A quasi-linear irreducibility test in K[[x]][y]

Adrien Poteaux, Martin Weimann

A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$

Adrien POTEAUX[1] and Martin WEIMANN[2]

[1]University of Lille, France
[2]University of French Polynesia, France

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 generalisation of Abhyankhar's irreducibility criterion to the case of non algebraically closed residue fields.

1 Introduction

Factorisation of polynomials defined over a ring of formal power series is an important issue of symbolic computation, with a view towards singularities of algebraic plane curves. In this paper, we develop a fast irreducibility test. In all of the sequel, we assume that $F \in \mathbb{K}[[x]][y]$ is a square-free Weierstrass polynomial defined over a perfect field $\mathbb{K}$ of characteristic 0 or greater than $d = \deg(F)$. We let δ stand for the x-valuation of the discriminant of F. We prove:

Theorem 1. *We can test if F is irreducible in $\mathbb{K}[[x]][y]$ with an expected $\mathcal{O}^{\sim}(\delta)$ operations over $\mathbb{K}$ and one univariate irreducibility test over $\mathbb{K}$ of degree at most d.*

If F is irreducible, the algorithm computes also its discriminant valuation δ, its index of ramification e and its residual degree f. As usual, the notation $\mathcal{O}^{\sim}()$ hides logarithmic factors ; see Section 5.1 for details. Up to our knowledge, this improves the best current complexity $\mathcal{O}^{\sim}(d\,\delta)$ [21, Section 3].

Our algorithm is Las Vegas, due to the computation of primitive elements[1] in the residue field extensions. In particular, if we test the irreducibility of F in $\overline{\mathbb{K}}[[x]][y]$, it becomes deterministic without univariate irreducibility test. The algorithm extends to non Weierstrass polynomials, but with complexity $\mathcal{O}^{\sim}(\delta+d)$ and at most two univariate irreducibility tests. If $F \in \mathbb{K}[x,y]$ is given as a square-free bivariate polynomial of bidegree (n,d),

[1]One should get a deterministic complexity $\mathcal{O}(\delta^{1+o(1)}\log^{1+o(1)}(d))$ thanks to the recent preprint [11].

we have $\delta < 2nd$, hence our algorithm is quasi-linear with respect to the arithmetic size nd of the input F. Moreover, we can avoid the square-free hypothesis in this case. These extended results are discussed in Subsection 5.5.

Main ideas. We recursively compute some well chosen approximate roots $\psi_0, \ldots, \psi_g$ of F, starting with ψ_0 the d^{th} approximate roots of F. At step $k+1$, we build the $(\psi_0, \ldots, \psi_k)$-adic expansion of F. We compute an induced generalised Newton polygon of F and check if it is straigth. If not, then F is reducible and the algorithm stops. Otherwise, we construct a related boundary polynomial (quasi-homogeneous and defined over some field extenion of $\mathbb{K}$) and test if it is the power of some irreducible polynomial. If not, then F is reducible and the algorithm stops. Otherwise, we deduce the degree of the next approximate root ψ_{k+1}. The degrees of the ψ_k's are strictly increasing and F is irreducible if and only if we reach $\psi_g = F$. 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.

Related results. Factorisation of polynomials defined over a ring of formal power series is an important issue in the algorithmic of algebraic curves, both for local aspects (classification of plane curves singularities) and for global aspects (integral basis of function fields [26], geometric genus of plane curves [21], bivariate factorisation [28], 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. [4, 5, 17–21, 24, 27] and the references therein). Up to our knowledge, the best current arithmetic complexity was obtained in [21], 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 $\mathcal{O}^{\sim}(d\,\delta)$ operations over $\mathbb{K}$. There exists also other methods for factorisation, as the Montes algorithm which allow to factor polynomials over general local fields [9, 15] 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 Φ-adic expansion of F, where Φ 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 $\mathcal{O}^{\sim}(d^2 + \delta^2)$ [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 [13, 14, 23]. 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 [3].

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

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 [6, 7] 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.

Organisation. In Section 2, we recall results of [20, 21], namely an improved version of the rational Newton-Puiseux algorithm of Duval [5]. From this algorithm we fix several notations and define a collection Φ of minimal polynomials of some truncated Puiseux series of F. We then show in Section 3 how to recover the edge data of F from its Φ-adic expansion. In Section 4, we show that Φ can be replaced by a collection Ψ of well chosen approximate roots of F, which can be computed in the aimed complexity bound. Section 5 is dedicated to complexity issues and to the proof of Theorem 1 ; in particular, we delay discussions on truncations of powers of x to this section. Finally, we give in Section 6 a new proof of Abhyankhar's absolute irreducibility criterion.

2 A Newton-Puiseux type algorithm

2.1 Classical definitions

Let $F = \sum_{i=0}^{d} a_i(x)\, y^i = \sum_{i,j} a_{ij} x^j y^i \in \mathbb{K}[[x]][y]$ be a Weierstrass polynomial, that is $a_d = 1$ and $a_i(0) = 0$ for $i < d$ (the general case will be considered in Section 5.5). We let v_x stand for 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 $i = 0, \dots, d$.

It is well known that if F is irreducible, then $\mathcal{N}(F)$ is straight (a single point being straight by convention). However, this condition is not sufficient.

Definition 2. We call $\bar{F} := \sum_{(i,j)\in\mathcal{N}(F)} a_{ij} x^j y^i$ the *boundary polynomial* of F.

Definition 3. We say that F is *degenerated* over $\mathbb{K}$ 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 $\mathcal{N}(F)$ is straight of slope $-m/q$ with q, m coprime, $q > 0$, and if

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

with $c \in \mathbb{K}^\times$, $N \in \mathbb{N}$ and $P \in \mathbb{K}[Z]$ monic and irreducible. We call P the *residual polynomial* 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.

2.2 A Newton-Puiseux type irreducibility test

We can associate to F a sequence of Weierstrass polynomials $H_0, \ldots, H_g$ of strictly decreasing degrees $N_0, \ldots, N_g$ such that either $N_g = 1$ and F is irreducible, either H_g is not degenerated and F is reducible.

• **Rank** $k = 0$. Let $N_0 = d$ and $\mathbb{K}_0 = \mathbb{K}$. We define $c_0(x) := -\mathrm{coeff}(F, y^{N_0-1})/N_0$ and let

$$H_0(x, y) := F(x, y + c_0(x)) \in \mathbb{K}_0[[x]][y].$$

Then H_0 is a new Weierstrass polynomial of degree N_0 with no terms of degree $N_0 - 1$. If $N_0 = 1$ or H_0 is not degenerated, we let $g = 0$.

• **Rank** $k > 0$. Suppose given $\mathbb{K}_{k-1}$ a field extension of $\mathbb{K}$ and $H_{k-1} \in \mathbb{K}_{k-1}[[x]][y]$ a degenerated Weierstrass polynomial of degree N_{k-1}, with no terms of degree $N_{k-1} - 1$. Denote (q_k, m_k, P_k, N_k) its edge data and $\ell_k = \deg(P_k)$. We let z_k stands for the residue class of Z_k in the field $\mathbb{K}_k := \mathbb{K}_{k-1}[Z_k]/(P_k(Z_k))$. We define (s_k, t_k) to be the unique positive integers such that $q_k s_k - t_k m_k = 1$, $0 \leq t_k < q_k$. As H_{k-1} is degenerated, we deduce from (1) that

$$H_{k-1}(z_k^{t_k} x^{q_k}, x^{m_k}(y + z_k^{s_k})) = x^{q_k m_k \ell_k N_k}\, G_k\, V_k, \tag{2}$$

where $V_k \in \mathbb{K}_k[[x, y]]$ is a unit and $G_k \in \mathbb{K}_k[[x]][y]$ is a Weierstrass polynomial of degree N_k which can be computed up to an arbitrary precision via Hensel lifting. We let $c_k := -\mathrm{coeff}(G_k, y^{N_k-1})/N_k$ and define

$$H_k(x, y) = G_k(x, y + c_k(x)) \in \mathbb{K}_k[[x]][y]. \tag{3}$$

It is a degree N_k Weierstrass polynomial with no terms of degree $N_k - 1$.

• **The N_k-sequence stops.** We have the relations $N_k = q_k \ell_k N_{k-1}$. As H_{k-1} is degenerated with no terms of degree $N_{k-1} - 1$, we must have $q_k \ell_k > 1$. Hence the sequence of integers $N_0, \ldots, N_k$ is strictly decreasing and there exists a smallest index g such that either $N_g = 1$ and $H_g = y$ or $N_g > 1$ and H_g is not degenerated. We collect the edge data of the polynomials $H_0, \ldots, H_{g-1}$ in a list

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

Note that $m_k > 0$ for all $1 \leq k \leq g$.

Proposition 1. *The polynomial F is irreducible if and only if $N_g = 1$.*

Proof. Follows from the rational Puiseux algorithm of Duval [5] (which is based on the transform (2)) combined with the "Abhyankhar's trick" (3) introduced in [20]. □

Following [21], we denote by `ARNP` the underlying algorithm. By considering suitable sharp truncation bounds, it is shown in [21, Section 3] that this algorithm performs an expected $\mathcal{O}(d\,\delta)$ arithmetic operations (this requires algorithmic tricks, especially

dynamic evaluation and primitive representation of residue fields). Unfortunately, the worst case complexity of this algorithm is $\Omega(d\,\delta)$, which is too high for our purpose. The main reason is that computing the intermediate polynomials G_k in (2) via Hensel lifting up to sufficient precision requires to compute $H_{k-1}(z_k^{t_k} x^{q_k}, x^{m_k}(y + z_k^{s_k}))$, that might have a size $\Omega(d\,\delta)$, as shows the following example.

Example 1. Consider $F = (y^\alpha - x^2)^2 + x^\alpha \in \mathbb{C}[[x]][y]$ with $\alpha > 4$ odd. We have $d = 2\,\alpha$, $\delta = 2\,\alpha^2 - 4\,\alpha + 4$, $H_0 = F$ and q_1, m_1, z_1 are respectively $\alpha, 2$ and 1. Applying results of [21, Section 3], one can show that an optimal truncation bound to compute G_1 is $\alpha^2 - 4\,\alpha + 1$. But the size of $H_0(x^\alpha, x^2\,(y+1))/x^{4\,\alpha} \mod x^{\alpha^2 - 4\,\alpha + 1}$ is $\Theta(\alpha^3) = \Theta(d\,\delta)$.

To solve this problem we will rather compute the boundary polynomial $\bar{H}_k$ using the $(\psi_0, \ldots, \psi_k)$-adic expansions of F, where the ψ_k's are well chosen approximate roots. As a first step towards the proof of this result, we begin by using a sequence $(\phi_0, \ldots, \phi_k)$ of minimal polynomials of F that we now define.

2.3 Minimal polynomials of truncated rational Puiseux expansions

Rational Puiseux Expansions. We keep notations of Section 2.2. We denote $\pi_0(x, y) = (x, y + c_0(x))$ and define inductively $\pi_k = \pi_{k-1} \circ \sigma_k$ where

$$\sigma_k(x, y) := (z_k^{t_k} x^{q_k}, x^{m_k}(y + z_k^{s_k} + c_k(x))) \tag{4}$$

for $k \geq 1$. It follows from (2) and (3) that there exists $v_k(F) \in \mathbb{N}$ such that

$$\pi_k^* F = x^{v_k(F)}\, H_k\, U_k \in \mathbb{K}_k[[x]][y], \tag{5}$$

with $U_k(0, 0) \in \mathbb{K}_k^\times$. This key point will be used several time in the sequel.

We deduce from (4) that

$$\pi_k(x, y) = (\mu_k x^{e_k}, \alpha_k x^{r_k} y + S_k(x)), \tag{6}$$

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 $v_x(S_k) \leq r_k$. Following [21], we call the pair

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

a (truncated) rational Puiseux parametrisation. This provides the roots of F (namely Puiseux series) truncated up to precision $\frac{r_k}{e_k}$, that increases with k [21, Section 3.2].

Minimal polynomials. It can be shown that the exponent e_k is coprime with the gcd of the support of S_k, and that the coefficients of the parametrisation $(\mu_k x^{e_k}, S_k)$ generate the current residue field extension $\mathbb{K}_k$ over $\mathbb{K}$ (see e.g. [5, Theorems 3 and 4]). It follows that there exists a unic monic irreducible polynomial $\phi_k \in \mathbb{K}[[x]][y]$ such that

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

where $f_k := [\mathbb{K}_k : \mathbb{K}] = \ell_1 \cdots \ell_k$. We call ϕ_k the k^{th} *minimal polynomial* of F. Note that $\phi_0 = y - c_0(x)$ and that we have the relations $d = N_k\, d_k$ for $k = 0, \ldots, g$.

By construction, a function call $\texttt{ARNP}(\phi_k)$ generates the same transformations π_i for $i \leq k$. In particular, we have

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

3 Edge data from the Φ-adic expansion

Let us fix an integer $0 \leq k \leq g$ and assume that $N_k > 1$. We keep using notations of Section 2. Assuming that we know the edge data $(q_1, m_1, P_1, N_1), \ldots, (q_k, m_k, P_k, N_k)$ of the Weierstrass polynomials $H_0, \ldots, H_{k-1}$, together with the minimal polynomials $\phi_0, \ldots, \phi_k$, we want to compute the boundary polynomial of the next Weierstrass polynomial H_k. In the following, we will omit for readibility the index k for the sets Φ, $\mathcal{B}$, V and Λ defined below.

3.1 Main results

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

$$\mathcal{B} := \{(b_{-1}, \ldots, b_k) \in \mathbb{N}^{k+2}\ ,\ b_{i-1} < q_i\, \ell_i\, , i = 1, \ldots, k\} \tag{8}$$

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 Φ-adic expansion of F. We have $b_k \leq N_k$ 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 compute $\bar{H}_k$ from the Φ-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 (6), we deduce that the pull-back morphism π_k^* is injective, so that v_k defines a discrete valuation. This is a valuation of transcendence degree one, thus an augmented valuation [23, Section 4.2], in the flavour of MacLane valuations [13, 14, 23] or Montes valuations [9, 15]. Note that $v_0(H) = v_x(H)$. We associate to Φ the vector

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

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

$$w_i := \min\{\langle B, V\rangle,\ b_k = i,\ f_B \neq 0\} - v_k(F) \tag{9}$$

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

Theorem 2. *The Newton polygon of H_k is the lower convex hull of $(i, w_i)_{0\leq i\leq N_k}$.*

This result leads us to introduce the sets

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

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 tc_y stands for the trailing coefficient with respect to y. We associate to Φ the vector

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

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

Theorem 3. *Let $B_0 := (0, \ldots, 0, N_k)$. The boundary polynomial $\bar{H}_k$ of H_k equals*

$$\bar{H}_k = \sum_{(i,w_i)\in\mathcal{N}(H_k)} \left(\sum_{B\in\mathcal{B}(i,w_i+v_k(F))} f_B \Lambda^{B-B_0}\right) x^{w_i} y^i. \tag{10}$$

Combined with the formulas (14) of Section 3.4 for the vectors V and Λ, Theorems 2 and 3 give an efficient way to decide if the Weierstrass polynomial H_k is degenerated, and if so, to compute its edge data.

Example 2. 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 2 stands from Definition 1. Moreover, $\mathcal{B}(i, w_i)$ is then reduced to the point (i, w_i) and Theorem 3 stands from Definition 2.

3.2 Proof of Theorems 2 and 3

Let us first establish some basic properties of the minimal polynomials ϕ_i of F. Given a ring $\mathbb{A}$, we denote by $\mathbb{A}^\times$ the subgroup of units. Note that $U \in \mathbb{A}[[x,y]]^\times$ if and only if $U(0,0) \in \mathbb{A}^\times$. For $-1 \leq i \leq k$, we introduce the notations

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

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.:*

1. $\pi_k^*(\phi_i) = x^{v_{k,i}}\, U_{k,i}$ *if* $i < k$,
2. $\pi_k^*(\phi_k) = x^{v_{k,k}}\, y\, U_{k,k}$.

Proof. As $\texttt{ARNP}(\phi_k)$ generates the same transform π_k, we deduce from (5):

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

with $U \in \mathbb{K}_k[[x,y]]^\times$ and $\beta \in \mathbb{K}_k[[x]]$. From (6) 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 λ_k. First equality is then obtained by applying the pull-backs σ_j^*, $j = i+1, \ldots, k$ to $\pi_i^*(\phi_i) = x^{v_{i,i}}\, y\, U_{i,i}$. □

Corollary 1. *With the standard notations for intersection multiplicities and resultants, we have for any $G \in \mathbb{K}[[x]][y]$ Weierstrass:*

$$v_k(G) = \frac{(G,\phi_k)_0}{f_k} = \frac{v_x(Res_y(G,\phi_k))}{f_k}.$$

Proof. As $v_x(S_k) \leq r_k$, we get from (6) $v_k(G) = v_x(\pi_k^*(G)) = v_x(G(\mu_k x^{e_k}, S_k(x)))$. But this last integer coincides with the intersection multiplicity of ϕ_i with any one of the f_k conjugate plane branches (i.e. irreducible factor in $\overline{\mathbb{K}}[[x]][y]$) of ϕ_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. Using point 2 of Lemma 1 at rank $k-1$ and equality $\pi_k^*(\phi_{k-1}) = \sigma_k^* \circ \pi_{k-1}^*(\phi_{k-1})$, we get

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

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 2 of Lemma 1. Items 1 and 3 follow. Similarly, using point 1 of Lemma 1 at rank $k-1$, we get for $i < k-1$

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

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

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

Proposition 2. *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

$$\sum_{B \in \mathcal{B}(0,w)} c_B \Lambda^B = \sum_{B \in \mathcal{B}(0,w)} c_B \lambda_{k,-1}^{b_{-1}} \cdots \lambda_{k,k-1}^{b_{k-1}} = 0. \tag{11}$$

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

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

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

$$q_k N_B = b_{k-1}(q_k s_k - m_k t_k) + t_k \sum_{j=-1}^{k-1} b_j v_{k,j} = b_{k-1} + t_k w, \tag{12}$$

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 (12) that $N_B = n + \alpha$ where $n = \lceil t_k w / q_k \rceil$ and $0 \leq \alpha < \ell_k$. Dividing (11) by z_k^n and using $\Lambda^B = \mu_B z_k^{N_B}$, we get

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

Since $a_\alpha \in \mathbb{K}_{k-1}$ and $z_k \in \mathbb{K}_k$ has minimal polynomial P_k of degree ℓ_k over $\mathbb{K}_{k-1}$, this implies $a_\alpha = 0$ for all $0 \leq \alpha < \ell_k$, i.e., using (12):

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

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* $\pi_k^*(G) = x^w\, y^i\, \tilde{U}$ *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 π_k^*, denoting $U = (U_{k,-1}, \ldots, U_{k,k})$ with $U_{k,i}$ defined in Lemma 1, we have

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

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

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

As $\sum_{B\in\mathcal{B}(i,w)} g_B\Lambda^B \neq 0$ by Proposition 2, the first two equalities follows. The last two equalities follow from the definitions of $v_k(G)$ and $\lambda_k(G)$. □

Proof of Theorems 2 and 3. 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 π_k^* implies

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

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. As H_k is Weierstrass of degree N_k, it follows from this formula combined with (5), that $\mathcal{N}(H_k)$ coincides with the lower convex hull of the points (i, w_i), $i = 0, \ldots, N_k$, proving Theorem 2. More precisely, we deduce that there exists $\mu \in \mathbb{K}_k^\times$ such that

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

As $\bar{H}_k$ is Weierstrass of degree N_k, then $w_{N_k} = 0$ and $w_i > 0$ for $i < N_k$. The previous equation forces

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

But F and ϕ_k being monic of respective degrees d and d_k, the vector $B_0 = (0, \ldots 0, N_k) \in \mathcal{B}$ is the unique exponent in the Φ-adic expansion of F with last coordinate $b_k = N_k = d/d_k$ and we have moreover $f_{B_0} = 1$. This forces $\mathcal{B}(N_k, v_k(F)) = \{B_0\}$ and we get $\mu = \Lambda^{B_0}$, thus proving Theorem 3. □

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

In order to use Theorems 2 and 3 for computing the edge data of H_k, we need to compute $v_{k,k} = v_k(\phi_k)$, $\lambda_{k,k} = \lambda_k(\phi_k)$, $v_k(F)$ and $\lambda_k(F)$ in terms of the previously computed edge data $(q_1, m_1, P_1, N_1), \ldots, (q_k, m_k, P_k, N_k)$ 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 2 and 3 that $\mathcal{B}(N_k, v_k(F)) = \{B_0\}$ with $B_0 = (0, \ldots, 0, N_k)$. By definition of $\mathcal{B}(N_k, v_k(F))$, we get the first point. From the definition of λ_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 $\mathrm{tc}_y\left(\bar{F}_k(0,y)\right) = \Lambda^{B_0}$. □

Proposition 3. *For any $1 \leq k \leq g$, we have the equalities*

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

Proof. To simplify the notations of this proof, let us denote $w = v_{k-1}(\phi_k)$, $\gamma = \lambda_{k-1}(\phi_k)$ and $(m, q, s, t, \ell, z) = (m_k, q_k, s_k, t_k, \ell_k, z_k)$. Remember from Section 2 that by definition of ϕ_k, both ϕ_k and F generate the same transformations σ_i and τ_i for $i \leq k$. As in (5), 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

$$\pi_k^*(\phi_k) = z^{t(w+m\ell)}\, x^{q\,(w+m\ell)}\,((\gamma + y\,R_2)\,G_k + x\,R)\,. \tag{13}$$

As $G_k(0,y)$ is not identically zero, we deduce from (13) 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 get $G_k(0,0) = P_k(z_k) = 0$ and $\partial_y G_k(0,0) = qz^{1-s}P_k'(z) \neq 0$. Combined with (13), this gives

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

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

3.4 Simple formulas for V and Λ

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 Λ 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 formulas:

$$\begin{cases} v_{k,i} = q_k v_{k-1,i} & -1 \leq i < k-1 \\ v_{k,k-1} = q_k v_{k-1,k-1} + m_k \\ v_{k,k} = q_k \ell_k v_{k,k-1} \end{cases} \qquad \begin{cases} \lambda_{k,i} = \lambda_{k-1,i} z_k^{t_k v_{k-1,i}} & -1 \leq i < k-1 \\ \lambda_{k,k-1} = \lambda_{k-1,k-1} z_k^{t_k v_{k-1,k-1} + s_k} \\ \lambda_{k,k} = q_k z_k^{1-s_k-\ell_k} P_k'(z_k) \lambda_{k,k-1}^{q_k \ell_k} \end{cases} \tag{14}$$

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 Φ-adic expansion of F, the updated lists V and Λ allow to compute in an efficient way the boundary polynomial $\bar{H}_k$ using formulas (9) and (10). Unfortunately, we do not know a way to compute the minimal polynomials ϕ_k in our aimed complexity bound: the computation of the $y^{N_k - 1}$ coefficient of G_k up to some suitable precision might cost $\Omega(d\,\delta)$ as explained in Section 2.

We now show that the main conclusions of all previous results remain true if we replace ϕ_k by the N_k^{th}-approximate root ψ_k of F, with the great advantage that these approximate roots can be computed in the aimed complexity (see Section 5). Up to our knowledge, such a strategy was introduced by Abhyankar who developped in [1] an irreducibility criterion in $\overline{\mathbb{K}}[[x, y]]$ avoiding 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 4. (*see e.g.* [16, 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 ψ is the N^{th}-approximate root of F if and only if the ψ-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 $\phi \in \mathbb{A}[y]$ monic of degree d/N and given $F = \sum_{i=0}^{N} a_i \phi^i$ the ϕ-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. [16, Proof of Proposition 6.3]). Hence, after applying at most d/N times the operator τ_F, the coefficient a'_{N-1} vanishes and the polynomial $\tau_F \circ \cdots \circ \tau_F(\phi)$ coincides with the approximate root ψ of F. Although this is not the best strategy from a complexity point of view (see Section 5), this construction will be used to prove Theorem 4 below.

Main result. We still consider $F \in \mathbb{K}[[x]][y]$ Weierstrass of degree d and keep notations from Section 2. We denote $\psi_{-1} := x$ and, for all $k = 0, \ldots, g$, we denote ψ_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 Ψ-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 (8). In the following, we denote by $w'_i \in \mathbb{N}$ the new integer defined by (9) 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 (10).

Theorem 4. *We have $\bar{H}_k = \bar{H}'_k$ for $0 \leq k < g$ and the boundary polynomials $\bar{H}_g$ and $\bar{H}'_g$ have same restriction to their Newton polygon's lowest edge.*

In other words, Theorems 2 and 3 hold when replacing minimal polynomials by approximate roots, up to a minor difference when $k = g$ that has no impact for degeneracy tests.

Intermediate results. The proof of Theorem 4 requires several steps. We denote by $-m_{g+1}/q_{g+1}$ the slope of the lowest 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 $(q, m) = (q_{k+1}, m_{k+1})$. The lemma is true if $\psi_k = \phi_k$ and ψ_k is obtained after successive applications of the operator τ_F to ϕ_k. It is thus sufficient to prove

$$v_k(\phi - \phi_k) > v_k(\phi_k) + m/q \Longrightarrow v_k(\tau_F(\phi) - \phi_k) > v_k(\phi_k) + m/q$$

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

$$v_k(a_{N_k - 1}) > v_k(\phi_k) + m/q. \tag{15}$$

• *Case* $\phi = \phi_k$. As $\phi_0 = \psi_0 = y + c_0$, we do not need to consider the case $k = 0$. Let $k \geq 1$. Theorem 2 and Lemma 3 give $v_k(a_{N_k-1}) \geq v_k(F) + m/q = N_k\, v_k(\phi_k) + m/q$. Note that $v_k(\phi_k) > 0$ when $k \geq 1$ by construction. We are thus done when $N_k > 1$. But $N_k = 1$ means $k = g$ and $H_g = y$, so that $v_g(a_0) = \infty$. 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

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

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

$$\pi_k^*(a_i\phi^i) = x^{\alpha_i}\,(y + x^\alpha U)^i\,U_i, \tag{16}$$

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, α_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 (5) 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 lowest edge Δ 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 Δ. 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 5. *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 5 holds for all $k' < k$. 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 π_{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 $\tilde{U} \in \mathbb{K}_{k-1}[[x, y]]^\times$. We deduce $\pi_k^*(\psi_{k-1}) = \pi_k^*(\phi_{k-1}) + x^{q_k\alpha} U_\alpha$ with $U_\alpha \in \mathbb{K}_k[[x, y]]^\times$ and $q_k\,\alpha > v_k(\phi_{k-1})$ using Lemma 2 ($q_k\, v_{k-1,k-1} + m_k = v_{k,k-1}$). This forces $v_k(\psi_{k-1}) = v_k(\phi_{k-1})$ 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 $U_i(0, 0) = 1$ (second equality by induction). Applying σ_k^* and using Lemma 2, we conclude in the same way $v_k(\psi_i) = v_k(\phi_i)$ and $\lambda_k(\psi_i) = \lambda_k(\phi_i)$. □

Corollary 3. *Let G of degree less than d_k and $\sum g'_B \Psi^B$ its Ψ-adic expansion. 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 Φ-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 5, 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 2. □

Proof of Theorem 4. Write $F = \sum_i a_i \psi_k^i$ the ψ_k-adic expansion of F. Similarly to (16), when $a_i \neq 0$, Corollary 2 and Lemma 4 imply:

$$\pi_k^*(a_i \psi_k^i) = x^{v_k(a_i \psi_k^i)} \, (y + x^\alpha \, \tilde{U})^i \, U, \tag{17}$$

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 lowest edge Δ of the Newton polygon of H_k (hence the whole 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 5. This shows that we may replace w_i by w'_i in (9). More precisely, it follows from (17) that the restriction $\bar{H}_{k|\Delta}$ of $\bar{H}_k$ to Δ is uniquely determined by the equality

$$\lambda_k(F) x^{v_k(F)} \bar{H}_{k|\Delta} = \sum_{(i,w'_i) \in \Delta} \lambda_k(a_i \psi_k^i) x^{v_k(a_i \psi_k^i)} y^i.$$

Using again Corollary 3 and Proposition 5, we get

$$\bar{H}_{k|\Delta} = \sum_{(i,w'_i) \in \Delta} \left(\sum_{B \in \mathcal{B}(i, w'_i + v_k(F))} f'_B \Lambda^{B - B_0} \right) x^{w'_i} y^i,$$

as required. □

Remark 1. Theorem 4 would still hold when replacing ψ_k by any monic polynomial ϕ of same degree for which $\pi_k^*(\phi) = x^{v_{k,k}} \, (y + \beta(x)) \, U$ with $v_x(\beta) > m_{k+1}/q_{k+1}$.

4.2 An Abhyankar type irreducibility test

Theorem 4 leads to the following sketch of algorithm. Subroutines `AppRoot`, `Expand` and `BoundaryPol` respectively compute the approximate roots, the Ψ-adic expansion and the current lowest boundary polynomial (using (9) and (10)). They are detailed in Section

5. Also, considerations about truncation bounds is postponed to Section 5.2. Given a ring $\mathbb{L}$ and $P \in \mathbb{L}[Z]$, we denote by $\mathbb{L}_P = \mathbb{L}[Z]/(P(Z))$.

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

Input: $F \in \mathbb{K}[[x]][y]$ Weierstrass 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, Ψ);
  $\bar{H} \leftarrow$ `BoundaryPol`(F, Ψ, V, Λ);
  if $\bar{H}$ *is not degenerated over* $\mathbb{L}$ **then return** *`False`*;
  $(q, m, P, N) \leftarrow$ `EdgeData`$(\bar{H})$;
  Update the lists V, Λ using (14);
  $\mathbb{L} \leftarrow \mathbb{L}_P$
return *`True`*

Theorem 5. *Algorithm* *`Irreducible`* *returns the correct answer.*

Proof. This follows from Theorem 2, 3 and 4, together with Proposition 1. □

Let us illustrate this algorithm on two simple examples.

Example 3. Let $F(x,y) = (y^2 - x^3)^2 - x^7$. This example was suggested by Kuo who asked 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 $\Lambda = (1,1)$.

Step k=0. The 4^{th} approximate root of F is $\psi_0 = y$. So $H_0 = F$ and we deduce from (10) (see Exemple 2) 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 (14), using here $z_1 = 1 \mod P_1$.

Step k=1. The 2^{nd} approximate root of F is $\psi_1 = y^2 - x^3$ and F has Ψ-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 (10) 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 4. 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 $\Lambda = (1,1)$.

Step k=0. The 8^{th} approximate root of F is $\psi_0 = y$. The monomials reaching the minimal values (9) in the $\Psi = (\psi_{-1}, \psi_0)$-adic expansion of F are ψ_0^8, $-4\psi_{-1}^3\psi_0^6$, $6\psi_{-1}^6\psi_0^4$, $-4\psi_{-1}^9\psi_0^2$, ψ_{-1}^{12} and we deduce from (10) 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 (14), 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 Ψ-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 (9) are ψ_1^4, $8\psi_{-1}^8\psi_1^2$, $16\psi_{-1}^{16}$ and we deduce from (10) 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 (14), 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^{nd} approximate roots of F is $\psi_2 = (y^2 - x^3)^2 + 4x^8$ and we get the current Ψ-adic expansion $F = \psi_2^2 + \psi_{-1}^{14}\psi_1$. The monomials reaching the minimal values (9) are ψ_2^2, $\psi_{-1}^{14}\psi_1$ and we deduce from (10) 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 2. Note that for $k \geq 2$, we really need to consider the Ψ-adic expansion: the (x, y, ψ_k)-adic expansion is not enough to compute the next data. At step $k = 2$ in the previous example, the ψ_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 Ψ-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 $v_2(x^{14}y^2) = v_2(x^{17}) = 34 < 36$.

4.3 Quasi-irreducibility

In order to perform a unique irreducibility test, we will rather 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 quasi-irreducibility test. 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 polynomial H defined over $\mathbb{A}$ is *square-free* if 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 $\mathbb{A}$.

Definition 4. We say that a Weierstrass polynomial $F \in \mathbb{A}[[x]][y]$ is *quasi-degenerated* if its boundary polynomial has shape

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

with q, m coprime and $P \in \mathbb{A}[Z]$ monic, *square-free* and satisfying $P(0) \in \mathbb{A}^\times$.

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

Definition 5. We call `Quasi-Irreducible` the new algorithm obtained when replacing degenerated tests by quasi-degenerated tests in algorithm `Irreducible`. $F \in \mathbb{K}[[x]][y]$ Weierstrass is said quasi-irreducible over $\mathbb{L}$ if `Quasi-Irreducible`$(F, \mathbb{L})$ outputs `True`.

As $P_k(0) \in \mathbb{K}_{k-1}^{\times}$ by assumption, z_k is not a zero divisor in $\mathbb{K}_k$. It follows straightforwardly that all results of Section 3 and Subsection 4.1 still hold when considering quasi-degeneracy. In particular, algorithm `Quasi-Irreducible` is well-defined and Definition 5 makes sense.

Lemma 5. *A square-free monic polynomial $F \in \mathbb{K}[[x]][y]$ is irreducible over $\mathbb{K}$ if and only if it is quasi-irreducible and $\mathbb{K}_g$ is a field.*

Proof. This follows immediately from Definitions 4 and 5 with Theorem 5. □

5 Complexity. Proof of Theorem 1

5.1 Complexity model

We use the algebraic RAM model of Kaltofen [10, 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 [8, Section 8.3]. We use the classical notations $\mathcal{O}()$ and $\mathcal{O}^{\sim}()$ that respectively hide constant and logarithmic factors [8, Chapter 25, Section 7].

F being Weierstrass, we have the following result. As $\delta > 0$, that ensures in particular that e.g. $\delta \log(d) \in \mathcal{O}^{\sim}(\delta)$ (this will be used several times in the following).

Lemma 6. *We have $d - 1 \leq \delta$. If F is quasi-irreducible with residual degree f, then $(d-1)\, f \leq \delta$.*

Proof. As F is Weierstrass, all its Puiseux series have valuation at least $1/d$. Seeing δ as the sum of the valuations of the difference of the Puiseux series of F concludes the first point. In the second case, the minimum valuation for the Puiseux series of F becomes f/d (just use the classical equality $d = e\, f$). □

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 [21] 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 6. *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, τ) 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 [21, 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 3. Another way to deal with tower extensions would be the recent preprint [11]. This would make all algorithms deterministic, with a cost $\mathcal{O}(\delta^{1+o(1)})$ instead of $\mathcal{O}^{\sim}(\delta)$. Note also [12] for dynamic evaluation.

5.2 Truncation bounds

In order to estimate the complexity in terms of arithmetic operations in $\mathbb{K}$, we will compute approximate roots and Ψ-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 [21, 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 τ.

The successive polynomials generated by the function call `Quasi-Irreducible`(F) are still denoted $H_0, \ldots, H_g$, and we let (q_{g+1}, m_{g+1}) stand for the slope of the lowest edge of H_g, with convention $(q_{g+1}, m_{g+1}) = (1,0)$ if $N_g = 1$. As $\deg(H_k) = N_k$ and $\mathcal{N}(H_k)$ has a lowest edge of slope $-m_{k+1}/q_{k+1}$, the computation of the lowest boundary polynomial $\bar{H}_k$ only depends on H_k truncated with precision $N_k m_{k+1}/q_{k+1}$. Combined with (5), and using $v_x(\pi_k^*(x)) = e_k$, we deduce that the k^{th}-edge data only depends on F truncated with precision

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

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

Lemma 7. *Denoting $\eta_{-1} = 0$, we have $\eta_k = \eta_{k-1} + \frac{N_k m_{k+1}}{e_{k+1}}$ for any $0 \le k \le g$. 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 for any $0 \le k \le g$

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

As $v_{0,0} = 0$, case $k = 0$ is proved. Let $k \geq 1$. Previous formula used at rank $k-1$ gives

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

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 Proposition 3. This gives $\eta_k = \eta_{k-1} + \frac{N_k m_{k+1}}{e_{k+1}}$ as required. The formula for $\eta(F)$ follows straightforwardly. □

Remark 4. 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 $k < g$, from respectively (5) and Corollary 1. We deduce in particular that the sequence $(N_0, d_0\eta_0, \ldots, d_{g-1}\eta_{g-1})$ is a minimal set of generators of the semi-group of F when F is irreducible in $\overline{\mathbb{K}}[[x]][y]$; see e.g. [16, Proposition 4.2 and Theorem 5.1].

Proposition 7. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d, with discriminant valuation δ. Then $\eta(F) \leq \frac{2\delta}{d}$. If moreover F is quasi-irreducible, then $\eta(F) \geq \delta/d$.*

Proof. It follows from Lemma 7 that $\eta(F)$ is smaller or equal than the quantity "N_i" defined in [21, Subsection 3.3] (take care of notations, these N_i are not the same as those defined here), with equality if F is quasi-irreducible. From [21, 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 quasi-irreducible, then we have also $v_i \leq \eta(F) = N_i$ by [21, Corollary 4]. As all v_i's are equal in that case, the lower bound follows too. □

Remark 5 (*Dealing with the precision*). As δ is not given, we do not have an *a piori* bound for the precision $\eta(F)$. To deal with this problem, one can either use *relaxed* computations [25] or just restart the whole computation when we realise that we are missing precision. With both solutions, we need to increase the precision each time the computed lowest edge of the Newton polygon is not "guaranted" in the sense of [21, Definition 8 and Figure 1.b]. In algorithm `Quasi-Irreducible` below, we use the second option; this is done at lines 6 and 7, thanks to Lemma 7. In terms of complexity, both solutions only multiply the complexity bound by a logarithmic factor.

5.3 Main subroutines

Computing approximate roots and Ψ-adic expansion.

Proposition 8. *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 ψ of F with $\mathsf{M}(d)$ operations over $\mathbb{A}$.*

Proof. 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 ψ is the reciprocal polynomial of the truncated series $\lceil S \rceil^{\frac{d}{N}}$ (see e.g. [16, 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 precision d/N within $\mathsf{M}(d)$ operations by quadratic Newton iteration [8, Theorem 9.25]. □

Proposition 9. *There exists an algorithm* `Expand` *which, given $F \in \mathbb{A}[y]$ of degree d and $\Psi = (\psi_0, \ldots, \psi_k)$ a collection of monic polynomials $\psi_i \in \mathbb{A}[y]$ of strictly increasing degrees $d_0 < \cdots < d_k \leq d$ returns the reduced Ψ-adic expansion of F in less than $\mathcal{O}((k+1)\,\mathsf{M}(d)\,\log(d))$ arithmetic operations over $\mathbb{A}$.*

Proof. The ψ_k-adic expansion of $F = \sum a_i \psi_k^i$ requires $\mathcal{O}(\mathsf{M}(d)\log(d))$ operations by [8, Theorem 9.15]. If $k > 0$, we recursively compute the $(\psi_0, \ldots, \phi_{k-1})$-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 $i = 0, \ldots, \lfloor d/d_k \rfloor$ gives $\mathcal{O}(k\,\mathsf{M}(d)\,\log(d))$ operations. □

Computing boundary polynomials.

Proposition 10. *Given F and $\Psi = (\psi_{-1}, \ldots, \psi_k)$ modulo $x^{\eta(F)+1}$, $V = (v_{k,-1}, \ldots, v_{k,k})$ and $\Lambda = (\lambda_{k,-1}, \ldots, \lambda_{k,k})$, there exists an algorithm* `BoundaryPol` *that computes the lowest boundary polynomial $\bar{H}_k \in \mathbb{K}_k[x, y]$ within $\mathcal{O}(\delta + f_k^2)$ operations over $\mathbb{K}$.*

Proof. First compute the Ψ-adic expansion $F = \sum f_B \Psi^B$ modulo $x^{\eta+1}$, with $\eta := \eta(F)$. As $\eta \leq 2\delta/d$, this is $\mathcal{O}(\delta)$ by Proposition 9 applied with $\mathbb{A} = \mathbb{K}[x]/(x^{\eta+1})$, using $k \leq \log(d)$ and Lemma 6. We compute the lowest edge of $\mathcal{N}(H_k)$ via Theorem 2; this takes no arithmetic operations[3]. It remains to compute the coefficient of each monomial $x^{w_i} y^i$ of $\bar{H}_k$, which is

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

by Theorem 3. The computation of $\Lambda^{B_0} = \lambda_{k,k}^{N_k}$ takes $\mathcal{O}(\log(d))$ operations over $\mathbb{K}_k$ via fast exponentiation. Also, there are at most f_k monomials Λ^B to compute from Proposition 2. 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 $w_i + v_k(F) \leq e_k \eta_k \leq 2\delta$ by definition of η_k and Proposition 7). This concludes. □

Testing quasi-degeneracy and computing edge data.

Proposition 11. *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* `Quasi-Degenerated` *that returns* `False` *if $\bar{H}$ is not quasi-degenerated, and the edge data (q, m, P, N) of $\bar{H}$ otherwise. It takes at most $\mathcal{O}(\deg_Z(Q)\deg_y(\bar{H})/q)$ operations over $\mathbb{K}$.*

Proof. As $\bar{H}$ is quasi-homogeneous, we have $\bar{H} = P_0(y^q/x^m)x^{m\deg(P_0)}$ for some coprime integers $q, m \in \mathbb{N}$ and some $P_0 \in \mathbb{K}_Q[T]$ of degree $\deg_y(\bar{H})/q$. We need 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 $\mathbb{K}[Z, T]$),

[3] for the interested reader, it can easily be shown that this takes $\mathcal{O}(\delta)$ bit operations

and that $P(0) \notin \mathbb{K}_Q^\times$. The first task is a special case of [21, Proposition 14] and fits in the aimed bound. Second one is just a gcd computation, bounded by $\mathcal{O}(\deg_Z(Q))$. □

5.4 The main algorithm. Proof of Theorem 1

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

Input: $F \in \mathbb{K}[[x]][y]$ Weierstrass of degree d not divisible by Char($\mathbb{K}$).

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

1 $F \leftarrow F \mod x^\eta$; `// All computations modulo` x^η
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, Ψ, V, Λ) ; `//` $\bar{H} \in \mathbb{K}_Q[x, y]$
6 $\quad e \leftarrow q\,e$; $\eta' \leftarrow \eta' + \frac{N\,m}{e}$; `//` (q, m) `the lowest edge of` $\bar{H}$
7 $\quad$ **if** $\eta \le \eta'$ **then return** `Quasi-Irreducible`$(F, 2\eta)$;
8 $\quad (Bool, (q, m, P, N)) \leftarrow$ `Quasi-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, Λ using (14);
12 $\quad (Q, \tau) \leftarrow$ `Primitive`(Q, P);
13 $\quad \Lambda \leftarrow \tau(\Lambda)$;
14 **return** (Data, Q);

Proposition 12. *Running* `Quasi-Irreducible`(F) *returns the correct output in an expected* $\mathcal{O}(\delta)$ *operations over* $\mathbb{K}$.

Proof. The polynomial $\bar{H}$ at line 8 is the correct lowest boundary polynomial thanks to Lemma 7 (see also Remark 5). Then correctness follows from Theorem 5 and Definition 5. As $q_k \ell_k \ge 2$, we have $g \le \log_2(d)$, while recursive calls of line 7 multiply the complexity by at most a logarithm too. Considering one iteration, and using $\eta < 2\,\eta(F) \le 4\,\delta/d$ (second inequality by Proposition 7), lines 4, 5, 8, 12 and 13 cost respectively $\mathcal{O}(\delta)$, $\mathcal{O}(\delta + f_k^2)$, $\mathcal{O}(f_k N_k/q_k) \subset \mathcal{O}(d)$, $\mathcal{O}(f_k^{(\omega+1)/2})$ and $\mathcal{O}(f_k^2)$ from respectively Propositions 8, 10, 11, 6 and 6 once again. Summing up, we conclude from Lemma 6 (note that if F is not quasi-irreducible, as long as the algorithm does not output `False`, F "looks" quasi-irreducible, so that we still have $(d-1)\,f_g \le \delta$). □

Proof of Theorem 1. Thanks to Lemma 5, F is irreducible if and only if it is quasi-irreducible and the residue ring $\mathbb{K}_g = \mathbb{K}[Z]/(Q(Z))$ is a field. This can be checked with a univariate irreducibility test in $\mathbb{K}[Z]$ of degree $\deg(Q) = f \le d$. □

Note that there are well known formulas for the valuation of the discriminant δ in terms of the edge data, see e.g. [22, Corollary 5].

Example 5. Let us illustrate algorithm `Quasi-Irreducible` on a simple example, considering $F = (y^4 - x^2)^4 + y^6x^{11} - y^4x^{12} - y^2x^{13} + x^{14} + x^{16}$ with $\mathbb{K} = \mathbb{Q}$.

Initialisation. We start with $N_0 = d = 16$, $\psi_{-1} = x$, $V = (1, 0)$ and $\lambda = (1, 1)$.

Step 0. The 16^{th}-approximate roots of F is $\psi_0 = y$ and we find $\bar{H}_0 = (y^4 - x^2)^4$. So H_0 is quasi-degenerated with edge data $(q_1, m_1, P_1, N_1) = (2, 1, Z_1^2 - 1, 4)$. Using (14), we update $V = (2, 1, 4)$ and $\lambda = (z_1, z_1, 4z_1)$, with $z_1 = Z_1 \mod P_1$ (i.e. $z_1^2 = 1$).

Step 1. We compute the 4^{th}-approximate root $\psi_1 = y^4 - x^2$ of F, then its Ψ-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 (9), and we deduce from (10) and equality $z_1^2 = 1$ that $\bar{H}_1 = y^4 + \frac{(1-z_1)}{4^3}x^{12}y + \frac{1}{4^4}x^{16}$, which is quasi-homogeneous with slope $(q_2, m_2) = (1, 4)$. We find that $P_0 = Z_2^4 + \frac{(1-z_1)}{4^3}Z_2 + \frac{1}{4^4}$ is square-free over $\mathbb{Q}_1$. Hence, $\bar{H}_1$ is quasi-degenerated with edge data $(q_2, m_2, P_2, N_2) = (1, 4, P_0, 1)$. As $N_2 = 1$, we deduce that F is quasi-irreducible. However, the last residue field $\mathbb{Q}_2 = \mathbb{Q}[Z_1, Z_2]/(P_1, P_2)$ is not a field so F is not irreducible (in practice, the algorithm would have computed $Q \in \mathbb{Q}[Z]$ of degree 8 such that $\mathbb{Q}_2 = \mathbb{Q}[Z]/(Q(Z))$, and eventually check the irreducibility of Q).

Remark 6. The polynomial Q might factor during the square-free test made at Line 8. In such a case, F is reducible and we should of course immediately return `False` at this stage. For instance testing square-freeness of P_0 in Example 5 requires to compute the gcd between P_0 and its derivative P_0'. The first euclidean division gives $P_0 = \frac{Z_2}{4}P_0' + R$ with $R = \frac{3}{4^4}(1 - z_1)Z_2 + \frac{1}{4^4}$. Before proceeding to the next division of P_0' by R, we need to check first that the leading coefficient of R is a unit in $\mathbb{Q}_1$. To this aim, we compute the gcd between $\frac{3}{4^4}(1 - Z_1)$ and P_1, discovering here that $Z_1 - 1$ divides P_1 so that P_1 is reducible. Hence F is reducible and we could have returned `False` at this point. We did not take into account this obvious improvement in our algorithm for readibility.

5.5 Further comments

Factorisation of quasi-irreducible polynomials. Not returning `False` when discovering a factor of Q also makes sense if we want further informations about the factorisation of F. Namely, if F is quasi-irreducible, then we can deduce from the field decomposition of $\mathbb{K}_g$ the number of irreducible factors of F in $\mathbb{K}[[x]][y]$ together with their residual degrees and index of ramification. In Example 5 above, we find 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 $q_1q_2 = 2$. In particular, they have respective degrees $8, 2, 6$.

In fact, quasi-irreducible polynomials behave like irreducible polynomials, in the sense that they are "balanced": all their absolutely irreducible factors in $\overline{\mathbb{K}}[[x]][y]$ have same sets of characteristic exponents and same sets of pairwise intersection multiplicities.

These important data can be deduced from the edge data, see [22, Section 8]; they characterise the equisingular type of the germ of curve $(F, 0)$, which coincides with the topological equivalent class in the case $\mathbb{K} = \mathbb{C}$. Unfortunately, F might be balanced without being quasi-irreducible. In order to characterise balanced polynomials, we need to modify slightly Definition 4, allowing several edges when $q = 1$. These aspects are considered in the longer preprint [22] and will be published in a forthcoming paper.

The case of non Weierstrass polynomials. Up to minor changes, we can use algorithm `Quasi-Irreducible` to test the irreducibility of any square-free polynomial $F \in \mathbb{K}[[x]][y]$, without assuming F Weierstrass. 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 and we are reduced to consider the case F monic. Then, algorithm `Quasi-Irreducible` works exactly as in the Weierstrass case. However, the bound $(d-1)\,f \leq \delta$ of Lemma 6 does not hold anymore. To get a similar complexity, we need to modify slightly the algorithm: we do not compute primitive elements of $\mathbb{K}_k$ over the field $\mathbb{K}$ but only over the next residue ring $\mathbb{K}_1 = \mathbb{K}_{P_1}$. It can be shown that the complexity becomes $\mathcal{O}^{\sim}(\delta + d)$. Moreover, we eventually get a bivariate representation $\mathbb{K}_g = \mathbb{K}[Z_1, Z](P_1(Z_1), Q(Z_1, Z))$ and checking that $\mathbb{K}_g$ is a field requires now two univariate irreducibility tests of degree at most d. See [22, Section 7.4] for details.

Bivariate polynomials. If the input F is given as a bivariate polynomial $F \in \mathbb{K}[x, y]$ with partial degrees $n := \deg_x(F)$ and $d = \deg_y(F)$, we get a complexity estimate $\mathcal{O}^{\sim}(nd)$ which is quasi-linear with respect to the arithmetic size of the input. Moreover, we need not to assume F square-free. Namely, we first reduce to the monic case as explained in the previous paragraph. Then, we run algorithm `Quasi-Irreducible` with parameters F and $4\,n$, except that we return `False` whenever test of line 7 fails. If F is square-free, we have the well known inequality $\delta \leq 2nd$ so that $\eta(F) \leq 4\,n$: the algorithm will return the correct answer with at most $\mathcal{O}^{\sim}(n\,d)$ operations over $\mathbb{K}$ as required, and so without reaching a value $\eta' > 4\,n$ at Line 7. 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 we end up with three possibilities:

- we reach a value $\eta' > 4\,n$ at Line 7, ensuring the non square-freeness (hence the non quasi-irreducibility) of F;
- the function call at Line 8 returns `False` and F is not quasi-irreducible;
- the function call at Line 8 computes an edge data which satisfies $q = \deg(P) = 1$ (this happens exactly when we compute an approximate root ψ such that $F = \psi^N$ modulo $x^{4\,n+1}$ for some $N > 1$). As this can not happen when F is square-free, we deduce that F is not square-free, hence not quasi-irreducible.

As we always truncate the powers of x with precision $4\,n$, we will return `False` within an expected $\mathcal{O}^{\sim}(n\,d)$ operations over $\mathbb{K}$ in all three cases. Note that in the second case, we can not conclude if F is square-free or not.

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 F is quasi-irreducible and $f_g = 1$. To check this we can slightly modify algorithm `Quasi-Irreducible`: just return `False` whenever $\ell_k > 1$. We thus have $\mathbb{K}_k = \mathbb{K}$ for all k, and do not need the Las-Vegas subroutine `Primitive`, nor any univariate irreducibility test. We obtain a deterministic algorithm running with $\mathcal{O}(\delta + d)$ operations over $\mathbb{K}$, which is $\mathcal{O}(\delta)$ is F is Weierstrass. Also, we could have used algorithm `AbhyankarTest` below with suitable precision for the same cost.

6 Abhyankhar's absolute irreducibility test

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 require to compute the boundary polynomials $\bar{H}_k$: knowing their Newton polygon is sufficient. Although we do not need this improvement from a complexity point of view, we show how to recover this result in our context for the sake of completness. We will use the following alternative characterisations of valuations and polygons. For convenience, we will rather compute the translated polygon $\mathcal{N}_k(F) := \mathcal{N}(H_k) + (0, v_k(F))$, which by (5) coincides with the union of edges of strictly negative slopes of $\mathcal{N}(\pi_k^*(F))$.

Lemma 8. *Suppose that $H_0, \ldots, H_{k-1}$ are degenerated.*

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

$$\mathcal{N}_k(F) = Conv\left(\left(i, v_k(c_i\psi_k^i)\right) + (\mathbb{R}^+)^2,\ c_i \neq 0\right). \tag{18}$$

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

$$v_k(G) = \min_i \left(q_k v_{k-1}(a_i\psi_{k-1}^i) + i m_k\right). \tag{19}$$

Proof. Equality (18) is a direct consequence of Corollary 3 with Theorems 2 and 4. Also, from (17), $\pi_k^*(c_i\psi_k^i)$ has a term of lowest x-valuati on of shape $u x^{v_k(a_i\,\psi_k^i)}\, y^i$ for some $u \in \mathbb{K}_k^\times$ and it follows that $v_k(F) = \min_i v_k(c_i\psi_k^i)$. This proves Point 1.

Applying (17) at rank $k-1$, we get $\pi_{k-1}^*(a_i\psi_{k-1}^i) = x^{v_{k-1}(a_i\psi_{k-1}^i)}\,(y + x^\alpha \tilde{U}_i)^i\, U_i$, where $\alpha > m_k/q_k$, and $U_i, \tilde{U}_i$ are units. As $m_k > 0$, we deduce that $V_i = U_i(z_k^{s_k} x^{q_k}, x^{m_k}(y + z_k^{t_k} + c_k(x))$ is a unit such that $V_i(0,y) = U_i(0,0) \in \mathbb{K}_k^\times$ is constant and a straightforward computation shows $\pi_k^*(a_i\psi_{k-1}^i) = x^{q_k v_{k-1}(a_i\psi_{k-1}^i) + i m_k} P_i(y) + h.o.t$, where $P_i \in \mathbb{K}[y]$ has degree exactly i. Equality (19) follows. □

Remark 7. Point 2 in Lemma 8 shows that our valuations coincide with the extended valuations used in the Montes algorithm over general local fields; see for instance [9, Point (3) of Proposition 2.7].

Hence, we may take (18) and (19) as alternative recursive definitions of valuations and Newton polygons. This new point of view has the great advantage to be independent of

the map π_k, hence of the Newton-Puiseux algorithm. In particular, it can be generalised at rank $k+1$ without assuming that H_k is degenerated.

Definition 6. 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 (19) and (18) applied at rank $k+1$.

Remark 8. This definition of the map v_{k+1} is equivalent to

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

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 to update valuations.

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.

$N \leftarrow d$, $v_0 \leftarrow v_x$, $k \leftarrow 0$;
while $N > 1$ **do**
  $\psi \leftarrow$ `AppRoot`(F, N);
  $\sum c_i \psi^i \leftarrow$ `Expand`(F, ψ);
  Compute $\mathcal{N}_k(F)$ using (18);
  if $(N, v_k(F)) \notin \mathcal{N}_k(F)$ *or* $\mathcal{N}_k(F)$ *is not straight or* $q = 1$ **then**
    return *False*
  $N \leftarrow N/q$, $k \leftarrow k+1$;
  Compute v_k from v_{k-1} via (19);
return *True*;

Proposition 13. *Algorithm* `AbhyankarTest` *works as specified.*

Proof. We need to show that it returns the same output as `Irreducible`$(F, \overline{\mathbb{K}})$. 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`. As $\mathcal{N}_g(F) = \mathcal{N}(H_g) + (0, v_g(F))$ (definition) and 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 ψ_{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 ψ_{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 ψ_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 (18), 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 (18), $\mathcal{N}_g(F)$ 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 6, this implies $v_{g+1}(c_i\psi_{g+1}^i) \leq v_{g+1}(F)$ which in turns forces $(N_{g+1}, v_{g+1}(F)) \notin \mathcal{N}_{g+1}(F)$. □

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] V. Cossart and G. Moreno-Socías. Irreducibility criterion: A geometric point of view. 33:27–42, 2003.

[4] 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.

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

[6] 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.

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

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

[9] 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.

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

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

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

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

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

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

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

[17] 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.

[18] 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.

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

[20] 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.

[21] A. Poteaux and M. Weimann. Computing Puiseux series: a fast divide and conquer algorithm, 2017. Preprint arXiv:1708.09067v2.

[22] A. Poteaux and M. Weimann. A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$, 2019. Preprint arXiv:1904.00286v1.

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

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

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

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

[27] 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.

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