Determining Puiseux Expansions by Hensel's Lemma and Dynamic Evaluation

Gema Diaz–Toca⋆1 and Laureano Gonzalez–Vega⋆2

[1] Departamento de Matematica Aplicada
Universidad de Murcia, Murcia, Spain
gemadiaz@um.es

[2] Departamento de Matemáticas, Estadística y Computación
Universidad de Cantabria, Santander, Spain
gvega@matesco.unican.es

Abstract. This paper is devoted to showing how to compute the Puiseux expansions of a polynomial in $\mathbb{L}[x, y]$ with $\mathbb{L}$ an algebraically closed field of characteristic 0 by using a matricial version of Hensel's Lemma over the companion matrix of the considered polynomial together with *Dynamic Evaluation* to deal with the involved algebraic numbers. First experimental results show a better behaviour than the classical methods based upon the Newton polygon.

1 Introduction

Let $\mathbb{L}$ be an algebraically closed field of characteristic 0. Let $f(x, y)$ be a monic and squarefree polynomial in y:

$$f(x, y) = y^n + a_{n-1}(x)y^{n-1} + \ldots + a_0(x),$$

with $a_i \in \mathbb{L}[x]$ and $a_0(x) \neq 0$. Puiseux's Theorem asserts the existence of n distinct formal series

$$y_i(x) = \sum_{k=b_i}^{\infty} c_{k,i}(x^{1/e_i})^k \quad (i = 1, \ldots, n),$$

such that $f(x, y_i(x)) = 0$ (i.e. each $y_i(x)$ is a root of $f(x, y)$ as polynomial in y). This paper studies the application of a version of Hensel's Lemma, called Hensel's matrix Lemma, to compute these roots. These roots belong to the so called Puiseux series field presented into the next definition.

Definition 1. *The union of all the fields* $\mathbb{L}((x^{1/n}))$, $\mathbb{L}((x))^*$, *is called the Puiseux series field.*

Furthermore the roots are called the n Puiseux expansions at $x = 0$ of the algebraic function y defined by $f(x, y) = 0$.

The field $\mathbb{L}((x))^*$ is algebraically closed and the most popular proof can be found in [5]. This paper is devoted to presenting an algorithm to determine the Puiseux expansion based on [1] and [6]. The key of this algorithm is the iterative decomposition of the companion matrix of $f(x, y)$ (as polynomial in y) until obtaining its Jordan canonical form and hence its eigenvalues, i.e. the roots of $f(x, y)$. *Dynamic Evaluation* is also used in the algorithm to avoid computing too many explicit computations with algebraic numbers.

The rest of the paper is organized as follows. In Section 2 the required algebraic preliminaries are presented. Section 3 is devoted to presenting the algorithm while Section 5 shows how *Dynamic Evaluation* must be used in order to get good experimental results by managing simultaneously the computation with several algebraic numbers or, equivalently, by dealing at the same time with several branches of the algorithm.

2 Algebraic Preliminaries

The next version of Hensel's Lemma is to be used to decompose the companion matrix of $f(x, y)$ denoted by $M(f)$.

⋆ Partially supported by DGESIC PB 98-0713-C02-02 (Ministerio de Educación y Cultura)

Lemma 2. *(Hensel's matrix Lemma) Let (R, v) be a complete valued field with the topology defined by a discrete valuation v. Denote by $\mathcal{V}$ the valuation ring, by $\mathcal{M}$ its only maximal ideal and by $x \to \overline{x}$ the natural mapping to the residue field $\mathcal{R} = \mathcal{V}/\mathcal{M}$. Let A be a partitioned matrix over $\mathcal{V}$ in the form:*

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}.$$

If $\overline{A_2} = 0$ and the characteristic polynomials of $\overline{A_1}$ and $\overline{A_4}$ are coprime then A is similar over R to a matrix of the form:

$$\begin{pmatrix} \mathbb{I} & -H \\ 0 & \mathbb{I} \end{pmatrix} \cdot \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \cdot \begin{pmatrix} \mathbb{I} & H \\ 0 & \mathbb{I} \end{pmatrix} = \begin{pmatrix} A_1' & 0 \\ A_3 & A_4' \end{pmatrix},$$

where H is a matrix over $\mathcal{V}$.

Proof. Suppose that A is a n–square matrix and that A_1 is a j–square matrix. The matrix H is defined as the limit of the Cauchy sequence in $M_{j,n-j}(R) \approx R^{j(n-j)}$, $(X_r)_{r \in \mathbb{N}}$, defined recursively by:

$$\begin{aligned} X_0 &= 0 \\ X_r A_4 - A_1 X_r &= A_2 - X_{r-1} A_3 X_{r-1}, \quad 1 \leq r \end{aligned}$$

such that

$$A \approx \begin{pmatrix} A_1 - HA_3 & 0 \\ A_3 & A_4 + A_3 H \end{pmatrix}.$$

with $A_1' = A_1 - HA_3$ and $A_4' = A_4 + A_3 H$ (for more details, see [6]).

Note that the field $(\mathbb{L}((x)), v)$ is a complete valued field with the valuation given by:

$$\begin{array}{rccc} v: & \mathbb{L}((x)) & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ & \sum_{n=m}^{\infty} a_n x^n & \mapsto & \min\{n \in \mathbb{Z} : a_n \neq 0\} \end{array}$$

with $v(0) = \infty$. Its valuation ring is $\mathbb{L}[[x]]$, its maximal ideal is (x) and the residual field is $\mathbb{L}$. Thus, given a polynomial in $\mathbb{L}[[x]][y]$, if it has some roots with nonzero independent coefficient but not all of them, Hensel's matrix Lemma can be applied to decompose its companion matrix. Nevertheless, if all its roots have the independent coefficient equal to zero (i.e. all the coefficients of the polynomial are in the ideal (x)) then the next lemma must be applied.

Lemma 3.
Let $\mathbb{K}$ be a field. Let $\mathcal{V} = \mathbb{K}[[x]]$. Given a polynomial in $\mathbb{K}[[x]][y]$,

$$f(x, y) = y^n + a_{n-1}(x) y^{n-1} + \ldots + a_0(x),$$

with

$$n > 1, \quad a_0(x) \neq 0, \quad a_j(0) = 0, \quad 0 \leq j < n,$$

then there exist $h \in \mathbb{Q}$ with $h > 0$, $m \in \{0, \ldots, n-1\}$ and a matrix over $\mathbb{K}[[x]]^*$, denoted by D and given by:

$$D = \begin{pmatrix} 0 & \cdots & 0 & -d_0 \\ 1 & \cdots & 0 & -d_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & -d_{n-1} \end{pmatrix},$$

such that the characteristic polynomial of $x^h D$ is equal to $f(x, y)$ and $d_m(0) \neq 0$.

If there are entries of the matrix D which are not in $\mathbb{K}[[x]]$ but in $\mathbb{K}[[x]]^*$, it is necessary to make a change of variable before applying Hensel's matrix Lemma because $\mathbb{K}((x))^*$ does not have a discrete valuation.

3 The Description of the Algorithm

Given a monic and squarefree polynomial,

$$f(x,y) = y^n + a_{n-1}(x)y^{n-1} + \ldots + a_0(x),$$

with $a_0(x) \neq 0$, its companion matrix (with respect to y) is going to be decomposed by using Hensel's matrix Lemma, but the algebraic conditions required to apply such lemma are not always verified. In fact the independent coefficients of roots show when it is possible to apply Hensel's matrix Lemma without performing any change of variables first.

3.1 General Case

The polynomial $f(x,y)$ has some roots in $\mathbb{L}((x))^*$ with independent coefficient equal to zero and some roots with independent coefficient different from zero. Thus:

$$\overline{M(f)} = \begin{pmatrix} 0 & \cdots\cdots\cdots & 0 & 0 \\ 1 & & & \vdots \\ & \ddots & & 0 \\ & & 1 & -a_j(0) \\ & & \ddots & \vdots \\ & & 1 & -a_{n-1}(0) \end{pmatrix},$$

with $j > 0$ and $-a_j(0) \neq 0$. This implies that it is possible to apply Hensel's matrix Lemma to decompose $M(f)$ and so there exists a matrix H such that:

$$M(f) \approx \begin{pmatrix} M(f)_1 - HM(f)_3 & 0 \\ M(f)_3 & M(f)_4 + M(f)_3 H \end{pmatrix} = \begin{pmatrix} M(f)'_1 & 0 \\ M(f)_3 & M(f)'_4 \end{pmatrix},$$

Hence,

$$f(x,y) = \chi(M(f)'_1, y) \cdot \chi(M(f)'_4, y)$$

where $\chi(A,y)$ denotes the characteristic polynomial of A in y. The roots of the polynomial $\chi(M(f)'_1, y)$ are the roots of $f(x,y)$ whose independent coefficient is zero; so Case 3.3 (described later) is to be applied in order to decompose $M(f)'_1$. The roots of the polynomial $\chi(M(f)'_4, y)$ are the roots of $f(x,y)$ whose independent coefficient is nonzero; so Case 3.2 (described later) is applied in order to decompose its companion matrix.

3.2 All the Roots with Independent Coefficient Different from Zero

In this case, $a_0(0) \neq 0$ and applying Hensel's matrix Lemma to $M(f)$ is not possible. Let β be a root of $f(0,y)$ in $\mathbb{L}$. Let $F(x,y)$ be a polynomial defined as

$$F(x,y) = f(x, y + \beta).$$

Then, since the roots of $f(x,y)$ are obtained by adding β to the roots of $F(x,y)$, the algorithm goes on with the decomposition of $M(F)$. If the independent coefficient of all the roots of $f(x,y)$ is equal to β then Case 3.3 is applied. Otherwise, when only some roots of $f(x,y)$ have the independent coefficient equal to β, Case 3.1 is applied.

3.3 All the Roots with Independent Coefficient Equal to Zero

In this case Lemma 3 is applied and thus there exists a matrix D over $\mathbb{L}[[x]]^*$ and $h \in \mathbb{Q}$, with $h > 0$, such that the characteristic polynomial of $x^h D$ is equal to $f(x,y)$. Moreover there exists d_m with $d_m(0) \neq 0$.

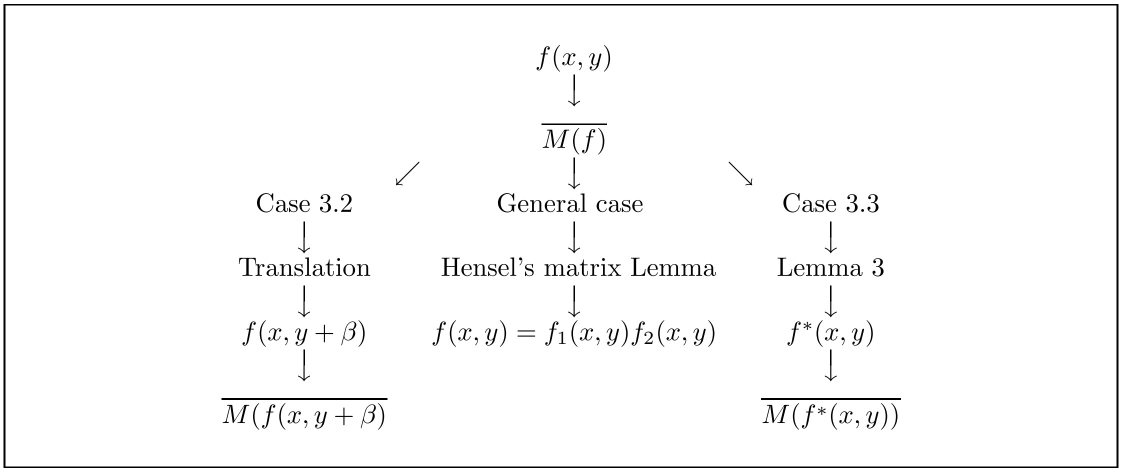
If the entries of D, denoted by $\{1, -d_0, \ldots, -d_{n-1}\}$, are in $\mathbb{L}[[x]]$ then the roots of $f(x,y)$ are obtained by multiplying the eigenvalues of D by x^h and the algorithm continues with the decomposition of D.

Otherwise, there exists $q_j \in \mathbb{N}$ such that $d_j \in \mathbb{L}[[x^{1/q_j}]]$. Let s be defined as

$$s = \text{mcm}\{q_j\}.$$

Then $d_j \in \mathbb{L}[[x^{1/s}]]$ for every j. Thus, with the change of variable $x^{\frac{1}{s}} = z$, the entries of D are in $\mathbb{L}[[z]]$: if the eigenvalues of D are obtained and we substitute $x^{\frac{1}{s}}$ for z, then we will obtain the eigenvalues of $f(x,y)$ by multiplying times x^h. So the algorithm continues with the decomposition of D by applying either Case 3.1 or Case 3.2.

The algorithm is summarized in the next diagram.



3.4 Example

Let $f(x,y) = y^3 + x^3y^2 + x^4y + x^4$ in $\mathbb{C}[x,y]$. Considering its companion matrix and the corresponding residual class:

$$M(f) = \begin{pmatrix} 0 & 0 & -x^4 \\ 1 & 0 & -x^4 \\ 0 & 1 & -x^3 \end{pmatrix}, \quad \overline{M(f)} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

it is clear that it is not possible to apply directly Hensel's matrix Lemma to decompose $M(f)$ and that all roots of $f(x,y)$ have independent coefficient equal to 0. Thus we are in **Case 3.3** and apply Lemma 3 to the matrix $M(f)$ obtaining:

$$h = \frac{4}{3}, \quad D = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -x^{4/3} \\ 0 & 1 & -x^{5/3} \end{pmatrix}.$$

Since D belongs to $\mathbb{Q}[[x^{\frac{1}{3}}]]$, $s = 3$ and the change of variable $z = x^{\frac{1}{3}}$ is performed it is obtained the following expression for D:

$$D = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -z^4 \\ 0 & 1 & -z^5 \end{pmatrix}.$$

Next the eigenvalues of D (depending on z) are determined, i.e. the roots of its characteristic polynomial which is denoted by $f_1(z,y)$:

$$f_1(z,y) = y^3 + z^5y^2 + z^4y + 1.$$

Since:

$$\overline{D} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

we are in **Case 3.1** and compute a root β of the polynomial $f_1(0,y) = y^3 + 1$.

We consider $\beta = -1$ and define the polynomial $F_1(z,y)$ as follows:

$$F_1(z,y) = f_1(z,y-1) = y^3 + \left(-3 + z^5\right)y^2 + \left(-2\,z^5 + 3 + z^4\right)y + z^4\,(z-1).$$

The matrix $M(F_1)$ and its residual are

$$M(F_1)=\begin{pmatrix}0&0&-z^5+z^4\\1&0&-3+2\,z^5-z^4\\0&1&3-z^5\end{pmatrix},\quad \overline{M(F_1)}=\begin{pmatrix}0&0&0\\1&0&-3\\0&1&3\end{pmatrix},$$

and so the required conditions to apply *Hensel's matrix Lemma* to $M(F_1)$ are verified. We consider the following partition of $M(F_1)$:

$$M(F_1)_1=(0),\; M(F_1)_2=\begin{pmatrix}0&-z^5+z^4\end{pmatrix},\; M(F_1)_3=\begin{pmatrix}1\\0\end{pmatrix},\; M(F_1)_4=\begin{pmatrix}0&-3+2\,z^5-z^4\\1&3-z^5\end{pmatrix},$$

such that

$$M(F_1)=\begin{pmatrix}M(F_1)_1&M(F_1)_2\\M(F_1)_3&M(F_1)_4\end{pmatrix},$$

and we compute an approximation to the limit of the sequence $(X_r)_{r\in\mathbb{N}}=((X_{1,r}\,,\;X_{2,r}))_{r\in\mathbb{N}}$ defined by

$$X_0=0_{1,2},\quad X_rM(F_1)_4-M(F_1)_1X_r=M(F_1)_2-X_{r-1}M(F_1)_3X_{r-1}.$$

In other words:

- $X_0=(0,0)$,
- $X_{1,r}(-3+2z^5-z^4)+X_{2,r}(3-z^5)=-z^5+z^4-X_{1,r-1}X_{2,r-1}$,
- $X_{2,r}=-X_{1,r-1}^2$.

Thus, if $H=(h_1,h_2)$ denotes such limit then $M(F_1)$ will be similar to the matrix:

$$M(F_1)\approx\begin{pmatrix}M(F_1)_1-HM(F_1)_3&0\\M(F_1)_3&M(F_1)_4+M(F_1)_3H\end{pmatrix}=\begin{pmatrix}-h_1&0&0\\1&h_1&-3+2z^5-z^4+h_2\\0&1&3-z^5\end{pmatrix},$$

such that $-h_1$ is one of the desired roots.

The first five terms of the sequence (X_r) are:

- $X_1\;=\;(X_{1,1}\,,\;X_{2,1})$,
  $X_{1,1}=-\frac{1}{3}z^4+\frac{1}{3}z^5+\frac{1}{9}z^8-\frac{1}{3}z^9+\mathbf{O}\left(z^{10}\right)$,
  $X_{2,1}=0$,
- $X_2\;=\;(X_{1,2}\,,\;X_{2,2})$,
  $X_{1,2}=-\frac{1}{3}z^4+\frac{1}{3}z^5-\frac{1}{9}z^9+\frac{1}{9}z^{10}+\frac{2}{27}z^{12}-\frac{2}{9}z^{13}+\mathbf{O}\left(z^{14}\right)$,
  $X_{2,2}=-\frac{1}{9}z^8+\frac{2}{9}z^9-\frac{1}{9}z^{10}+\frac{2}{27}z^{12}-\frac{8}{27}z^{13}+\mathbf{O}\left(z^{14}\right)$,
- $X_3\;=\;(X_{1,3}\,,\;X_{2,3})$,
  $X_{1,3}=-\frac{z^4}{3}+\frac{z^5}{3}-\frac{z^9}{9}+\frac{z^{10}}{9}+\frac{z^{12}}{81}-\frac{z^{13}}{27}+\frac{2z^{15}}{81}+\frac{z^{16}}{27}-\frac{32z^{17}}{243}+\mathbf{O}\left(z^{18}\right)$,
  $X_{2,3}=-\frac{z^8}{9}+\frac{2z^9}{9}-\frac{z^{10}}{9}-\frac{2z^{13}}{27}+\frac{4z^{14}}{27}-\frac{2z^{15}}{27}+\frac{4z^{16}}{81}-\frac{16z^{17}}{81}+\mathbf{O}\left(z^{18}\right)$,
- $X_4\;=\;(X_{1,4}\,,\;X_{2,4})$,
  $X_{1,4}=-\frac{z^4}{3}+\frac{z^5}{3}-\frac{z^9}{9}+\frac{z^{10}}{9}+\frac{z^{12}}{81}-\frac{z^{13}}{27}+\frac{2z^{15}}{81}+\frac{z^{16}}{243}-\frac{2z^{18}}{81}+\frac{5z^{19}}{243}+\mathbf{O}\left(z^{20}\right)$,
  $X_{2,4}=-\frac{z^8}{9}+\frac{2z^9}{9}-\frac{z^{10}}{9}-\frac{2z^{13}}{27}+\frac{4z^{14}}{27}-\frac{2z^{15}}{27}+\frac{2z^{16}}{243}-\frac{8z^{17}}{243}+\frac{z^{18}}{81}+\frac{10z^{19}}{243}+\mathbf{O}\left(z^{20}\right)$,
- $X_5\;=\;(X_{1,5}\,,\;X_{2,5})$,
  $X_{1,5}=-\frac{z^4}{3}+\frac{z^5}{3}-\frac{z^9}{9}+\frac{z^{10}}{9}+\frac{z^{12}}{81}-\frac{z^{13}}{27}+\frac{2z^{15}}{81}+\frac{z^{16}}{243}-\frac{2z^{18}}{81}+\frac{5z^{19}}{243}+\mathbf{O}\left(z^{21}\right)$,
  $X_{2,5}=-\frac{z^8}{9}+\frac{2z^9}{9}-\frac{z^{10}}{9}-\frac{2z^{13}}{27}+\frac{4z^{14}}{27}-\frac{2z^{15}}{27}+\frac{2z^{16}}{243}-\frac{8z^{17}}{243}+\frac{z^{18}}{81}+\frac{10z^{19}}{243}-\frac{19z^{20}}{729}+\mathbf{O}\left(z^{21}\right)$.

Moreover, denoting $\mathbf{v}(A) = \min\{v(a_{i,j})\}$ for a given matrix $A = (a_{i,j})$, since the following equalities are verified:

$$\begin{array}{ll} \mathbf{v}(X_2 - X_1) = 8 & \mathbf{v}(X_3 - X_2) = 12 \\ \mathbf{v}(X_4 - X_3) = 16 & \mathbf{v}(X_5 - X_4) = 20 \end{array}$$

then the entries of H up to order 20 have been obtained through the computation of X_5. As a result, we have computed all the terms up to order 23/3 of one root of $f(x,y)$:

$$y_1(x) = -x^{4/3} + \frac{x^{8/3}}{3} - \frac{x^3}{3} + \frac{x^{13/3}}{9} - \frac{x^{14/3}}{9} - \frac{x^{16/3}}{81} + \frac{x^{\frac{17}{3}}}{27} - \frac{2x^{\frac{19}{3}}}{81} - \frac{x^{\frac{20}{3}}}{243} + \frac{2x^{\frac{22}{3}}}{81} - \frac{5x^{\frac{23}{3}}}{243} + \mathbf{O}\left(x^{\frac{24}{3}}\right).$$

The next step in the algorithm is the computation of the other two roots which are the eigenvalues of $M(F_1)_4 + M(F_1)_3 H$:

$$M(F_1)_4 + M(F_1)_3 H = \begin{pmatrix} h_1 & -3 + 2z^5 - z^4 + h_2 \\ 1 & 3 - z^5 \end{pmatrix}.$$

Similarly, if $f_2(z,y)$ denotes the characteristic polynomial of $M(F_1)_4 + M(F_1)_3 H$,

$$f_2(z,y) = \chi(M(F_1)_4 + M(F_1)_3 H, y),$$

we consider the matrix $M(f_2)$ (companion matrix of $f_2(z,y)$) given by

$$M(f_2) = \begin{pmatrix} 0 & h_1(-3+z^5) + h_2 - 3 + 2z^5 - z^4 \\ 1 & h_1 + 3 - z^5 \end{pmatrix}.$$

Note that since we stopped, when computing the first root, at X_5, we work with the following matrix:

$$M(f_2) = \begin{pmatrix} 0 & \frac{5}{243}z^{24} - \frac{2}{81}z^{23} + \frac{1}{243}z^{21} - \frac{1}{729}z^{20} - \frac{5}{243}z^{19} + \ldots + \frac{2}{9}z^9 - \frac{1}{9}z^8 + z^5 - 3 \\ 1 & \frac{5}{243}z^{19} - \frac{2}{81}z^{18} + \frac{1}{243}z^{16} + \frac{2}{81}z^{15} - \frac{1}{27}z^{13} + \frac{1}{81}z^{12} + \frac{1}{9}z^{10} - \frac{z^9}{9} - \frac{2z^5}{3} - \frac{z^4}{3} + 3 \end{pmatrix}.$$

Since:

$$\overline{M(f_2)} = \begin{pmatrix} 0 & -3 \\ 1 & 3 \end{pmatrix},$$

we are in **Case 3.1** and we compute one root, α, of $f_2(0,y) = y^2 - 3y + 3$. We consider $\alpha = \frac{3}{2} + \frac{1}{2}\sqrt{3}i$ and define the polynomial $F_2(z,y)$ as it follows:

$$F_2(z,y) = f_2(z, y+\alpha) = y^2 + b_1(z,\alpha)y + b_2(z,\alpha).$$

The residual matrix for the companion matrix of $F_2(z,y)$ is:

$$\overline{M(F_2)} = \begin{pmatrix} 0 & 0 \\ 1 & -i\sqrt{3} \end{pmatrix},$$

and so, the required conditions in order to apply *Hensel's matrix Lemma* to $M(F_2)$ are verified. We consider the following partition:

$$M(F_2)_1 = \begin{pmatrix} 0 \end{pmatrix}, \quad M(F_2)_2 = \begin{pmatrix} -b_2 \end{pmatrix}, \quad M(F_2)_3 = \begin{pmatrix} 1 \end{pmatrix}, \quad M(F_2)_4 = \begin{pmatrix} -b_1 \end{pmatrix}$$

such that

$$M(F_2) = \begin{pmatrix} M(F_2)_1 & M(F_2)_2 \\ M(F_2)_3 & M(F_2)_4 \end{pmatrix},$$

and we compute an approximation up to order 20 to the limit of the sequence $(X_r)_{r\in\mathbb{N}}$ defined by:

$$X_0 = 0, \quad X_r M(F_2)_4 - M(F_2)_1 X_r = M(F_2)_2 - X_{r-1} M(F_2)_3 X_{r-1}.$$

In this case $X_0 = 0$ and $-X_r b_1 = -b_2 - X_{r-1}^2$.

Thus, if H denotes that limit then $M(F_2)$ will be similar to the matrix:

$$M(F_2) \approx \begin{pmatrix} M(F_2)_1 - H M(F_2)_3 & 0 \\ M(F_2)_3 & M(F_2)_4 + M(F_2)_3 H \end{pmatrix} = \begin{pmatrix} -H & 0 \\ 1 & -b_1 + H \end{pmatrix}$$

with $-H$ and $H-b_1$ the two desired roots.

The first five terms of the sequence $(X_r)_{r\in\mathbb{N}}$ are:

$$X_1 = -\frac{\sqrt{3}z^4 i\left(3+i\sqrt{3}\right)}{18} + \frac{z^5}{3} - \frac{\sqrt{3}z^8 i\left(1+i\sqrt{3}\right)}{54} - \frac{\sqrt{3}z^9 i\left(-5+3i\sqrt{3}\right)}{54} + \mathbf{O}\left(z^{10}\right),$$

$$X_2 = -\frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^4}{18} + \frac{z^5}{3} - \frac{i\left(-3+i\sqrt{3}\right)\sqrt{3}z^9}{54} + \frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^{10}}{54} + \frac{i\left(5\,i\sqrt{3}-3\right)\sqrt{3}z^{12}}{486} + \frac{i\left(-9+i\sqrt{3}\right)\sqrt{3}z^{13}}{162} + \mathbf{O}\left(z^{14}\right),$$

$$X_3 = -\frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^4}{18} + \frac{z^5}{3} + \frac{z^9(1+i\sqrt{3})}{18} + \frac{z^{10}(-1+i\sqrt{3})}{18} - \frac{z^{12}(1+i\sqrt{3})}{162} + \frac{z^{13}(1-i\sqrt{3})}{54} - \frac{z^{15}(1+i\sqrt{3})}{81} + \left(\frac{7i\sqrt{3}}{1458} + \frac{1}{162}\right)z^{16} + \frac{16i\sqrt{3}z^{17}}{729} + \mathbf{O}\left(z^{18}\right),$$

$$X_4 = -\frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^4}{18} + \frac{z^5}{3} - \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^9}{54} + \frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^{10}}{54} + + \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^{12}}{486} - \frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^{13}}{162} + \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^{15}}{243} + \frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^{16}}{1458} - \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^{18}}{243} + \frac{5i\left(3+i\sqrt{3}\right)\sqrt{3}z^{19}}{1458} + \mathbf{O}\left(z^{20}\right),$$

$$X_5 = -\frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^4}{18} + \frac{z^5}{3} - \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^9}{54} + \frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^{10}}{54} + \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^{12}}{486} - \frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^{13}}{162} + \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^{15}}{243} + \frac{i\left(3+i\sqrt{3}\right)\sqrt{3}z^{16}}{1458} - \frac{i\left(i\sqrt{3}-3\right)\sqrt{3}z^{18}}{243} + \frac{5i\left(3+i\sqrt{3}\right)\sqrt{3}z^{19}}{1458} + \mathbf{O}\left(z^{21}\right).$$

Moreover, since the following equalities are verified:

$$\mathbf{v}(X_2 - X_1) = 8 \qquad \mathbf{v}(X_3 - X_2) = 12$$
$$\mathbf{v}(X_4 - X_3) = 16 \qquad \mathbf{v}(X_5 - X_4) = 20,$$

the entries of H up to order 20 have been obtained by computing X_5. As a result, after performing the required substitutions, we have computed all the terms up to order 23/3 of the two remaining roots:

$$y_2(x) = \left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)x^{4/3} + \left(\frac{i\sqrt{3}}{6} - \frac{1}{6}\right)x^{8/3} - \frac{1}{3}x^3 - \left(\frac{i\sqrt{3}}{18} + \frac{1}{18}\right)x^{13/3} + \left(-\frac{i\sqrt{3}}{18} + \frac{1}{18}\right)x^{14/3} + \left(\frac{i\sqrt{3}}{162} + \frac{1}{162}\right)x^{16/3} + \left(\frac{i\sqrt{3}}{54} - \frac{1}{54}\right)x^{\frac{17}{3}} + \left(\frac{1}{81} + \frac{i\sqrt{3}}{81}\right)x^{\frac{19}{3}} + \left(-\frac{i\sqrt{3}}{486} + \frac{1}{486}\right)x^{\frac{20}{3}} - \left(\frac{1}{81} + \frac{i\sqrt{3}}{81}\right)x^{\frac{22}{3}} + \left(-\frac{5i\sqrt{3}}{486} + \frac{5}{486}\right)x^{\frac{23}{3}} + \mathbf{O}(x^{\frac{24}{3}}),$$

$$y_3(x) = \left(\frac{1}{2} - \frac{i\sqrt{3}}{2}\right)x^{4/3} - \left(\frac{1}{6} + \frac{i\sqrt{3}}{6}\right)x^{8/3} - \frac{1}{3}x^3 + \left(\frac{i\sqrt{3}}{18} - \frac{1}{18}\right)x^{13/3} + \left(\frac{1}{18} + \frac{i\sqrt{3}}{18}\right)x^{14/3} + \left(\frac{1}{162} - \frac{i\sqrt{3}}{162}\right)x^{16/3} - \left(\frac{i\sqrt{3}}{54} + \frac{1}{54}\right)x^{\frac{17}{3}} + \left(\frac{1}{81} - \frac{i\sqrt{3}}{81}\right)x^{\frac{19}{3}} + \left(\frac{i\sqrt{3}}{486} + \frac{1}{486}\right)x^{\frac{20}{3}} + \left(-\frac{1}{81} + \frac{i\sqrt{3}}{81}\right)x^{\frac{22}{3}} + \left(\frac{5}{486} + \frac{5i\sqrt{3}}{486}\right)x^{\frac{23}{3}} + \mathbf{O}(x^{\frac{24}{3}}).$$

All this process requires the computation and manipulation of the roots of the polynomials T^3+1 and T^2-3T+3. Instead of computing explicitly these roots (or dealing with towers of algebraic extensions or primitive elements), next section shows how the use of the *Dynamic Evaluation* simplifies the management of the algebraic numbers involved in the algorithm.

4 Dynamic Evaluation

The *Dynamic Evaluation* was introduced in [3] to perform computations with algebraic numbers without factoring polynomials over algebraic extensions or computing primitive elements. The application of the *Dynamic Evaluation* in the algorithm presented in the previous section is described as follows.

Let $f(x,y) \in \mathbb{L}[x,y]$ be the considered polynomial. Suppose that $f(0,0) \neq 0$ and Case 3.2 is applied to decompose the matrix $M(f)$. However, the squarefree decomposition of $f(0,y)$,

$$f(0,y) = p_1(y) \cdot p_2^2(y) \cdot \ldots \cdot p_m^m(y),$$

is computed instead of the roots of $f(0,y)$. Let $p_t(y)$ be supposed to be a nonconstant factor of such decomposition. Note that for every root of $p_t(y)$, α, there are t roots of $f(x,y)$ with independent coefficient equal to α.

Let β_t be any root in $\mathbb{L}$ of $p_t(y)$: $p_t(\beta_t) = 0$. Then the algorithm continues with the decomposition of the polynomial

$$F(x,y) = f(x, y + \beta_t),$$

simplifying the expressions module $p_t(\beta_t)$ to avoid the growth of the coefficients. Now, depending on the value of t, there exist three different ways of continuing:

- $\mathbf{t = n}$:
  $f(0,y)$ only has one root and so Lemma 3 is applied to decompose $M(F)$. Hence a matrix D is obtained. Then, either Hensel's matrix Lemma is used to decompose D or Case 3.2 is applied. Applying Case 3.2 implies computing the squarefree decomposition of a polynomial whose coefficients depend on the parameter β_t. A method for the parametric squarefree decomposition is presented in [2].
- $\mathbf{1 < t < n}$:
  Hensel's matrix Lemma is applied to decompose $M(F)$ and, similarly, the algorithm goes on with the decomposition of $M(F)_1^{'}$. Hence the next step is the application of Lemma 3 and the decomposition of the obtained matrix D afterwards. Note that it is possible to obtain more than one matrix D because the valuations of the entries of $M(F)_1^{'}$ depend on the parameter β_t.
- $\mathbf{1 = t}$:
  Hensel's matrix Lemma is applied and the matrix $M(F)_1^{'}$ provides $\deg(p_t)$–roots of $f(x,y)$.

4.1 Example Using Dynamic Evaluation

For the polynomial already considered in 3.4, after applying Lemma 3 to the matrix $M(f)$ and making the corresponding change of variable, the following matrix is obtained:

$$\overline{D} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

Thus we are in **Case 3.1** and:

$$\chi(D,y) = f_1(z,y) \;=\; y^3 + z^5 y^2 + z^4 y + 1,$$
$$f_1(0,y) = y^3 + 1.$$

In this case $f_1(0,y)$ is squarefree. Let β be satisfying $\beta^3 + 1 = 0$ and $F_1(z,y)$ be the polynomial:

$$\begin{aligned} F_1(z,y) &= f_1(z, y+\beta) = \\ &= (y+\beta)^3 + z^5\,(y+\beta)^2 + z^4\,(y+\beta) + 1 = \\ &= y^3 + \left(3\,\beta + z^5\right) y^2 + \left(2\,z^5\beta + 3\,\beta^2 + z^4\right) y + \beta\, z^4\,(\beta\, z + 1)\,. \end{aligned}$$

The companion matrix of $F_1(z,y)$ and its residual are

$$M(F_1) = \begin{pmatrix} 0 & 0 & -z^5\beta^2 - z^4\beta \\ 1 & 0 & -3\,\beta^2 - 2\,z^5\beta - z^4 \\ 0 & 1 & -3\,\beta - z^5 \end{pmatrix}, \quad \overline{M(F_1)} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -3\,\beta^2 \\ 0 & 1 & -3\,\beta \end{pmatrix},$$

and so we can apply *Hensel's matrix Lemma* to decompose $M(F_1)$. We consider the next partition:

$$M(F_1)_1 = (0),\ M(F_1)_2 = \begin{pmatrix} 0 & -z^5\beta^2 - z^4\beta \end{pmatrix},\ M(F_1)_3 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ M(F_1)_4 = \begin{pmatrix} 0 & -3\beta^2 - 2\beta z^5 - z^4 \\ 1 & -3\beta - z^5 \end{pmatrix},$$

such that

$$M(F_1) = \begin{pmatrix} M(F_1)_1 & M(F_1)_2 \\ M(F_1)_3 & M(F_1)_4 \end{pmatrix},$$

and we compute an approximation to the limit of the sequence $(X_r)_{r\in\mathbb{N}} = ((X_{1,r}, X_{2,r}))_{r\in\mathbb{N}}$ defined by:

- $X_0 = 0_{1,2}$,
- $X_r M(F_1)_4 - M(F_1)_1 X_r = M(F_1)_2 - X_{r-1} M(F_1)_3 X_{r-1}$.

In other words:

- $X_0 = (0, 0)$,
- $X_{1,r}(-3\beta^2 - 2\beta z^5 - z^4) + X_{2,r}(-3\beta - z^5) = -z^5\beta^2 - z^4\beta - X_{1,r-1}X_{2,r-1}$,
- $X_{2,r} = -X_{1,r-1}^2$.

Thus, if $H = (h_1, h_2)$ denotes that limit then the matrix $M(F_1)$ is similar to the matrix:

$$\begin{pmatrix} M(F_1)_1 - HM(F_1)_3 & 0 \\ M(F_1)_3 & M(F_1)_4 + M(F_1)_3 H \end{pmatrix}.$$

and in this way $M(F_1)_1 - HM(F_1)_3$ provides, after performing the needed substitutions, not only one but all the desired roots simultaneously.

The first five terms of this sequence are:

- $X_1 = (X_{1,1}, X_{2,1})$,
  $X_{1,1} = -\frac{1}{3}\beta^2 z^4 + \frac{1}{3}z^5 + \frac{1}{9}z^8 + \frac{1}{3}\beta\, z^9 + \mathbf{O}\left(z^{10}\right)$,
  $X_{2,1} = 0$,
- $X_2 = (X_{1,2}\,,\, X_{2,2})$,
  $X_{1,2} = -\frac{1}{3}\beta^2 z^4 + \frac{1}{3}z^5 + \frac{1}{9}\beta\, z^9 + \frac{1}{9}\beta^2 z^{10} - \frac{2}{27}\beta z^{12} - \frac{2}{9}\beta^2 z^{13} + \mathbf{O}\left(z^{14}\right)$,
  $X_{2,2} = \frac{1}{9}\beta z^8 + \frac{2}{9}\beta^2 z^9 - \frac{1}{9}z^{10} + \frac{2}{27}\beta^2 z^{12} - \frac{8}{27}z^{13} + \mathbf{O}\left(z^{14}\right)$,
- $X_3 = (X_{1,3}\,,\, X_{2,3})$,
  $X_{1,3} = -\frac{\beta^2 z^4}{3} + \frac{z^5}{3} + \frac{\beta z^9}{9} + \frac{\beta^2 z^{10}}{9} - \frac{\beta z^{12}}{81} - \frac{\beta^2 z^{13}}{27} - \frac{2\beta z^{15}}{81} + \frac{\beta^2 z^{16}}{27} - \frac{32 z^{17}}{243} + \mathbf{O}\left(z^{18}\right)$,
  $X_{2,3} = \frac{\beta z^8}{9} + \frac{2\beta^2 z^9}{9} - \frac{z^{10}}{9} - \frac{2z^{13}}{27} - \frac{4\beta z^{14}}{27} - \frac{2\beta^2 z^{15}}{27} + \frac{4z^{16}}{81} + \frac{16\beta z^{17}}{81} + \mathbf{O}\left(z^{18}\right)$,
- $X_4 = (X_{1,4}\,,\, X_{2,4})$,
  $X_{1,4} = -\frac{\beta^2 z^4}{3} + \frac{z^5}{3} + \frac{\beta z^9}{9} + \frac{\beta^2 z^{10}}{9} - \frac{\beta z^{12}}{81} - \frac{\beta^2 z^{13}}{27} - \frac{2\beta z^{15}}{81} + \frac{\beta^2 z^{16}}{243} + \frac{2\beta z^{18}}{81} \frac{5\beta^2 z^{19}}{243} + \mathbf{O}\left(z^{20}\right)$,
  $X_{2,4} = \frac{\beta z^8}{9} + \frac{2\beta^2 z^9}{9} - \frac{z^{10}}{9} - \frac{2z^{13}}{27} - \frac{4\beta z^{14}}{27} - \frac{2\beta^2 z^{15}}{27} + \frac{2z^{16}}{243} + \frac{8\beta z^{17}}{243} + \frac{\beta^2 z^{18}}{81} + \frac{10 z^{19}}{243} + \mathbf{O}\left(z^{20}\right)$,
- $X_5 = (X_{1,5}\,,\, X_{2,5})$,
  $X_{1,5} = -\frac{\beta^2 z^4}{3} + \frac{z^5}{3} + \frac{\beta z^9}{9} + \frac{\beta^2 z^{10}}{9} - \frac{\beta z^{12}}{81} - \frac{\beta^2 z^{13}}{27} - \frac{2\beta z^{15}}{81} + \frac{\beta^2 z^{16}}{243} + \frac{2\beta z^{18}}{81}$
  $+\frac{5\beta^2 z^{19}}{243} + \mathbf{O}\left(z^{21}\right)$,
  $X_{2,5} = \frac{\beta z^8}{9} + \frac{2\beta^2 z^9}{9} - \frac{z^{10}}{9} - \frac{2z^{13}}{27} - \frac{4\beta z^{14}}{27} - \frac{2\beta^2 z^{15}}{27} + \frac{2z^{16}}{243} + \frac{8\beta z^{17}}{243} + \frac{\beta^2 z^{18}}{81} + \frac{10 z^{19}}{243}$
  $+\frac{19\beta z^{20}}{729} + \mathbf{O}\left(z^{21}\right)$,

Moreover, since the following equalities are verified:

$$\mathbf{v}(X_2 - X_1) = 8 \qquad \mathbf{v}(X_3 - X_2) = 12$$
$$\mathbf{v}(X_4 - X_3) = 16 \qquad \mathbf{v}(X_5 - X_4) = 20$$

the entries of H up to order 20 have been obtained by computing X_5. As a result, we have computed all the terms up to order 23/3 of one expression which provides all the roots of $f(x, y)$:

$$y(x) = \beta x^{4/3} + \frac{1}{3}\beta^2 x^{8/3} - \frac{1}{3}x^3 - \frac{1}{9}\beta x^{13/3} - \frac{1}{9}\beta^2 x^{14/3} + \frac{1}{81}\beta x^{16/3} + \frac{1}{27}\beta^2 x^{\frac{17}{3}} + \frac{2}{81}\beta x^{\frac{19}{3}}$$
$$- \frac{1}{243}\beta^2 x^{\frac{20}{3}} - \frac{5}{243}\beta^2 x^{\frac{23}{3}} - \frac{2}{81}\beta x^{\frac{22}{3}} + \mathbf{O}\left(x^{24/3}\right),$$

with β satisfying $\beta^3 + 1 = 0$.

Note that the use of the *Dynamic Evaluation* has allowed to simplify the final expressions and the required computations that were necessary to perform when we have applied the same algorithm but dealing directly with every individual algebraic number appearing in the computations.

5 Conclusions

The combination of Hensel's matrix Lemma and *Dynamic Evaluation* provides a new algorithm for computing the Puiseux expansions of a polynomial different from the classical algorithm based on the use of the Newton's polygon. The classical algorithm requires the computation of (and with) the roots of the same polynomials appearing in Case

3.2. Moreover the valuations of the polynomials of the companion matrix used in our algorithm are highly related to the slopes that appear in the different Newton's polygons used in the classical algorithm. On the other hand, the use of *Dynamic Evaluation* and Hensel's matrix Lemma enables to obtain expressions which provides different roots and several terms in only one step, while the classical algorithm computes one term of one root in every step.

References

1. P. M. Cohn: Puiseux'x Theorem revisited. J. of Pure and App. Algebra 31, 1–4 (1984).
2. G. M. Diaz–Toca and L. Gonzalez–Vega: Squarefree decomposition of univariate polynomials depending on a parameter. Journal of Symbolic Computation 32, 191–209 (2001).
3. D. Duval: Algebraic Numbers: An Example of Dynamic Evaluation. Journal of Symbolic Computation 18, 5, 429–445 (1994).
4. I. Newton: La méthode des fluxions et des suites infinies. Translated by M. de Buffon, Librairie Albert Blanchard, Paris (1966).
5. R. J. Walker: Algebraic Curves. Dover Publ. (1950).
6. M. A. Zurro: Matrices de series y teorema de Puiseux (in spanish). Master Thesis, Universidad de Valladolid, Spain (1990).