# Using approximate roots for irreducibility and equi-singularity issues in K[[x]][y]

Adrien Poteaux, Martin Weimann

# Using approximate roots for irreducibility and equi-singularity issues in $\mathbb{K}[[x]][y]$

Adrien POTEAUX,
CRIStAL-INRIA
Université de Lille
UMR CNRS 9189, Bâtiment M3
59655 Villeneuve d'Ascq, France
adrien.poteaux@univ-lille.fr

Martin WEIMANN,
GAATI*
Université de Polynésie Française
BP 6570, 98702 Faa'a
martin.weimann@upf.pf

November 4, 2019

We provide an irreducibility test in the ring $\mathbb{K}[[x]][y]$ whose complexity is quasi-linear with respect to the discriminant valuation, assuming the input polynomial $F$ square-free and $\mathbb{K}$ a perfect field of characteristic zero or greater than $\deg(F)$. The algorithm uses the theory of approximate roots and may be seen as a generalization of Abhyankhar's irreducibility criterion to the case of non algebraically closed residue fields. More generally, we show that we can test within the same complexity if a polynomial is pseudo-irreducible, a larger class of polynomials containing irreducible ones. If $F$ is pseudo-irreducible, the algorithm computes also the discriminant valuation of $F$ and the equisingularity classes of the germs of plane curves defined by $F$ along the fiber $x = 0$.

*Current delegation. Permanent position at LMNO, University of Caen-Normandie, BP 5186, 14032 Caen Cedex, France.

# 1 Introduction

**Context and main result.** This paper provides new complexity results for testing the irreducibility of polynomials with coefficients in a ring of formal power series of characteristic zero or big enough. We consider $\mathbb{K}$ a perfect field, $x$ and $y$ two indeterminates over $\mathbb{K}$ and $F \in \mathbb{K}[[x]][y]$ a polynomial of degree $d$. In all of the sequel, we will assume that the following hypothesis holds:

*The characteristic of* $\mathbb{K}$ *is either* 0 *or greater than* $d$.

Assuming $F$ square-free, we let $\delta$ be the $x$-valuation of the resultant between $F$ and its $y$-derivative $F_y$. We prove:

**Theorem 1.** *There exists an algorithm which tests if* $F$ *is irreducible in* $\mathbb{K}[[x]][y]$ *with an expected* $\mathcal{O}^{\sim}(\delta + d)$ *operations over* $\mathbb{K}$ *and two univariate irreducibility tests over* $\mathbb{K}$ *of degree at most* $d$.

If $F$ is Weierstrass[1], the complexity drops to $\mathcal{O}^{\sim}(\delta)$ operations over $\mathbb{K}$ and one univariate irreducibility test of degree at most $d$. The notation $\mathcal{O}^{\sim}()$ hides logarithmic factors. Our algorithm is Las Vegas, due to the computation of primitive elements; it should become deterministic via the preprint [29]. See Section 7 for more details, including our complexity model.

We say that $F$ is absolutely irreducible if it is irreducible in $\overline{\mathbb{K}}[[x]][y]$, where $\overline{\mathbb{K}}$ stands for the algebraic closure of $\mathbb{K}$. In such a case, we avoid univariate irreducibility tests and there is no need to deal with extensions of residue fields. We get:

**Theorem 2.** *There exists a deterministic algorithm which tests if* $F$ *is absolutely irreducible with* $\mathcal{O}^{\sim}(\delta + d)$ *operations over* $\mathbb{K}$*, which is* $\mathcal{O}^{\sim}(\delta)$ *when* $F$ *is Weierstrass.*

**Pseudo-Irreducible polynomials.** If $F$ is irreducible, the algorithms above compute also the discriminant valuation $\delta$ and the number of absolutely irreducible factors together with their sets of characteristic exponents and pairwise intersection multiplicities. These numerical data capture the main relevant information about the singularities of the germs of plane curves defined by $F$ along $x = 0$. In particular, they uniquely determine their equisingularity classes, hence their topological classes if $\mathbb{K} = \mathbb{C}$. It turns out that we can compute these invariants within the same complexity (avoiding furthermore any univariate irreducibility test) for a larger class of polynomial: we say that $F$ is *pseudo-irreducible* (the terminology *balanced* will also be used in the sequel) if its irreducible factors in $\overline{\mathbb{K}}[[x]][y]$ have same characteristic exponents and same sets of pairwise intersection multiplicities (see Section 8). If $F$ is irreducible in $\mathbb{L}[[x]][y]$ for some field extension $\mathbb{L}$ of $\mathbb{K}$, then it is pseudo-irreducible by a Galois argument, but the converse does not hold.

[1] We recall that in our context, $F = \sum_{i=0}^{d} a_i(x)\, y^i$ is Weierstrass if $a_d = 1$ and $a_i(0) = 0$ for $i < d$

**Theorem 3.** *There exists an algorithm which tests if $F$ is pseudo-irreducible with an expected $\mathcal{O}(d+\delta)$ operations over $\mathbb{K}$, which is $\mathcal{O}(\delta)$ if $F$ is Weierstrass. If $F$ is pseudo-irreducible, the algorithm computes $\delta$ and the number of irreducible factors in $\overline{\mathbb{K}}[[x]][y]$ together with their characteristic exponents and pairwise intersection multiplicities.*

Note that if $F$ is pseudo-irreducible, all its absolutely irreducible factors have same degree, and the algorithm computes it. We can compute also the degrees, residual degrees and ramifications indices of the irreducible factors of $F$ in $\mathbb{L}[[x]][y]$ over any given field extension $\mathbb{L}$ of $\mathbb{K}$ by performing an extra univariate factorization of degree $d$ over $\mathbb{L}$.

**Bivariate case.** If $F \in \mathbb{K}[x,y]$ is a square-free bivariate polynomial of bidegree $(n,d)$, we have $\delta \leq 2nd-n$, hence our algorithms are quasi-linear with respect to the arithmetic size $nd$ of $F$. In fact, we can avoid the square-free hypothesis in this case:

**Theorem 4.** *If $F \in \mathbb{K}[x,y]$, then the previous irreducibility or pseudo-irreducibility tests have complexity $\mathcal{O}(nd)$ up to univariate irreducibility tests, and so without assuming square-freeness of $F$.*

Note that this does not mean that we can check square-freeness of $F$ within $\mathcal{O}(nd)$ operations (this costs $\mathcal{O}(nd^2)$ operations with usual algorithms). Also, note that there is no hope to test irreducibility of a non square-free polynomial $F \in \mathbb{K}[[x]][y]$, as this would require to deal with an infinite precision.

**Local case.** Our algorithms provide also (pseudo)-irreducibility tests in the local rings $\mathbb{K}[[x,y]]$ or $\overline{\mathbb{K}}[[x,y]]$. To this aim, we first apply the Weierstrass Preparation Theorem and compute a factorization $F = UH$ up to a suitable precision using a Hensel like strategy, with $H \in \mathbb{K}[[x]][y]$ a Weierstrass polynomial and $U$ a unit in $\mathbb{K}[[x,y]]$, and we eventually check the (pseudo)-irreducibility of $H$ using algorithms above. Unfortunately, if $F$ is non Weierstrass, the computation of $H$ up to a suitable precision is $\Omega(d\delta)$ in the worst case scenario ([25, Example 5] provides an explicit family of polynomials $F \in \mathbb{K}[x,y]$ for which a local irreducibility test in $\mathbb{K}[[x,y]]$ is cubic in the total degree).

**Main ideas.** All algorithms are based on the same idea. We recursively compute some well chosen approximate roots $\psi_0, \ldots, \psi_g$ of $F$. At each step, we compute the $(\psi_0, \ldots, \psi_k)$-adic expansion of $F$. We deduce the $k$-th generalised Newton polygon and check if it is straigth. If so, we compute the related boundary polynomial and test if it is the power of some irreducible polynomial. In such a case, we deduce the degree of the next approximate root $\psi_{k+1}$ that has to be computed. The algorithm gives moreover the characteristic exponents of $F$, and so without performing any blow-ups and liftings inherent to the classical Newton-Puiseux algorithm. Such a strategy was developped by Abhyankar for testing irreducibility in $\mathbb{C}[[x]][y]$ in [1]. A major difference here is

that testing irreducibility for non algebraically closed residue field $\mathbb{K}$ requires to compute also the boundary polynomials, a key point which is not an issue in Abhyankhar's algorithm. Also, in order to perform a unique univariate irreducibility test over $\mathbb{K}$, we rely on dynamic evaluation and rather check if the boundary polynomials are powers of a square-free polynomial. The pseudo-irreducibility test is based on such a modification, allowing moreover several edges of the Newton polygon in some particular cases.

**Related results.** Factorization in $\mathbb{K}[[x]][y]$ (and *a fortiori* irreducibility test) is an important issue in the algorithmic of algebraic curves, both for local aspects (studying plane curves singularities) and for global aspects (e.g. computing integral basis of function fields [31], computing the geometric genus [25], factoring polynomials in $\mathbb{K}[x, y]$ taking advantage of critical fibers [34], etc). Probably the most classical approach for factoring polynomials in $\mathbb{K}[[x]][y]$ is derived from the Newton-Puiseux algorithm, as a combination of blow-ups (monomial transforms and shifts) and Hensel liftings. This approach allows moreover to compute the roots of $F$ - represented as fractional Puiseux series - up to an arbitrary precision. The Newton-Puiseux algorithm has been studied by many authors (see e.g. [6, 7, 21–25, 27, 33] and the references therein). Up to our knowledge, the best current arithmetic complexity was obtained in [25], using a divide and conquer strategy leading to a fast Newton-Puiseux algorithm (hence an irreducibility test) which computes the singular parts of all Puiseux series above $x = 0$ in an expected $\mathcal{O}(d\,\delta)$ operations over $\mathbb{K}$. There exists also other methods for factorization, as the Montes algorithm which allow to factor polynomials over general local fields [14, 19] with no assumptions on the characteristic of the residue field. Similarly to the algorithms we present in this paper, Montes et al. compute higher order Newton polygons and boundary polynomials from the $\Phi$-adic expansion of $F$, where $\Phi$ is a sequence of some well-chosen polynomials which is updated at each step of the algorithm. With our notations, this leads to an irreducibility test in $\mathcal{O}(d^2+\delta^2)$ [2, Corollary 5.10 p.163] when $\mathbb{K}$ is a "small enough" finite field[2]. In particular, their work provide a complete description of *augmented valuations*, apparently rediscovering the one of MacLane [16, 17, 26]. The closest related result to this topic is the work of Abhyanhar [1], which provides a new irreducibility test in $\mathbb{C}[[x]][y]$ based on approximate roots, generalised to algebraically closed residue fields of arbitrary characteristic in [5]. No complexity estimates have been made up to our knowledge, but we will prove that Abhyanhar's irreducibility criterion is $\mathcal{O}(\delta)$ when $F$ is Weierstrass. In this paper, we extend this result to non algebraically closed residue field $\mathbb{K}[[x]][y]$ of characteristic zero or big enough. In some sense, our approach establishes a bridge between the Newton-Puiseux algorithm, the Montes algorithm and Abhyankar's irreducibility criterion. Let us mention also [9, 10] where an other irreducibility criterion in $\overline{\mathbb{K}}[[x]][y]$ is given in terms of the Newton polygon of the discriminant curve of $F$, without complexity estimates, and [20], which provides a good reference for the relations between approximate roots, Puiseux series and resolution of singularities of an irreducible Weierstrass polynomial $F \in \mathbb{C}[[x]][y]$.

[2]This restriction on the field $\mathbb{K}$ is due to the univariate factorization complexity. It could be probably avoided by using dynamic evaluation.

**Organisation.** In Section 2 below, we describe briefly the rational Newton-Puiseux algorithm of Duval [6] and its improved version of [24] due to the so-called Abhyankar trick. In section 3, we show how to recover the edge data of $F$ from its $\Phi$-adic expansion, where $\Phi$ is the collection of minimal polynomials of the truncated Puiseux series of $F$. We show in Section 4 that $\Phi$ can be replaced by a collection $\Psi$ of approximate roots of $F$ which can be computed in the aimed complexity bound. Section 5 is dedicated to the absolute case, and a new proof of Abhyankhar's irreducibility criterion is given. In Section 6, we allow residual polynomials to be square-free, leading to the notion of pseudo-irreducible polynomials. Section 7 is dedicated to complexity issues and to the proofs of Theorems 1, 2 and 4. We show in Section 8 that a polynomial is pseudo-irreducible if and only if its absolutely irreducible factors are equisingular and have same sets of pairwise intersection sets (balanced polynomials), in which case we give explicit formulas for characteristic exponents and intersection multiplicities in terms of the edges data, thus proving Theorem 3. We conclude in Section 9 with ongoing researches about factorization of polynomials over general local fields of arbitrary residual characteristic.

## 2 The Newton-Puiseux algorithm and Abhyankar trick

**Classical definitions.** We first recall classical definitions that play a central role for our purpose, namely the Newton polygon and the residual polynomial. In the following, we denote $F = \sum_{i=0}^{d} a_i(x)\, y^i$ and $v_x$ the usual $x$-valuation of $\mathbb{K}[[x]]$.

**Definition 1.** The *Newton polygon* of $F$ is the lower convex hull $\mathcal{N}(F)$ of the set of points $(i, v_x(a_i))$ for $i = 0, \dots, d$. The *principal Newton polygon* $\mathcal{N}^-(F)$ is the union of edges of negative slopes of $\mathcal{N}(F)$.

Note that $\mathcal{N}^-(F) = \mathcal{N}(F)$ if $F$ is Weierstrass. The Newton polygon is used at the first call of our main algorithms, while the principal Newton polygon is used for recursive calls. It is well known that irreducibility in $\mathbb{K}[[x]][y]$ (resp. in $\mathbb{K}[[x, y]]$) implies straightness of $\mathcal{N}(F)$ (resp. $\mathcal{N}^-(F)$), a single point being straight by convention. However, straightness condition is not sufficient.

**Definition 2.** Given the (principal or not) Newton polygon $\mathcal{N}$ of $F$, we call $\bar{F} := \sum_{(i,j)\in\mathcal{N}} a_{ij} x^j y^i$ the *boundary polynomial* of $F$.

**Definition 3.** We say that $F$ is *degenerated* over $\mathbb{K}$ with respect to $\mathcal{N}$ if its boundary polynomial $\bar{F}$ is the power of an irreducible quasi-homogeneous polynomial.

In other words, $F$ is degenerated if and only if $\mathcal{N}$ is straight of slope $-m/q$ with $q, m$ coprime, $q > 0$, and if

$$\bar{F} = c \left( P\left( \frac{y^q}{x^m} \right) x^{\varepsilon m \deg(P)} \right)^N \tag{1}$$

with $c \in \mathbb{K}^\times$, $N \in \mathbb{N}$ and $P \in \mathbb{K}[Z]$ monic and irreducible, and where $\varepsilon = 1$ if $m \geq 0$

and $\varepsilon = 0$ otherwise. We call $P$ the *residual polynomial*[3] of $F$. We call the tuple $(q, m, P, N)$ the *edge data* of the degenerated polynomial $F$ and denote `EdgeData` an algorithm computing this tuple.

**Newton-Puiseux irreducibility test.** If $F$ is irreducible in $\mathbb{K}[[x]][y]$, it is degenerated. The converse holds if $N = 1$. If $N > 1$, the Newton-Puiseux algorithm ensures that $F$ is irreducible if and only if all the successive so-called Puiseux transforms of $F$ (line 5 of `RNP`) are degenerated until we reach an edge data with $N = 1$.

We let $\ell := \deg(P)$ and $\mathbb{K}_P := \mathbb{K}[Z]/(P(Z))$. We denote by $z \in \mathbb{K}_P$ the residue class of $Z$. Finally, we let $s, t$ be the unique integers such that the Bézout relation $qs - mt = 1$ holds with $0 \leq t < q$. The rational version of the Newton-Puiseux algorithm of Duval [7] induces the following irreducibility test. Therein, we check degeneracy with respect to $\mathcal{N}(F)$ at the first call and with respect to $\mathcal{N}^-(F)$ at the recursive calls.

**Algorithm:** `RNP`$(F, \mathbb{K})$
**Input:** $F \in \mathbb{K}[[x]][y]$ of degree $d > 0$.
**Output:** `True` if $F$ is irreducible in $\mathbb{K}[[x]][y]$, and `False` otherwise.
1 $N \leftarrow d$;
2 **while** $N > 1$ **do**
3  **if** $F$ *is not degenerated over* $\mathbb{K}$ **then return** *`False`*;
4  $(q, m, P, N) \leftarrow$ `EdgeData`$(F)$;
5  $F \leftarrow F(z^t x^q, x^m(y + z^s))/x^{qm\ell N}$; `// Puiseux transform`
6  $\mathbb{K} \leftarrow \mathbb{K}_P$;
7 **return** *`True`*;

The transform performed in `RNP` differs slightly from the classical Newton-Puiseux transform $F(x^q, x^m(y + z^{1/q}))$. This trick due to Duval avoids to introduce useless field extension $\mathbb{K}[z^{1/q}]$ of $\mathbb{K}[z] = \mathbb{K}_P$ inherent to ramification. The number of iterations is bounded by $\delta$ and powers of $x$ can be truncated modulo $x^{\delta+1}$, leading to a complexity $\mathcal{O}(d\,(\delta+1)^2)$ [22, Lemma 4, page 213][4].

**The Abhyankar trick.** At each recursive call, the Weierstrass Preparation Theorem ensures that the current polynomial $F$ of line 3 equals a Weierstrass polynomial $G = \sum_{i=0}^{N} g_i(x) y^i$ times a unit of $\mathbb{K}[[x, y]]$, and we can compute $G$ up to an arbitrary precision via Hensel lifting. The Abhyankar trick consists to replace the current polynomial $F$ by the *Abhyankhar shift* $H$ of its Weierstrass polynomial $G$:

$$H(x, y) \leftarrow G\big(x, y + c(x)\big), \qquad c(x) := -\frac{g_{N-1}(x)}{N}. \tag{2}$$

[3] In the Montes algorithm [14, Definition 1.9, page 368], the residual polynomial would rather design $P^{qN}$ in our context

[4] In [22], $\mathbb{K}$ is assumed to be a finite field. This result remains correct on any perfect field if one uses dynamic evaluation instead of univariate factorization or irreducibility test.

At the first call, we assume $F$ monic and we rather consider $G = F$ in (2). We call $H$ the *Abhyankar transform* of $F$, and denote $\texttt{Abhyankar}(F)$ the subroutine computing it (with infinite precision in what follows, but with a suitable finite precision in practice, see [25, Section 3.3]). The polynomial $H$ has now no terms of degree $N-1$, ensuring $q\ell > 1$ at line 4. This leads to the following variant of [24, Algorithm ARNP], where we stop computations if we find out that $F$ is reducible (therein, we keep the notations $\mathbb{K}_P$ and $z$ asociated to $P$).

**Algorithm:** $\texttt{ARNP}(F, \mathbb{K})$

**Input:** $F \in \mathbb{K}[[x]][y]$ monic of degree $d > 0$.
**Output:** `True` if $F$ is irreducible in $\mathbb{K}[[x]][y]$, and `False` otherwise.

1 $N \leftarrow d$;
2 **while** $N > 1$ **do**
3 $\quad H \leftarrow \texttt{Abhyankar}(F)$ ;
4 $\quad$ **if** $H$ *is not degenerated over* $\mathbb{K}$ **then return** *`False`*;
5 $\quad (q, m, P, N) \leftarrow \texttt{EdgeData}(H)$;
6 $\quad F \leftarrow H(z^t x^q, x^m(y + z^s))/x^{qm\ell N}$ ;
7 $\quad \mathbb{K} \leftarrow \mathbb{K}_P$;
8 **return** *`True`*;

*Remark* 1. The $(q, m)$-sequence of ARNP is not the same as the $(q, m)$-sequence of RNP, but can be deduced from it [25, Remark 5 and Example 2]. It contains enough information for computing the characteristic exponents of $F$; see Section 8.

Since $H$ has degree $N$ with no terms of degree $N-1$, either it is not degenerated, either its edge data satisfies $q\ell \geq 2$. The product of these invariants over all iterations satisfies $\prod_k q_k \ell_k \leq d$ (with equality if and only if $F$ is irreducible), and the number of calls is less than $\log(d)$. See [24, Section 4] for details. If $F$ is irreducible, we have moreover $v_x(F_y(S)) = \frac{\delta}{d}$ for any Puiseux series $S$ of $F$. Then, [25, Lemma 6] and [25, Corollary 4] prove that computations can be made modulo $x^{\frac{2\delta}{d}+1}$, leading to an expected number of operations over $\mathbb{K}$ bounded by $\mathcal{O}((\delta+1)\, d)$ [25, Proposition 18]. Moreover, as mentionned in the conclusion of [25], this complexity estimates is sharp. This is mainly due to the fact that despite the input data being of size $\delta$ after truncation, the Puiseux transform of line 6 generates a polynomial $F$ that can be of size $\Omega(d\,\delta)$ (which is then again reduced to size $\mathcal{O}(\delta)$ at line 3). The approach we propose in this paper avoids this intermediate increased size thanks to the theory of approximate roots.

**Notations.** If $\mathcal{N}(F)$ is not straight, then $F$ is reducible. If $\mathcal{N}(F)$ is straight with positive slope, we replace $F$ by its reciprocal polynomial. The leading coefficient is now invertible. Consequently, we assume in the remaining of this paper that $F$ is monic.

We denote by $H_0 := \texttt{Abhyankar}(F)$ and let $N_0 := \deg(H_0) = d$. If $N_0 = 1$ or $H_0$ is not degenerated, we let $g = 0$. Otherwise, we denote by $H_0, \ldots, H_{g-1}$ the successive

degenerated polynomials encountered at line 3 when running $\texttt{ARNP}(F, \mathbb{K})$. We collect their respective edge data in a list

$$\mathrm{Data}(F) := \big((q_1, m_1, P_1, N_1), \ldots, (q_g, m_g, P_g, N_g)\big).$$

The monic polynomial $H_0$ might have horizontal slope (in which case $q_1 = 1$ and $m_1 = 0$) while $H_k$ is Weierstrass and $m_{k+1} > 0$ for $1 \leq k < g$. We include the $N_k$'s in the list for convenience, although they can be deduced from the remaining data by (3). This data is closely related to what is called *a type* in [14]. The integer $g$ is defined in such a way that we have either $N_g = 1$ and $F$ is irreducible, either the next Weierstrass polynomial $H_g$ is not degenerated and $F$ is reducible. If $F$ is irreducible, we can deduce from $\mathrm{Data}(F)$ the characteristic monomials (exponents and coefficients) of any of its conjugated Puiseux series, see Section 8.

We let $\mathbb{K}_0 = \mathbb{K}$ and we denote $\mathbb{K}_k = \mathbb{K}_{k-1}[Z_k]/(P_k(Z_k))$ the field extension of $\mathbb{K}_{k-1}$ generated by $P_k$, where $Z_k$ is a new undeterminate. It is a finite extension of $\mathbb{K}$ of degree $f_k := \ell_1 \cdots \ell_k$, where $\ell_k := \deg(P_k)$; it represents the part of the residual extension discovered so far. We let $z_k \in \mathbb{K}_k$ be the residue class of $Z_k \mod P_k$.

For all $1 \leq k \leq g$, we have $H_k \in \mathbb{K}_k[[x]][y]$. The integer $N_k$ satisfies

$$N_k = \deg(H_k) \text{ and } N_{k-1} = N_k q_k \ell_k. \tag{3}$$

As $\ell_k q_k > 1$ for all $1 \leq k \leq g$, the sequence $N_0, \ldots, N_g$ is a strictly decreazing sequence of integers with $N_k$ dividing $N_{k-1}$.

We associate to $F$ the maps

$$\begin{cases} \tau_k(x, y) = (x, y + c_k(x)), & 0 \leq k \leq g, \\ \sigma_k(x, y) = (z_k^{t_k} x^{q_k}, x^{m_k}(y + z_k^{s_k})), & 1 \leq k \leq g \end{cases} \tag{4}$$

respectively defined to be the successive Abhyankhar shifts (2) and rational Newton-Puiseux transforms performed while running $\texttt{ARNP}(F, \mathbb{K})$: $\tau_k$ performed at line 3 on the Weierstrass polynomial of $F$ (or directly on $F$ for $k = 0$) and $\sigma_k$ at line 6, with $(s_k, t_k)$ the Bézout co-factors of $(q_k, m_k)$. Note that $c_k(0) = 0$ if $k \geq 1$ by (2). Defining $\pi_0 = \tau_0$, and $\pi_k = \pi_{k-1} \circ \sigma_k \circ \tau_k$ for $1 \leq k \leq g$, we get - see Lemma 8 for an explicit formula in terms of $\mathrm{Data}(F)$:

$$\pi_k(x, y) = (\mu_k x^{e_k}, \alpha_k x^{r_k} y + S_k(x)), \tag{5}$$

where $e_k := q_1 \cdots q_k$ (the ramification index discovered so far), $\mu_k, \alpha_k \in \mathbb{K}_k^\times$, $r_k \in \mathbb{N}$ and $S_k \in \mathbb{K}_k[[x]]$ satisfies $v_x(S_k) \leq r_k$. The pair $R_k = (\mu_k x^{e_k}, S_k \mod x^{r_k+1})$ is called in [25, Section 3.2] a *truncated rational Puiseux expansion*. We can deduce from $R_k$ all the roots of $F$ (seen as Puiseux series) truncated up to precision $\frac{r_k}{e_k}$, that increases with $k$.

By construction, there exists an integer $v_k(F) \in \mathbb{N}$ such that

$$\pi_k^* F = x^{v_k(F)} U_k H_k \in \mathbb{K}_k[[x]][y], \tag{6}$$

where $U_k(0, 0) \in \mathbb{K}_k^\times$. This key point will be used several times in the sequel. Also, note that the coefficient of $y^{N_k - 1}$ in $H_k$ is 0 from the Abhyankar shift (2).

**Minimal polynomials.** There exists a unic monic irreducible polynomial $\phi_k \in \mathbb{K}[[x]][y]$ (in practice in $\mathbb{K}[x][y]$ when truncating powers of $x$) such that

$$\phi_k(\mu_k x^{e_k}, S_k) = 0 \text{ and } d_k := \deg(\phi_k) = e_k f_k. \tag{7}$$

In particular, $\phi_0 = y - c_0(x)$ has degree 1. We call $\phi_k$ the $k^{th}$ *minimal polynomial* of $F$. We deduce from (3) $d = N_k\, d_k$ for all $k = 0, \ldots, g$. By construction, the function call $\texttt{ARNP}(\phi_k)$ generates the same transformations $\tau_i$, $\sigma_i$ for $i \leq k$ and we have

$$\text{Data}(\phi_k) = \big((q_1, m_1, P_1, N_1'), \ldots, (q_k, m_k, P_k, N_k' = 1)\big) \text{ with } N_i' := N_i/N_k. \tag{8}$$

Note that up to some constant $c$, $\phi_k$ may be computed as a multivariate resultant

$$\phi_k(x, y) = c\,\text{Res}_{\underline{Z},T}(x - \mu_k(\underline{Z})T^e, y - S_k(\underline{Z}, T), P_1(Z_1), \ldots, P_k(Z_1, \ldots, Z_k)), \tag{9}$$

where we consider here any liftings of the coefficients of $\mu_k, S_k, P_1, \ldots, P_k$ from $\mathbb{K}_k = \mathbb{K}[z_1, \ldots, z_k]$ to the polynomial ring $\mathbb{K}[\underline{Z}] := \mathbb{K}[Z_1, \ldots, Z_k]$.

# 3 Edge data from the $\Phi$-adic expansion

Let us fix an integer $0 \leq k \leq g$ and assume that $N_k > 1$. Given the edges data $(q_1, m_1, P_1, N_1), \ldots, (q_k, m_k, P_k, N_k)$ and the minimal polynomials $\phi_0, \ldots, \phi_k$, we want to decide if the next Weierstrass polynomial $H_k$ is degenerated and if so, to compute its edge data $(q_{k+1}, m_{k+1}, P_{k+1}, N_{k+1})$.

In the following, we will omit for readibility the index $k$ for the sets $\Phi$, $\mathcal{B}$, $V$ and $\Lambda$ defined below.

## 3.1 Main results

**$\Phi$-adic expansion.** Let $\phi_{-1} := x$ and denote $\Phi = (\phi_{-1}, \phi_0, \ldots, \phi_k)$. Let

$$\mathcal{B} := \{(b_{-1}, \ldots, b_k) \in \mathbb{N}^{k+2}\ ,\ b_{i-1} < q_i\, \ell_i\, , i = 1, \ldots, k\} \tag{10}$$

and denote $\Phi^B := \prod_{i=-1}^{k} \phi_i^{b_i}$. Thanks to the relations $\deg(\phi_i) = \deg(\phi_{i-1}) q_i \ell_i$ for all $1 \leq i \leq k$, an induction argument shows that $F$ admits a unique expansion

$$F = \sum_{B \in \mathcal{B}} f_B \Phi^B, \quad f_B \in \mathbb{K}.$$

We call it the $\Phi$-adic expansion of $F$. Note that we have necessarily $b_k \leq N_k$ while we do not impose any *a priori* condition to the powers of $\phi_{-1} = x$ in this expansion. The aim of this section is to show that one can extract the edge data of $H_k$ from the $\Phi$-adic expansion of $F$.

**Newton polygon.** Consider the semi-group homomorphism

$$\begin{array}{rccl} v_k: & (\mathbb{K}[[x]][y],\times) & \to & (\mathbb{N}\cup\{\infty\},+) \\ & H & \mapsto & v_k(H):=v_x(\pi_k^*H), \end{array}$$

From (5), we deduce that the pull-back morphism $\pi_k^*$ is injective, so that $v_k$ defines a discrete valuation. This is a valuation of transcendence degree one, thus an augmented valuation [26, Section 4.2], in the flavour of MacLane valuations [16, 17, 26] or Montes valuations [14, 19]. Note that $v_0(H)=v_x(H)$. We associate to $\Phi$ the vector

$$V:=(v_k(\phi_{-1}),\dots,v_k(\phi_k)),$$

so that $v_k(\Phi^B)=\langle B,V\rangle$, where $\langle\ ,\ \rangle$ stands for the usual scalar product. For all $i\in\mathbb{N}$, we define the integer

$$w_i:=\min\{\langle B,V\rangle,\ b_k=i,\ f_B\neq 0\}-v_k(F) \tag{11}$$

with convention $w_i:=\infty$ if the minimum is taken over the empty set.

**Theorem 5.** *The Newton polygon of $H_k$ is the lower convex hull of $(i,w_i)_{0\le i\le N_k}$.*

This result leads us to introduce the sets

$$\mathcal{B}(i):=\{B\in\mathcal{B};b_k=i\}\quad\text{and}\quad\mathcal{B}(i,w):=\{B\in\mathcal{B}(i)\mid\langle B,V\rangle=w\}$$

for all $i\in\mathbb{N}$ and all $w\in\mathbb{N}\cup\{\infty\}$, with convention $\mathcal{B}(i,\infty)=\emptyset$.

**Boundary polynomial.** Consider the semi-group homomorphism

$$\begin{array}{rccl} \lambda_k: & (\mathbb{K}[[x]][y],\times) & \to & (\mathbb{K}_k,\times) \\ & H & \mapsto & \lambda_k(H):=\mathrm{tc}_y\left(\left(\frac{\pi_k^*(H)}{x^{v_k(H)}}\right)_{|x=0}\right) \end{array}$$

with convention $\lambda_k(0)=0$, and where $\mathrm{tc}_y$ stands for the trailing coefficient with respect to $y$ (initial coefficient). We associate to $\Phi$ the vector

$$\Lambda:=(\lambda_k(\phi_{-1}),\dots,\lambda_k(\phi_k))$$

and denote $\Lambda^B:=\prod_{i=-1}^k\lambda_k(\phi_i)^{b_i}$. Note that $\Lambda^B\in\mathbb{K}_k$ is non zero for all $B$.

**Theorem 6.** *Let $B_0:=(0,\dots,0,N_k)$. The boundary polynomial $\bar{H}_k$ of $H_k$ equals*

$$\bar{H}_k=\sum_{(i,w_i)\in\mathcal{N}(H_k)}\left(\sum_{B\in\mathcal{B}(i,w_i+v_k(F))}f_B\Lambda^{B-B_0}\right)x^{w_i}y^i. \tag{12}$$

**Example 1.** If $k=0$, we have by definition $V=(1,0)$ and $\Lambda=(1,1)$ while $v_0(F)=v_x(H_0)=0$. Assuming $H_0=\sum_{j=0}^d a_i(x)y^i$, we find $w_i=v_x(a_i)$ and Theorem 5 stands from Definition 1. Moreover, $\mathcal{B}(i,w_i)$ is then reduced to the point $(i,w_i)$ and Theorem 6 stands from Definition 2.

### 3.2 Key Proposition and proofs of Theorems 5 and 6

Let us first establish some basic properties of the minimal polynomials $\phi_i$ of $F$. Given a ring $\mathbb{A}$, we denote by $\mathbb{A}[[x,y]]^\times$ the set of all $U \in \mathbb{A}[[x,y]]$ for which $U(0,0) \neq 0$. If $\mathbb{A}$ is a field (which might not be the case in Sections 7 and 8), this is simply the group of units of the ring $\mathbb{A}[[x,y]]$. For $-1 \leq i \leq k$, we introduce the notations

$$v_{k,i} := v_k(\phi_i) = v_x(\pi_k^*(\phi_i)) \quad \text{and} \quad \lambda_{k,i} := \lambda_k(\phi_i) = \mathrm{tc}_y\left(\left(\frac{\pi_k^*(\phi_i)}{x^{v_{k,i}}}\right)_{|x=0}\right).$$

**Lemma 1.** *Let $-1 \leq i \leq k$. There exists $U_{k,i} \in \mathbb{K}_k[[x,y]]^\times$ with $U_{k,i}(0,0) = \lambda_{k,i}$ s.t.:*

$$\begin{cases} \pi_k^*(\phi_i) = U_{k,i} x^{v_{k,i}} \text{ if } i < k \\ \pi_k^*(\phi_k) = U_{k,k} x^{v_{k,k}} y, \end{cases}$$

*Proof.* As $\texttt{ARNP}(\phi_k)$ generates the same transform $\pi_k$, we deduce from (6):

$$\pi_k^*(\phi_k) = x^{v_k(\phi_k)}\, U(x,y)\,(y + \beta(x))$$

with $U \in \mathbb{K}_k[[x,y]]^\times$ and $\beta \in \mathbb{K}_k[[x]]$. From (5) and (7), we get $x^{v_{k,k}} U(x,0)\beta(x) = \phi_k(\mu_k x^{e_k}, S_k) = 0$, i.e. $\beta = 0$. Second equality follows, since $U(0,0) = \lambda_{k,k}$ by definition of $\lambda_k$. First equality follows from the second one by applying the pull-backs $(\sigma_j \circ \tau_j)^*$, $j = i+1, \ldots, k$ to $\pi_i^*(\phi_i) = x^{v_{ii}}\, y\, U_{ii}$. □

**Corollary 1.** *With the standard notations for intersection multiplicities and resultants, we have*

$$v_k(\phi_i) = \frac{(\phi_i, \phi_k)_0}{f_k} = \frac{v_x(Res_y(\phi_i, \phi_k))}{f_k}, \ -1 \leq i \leq k-1.$$

*Proof.* By point 2 in Lemma 1, we deduce that

$$v_k(\phi_i) := v_x(\pi_k^*(\phi_i)) = v_x(\phi_i(\mu_k x^{e_k}, S_k(x))) \text{ since } v_x(S_k) \leq r_k.$$

But this last integer coincides with the intersection multiplicity of $\phi_i$ with any one of the $f_k$ conjugate plane branches (i.e. irreducible factor in $\overline{\mathbb{K}}[[x]][y]$) of $\phi_k$. The first equality follows. The second is well known (the intersection multiplicity at $(0,0)$ of two Weierstrass polynomials coincides with the $x$-valuation of their resultant). □

**Lemma 2.** *We have initial conditions $v_{0,-1} = 1$, $v_{0,0} = 0$, $\lambda_{0,-1} = 1$ and $\lambda_{0,0} = 1$. Let $k \geq 1$. The following relations hold (we recall $q_k s_k - m_k t_k = 1$ with $0 \leq t_k < q_k$) :*

1. $v_{k,k-1} = q_k v_{k-1,k-1} + m_k$
2. $v_{k,i} = q_k v_{k-1,i}$ *for all* $-1 \leq i < k-1$.
3. $\lambda_{k,k-1} = \lambda_{k-1,k-1} z_k^{t_k v_{k-1,k-1} + s_k}$.
4. $\lambda_{k,i} = \lambda_{k-1,i} z_k^{t_k v_{k-1,i}}$ *for all* $-1 \leq i < k-1$.

*Proof.* Initial conditions follow straightforwardly from the definitions. From point 1 of Lemma 1 and the definition of $\pi_k$, we have $\pi_k^*(\phi_{k-1}) = \tau_k^* \circ \sigma_k^* \circ \pi_{k-1}^*(\phi_{k-1})$, i.e.

$$\pi_k^*(\phi_{k-1}) = z_k^{t_k v_{k-1,k-1}} x^{q_k v_{k-1,k-1}+m_k}\, \tilde{y} U_{k-1,k-1}(z_k^{t_k} x^{q_k}, x^{m_k}\, \tilde{y}).$$

where $\tilde{y} = y + z_k^{s_k} + c_k(x)$. As $c_k(0) = 0$, $m_k > 0$ and $z_k \neq 0$, it follows that

$$\pi_k^*(\phi_{k-1}) = z_k^{t_k v_{k-1,k-1}+s_k} x^{q_k\, v_{k-1,k-1}+m_k} \tilde{U}(x, y)$$

with $\tilde{U}(0,0) = U_{k-1,k-1}(0,0)$, that is $\lambda_{k-1,k-1}$ by point 1 of Lemma 1. Items 1 and 3 follow. Similarly, using point 2 of Lemma 1, we get for all $i < k-1$

$$\pi_k^*(\phi_i) = \tau_k^* \circ \sigma_k^* \circ \pi_{k-1}^*(\phi_i) = z_k^{t_k v_{k-1,i}} x^{q_k v_{k-1,i}} U_{k-1,i}(z_k^{t_k} x^{q_k}, x^{m_k}(y + z_k^{s_k} + c_k(x))).$$

As $U_{k-1,i}(0,0) = \lambda_{k-1,i} \neq 0$ once again by Point 2 of Lemma 1, items 2 and 4 follow. □

The proof of both theorems is based on the following key result:

**Proposition 1.** *For all $i, w \in \mathbb{N}$, the family $\left(\Lambda^B, B \in \mathcal{B}(i,w)\right)$ is free over $\mathbb{K}$. In particular, Card$(\mathcal{B}(i,w)) \leq f_k$.*

*Proof.* We show this property by induction on $k$. If $k = 0$, the result is obvious since $\mathcal{B}(i,w) = \{(i,w)\}$ and $\Lambda = (1,1)$. Suppose $k > 0$. As $\lambda_{k,k}$ is invertible and $b_k = i$ is fixed, we are reduced to show that the family $\left(\Lambda^B, B \in \mathcal{B}(0,w)\right)$ is free for all $w \in \mathbb{N}$. Suppose given a $\mathbb{K}$-linear relation

$$\sum_{B \in \mathcal{B}(0,w)} c_B \Lambda^B = \sum_{B \in \mathcal{B}(0,w)} c_B \lambda_{k,-1}^{b_{-1}} \cdots \lambda_{k,k-1}^{b_{k-1}} = 0. \tag{13}$$

Using $b_k = 0$, points 3 and 4 in Lemma 2 give $\Lambda^B = \mu_B z_k^{N_B}$ where

$$\mu_B = \prod_{j=-1}^{k-1} \lambda_{k-1,j}^{b_j} \in \mathbb{K}_{k-1} \quad \text{and} \quad N_B = b_{k-1} s_k + t_k \sum_{j=-1}^{k-1} b_j v_{k-1,j}.$$

Points 1 ($q_k\, v_{k-1,k-1} = v_{k,k-1} - m_k$) and 2 ($q_k\, v_{k-1,j} = v_{k,j}$) in Lemma 2 give

$$q_k N_B = b_{k-1}(q_k s_k - m_k t_k) + t_k \sum_{j=-1}^{k-1} b_j v_{k,j} = b_{k-1} + t_k w, \tag{14}$$

the second equality using $\langle B, V \rangle = w$ and $b_k = 0$. Since $0 \leq b_{k-1} < q_k \ell_k$ and $N_B$ is an integer, it follows from (14) that $N_B = n + \alpha$ where $n = \lceil t_k w / q_k \rceil$ and $0 \leq \alpha < \ell_k$. Dividing (13) by $z_k^n$, we get

$$\sum_{\alpha=0}^{\ell_k - 1} a_\alpha z_k^\alpha = 0, \quad \text{where} \quad a_\alpha = \sum_{B \in \mathcal{B}(0,w), N_B = \alpha + n} c_B \mu_B.$$

Since $a_\alpha \in \mathbb{K}_{k-1}$ and $z_k \in \mathbb{K}_k$ has minimal polynomial $P_k$ of degree $\ell_k$ over $\mathbb{K}_{k-1}$, this implies $a_\alpha = 0$ for all $0 \le \alpha < \ell_k$, i.e., using (14):

$$\sum_{\substack{B\in\mathcal{B}(0,w)\\ b_{k-1}=q_k\,(\alpha+n)-t_k\,w}} c_B \lambda_{k-1,-1}^{b_{-1}} \cdots \lambda_{k-1,k-1}^{b_{k-1}} = 0.$$

By induction, we get $c_B = 0$ for all $B \in \mathcal{B}(0,w)$, as required. The first claim is proved. The second claim follows immediately since $\Lambda^B \in \mathbb{K}_k$ is non zero for all $B$. □

**Corollary 2.** *Consider $G = \sum_{B\in\mathcal{B}(i)} g_B \Phi^B$ non zero. Then $\pi_k^*(G) = \tilde{U} x^w\, y^i$ with $\tilde{U} \in \mathbb{K}_k[[x,y]]^\times$, $w = \min_{g_B\neq 0}\langle B, V\rangle$ and $\tilde{U}(0,0) = \sum_{B\in\mathcal{B}(i,w)} g_B \Lambda^B \neq 0$. In particular, $v_k(G) = w$ and $\lambda_k(G) = \tilde{U}(0,0)$.*

*Proof.* By linearity of $\pi_k^*$, denoting $U = (U_{k,-1}, \ldots, U_{k,k})$ with $U_{k,i}$ defined in Lemma 1, we have

$$\pi_k^*(G) = \left( \sum_{B\in\mathcal{B}(i)} g_B U^B x^{<B,V>} \right) y^i \text{ with } U(0,0) = \Lambda.$$

Letting $w = \min_{g_B\neq 0}\langle B, V\rangle$, we deduce

$$\pi_k^*(G) = \left( \sum_{B\in\mathcal{B}(i,w)} g_B \Lambda^B + R \right) x^w y^i \quad \text{where } R \in \mathbb{K}_k[[x,y]] \text{ satisfies } R(0,0) = 0.$$

As $\sum_{B\in\mathcal{B}(i,w)} g_B \Lambda^B \neq 0$ by Proposition 1, the first two equalities follows. The last two equalities follow from the definitions of $v_k(G)$ and $\lambda_k(G)$. □

**Proof of Theorems 5 and 6.** We prove both theorems simultaneously. We may write $F = \sum_{i=0}^{N_k} \sum_{B\in\mathcal{B}(i)} f_B \Phi^B$. Hence, Corollary 2 combined with the definition of $w_i$ and the linearity of $\pi_k^*$ implies

$$F_k := \frac{\pi_k^*(F)}{x^{v_k(F)}} = \sum_{i=0}^{N_k} \tilde{U}_i\, x^{w_i}\, y^i \tag{15}$$

where $\tilde{U}_i \in \mathbb{K}_k[[x,y]]$ is 0 if $w_i = \infty$, and $\tilde{U}_i(0,0) = \sum_{B\in\mathcal{B}(i,w_i+v_k(F))} f_B \Lambda^B \neq 0$ otherwise. Let $\mathcal{N}$ stands for the lower convex hull of the set $((i,w_i), i = 0,\ldots,N_k)$ and let $\mathcal{N}^-$ be the subset of negative slopes. If $k = 0$, then $H_0 = F_0$ and we have moreover $\tilde{U}_i \in \mathbb{K}$ for all $i$ (use that $\pi_0^*(\phi_0) = y$). It follows immediately from (15) that $\mathcal{N}(H_0) = \mathcal{N}$, as required. If $k > 0$, then we deduce from (15) that $\mathcal{N}^-(F_k) = \mathcal{N}^-$. Combined with (6), we get $\mathcal{N}^-(H_k) = \mathcal{N}^-$. As $k \ge 1$, $H_k$ is Weierstrass of degree $N_k$, which forces $\mathcal{N}(H_k) = \mathcal{N}$ as required. This proves Theorem 5. Combined with (6), we deduce more precisely that there exists $\mu \in \mathbb{K}_k^\times$ such that

$$\mu \bar{H}_k = \sum_{(i,w_i)\in\mathcal{N}} \left( \sum_{B\in\mathcal{B}(i,w_i+v_k(F))} f_B \Lambda^B \right) x^{w_i} y^i. \tag{16}$$

Since $\bar{H}_k$ is monic of degree $N_k$, we get $w_{N_k} = 0$ and $w_i \geq 0$ for $i < N_k$ and we deduce from (16) that

$$\mu = \sum_{B \in \mathcal{B}(N_k, v_k(F))} f_B \Lambda^B. \tag{17}$$

But $F$ and $\phi_k$ being monic of respective degrees $d$ and $d_k$, the vector $B_0 = (0, \dots 0, N_k) \in \mathcal{B}$ is the unique exponent in the $\Phi$-adic expansion of $F$ with last coordinate $b_k = N_k = d/d_k$ and we have moreover $f_{B_0} = 1$. Since $\mathcal{B}(N_k, v_k(F))$ is non empty by construction, this forces $\mathcal{B}(N_k, v_k(F)) = \{B_0\}$ and (17) becomes $\mu = \Lambda^{B_0}$. Theorem 6 follows. □

### 3.3 Formulas for $\lambda_k(\phi_k)$ and $v_k(\phi_k)$

In order to use Theorems 5 and 6 for computing the edge data of $H_k$, we need to compute $v_{k,k} := v_k(\phi_k)$ and $\lambda_{k,k} := \lambda_k(\phi_k)$ in terms of the previously computed edges data $(q_1, m_1, P_1, N_1), \dots, (q_k, m_k, P_k, N_k)$ of $F$. We begin with the following lemma:

**Lemma 3.** *Let $0 \leq k \leq g$. We have $v_k(F) = N_k v_{k,k}$ and $\lambda_k(F) = \lambda_{k,k}^{N_k}$.*

*Proof.* We have shown during the proof of Theorems 5 and 6 that $\mathcal{B}(N_k, v_k(F)) = \{B_0\}$ where $B_0 = (0, \dots, 0, N_k)$. By definition of $\mathcal{B}(N_k, v_k(F))$, we get the first point. By definition of $\lambda_k$, we have $\lambda_k(F) = \mathrm{tc}_y\left(F_k(0,y)\right) = \mathrm{tc}_y\left(\bar{F}_k(0,y)\right)$ and we have shown that $\bar{F}_k(0,y) = \Lambda^{B_0}\bar{H}_k(0,y)$. Since $\bar{H}_k$ is monic, we deduce that $\mathrm{tc}_y\left(\bar{F}_k(0,y)\right) = \Lambda^{B_0}$, giving the second claim. □

**Proposition 2.** *For any $1 \leq k \leq g$, we have the equalities*

$$v_{k,k} = q_k \ell_k v_{k,k-1} \quad \text{and} \quad \lambda_{k,k} = q_k z_k^{1-s_k-\ell_k} P_k'(z_k) \lambda_{k,k-1}^{q_k \ell_k}.$$

*Proof.* To simplify the notations of this proof, let us denote $w = v_{k-1}(\phi_k)$, $\gamma = \lambda_{k-1}(\phi_k)$ and $(m, q, s, t, \ell, z) = (m_k, q_k, s_k, t_k, \ell_k, z_k)$. By definition of $\phi_k$, both $\phi_k$ and $F$ generate the same transformations $\sigma_i$ and $\tau_i$ for $i \leq k$. As in (6), there exists $\tilde{U}_{k-1} \in \mathbb{K}[[x,y]]^\times$ satisfying $\tilde{U}_{k-1}(0,0) = \gamma$ and $\tilde{H}_{k-1} \in \mathbb{K}[[x]][y]$ Weierstrass of degree $q\,\ell$ such that $\pi_{k-1}^*(\phi_k) = x^w \tilde{H}_{k-1}\tilde{U}_{k-1}$, where

$$\tilde{H}_{k-1}(x,y) = P_k(x^{-m}\,y^q)x^{m\ell} + \sum_{mi+qj > mq\ell} h_{ij} x^j y^i.$$

We deduce that there exists $R_0, R_1, R_2 \in \mathbb{K}_k[[x,y]]$ such that

$$\begin{aligned} \pi_k^*(\phi_k) &:= (\pi_{k-1}^*(\phi_k))(z^t x^q, x^m(y + z^s + c_k(x))) \\ &= z^{tw} x^{qw} \left( z^{tm\ell}\, x^{mq\ell} (G_k + xR_0) \right) (\gamma + x\,R_1 + y\,R_2) \end{aligned}$$

where we let $G_k(x,y) := P_k(z^{-tm}(y + z^s + c_k(x))^q) \in \mathbb{K}_k[[x]][y]$. It follows that there exists $R \in \mathbb{K}_k[[x,y]]$ such that

$$\pi_k^*(\phi_k) = \gamma\, z^{t(w+m\ell)}\, x^{q\,(w+m\ell)}\, (G_k(1 + yR_2) + x\,R) \tag{18}$$

As $G_k(0,y)$ is not identically zero, we deduce from (18) that $v_k(\phi_k) = q\,(w+m\ell)$. Using Lemma 3 for $F=\phi_k$ and the valuation $v_{k-1}$, together with Point 1 of Lemma 2, we have $w+m\ell = \ell v_{k,k-1}$, which implies $v_{k,k} = q\,\ell\,v_{k,k-1}$ as expected. Using $c_k(0)=0$ and the relation $sq-tm=1$, we see that $G_k(0,0) = P_k(z_k) = 0$ and $\partial_y G_k(0,0) = qz^{1-s}P_k'(z)$ is non zero. Combined with (18), we get that

$$\lambda_{k,k} = \gamma z^{t\,\ell\,v_{k,k-1}}\left(qz^{1-s}P_k'(z)\right) = \gamma\, z^{q\,\ell\,t\,v_{k-1,k-1}+\ell\,t\,m+1-s}\,q\,P_k'(z),$$

the second equality using Point 1 of Lemma 2 once again. Now, using Lemma 3 for $F=\phi_k$ and the morphism $\lambda_{k-1}$, we get $\gamma = \lambda_{k-1,k-1}^{\ell q}$ so that $\lambda_{k,k} = qP_k'(z)\lambda_{k,k-1}^{q\ell}z^{1-s-\ell}$ as expected. □

*Remark* 2. If $q_k = 1$, the second formula simplifies as $\lambda_{k,k} = P_k'(z_k)\lambda_{k-1,k-1}^{\ell_k}$. Moreover, we then have $t=0$ and $s=1$ so that no division by $z_k$ is done in the above proof. This remark is used in Sections 7 and 8 where $z_k$ might be a zero divisor when $q_k = 1$.

### 3.4 Simple formulas for $V$ and $\Lambda$.

For convenience to the reader, let us summarize the formulas which allow to compute in a simple recursive way both lists $V = (v_{k,-1},\dots,v_{k,k})$ and $\Lambda = (\lambda_{k,-1},\dots,\lambda_{k,k})$.

If $k=0$, we let $V=(1,0)$ and $\Lambda=(1,1)$. Assume $k\geq 1$. Given the lists $V$ and $\Lambda$ at rank $k-1$ and given the $k$-th edge data $(q_k, m_k, P_k, N_k)$, we update both lists at rank $k$ thanks to the formulæ:

$$\begin{cases} v_{k,i} = q_k v_{k-1,i} & -1\leq i<k-1 \\ v_{k,k-1} = q_k v_{k-1,k-1} + m_k \\ v_{k,k} = q_k \ell_k v_{k,k-1} \end{cases} \qquad \begin{cases} \lambda_{k,i} = \lambda_{k-1,i} z_k^{t_k v_{k-1,i}} & -1\leq i<k-1 \\ \lambda_{k,k-1} = \lambda_{k-1,k-1} z_k^{t_k v_{k-1,k-1}+s_k} \\ \lambda_{k,k} = q_k z_k^{1-s_k-\ell_k} P_k'(z_k)\lambda_{k,k-1}^{q_k\ell_k} \end{cases} \tag{19}$$

where $q_k s_k - m_k t_k = 1$, $0\leq t_k < q_k$ and $z_k = Z_k \mod P_k$.

## 4 From minimal polynomials to approximate roots

Given $\Phi = (\phi_{-1},\dots,\phi_k)$ and $F = \sum f_B \Phi^B$ the $\Phi$-adic expansion of $F$, the updated lists $V$ and $\Lambda$ then allow to compute in an efficient way the boundary polynomial $\bar{H}_k$ thanks to the formulas (11) and (12). Unfortunately, the computation of the minimal polynomials $\phi_k$ is up to our knowledge too expensive to fit in our aimed complexity bound. For instance, it requires to know the $y^{N_k-1}$ coefficients of the Puiseux transform of $H_{k-1}$ up to some suitable precision, and computing this Puiseux transform might be costly, as explained in Section 2.

In this section, we show that the main conclusions of all previous results remain true if we replace $\phi_k$ by the $N_k^{th}$-approximate root $\psi_k$ of $F$, with the great advantage that these approximate roots can be computed in the aimed complexity (see Section 7). Up to our knowledge, such a strategy was introduced by Abhyankar who developped in [1]

an irreducibility criterion in $\overline{\mathbb{K}}[[x,y]]$ which avoids to perform any Newton-Puiseux type transforms.

## 4.1 Approximate roots and main result

**Approximate roots.** The approximate roots of a monic polynomial $F$ are defined thanks to the following proposition:

**Proposition 3.** (*see e.g.* [20, Proposition 3.1]). *Let $F \in \mathbb{A}[y]$ be monic of degree $d$, with $\mathbb{A}$ a ring whose characteristic does not divide $d$. Let $N \in \mathbb{N}$ dividing $d$. There exists a unique polynomial $\psi \in \mathbb{A}[y]$ monic of degree $d/N$ such that $\deg(F - \psi^N) < d - d/N$. We call it the $N^{th}$ approximate roots of $F$.*

A simple degree argument implies that $\psi$ is the $N^{th}$-approximate root of $F$ if and only if the $\psi$-adic expansion $\sum_{i=0}^{N} a_i \psi^i$ of $F$ satisfies $a_{N-1} = 0$. For instance, if $F = \sum_{i=0}^{d} a_i y^i$, the $d^{th}$ approximate root coincides with the Tschirnhausen transform of $y$

$$\tau_F(y) = y + \frac{a_{d-1}}{d}.$$

More generally, the $N^{th}$ approximate root can be constructed as follows. Given $\phi \in R[y]$ a monic of degree $d/N$ and given $F = \sum_{i=0}^{N} a_i \phi^i$ the $\phi$-adic expansion of $F$, we consider the new polynomial

$$\tau_F(\phi) := \phi + \frac{a_{N-1}}{N}$$

which is again monic of degree $d/N$. It can be shown that the resulting $\tau_F(\phi)$-adic expansion $F = \sum a'_i \tau_F(\phi)^i$ satisfies $\deg(a'_{N-1}) < \deg(a_{N-1}) < d/N$ (see e.g. [20, Proof of Proposition 6.3]). Hence, after applying at most $d/N$ times the operator $\tau_F$, the coefficient $a'_{N-1}$ vanishes and the polynomial $\tau_F \circ \cdots \circ \tau_F(\phi)$ coincides with the approximate root $\psi$ of $F$. Although this is not the best strategy from a complexity point of view (see Section 7), this construction will be used to prove Theorem 7 below.

**Main result.** We still consider $F \in \mathbb{K}[[x]][y]$ monic of degree $d$ and keep notations from Section 2. We denote $\psi_{-1} := x$ and, for all $k = 0, \ldots, g$, we denote $\psi_k$ the $N_k^{th}$-approximate root of $F$. Fixing $0 \leq k \leq g$, we denote $\Psi = (\psi_{-1}, \psi_0, \ldots, \psi_k)$, omitting once again the index $k$ for readibility.

Since $\deg \Psi = \deg \Phi$ by definition, the exponents of the $\Psi$-adic expansion

$$F = \sum_{B \in \mathcal{B}} f'_B \Psi^B, \quad f'_B \in \mathbb{K}$$

take their values in the same set $\mathcal{B}$ introduced in (10). In the following, we denote by $w'_i \in \mathbb{N}$ the new integer defined by (11) when replacing $f_B$ by $f'_B$ and we denote $\bar{H}'_k$ the new polynomial obtained when replacing $w_i$ by $w'_i$ and $f_B$ by $f'_B$ in (12).

**Theorem 7.** *We have $\bar{H}_k = \bar{H}'_k$ for $0 \leq k < g$ and the boundary polynomial $\bar{H}_g$ and $\bar{H}'_g$ have same restriction to their Newton polygon's lower edge.*

In other words, Theorems 5 and 6 still hold when replacing minimal polynomials by approximate roots, up to a minor difference when $k = g$ which has no impact for degeneracy tests.

**Intermediate results.** The proof of Theorem 7 requires several steps. We denote by $-m_{g+1}/q_{g+1}$ the slope of the lower edge of $H_g$.

**Lemma 4.** *We have $v_k(\psi_k - \phi_k) > v_k(\phi_k) + m_{k+1}/q_{k+1}$ for all $k = 0, \ldots, g$.*

*Proof.* Let $(q, m) = (q_{k+1}, m_{k+1})$. Since the lemma is true if $\psi_k = \phi_k$ and since $\psi_k$ is obtained after successive applications of the operator $\tau_F$ to $\phi_k$, it is sufficient to prove

$$v_k(\phi - \phi_k) > v_k(\phi_k) + m/q \Longrightarrow v_k(\tau_F(\phi) - \phi_k) > v_k(\phi_k) + m/q \tag{20}$$

for any $\phi \in \mathbb{K}[[x]][y]$ monic of degree $d_k$. Suppose given such a $\phi$ and consider the $\phi$-adic expansion $F = \sum_{j=0}^{N_k} a_j \phi^j$. Then (20) holds if and only if

$$v_k(a_{N_k-1}) > v_k(\phi_k) + m/q. \tag{21}$$

• *Case $\phi = \phi_k$.* Then we have $v_k(a_{N_k-1}) \geq v_k(F) + m/q = N_k\, v_k(\phi_k) + m/q$ from Theorem 5 and Lemma 3. Suppose first that $v_k(\phi_k) = 0$. This may happen only when $k = 0$, or $k = 1$ if $m_1 = 0$. As $\phi_0 = \psi_0$, we do not need to consider the case $k = 0$. If $m_1 = 0$, the first slope is horizontal and the Abhyankhar transform (2) ensures that the coefficient of $y^{N_1-1}$ has no constant term, so that $v_1(a_{N_1-1}) > 0$ as required. Suppose now $v_k(\phi_k) > 0$. If $N_k > 1$, we are done. If $N_k = 1$, we must have $k = g$ and $H_g = y$, so that $v_g(a_0) = \infty$ from Theorem 5 and the claim follows.

• *Case $\phi \neq \phi_k$.* First note that $v_k(\phi - \phi_k) > v_k(\phi_k)$ implies $v_k(\phi) = v_k(\phi_k)$. As $\deg(\phi - \phi_k) < d_k$, we deduce from Corollary 2 (applied to $G = \phi - \phi_k$ and $i = 0$) and Lemma 1 that

$$\pi_k^*(\phi) = \pi_k^*(\phi - \phi_k) + \pi_k^*(\phi_k) = x^{v_k(\phi)} U(y + x^\alpha \tilde{U})$$

where $\alpha := v_k(\phi - \phi_k) - v_k(\phi_k) > m/q$ (hypothesis) and for some units $U, \tilde{U} \in \mathbb{K}_k[[x, y]]^\times$. As $a_i$ has also degree $< d_k$, we deduce again from Corollary 2 that when $a_i \neq 0$,

$$\pi_k^*(a_i \phi^i) = x^{\alpha_i} U_i (y + x^\alpha \tilde{U})^i, \tag{22}$$

where $\alpha_i := v_k(a_i \phi^i)$ and $U_i \in \mathbb{K}[[x, y]]^\times$. As $\alpha > m/q$, this means that the lowest line with slope $-q/m$ which intersects the support of $\pi_k^*(a_i \phi^i)$ intersects it at the unique point $(i, \alpha_i)$. Since $\pi_k^*(F) = \sum_{i=0}^{N_k} \pi_k^*(a_i \phi^i)$, we deduce that the edge of slope $-q/m$ of the Newton polygon of $\pi_k^*(F)$ coincides with the edge of slope $-q/m$ of the lower convex hull of $((i, \alpha_i)\, ; a_i \neq 0, 0 \leq i \leq N_k)$. Thanks to (6) combined with $v_k(F) = N_k v_k(\phi_k)$ (Lemma 3) and $v_k(\phi_k) = v_k(\phi)$ (hypothesis), we deduce that the lower edge $\Delta$ of $H_k$ with slope

$-q/m$ coincides with the edge of slope $-q/m$ of the lower convex hull of the points $((i, v_k(a_i) + (i - N_k)\, v_k(\phi))\, ; a_i \neq 0, 0 \leq i \leq N_k)$. Since $H_k$ is monic of degree $N_k$ *with no terms of degree* $N_k - 1$, we deduce that $(N_k, 0) \in \Delta$ while $(N_k - 1, v_k(a_{N_k-1}) - v_k(\phi))$ must lie above $\Delta$. It follows that $mN_k < m(N_k - 1) + q(v_k(a_{N_k-1}) - v_k(\phi))$, leading to the required inequality $v_k(a_{N_k-1}) > v_k(\phi) + m/q$. The lemma is proved. □

**Proposition 4.** *We have* $v_k(\Psi) = v_k(\Phi)$ *and* $\lambda_k(\Psi) = \lambda_k(\Phi)$ *for all* $k = 0, \ldots, g$.

*Proof.* We show this result by induction. If $k = 0$, we are done since $\psi_0 = \tau_F(y) = \phi_0$. Let us fix $1 \leq k \leq g$ and assume that Proposition 4 holds for all $k' \leq k - 1$. We need to show that $v_k(\psi_i) = v_k(\phi_i)$ and $\lambda_k(\psi_i) = \lambda_k(\phi_i)$ for all $i \leq k$. Case $i = k$ is a direct consequence of Lemma 4. For $i = k - 1$, there is nothing to prove if $\phi_{k-1} = \psi_{k-1}$. Otherwise, using the linearity of $\pi^*_{k-1}$, Corollary 2 (applied at rank $k - 1$ with $G = \phi_{k-1} - \psi_{k-1}$ and $i = 0$) and Lemma 4 give $\pi^*_{k-1}(\psi_{k-1}) = \pi^*_{k-1}(\phi_{k-1}) + x^\alpha \tilde{U}$ with $\alpha > v_{k-1}(\phi_{k-1}) + m_k/q_k$ and $\tilde{U} \in \mathbb{K}_{k-1}[[x, y]]^\times$. As $\pi^*_k(\psi_{k-1}) = (\sigma_k \circ \tau_k)^*(\pi^*_{k-1}(\psi_{k-1}))$, it follows that

$$\pi^*_k(\psi_{k-1}) = \pi^*_k(\phi_{k-1}) + x^{q_k \alpha} U_\alpha$$

with $U_\alpha \in \mathbb{K}_k[[x, y]]^\times$. As $q_k\, \alpha > v_k(\phi_{k-1})$ using Lemma 2 ($q_k\, v_{k-1,k-1} + m_k = v_{k,k-1}$), we deduce $v_k(\psi_{k-1}) = v_k(\phi_{k-1})$ and $\lambda_k(\psi_{k-1}) = \lambda_k(\phi_{k-1})$. Finally, for $i < k - 1$, as $\deg(\psi_i) < d_{k-1}$, Corollary 2 (applied at rank $k - 1$ with $G = \psi_i$ and $i = 0$) gives

$$\pi^*_{k-1}(\psi_i) = x^{v_{k-1}(\psi_i)} \lambda_{k-1}(\psi_i) U_i = x^{v_{k-1}(\phi_i)} \lambda_{k-1}(\phi_i) U_i,$$

where $U_i(0, 0) = 1$ (the second equality using the induction hypothesis). Applying $(\tau_k \circ \sigma_k)^*$ and using Lemma 2, we conclude $v_k(\psi_i) = v_k(\phi_i)$ and $\lambda_k(\psi_i) = \lambda_k(\phi_i)$. □

**Corollary 3.** *Let* $G$ *of degree less than* $d_k$ *and with* $\Psi$*-adic expansion* $G = \sum g'_B \Psi^B$. *Then*

$$v_k(G) = \min(\langle B, V \rangle, g'_B \neq 0) \quad \textit{and} \quad \lambda_k(G) = \sum_{B \in \mathcal{B}(0, v_k(G))} g'_B \Lambda^B.$$

*In particular, if* $G$ *has* $\Phi$*-adic expansion* $\sum g_B \Phi^B$, *then* $g_B = g'_B$ *when* $\langle B, V \rangle = v_k(G)$.

*Proof.* As already shown in the proof of Proposition 4, from Corollary 2, if $i < k$, we have $\pi^*_k(\psi_i) = x^{v_{k,i}} \lambda_{k,i}\, U_i$ with $U_i(0, 0) = 1$. As $\deg(G) < d_k$, we deduce

$$\pi^*_k(G) = \sum g'_B \Lambda^B x^{\langle B, V \rangle} U_B$$

with $U_B(0, 0) = 1$. This shows the result, using Proposition 1. □

**Proof of Theorem 7.** Write $F = \sum_i a_i \psi_k^i$ the $\psi_k$-adic expansion of $F$. Similarly to (22), when $a_i \neq 0$, Corollary 2 and Lemma 4 imply:

$$\pi^*_k(a_i \psi_k^i) = x^{v_k(a_i \psi_k^i)} U (y + x^\alpha \tilde{U})^i, \tag{23}$$

with $\alpha > m_{k+1}/q_{k+1}$, $U, \tilde{U} \in \mathbb{K}_k[[x,y]]^\times$ and $U(0,0) = \lambda_k(a_i\,\psi_k^i)$. Applying the same argument than in the proof of Lemma 4, we get that each point $(i, w_i = N_k - i\,m_{k+1}/q_{k+1})$ of the lower edge $\mathcal{N}_k^*$ of the Newton polygon of $H_k$ (hence the all polygon if $k < g$) is actually $(i, v_k(a_i\,\psi_k^i) - v_k(F))$, that is $(i, w_i')$ from Corollary 3 (applied to $G = a_i$) and Proposition 4. This shows that we may replace $w_i$ by $w_i'$ in (11). More precisely, it follows from (23) that the restriction $\bar{H}_k^*$ of $\bar{H}_k$ to $\mathcal{N}_k^*$ is uniquely determined by the equality

$$\lambda_k(F)x^{v_k(F)}\bar{H}_k^* = \sum_{(i,w_i')\in\mathcal{N}_k^*} \lambda_k(a_i\psi_k^i)x^{v_k(a_i\psi_k^i)}y^i.$$

Using again Corollary 3 and Proposition 4, we get

$$\bar{H}_k^* = \sum_{(i,w_i')\in\mathcal{N}_k^*} \left( \sum_{B\in\mathcal{B}(i,w_i'+v_k(F))} f_B'\Lambda^{B-B_0} \right) x^{w_i'}y^i,$$

as required. □

*Remark* 3. Theorem 7 would still hold when replacing $\psi_k$ by any monic polynomial $\phi$ of same degree for which $\pi_k^*(\phi) = Ux^{v_{k,k}}(y + \beta(x))$ with $v_x(\beta) > m_{k+1}/q_{k+1}$.

### 4.2 An Abhyankar type irreducibility test for Weierstrass polynomials

Theorem 7 leads to the following sketch of algorithm. Subroutines `AppRoot`, `Expand` and `BoundaryPol` respectively compute the approximate roots, the $\Psi$-adic expansion and the current lower boundary polynomial (using (11) and (12)). They are detailed in Section 7. Also, considerations about truncation bounds is postponed to Section 7.2.

**Algorithm:** `Irreducible`$(F, \mathbb{L})$

**Input:** $F \in \mathbb{K}[[x]][y]$ monic with $d = \deg(F)$ not divisible by the characteristic of $\mathbb{K}$ ; $\mathbb{L}$ a field extension of $\mathbb{K}$.

**Output:** `True` if $F$ is irreducible in $\mathbb{L}[[x]][y]$, and `False` otherwise.

$N \leftarrow d$, $V \leftarrow (1,0)$, $\Lambda \leftarrow (1,1)$, $\Psi \leftarrow (x)$;
**while** $N > 1$ **do**
  $\Psi \leftarrow \Psi \cup$ `AppRoot`$(F, N)$;
  $\sum_B f_B\Psi^B \leftarrow$ `Expand`$(F, \Psi)$;
  $\bar{H} \leftarrow$ `BoundaryPol`$(F, \Psi)$;
  **if** $\bar{H}$ *is not degenerated over* $\mathbb{L}$ **then return** *`False`*;
  $(q, m, P, N) \leftarrow$ `EdgeData`$(\bar{H})$;
  Update the lists $V, \Lambda$ thanks to formula (19);
  $\mathbb{L} \leftarrow \mathbb{L}_P$
**return** *`True`*

**Theorem 8.** *Algorithm* `Irreducible` *returns the correct answer.*

*Proof.* This follows from Theorem 5, 6 and 7, together with the correctness of `ARNP`. □

Let us illustrate this algorithm on two simple examples.

**Example 2.** Let $F(x,y) = (y^2 - x^3)^2 - x^7$. This example was suggested by Kuo who wondered if we could show that $F$ is reducible in $\overline{\mathbb{Q}}[[x]][y]$ without performing Newton-Puiseux type tranforms. Abhyankhar solved this challenge in [1] thanks to approximate roots. Let us show that we can prove further that $F$ is reducible in $\mathbb{Q}[[x]][y]$ without performing Newton-Puiseux type tranforms.

*Initialisation.* Start from $\psi_{-1} = x$, $N_0 = d = 4$, $V = (1,0)$ and $\mathcal{N} = (1,1)$.

*Step k=0.* The 4-th approximate root of $F$ is $\psi_0 = y$. So $H_0 = F$ and we deduce from (12) (see Exemple 1) that $\bar{H}_0 = (y^2 - x^3)^2$. Hence, $F$ is degenerated with edge data $(q_1, m_1, P_1, N_1) = (2, 3, Z_1 - 1, 2)$ and we update $V = (2,3,6)$ and $\Lambda = (1,1,2)$ thanks to (19), using here $z_1 = 1 \mod P_1$.

*Step k=1.* The 2-th approximate root of $F$ is $\psi_1 = y^2 - x^3$ and $F$ has $\Psi$-adic expansion $F = \psi_1^2 - \psi_{-1}^7$. We have $v_1(\psi_1^2) = 2v_{1,1} = 12$, $\lambda_1(\psi_1^2) = \lambda_{1,1}^2 = 4$ while $v_1(\psi_{-1}^7) = 7v_{-1,1} = 14$ and $\lambda_1(\psi_{-1}^7) = \lambda_{-1,1}^7 = 1$. We deduce from (12) that $\bar{H}_1 = y^2 - \frac{1}{4}x^2$. As the polynomial $Z_2^2 - \frac{1}{4}$ is reducible in $\mathbb{Q}_{P_1}[Z_2] = \mathbb{Q}[Z_2]$, we deduce that $F$ is reducible in $\mathbb{Q}[[x]][y]$.

**Example 3.** Consider $F = ((y^2 - x^3)^2 + 4x^8)^2 + x^{14}(y^2 - x^3)$ (we assume that we only know its expanded form at first).

*Initialisation.* We start with $\psi_{-1} = x$, $N_0 = d = 8$, $V = (1,0)$ and $\mathcal{N} = (1,1)$.

*Step k=0.* The 8-th approximate root of $F$ is $\psi_0 = y$. The monomials reaching the minimal values (11) in the $\Psi = (\psi_{-1}, \psi_0)$-adic expansion of $F$ are $\psi_0^8$ $-4\psi_{-1}^3\psi_0^6$, $6\psi_{-1}^6\psi_0^4$ ,$-4\psi_{-1}^9\psi_0^2$, $\psi_{-1}^{12}$ and we deduce from (12) that $\bar{H}_0 = (y^2 - x^3)^4$. Hence, $(q_1, m_1, P_1, N_1) = (2, 3, Z_1 - 1, 4)$ and we update $V = (2,3,6)$ and $\Lambda = (1,1,2)$ thanks to (19), using here $z_1 = 1 \mod P_1$.

*Step k=1.* The 4-th approximate root of $F$ is $\psi_1 = y^2 - x^3$ and we get the current $\Psi$-adic expansion $F = \psi_1^4 + 8\psi_{-1}^8\psi_1^2 + \psi_{-1}^{14}\psi_1 + 16\psi_{-1}^{16}$. The monomials reaching the minimal values (11) are $\psi_1^4$, $8\psi_{-1}^8\psi_1^2$, $16\psi_{-1}^{16}$ and we deduce from (12) that $\bar{H}_1 = (y^2 + x^4)^2$. Hence $(q_2, m_2, P_2, N_2) = (1, 2, Z_2^2 + 1, 2)$ and we update $V = (2,3,8,16)$ and $\Lambda = (1,1,2z_2,8z_2)$ thanks to (19), where $z_2 = Z_2 \mod P_2$ and using the Bézout relation $q_2 s_2 - m_2 t_2 = 1$ with $(s_2, t_2) = (1,0)$. Note that we know at this point that $F$ is reducible in $\overline{\mathbb{Q}}[[x]][y]$ since $P_2$ has two distinct roots in $\overline{\mathbb{Q}}$.

*Step k=2.* The 2-th approximate roots of $F$ is $\psi_2 = (y^2 - x^3)^2 + 4x^8$ and we get the current $\Psi$-adic expansion $F = \psi_2^2 + \psi_{-1}^{14}\psi_1$. The monomials reaching the minimal values (11) are $\psi_2^2$, $\psi_{-1}^{14}\psi_1$ and we deduce from (12) that $\bar{H}_2 = y^2 + (32z_2)^{-1}x$ (note that $z_2$ is invertible in $\mathbb{Q}_{P_2}$). Hence $\bar{H}_2$ is degenerated with edge data $(q_3, m_3, P_3, N_3) = (2, 1, Z_3 + (32z_2)^{-1}, 1)$. As $N_3 = 1$, we deduce that $F$ is irreducible in $\mathbb{Q}[[x]][y]$ ($g = 3$ here).

*Remark* 4. Note that for $k \geq 2$, we really need to consider the $\Psi$-adic expansion: the $(x, y, \psi_k)$-adic expansion is not enough to compute the next data. At step $k = 2$ in the previous example, the $\psi_2$-adic expansion of $F$ is $F = \psi_2^2 + a$ where $a = x^{14}y^2 - x^{17}$. We need to compute $v_2(a)$. Using the $\Psi$-adic expansion $a = \psi_{-1}^{14}\psi_1$, we find $v_2(a) =$

$14 \times 2 + 8 = 36$. Considering the $(x, y)$-adic expansion of $a$ would have led to the wrong value $v_2(x^{14}y^2) = v_2(x^{17}) = 34 < 36$.

## 5 Absolute irreducibility

We say that $F \in \mathbb{K}[[x]][y]$ is absolutely irreducible if it is irreducible in $\overline{\mathbb{K}}[[x]][y]$, that is if $\texttt{Irreducible}(F, \overline{\mathbb{K}})$ returns `True`. In particular, in this context, we always have $\ell_k = 1$. As already mentionned, Abhyankhar's absolute irreducibility test avoids any Newton-Puiseux type transforms or Hensel type liftings. In fact, it is even stronger as it does not even compute the boundary polynomials $\bar{H}_k$, but only their Newton polygon. Although we don't need this improvement from a complexity point of view (see Subsection 7.4), we show how to recover this result in our context for the sake of completness. We will use the following alternative characterizations of valuations and polygons:

**Lemma 5.** *Suppose that $H_0, \dots, H_{k-1}$ are degenerated.*

1. *Write $F = \sum c_i \psi_k^i$ the $\psi_k$-adic expansion of $F$. Then $v_k(F) = \min_i v_k(c_i\psi_k^i)$ and*

$$\mathcal{N}_k(F) := \mathcal{N}^-(\pi_k^*(F)) = Conv\left(\left(i, v_k(c_i\psi_k^i)\right) + (\mathbb{R}^+)^2,\ c_i \neq 0\right). \tag{24}$$

2. *Let $k \geq 1$ and $G \in \mathbb{K}[[x]][y]$ with $\psi_{k-1}$-adic expansion $G = \sum_i a_i \psi_{k-1}^i$. We have*

$$v_k(G) = \min_i \left(q_k v_{k-1}(a_i\psi_{k-1}^i) + im_k\right). \tag{25}$$

*Proof.* 1. Equality (24) is a direct consequence of Corollary 3 with Theorems 5 and 7. Also, from (23), $\pi_k^*(c_i\psi_k^i)$ has a term of lowest $x$-valuation of shape $ux^{v_k(a_i\,\psi_k^i)}\,y^i$ for some $u \in \mathbb{K}_k^\times$ and it follows that $v_k(F) = \min_i v_k(c_i\psi_k^i)$, as required.

2. By (23) applied to rank $k-1$, we get $\pi_{k-1}^*(a_i\psi_{k-1}^i) = x^{v_{k-1}(a_i\psi_{k-1}^i)}U_i(y + x^\alpha\tilde{U}_i)$, where $\alpha > m_k/q_k$, and $U_i, \tilde{U}_i$ are units. Suppose $m_k > 0$. Then $V_i = U_i(z_k^{s_k}x^{q_k}, x^{m_k}(y + z_k^{t_k} + c_k(x))$ is a unit such that $V_i(0, y) = U_i(0, 0) \in \mathbb{K}_k^*$ is constant and a straightforward computation shows that $\pi_k^*(a_i\psi_{k-1}^i) = x^{q_kv_{k-1}(a_i\psi_{k-1}^i)+im_k}P_i(y) + h.o.t$, where $P_i \in \mathbb{K}[y]$ has degree exactly $i$. Equality (25) follows. The case $m_k = 0$ may occur only when $k = 1$, $q_1 = 1$. In such a case, we have $\pi_1^*(G) = \sum_i a_i(x)(y + z_1 + c(x))^i$ with $v_x(c) > 0$ and the same conclusion holds. □

*Remark* 5. Point 2 in Lemma 5 shows that our valuations coincide with the extended valuations used in Montes algorithm over general local fields, see for instance [14, point (3) of Proposition 2.7].

Hence, we may take (24) and (25) as alternative recursive definitions of valuations and Newton polygons. This new point of view has the great advantage to be independent of the map $\pi_k$, hence of the Newton-Puiseux algorithm. In particular, it can be generalized at rank $k+1$ without assuming that $H_k$ is degenerated.

**Definition 4.** Suppose that $H_0, \ldots, H_{k-1}$ are degenerated and let $-m_{k+1}/q_{k+1}$ be the slope of the lowest edge of $H_k$. We still define the valuation $v_{k+1}$ and the Newton polygon $\mathcal{N}_{k+1}(F)$ by formulas (25) and (24) applied at rank $k+1$.

We obtain the following absolute irreducibility test which only depends on the geometry of the successive Newton polygons.

**Algorithm:** `AbhyankarTest`$(F)$
**Input:** $F \in \mathbb{K}[[x]][y]$ Weierstrass s.t. Char($\mathbb{K}$) does not divide $d = \deg(F)$.
**Output:** `True` if $F$ is irreducible in $\overline{\mathbb{K}}[[x]][y]$, `False` otherwise.

$N \leftarrow d$, $v = v_x$;
**while** $N > 1$ **do**
  $\psi \leftarrow$ `AppRoot`$(F, N)$;
  $\sum c_i \psi^i \leftarrow$ `Expand`$(F, \psi)$;
  Compute the current polygon $\mathcal{N}(F)$ with (24);
  **if** $(N, v(F)) \notin \mathcal{N}(F)$ *or* $\mathcal{N}(F)$ *is not straight or* $q = 1$ **then**
    **return** *False*
  $N \leftarrow N/q$;
  Update $v$ with (25);
**return** *True*;

**Proposition 5.** *Algorithm* `AbhyankarTest` *works as specified.*

*Proof.* Suppose that $F$ is not absolutely irreducible. Let us abusively still denote by $g$ be the first index $k$ such that $H_k$ is not degenerated over $\overline{\mathbb{K}}$ or $N_k = 1$: so both algorithms `AbhyankarTest`$(F)$ and `Irreducible`$(F, \overline{\mathbb{K}})$ compute the same data $\psi_0, \ldots, \psi_{g-1}$ and $(q_1, N_1), \ldots, (q_g, N_g)$. If $N_g = 1$, then $F$ is absolutely irreducible, and both algorithms return `True` as required. If $N_g > 1$, then `Irreducible`$(F, \overline{\mathbb{K}})$ returns `False`. Note that $\mathcal{N}(H_g)$ equals $\mathcal{N}_g(F) - (0, v_g(F))$ by definition of $\mathcal{N}_g$. As $H_g$ is Weierstrass of degree $N_g$, we have $(N_g, v_g(F)) \in \mathcal{N}_g(F)$ at this stage. If $\mathcal{N}_g(F)$ is not straight or $q_{g+1} = 1$, then so does $\mathcal{N}(H_g)$ and `AbhyankarTest`$(F)$ returns `False` as required. There remains to treat the case where $\mathcal{N}_g(F)$ is straight with $q_{g+1} > 1$ (still assuming $N_g > 1$ and $H_g$ not degenerated over $\overline{\mathbb{K}}$). In such a case, `AbhyankarTest`$(F)$ computes the next $N_{g+1}^{th}$ approximate roots $\psi_{g+1}$ of $F$ where $N_{g+1} = N_g/q_{g+1}$. We will show that $(N_{g+1}, v_{g+1}(F)) \notin \mathcal{N}_{g+1}(F)$ so that `AbhyankarTest` returns `False` at this step.

Let $F = \sum_{i=0}^{N_{g+1}} c_i \psi_{g+1}^i$ be the $\psi_{g+1}$-adic expansion of $F$. By hypothesis, we know that

$$\pi_g^*(F) = x^{v_g(F)}\, H_g\, U, \text{ with } U(0,0) \neq 0$$

where $\bar{H}_g = \prod_{Q(\zeta)=0}(y^{q_{g+1}} - \zeta x^{m_{g+1}})$, with $Q \in \mathbb{K}[Z]$ of degree $N_{g+1} := N_g/q_{g+1}$ having at least two distinct roots. In particular, $\bar{H}_g$ is not the $N_{g+1}$-power of a polynomial and it follows that $\pi_g^*(\psi_{g+1}^{N_{g+1}})$ and $\pi_g^*(F)$ can not have the same boundary polynomials. We deduce that there is at least one index $i < N_{g+1}$ such that $\mathcal{N}_g(c_i \psi_{g+1}^i)$ has a point on

or below $\mathcal{N}_g(F)$. Consider the $\psi_g$-adic expansions $c_i\psi_{g+1}^i = \sum_j a_j\psi_g^j$ and $F = \sum_j \alpha_j\psi_g^j$. Thanks to (24), there exists at least one index $j$ such that $(j, v_g(a_j\psi_g^j)) \in \mathcal{N}_g(c_i\psi_{g+1}^i)$. By (24), $\mathcal{N}_g(F)$ is the lower convex hull of $(j, v_g(\alpha_j\psi_g^j))$, which is by assumption straight of slope $-q_{g+1}/m_{g+1}$. It follows that

$$\min_j(q_{g+1}v_g(a_j\psi_g^j) + m_{g+1}j) \leq \min_j(q_{g+1}v_g(\alpha_j\psi_g^j) + m_{g+1}j).$$

Thanks to Definition 4, this implies $v_{g+1}(c_i\psi_{g+1}^i) \leq v_{g+1}(F)$ which in turns forces $(N_{g+1}, v_{g+1}(F)) \notin \mathcal{N}_{g+1}(F)$. □

*Remark* 6. At step $k+1$ of the algorithm, we know that $H_0, \ldots, H_{k-1}$ are degenerated over $\overline{\mathbb{K}}$. Hence the recursive definition of the map $v_{k+1}$ is equivalent to

$$v_{k+1}(G) = \min_{g_B \neq 0} (q_{k+1}\langle B, V\rangle + m_{k+1}b_k) \tag{26}$$

where $G$ has $(\psi_{-1}, \ldots, \psi_k)$-adic expansion $G = \sum g_B\Psi^B$ and $V = (v_{k,-1}, \ldots, v_{k,k})$. This is the approach we shall use in practice for valuations updates.

## 6 Pseudo-irreducibility

As mentionned in the introduction, performing too many irreducibility tests might be costly. We therefore relax the degeneracy condition by allowing square-freeness of the involved residual polynomial $P_1, \ldots, P_g$, and eventually check if $\mathbb{K}_g$ is a field. This leads to what we call a pseudo-irreducibility test. Despite of its complexity interest, we will show in Section 8 that this modification allows to characterise balanced polynomials, thus proving Theorem 3.

If we allow the $P_k$'s to be square-free, the fields $\mathbb{K}_k$'s become ring extensions of $\mathbb{K}$ isomorphic to a direct product of fields and we have to take care of zero divisors. Let $\mathbb{A} = \mathbb{L}_0 \oplus \cdots \oplus \mathbb{L}_r$ be a direct product of perfect fields. We say that a (possibly multivariate) polynomial $H$ defined over $\mathbb{A}$ is *square-free* if all its projections under the natural morphisms $\mathbb{A} \to \mathbb{L}_i$ are square-free (in the usual sense over a field). If the polynomial is univariate and monic, this exactly means that its discriminant is not a zero divisor in $\mathbb{A}$.

In the following, we call the lower boundary polynomial of $F$ the restriction of $F$ to the lower edge of its Newton polygon, that we abusively still denote by $\bar{F}$.

**Definition 5.** We say that a monic polynomial $F \in \mathbb{A}[[x]][y]$ is pseudo-degenerated if its *lower boundary polynomial* is the power of a *square-free* quasi-homogeneous polynomial of shape

$$\bar{F} = \left(P\left(\frac{y^q}{x^m}\right)x^{m\deg(P)}\right)^N, \tag{27}$$

with $P \in \mathbb{A}[Z]$ square-free and $P(0) \in \mathbb{A}^\times$ if $q > 1$.

We still call $P$ the *residual polynomial* of $F$ and $(q, m, N, P)$ the *edge data* of $F$ (with convention $(q, m) = (1, 0)$ if the Newton polygon is reduced to a point).

*Remark* 7. If $q > 1$, then $\mathcal{N}(F)$ is straight, and Definition 5 is the analoguous of Definition 3 of degenerated polynomials (square-freeness replacing irreducibility). However, in contrast to degenerated polynomials, we authorize here $P(0) = 0$ (or more generally a zero-divisor) if $q = 1$. In such a case, $\mathcal{N}(F)$ may have several edges. For instance, $F = (y-x)(y-x^2)$ has two edges but is pseudo-degenerated (we get as $\bar{F} = y^2 - xy$ and $P = Z^2 - Z$). A more complicated example is $F = (y^2-x^2)^2(y-x^2)(y-x^3)+x^{10}$ which has three edges but is pseudo-degenerated (we get $\bar{F} = (y^3 - x^2y)^2$ and $P = Z^3 - Z$). Although having several edges implies reducibility, this definition will make sense when considering balanced polynomials (Remark 5 and Example 6).

**Definition 6.** We call `Pseudo-ARNP` and `Pseudo-Irreducible` the new algorithms obtained when replacing degenerated tests by pseudo-degenerated tests respectively in algorithms `ARNP` and `Irreducible`.

*Remark* 8. Note that any assertions in previous sections of type $a \neq 0$ still has to be read as such ($a$ is non zero), while any assertion of type $a \in \mathbb{K}_k^\times$ still has to be read as such (meaning now $a$ is not a zero divisor). In particular, given $a \in \mathbb{A}[[x]]$, $v_x(a)$ is computed via the smallest monomial with *non-zero* coefficient (and not "non zero divisor"). This remark also applies to formula (11).

**Proposition 6.** *Algorithms* `Pseudo-Irreducible` *and* `Pseudo-ARNP` *are well-defined. Moreover, they give the same output and compute the same edges data. We say that a monic polynomial $F \in \mathbb{K}[[x]][y]$ is pseudo-irreducible if this output is* `True`*.*

*Proof.* We need to show that both algorithms are well-defined and that all results of Section 3 and Section 4 still hold when considering pseudo-degeneracy. We have to take care of the fact that $z_k$ might be now a zero divisor. It is however sufficient to prove that $\lambda_{k,k} \in \mathbb{K}_k^\times$. Indeed, then the computation of the Weierstrass polynomial $H_k$ is possible, the statement of Theorem 6 is correct, and so is the proof of Proposition 1. This also implies that the functorial properties $v_k(a\phi_k^j) = v_k(a) + jv_k(\phi_k)$ and $\lambda_k(a\phi_k^j) = \lambda_k(a)\lambda_k(\phi_k)^j$ hold for all $a \in \mathbb{K}[[x]][y]$. As $v_k$ still obeys to the triangular inequality, all these implications mean that all results of Sections 4 hold too.

We now prove that $\lambda_{k,k} \in \mathbb{K}_k^\times$ by induction. The claim is obvious when $k = 0$. Now, let $k > 0$ and assume that $\lambda_{i,i} \in \mathbb{K}_i^\times$ for $i < k$. If $z_k \in \mathbb{K}_k^\times$, then we are done. Otherwise, we must have $q_k = 1$ and $t_k = 0$ so that the definition of $\phi_k$ makes sense by (4), (5) and (7) (we use $\mu_k \in \mathbb{K}_k^\times$) and Lemma 1 and 2 hold up to rank $k$. The proof of Proposition 1 remains valid (we use $n = \lfloor wt_k/q_k \rfloor = 0$ in that case) and the proof of Proposition 2 remains valid too (we use $P_k'(z_k) \in \mathbb{K}_k^\times$ since by assumption $P_k$ is square-free over a product of perfect fields). This implies $\lambda_{k,k} \in \mathbb{K}_k^\times$ from Remark 2. Finally, note that some splittings might appear during the algorithm (see Example 4), not changing the output of the algorithm (see [25, Section 5] for details). □

*Remark* 9. Note that $\lambda_{k,i}$ might be a zero divisor when $i < k$. For instance, the polynomial $F = (y^3 - x^2y)^N + \cdots$ is pseudo-degenerated with residual polynomial $P_1 = Z^3 - Z$, so that $z_1 := Z \mod P_1 \in \mathbb{K}_1$ is not invertible. We compute $\pi_1^*(\phi_0) = \pi_1^*(y) = x(y + z_1)$ from which it follows that $\lambda_{1,0} = z_1$ is a zero-divisor. The key point is that the families $\Lambda^B, B \in \mathcal{B}(w, j)$ remain free over $\mathbb{K}$.

*Remark* 10. The polynomials $\phi_k$ are no longer irreducible (nor the $\psi_k$'s) when considering algorithm `Pseudo-ARNP`, but only pseudo-irreducible. However, they still obey to equalities $\deg(\phi_k) = e_k f_k$ and $\pi_k^*(\phi_k) = x^{v_{k,k}} U_{k,k}(x, y)\, y$, with $U_k(0, 0) = \lambda_{k,k} \in \mathbb{K}_k^\times$.

**Corollary 4.** *A square-free monic polynomial $F \in \mathbb{K}[[x]][y]$ is irreducible over $\mathbb{K}$ if and only if it is pseudo-irreducible and $\mathbb{K}_g$ is a field.*

*Proof.* This follows immediately from Definition 5 and Proposition 6. □

We will check irreducibility using Corollary 4, thus avoiding to perform too many univariate irreducibility tests. Besides this advantage, testing pseudo-degeneracy will allow us to characterize a larger class than irreducible polynomials in $\mathbb{K}[[x]][y]$, namely the class of balanced polynomials. In particular, if $F$ is pseudo-irreducible, we can compute easily the ramification index and the residual degrees of all its irreducible factors in $\mathbb{K}[[X]][Y]$ (see Example 4), and the characteristic exponents and pairwise intersection multiplicities of all its absolutely irreducible factors (see Examples 6, 7, 8).

# 7 Complexity. Proof of Theorems 1 and 2

## 7.1 Complexity model

We use the algebraic RAM model of Kaltofen [15, Section 2], counting only the number of arithmetic operations in our base field $\mathbb{K}$. Most subroutines are deterministic; for them, we consider the worst case. However, computation of primitive elements in residue fields uses a probabilistic algorithm of Las Vegas type, and we consider then the average running time. We denote by $\mathsf{M}(d)$ the number of arithmetic operations for multiplying two polynomials of degree $d$. We use fast multiplication, so that $\mathsf{M}(d) \in \mathcal{O}^\sim(d)$ and $d'\mathsf{M}(d) \leq \mathsf{M}(d'd)$, see [11, Section 8.3]. We denote by $\mathsf{I}(d)$ the number of arithmetic operations for testing irreducibility of a degree $d$ polynomial over $\mathbb{K}$. We assume that $d \in \mathsf{I}(d)$ and $d'\mathsf{I}(d) \leq I(dd')$, which is consistent with the known bounds for $\mathsf{I}(d)$ (see e.g. [11, Theorem 14.37] for $\mathbb{K} = \mathbb{F}_q$ and [11, Theorem 15.5] for $\mathbb{K} = \mathbb{Q}$). We use the classical notations $\mathcal{O}()$ and $\mathcal{O}^\sim()$ that respectively hide constant and logarithmic factors ([11, Chapter 25, Section 7]). In particular, we will abusively denote $\mathcal{O}^\sim(\delta)$ a complexity result as $\delta \log(d)$ (which is bounded by $\delta \log(\delta)$ only when $F$ is Weierstrass).

**Primitive representation of residue rings.** The $\mathbb{K}$-algebra $\mathbb{K}_k$ is given inductively as a tower extension of $\mathbb{K}$ defined by the radical triangular ideal $(P_1(Z_1), \ldots, P_k(Z_1, \ldots, Z_k))$. It turns out that such a representation does not allow to reduce a basic operation in $\mathbb{K}_k$

to $\mathcal{O}^{\sim}(f_k)$ operations over $\mathbb{K}$ (see [25] for details). To solve this problem, we compute a primitive representation of $\mathbb{K}_k$, introducing the notation $\mathbb{K}_Q := \mathbb{K}[T]/(Q(T))$.

**Proposition 7.** *Let $Q \in \mathbb{K}[T]$ and $P \in \mathbb{K}_Q[Z]$ square-free, and assume that $\mathbb{K}$ has at least $(\deg_T(Q)\deg_Z(P))^2$ elements. There exists a Las Vegas algorithm* `Primitive` *that returns $(Q_1, \tau)$ with $Q_1 \in \mathbb{K}[W]$ square-free and $\tau : \mathbb{K}[T,Z]/(Q,P) \to \mathbb{K}[W]/(Q_1)$ an isomorphism. It takes an expected $\mathcal{O}((\deg_T(Q)\deg_Z(P))^{(\omega+1)/2})$ operations over $\mathbb{K}$. Given $\alpha \in \mathbb{K}[T,Z]/(Q,P)$, one can compute $\tau(\alpha)$ in less than $\mathcal{O}^{\sim}(\deg_T(Q)^2\deg_Z(P))$.*

*Proof.* Use [25, Proposition 15] with $I = (Z_1, Q(Z_2))$ (see notations therein). □

In the following, we use that an operation in $\mathbb{K}_k$ costs $\mathcal{O}^{\sim}(f_k)$ operations in $\mathbb{K}$.

*Remark* 11. Another way to deal with tower extensions would be the recent preprint [29]. This would make all algorithms deterministic, with a cost $\mathcal{O}(\delta^{1+o(1)})$ instead of $\mathcal{O}^{\sim}(\delta)$. Note also [30] for dynamic evaluation.

## 7.2 Truncation bounds

In order to estimate the complexity in terms of arithmetic operations in $\mathbb{K}$, we will compute approximate roots and $\Psi$-adic expansions modulo a suitable truncation bound for the powers of $\psi_{-1} = x$. We show here that the required sharp precision is the same than the one obtained in [25, Section 3] for the Newton-Puiseux type algorithm. Note also [2, Theorem 2.3, page 144] that provides similar results in the context of irreducibility test. In the following, when we say that we truncate a polynomial with precision $\tau \in \mathbb{Q}$, we mean that we keep only powers of $X$ less or equal than $\tau$.

The successive polynomials generated by `Pseudo-ARNP`$(F)$ are still denoted $H_0, \dots, H_g$, and we let $(q_{g+1}, m_{g+1})$ stand for the slope of the lower edge of $H_g$ ($(q_{g+1}, m_{g+1}) := (1,0)$ if $N_g = 1$). As $\deg(H_k) = N_k$ and $\mathcal{N}(H_k)$ has a lower edge of slope $-m_{k+1}/q_{k+1}$, the computation of the lower boundary polynomial $\bar{H}_k$ only depends on $H_k$ truncated with precision $N_k m_{k+1}/q_{k+1}$. Combined with (6), and using $v_x(\pi_k^*(x)) = e_k$, we deduce that the $k^{th}$-edge data only depends on $F$ truncated with precision

$$\eta_k := \frac{v_k(F)}{e_k} + N_k \frac{m_{k+1}}{e_{k+1}}. \tag{28}$$

Denoting $\eta(F) := \max_{0 \le k \le g}(\eta_k)$, we deduce that running `Pseudo-Irreducible` modulo $x^{\eta(F)+1}$ return the correct answer, this bound being sharp by construction.

**Lemma 6.** *We have $\eta_k = \eta_{k-1} + \frac{N_k m_{k+1}}{e_{k+1}}$. In particular, $\eta(F) = \eta_g = \sum_{k=1}^{g+1} \frac{N_{k-1} m_k}{e_k}$.*

*Proof.* As $v_k(F) = N_k\, v_{k,k}$ from Lemma 3, we get

$$\eta_k = \frac{N_k v_{k,k}}{e_k} + \frac{N_k m_{k+1}}{e_{k+1}} \tag{29}$$

for all $0 \leq k \leq g$. If $k = 0$, we have $\eta_0 = N_0\, m_1/q_1$ as required, as $v_{0,0} = 0$. Suppose $k \geq 1$. Applying (29) at rank $k-1$, we obtain for $k = 1, \ldots, g$ the relations

$$\eta_{k-1} = \frac{N_{k-1} v_{k,k-1}}{e_k} = \frac{N_k v_{k,k}}{e_k}, \tag{30}$$

first equality using Point 1 of Lemma 2 ($v_{k,k-1} = q_k v_{k-1,k-1} + m_k$) and second equality using $N_{k-1} = q_k \ell_k N_k$ and equality $v_{k,k} = q_k \ell_k v_{k,k-1}$ of Theorem 2. Hence (29) and (30) give $\eta_k = \eta_{k-1} + \frac{N_k m_{k+1}}{e_{k+1}}$ as required. The formula for $\eta(F)$ follows straightforwardly. □

*Remark* 12. We have the formula $\eta_k = \frac{v_x(\pi_k^* F(x,0))}{e_{k+1}} = \frac{(F,\phi_k)_0}{d_k}$ for $k \leq g-1$, the first equality following again from (6) and the second equality from Corollary 1. Since $(F,\phi_k)_0 = (F,\psi_k)_0$, we deduce in particular that the sequence of integers $(N_0, d_0\eta_0, \ldots, d_{g-1}\eta_{g-1})$ form a minimal set of generators of the semi-group of $F$ when $F$ is irreducible in $\overline{\mathbb{K}}[[x]][y]$ ; see e.g. [20, Proposition 4.2 and Theorem 5.1].

**Proposition 8.** *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree $d$, with discriminant valuation $\delta$. Then $\eta(F) \leq \frac{2\delta}{d}$. If moreover $F$ is pseudo-irreducible, then $\eta(F) \geq \delta/d$.*

*Proof.* It follows from Lemma 6 that $\eta(F)$ is smaller or equal than the quantity "$N_i$" defined in [25, Subsection 3.3] (take care of notations, these $N_i$ are not the same as those defined here), with equality if $F$ is pseudo-irreducible. From [25, Corollary 4], we deduce $\eta(F) \leq 2v_i$ for $i = 1, \ldots, d$, where $v_i := v_x(\partial_y F(y_i))$, $y_i$ denoting the roots of $F$. As $\delta = \sum v_i$, we have $\min v_i \leq \delta/d$ and the upper bound for $\eta(F)$ follows. If $F$ is pseudo-irreducible, then we have also $v_i \leq \eta(F) = N_i$ by [25, Corollary 4]. As all $v_i$'s are equal in that case, the lower bound follows too. □

*Remark* 13 (*Dealing with the precision*). As $\delta$ is not given, we do not have an *a piori* bound for the precision $\eta(F)$. To deal with this problem, we start from some low precision, and double it each time the computed lower edge of the Newton polygon is not "guaranted" [25, Definition 8 and Figure 1.b], which can be checked thanks to Lemma 6 (lines 6 and 7 of algorithm `Pseudo-Irreducible` below). We could use also relaxed computations [28]. In both solutions, this only multiply the complexity result by at most a logarithm factor.

## 7.3 Main subroutines

### Computing approximate roots and Ψ-adic expansion.

**Proposition 9.** *There exists an algorithm `AppRoot` which given $F \in \mathbb{A}[y]$ a degree $d$ monic polynomial defined over a ring of characteristic not dividing $d$ and given $N$ which divides $d$, returns the $N^{th}$ approximate root of $F$ with $\mathsf{M}(d)$ operations over $\mathbb{A}$.*

*Proof.* $\psi$ can be computed as follows. Let $G = y^d F(1/y)$ be the reciprocal polynomial of $F$. So $G(0) = 1$ and there exists a unique series $S \in \mathbb{A}[[y]]$ such that $S(0) = 1$ and

$G = S^N$. Then $\psi$ is the reciprocal polynomial of the truncated series $\lceil S \rceil^{\frac{d}{N}}$ (see e.g. [20, Proposition 3.4]). The serie $S$ is solution of the equation $Z^N - G = 0$ in $\mathbb{A}[[y]][Z]$ and can be computed up to an arbitrary precision $\sigma$ with $\mathsf{M}(N\sigma)$ operations by quadratic Newton iteration [11, Theorem 9.25], hence $\mathsf{M}(d)$ operations with $\sigma = d/N$. □

**Proposition 10.** *There exists an algorithm* `Expand` *which, given $F \in \mathbb{A}[y]$ of degree $d$ and $\Psi = (\psi_0, \dots, \psi_k)$ a collection of monic polynomials $\psi_i \in \mathbb{A}[y]$ of strictly increazing degrees $d_0 < \cdots < d_k \leq d$ returns the reduced $\Psi$-adic expansion of $F$ within $\mathcal{O}((k+1)\mathsf{M}(d)\log(d))$ arithmetic operations over $\mathbb{A}$.*

*Proof.* The $\psi_k$-adic expansion of $F = \sum a_i \psi_k^i$ requires $\mathcal{O}(\mathsf{M}(d)\log(d))$ operations by [11, Theorem 9.15]. If $k > 0$, we recursively compute the $(\psi_0, \dots, \phi_{k-1})$-adic expansion of $a_i$ in $\mathcal{O}(k\mathsf{M}(\deg a_i)\log(\deg a_i))$ operations. Since $\deg(a_i) < d_k$, summing over all $i = 0, \dots, \lfloor d/d_k \rfloor$ gives $\mathcal{O}(k\mathsf{M}(d)\log(d))$ operations. □

**Computing boundary polynomials.**

**Proposition 11.** *Given $F$ and $\Psi = (\psi_{-1}, \dots, \psi_k)$ modulo $x^{\eta(F)+1}$, $V = (v_{k,-1}, \dots, v_{k,k})$ and $\Lambda = (\lambda_{k,-1}, \dots, \lambda_{k,k})$, there exists an algorithm* `BoundaryPol` *that computes the lower boundary polynomial $\bar{H}_k \in \mathbb{K}_k[x, y]$ within $\mathcal{O}^{\sim}(\delta + f_k^2)$ operations over $\mathbb{K}$.*

*Proof.* First compute the $\Psi$-adic expansion $F = \sum f_B \Psi^B$ modulo $x^{\eta+1}$, with $\eta := \eta(F)$. As $\eta \leq 2\delta/d$, this is $\mathcal{O}^{\sim}(\delta)$ by Proposition 10 applied with $\mathbb{A} = \mathbb{K}[x]/(x^{\eta+1})$. The computation of the lower edge of $\bar{H}_k$ is done with Theorem 6 and take no arithmetic operations (this takes $\mathcal{O}^{\sim}(\delta)$ bit operations as $\langle B, V \rangle \in \mathcal{O}(\delta)$ and there are at most $e_k f_k N_k \eta \leq 2\delta$ such scalar products to compute). It remains to compute the coefficient of each monomial $x^{w_i} y^i$ of $\bar{H}_k$, which is (Theorem 6):

$$c_{k,i} := \sum_{B \in \mathcal{B}(i, w_i + v_k(F))} f_B \Lambda^{B - B_0}.$$

Note first that computing $\Lambda^{B_0} = \lambda_{k,k}^{N_k}$ takes $\mathcal{O}(\log(d))$ operations over $\mathbb{K}_k$ via fast exponentiation. Then, there are at most $f_k$ monomials $\Lambda^B$ to compute from Proposition 1. Each of them can be computed in $\mathcal{O}(k\,\log(\delta))$ operations in $\mathbb{K}_k$ via fast exponentiation on each $\lambda_{k,i}$ (we have $w_i \leq v_x(H_k(x,0)) = N_k m_{k+1}/q_{k+1}$, thus $w_i + v_k(F) \leq e_k \eta_k \leq 2\delta$ from (28) and Proposition 8). This concludes. □

**Testing pseudo-degeneracy and computing edge data.** There remains to test the pseudo-degeneracy of the boundary polynomials.

**Proposition 12.** *Given $Q \in \mathbb{K}[Z]$ square-free and $\bar{H} \in \mathbb{K}_Q[x, y]$ monic in $y$ and quasi-homogeneous, there exists an algorithm* `Pseudo-Degenerated` *that returns* `False` *if $\bar{H}$ is not pseudo-degenerated, and the edge data $(q, m, P, N)$ of $\bar{H}$ otherwise. It takes at most $\mathcal{O}^{\sim}(\deg_Z(Q)\deg(H))$ operations over $\mathbb{K}$.*

*Proof.* As $\bar{H}$ is quasi-homogeneous, we have $\bar{H} = y^r P_0(y^q/x^m)x^{m\deg(P_0)}$ for some coprime integers $q, m \in \mathbb{N}$, $0 \leq r < q$ and some $P_0 \in \mathbb{K}_Q[T]$ which can be computed with the aimed complexityIf $r \neq 0$, then $H$ is not pseudo-degenerated. Otherwise, there remains to check if $P_0 = P^N$ for some $N \in \mathbb{N}$ and $P \in \mathbb{K}_Q[T]$ square-free (i.e $(Q, P)$ radical ideal in $\mathbb{K}[Z, T]$), and that $P(0) \notin \mathbb{K}_Q^\times$ when $q > 1$. The first task is a special case of [25, Proposition 14] and fits in the aimed bound. Second one is just a gcd computation, bounded by $\mathcal{O}^\sim(\deg_Z(Q))$. □

*Remark* 14. We might discover that $Q$ factors and perform some splittings of the ring $\mathbb{K}_Q$ in course of the square-free test (see Example 4). In such a case, we do not necessarily return `False`: although this is the natural option when testing irreducibility, we don't want to stop the algorithm if $Q$ factors when testing balancedness (see Section 8).

### 7.4 The main algorithm. Proofs of Theorems 1, 2 and 4

**Algorithm:** `Pseudo-Irreducible`$(F, \eta = 1)$

**Input:** $F \in \mathbb{K}[[x]][y]$ monic of degree $d$ not divisible by the characteristic of $\mathbb{K}$

**Output:** `False` if $F$ is not pseudo-irreducible, and $(\text{Data}, Q)$ otherwise, with Data the edges data of $F$ and $\mathbb{K}_g = \mathbb{K}_Q$.

1 $F \leftarrow F \mod x^\eta$ ; `// All computations modulo` $x^\eta$
2 $N \leftarrow d$, $V \leftarrow [1, 0]$, $\Lambda \leftarrow [1, 1]$, $\Psi \leftarrow [x]$, $Q \leftarrow Z$, $(e, \eta') \leftarrow (1, 0)$, Data $\leftarrow [\,]$;
3 **while** $N > 1$ **do**
4 $\quad \Psi \leftarrow \Psi \cup$ `AppRoot`$(F, N)$;
5 $\quad \bar{H} \leftarrow$ `BoundaryPol`$(F, \Psi, V, \lambda)$ ; `//` $\bar{H} \in \mathbb{K}_Q[x, y]$
6 $\quad e \leftarrow q\,e$ ; $\eta' \leftarrow \eta' + \frac{N\,m}{e}$ ; `//` $(q, m)$ `lower edge of` $\bar{H}$
7 $\quad$ **if** $\eta \leq \eta'$ **then return** `Pseudo-Irreducible`$(F, 2\eta)$;
8 $\quad (Bool, (q, m, P, N)) \leftarrow$ `Pseudo-Degenerated`$(\bar{H}, Q)$ ;
9 $\quad$ **if** $Bool =$ `False` **then return** `False`;
10 $\quad$ Data $\leftarrow$ Data $\cup\, (q, m, P, N)$;
11 $\quad$ Update the lists $V, \Lambda$ thanks to formula (19);
12 $\quad (Q, \tau) \leftarrow$ `Primitive`$(Q, P)$;
13 $\quad \Lambda \leftarrow \tau(\Lambda)$;
14 **return** $(\text{Data}, Q)$;

**Proposition 13.** *Running* `Pseudo-Irreducible`$(F)$ *returns the correct output. If $F$ is Weierstrass, it takes at most $\mathcal{O}^\sim(\delta)$ operations over $\mathbb{K}$. If $F$ is monic, it takes $\mathcal{O}^\sim(\delta + d)$ operations, assuming a slight change of line 12 and a bivariate representation $\mathbb{K}_g = \mathbb{K}_{P_1,Q}$ (see the proof below).*

*Proof.* The polynomial $\bar{H}$ at line 8 is the correct lower boundary polynomial thanks to Lemma 6 (see also Remark 13). Then correctness follows from Theorem 8 and 9, together with Proposition 8. As $q_k \ell_k \geq 2$, we have $g \leq \log_2(d)$, while recursive calls of line 7 multiplies the complexity by at most a logarithm too. Considering one iteration, lines 4,

5, 8, 12 and 13 cost respectively $\mathcal{O}(\delta)$, $\mathcal{O}(\delta + f_k^2)$, $\mathcal{O}(f_k N_k) \subset \mathcal{O}(d)$, $\mathcal{O}(f_k^{(\omega+1)/2})$ and $\mathcal{O}(f_k)$ from respectively Propositions 9 (used with precision $\eta(F) \leq 2\,\delta/d$), 11, 12, 7 and 7 once again. Summing up, we get a total cost $\mathcal{O}(\delta + d + f^2)$. Lemma 6 gives $\eta(F) \geq dm_1/q_1$. If $F$ is Weierstrass, we have $m_1 > 0$. Hence $\eta(F) \geq d/q_1 \geq f$ from which it follows that $df \leq 2\delta$. Therefore, both $d$ and $f^2 \leq fd$ belong to $\mathcal{O}(\delta)$, proving Proposition 13 for Weierstrass polynomials. If $F$ is monic and not Weierstrass, then $m_1 = 0$ and the inequality $df \leq 2\delta$ doesn't hold anymore. We thus modify the algorithm as follows: we do not compute primitive elements of $\mathbb{K}_k$ over the field $\mathbb{K}$ but only over the next residue ring $\mathbb{K}_1 = \mathbb{K}_{P_1}$. We thus get a representation $\mathbb{K}_k = \mathbb{K}[Z_1, Z_2]/(P_1(Z_1), Q_k(Z_1, Z_2))$ for all $k \geq 2$, with $Q_k \in \mathbb{K}_1[Z_2]$ square-free of degree $f_k/\ell_1$. Given $P_{k+1}$, we compute then $Q_{k+1}$ such that $(P_1, Q_{k+1}) = (P_1, Q_k, P_k)$, thus dealing with at most trivariate triangular sets. Propositions 7 and 12 need to be adapted slightly: the base field $\mathbb{K}$ has to be replaced by the ring $\mathbb{K}_1 = \mathbb{K}_{P_1}$. This is possible thanks to [25, Propositions 14 and 15], computing now $Q_k$ with smaller complexity $\mathcal{O}(d_{P_1}(d_{Q_{k-1}} d_{P_k})^{(\omega+1)/2}) \subset \mathcal{O}(\ell_1(f_k/\ell_1)^{(\omega+1)/2})$ and still checking pseudo-degeneracy of $\bar{H}_k$ with $\mathcal{O}(d_{P_1} d_{Q_k} N_k) = \mathcal{O}(d)$. As $m_2 > 0$, Lemma 6 gives $\eta(F) \geq N_1 m_2/q_2 = d/\ell_1 q_1 q_2 \geq f_k/\ell_1$ from which it follows that $\ell_1(f_k/\ell_1)^2 = \ell_1 f_k^2 \leq 2 f_k \eta(F) \leq 2\delta$. The all complexity of this slightly modified algorithm becomes $\mathcal{O}(\delta + d)$, as required. □

**Proof of Theorem 1.** If $F$ is monic, then it is irreducible in $\mathbb{K}[[x]][y]$ if and only if it is pseudo-irreducible and $\mathbb{K}_g$ is a field (Corollary 4). If $F$ is Weierstrass, we have $\mathbb{K}_g = \mathbb{K}[Z]/(Q(Z))$ and we check if $\mathbb{K}_g$ is a field with a univariate irreducibility test in $\mathbb{K}[Z]$ of degree $\deg(Q) = f \leq d$ (cost $\mathsf{I}(d)$). If $F$ is monic but not Weierstrass, we have $\mathbb{K}_g = \mathbb{K}_{P_1}[Z]/(Q(Z))$ and $\mathbb{K}_g$ is a field if and only if $P_1$ and $Q$ are irreducible. This cost $\mathsf{I}(\ell_1) \subset \mathsf{I}(d)$ operations in $\mathbb{K}$ for $P_1$ and $\mathsf{I}(f/\ell_1)$ operations in $\mathbb{K}_1$ for $Q$ (assuming $P_1$ irreducible), that is $\mathcal{O}(\mathsf{I}(d))$ operations over $\mathbb{K}$ (use assumption $d\mathsf{I}(n) \leq \mathsf{I}(dn)$). If $F$ is not monic and its leading coefficient has valuation 0, we simply invert it. Otherwise, either its Newton polygon has more than one slope and $F$ is reducible, either $F(0)$ has valuation 0 and we can run the algorithm on the reciprocal polynomial of $F$. We are thus done from Proposition 13. □

**Proof of Theorem 2.** The polynomial $F$ is absolutely irreducible if and only if it is pseudo-irreducible and $f_g = 1$. We thus apply algorithm `Pseudo-Irreducible`, except that we return `False` if we find out that $\ell_k > 1$. We thus have $\mathbb{K}_k = \mathbb{K}$ for all $k$, and we need not to deal with the Las-Vegas subroutine `Primitive`, nor with univariate irreducibility tests. We obtain a deterministic algorithm running with $\mathcal{O}(\delta + d)$ operations over $\mathbb{K}$, which is $\mathcal{O}(\delta)$ is $F$ is Weierstrass (or more generally if $F(0, y)$ has a unique root: in such a case, we have $\ell_1 = 1$ which implies $q_1 > 1$ and $m_1 > 0$ so that the inequality $f_g\, d = d \leq 2\delta$ holds). Note that the non-monic case is handled in the same way than in the proof of Theorem 1. Also, we could have used algorithm `AbhyankarTest` with suitable precisions for the same cost. □

**Proof of Theorem 4.** If the input $F \in \mathbb{K}[x,y]$ is monic in $y$ with partial degrees $n := \deg_x(F)$ and $d = \deg_y(F)$, we run algorithm `Pseudo-Irreducible` with parameters $F$ and $4\,n$, except that we return `False` whenever the Newton polygon test of line 7 fails. If $F$ is square-free, we have the well known inequality $\delta \leq 2nd$ so that $\eta(F) \leq 4n$: the algorithm will return the correct answer with at most $\mathcal{O}(nd)$ operations over $\mathbb{K}$ as required, and so without performing recursive calls of line 7 (see Remark 13 once again). If $F$ is not square-free, then $\bar{H}_k$ is never square-free. Hence, we will never reach the case $N_k = 1$, and either the pseudo-degenarcy test of line 8 or the Newton polygon test of line 7 will fail at some point during the algorithm, in which case we return `False` within $\mathcal{O}(nd)$ as required. If $F$ is not monic, the result is similar, applying the same strategy as in the proof of Theorems 1 and 2. □

**Example 4.** Let us illustrate algorithm `Pseudo-Irreducible` on a simple example. Consider $F = (Y^4 - X^2)^4 + Y^6X^{11} - Y^4X^{12} - Y^2X^{13} + X^{14} + X^{16} \in \mathbb{Q}[X,Y]$.

*Initialisation.* We have $N_0 = d = 16$, and we let $\psi_{-1} = X$, $V = (1,0)$ and $\lambda = (1,1)$.

*Step* 0. The $16^{th}$-approximate roots of $F$ is $\psi_0 = Y$ and we find $\bar{H}_0 = (Y^4 - X^2)^4$, meaning that $H_0$ is pseudo-degenerated with edge data $(q_1, m_1, P_1, N_1) = (2, 1, Z_1^2 - 1, 4)$. Accordingly to (19), we update $V = (2,1,4)$ and $\lambda = (z_1, z_1, 4z_1)$, with $z_1 = Z_1 \mod P_1$ (i.e. $z_1^2 = 1$). Note that $Z_1$ is coprime to $P_1$ so that $\lambda_{1,1} = 4\,z_1^3 = 4\,z_1$ is invertible in $\mathbb{Q}_1$ as predicted by the proof of Proposition 6.

*Step* 1. As $N_1 = 4$, we compute the $4^{th}$-approximate root of $F$, getting $\psi_1 = Y^4 - X^2$. $F$ has $\Psi = (\psi_{-1}, \psi_0, \psi_1)$-adic expansion $F = \psi_1^4 + \psi_{-1}^{11}\psi_0^2\psi_1 - \psi_{-1}^{12}\psi_1 + \psi_{-1}^{16}$. All involved monomials reach the minimal values (11), and we deduce from (12) and equality $z_1^2 = 1$ that $\bar{H}_1 = Y^4 + \frac{(z_1-1)}{(4z_1)^3}X^{12}Y + \frac{1}{(4z_1)^4}X^{16}$. Here, $\bar{H}_1$ is quasi-homogeneous with slope $(q_2, m_2) = (1,4)$. As $4\,z_1$ is a unit of $\mathbb{Q}_1$, $H_1$ is pseudo-degenerated if and only if the univariate polynomial $Q(Z_2) = Z_2^4 + (z_1 - 1)Z_2 + 1$ is the power of a square-free polynomial $P_2$ in $\mathbb{Q}_1[Z_2]$. To check this, we apply the euclidean algorithm to compute the gcd between $Q$ and its derivative $Q'$. The first euclidean division gives $Q = \frac{Z_2}{4}\,Q' + R$ with $R = \frac{3}{4}\,(z_1 - 1)\,Z_2 + 1$. As $Z_1 - 1$ divides $P_1$, the leading coefficient of the remainder $R$ is a zero divisor in $\mathbb{Q}_1$. Hence, performing the next euclidean division of $Q'$ by $R$ requires to split $Q$ accordingly to the decomposition of the current residue ring $\mathbb{Q}_1 = \mathbb{Q}_{1,1} \oplus \mathbb{Q}_{1,2}$ induced by the factorization $P_1 = (Z_1 - 1)(Z_1 + 1)$ discovered so far. Then we continue the euclidean algorithm in each fields summands. We find here that both reductions $Q_1 \in \mathbb{Q}_{1,1}[Z_2]$ and $Q_2 \in \mathbb{Q}_{1,2}[Z_2]$ of $Q$ are square-free, from which it follows by definition that $Q$ is square-free in $\mathbb{Q}_1[Z_2]$. Hence, $H_1$ is pseudo-degenerated with edge data $(q_2, m_2, P_2, N_2) = (1, 4, Z_2^4 + (z_1 - 1)Z_2 + 1, 1)$. As $N_2 = 1$, we deduce that $F$ is pseudo-irreducible.

Note that $F$ is thus balanced (see Section 8). In particular, it has $\ell_1\ell_2 = 8$ irreducible factors in $\overline{\mathbb{Q}}[[X]][Y]$ all with same ramification index $q_1q_2 = 2$ and whose characteristic exponents and intersection multiplicities can be deduced from the edges data thanks to Theorem 9 and formula (32). If we want furthermore to compute the number of irreducible factors in $\mathbb{Q}[[X]][Y]$ together with their residual degrees, there only remains to compute the decomposition of the last residue ring $\mathbb{Q}_2$ into fields summand. We find

here the field decomposition:

$$\mathbb{Q}_2 \simeq \frac{\mathbb{Q}[Z_1,Z_2]}{(Z_1-1,Z_2^4+1)} \oplus \frac{\mathbb{Q}[Z_1,Z_2]}{(Z_1+1,Z_2-1)} \oplus \frac{\mathbb{Q}[Z_1,Z_2]}{(Z_1+1,Z_2^3+Z_2^2+Z_2-1)}.$$

It follows that $F$ has three irreducible factors in $\mathbb{Q}[[X]][Y]$ of respective residual degrees $4,1,3$ (which are given together with their residue fields) and ramification index 2. In particular, they have respective degrees $8,2,6$.

*Remark* 15. This example was chosen to illustrate that it might be necessary to perform some splittings in course of the involved square-free tests, as mentionned in Remark 14. In case of pseudo-degeneracy, the splittings recombine thanks to the Chinese Remainder Theorem, and we pursue the algorithm over a single residue field: in the previous example, if we would have found $Q_1 = P_{2,1}^{N_2}$ and $Q_2 = P_{2,2}^{N_2}$ with $P_{2,i} \in \mathbb{Q}_{1,i}[Z_2]$ square-free and with *the same* exponent $N_2 > 1$ for $i = 1,2$, we would have continue the algorithm over the single current residue ring $\mathbb{Q}_2 = \mathbb{Q}_1[Z_2]/(P_2)$, with $P_2 \in \mathbb{Q}_1[Z_2]$ square-free, recovered from its reductions $P_{2,1}$ and $P_{2,2}$.

The reader will find more examples in Subsection 8.4.

# 8 Pseudo-irreducible means balanced

We show in this section that a polynomial is pseudo-irreducible if and only if its absolutely irreducible factors are equisingular and have same sets of pairwise intersection multiplicities (balanced polynomials). In this case, we give explicit formulas for the characteristic exponents and the intersection multiplicities in terms of the edges data. This leads us to the proof of Theorem 3.

## 8.1 Balanced polynomials

**Characteristic exponents.** Let $F \in \overline{\mathbb{K}}[[x]][y]$ be an irreducible polynomial of degree $e$ satisfying $F(0,0) = 0$. We still assume that $\mathrm{Char}(\mathbb{K})$ is zero or greater than $e$ and we let $(T^e, \sum a_i T^i)$ be the Puiseux parametrization of the germ of plane curve $(F,0)$ (or branch) defined by $F$. The *characteristic exponents* of $F$ are those exponents $i$ for which a non trivial factor of the ramification index is discovered. Namely, they are defined as

$$\beta_0 = e, \quad \beta_k = \min\left(i \ \text{ s.t. } a_i \neq 0,\ gcd(\beta_0,\ldots,\beta_{k-1}) \not| i\right), \quad k = 1,\ldots,G,$$

where $G$ is the least integer for which $gcd(\beta_0,\ldots,\beta_G) = 1$ (characteristic exponents are sometimes refered to the rational numbers $\beta_i/e$ in the litterature). It is wellknown that the data

$$\mathrm{C}(F) = (\beta_0;\beta_1,\ldots,\beta_G)$$

determines the *equisingularity class* of the germ $(F,0)$. The equisingular equivalence of two germs of plane curves was developped by Zariski in [35]. There are several equivalent

definitions, a usual one being in terms of the multiplicity sequences of the infinitely near points of the singularity. This notion is particularly important as it agrees with the topological class when $\mathbb{K} = \mathbb{C}$ (see e.g. [32]). Conversely, two equisingular germs of curves which are not tangent to the $x$-axis have same characteristic exponents [4, Corollary 5.5.4]. If tangency occurs, we rather need to consider "generic characteristic exponents", which form a complete set of equisingular (hence topological if $\mathbb{K} = \mathbb{C}$) invariants. The set $\mathrm{C}(F)$ and the set of generic characteristic exponents determine each others assuming that we are given $\beta_0$ (contact order with $x$-axis) [20, Proposition 4.3] or [4, Corollary 5.6.2]. Note that a data equivalent to $\mathrm{C}(F)$ is given by the list of intersection multiplicities of $F$ with its characteristic approximate roots $\psi_{-1}, \psi_0, \ldots, \psi_g$ [4, Cor. 5.8.5 and 5.9.11], or equivalently with its characteristic minimal polynomials $\phi_{-1}, \ldots, \phi_g$ (use e.g. Proposition 9 and Lemma 2, or see [20]).

More generally, if $F \in \overline{\mathbb{K}}[[x]][y]$ is irreducible, it defines a unique germ of irreducible curve on the line $x = 0$, with center $(0, c)$, $c \in \overline{\mathbb{K}} \cup \{\infty\}$. We define then the characteristic exponents of $F$ as those of the shifted polynomial $F(x, y+c)$ if $c \in \overline{\mathbb{K}}$ or of the reciprocal polynomial $\tilde{F} = y^d F(x, y^{-1})$ if $c = \infty$.

**Intersection sets.** If we want to determine the equisingularity class of a reducible polynomial $(F, 0)$, we need to consider also the intersection multiplicities between the branches of $F$. The intersection multiplicity between two coprime polynomials $G, H \in \mathbb{K}[[x]][y]$ is defined as

$$(G, H)_0 := v_x(\mathrm{Res}_y(G, H)) = \dim_{\overline{\mathbb{K}}} \frac{\overline{\mathbb{K}}[[x]][y]}{(G, H)},$$

the right hand equality following from classical properties of the resultant. The intersection multiplicity is zero if and only if $G$ and $H$ do not have branches with same center. Suppose that $F$ has (distinct) irreducible factors $F_1, \ldots, F_f \in \overline{\mathbb{K}}[[x]][y]$. We introduce *the intersection sets* of $F$, defined for $i = 1, \ldots, f$ as

$$\Gamma_i(F) := \big((F_i, F_j)_0,\ 1 \le j \le f, j \ne i\big).$$

By convention, we take into account repetitions, $\Gamma_i(F)$ being considered as an unordered list with cardinality $f - 1$. If $F$ is Weierstrass, the equisingular class (hence the topological class if $\mathbb{K} = \mathbb{C}$) of the germ $(F, 0)$ is uniquely determined by the characteristic exponents and the intersections sets of the branches of $F$ [36]. Note that the set $\mathrm{C}(F_i)$ only depends on $F_i$ while $\Gamma_i(F)$ depends on $F$.

**Balanced polynomials.** Theorem 3 asserts that in some "balanced" situation, we can compute in quasi-linear time characteristic exponents and intersection sets of some reducible polynomials.

**Definition 7.** We say that $F$ is *balanced* if $\mathrm{C}(F_i) = \mathrm{C}(F_j)$ and $\Gamma_i(F) = \Gamma_j(F)$ for all $i, j$. In such a case, we denote simply these sets by $\mathrm{C}(F)$ and $\Gamma(F)$.

Thus, if $F$ is a balanced Weierstrass polynomial, its absolutely irreducible factors are equisingular and have same sets of pairwise intersection multiplicities, and the converse holds if no branch is tangent to the $x$-axis or all branches are tangent to the $x$-axis.

**Example 5.** Let us illustrate this definition with some basic examples. Note that the second and third examples show in particular that no condition implies the other in Definition 7.

• If $F \in \mathbb{K}[[x]][y]$ is irreducible, a Galois argument shows that it is balanced (follows from Theorem 9 below). The converse doesn't hold: $F = (y-x)(y+x^2)$ is reducible, but it is balanced. This example also shows that balancedness does not imply straightness of the Newton polygon.

• The polynomial $F = (y^2-x^3)(y^2+x^3)(y^2+x^3+x^4)$ is not balanced. It has 3 absolutely irreducible factors with same sets of characteristic exponents $\mathrm{C}(F_i) = (2;3)$ for all $i$, but $\Gamma_1(F) = (6,6)$ while $\Gamma_2(F) = \Gamma_3(F) = (6,8)$.

• The polynomial $F = (y-x-x^2)(y-x+x^2)(y^2-x^3)$ is not balanced. It has 3 absolutely irreducible factors with same sets of pairwise intersection multiplicities $\Gamma_i(F) = (2,2)$, but $\mathrm{C}(F_1) = \mathrm{C}(F_2) = (1)$ while $\mathrm{C}(F_3) = (2;3)$.

• The polynomial $F = (y-2x^2)^2 - 8yx^5 - 2x^8$ has four irreducible factors in $\overline{\mathbb{Q}}[[x]][y]$, namely $F_1 = y - \sqrt{2}x - \sqrt[4]{2}x^2$, $F_2 = y - \sqrt{2}x + \sqrt[4]{2}x^2$, $F_3 = y + \sqrt{2}x - i\sqrt[4]{2}x^2$ and $F_4 = y - \sqrt{2}x + i\sqrt[4]{2}x^2$. We have $C(F_i) = (1)$ and $\Gamma_i(F) = (1,1,2)$ for all $i$ so $F$ is balanced. Note that this example shows that balancedness does not imply that all factors intersect each others with the same multiplicity.

• The polynomial $F = (y^2 - x^3)(y^3 - x^2)$ is not balanced. However, it defines two equisingular germs of plane curve (one is tangent to the $x$-axis while the other is not).

**Noether-Merle's Formula.** If $F, G \in \overline{\mathbb{K}}[[x]][y]$ are two irreducible Weierstrass polynomials of respective degrees $e_F$ and $e_G$, their intersection multiplicty $(F,G)_0$ at the origin is closely related to the characteristic exponents $(\beta_0, \ldots, \beta_G)$ of $F$. Let us denote by

$$\mathrm{Cont}(F,G) := e_F \max_{\substack{F(y_F)=0 \\ G(y_G)=0}} v_x(y_F - y_G)$$

the *contact order* of the branches $F$ and $G$. Then Noether-Merle's [18] formula states

$$(F,G)_0 = \frac{e_G}{e_F}\left(\sum_{k\le K}(E_{k-1}-E_k)\beta_k + E_K \mathrm{Cont}(F,G)\right), \tag{31}$$

where $E_k := gcd(\beta_0, \ldots, \beta_k)$ and $K = \max(k \,|\, \beta_k \le \mathrm{Cont}(F,G))$. A proof can be found in [20, Proposition 6.5] (or references therein), where a formula is given in terms of the semi-group generators, which turns out to be equivalent to (31) thanks to [20, Proposition 4.2].

**$PGL_2(\mathbb{K})$-invariance of characteristic exponents and intersection sets.** As we will consider also non monic polynomials, we will need the following lemma in order to reduce to the monic case.

**Lemma 7.** *Let $a, b, c, d \in \mathbb{K}$ such that $ad - bc \neq 0$. Then $F$ and $\tilde{F} := (cy+d)^d F\left(\frac{ay+b}{cy+d}\right)$ have same number of irreducible factors in $\mathbb{K}[[x]][y]$, same numbers of irreducible factors in $\overline{\mathbb{K}}[[x]][y]$, same sets of characteristic exponents and same intersection sets. In particular, $F$ is balanced if and only if $\tilde{F}$ is.*

*Proof.* As $\tilde{F}$ is obtained after a projective change of coordinate over $\mathbb{K}$, it's clear that $F$ and $\tilde{F}$ have same number of factors over any given field extension of $\mathbb{K}$. If $F$ has irreducible factors $F_1, \ldots, F_f$ over $\overline{\mathbb{K}}$, then $\tilde{F}$ has irreducible factors $\tilde{F}_i = (cy+d)^{d(F_i)} F_i((ay+b)/(cy+d))$, $i = 1, \ldots, f$. It follows immediately that $\mathrm{C}(F_i) = \mathrm{C}(\tilde{F}_i)$ as the characteristic exponents are computed after translation to $y = 0$. We have also $\Gamma_i(F) = \Gamma_i(\tilde{F})$ as the $x$-valuation of the resultant is invariant under projective change of the $y$ coordinate (see e.g. [12, Chapter 12]). □

## 8.2 Balanced is equivalent to pseudo-irreducible

**Notations and main results.** Let $F \in \mathbb{K}[[x]][y]$ be a monic and square-free polynomial. As usual we let $(q_1, m_1, P_1, N_1), \ldots, (q_g, m_g, P_g, N_g)$ its edge data computed by algorithm `Pseudo-Irreducible`. We denote $e = e_g = q_1 \cdots q_g$ and let $\hat{e}_k = e/e_k$. We define $f = f_g = \ell_1 \cdots \ell_g$ and $\hat{f}_k = f/f_k$ in the analoguous way, where as usual $\ell_k = \deg(P_k)$. For all $k = 1, \ldots, g$, we define

$$B_k = m_1\hat{e}_1 + \cdots + m_k\hat{e}_k \quad \text{and} \quad M_k = m_1\hat{e}_0\hat{e}_1 + \cdots + m_k\hat{e}_{k-1}\hat{e}_k \tag{32}$$

and we let $B_0 = e$. They are positive integers related by the formula

$$M_k = \sum_{i=1}^{k} (\hat{e}_{i-1} - \hat{e}_i)B_i + \hat{e}_k B_k. \tag{33}$$

Note that $0 \leq B_1 \leq \cdots \leq B_g$ and $B_0 \leq B_g$. We have $B_1 > 0$ if and only if $m_1 > 0$, or equivalently, $F$ is Weierstrass. In such a case, the inequality $B_0 \leq B_1$ is equivalent to that $q_1 \leq m_1$, meaning that the germ $(F, 0)$ is not tangent to the $x$-axis. We check easily that $\hat{e}_k = gcd(B_0, \ldots, B_k)$. In particular, $gcd(B_0, \ldots, B_g) = 1$.

**Theorem 9.** *A monic polynomial $F \in \mathbb{K}[[x]][y]$ is balanced if and only if it is pseudo-irreducible. In such a case, it has $f$ irreducible factors in $\overline{\mathbb{K}}[[x]][y]$ of degree $e$ and*

1. *$C(F) = (B_0; B_k \,|\, q_k > 1)$*
2. *$\Gamma(F) = (M_k \,|\, \ell_k > 1)$, where $M_k$ appears $\hat{f}_{k-1} - \hat{f}_k$ times.*

Note that taking into account repetitions, the intersection set has cardinality $\sum_{k=1}^{g}(\hat{f}_{k-1} - \hat{f}_k) = f - 1$, as required. Of course, it is empty if and only if $f = 1$, that is if $F$ is irreducible in $\overline{\mathbb{K}}[[x]][y]$.

**Corollary 5.** *Let $F \in \mathbb{K}[[x]][y]$ balanced and monic. Then, the discriminant of $F$ has valuation*

$$\delta = f\Big(\sum_{\ell_k>1}(\hat{f}_{k-1}-\hat{f}_k)M_k + \sum_{q_k>1}(\hat{e}_{k-1}-\hat{e}_k)B_k\Big)$$

*and the discriminants of the absolutely irreducible factors of $F$ all have same valuation $\bar{\delta} = \sum_{q_k>1}(\hat{e}_{k-1}-\hat{e}_k)B_k$.*

*Proof. (of Corollary 5)* Suppose that $F$ is balanced. Then it has $f$ irreducible factors $F_1, \ldots, F_f$ of same degree $e$, with discriminant valuations say $\delta_1, \ldots, \delta_f$. The multiplicative property of the discriminant gives the well-known formula

$$\delta = \sum_{1\le i\le f}\delta_i + \sum_{1\le i\ne j\le f}(F_i, F_j)_0. \tag{34}$$

Let $y_1, \ldots, y_e$ be the roots of $F_i$. Thanks to [32, Proposition 4.1.3 (ii)] combined with point 1 of Theorem 9, we deduce that for each fixed $a = 1, \ldots, e$, the list $(v_x(y_a - y_b), b \ne a)$ consists of the values $B_k/e$ repeated $\hat{e}_{k-1} - \hat{e}_k$ times for $k = 1, \ldots, g$. Since $\delta_i = \sum_{1\le a\ne b\le e} v_x(y_a - y_b)$, we deduce that $\bar{\delta} := \delta_1 = \cdots = \delta_f$ satisfies the claimed formula. The formula for $\delta$ then follows straightforwardly from (34) combined with point 2 in Theorem 9. □

The proof of Theorem 9 requires some intermediate results. We begin by investigating the relations between (pseudo)-rational Puiseux expansions and the Puiseux series of $F$.

**Structure of the pseudo-rational Puiseux expansion.** Contrarly to [25] where dynamic evaluation is also considered, we do not necessarily "split" the Newton-Puiseux type algorithm when we meet several edges. However, we show that this has no impact for our purpose and that algorithm `Pseudo-ARNP` still allow to recover all the Puiseux series of a pseudo-irreducible polynomial. To this aim, we need to study in more details the so-called pseudo-rational Puiseux expansion (pseudo-RPE for short)

$$(\mu_k T^{e_k}, S_k(T)) := \pi_k(T, 0)$$

computed when running algorithm `Pseudo-ARNP`. As an induction argument is used, we need some further notations.

*Exponents data.* For all $0 \le i \le k \le g$, we define $Q_{k,i} = q_{i+1}\cdots q_k$ with convention $Q_{k,k} = 1$ and let

$$B_{k,i} = m_1 Q_{k,1} + \cdots + m_i Q_{k,i} \tag{35}$$

with convention $B_{k,0} = 0$. We have $Q_{k+1,i} = Q_{k,i}q_{k+1}$ and $B_{k+1,i} = q_{k+1}B_{k,i}$ for all $i \le k$ and $B_{k+1,k+1} = q_{k+1}B_{k,k} + m_{k+1}$.

*Coefficients data.* For all $0 \le i \le k \le g$, we define $\mu_{k,i} := z_{i+1}^{t_{i+1}Q_{i,i}} \cdots z_k^{t_k Q_{k-1,i}}$ with convention $\mu_{k,k} = 1$ and let

$$\alpha_{k,i} := \mu_{k,1}^{m_1} \cdots \mu_{k,i}^{m_i}, \tag{36}$$

with conventions $\alpha_{k,0} = 1$. We have $\mu_{k+1,i} = \mu_{k,i} z_{k+1}^{t_{k+1} Q_{k,i}}$ and $\alpha_{k+1,i} = \alpha_{k,i} z_{k+1}^{t_{k+1} B_{k,i}}$ for all $1 \leq i \leq k$, and $\alpha_{k+1,k+1} = \alpha_{k+1,k}$.

*Remark* 16. Note that $\mu_{k,0}$ is invertible in the product of fields $\mathbb{K}_k$. Namely, if $z_i \notin \mathbb{K}_i^\times$, then $P_i(0)$ is a zero divisor and we must have $q_i = 1$ by definition of pseudo-degeneracy (see Remark 7). In such a case, we have $t_i = 0$ and $z_i$ does not appear as a factor of $\mu_{k,0}$.

**Lemma 8.** *Let $z_0 = 0$. For all $k = 0, \dots, g$, we have the formula*

$$\pi_k(x, y) = \left( \mu_{k,0} x^{Q_{k,0}}, \sum_{i=0}^{k} \alpha_{k,i} x^{B_{k,i}} \left( z_i^{s_i} + c_i\left(\mu_{k,i} x^{Q_{k,i}}\right) \right) + \alpha_{k,k} x^{B_{k,k}} y \right).$$

*Proof.* This is correct for $k = 0$: the formula becomes $\pi_0(x, y) = (x, y + c_0(x))$. For $k > 0$, we conclude by induction, using the the relations (35) and (36) above with definition $\pi_k(x, y) = \pi_{k-1}(z_k^{t_k} x^{q_k}, x^{m_k}(z_k^{s_k} + c_k(x) + y))$. □

Given $\alpha$ an element of a ring $\mathbb{L}$, we denote by $\alpha^{1/e}$ the residue class of $Z$ in $\mathbb{L}[Z]/(Z^e - \alpha)$. By Remark 16 we know that $\mu_{k,0} \in \mathbb{K}_k$ is invertible for all $k = 0, \dots, g$ and we introduce the ring extension

$$\mathbb{L}_k := \mathbb{K}_k[\theta_k] = \mathbb{K}[z_1, \dots, z_k][\theta_k], \quad \text{where} \quad \theta_k := \left(\mu_{k,0}^{-\hat{e}_k}\right)^{\frac{1}{e}}.$$

Note that $\mathbb{L}_0 = \mathbb{K}$ and we check straightforwardly from the definition that $\theta_k \in \mathbb{L}_{k+1}$. In particular, we have a natural strict inclusion $\mathbb{L}_k \subset \mathbb{L}_{k+1}$.

**Proposition 14.** *Let $F \in \mathbb{K}[[x]][y]$ be Weierstrass and $\tilde{S} = S(\mu^{-1/e} T)$ with $(\mu\, T^e, S(T)) := \pi_g(T, 0)$. We have*

$$\tilde{S}(T) = \sum_{B > 0} a_B T^B \in \mathbb{L}_g[[T]],$$

*where $gcd(B_0, \dots, B_k) | B$ and $a_B \in \mathbb{L}_k$ for all $B < B_{k+1}$ (with convention $B_{g+1} := +\infty$). Moreover, we have for all $1 \leq k \leq g$*

$$a_{B_k} = \begin{cases} \varepsilon_k (z_k \theta_{k-1}^{m_k})^{\frac{1}{q_k}} & \text{if} \quad q_k > 1 \\ \varepsilon_k z_k \theta_{k-1}^{m_k} + \rho_k & \text{if} \quad q_k = 1 \end{cases} \tag{37}$$

*where $\varepsilon_k \in \mathbb{L}_{k-1}$ is invertible and $\rho_k \in \mathbb{L}_{k-1}$. In particular $a_{B_k} \in \mathbb{L}_k \setminus \mathbb{L}_{k-1}$.*

*Proof.* Note first that we have $\mu = \mu_{g,0}$ thanks to Lemma 8, so that $\tilde{S}(T) = S(\theta_g T)$ lies in $\mathbb{L}_g[[T]]$ as required. Thanks to definitions (35) and (36), we compute

$$\mu_{g,k} \mu_{g,0}^{-\hat{e}_k/e} = \theta_k \in \mathbb{L}_k \quad \text{and} \quad \alpha_{g,k} \mu_{g,0}^{-B_k/e} = \prod_{j=1}^{k} \left( \mu_{g,j} \mu_{g,0}^{-\hat{e}_j/e} \right)^{m_j} = \prod_{j=1}^{k} \theta_j^{m_j} \in \mathbb{L}_k. \tag{38}$$

Combined with Lemma 8 applied to rank $k = g$, we deduce

$$\tilde{S}(T) = \sum_{k=0}^{g} U_k(\theta_k T^{\hat{e}_k}) T^{B_k}, \qquad U_k(T) := \left(z_k^{s_k} + c_k(T)\right) \prod_{j=1}^{k} \theta_j^{m_j} \in \mathbb{L}_k[[T]]. \tag{39}$$

As $\hat{e}_k = gcd(B_0, \ldots, B_k)$ divides both $\hat{e}_i$ and $B_i$ for all $i \leq k$, this forces $gcd(B_0, \ldots, B_k)$ to divide $B$ for all $B < B_{k+1}$. In the same way, as $\mathbb{L}_i \subset \mathbb{L}_k$ for all $i \leq k$, we get $a_B \in \mathbb{L}_k$ for all $B < B_{k+1}$. There remains to show the formula for $a_{B_k}$ for $k \geq 1$. As $c_k(0) = 0$, we deduce that

$$U_k(0) = z_k^{s_k} \prod_{j=1}^{k} \theta_j^{m_j} = (z_k \theta_{k-1}^{m_k})^{\frac{1}{q_k}} \prod_{j=1}^{k-1} \theta_j^{m_j}, \tag{40}$$

the second equality using the Bézout relation $s_k q_k - t_k m_k = 1$. Note that $\varepsilon_k := \prod_{j=1}^{k-1} \theta_j^{m_j} \in \mathbb{L}_{k-1}$ is invertible by Remark 16. In particular, $(z_k \theta_{k-1}^{m_k})^{\frac{1}{q_k}} \in \mathbb{L}_k$ (although $z_k^{1/q_k}$ might not belong to $\mathbb{L}_k$). Let $\rho_k$ be the sum of the contribution of the terms $T^{B_i} U_i$ to the coefficient of the monomial $T^{B_k}$. So $a_{B_k} = U_k(0) + \rho_k$. As $B_1 \leq \cdots \leq B_g$ and $k \geq 1$, we deduce that if $U_i T^{B_i}$ contributes to $T^{B_k}$, then $i < k$ so that $U_i T^{B_i} \in \mathbb{L}_{k-1}[[T^{\hat{e}_{k-1}}]]$. We deduce that $\rho_k \in \mathbb{L}_{k-1}$. Moreover, $\rho_k \neq 0$ forces $\hat{e}_{k-1}$ to divide $B_k$. By definition (32) of $B_k$, and using that $m_k$ is coprime to $q_k$, we must have $q_k = 1$, as required. □

*Remark* 17. While algorithm `Pseudo-ARNP` allows to compute the all parametrization $\sum_B a_B T^B$ (up to some truncation bound), algorithm `Pseudo-Irreducible` precisely allows to compute the monomials $(a_{B_k} - \rho_k) T^{B_k}$, $k = 0, \ldots, g$ (using (37) and explicit formula of $\varepsilon_k$ in terms of edges data). As the remaining part of this section shows, this is precisely the minimal information required for testing balancedness. For instance, the Puiseux series of $F = (y - x - x^2)^2 - 2x^4$ are $S_1 = T + T^2(-\sqrt{2} + 1)$ and $S_2 = T + T^2(\sqrt{2} + 1)$. While algorithm `Pseudo-ARNP` allows to compute $S_1$ and $S_2$, algorithm `Pseudo-Irreducible` will compute only the "essential monomials" $-\sqrt{2}T^2$ and $\sqrt{2}T^2$ with approximate roots. Computing the singular part of the Puiseux series of a (pseudo)-irreducible polynomial in quasi-linear time remains an open challenge (see Section 9 for some hints towards such a result).

For all $\zeta \in W$, we denote by $\theta_g(\zeta)$ a $e^{th}$-roots of $\mu(\zeta)^{-1} = \mu_{g,0}(\zeta)^{-1}$. Such a choice induces a natural evaluation map

$$ev_\zeta : \mathbb{L}_g = \mathbb{K}[z_1, \ldots, z_g][\theta_g] \to \mathbb{K}[\zeta_1, \ldots, \zeta_g][\theta_g(\zeta)] \subset \overline{\mathbb{K}}$$

and we denote for short $a(\zeta) \in \overline{\mathbb{K}}$ the evaluation of $a \in \mathbb{L}_g$ at $\zeta$.

Let $\zeta' \in W$. By construction, when $\theta_g(\zeta')$ runs over the $q^{th}$-roots of $\mu(\zeta')^{-1}$, then $\theta_k(\zeta')$ runs over the $e_k = e/\hat{e}_k$ roots of $\mu_{k,0}(\zeta'_1, \ldots, \zeta'_k)$. Hence it is always possible to choose $\theta_g(\zeta')$ in such a way that

$$(\zeta_1, \ldots, \zeta_k) = (\zeta'_1, \ldots, \zeta'_k) \quad \Longrightarrow \quad \theta_k(\zeta) = \theta_k(\zeta'), \tag{41}$$

We assume this from now. In such a case, we have $a(\zeta) = a(\zeta')$ for all $a \in \mathbb{L}_k$. The following lemma is crucial for our purpose.

**Lemma 9.** *Let us fix $\omega$ such that $\omega^e = 1$ and let $\zeta, \zeta' \in W$. For all $k = 0, \dots, g$, the following assertions are equivalent:*

1. *$a_B(\zeta) = a_B(\zeta')\omega^B$ for all $B \leq B_k$.*
2. *$a_B(\zeta) = a_B(\zeta')\omega^B$ for all $B < B_{k+1}$.*
3. *$(\zeta_1, \dots, \zeta_k) = (\zeta'_1, \dots, \zeta'_k)$ and $\omega^{\hat{e}_k} = 1$.*

*Proof.* By Proposition 14, we have $a_B \in \mathbb{L}_k$ and $\hat{e}_k | B$ for all $B < B_{k+1}$ from which we deduce 3) $\Rightarrow$ 2) thanks to hypothesis (41). As 2) $\Rightarrow$ 1) is obvious, we need to show 1) $\Rightarrow$ 3). We show it by induction. If $k = 0$, the claim follows immediately since $\hat{e}_0 = q$. Suppose 1) $\Rightarrow$ 3) holds true at rank $k-1$ for some $k \geq 1$. Let us denote by $\zeta_k^{1/q_k} := ev_\zeta(z_k^{1/q_k})$. If $a_B(\zeta) = a_B(\zeta')\omega^B$ for all $B \leq B_k$, then this holds true for all $B \leq B_{k-1}$. As $\varepsilon_k, \rho_k \in \mathbb{L}_{k-1}$, the induction hypothesis combined with (41) gives $\varepsilon_k(\zeta) = \varepsilon_k(\zeta') \neq 0$ and $\rho_k(\zeta) = \rho_k(\zeta')$. Let us use now $a_{B_k}(\zeta) = a_{B_k}(\zeta')\omega^{B_k}$. Two cases occur:

- If $q_k > 1$, we deduce from (37) that $\left(\zeta_k \theta_{k-1}^{m_k}(\zeta)\right)^{\frac{1}{q_k}} = \left(\zeta'_k \theta_{k-1}^{m_k}(\zeta')\right)^{\frac{1}{q_k}} \omega^{B_k}$. Raising to the power $q_k$, and using that $\hat{e}_{k-1} | q_k B_k$ forces $\omega^{q_k B_k} = 1$ by induction hypothesis, we deduce that $\zeta_k \theta_{k-1}^{m_k}(\zeta) = \zeta'_k \theta_{k-1}^{m_k}(\zeta')$. As $\theta_{k-1} \in \mathbb{L}_{k-1}^\times$, we get $\zeta_k = \zeta'_k$ thanks again to the induction hypothesis. Furthermore, as $\zeta_k = \zeta'_k$ implies $a_{B_k}(\zeta) = a_{B_k}(\zeta')$ thanks to (41), we have also $\omega^{B_k} = 1$.
- If $q_k = 1$, we deduce from (37) that $\zeta_k \theta_{k-1}^{m_k}(\zeta) + \rho_k(\zeta) = \omega^{B_k}(\zeta'_k \theta_{k-1}^{m_k}(\zeta') + \rho_k(\zeta'))$. As $q_k = 1$ implies $\hat{e}_{k-1} = \hat{e_k} | B_k$ and $\rho_k \in \mathbb{L}_{k-1}$, $\theta_{k-1} \in \mathbb{L}_{k-1}^\times$, induction hypothesis gives again $\omega^{B_k} = 1$ and $\zeta_k = \zeta'_k$.

To conclude, use that $B_k = \sum_{s \leq k} m_s \hat{e}_s$, so that induction hypothesis gives $(\omega^{\hat{e}_k})^{m_k} = 1$. Since $m_k$ is coprime to $q_k$ and $(\omega^{\hat{e}_k})^{q_k} = \omega^{\hat{e}_{k-1}} = 1$, this forces $\omega^{\hat{e}_k} = 1$. □

In particular, Lemma 9 above implies that algorithm `Pseudo-ARNP` still allow to recover all the Puiseux series of a pseudo-irreducible polynomial, as required.

**Corollary 6.** *Suppose that $F$ is pseudo-irreducible and Weierstrass. Then $F$ admits exactly $f$ distinct monic irreducible factors $F_\zeta \in \overline{\mathbb{K}}[[x]][y]$ indexed by $\zeta \in W$. Each factor $F_\zeta$ has degree $e$ and defines a branch with classical Puiseux parametrizations $(T^e, \tilde{S}_\zeta(T))$ where*

$$\tilde{S}_\zeta(T) = \sum_B a_B(\zeta) T^B. \tag{42}$$

*The $e$ Puiseux series of $F_\zeta$ are given by $\tilde{S}_\zeta(\omega x^{\frac{1}{e}})$ where $\omega$ runs over the $e^{th}$-roots of unity and this set of Puiseux series does not depend of the choice of the $e^{th}$-roots $\theta_g(\zeta)$.*

*Proof.* As $F$ is pseudo-irreducible, $H_g = y$ (Weierstrass polynomial of degree $N_g = 1$ with no terms of degree $N_g - 1$),thus $\pi_g^* F(x, 0) = 0$. We deduce $F(T^e, \tilde{S}_\zeta(T)) = 0$ for all $\zeta \in W$. By (37), we have $a_{B_k}(\zeta) \neq 0$ for all $k$ such that $q_k > 1$. Since $gcd(B_0 = e, B_k \,|\, q_k > 1)) = gcd(B_0, \dots, B_g) = \hat{e}_g = 1$, the parametrization $(T^e, \tilde{S}_\zeta(T))$ is primitive,

that is the greatest common divisor of the exponents of the series $T^e$ and $\tilde{S}_\zeta(T)$ equals one. Hence, this parametrization defines a branch $F_\zeta = 0$, where $F_\zeta \in \overline{\mathbb{K}}[[x]][y]$ is an irreducible monic factor of $F$ of degree $e$. Thanks to Lemma 9, these $f$ branches are distinct when $\zeta$ runs over $W$. As $\deg(F) = e\,f$, we obtain in such a way all irreducible factors of $F$. The last claim follows straightforwardly. □

**Pseudo-irreducible implies balanced.** This is the easiest implication. Let us first consider the characteristic exponents. We get:

**Proposition 15.** *Let $F \in \mathbb{K}[[x]][y]$ be pseudo-irreducible. Then each branch $F_\zeta$ of $F$ has characteristic exponents $(B_0; B_k \,|\, q_k > 1)$, $k = 1, \dots, g)$.*

*Proof.* Thanks to Corollary 6, all polynomials $F_\zeta$ have same first characteristic exponent $B_0 = e$. Using again that $a_{B_k}(\zeta) \neq 0$ for all $k \geq 1$ such that $q_k > 1$ (by (37)), it follows immediately from Proposition 14 and Corollary 6 that the remaining characteristic exponents of $F_\zeta$ are those $B_k$ for which $k \geq 1$ and $q_k > 1$. □

Concerning the intersection multiplicities, we get:

**Proposition 16.** *Let $F \in \mathbb{K}[[x]][y]$ be pseudo-irreducible with at least two branches $F_\zeta, F_{\zeta'}$. We have*

$$(F_\zeta, F_{\zeta'})_0 = M_\kappa, \quad \kappa := \min\left(k = 1, \dots, g \,|\, \zeta_k \neq \zeta'_k\right).$$

*and this value is reached exactly $\hat{f}_{\kappa-1} - \hat{f}_\kappa$ times when $\zeta'$ runs over the set $W \setminus \{\zeta\}$.*

*Proof.* Noether-Merle's formula (31) combined with Proposition 15 gives

$$(F_\zeta, F_{\zeta'})_0 = \sum_{k \leq K} (\hat{e}_{k-1} - \hat{e}_k) B_k + \hat{e}_K \mathrm{Cont}(F_\zeta, F_{\zeta'}) \tag{43}$$

with $K = \max\{k \,|\, \mathrm{Cont}(F_\zeta, F_{\zeta'}) \geq B_k\}$. Note that the $B_k$'s which are not characteristic exponents do not appear in the first summand of formula (43) ($q_k = 1$ implies $\hat{e}_{k-1} - \hat{e}_k = 0$). It is a classical fact that we can fix any root $y$ of $F$ for computing the contact order (see e.g. [8, Lemma 1.2.3]). Combined with Corollary 6, we obtain the formula

$$\mathrm{Cont}(F_\zeta, F_{\zeta'}) = \max_{\omega^e = 1} \left( v_T \left( \tilde{S}_\zeta(T) - \tilde{S}_{\zeta'}(\omega T) \right) \right). \tag{44}$$

We deduce from Lemma 9 that

$$v_T \left( \tilde{S}_\zeta(T) - \tilde{S}_{\zeta'}(\omega T) \right) = B_{\bar{\kappa}}, \quad \bar{\kappa} := \min \left\{ k = 1, \dots, g \mid \zeta_k \neq \zeta'_k \text{ or } \omega^{\hat{e}_k} \neq 1 \right\}.$$

As $\omega = 1$ satisfies $\omega^{\hat{e}_k} = 1$ for all $k$, we deduce from the last equality that the maximal value in (44) is reached for $\omega = 1$ (it might be reached for other values of $\omega$). It follows that $\mathrm{Cont}(F_\zeta, F_{\zeta'}) = B_\kappa$ with $\kappa = \min\{k \,|\, \zeta_k \neq \zeta'_k\}$. We thus have $K = \kappa$ and (43) gives

$(F_\zeta, F_{\zeta'})_0 = \sum_{k=1}^{\kappa}(\hat{e}_{k-1} - \hat{e}_k)B_k + \hat{e}_\kappa B_\kappa = M_\kappa$, the last equality by (33). Let us fix $\zeta$. As said above, we may choose $\omega = 1$ in (44). We have $v_T(\tilde{S}_\zeta(T) - \tilde{S}_{\zeta'}(T)) = B_\kappa$ if and only if $\zeta'_k = \zeta_k$ for $k < \kappa$ and $\zeta_\kappa \neq \zeta'_\kappa$. This concludes, as the number of possible such values of $\zeta'$ is precisely $\hat{f}_{\kappa-1} - \hat{f}_\kappa$. □

If $F$ is pseudo-irreducible, then it is balanced and satisfies both items of Theorem 9 thanks to Proposition 15 and Proposition 16. There remains to show the converse.

**Balanced implies pseudo-irreducible.** We need to show that then $N_g = 1$ if $F$ is balanced. We denote more simply $H := H_g \in \mathbb{K}_g[[x]][y]$, and $\pi_g(T, 0) = (\mu T^e, S(T))$. We denote $H_\zeta, S_\zeta, \mu_\zeta$ the images of $H, S, \mu$ after applying (coefficient wise) the evaluation map $ev_\zeta : \mathbb{K}_g \to \overline{\mathbb{K}}$.

**Lemma 10.** *Suppose that $F$ is balanced. Then all irreducible factors of all $H_\zeta$, $\zeta \in W$ have same degree.*

*Proof.* Let $\zeta \in W$ and let $y_\zeta$ be a roots of $H_\zeta$. As $H_\zeta$ divides $(\pi_g^* F)_\zeta = \pi_{g,\zeta}^* F$ by (6), we deduce from Lemma 8 (use $B_{gg} = B_g$) that

$$F(\mu_\zeta x^e, S_\zeta(x) + x^{B_g} y_\zeta(x)) = 0.$$

Hence, $y_0(x) := \tilde{S}_\zeta(x^{\frac{1}{e}}) + \mu_\zeta^{-\frac{B_g}{e}} x^{\frac{B_g}{e}} y_\zeta(\mu_\zeta^{-\frac{1}{e}} x^{\frac{1}{e}})$ is a root of $F$ and we have moreover the equality

$$\deg_{\overline{\mathbb{K}}((x))}(y_0) = e \deg_{\overline{\mathbb{K}}((x))}(y_\zeta), \tag{45}$$

where we consider here the degrees of $y_0$ and $y_\zeta$ seen as algebraic elements over the field $\overline{\mathbb{K}}((x))$. As $F$ is balanced, all its irreducible factors - hence all its roots - have same degree. Combined with (45), this implies that all roots - hence all irreducible factors - of all $H_\zeta$, $\zeta \in W$ have same degree. □

**Corollary 7.** *Suppose $F$ balanced and $N_g > 1$. Then there exist some coprime positive integers $(q, m)$ and $Q \in \mathbb{K}_g[Z]$ monic with non zero constant term such that $H$ has lower boundary polynomial*

$$\bar{H}(x, y) = Q\left(y^q / x^m\right) x^{m \deg(Q)}.$$

*Proof.* As $N_g > 1$, the Weierstrass polynomial $H = H_g$ is not pseudo-degenerated and admits a lower slope $(q, m)$ (we can not have $H_g = y^{N_g}$ as $F$ would not be square-free). Hence, its lower boundary polynomial may be written in a unique way

$$\bar{H}(x, y) = y^r \tilde{Q}\left(y^q / x^m\right) x^{m \deg(\tilde{Q})} \tag{46}$$

for some non constant monic polynomial $\tilde{Q} \in \mathbb{K}_g[Z]$ with non zero constant term and some integer $r \geq 0$. Let $\zeta \in W$ such that $\tilde{Q}_\zeta(0) \neq 0$ and suppose $r > 0$. By applying the evaluation map $ev_\zeta$ to (46), we deduce that the Newton polygon of $H_\zeta$ has a vertice of type $(r, i)$, $0 \leq r \leq d$ and the Newton-Puiseux algorithm (over a field) implies that $H_\zeta$

admits two factors $A, B$ such that $\deg(A) = r$ and $\deg(B) = q\deg(\tilde{Q})$. By Lemma 10, this forces $q$ to divide $r$. Hence $r = nq$ for some $n \in \mathbb{N}$ and the claim follows by taking $Q(Z) = Z^n\tilde{Q}(Z)$. □

**Lemma 11.** *Suppose $F$ balanced and $N_g > 1$. We keep notations $q$ and $Q$ from Corollary 7. Let $G \in \overline{\mathbb{K}}[[x]][y]$ be an irreducible monic factor of $F$. Then $e\,q$ divides $n := \deg(G)$ and there exists a unique $\zeta \in W$ and a unique root $\alpha$ of $Q_\zeta$ such that $G$ admits a parametrization $(T^n, S_G(T))$, where*

$$S_G(T) \equiv \tilde{S}_\zeta(T^{\frac{n}{e}}) + \alpha^{\frac{1}{q}}\mu_\zeta^{-\frac{B_g}{e}}T^{\frac{n}{e}B_g+\frac{nm}{eq}} \mod T^{\frac{n}{e}B_g+\frac{nm}{eq}+1}, \tag{47}$$

*with $\alpha^{1/q}$ an arbitrary $q^{th}$-roots of $\alpha$ (we may a priori have $\alpha = 0$). Conversely, given $\zeta \in W$ and $\alpha$ a roots of $Q_\zeta$, there exists at least one irreducible factor $G$ for which (47) holds.*

*Proof.* Let $y_\zeta^{(i)}$, $i = 1, \dots, N_g$ be the roots of $H_\zeta$. Following the proof of Lemma 10, we know that each roots $y_\zeta^{(i)}$ gives rise to a family of $e$-roots of $F$

$$y_{\zeta,\omega}^{(i)} := \tilde{S}_\zeta(\omega x^{\frac{1}{e}}) + \omega\mu_\zeta^{-\frac{B_g}{e}}x^{\frac{B_g}{e}}y_\zeta^{(i)}(\omega\mu_\zeta^{-\frac{1}{e}}x^{\frac{1}{e}}),$$

where $\omega$ runs over the $e^{th}$ roots of unity. As $H_\zeta$ has distinct roots and $\tilde{S}_\zeta(\omega x^{1/e}) \neq \tilde{S}_{\zeta'}(\omega' x^{1/e})$ when $(\zeta, \omega) \neq (\zeta', \omega')$ (Lemma 9), we deduce that the $efN_g = \deg(F)$ Puiseux series $y_{\zeta,\omega}^{(i)}$ are distinct, getting all roots of $F$. As $e$ divides $n := \deg_{\overline{\mathbb{K}}((x))}(y_{\zeta,\omega}^{(i)})$ (use (45)), the roots $y_{\zeta,\omega}^{(i)}$, $\omega^e = 1$ belong to the same orbit of the Galois group of the field extension $\overline{\mathbb{K}}((x)) \to \overline{\mathbb{K}}((x^{1/n}))$. Thus, any irreducible factor $G$ of $F$ has degree $n$ and admits a root of type $y_{\zeta,1}^{(i)}$ for some pair $(\zeta, i)$. Hence $G$ admits a parametrization $(T^n, S_G(T))$, where $S_G(T) := y_{\zeta,1}^{(i)}(T^n)$. Since $y_\zeta^{(i)}(x) = \alpha^{1/q}x^{m/q} + h.o.t$ for some uniquely determined roots $\alpha$ of $Q_\zeta$ (use Corollary 7), we get the claimed formula. Since there exists at least one root $\alpha \neq 0$ of $Q_\zeta$, the fact that $S_G \in \overline{\mathbb{K}}[[T]]$ forces $nm/eq \in \mathbb{N}$. Hence $eq$ divides $n$ since $e$ divides $n$ and $q$ and $m$ are coprime. Conversely, if $\zeta \in W$ and $Q_\zeta(\alpha) = 0$, there exists at least one root $y_\zeta^{(i)}$ of $H_\zeta$ such that $y_\zeta^{(i)}(x) = \alpha^{1/q}x^{m/q} + h.o.t$ and by the same arguments as above, there exists at least one irreducible factor $G$ such that (47) holds. □

For any irreducible factor $G$ of $F$, we denote by $(\zeta(G), \alpha(G)) \in W \times \overline{\mathbb{K}}$ the unique pair $(\zeta, \alpha)$ such that (47) holds.

**Corollary 8.** *Suppose $F$ balanced and $N_g > 1$. Let $n$ stands for the degree of any of its irreducible factor and let $q$ as in Lemma 11. Then the lists of the characteristic exponents of the irreducible factors of $F$ all begin as $\{n\} \cup \{\frac{n}{e}B_k, q_k > 1, k = 1, \dots, g\}$. Moreover the next characteristic exponent of any factor $G$ is greater or equal than $\frac{n}{e}B_g + \frac{nm}{eq} \in \mathbb{N}$, with equality if and only if $q > 1$ and $\alpha(G) \neq 0$.*

*Proof.* This follows straightforwardly from Lemma 11 combined with Proposition 14 (similar argument than for Proposition 15). □

**Corollary 9.** *Suppose $F$ balanced with $N_g > 1$ and with $\rho \geq 2$ irreducible factors $G_1, \ldots, G_\rho \in \overline{\mathbb{K}}[[x]][y]$. We have*

$$(G_i, G_j)_0 > \frac{n^2}{e^2}\left(M_g + \frac{m}{q}\right) \quad \Longleftrightarrow \quad (\zeta(G_i), \alpha(G_i)) = (\zeta(G_j), \alpha(G_j)).$$

*Proof.* Using similar arguments than Proposition 16, we get $\mathrm{Cont}(G_i, G_j) = v_T(S_{G_i} - S_{G_j})$ and we deduce from (47) and Lemma 9 that $\mathrm{Cont}(G_i, G_j) > \frac{n}{e}B_g + \frac{nm}{eq}$ if and only if $\zeta(G_i) = \zeta(G_j)$ and $\alpha(G_i) = \alpha(G_j)$ . The claim then follows from Noether-Merle's formula (31) combined with Corollary 8. □

**Proposition 17.** *If $F$ is balanced, then it is pseudo-irreducible.*

*Proof.* We need to show that $N_g = 1$. Suppose on the contrary that $N_g > 1$. Let $\zeta \in W$ and let $G_i$ such that $\zeta(G_i) = \zeta$. Thanks to Lemma 11, we deduce from algorithm `ARNP` (over a field) that $\pi^*_{g,\zeta}(G_i)$ has an boundary polynomial of shape $(y^q - \alpha(G_i)x^m)^{N(G_i)}$ where $eqN(G_i) = \deg(G_i) = n$. In particular, $N(G_i) = n/eq$ is constant for all $i = 1, \ldots, \rho$. We deduce that $\bar{H}_\zeta = \prod_{i|\zeta(G_i)=\zeta}(y^q - \alpha(G_i)x^m)^{N(G_i)}$, hence

$$Q_\zeta(Z) = \prod_{i|\zeta(G_i)=\zeta} (Z - \alpha(G_i))^{N(G_i)}. \tag{48}$$

Let $\alpha$ be a root of $Q_\zeta$ and $j$ such that $(\zeta(G_j), \alpha(G_j)) = (\zeta, \alpha)$. Denote $I_j := \{i \neq j \,|\, (\zeta(G_i), \alpha(G_i)) = (\zeta(G_j), \alpha(G_j))\}$. Thanks to (48), we deduce that the root $\alpha$ has multiplicity $N(G_j) + \sum_{i\in I_j} N(G_i) = (\mathrm{Card}(I_j) + 1)n/eq$. As $F$ is balanced, all factors have same intersection sets and Corollary 9 implies that all sets $I_j$ have same cardinality. It follows that all roots $\alpha$ of all polynomials $Q_\zeta$ have same multiplicity. In other words, $Q$ is the power of some square-free polynomial $P \in \mathbb{K}_g[Z]$. If $q = 1$, this implies that $H = H_g$ is pseudo-degenerate (Definition 5), contradicting $N_g > 1$. If $q > 1$, we need to show moreover that $P$ has invertible constant term. Since there exists at least one non zero root $\alpha$ of some $Q_\zeta$ (Corollary 7), we deduce from Corollary 8 that at least one factor $G_i$ has next characteristic exponent $\frac{n}{e}B_g + \frac{nm}{eq}$ (use $q > 1$). As $F$ is balanced, it follows that all $G_i$'s have next characteristic exponent $\frac{n}{e}B_g + \frac{nm}{eq}$, which by Corollary 8 forces all $\alpha(G_i)$ - thus all roots $\alpha$ of all $Q_\zeta$ by last statement of Lemma 11 - to be non zero. Thus $P$ has invertible constant term and $H = H_g$ is pseudo-degenerate (Definition 5), contradicting $N_g > 1$. Hence $N_g = 1$ and $F$ is pseudo-irreducible. □

The proof of Theorem 9 is complete. □

## 8.3 Proof of Theorem 3.

If $F$ is monic, the result follows immediately from Proposition 13 and from Theorem 9 (see Section 8). Namely, $F$ is balanced if and only if it is pseudo-irreducible and in such a case, the edges data allow to compute characteristic exponents and pairwise intersection multiplicities as well as the discriminant valuation $\delta$ (Corollary 5). If $F = c(x)y^d + \cdots$ has invertible leading coefficient $c \in \mathbb{K}[[x]]$, $c(0) \neq 0$, we invert $c$ after line 1 up to precision $\eta \leq \eta(F)$, for a cost $\mathcal{O}(\eta) \subset \mathcal{O}(\delta)$, thus reducing in the aimed bound to the monic case. If the leading coefficient of $F$ is not invertible, we can find $z \in \mathbb{K}$ such that $F(0,z) \neq 0$ with at most $d$ evaluation of $F(0,y)$ at $z = 0, 1, \ldots, d$ (use here that $\mathbb{K}$ has at least $d$ elements). This costs at most $\mathcal{O}(d)$ using fast multipoint evaluation [11, Corollary 10.8]. One such a $z$ is found, we can apply previous strategy to the polynomial $\tilde{F} := y^d F\left(\frac{zy+1}{y}\right) \in \mathbb{K}[[x]][y]$ which has by construction an invertible coefficient. We have $\deg(F) = \deg(\tilde{F})$ and $\delta(F) = \delta(\tilde{F})$ [5] so the complexity remains the same. Moreover, Lemma 7 shows that $F$ is balanced if and only if $\tilde{F}$ is, and there is a one-to-one correspondance between the irreducible factors of $F$ and $\tilde{F}$ in $\bar{\mathbb{K}}[[x]][y]$ such that $F_i$ and $\tilde{F}_i$ have same characteristic exponents and same sets of intersection multiplicities. Hence we are reduced to the monic case, and so within the aimed complexity. Theorem 3 is proved. □

## 8.4 Some examples

**Example 6 (balanced).** Let $F = y^6 - 3x^3y^4 - 2x^2y^4 + 3x^6y^2 + x^4y^2 - x^9 + 2x^8 - x^7 \in \mathbb{Q}[x,y]$. This small example is constructed in such a way that $F$ has 3 irreducible factors $(y-x)^2 - x^3$, $(y+x)^2 - x^3$, $y^2 - x^3$ and we can check that $F$ is balanced, with $e = 2$, $f = 3$ and $\mathrm{C}(F_i) = (2;3)$ and $\Gamma_i(F) = (4,4)$ for all $i = 1,2,3$. Let us recover this with algorithm `Pseudo-Irreducible`.

*Initialise.* We have $N_0 = d = 6$, and we let $\psi_{-1} = x$, $V = (1,0)$ and $\Lambda = (1,1)$.

*Step* 0. The $6^{th}$-approximate roots of $F$ is $\psi_0 = y$ and we deduce that $\bar{H}_0 = y^6 - 2x^2y^4 + x^4y^2 = (y(y^2-x^2))^2$. Thus, $H_0$ is pseudo-degenerated with edge data $(q_1, m_1, P_1, N_1) = (1, 1, Z_1^3 - Z_1, 2)$. Accordingly to (19), we update $V = (1,1,1)$ and $\Lambda = (1, z_1, 3z_1^2 - 1)$. Note that the Newton polygon $\mathcal{N}$ of $F$ is not straight. In particular, $P_1$ is reducible over $\mathbb{Q}$ and $F$ is reducible over $\mathbb{Q}[[x]][y]$.

*Step* 1. The $2^{th}$-approximate root of $F$ is $\psi_1 = y^3 - \frac{3}{2}x^3y - x^2y$ and $F$ has $\Psi$-adic expansion $F = \psi_1^2 - 3\psi_0^2\psi_{-1}^5 + \frac{3}{4}\psi_0^2\psi_{-1}^6 - \psi_{-1}^7 + 2\psi_{-1}^8 - \psi_{-1}^9$. The monomials reaching the minimal values (11) are $\psi_1^2$ (for $j = 2$) and $-3\psi_0^2\psi_{-1}^5$ and $\psi_{-1}^7$ (for $j = 0$). We deduce from (12) that $\bar{H}_1 = y^2 - \alpha x$, where $\alpha = (3z_1^2+1)/(3z_1^2-1)^2$ is easily seen to be invertible in $\mathbb{Q}_1$ (in practice, we compute $P \in \mathbb{Q}[Z_1]$ such that $\alpha = P \mod P_1$ and we check $gcd(P_1, P) = 1$). We deduce that $H_1$ is pseudo-degenerated with edges data

[5] This equality explains why we consider the valuation of the resultant between $F$ and $F_y$ as main complexity indicator instead of the valuation of the discriminant which may vary under projective change of coordinates.

$(q_2, m_2, P_2, N_2) = (2, 1, Z_2 - \alpha, 1)$. As $N_2 = 1$, we deduce that $F$ is balanced with $g = 2$.

*Conclusion.* We deduce from Theorem 9 that $F$ has $f = \ell_1\ell_2 = 3$ irreducible factors over $\overline{\mathbb{K}}[[x]][y]$ of same degrees $e = q_1q_2 = 2$. Thanks to (32), we compute $B_0 = e = 2$, $B_1 = 2$, $B_2 = 3$ and $M_1 = 4$, $M_2 = 6$. We deduce that all factors of $F$ have same characteristic exponents $\mathrm{C}(F_i) = (B_0; B_2) = (2; 3)$ and same intersection sets $\Gamma_i(F) = (M_1, M_1) = (4, 4)$ (i.e. $M_1$ which appears $\hat{f}_0 - \hat{f}_1 = 3 - 1$ times), as required.

**Example 7 (non balanced).** Let $F = y^6 - x^6y^4 - 2x^4y^4 - 2x^2y^4 + 2x^{10}y^2 + 3x^8y^2 - 2x^6y^2 + x^4y^2 - x^{14} + 2x^{12} - x^{10} \in \mathbb{Q}[x, y]$. This second small example is constructed in such a way that $F$ has 6 irreducible factors $y + x - x^2$, $y + x - x^2$, $y - x - x^2$, $y - x + x^2$, $y - x^3$ and $y + x^3$ and we check that $F$ is not balanced, as $\Gamma_i(F) = (1, 1, 1, 1, 2)$ for $i = 1, \ldots, 4$ while with $\Gamma_i(F) = (1, 1, 1, 1, 3)$ for $i = 5, 6$. Let us recover this with algorithm `Pseudo-Irreducible`.

*Initialise.* We have $N_0 = d = 6$, and we let $\psi_{-1} = x$, $V = (1, 0)$ and $\Lambda = (1, 1)$.

*Step* 0. The $6^{th}$-approximate roots of $F$ is $\psi_0 = y$ and we deduce that $\bar{H}_0 = y^6 - 2x^2y^4 + x^4y^2 = (y(y^2 - x^2))^2$. Thus, as in Example 6, $H_0$ is pseudo-degenerated with edge data $(q_1, m_1, P_1, N_1) = (1, 1, Z_1^3 - Z_1, 2)$. Accordingly to (19), we update $V = (1, 1, 1)$ and $\Lambda = (1, z_1, 3z_1^2 - 1)$.

*Step* 1. The $2^{th}$-approximate root of $F$ is $\psi_1 = y^3 - yx^2 - yx^4 - \frac{1}{2}yx^6$ and $F$ has $\Psi$-adic expansion $F = \psi_1^2 - \psi_{-1}^{10} + 2\psi_{-1}^{12} - \psi_{-1}^{14} - 4\psi_{-1}^6\psi_0^2 + \psi_{-1}^8\psi_0^2 + \psi_{-1}^{10}\psi_0^2 - \frac{1}{4}\psi_{-1}^{12}\psi_0^2$. The monomials reaching the minimal values (11) are $\psi_1^2$ (for $j = 2$) and $-4\psi_{-1}^6\psi_0^2$ (for $j = 0$). We deduce from (12) that $\bar{H}_1 = y^2 - \alpha x^2$, where $\alpha = 4z_1^2/(3z_1^2 - 1)^2$. As $z_1$ is a zero divisor in $\mathbb{Q}_1 = \mathbb{Q}[Z_1]/(Z_1^3 - Z_1)$ and $(3z_1^2 - 1) = P_1'(z_1)$ is invertible in $\mathbb{Q}_1$, we deduce that $\alpha$ is a zero divisor. It follows that $\bar{H}_1$ is not the power of a square-free polynomial. Hence $H_1$ is not pseudo-degenerated and $F$ is not balanced (with $g = 1$), as required. In order to desingularise $F$, we would need at this stage to split the algorithm accordingly to the discovered factorization $P_1 = Z_1(Z_1^2 - 1)$ before continuing the process, as described in [25].

**Example 8 (non Weierstrass).** Let $F = (y + 1)^6 - 3x^3(y + 1)^4 - 2(y + 1)^4 + 3x^6(y + 1)^2 + (y + 1)^2 - x^9 + 2x^6 - x^3$. We have $F = ((y + 2)^2 - x^3)((y + 1)^2 - x^3)(y^2 - x^3)$ from which we deduce that $F$ is balanced with three irreducible factors with characteristic exponents $\mathrm{C}(F_i) = (2, 3)$ and intersection sets $\Gamma_i(F) = (0, 0)$. Let us recover this with algorithm `Pseudo-Irreducible`.

*Initialise.* We have $N_0 = d = 6$, and we let $\psi_{-1} = x$, $V = (1, 0)$ and $\Lambda = (1, 1)$.

*Step* 0. The $6^{th}$-approximate roots of $F$ is $\psi_0 = y + 1$. We have $F = \psi_0^6 - 3\psi_{-1}^3\psi_0^4 - 2\psi_0^4 + 3\psi_{-1}^6\psi_0^2 + \psi_0^2 - \psi_{-1}^9 + 2\psi_0^6 - \psi_{-1}^3$. By (11), the monomials involved in the lower edge of $H_0$ are $\psi_0^6, -2\psi_0^4, \psi_0^2$. We deduce from (12) that $\bar{H}_0 = (y^3 - y)^2$ so that $H_0$ is pseudo-degenerated with edge data $(q_1, m_1, P_1, N_1) = (1, 0, Z_1^3 - Z_1, 2)$. Note that $m_1 = 0$. This is the only step of the algorithm where this may occur. Using (19), we update $V = (1, 0, 0)$ and $\Lambda = (1, z_1, 3z_1^2 - 1)$.

*Step* 1 The $N_1 = 2^{th}$ approximate roots of $F$ is $\psi_1 = (y + 1)^3 - 3/2x^3(y + 1) - (y + 1)$ and $F$ has $\Psi$-adic expansion $F = \psi_1^2 - \psi_{-1}^3 - 3\psi_{-1}^3\psi_0^2 + 2\psi_{-1}^6 - \psi_{-1}^9 + 3/4\psi_{-1}^6\psi_0^2$. We

deduce that the monomials reaching the minimal values (11) are $\psi_1^2$ (for $j=2$) and $-\psi_{-1}^3$, $-3\psi_{-1}^3\psi_0^2$ (for $j=0$). We deduce from (12) that $\bar{H}_1 = y^2 - \alpha x^3$, where $\alpha = (\lambda_{1,-1}^3 + 3\lambda_{1,-1}^3\lambda_{1,0}^2)\lambda_{1,1}^{-2} = (3z_1^2+1)/(3z_1^2-1)^2$ is easily seen to be invertible in $\mathbb{Q}_1$. We deduce that $H_1$ is pseudo-degenerated with edges data $(q_2, m_2, P_2, N_2) = (2, 3, Z_2 - \alpha, 1)$. As $N_2 = 1$, we deduce that $F$ is balanced with $g = 2$. By Theorem 9 (assuming only $F$ monic), we get that $F$ has $f = \ell_1\ell_2 = 3$ irreducible factors over $\overline{\mathbb{K}}[[x]][y]$ of same degrees $e = q_1q_2 = 2$. Thanks to (32), we compute $B_0 = e = 2$, $B_1 = 0$, $B_2 = 3$ and $M_1 = 0$, $M_2 = 6$. By Theorem 9, we deduce that all factors of $F$ have same characteristic exponents $\mathrm{C}(F_i) = (B_0; B_2) = (2; 3)$ and same intersection sets $\Gamma_i(F) = (M_1, M_1) = (0, 0)$ as required.

## 9 Further comments

We conclude this paper with some ongoing work that will deserve further publication, providing the main perspectives. They are twofold. We start by discussing a way to factorize the input polynomial once non irreducibility has been discovered by our main algorithm. Then we discuss the more general context of polynomials defined over discrete valuation rings (e.g. $F \in \mathbb{Q}_p[y]$) and conclude by an open question concerning the assumption on the base field we are making in this paper.

**Analytic factorization.** Let's assume that $N_g > 1$. Then $\mathcal{N}_g(F)$ has two distinct edges, or its boundary polynomial factorizes. In both cases, if $v$ denotes the extended valuation defined by the lower edge of $\mathcal{N}_g(F)$, we get from the boundary polynomial two polynomials $G$ and $H$ such that $v(F - G\,H) > v(F)$. Then, using the classical Hensel Lemma [11, Section 15.4], we get a quadratic lifting of $G$ and $H$. As in [3], we start with euclidean division, denoting $\psi = \psi_g$ (it is important that $\psi$ is monic, so that $v(\psi) \geq 0$), and `QuoRem` the euclidean algorithm.

**Lemma 12.** *Let $A$, $B \in \mathbb{K}[[x]][y]$ such that $B$ is monic in $\psi$ (i.e. $B = \psi^b + \cdots$) and $v(B) = b\,v(\psi)$. Then, $Q, R =$ `QuoRem`$(A, B)$ satisfies $v(R) \geq v(A)$ and $v(Q) \geq v(A) - v(B)$.*

*Proof.* We focus on the computation of $R$. First note that it be computed as follows[6]: write $A = \sum_{i=0}^m a_i\,\psi^i$ the $\psi$-adic expansion of $A$, then compute $\tilde{A} = A - a_m\,B$, and apply recursively this strategy to $\tilde{A}$. As $\deg(\tilde{A}) < \deg(A)$, this procedure converges towards the unique remainder $R$. We now prove the result by induction on the degree of $A$. Nothing has to be done whe $\deg(A) < d$. When $\deg(A) = d$, then $A = c\,\psi^b$ with $c \in \mathbb{A}$ and result is straightforward for $\psi^d$ (we have $v(B - \psi^d) \geq v(B)$ by assumption). Finally, when $\deg(A) > d$, apply the above step $\tilde{A} = A - a_m\,B$. We have $v(a_m\,B) \geq v(A)$ so that $v(\tilde{A}) \geq v(A)$, and $\deg(\tilde{A}) < \deg(A)$, which proves the lemma for $R$ recursively. Result for $Q$ is then a straightforward consequence, as $v(Q\,B) = v(A - R)$. □

[6] in practice, we use the classical algorithm of $\mathbb{A}[y]$, this is only for this proof purpose

From this Lemma, it is trivial to show that the Hensel lemma, when starting with correct initial polynomials, "double the precision" according to an extended valuation $(v, \psi)$: given $F$, $G$, $H$, $S$, $T \in \mathbb{A}[Y]$ with $H$ monic in $\psi$, and $n \in \mathbb{N}^*$ satisfying,

- $v(F - G\,H) \geq v(F) + n$
- $v(S\,G + T\,H - 1) \geq n$ with $\deg(S) < \deg(H)$, $\deg(T) < \deg(G)$, $v(S) = -v(G)$ and $v(T) = -v(H)$.

it outputs polynomials $\tilde{G}$, $\tilde{H}$, $\tilde{S}$, $\tilde{T} \in \mathbb{K}[X, Y]$ with $\tilde{H}$ monic in $\psi$ such that:

- $v(F - \tilde{G}\,\tilde{H}) > v(F) + 2\,n$, with $v(\tilde{G} - G) \geq n + v(G)$ and $v(\tilde{H} - H) \geq n + v(H)$,
- $v(\tilde{S}\,\tilde{G} + \tilde{T}\,\tilde{H} - 1) > 2\,n$ ; $\deg(\tilde{T}) < \deg(\tilde{G})$, $\deg(\tilde{S}) < \deg(\tilde{H})$, $v(\tilde{S}) = -v(G)$ and $v(\tilde{T}) = -v(H)$.

We recall the algorithm (this is exactly [11, Algorithm 15.10]):

**Algorithm:** `HenselStep`$(F, G, H, S, T)$

1 $\alpha \leftarrow (F - G\,H)$;
2 $Q, R \leftarrow$ `QuoRem`$(S\,\alpha, H)$;
3 $\tilde{G} \leftarrow G + \alpha\,T + Q\,G$;
4 $\tilde{H} \leftarrow H + R$;
5 $\beta \leftarrow (S\,\tilde{G} + T\,\tilde{H}) - 1$;
6 $A, B \leftarrow$ `QuoRem`$(S\,\beta, \tilde{H})$;
7 $\tilde{S} \leftarrow S - B$;
8 $\tilde{T} \leftarrow T - \beta\,T - A\,\tilde{G}$;
9 **return** $\tilde{H}$, $\tilde{G}$, $\tilde{S}$, $\tilde{T}$

**Proposition 18.** *Algorithm* `HenselStep` *is correct.*

*Proof.* We have $F - \tilde{G}\,\tilde{H} = (1 - S\,G + T\,H)\,\alpha - S\,T\,\alpha^2 - (S\,G - T\,H)\,Q\,\alpha + G\,H\,Q^2$. By assumption, we have $v(\alpha) \geq v(F) + n$, $v(S\,T) = -v(F)$, and by Lemma 12, $v(Q) \geq n$. This shows $v(F - \tilde{G}\,\tilde{H}) > v(F) + 2\,n$. Similarly, $v(\tilde{G} - G) = v(T\,\alpha + Q\,G) \geq n + v(G)$ and $v(\tilde{H} - H) = v(R) \geq n + v(H)$. As for monicity of $\tilde{H}$, it is a obvious as $\deg(R) < \deg(H)$.

To conclude, as $\tilde{S}\,\tilde{G} + \tilde{T}\,\tilde{H} - 1 = \beta\,((\tilde{G} - G)\,S + (\tilde{H} - H)\,T - \beta)$, $v(\beta) \geq n$ (assumption), $v((\tilde{G} - G)\,S) > n$ and $v((\tilde{H} - H)\,T) > n$ (see above), we get $v(\tilde{S}\,\tilde{G} + \tilde{T}\,\tilde{H} - 1) > 2\,n$. As $v(B) > v(S)$ and $v(\beta\,T - A\,\tilde{G}) > v(T)$, we obsiously have $v(\tilde{S}) = -v(G)$ and $v(\tilde{T}) = -v(H)$. Condition $\deg(\tilde{S}) < \deg(\tilde{H})$ is obvious as $\deg(B) < \deg(\tilde{H})$. □

To conclude this paragraph, let us illustrate how to get the initial $G$, $H$, $S$ and $T$ with $H$ monic on an example.

**Example 9.** Consider $F = \psi^3 + y^2\,x^3\,\psi + x^6\,y \in \mathbb{Q}[[x]][y]$ with $\psi = y^3 - x^2$ and the associated valuation $V_1 = (3, 2, 6)$. Considering the lower edge $((1, 1), (3, 0))$, we get $V = (6, 4, 13)$. Then, we can initialise $G$ and $H$ as respectively $\psi^2 + y^2\,x^3$ and

$\psi$, so that $v(F - G\,H) = v(x^6\,y) = 40 > 39 = v(F)$. We then use the extended euclidean algorithm over $\mathbb{Q}[Z]$, getting $s = 1$ and $t = -Z$ such that $s\,(Z^2+1) + t\,Z = 1$. Then, we can multiply $s$ and $t$ by a monomial of valuation 26, so that $v(S) = -v(G)$ and $v(T) = - = v(H)$, getting $S = x^{-5}\,y$ and $T = -x^{-5}\,y\,\psi$. They indeed satisfy $v(S\,G + T\,H - 1) = v(x^{-2}\psi) = 1 > 0$.

Finally, not that finding the monomial $x^{-5}\,y$ in the above example is always possible (see e.g. [26, Lemma 4.23, page 24]).

Such a factorization done, we can recursively apply our main algorithm on each factor, factorising again if needed, until we get the full factorization. This provides an algorithm with complexity $\mathcal{O}(n\,\rho\,d)$ to get the $\rho$ factors separable from precision $n$, improving the bound $\mathcal{O}(n\,d^2)$ of [25, Proposition 7]. Nevertheless, this will not improve the overall complexity of [25, Section 7] (we might need to take $n = \delta$), and the divide and conquer strategy therein will still have to be used. Details concerning this algorithm will be presented in a forthcoming paper.

**Working over $\mathbb{A}[y]$ and small characteristic.** The algorithm using approximate roots described in our paper can be adapted to the case where for instance $F \in \mathbb{Q}_p[y]$, using $v_p$ instead of $v_x$ as initial valuation. In such a context, we would not define the valuations $v_k$ as in Section 3.1, but as augmented valuations (see [16, 17, 26] or [14, 19]). They would however be computed exactly as described in Section 3.4 or - equivalently - as in Definition 4 of Section 5. This strategy improves the computation of *optimal representatives of types* [13, Section 3]: the computed approximate root is actually always optimal (in the sense they described in [13]), and we do not need the *refinment process* anymore.

However, several points remain to be investigated: is there any need to use some "correcting terms" as we are doing here with the morphisms $\lambda_k$ ? And how to deal with the case where the characteristic of the field divides $d$ (or more generally is less than $d$ when considering the factorization algorithm described above), in which case Proposition 3 does not make sense anymore. These points are being studied by the authors at the time of the writing, and will be the topic of a further paper.

**Computing Puiseux series using approximate roots ?** As mentioned in Remark 17, our strategy does not compute all terms of the Puiseux series of the input polynomial. However, there might be ways to compute them. We here comment a few special cases. First note that the coefficients corresponding to integer exponents are given by the $d$-th approximate root. Then, if $N_1 = d/2$, we then have $\psi_1 = \psi_0^2 + X^{m_1}\,S_1(X)^2$, so that $S_1(X)$ can be computed via quadratic Newton iteration (this provides all coefficients corresponding to exponents with denominator 2). When $q_1 > 2$, one can probably compute additional coefficients of the Puiseux series by solving a linear system. For instance, the case $q_1 = 3$ can be dealt with as follows: if $S_1(x) = x^{\frac{1}{3}}\,P_1(x) + x^{\frac{2}{3}}\,P_2(x)$, then we have $\psi_1 = \psi_0^3 - 3\,x\,P_1\,P_2\,\psi_0 - x\,P_1^3 - x^2\,P_2^3$, defining the linear system to solve.

## References


[1] S. S. Abhyankar. Irreducibility criterion for germs of analytic functions of two complex variables. *Adv. Mathematics*, 35:190–257, 1989.

[2] J.-D. Bauch, E. Nart, and H. Stainsby. Complexity of the OM factorizations of polynomials over local fields. *LMS Journal of Computation and Mathematics*, 16:139–171, 2013.

[3] X. Caruso, D. Roe, and T. Vaccon. Division and slope factorization of p-adic polynomials. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 159–166, New York, NY, USA, 2016. ACM.

[4] E. Casas-Alvero. *Plane curve singularities*, volume 276 of *LMS Lecture Notes*. Cambridge University Press, 2000.

[5] V. Cossart and G. Moreno-Socías. Irreducibility criterion: a geometric point of view. *Fields Inst. Commun.*, 33:27–42, 2003.

[6] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *EUROCAL 85*. Springer-Verlag LNCS 204, 1985.

[7] D. Duval. Rational Puiseux expansions. *Compositio Math.*, 70(2):119–154, 1989.

[8] E. R. Garciá Barroso. Invariants des singularités de courbes planes et courbure des fibres de milnor. *Phd Tesis*, ftp://tesis.bbtk.ull.es/ccppytec/cp16.pdf, 1995.

[9] E. R. Garciá Barroso and J. Gwoździewicz. Characterization of jacobian newton polygons of plane branches and new criteria of irreducibility. *Ann. Institut Fourier*, 60(2):683–709, 2010.

[10] E. R. Garciá Barroso and J. Gwoździewicz. A discriminant criterion of irreducibility. *Kodai Math. J.*, 35:403–414, 2012.

[11] J. v. z. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 3rd edition, 2013.

[12] I. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Birkhäuser, 1994.

[13] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. Théor. Nombres Bordx.*, 23(3):667–696, 2011.

[14] J. Guàrdia, J. Montes, and E. Nart. Newton polygons of higher order in algebraic number theory. *Transsactions of the American Mathematical Society*, 364:361–416, 2012.

[15] E. Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *J. ACM*, 35(1):231–264, Jan. 1988.

[16] S. Mac Lane. A construction for prime ideals as absolute values of an algebraic field. *Duke Math. J.*, 2(3):492–510, 1936.

[17] S. MacLane. A construction for absolute values in polynomial rings. *Trans. Amer. Math. Soc.*, 40(3):363–395, 1936.

[18] M. Merle. Invariants polaires des courbes planes. *Inventiones Math.*, 41:103–111, 1977.

[19] J. M. Peral. *Polígonos de newton de orden superior y aplicaciones aritméticas*. PhD thesis, Universitat de Barcelona, 1999.

[20] P. Popescu-Pampu. Approximate roots. *Fields Institute Communiations*, 33:1–37, 2002.

[21] A. Poteaux. *Calcul de développements de Puiseux et application au calcul de groupe de monodromie d'une courbe algébrique plane*. PhD thesis, Université de Limoges, 2008.

[22] A. Poteaux and M. Rybowicz. Complexity bounds for the rational newton-puiseux algorithm over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 22:187–217, 2011. 10.1007/s00200-011-0144-6.

[23] A. Poteaux and M. Rybowicz. Good reduction of puiseux series and applications. *Journal of Symbolic Computation*, 47(1):32 – 63, 2012.

[24] A. Poteaux and M. Rybowicz. Improving complexity bounds for the computation of puiseux series over finite fields. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '15, pages 299–306, New York, NY, USA, 2015. ACM.

[25] A. Poteaux and M. Weimann. Computing Puiseux series: a fast divide and conquer algorithm. Preprint, 2017.

[26] J. Rüth. *Models of curves and valuations*. PhD thesis, Universität Ulm, 2014.

[27] J. Teitelbaum. The computational complexity of the resolution of plane curve singularities. *Math. Comp.*, 54(190):797–837, 1990.

[28] J. van der Hoeven. Relax, but don't be too lazy. *JSC*, 34:479–542, 2002.

[29] J. Van Der Hoeven and G. Lecerf. Accelerated tower arithmetic. Preprint, 2018.

[30] J. Van Der Hoeven and G. Lecerf. Directed evaluation. Preprint, 2019.

[31] M. van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *J. Symb. Comp.*, 18:353–363, 1994.

[32] C. Wall. *Singular Points of Plane Curves*. London Math. Soc., 2004.

[33] P. G. Walsh. A polynomial-time complexity bound for the computation of the singular part of an algebraic function. *Math. of Comp.*, 69:1167–1182, 2000.

[34] M. Weimann. Bivariate factorization using a critical fiber. *Journal of Foundations of Computational Mathematics*, pages 1–45, 2016.

[35] O. Zariski. Studies in equisingularity i. *American J. Math*, 87:507–535, 1965.

[36] O. Zariski. Le problème des modules pour les branches planes. *Centre de Maths de l'X*, 1973.