}^{k+1}. \quad (11)$$

Note: the term q_j^{k+1} is missing in the formula at the top of the left column on p. 3 of [5].

It follows from Equation (11) 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 (10) and (11)) and k multiplications for the new terms (see Equation(11)). All multiplications are product of a polynomial of degree m_j to a polynomial of degree $m_1 + \cdots + m_{j-1}$. Let C_{lift} be the cost of computing P_r^{k+1}. We have: $C_{\text{lift}} = \sum_{l=2}^{r}(k+2)\mathsf{M}(\max(m_1 + \cdots + m_{l-1}, m_l))\mathsf{A}(d)$. This leads us to the following result.

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

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 [2], 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 $W(T)$). We are now interested in 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. To this end, we adapt the algorithm of [2]. The LimitPoints command of the RegularChains library in Maple handles both cases, $\overline{W(T)} \setminus W(T)$ and $\overline{W_{\mathbb{R}}(T)} \setminus W_{\mathbb{R}}(T)$. The *Puiseux parametrizations* of the regular chain T in Definition 1 encode all the branches of $V(\text{sat}(T))$ when the free variable U approaches zero. It is proved in [2] that the non-trivial limit points of $W(T)$ around $U = 0$, where $U = 0$ is a root of the product h_T of the initials of T, are obtained by letting U to be zero in all the Puiseux parametrizations of T around $U = 0$. Therefore, for computing all the non-trivial limit points of $W(T)$, one needs to compute all the Puiseux parametrizations of T when U approaches any root of h_T.

Definition 1. *Let $T := \{t_1, \ldots, t_{n-1}\} \subset \mathbb{Q}[X_1 < \cdots < X_n]$ be a one-dimensional and strongly normalized regular chain whose free variable is $U = X_1$. Thus, the product h_T of the initials of T is a univariate polynomial in X_1. Assume that $X_1 = 0$ is a root of h_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 positive 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 $\varsigma := \text{lcm}(\varsigma_2, \ldots, \varsigma_n)$ 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 $U = 0$.*

Remark 4. *If α is a root of h_T, one can define the Puiseux parametrizations of T at $X_1 = \alpha$, by reducing to the case $\alpha = 0$ via a change of coordinates and proceed as in Definition 1. For convenience, when we talk about any Puiseux parametrization of T at a root of h_T, we assume w.l.o.g that the given Puiseux parametrization is for $X_1 = 0$. Observe that $(U^s, \phi_2, \ldots, \phi_n)$ belongs to $\mathbb{C}\langle U\rangle^n$.*

Definition 2. *Using the notations of Definition 1, the Puiseux parametrization $(U^s, \phi_2, \ldots, \phi_n)$ is called a* real Puiseux parametrization *of T if $\phi_i \in \mathbb{R}\langle U\rangle$, for $i = 2, \ldots, n$.*

As we shall see, one can obtain the non-trivial limit points of $Z_{\mathbb{R}}(T)$ by computing the real Puiseux parametrizations of $Z_{\mathbb{R}}(T)$ when its free variable approaches any root of h_T. Proposition 2 gives a characterization of all the Puiseux expansions of a univariate polynomial over the field of convergent univariate Puiseux series.

Proposition 2. *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 $\chi_\ell(U) \in \mathbb{K}(\Theta_\ell^1, \ldots, \Theta_\ell^{\sigma_\ell})((U^*))$., $i = 1, \ldots, \sigma_\ell$.

Proposition 2 follows from the *extended Hensel construction*. 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 roots of each polynomial $h_\ell^i(Y)$ will appear in some of Puiseux expansions of $f(U, Y)$. Since some of those roots may not be real, it is necessary to use an encoding of the roots of $h_\ell^i(Y)$ that allows us to separate the real ones from the others. For simplicity of presentation, we do that by considering the splitting fields of $h_\ell^i(Y)$, see Remark 5. For computational efficiency, one should prefer techniques based on *real algebraic closures* as in [20].

Remark 5. *Let $h(Y) \in \mathbb{K}[Y]$ be an irreducible and monic polynomial with degree s. Denote by $\frac{\mathbb{K}[X_1, \ldots, X_n]}{\langle F\rangle}$ the residue class ring of $\mathbb{K}[X_1, \ldots, X_n]$ w.r.t. to F, for $F \subset \mathbb{K}[X_1, \ldots, X_n]$. 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 $h(Y)$. See [16] and [24].*

Using regular chains $R_1, \ldots, R_{s'}$ in Remark 5, 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.

Definition 3. *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 a* regular chain encoding of Θ.

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

```
1: procedure RealPuiseuxExpansions(f(U,Y), U = 0)
2:     B := Puiseux expansions of f(U,Y) at U = 0;
3:     R := {};
4:     for χ(U) ∈ B do
5:         let χ(U) ∈ K(Θ^1, ..., Θ^σ)((U^*));
6:         let R^i_{j_i} ⊂ K[X_{i,1}, ..., X_{i,j_i}] be the zero-dimensional regular chain encoding the algebraic number Θ^i, for i = 1, ..., σ;
7:         let C be a regular chain encoding the field K;
8:         F := C ∪ R^1_{j_1} ∪ ··· ∪ R^σ_{j_σ};
9:         if RealTriangularize(F) ≠ ∅ then
10:            R := R ∪ {χ(U)};
11:        end if
12:    end for
13:    return R;
14: end procedure
```

Following up on Definition 3, determining whether or not 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 the 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 real solutions, then we deduce that Θ is a real algebraic number over $\mathbb{K}$.

Algorithm 2 implements the above idea and computes the real Puiseux expansions of the 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.

Proposition 3. *With the notations of Definition 1, consider the Puiseux parametrization $(U^s, \phi_2, \ldots, \phi_n)$ 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. Moreover, $(U^s, \phi_2(U), \ldots, \phi_n(U))$ is a real Puiseux parametrization of T if and only if $\mathbb{K}_n$ is a real extension of $\mathbb{Q}$.*

6 EXPERIMENTATION

Table 1 gathers running times for comparing the EHC and Kung-Traub's method for $k = 10$ and $k = 20$, where k is as in Section 1. 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 from 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 [22]. 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 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. These experimental results were obtained on an Ubuntu desktop (1.6GHz Intel(R) Xeon(R) CPU).

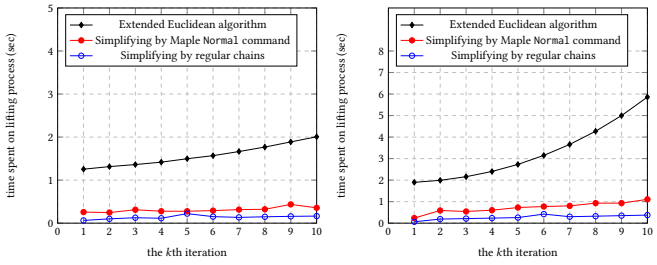

Figure 3: For each k on the x-axis, these plots show the time spent for lifting the factors of EHC, from step $k-1$ to step k see Lines 8-12 in Algorithm 1: (1) the black curve corresponds to the original EHC [22]; (2) The red curve corresponds to the implementation of EHC with the optimization tricks 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 1: Comparing EHC versus Kung-Traub's method

Figure 3 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.

Acknowledgements

The authors are grateful to Professor Tateaki Sasaki for his suggestions and comments. The authors would also like to thank the referees for their helpful comments.

REFERENCES

[1] S. S. Abhyankar. 1989. Irreducibility criterion for germs of analytic functions of two complex variables. *Advances in Mathematics* 74, 2 (1989), 190 – 257.
[2] P. Alvandi, C. Chen, and M. Moreno Maza. 2013. Computing the Limit Points of the Quasi-Component of a Regular Chain in Dimension One. In *Proc. of CASC*, Vol. 8136. 30–45.
[3] P. Alvandi, M. Kazemi, and M. Moreno Maza. 2016. Computing Limits of Real Multivariate Rational Functions. In *ISSAC*. 39–46.
[4] P. Alvandi, M. Moreno Maza, É. Schost, and P. Vrbik. 2015. A Standard Basis Free Algorithm for Computing the Tangent Cones of a Space Curve. In *CASC*. 45–60.
[5] L. Bernardin. 1998. On Bivariate Hensel and Its Parallelization. In *ISSAC*. 96–100.
[6] M. Bocher. 1900. The Theory of Linear Dependence. *Annals of Mathematics, Second Series* 2, 1/4 (1900), 81–96.
[7] D. V. Chudnovsky and G. V. Chudnovsky. 1986. On expansion of algebraic functions in power and Puiseux series, I. *J. Complexity* 2, 4 (1986), 271–294.
[8] G. Fischer. 2001. *Plane Algebraic Curves*. AMS.
[9] J. V. Z. Gathen and J. Gerhard. 2003. *Modern Computer Algebra* (2 ed.). Cambridge University Press.
[10] D. L. Hilliker and E. G. Straus. 1983. Determination of Bounds for the Solutions to those Binary Diophantine Equations that Satisfy the Hypotheses of Runge's Theorem. *Trans. AMS* 280, 2 (1983), 637–657.
[11] D. Inaba. 2005. Factorization of Multivariate Polynomials by Extended Hensel Construction. *SIGSAM Bull.* 39, 1 (2005), 2–14.
[12] D. Inaba and T. Sasaki. 2007. A Numerical Study of Extended Hensel Series. In *SNC*. 103–109.
[13] M. Iwami. 2003. Analytic Factorization of the Multivariate Polynomial. In *CASC*. 213–225.
[14] H. T. Kung and J. F. Traub. 1978. All Algebraic Functions Can Be Computed Fast. *J. ACM* 25, 2 (1978), 245–260.
[15] T. Kuo. 1989. Generalized Newton-Puiseux Theory and Hensel's Lemma in $\mathbb{C}[x, y]$. *Canad. J. Math.* 41 (1989), 1101–1116.
[16] S. Landau and G. L. Miller. 1983. Solvability by Radicals is in Polynomial Time. In *STOC*. 140–151.
[17] B. Mannaa and T. Coquand. 2013. Dynamic Newton-Puiseux theorem. *J. Logic & Analysis* 5 (2013).
[18] J. Moses and D.Y.Y. Yun. 1973. The EZ-GCD algorithm. In *Proc. ACM National Conference*. 159–166.
[19] A. Poteaux and M. Rybowicz. 2015. Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields. In *ISSAC*. 299–306.
[20] R. Rioboo. 1992. Real Algebraic Closure of an Ordered Field: Implementation in *Axiom*. In *ISSAC*. 206–215.
[21] T. Sasaki and D. Inaba. 2016. Enhancing the Extended Hensel Construction by Using Gröbner Bases. In *CASC*, Vol. 9890. 457–472.
[22] T. Sasaki and F. Kako. 1999. Solving multivariate algebraic equation by Hensel construction. *Japan J. Indust. and Appl. Math.* (1999).
[23] T. Sasaki and S. Yamaguchi. 1998. An Analysis of Cancellation Error in Multivariate Hensel Construction with Floating-point Number Arithmetic. In *ISSAC*. 1–8.
[24] B. M. Trager. 1976. Algebraic Factoring and Rational Function Integration. In *SYMSAC*. 219–226.
[25] K. Tsuji. 2009. An improved EZ-GCD algorithm for multivariate polynomials. *J. Symb. Comput.* 44, 1 (2009), 99–110.