View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Archive Ouverte en Sciences de l'Information et de la Communication

Computing the equisingularity type of a pseudo-irreducible polynomial

Adrien Poteaux, Martin Weimann

To cite this version:

Adrien Poteaux, Martin Weimann. Computing the equisingularity type of a pseudo-irreducible polynomial. 2019. hal-02354930

HAL Id: hal-02354930

https://hal.archives-ouvertes.fr/hal-02354930

Submitted on 8 Nov 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Computing the equisingularity type of a pseudo-irreducible polynomial

Adrien Poteaux,

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

Martin Weimann

GAATI*, Université de Polynésie Française
UMR CNRS 6139, BP 6570
98702 Faa'a, Polynésie Française
martin.weimann@upf.pf

Germs of plane curve singularities can be classified accordingly to their equisingularity type. For singularities over $\mathbb{C}$, this important data coincides with the topological class. In this paper, we characterise a family of singularities, containing irreducible ones, whose equisingularity type can be computed in quasi-linear time with respect to the discriminant valuation of a Weierstrass equation.

1 Introduction

Equisingularity is the main notion of equivalence for germs of plane curves. It was developed in the 60's by Zariski over algebraically closed fields of characteristic zero in [28–30] and generalised in arbitrary characteristic by Campillo [2]. This concept is of

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

particular importance as for complex curves, it agrees with the topological equivalence class [27]. As illustrated by an extensive litterature (see e.g. the book [9] and the references therein), equisingularity plays nowadays an important role in various active fields of singularity theory (resolution, equinormalisable deformation, moduli problems, analytic classification, etc). It is thus an important issue of computer algebra to design efficient algorithms for computing the equisingularity type of a singularity. This paper is dedicated to characterise a family of reduced germs of plane curves, containing irreducible ones, for which this task can be achieved in quasi-linear time with respect to the discriminant valuation of a Weierstrass equation.

Main result. There exist several equivalent definitions of the equisingularity of two germs of a reduced plane curve, a classical one being that there is a one-to-one correspondance between their branches which preserves the characteristic Puiseux exponents and the pairwise intersection multiplicities; this will be our point of view in this paper. More precisely, we consider a square-free Weierstrass polynomial $F \in \mathbb{K}[[x]][y]$ of degree d, with $\mathbb{K}$ a perfect field of characteristic zero or greater than d[1], and denote δ the valuation of its discriminant. With our assumption on $\mathbb{K}$, the Puiseux series of F are well defined and allow to determine the equisingularity type of the germ $(F, 0)$ (the case of small characteristic requires Hamburger-Noether expansions [2]). In particular, it follows from [19] that we can compute the equisingularity type in an expected $\tilde{\mathcal{O}}(d\,\delta)$ operations over $\mathbb{K}$. If moreover F is irreducible, it is shown in [20] that we can reach the lower complexity $\tilde{\mathcal{O}}(\delta)$ thanks to the theory of approximate roots. In this paper, we extend this result to a larger class of polynomials.

We say that F is *balanced* or *pseudo-irreducible*[2] if all its absolutely irreducible factors have the same set of characteristic exponents and the same set of pairwise intersection multiplicities, see Section 2. Irreducibility over any algebraic field extension of $\mathbb{K}$ implies pseudo-irreducibility by a Galois argument, but the converse does not hold. As a basic example, the Weierstrass polynomial $F = (y - x)(y - x^2)$ is pseudo-irreducible, but is obviously reducible. We prove:

Theorem 1. *There exists an algorithm which tests if F is pseudo-irreducible with an expected $\tilde{\mathcal{O}}(\delta)$[3] operations over $\mathbb{K}$. If F is pseudo-irreducible, the algorithm computes also δ and the number of absolutely irreducible factors of F together with their sets of characteristic exponents and sets of pairwise intersection multiplicities. In particular, it computes the equisingularity type of the germ $(F, 0)$.*

The algorithm contains a Las Vegas subroutine for computing primitive elements in residue rings; however it should become deterministic thanks to the recent preprint [24]. For a given field extension $\mathbb{L}$ of $\mathbb{K}$, we can also compute the degrees, residual degrees

[1] Our results still hold under the weaker assumption that the characteristic of $\mathbb{K}$ does not divide d.

[2] In the sequel, we rather use first the terminology *balanced* and give an alternative definition of pseudo-irreducibility based on a Newton-Puiseux type algorithm. Both notions agree from Theorem 2.

[3] As usual, the notation $\tilde{\mathcal{O}}()$ hides logarithmic factors. Note that F being Weierstrass, we have $d \le \delta$ and $\delta \log(d) \in \tilde{\mathcal{O}}(\delta)$.

and ramification indices of the irreducible factors of F in $\mathbb{L}[[x]][y]$ by performing an extra univariate factorisation of degree at most d over $\mathbb{L}$. Having a view towards fast factorisation in $\mathbb{K}[[x]][y]$, we can extend the definition of pseudo-irreducibility to non Weierstrass polynomials, taking into account all germs of curves defined by F along the line $x = 0$. Our approach adapts to this more general setting, with complexity $\mathcal{O}(\delta + d)$[4] (see Section 5).

Main tools. We generalise the irreducibility test obtained in [20], which is itself a generalisation of Abhyankhar's absolute irreducibility criterion [1], based on the theory of approximate roots. The main idea is to compute recursively some suitable approximate roots $\psi_0, \ldots, \psi_g$ of F of strictly increasing degrees such that F is pseudo-irreducible if and only if we reach $\psi_g = F$. At step k, we compute the $(\psi_0, \ldots, \psi_k)$-adic expansion of F from which we can construct a generalised Newton polygon. If the corresponding boundary polynomial of F is not pseudo-degenerated (Definition 4), then F is not pseudo-irreducible. Otherwise, we deduce the degree of the next approximate root ψ_{k+1} that has to be computed.

The key difference when compared to the irreducibility test developped in [20] is that we may allow the successive generalised Newton polygons to have several edges, although no splittings and no Hensel liftings are required. Except this slight modification, most of the algorithmic considerations have already been studied in [20] and this paper is more of a theoretical nature, focused on two main points : proving that pseudo-degeneracy is the right condition for characterising pseudo-irreducibility, and giving formulas for the intersection multiplicities and characteristic exponents in terms of the underlying edge data sequence. This is our main Theorem 2.

Related results. Computing the equisingularity type of a plane curve singularity is a classical topic for which both symbolic and numerical methods exist. A classical approach is derived from the Newton-Puiseux algorithm, as a combination of blow-ups (monomial transforms and shifts) and Hensel liftings. This approach allows to compute the roots of F - represented as fractional Puiseux series - up to an arbitrary precision, from which the equisingularity type of the germ $(F, 0)$ can be deduced (see e.g. Theorem 2 for precise formulas). The Newton-Puiseux algorithm has been studied by many authors (see e.g. [4, 5, 16–20, 23, 26] and the references therein). Up to our knowledge, the best current arithmetic complexity was obtained in [19], computing the singular parts of all Puiseux series above $x = 0$ - hence the equisingularity type of all germs of curves defined by F along this line - in an expected $\mathcal{O}(d\,\delta)$ operations over $\mathbb{K}$. Here, we get rid of the d factor for pseudo-irreducible polynomials, generalising the irreducible case considered in [20]. For complex curves, the equisingularity type agrees with the topological class and there exists other numerical-symbolic methods of a more topological nature (see e.g. [10–12, 14, 22] and the references therein). This paper comes from a longer preprint [21] which contains also results of [20].

[4] When F is not Weierstrass, we might have $d \notin \mathcal{O}(\delta)$.

Organisation. We define balanced polynomials in Section 2. Section 3 introduces the notion of pseudo-degeneracy. This leads to an alternative definition of a pseudo-irreducible polynomial, based on a Newton-Puiseux type algorithm. In Section 4, we prove that being balanced is equivalent to being pseudo-irreducible and we give explicit formulas for characteristic exponents and intersection multiplicities in terms of edge data (Theorem 2). In the last Section 5, we design a pseudo-irreducibility test based on approximate roots with quasi-linear complexity, thus proving Theorem 1. We illustrate our method on various examples.

2 Balanced polynomials

Let us fix $F \in \mathbb{K}[[x]][y]$ a Weierstrass polynomial defined over a perfect field $\mathbb{K}$ of characteristic zero or greater than $d = \deg(F)$. For simplicity, we abusively denote by $(F, 0) \subset (\overline{\mathbb{K}}^2, 0)$ the germ of the plane curve defined by F at the origin of the affine plane $\overline{\mathbb{K}}^2$. We say that F is absolutely irreducible if it is irreducible in $\overline{\mathbb{K}}[[x]][y]$. The germs of curves defined by the absolutely irreducible factors of F are called the branches of the germ $(F, 0)$.

2.1 Characteristic exponents

We assume here that F is absolutely irreducible. As the characteristic of $\mathbb{K}$ does not divide d, there exists a unique series $S(T) = \sum c_i T^i \in \overline{\mathbb{K}}[[T]]$ such that $F(T^d, S(T)) = 0$. The pair $(T^d, S(T))$ is the classical Puiseux parametrisation of the branch $(F, 0)$. The *characteristic exponents* of F are defined as

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

where g is the least integer for which $gcd(\beta_0, \ldots, \beta_g) = 1$ (characteristic exponents are sometimes refered to the rational numbers β_i/d in the litterature). These are the exponents i for which a non trivial factor of the ramification index is discovered. It is well known that the data

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

determines the equisingularity type of the germ $(F, 0)$, see e.g. [27]. Conversely, the Weierstrass equations of two equisingular germs of curves which are not tangent to the x-axis have same characteristic exponents [3, Corollary 5.5.4]. If tangency occurs, we rather need to consider the characteristic exponents of the local equation obtained after a generic change of local coordinates, 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 β_0 (contact order with x-axis) [15, Proposition 4.3] or [3, Corollary 5.6.2]. It is well known that a data equivalent to $\mathrm{C}(F)$ is given by the semi-group of F, and that this semi-group admits the intersection multiplicities of F with its characteristic approximate roots $\psi_{-1}, \psi_0, \ldots, \psi_g$ as a minimal system of generators (see Section 5.1 and [3, Corollaries 5.8.5 and 5.9.11]).

2.2 Intersection sets

If we want to determine the equisingularity type of a reducible germ $(F, 0)$, we need to consider also the pairwise intersection multiplicities between the absolutely irreducible factors of F. The intersection multiplicity between two coprime Weierstrass polynomials $G, H \in \mathbb{K}[[x]][y]$ is defined as

$$(G, H)_0 := v_x(\mathrm{Res}_y(G, H)) = \dim_{\overline{\mathbb{K}}} \frac{\overline{\mathbb{K}}[[x]][y]}{(G, H)}, \tag{1}$$

where Res_y stands for the resultant with respect to y and v_x is the usual x-valuation. The right hand equality follows from classical properties of the resultant. Suppose that F has (distinct) absolutely irreducible factors $F_1, \ldots, F_f$. We introduce *the intersection sets* of F, defined for $i = 1, \ldots, f$ as

$$\Gamma_i(F) := ((F_i, F_j)_0,\, 1 \leq j \leq f, j \neq i)\,.$$

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 type (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 [31]. Note that the set $\mathrm{C}(F_i)$ only depends on F_i while $\Gamma_i(F)$ depends on F.

2.3 Balanced polynomials

Definition 1. We say that a square-free Weierstrass[5] polynomial $F \in \mathbb{K}[[x]][y]$ 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 balanced, its branches are equisingular and have the same set of pairwise intersection multiplicities. The converse holds if no branch is tangent to the x-axis or all branches are tangent to the x-axis.

Example 1. 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 1.

1. If $F \in \mathbb{K}[[x]][y]$ is irreducible, a Galois argument shows that it is balanced (follows from Theorem 2 below). The converse doesn't hold: $F = (y - x)(y + x^2)$ is reducible, but it is balanced. This example also shows that being balanced does not imply the Newton polygon to be straight.
2. $F = (y^2 - x^3)(y^2 + x^3)(y^2 + x^3 + x^4)$ 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 $\Gamma_2(F) = \Gamma_3(F) = (6, 8)$.

[5] We can extend this definition to non Weierstrass polynomials, see Subsection 5.3.

3. $F = (y-x-x^2)(y-x+x^2)(y^2-x^3)$ 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 $\mathrm{C}(F_3) = (2;3)$.
4. $F = (y^2-x^2)^2 - 2x^4y^2 - 2x^6 + x^8$ has four absolutely irreducible factors, namely $F_1 = y + x + x^2$, $F_2 = y + x - x^2$, $F_3 = y - x + x^2$ and $F_4 = y - x - x^2$. 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 being balanced does not imply that all factors intersect each others with the same multiplicity.
5. $F = (y^2-x^3)(y^3-x^2)$ is not balanced. However, it defines two equisingular germs of plane curves (but 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 d_F and d_G, their intersection multiplicty $(F,G)_0$ is closely related to the characteristic exponents $(\beta_0, \ldots, \beta_g)$ of F. Let us denote by

$$\mathrm{Cont}(F,G) := d_F \max\left(v_x(y-y') \mid F(y) = 0,\ G(y') = 0\right) \tag{2}$$

the *contact order* of the branches F and G and let $\kappa = \max\{k \,|\, \mathrm{Cont}(F,G) \geq \beta_k\}$. Then Noether-Merle's [13, Proposition 2.4] formula states

$$(F,G)_0 = \frac{d_G}{d_F}\left(\sum_{k\leq\kappa}(E_{k-1}-E_k)\beta_k + E_\kappa\,\mathrm{Cont}(F,G)\right), \tag{3}$$

where $E_k := gcd(\beta_0, \ldots, \beta_k)$. A proof can be found in [15, Proposition 6.5] (and references therein), where a formula is given in terms of the semi-group generators, which turns out to be equivalent to (3) thanks to [15, Proposition 4.2]. Note that the original proof in [13] assumes that the germs F and G are transverse to the x-axis.

3 Pseudo-irreducible polynomials

3.1 Pseudo-degenerated polynomials.

We first recall classical definitions that play a central role for our purpose, namely the Newton polygon and the residual polynomial. We will have to work over various residue rings isomorphic to some direct product of fields extension of the base field $\mathbb{K}$. Let $\mathbb{A} = \mathbb{L}_0 \oplus \cdots \oplus \mathbb{L}_r$ be such a ring. If $S = \sum c_i x^i \in \mathbb{A}[[x]]$, we define $v_x(S) = \min(i\,,\, c_i \neq 0)$ with convention $v_x(0) = +\infty$. Note that in contrast to usual valuations, we have $v_x(S_1\,S_2) \geq v_x(S_1) + v_x(S_2)$ and strict inequality might occur since $\mathbb{A}$ is allowed to contain zero divisors.

In the following definitions, we assume that $F \in \mathbb{A}[[x]][y]$ is a Weierstrass polynomial and we let $F = \sum_{i=0}^d a_i(x)\,y^i = \sum_{i,j} a_{ij}x^jy^i$.

Definition 2. The *Newton polygon* of F is the lower convex hull $\mathcal{N}(F)$ of the set of points $(i, v_x(a_i))$ with $a_i \neq 0$ and $i = 0, \ldots, d$. We denote by $\mathcal{N}_0(F)$ the lower edge (right hand edge) of the Newton polygon.

The lower edge has equation $mi + qj = l$ for some uniquely determined coprime positive integers q, m and $l \in \mathbb{N}$. We say for short that $\mathcal{N}_0(F)$ has slope (q, m), with convention $(q, m) = (1, 0)$ if the Newton polygon of F is reduced to a point.

Definition 3. We call $\bar{F} := \sum_{(i,j)\in\mathcal{N}_0(F)} a_{ij} x^j y^i$ the *lower boundary polynomial* of F.

We say that a polynomial $P \in \mathbb{A}[Z]$ is *square-free* if its images under the natural morphisms $\mathbb{A} \to \mathbb{L}_i$ are square-free (in the usual sense over a field).

Definition 4. We say that $F \in \mathbb{A}[[x]][y]$ is *pseudo-degenerated* if there exists $N \in \mathbb{N}$ and $P \in \mathbb{A}[Z]$ monic and square-free such that

$$\bar{F} = \left(P\left(\frac{y^q}{x^m}\right) x^{m \deg(P)} \right)^N, \tag{4}$$

with moreover $P(0) \in \mathbb{A}^\times$ (units of $\mathbb{A}$) if $q > 1$. We call P the *residual polynomial* of F. The tuple (q, m, P, N) is the *edge data* of F.

Remark 1. In practice, we check pseudo-degeneracy as follows. If q does not divide d, then F is not pseudo-degenerated. If q divides d, then $q|i$ for all $(i, j) \in \mathcal{N}_0(F)$ as $(d, 0) \in \mathcal{N}_0(F)$ by construction. Hence we may consider $Q = \sum_{(i,j)\in\mathcal{N}_0(F)} a_{ij} Z^{i/q} \in \mathbb{A}[Z]$ and F is pseudo-degenerated if and only if $Q = P^N$ for some square-free polynomial P such that $P(0) \in \mathbb{A}^\times$ if $q > 1$.

Remark 2. If $q > 1$, the extra condition $P(0) \in \mathbb{A}^\times$ implies that $\mathcal{N}(F)$ is straight. If $q = 1$, we allow $P(0)$ to be a zero-divisor (in contrast to Definition 4 of quasi-degeneracy in [20]), in which case $\mathcal{N}(F)$ may have several edges. Note that if F is pseudo-degenerated, $\bar{F}$ is the power of a square-free quasi-homogeneous polynomial, but the converse doesn't hold (case 4 below).

Example 2.

1. Let $F = (y^2 - x^2)^2(y - x^2)(y - x^3)$. Then $\mathcal{N}(F)$ has three edges, the lower one of slope $(q, m) = (1, 1)$. We get $\bar{F} = (y^3 - x^2 y)^2$ and $Q = (Z^3 - Z)^2$. Hence, F is pseudo-degenerated, with $P = Z^3 - Z$ and $N = 2$.
2. Let $F = (y^2 - x^2)^2(y - x^2)$. Then $\mathcal{N}(F)$ has two edges, the lower one of slope $(q, m) = (1, 1)$. We get $\bar{F} = y(y^2 - x^2)^2$ and $Q = Z(Z^2 - 1)^2$ is not a power of a square-free polynomial. Hence, F is not pseudo-degenerated.
3. Let $F = (y^2 - x^3)^2(y - x^4)$. Then $\mathcal{N}(F)$ has two edges, the lower one of slope $(q, m) = (2, 3)$. As q does not divide $d = 5$, F is not pseudo-degenerated.
4. Let $F = (y^2 - x^3)^2(y - x^4)^2$. Then $\mathcal{N}(F)$ is straight of slope $(q, m) = (2, 3)$. Here q divides $d = 6$. We get $\bar{F} = y^2(y^2 - x^3)^2$ which is a power of a square-free polynomial. However, $Q = Z(Z - 1)^2$ is not. Hence, F is not pseudo-degenerated.

5. Let $F = (y^2 - x^3)^2(y^2 - x^4)^2$. Then $\mathcal{N}(F)$ has two edges, the lower one of slope $(q, m) = (2, 3)$. Here q divides $d = 8$. We get $\bar{F} = (y^4 - y^2x^3)^2$ and $Q = (Z^2 - Z)^2$ is the power of the square-free polynomial $P = Z^2 - Z$. However, $q > 1$ and $P(0) = 0$ so F is not pseudo-degenerated.

Note that we could also treat cases 3, 4 and 5 simply by using Remark 2: $q > 1$ and $\mathcal{N}(F)$ not straight imply that F is not pseudo-degenerated.

The next lemma allows to associate to a pseudo-degenerated polynomial F a new Weierstrass polynomial of smaller degree, generalising the usual case (e.g. [5, Section 4], [18, Prop.3], [19, Prop.2]) to the case of product of fields.

Lemma 1. *Suppose that F is pseudo-degenerated with edge data (q, m, P, N) and denote (s, t) the unique positive integers such that $s\,q - t\,m = 1$, $0 \le t < q$. Let z be the residue class of Z in the ring $\mathbb{A}_P := \mathbb{A}[Z]/(P(Z))$ and $\ell := \deg(P)$. Then*

$$F(z^t x^q, x^m(y + z^s)) = x^{qm\ell N} UG, \tag{5}$$

where $U, G \in \mathbb{A}_P[[x]][y]$, $U(0, 0) \in \mathbb{A}_P^\times$ and G is a Weierstrass polynomial of degree N dividing d. Moreover, if $F \ne y^d$ and F has no terms of degree $d - 1$, then $N < d$.

Proof. Let $\tilde{F}(x, y) = F(z^t x^q, x^m(y+z^s))x^{-qm\ell N}$. We deduce from (4) that $\tilde{F} \in \mathbb{A}_P[[x]][y]$ and $\tilde{F}(0, y) = R(y)^N$ where $R(y) = P((y + z^s)^q/z^{tm})$. We have $R(0) = P(z) = 0$ while $R'(0) = qz^{1-s}P'(0)$. As P is square-free and the characteristic of $\mathbb{A}$ does not divide $\deg(P)$ by assumption, we have $P'(0) \in \mathbb{A}^\times$. As $qz^{1-s} \in \mathbb{A}_P^\times$ (if $q > 1$, the assumption $P(0) \in \mathbb{A}^\times$ implies P and Z coprime, that is $z \in \mathbb{A}_P^\times$; if $q = 1$, then $s = 1$), it follows that $R'(0) \in \mathbb{A}_P^\times$. We deduce that $\tilde{F}(0, y) = y^N S(y)$ where y^N and $S(y)$ are coprime in $\mathbb{A}_P[y]$. We conclude thanks to the Weierstrass preparation theorem that F factorises as in (5). Note that $N|d$ by (4). If $N = d$, then (4) forces $\bar{F} = (y + \alpha x^m)^d$ for some $\alpha \in \mathbb{A}$. If $\alpha = 0$, then $\mathcal{N}(F)$ is reduced to a point and we must have $F = y^d$. If $\alpha \ne 0$, the coefficient of y^{d-1} in F is $d\alpha x^{md} + h.o.t$, hence is non zero since the characteristic of $\mathbb{A}$ does not divide d. □

Remark 3. As $P \in \mathbb{A}[Z]$ is square-free, the ring $\mathbb{A}_P = \mathbb{A}[Z]/(P(Z))$ is still isomorphic to a direct product of perfect fields thanks to the Chinese Reminder Theorem. Note also that z^t is invertible: if z is a zero divisor, we must have $q = 1$ so that $t = 0$ and $z^t = 1$.

3.2 Pseudo-irreducible polynomials

The definition of a pseudo-irreducible polynomial is based on a variation of the classical Newton-Puiseux algorithm. Thanks to Lemma 1, we associate to F a sequence a Weierstrass polynomials $H_0, \dots, H_g$ of strictly decreasing degrees $N_0, \dots, N_g$ such that H_k is pseudo-degenerated if $k < g$ and such that either H_g is not pseudo-degenerated either $N_g = 1$ and $H_g = y$. We proceed recursively as follows:

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

$$H_0(x, y) := F(x, y + c_0(x)) \in \mathbb{K}_0[[x]][y]. \tag{6}$$

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 pseudo-degenerated, we let $g = 0$.

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

$$H_{k-1}(z_k^{t_k} x^{q_k}, x^{m_k}(y + z_k^{s_k})) = x^{q_k m_k \ell_k N_k} V_k G_k, \tag{7}$$

where $V_k(0, 0) \in \mathbb{K}_k^\times$ and $G_k \in \mathbb{K}_k[[x]][y]$ is a Weierstrass polynomial of degree N_k. Letting $c_k := -\mathrm{Coef}(G_k, y^{N_k-1})/N_k$, we define

$$H_k(x, y) = G_k(x, y + c_k(x)) \in \mathbb{K}_k[[x]][y]. \tag{8}$$

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 pseudo-degenerated with no terms of degree $N_{k-1} - 1$, we must have $q_k \ell_k > 1$ (see e.g. [19]). 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 $H_g = y$, either $N_g > 1$ and H_g is not pseudo-degenerated. We collect the edge data of the polynomials $H_0, \ldots, H_{g-1}$ in a list

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

Note that $m_k > 0$ for all $1 \le k \le g$. We include the N_k's in the list for convenience (they could be deduced from the remaining data via the relations $N_k = N_{k-1}/q_k \ell_k$).

Definition 5. We say that F is *pseudo-irreducible* if $N_g = 1$.

4 Pseudo-irreducible is equivalent to balanced.

We prove here our main result, Theorem 2: a square-free Weierstrass polynomial $F \in \mathbb{K}[[x]][y]$ is pseudo-irreducible if and only if it is balanced, in which case we compute characteristic exponents and intersection sets of the irreducible factors.

4.1 Notations and main results.

We keep notations of Section 3; in particular $(q_1, m_1, P_1, N_1), \ldots, (q_g, m_g, P_g, N_g)$ denote the edge data of F. We define $e_k := q_1 \cdots q_k$ (current index of ramification), $e := e_g$,

$\hat{e}_k := e/e_k$ and in an analoguous way $f_k := \ell_1 \cdots \ell_k$ (current residual degree), $f := f_g$ and $\hat{f}_k := f/f_k$. For all $k = 1, \dots, g$, we define

$$B_k = m_1\hat{e}_1 + \cdots + m_k\hat{e}_k \quad \text{and} \quad M_k = m_1\hat{e}_0\hat{e}_1 + \cdots + m_k\hat{e}_{k-1}\hat{e}_k \tag{9}$$

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

$$M_k = \sum_{i=1}^{k} (\hat{e}_{i-1} - \hat{e}_i)B_i + \hat{e}_k B_k. \tag{10}$$

Note that $0 < B_1 \le \cdots \le B_g$[6] and $B_0 \le B_g$. We have $B_0 \le B_1$ if and only if $q_1 \le m_1$, if and only if $F = 0$ is not tangent to the x-axis at the origin. We check easily that $\hat{e}_k = gcd(B_0, \dots, B_k)$. In particular, $gcd(B_0, \dots, B_g) = 1$.

Theorem 2. *A Weierstrass polynomial $F \in \mathbb{K}[[x]][y]$ is balanced if and only if it is pseudo-irreducible. It such a case, F has f irreducible factors in $\overline{\mathbb{K}}[[x]][y]$, all with degree e, and*

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

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 is absolutely irreducible.

Corollary 1. *Let $F \in \mathbb{K}[[x]][y]$ be a balanced Weierstrass polynomial. Then, the discriminant of F has valuation*

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

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

Proof. (*of Corollary 1*) When F is balanced, it has f irreducible factors $F_1, \dots, F_f$ of same degree e, with discriminant valuations say $\delta_1, \dots, \delta_f$. The multiplicative property of the discriminant gives the well-known formula

$$\delta = \sum_{1 \le i \le f} \delta_i + \sum_{1 \le i \ne j \le f} (F_i, F_j)_0. \tag{11}$$

Let $y_1, \dots, y_e$ be the roots of F_i. Thanks to [25, Proposition 4.1.3 (ii)] combined with point 1 of Theorem 2, we deduce that for each fixed $a = 1, \dots, e$, 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 $k = 1, \dots, g$. Since $\delta_i = \sum_{1 \le a \ne b \le e} v_x(y_a - y_b)$, we deduce that $\delta_1 = \cdots = \delta_f = \sum_{q_k > 1}(\hat{e}_{k-1} - \hat{e}_k)B_k$. The formula for δ follows directly from (11) combined with point 2 of Theorem 2. □

[6]We may allow $m_1 = B_1 = 0$ when considering non Weierstrass polynomials, see Subsection 5.3.

The remaining part of this section is dedicated to the proof of Theorem 2. It is quite technical, but has the advantage to be self-contained. We first establish the relations between the (pseudo)-rational Puiseux expansions and the classical Puiseux series of F (Subsection 4.2). This allows us to deduce the characteristic exponents and the intersection sets of a pseudo-irreducible polynomial (thanks to Noether-Merle's formula), proving in particular that pseudo-irreducible implies balanced (Subsection 4.3). We prove the more delicate reverse implication in Subsection 4.4.

4.2 Pseudo-rational Puiseux expansion.

Keeping notations of Section 3, let $\pi_0(x,y) = (x, y + c_0(x))$ and $\pi_k = \pi_{k-1} \circ \sigma_k$ where

$$\sigma_k(x,y) := (z_k^{t_k} x^{q_k}, x^{m_k}(y + z_k^{s_k} + c_k(x))) \tag{12}$$

for $k \geq 1$. It follows from equalities (6), (7) and (8) that

$$\pi_k^* F = U_k H_k \in \mathbb{K}_k[[x,y]], \tag{13}$$

for some U_k such that $U_k(0,0) \in \mathbb{K}_k^\times$. We deduce from (12) that

$$\pi_k(x,y) = (\mu_k x^{e_k}, \alpha_k x^{r_k} y + S_k(x)), \tag{14}$$

where $\mu_k, \alpha_k \in \mathbb{K}_k^\times$, $r_k \in \mathbb{N}$ and $S_k \in \mathbb{K}_k[[x]]$ satisfies $v_x(S_k) \leq r_k$. Following [19], we call the parametrisation

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

a pseudo-rational Puiseux expansion (pseudo-RPE for short). Its ring of definition equals the current residue ring $\mathbb{K}_k$, which is a reduced zero-dimensional $\mathbb{K}$-algebra of degree f_k over $\mathbb{K}$. When F is irreducible, the $\mathbb{K}_k$'s are fields and the parametrisation $\pi_k(T,0)$ allows to compute the Puiseux series of F truncated up to precision $\frac{r_k}{e_k}$, which increases with k [19, Section 3.2]. We show here that the same conclusion holds when F is pseudo-irreducible, taking care of possible zero-divisors in $\mathbb{K}_k$. To this aim, we prove by induction an explicit formula for $\pi_k(T,0)$. We need further notations.

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

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

with convention $B_{k,0} = 0$. Note that $Q_{i,0} = e_i$, $Q_{g,i} = \hat{e}_i$ and $B_{g,i} = B_i$ for all $i \leq g$. We have the relations $Q_{k+1,i} = q_{k+1} Q_{k,i}$ and $B_{k+1,i} = q_{k+1} B_{k,i}$ for all $i \leq k$ and $B_{k+1,k+1} = q_{k+1} B_{k,k} + m_{k+1}$.

Coefficients data. For all $0 \leq i \leq k \leq g$, 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

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

with convention $\alpha_{k,0} = 1$. 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 $\alpha_{k+1,k+1} = \alpha_{k+1,k}$.

Lemma 2. *Let $z_0 = 0$ and $s_0 = 1$. 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 recursives relations for $B_{k,i}$, $\mu_{k,i}$ and $\alpha_{k,i}$ above with the 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 α an element of a ring $\mathbb{L}$, we denote by $\alpha^{1/e}$ the residue class of Z in $\mathbb{L}[Z]/(Z^e - \alpha)$. For all $k = 0, \dots, g$, we define the ring extension

$$\mathbb{L}_k := \mathbb{K}_k\big[z_1^{\frac{1}{e}}, \dots, z_k^{\frac{1}{e}}\big].$$

Note that $\mathbb{L}_0 = \mathbb{K}$. Moreover, since $z_k^{1/e}$ has degree $e\ell_k > 1$ over $\mathbb{L}_{k-1}$, the natural inclusion $\mathbb{L}_{k-1} \subset \mathbb{L}_k$ is *strict*.

Remark 4. Note that $\theta_k := \mu_{k,0}^{-1/e_k}$ is a well defined invertible element of $\mathbb{L}_k$ (use Remark 3), which by Lemma 2 plays an important role in the connections between pseudo-RPE and Puiseux series (proof of Proposition 1 below). In fact, we could rather use the "sharp" subring $\mathbb{K}_k[\theta_k] \subset \mathbb{L}_k$ of degree $e_k f_k$ over $\mathbb{K}$, see [21]. We use $\mathbb{L}_k$ for convenience - especially since z_k^{1/q_k} might not lie in $\mathbb{K}_k[\theta_k]$ -, the key points being that $\theta_k \in \mathbb{L}_k$ and that the inclusion $\mathbb{L}_{k-1} \subset \mathbb{L}_k$ is strict.

Proposition 1. *Let $F \in \mathbb{K}[[x]][y]$ be Weierstrass and consider $\tilde{S} := S(\mu^{-1/e}T)$, where $(\mu T^e, S(T)) := \pi_g(T, 0)$. 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 $1 \le k \le g$

$$a_{B_k} = \begin{cases} \varepsilon_k z_k^{\frac{1}{q_k}} & \text{if} \quad q_k > 1 \\ \varepsilon_k z_k + \rho_k & \text{if} \quad q_k = 1 \end{cases} \tag{15}$$

where $\varepsilon_k \in \mathbb{L}_{k-1}^{\times}$ 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 $\mu = \mu_{g,0}$ by Lemma 2, so that $\theta_g := \mu^{-1/e}$ is a well defined invertible element of $\mathbb{L}_g$ (Remark 4). In particular, $\tilde{S} \in \mathbb{L}_g[[T]]$ as required. Lemma 2 applied at rank $k = g$ gives

$$S(T) = \sum_{k=0}^{g} \alpha_{g,k} T^{B_k}\left(z_k^{s_k} + c_k\left(\mu_{g,k}T^{\hat{e}_k}\right)\right). \tag{16}$$

Denote by $\theta_k := \mu_{k,0}^{-1/e_k} \in \mathbb{L}_k^\times$ (Remark 4). Using the definitions of $\mu_{g,k}$ and $\alpha_{g,k}$, a straightforward computation gives

$$\mu_{g,k}\,\theta_g^{\hat{e}_k} = \theta_k \in \mathbb{L}_k \quad \text{and} \quad \alpha_{g,k}\,\theta_g^{B_k} = \prod_{j=1}^{k}\left(\mu_{g,j}\theta_g^{\hat{e}_j}\right)^{m_j} = \prod_{j=1}^{k}\theta_j \in \mathbb{L}_k. \tag{17}$$

Combining (16) and (17), we deduce that $\tilde{S}(T) = S(\theta_g T)$ may be written as

$$\tilde{S}(T) = \sum_{k=0}^{g} U_k(\theta_k T^{\hat{e}_k})T^{B_k}, \quad U_k(T) := \left(z_k^{s_k} + c_k(T)\right)\prod_{j=1}^{k}\theta_j \in \mathbb{L}_k[[T]]. \tag{18}$$

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 (15). As $c_k(0) = 0$, we deduce that

$$U_k(0) = z_k^{s_k}\prod_{j=1}^{k}\theta_j^{m_j} = \varepsilon_k z_k^{1/q_k} \quad \text{with} \quad \varepsilon_k := \prod_{j=1}^{k-1}\theta_j\, z_j^{\frac{-t_j m_k}{q_j\cdots q_k}} \in \mathbb{L}_{k-1}, \tag{19}$$

the second equality using the Bézout relation $s_k q_k - t_k m_k = 1$. Note that $\varepsilon_k \in \mathbb{L}_{k-1}^\times$ (Remarks 3 and 4). Let ρ_k be the sum of the contributions of the terms $T^{B_i}U_i(\theta_i T^{\hat{e}_i})$, $i \neq k$ to the coefficient T^{B_k} of $\tilde{S}$. 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 $U_i(\theta_i T^{\hat{e}_i})T^{B_i}$ contributes to T^{B_k}, then $i < k$ so that $U_i(\theta_i T^{\hat{e}_i})T^{B_i} \in \mathbb{L}_{k-1}[[T^{\hat{e}_{k-1}}]]$. We deduce that $\rho_k \in \mathbb{L}_{k-1}$. Moreover, $\rho_k \neq 0$ forces $\hat{e}_{k-1}|B_k$. Since m_k is coprime to q_k, we deduce from (9) that $q_k = 1$. $\square$

Remark 5. In contrast to the Newton-Puuiseux type algorithms of [19] which compute $\sum_B a_B T^B$ (up to some truncation bound), algorithm `Pseudo-Irreducible` of Section 5.2 only allows to compute $(a_{B_k} - \rho_k)T^{B_k}$, $k = 0,\ldots,g$ in terms of the edge data thanks to (15) and (19). As shown in this section, this is precisely the minimal information required to test pseudo-irreducibility and compute the equi-singularity type. For instance, the Puiseux series of $F = (y-x-x^2)^2 - 2x^4$ are $S_1 = T + T^2(1-\sqrt{2})$ and $S_2 = T + T^2(1+\sqrt{2})$ and we only compute here the "separating" terms $-\sqrt{2}T^2$ and $\sqrt{2}T^2$. Computing all terms of the singular part of the Puiseux series of a (pseudo)-irreducible polynomial in quasi-linear time remains an open challenge.

Let us denote by $W \subset \overline{\mathbb{K}}^g$ the zero locus of the polynomial system defined by the canonical liftings of $P_1,\ldots,P_g$ in $\mathbb{K}[Z_1,\ldots,Z_g]$. Note that $\mathrm{Card}(W) = f$.

Given $\zeta = (\zeta_1,\ldots,\zeta_g) \in W$, the choice of some e^{th}-roots $\zeta_1^{1/e},\ldots,\zeta_g^{1/e}$ in $\overline{\mathbb{K}}$ induces a natural evaluation map

$$ev_\zeta : \mathbb{L}_g \simeq \mathbb{K}\big[z_1^{\frac{1}{e}},\ldots,z_g^{\frac{1}{e}}\big] \longrightarrow \overline{\mathbb{K}}$$

and we denote for short $a(\zeta) \in \overline{\mathbb{K}}$ the evaluation of $a \in \mathbb{L}_g$ at ζ. There is no loss to assume that when $\zeta, \zeta' \in W$ satisfy $\zeta_k = \zeta'_k$, we choose $\zeta_k^{1/e} = \zeta_k'^{1/e}$. We thus have

$$(\zeta_1,\ldots,\zeta_k) = (\zeta'_1,\ldots,\zeta'_k) \quad \Longrightarrow \quad a(\zeta) = a(\zeta') \quad \forall\, a \in \mathbb{L}_k. \tag{20}$$

The following lemma is crucial for our purpose.

Lemma 3. *Let us fix ω such that $\omega^e = 1$ and let $\zeta, \zeta' \in W$. For all $k = 0, \ldots, g$, the following assertions are equivalent:*

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

Proof. By Proposition 1, 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 (20). As 2) $\Rightarrow$ 1) is obvious, we need to show 1) $\Rightarrow$ 3). We show it by induction on k. If $k = 0$, the claim follows immediately since $\hat{e}_0 = e$. Suppose 1) $\Rightarrow$ 3) holds true at rank $k-1$ for some $k \ge 1$. If $a_B(\zeta) = a_B(\zeta')\omega^B$ for all $B \le B_k$, then this holds true for all $B \le B_{k-1}$. As $\varepsilon_k \in \mathbb{L}_{k-1}^\times$ and $\rho_k \in \mathbb{L}_{k-1}$, the induction hypothesis combined with (20) gives $\varepsilon_k(\zeta) = \varepsilon_k(\zeta') \neq 0$ and $\rho_k(\zeta) = \rho_k(\zeta')$. We use now the assumption $a_{B_k}(\zeta) = a_{B_k}(\zeta')\omega^{B_k}$. Two cases occur:

- If $q_k > 1$, we deduce from (15) that $\zeta_k^{1/q_k} = \zeta_k'^{1/q_k}\omega^{B_k}$, so that $\zeta_k = \zeta'_k\omega^{q_k B_k}$. As $\hat{e}_{k-1}$ divides $q_k B_k$ and $\omega^{\hat{e}_{k-1}} = 1$ by induction hypothesis, we deduce $\zeta_k = \zeta'_k$, as required. Moreover, we get $a_{B_k}(\zeta_k) = a_{B_k}(\zeta'_k)$ thanks to (20), so that $\omega^{B_k} = 1$.
- If $q_k = 1$, we deduce from (15) that $\zeta_k + \rho_k(\zeta) = \omega^{B_k}(\zeta'_k + \rho_k(\zeta'))$. As $q_k = 1$ implies $\hat{e}_{k-1} = \hat{e_k}|B_k$, we deduce again $\omega^{B_k} = 1$ and $\zeta_k = \zeta'_k$.

As $B_k = \sum_{s \le k} m_s \hat{e}_s$, 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 $\omega^{\hat{e}_k} = 1$. $\square$

Finally, we can recover all the Puiseux series of a pseudo-irreducible polynomial from the parametrisation $\pi_g(T, 0)$, as required. More precisely :

Corollary 2. *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_ζ has degree e and defines a branch with classical Puiseux parametrisations $(T^e, \tilde{S}_\zeta(T))$ where*

$$\tilde{S}_\zeta(T) = \sum_B a_B(\zeta) T^B. \tag{21}$$

The e Puiseux series of F_ζ are given by $\tilde{S}_\zeta(\omega x^{\frac{1}{e}})$ where ω 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 $\zeta_1^{1/e}, \ldots, \zeta^{1/e}$.

Proof. As F is pseudo-irreducible, $H_g = y$ (see Section 3.2) and $\pi_g^* F(x, 0) = 0$ by (13). We deduce $F(T^e, \tilde{S}_\zeta(T)) = 0$ for all $\zeta \in W$. By (15), we have $a_{B_k}(\zeta) \neq 0$ for all k such that $q_k > 1$. Since $gcd(B_0 = e, B_k \,|\, q_k > 1)) = gcd(B_0, \ldots, B_g) = \hat{e}_g = 1$, the parametrisation $(T^e, \tilde{S}_\zeta(T))$ 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 parametrisation 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 3, these f branches are distinct when ζ runs over W. As $\deg(F) = e\,f$, we obtain in such a way all irreducible factors of F. Considering other choices of the e^{th} roots of the ζ_k's would lead to the same conclusion by construction, and the last claim follows straightforwardly. □

4.3 Pseudo-irreducible implies balanced

Proposition 2. *Let $F \in \mathbb{K}[[x]][y]$ be pseudo-irreducible. Then each branch F_ζ of F has characteristic exponents $(B_0; B_k \,|\, q_k > 1)$, $k = 1, \ldots, g)$.*

Proof. Thanks to Corollary 2, all polynomials F_ζ have same first characteristic exponent $B_0 = e$. We also showed in the proof of Corollary 2 that $a_{B_k}(\zeta) \neq 0$ for all $k \geq 1$ such that $q_k > 1$. We conclude by Proposition 1. □

Proposition 3. *Let $F \in \mathbb{K}[[x]][y]$ be pseudo-irreducible with at least two branches $F_\zeta, F_{\zeta'}$. We have*

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

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

Proof. Noether-Merle's formula (3) combined with Proposition 2 gives

$$(F_\zeta, F_{\zeta'})_0 = \sum_{k \leq K} (\hat{e}_{k-1} - \hat{e}_k) B_k + \hat{e}_K \mathrm{Cont}(F_\zeta, F_{\zeta'}) \tag{22}$$

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 (22) ($q_k = 1$ 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 in formula (2) (see e.g. [6, Lemma 1.2.3]). Combined with Corollary 2, we obtain the formula

$$\mathrm{Cont}(F_\zeta, F_{\zeta'}) = \max_{\omega^e = 1} \left(v_T \left(\tilde{S}_\zeta(T) - \tilde{S}_{\zeta'}(\omega T) \right) \right). \tag{23}$$

We deduce from Lemma 3 that

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

As $\omega = 1$ satisfies $\omega^{\hat{e}_k} = 1$ for all k, we deduce from the last equality that the maximal value in (23) is reached for $\omega = 1$ (it might be reached for other values of ω). 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 (22) 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 (10). Let us fix ζ. As said above, we may choose $\omega = 1$ in (23). 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 ζ' is precisely $\hat{f}_{\kappa-1} - \hat{f}_\kappa$. □

If F is pseudo-irreducible, then it is balanced and satisfies both items of Theorem 2 thanks to Propositions 2 and 3. There remains to show the converse.

4.4 Balanced implies pseudo-irreducible

We need to show that $N_g = 1$ 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, μ after applying (coefficient wise) the evaluation map $ev_\zeta : \mathbb{K}_g \to \overline{\mathbb{K}}$. In what follows, irreducible means absolutely irreducible.

Lemma 4. *Suppose that F is balanced. Then all irreducible factors of all H_ζ, $\zeta \in W$ have same degree.*

Proof. Let $\zeta \in W$ and let y_ζ be a root of H_ζ. As H_ζ divides $(\pi_g^* F)_\zeta$ by (13), we deduce from Lemma 2 (remember $B_{gg} = B_g$) 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

$$\deg_{\overline{\mathbb{K}((x))}}(y_0) = e \deg_{\overline{\mathbb{K}((x))}}(y_\zeta), \tag{24}$$

where we consider here the degrees of y_0 and y_ζ 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 (24), this implies that all roots - hence all irreducible factors - of all H_ζ, $\zeta \in W$ have same degree. □

Corollary 3. *Suppose F balanced and $N_g > 1$. Then there exists 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

$$\bar{H}(x,y) = y^r \tilde{Q}\left(y^q/x^m\right) x^{m \deg(\tilde{Q})} \tag{25}$$

for some non constant monic polynomial $\tilde{Q} \in \mathbb{K}_g[Z]$ with non zero constant term and some integer $r \geq 0$. If $r = 0$, we are done, taking $Q = \tilde{Q}$. Suppose $r > 0$. Let $\zeta \in W$ such that $\tilde{Q}_\zeta(0) \neq 0$. Applying ev_ζ to (25), we deduce that $\mathcal{N}(H_\zeta)$ has a vertice of type (r,i), $0 < r < d$ from which follows the wellknown fact that $H_\zeta = AB \in \overline{\mathbb{K}}[[x]][y]$, with $\deg(A) = r$ and $\deg(B) = q \deg(\tilde{Q})$. By Lemma 4, 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 5. *Suppose F balanced and $N_g > 1$. We keep notations of Corollary 3. Let G be an irreducible factor of F in $\overline{\mathbb{K}}[[x]][y]$. Then $e\,q$ divides $n := \deg(G)$ and there* *exists a unique $\zeta \in W$ and a unique root α of Q_ζ such that G admits a parametrisation $(T^n, S_G(T))$, where*

$$S_G(T) \equiv \tilde{S}_\zeta(T^{\frac{n}{e}}) + \alpha^{\frac{1}{q}} \mu_\zeta^{-\frac{B_g}{e}} T^a \mod T^{a+1}, \tag{26}$$

with $a = \frac{n}{e}B_g + \frac{nm}{eq} \in \mathbb{N}$, $\alpha^{1/q}$ an arbitrary q^{th}-root of α. Conversely, given $\zeta \in W$ and α a root of Q_ζ, there exists at least one irreducible factor G for which (26) holds.

Proof. Let $y_\zeta^{(i)}$, $i = 1, \ldots, N_g$ be the roots of H_ζ. Following the proof of Lemma 4, we know that each root $y_\zeta^{(i)}$ gives rise to a family of e roots of F

$$y_{\zeta,\omega}^{(i)} := \tilde{S}_\zeta(\omega x^{\frac{1}{e}}) + \omega^{B_g} \mu_\zeta^{-\frac{B_g}{e}} x^{\frac{B_g}{e}} y_\zeta^{(i)}(\omega \mu_\zeta^{-\frac{1}{e}} x^{\frac{1}{e}}), \qquad \omega^e = 1. \tag{27}$$

As H_ζ 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 3), we deduce that the $efN_g = \deg(F)$ Puiseux series $y_{\zeta,\omega}^{(i)}$ are distinct, getting all roots of F. Let G be an irreducible factor of F vanishing say at $y_0 = y_{\zeta,\omega}^{(i)}$. The roots of G are $y_0(\omega' x)$, $\omega'^n = 1$, where $n := \deg(G) = \deg_{\overline{\mathbb{K}}((x))}(y_{\zeta,\omega}^{(i)})$. As e divides n (use (24)), it follows from (27) that G vanishes at $y_{\zeta,1}^{(i)}$, hence admits a parametrisation $(T^n, S_G(T))$, where $S_G(T) := y_{\zeta,1}^{(i)}(T^n)$. Corollary 3 ensures that $y_\zeta^{(i)}(x) = \alpha^{1/q} x^{m/q} + h.o.t.$ for some uniquely determined root α of Q_ζ. Combined with (27), we get the claimed formula for S_G. Conversely, if $\zeta \in W$ and $Q_\zeta(\alpha) = 0$, there exists at least one root $y_\zeta^{(i)}$ of H_ζ 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 (26) holds. Finally, since $S_G \in \overline{\mathbb{K}}[[T]]$ and since there exists at least one root $\alpha \neq 0$ of Q_ζ, we must have $nm/eq \in \mathbb{N}$. As $e|n$ and q and m are coprime, we get $eq|n$, as required. □

For a given irreducible factor G of F, we denote by $(\zeta(G), \alpha(G)) \in W \times \overline{\mathbb{K}}$ the unique pair (ζ, α) such that (26) holds. Given $\zeta \in W$, Corollary 3 and Lemma 5 imply that

$$\bar{H}_\zeta = \prod_{i|\zeta(G_i)=\zeta} (y^q - \alpha(G_i) x^m)^{N(G_i)}, \tag{28}$$

where $G_1, \ldots, G_\rho$ stand for the irreducible factors of F and where $N(G_i) := \deg(G_i)/eq$. Note that by Lemma 4, $\deg(G_i)$ and $N(G_i)$ are constant for all $i = 1, \ldots, \rho$.

Corollary 4. *Suppose F balanced and $N_g > 1$. Keeping notations as above, the lists of the characteristic exponents of the G_i's all begin as $\{n\} \cup \{\frac{n}{e}B_k, q_k > 1, k = 1, \ldots, g\}$. The next characteristic exponent 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 $\alpha(G_i) \neq 0$.*

Proof. This follows straightforwardly from Lemma 5 combined with Proposition 1 (similar argument than for Proposition 2). □

Corollary 5. *Suppose F balanced with $N_g > 1$. Then*

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

Proof. Using similar arguments than Proposition 3, we get $\mathrm{Cont}(G_i, G_j) = v_T(S_{G_i} - S_{G_j})$ and we deduce from (26) and Lemma 3 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 (3) combined with Corollary 4. □

Proposition 4. *If F is balanced, then it is pseudo-irreducible.*

Proof. We need to show that $N_g = 1$. Suppose on the contrary that $N_g > 1$. We deduce from (28) that the polynomial Q of Corollary 3 satisfies

$$Q_\zeta(Z) = \prod_{i|\zeta(G_i)=\zeta} (Z - \alpha(G_i))^{n/eq} \tag{29}$$

for all $\zeta \in W$. Let α be a root of Q_ζ and $I_{\zeta,\alpha} := \{i \,|\, (\zeta(G_i), \alpha(G_i)) = (\zeta, \alpha)\}$. Hence, (29) implies that α has multiplicity $\frac{n}{eq}\mathrm{Card}(I_{\zeta,\alpha})$. As F is balanced, all factors have same intersection sets and Corollary 5 implies that all sets $I_{\zeta,\alpha}$ have same cardinality. Thus all roots α of all specialisations Q_ζ, $\zeta \in W$ 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-degenerated (Definition 4), 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 α of some Q_ζ (Corollary 3), we deduce from Corollary 4 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 4 forces all $\alpha(G_i)$ - thus all roots α of all Q_ζ by last statement of Lemma 5 - to be non zero. Thus P has invertible constant term and $H = H_g$ is pseudo-degenerated, contradicting $N_g > 1$. Hence $N_g = 1$ and F is pseudo-irreducible. □

The proof of Theorem 2 is complete. □

5 A quasi-optimal pseudo-irreducibility test

Finally, we explain here the main steps of an algorithm which tests the pseudo-irreducibility of a Weierstrass polynomial and computes its equisingularity type in quasi-linear time with respect to δ, and we illustrate it on some examples. Details can be found in [20, 21].

5.1 Computing the lower boundary polynomial

We still consider $F \in \mathbb{K}[[x]][y]$ a degree d square-free Weierstrass polynomial. In the following, we fix an integer $0 \leq k \leq g$ and assume that $N_k > 1$. For readability, we will omit the index k for the objects $\Psi, V, \Lambda, \mathcal{B}$ introduced below.

Given the edge data $(q_1, m_1, P_1, N_1), \ldots, (q_k, m_k, P_k, N_k)$, we want to compute $\bar{H}_k$ in quasi-linear time with respect to δ.

The (V, Λ) sequence. We define recursively two lists

$$V = (v_{k,-1}, \ldots, v_{k,k}) \in \mathbb{N}^{k+2} \text{ and } \Lambda = (\lambda_{k,-1}, \ldots, \lambda_{k,k}) \in \mathbb{K}_k^{k+2}.$$

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 formulæ:

$$\begin{cases} v_{k,i} = q_k v_{k-1,i} & -1 \leq i < k-1 \\ v_{k,k-1} = q_k v_{k-1,k-1} + m_k \\ v_{k,k} = q_k \ell_k v_{k,k-1} \end{cases} \qquad \begin{cases} \lambda_{k,i} = \lambda_{k-1,i} z_k^{t_k v_{k-1,i}} & -1 \leq i < k-1 \\ \lambda_{k,k-1} = \lambda_{k-1,k-1} z_k^{t_k v_{k-1,k-1} + s_k} \\ \lambda_{k,k} = q_k z_k^{1-s_k-\ell_k} P_k'(z_k) \lambda_{k,k-1}^{q_k \ell_k} \end{cases} \tag{30}$$

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

Approximate roots and Ψ-adic expansion. Given an integer N dividing d, there exists a unique polynomial $\psi \in \mathbb{K}[[x]][y]$ monic of degree d/N such that $\deg(F - \psi^N) < d - d/N$ (see e.g. [15, Proposition 3.1]). We call it the N^{th} *approximate root* of F. Approximate roots are used in an irreducibility criterion in $\mathbb{C}[[x, y]]$ due to Abhyankhar [1].

We denote by ψ_k the N_k^{th}-approximate root of F and we let $\psi_{-1} := x$. We denote $\Psi = (\psi_{-1}, \psi_0, \ldots, \psi_k)$ and introduce the set

$$\mathcal{B} := \{(b_{-1}, \ldots, b_k) \in \mathbb{N}^{k+2} \ , \ b_{i-1} < q_i \, \ell_i \, , i = 1, \ldots, k\}. \tag{31}$$

Thanks to the relations $\deg(\psi_i) = \deg(\psi_{i-1}) q_i \ell_i$ for all $1 \leq i \leq k$, an induction argument shows that F admits a unique expansion

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

where $\Psi^B := \prod_{i=-1}^{k} \psi_i^{b_i}$. We call it the Ψ-*adic expansion* of F. We have necessarily $b_k \leq N_k$ while we do not impose any *a priori* condition to the powers of $\psi_{-1} = x$ in this expansion.

A formula for the lower boundary polynomial. For $i \in \mathbb{N}$, we define the integer

$$w_i := \min \{ \langle B, V \rangle, \ b_k = i, \ f_B \neq 0 \} - v_k(F) \tag{32}$$

where $\langle \, , \, \rangle$ stands for the usual scalar product and with convention $w_i := \infty$ if the minimum is taken over the empty set. We introduce the set

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

for any $i \in \mathbb{N}$ and any $w \in \mathbb{N} \cup \{\infty\}$, with convention $\mathcal{B}(i, \infty) = \emptyset$. We get the following key result:

Theorem 3. *The lower edge $\mathcal{N}_0(H_k)$ coincides with the lower edge of the convex hull of $(i, w_i)_{0 \le i \le N_k}$. The lower boundary polynomial of H_k equals*

$$\bar{H}_k = \sum_{(i,w_i) \in \mathcal{N}_0(H_k)} \left(\sum_{B \in \mathcal{B}(i, w_i + v_k(F))} f_B \Lambda^{B - B_0} \right) x^{w_i} y^i, \tag{33}$$

where $B_0 := (0, \ldots, 0, N_k)$.

Proof. This is a variant of Theorems 2, 3 and 4 in [20], where degeneracy conditions are replaced now by pseudo-degeneracy conditions. The delicate point is that z_k might be here a zero divisor when $q_k = 1$. However, we can show that we always have $\lambda_{kk} \in \mathbb{K}_k^\times$. In particular, (33) is well-defined and a careful reading shows that the proofs of Theorem 2, 3 and 4 in [20] remain valid under the weaker hypothesis of pseudo-degeneracy. We refer to Proposition 6 in the longer preprint [21] for details. □

Example 3. If $F = \sum_{i=0}^{d} a_i y^i$, then $\psi_0 = y - c_0(x)$ where $c_0 = -\frac{a_{d-1}}{d}$. It follows that at rank $k = 0$, the coefficients of the Ψ-adic expansion of F coincide with the coefficients of the (x, y)-adic expansion of H_0 as defined in (6). This illustrates that (33) holds at rank $k = 0$.

5.2 The algorithm

We obtain the following sketch of algorithm. Subroutines `AppRoot`, `Expand` and `EdgeData` respectively compute the approximate root, the Ψ-adic expansion and the edge data.

Algorithm: `Pseudo-Irreducible`(F)
Input: $F \in \mathbb{K}[[x]][y]$ Weierstrass with $\mathrm{Char}(\mathbb{K})$ not dividing $\deg(F)$.
Output: `True` if F is pseudo-irreducible, and `False` otherwise.

$N \leftarrow \deg(F)$, $V \leftarrow (1, 0)$, $\Lambda \leftarrow (1, 1)$, $\Psi \leftarrow (x)$;
while $N > 1$ **do**
    $\Psi \leftarrow \Psi \cup$ `AppRoot`(F, N);
    $\sum_B f_B \Psi^B \leftarrow$ `Expand`(F, Ψ);
    Compute $\bar{H}$ using (33);
    if $\bar{H}$ *is not pseudo-degenerated* **then return** *False*;
    $(q, m, P, N) \leftarrow$ `EdgeData`$(\bar{H})$;
    Update V, Λ using (30)
return *True*

Theorem 4. *Algorithm* `Pseudo-Irreducible` *returns the correct answer.*

Proof. Follows from Definition 5, Theorem 2 and Theorem 3. □

Proof of Theorem 1. We deduce from [20, Prop.12] that algorithm `Pseudo-Irreducible` may run with an expected $\mathcal{O}(\delta)$ operations over $\mathbb{K}$[7]. To this aim, we use:

- Suitable truncation bounds for the powers of x, updated at each step.
- Primitive representation of the various residue rings $\mathbb{K}_k$ (Las-Vegas subroutines)
- Suitable implementation of subroutines `AppRoot`, `Expand`, `EdgeData` and of the pseudo-degeneracy tests (square-free univariate factorisation over direct product of fields, see Remark 1).

If F is pseudo-irreducible, we can deduce from the edge data of F the characteristic exponents and the intersection sets of F (Theorem 2), together with the discriminant valuation δ (Corollary 1). Theorem 1 follows. □

Remark 6. Note that if we rather use computations (7) and (8) up to suitable precision to check if F is pseudo-irreducible (hence balanced), the underlying algorithm has complexity $\mathcal{O}(d\delta)$ when using similar cautious algorithmic tricks as above (see [19, Section 3]). This bound is sharp (see e.g. [20, Example 1]) and is too high for our purpose. One of the main reason is that computing the intermediate polynomials G_k in (7) via Hensel lifting up to sufficient precision might cost $\Omega(d\delta)$. This shows the importance of using approximate roots.

5.3 Non Weierstrass polynomials.

From a computational aspect with a view towards factorisation in $\mathbb{K}[[x]][y]$, it seems interesting to extend Theorems 1 and 2 to the case of non Weierstrass polynomials.

Non Weierstrass balanced polynomials. If F is absolutely irreducible but not necessarily Weierstrass, it defines a unique germ of irreducible curve on the line $x = 0$, with center $(0, c)$, $c \in \overline{\mathbb{K}} \cup \{\infty\}$. It seems to be a natural option to require that the equisingularity type of a germ of plane curve along the line $x = 0$ does not depend on its center. This point of view leads us to 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 $c = \infty$ (note that these change of coordinates have not impact on the tangency with the x-axis). The formula (1) of the intersection multiplicity also extends by linearity to arbitrary coprime polynomials $G, H \in \overline{\mathbb{K}}[[x]][y]$, taking into account the sum of intersection multiplicities between all germs of curves defined by G and H along the line $x = 0$. The intersection might be now zero if (and only if) G and H do not have branches with the same center. We can thus extend the definition of intersection sets to non Weierstrass polynomials, allowing now $0 \in \Gamma(F_i)$. Finally, we may extend Definition 1 to an arbitrary square-free polynomial $F \in \mathbb{K}[[x]][y]$.

[7] In [20, Prop.12], the condition $P_k(0) \in \mathbb{K}_k^\times$ is imposed even if $q_k = 1$, but this has no impact from a complexity point of view.

Pseudo-Irreducibility of non Weierstrass polynomials. We distinguish the monic case, for which approximate roots are defined, and the non monic case.

• If F is monic, the construction of Section 3 remains valid, a slight difference being that the first polynomial H_0 might be now monic (and $m_1 = 0$ is allowed). However the remaining polynomials H_k are still Weierstrass for $k \geq 1$. Hence the definition of a pseudo-irreducible polynomial extends to the monic case and we can check that Theorem 2 still hold for monic polynomials. Moreover, the approximate root of a monic polynomial F are still defined, and it is shown in [20] that Theorem 3 holds too in this case. Hence, we let run algorithm `Pseudo-Irreducible` as in the Weierstrass case. However to keep a small complexity, we do not compute primitive elements of $\mathbb{K}_k$ over the field $\mathbb{K}$ but only over the next residue ring $\mathbb{K}_1 = \mathbb{K}_{P_1}$. The overall complexity of this slightly modified algorithm becomes $\tilde{\mathcal{O}}(\delta + d)$. We refer the reader to [20] for details.

• There remains to consider the case when F is not monic. One way to deal with this problem is to use a projective change of the y coordinates in order to reduce to the monic case. Since $\mathbb{K}$ has at least $d+1$ elements by assumption, we can compute $z \in \mathbb{K}$ such that $F(0, z) \neq 0$ with at most $d+1$ evaluation of $F(0, y)$ at $z = 0, 1, \ldots, d$. This costs at most $\tilde{\mathcal{O}}(d)$ using fast multipoint evaluation [7, Corollary 10.8]. One such a z is found, we can apply the 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 that we simply invert up to suitable precision. We have $\deg(F) = \deg(\tilde{F})$ and $\delta(F) = \delta(\tilde{F})$ (assuming that δ is then defined as the valuation of the resultant between F and F_y instead of the valuation of the discriminant which may vary under projective change of coordinates). So the complexity remains the same. Moreover, F and $\tilde{F}$ have same number of absolutely irreducible factors, same sets of characteristic exponents (by the very definition) and same intersection sets (use that the x-valuation of the resultant is invariant under projective change of the y coordinate (see e.g. [8, Chapter 12]). In particular, F is balanced if and only if $\tilde{F}$ is. This shows that we can test if an arbitrary square-free polynomial F is balanced - and if so, compute the equisingular types of all germs of curves it defines along the line $x = 0$ - within $\tilde{\mathcal{O}}(\delta + d)$ operations over $\mathbb{K}$. We refer the reader to [20] for details.

Remark 7. If F is not monic, we could also have followed the following option. We can extend the construction of Section 3 by allowing positive slopes at the first call (so $m_1 < 0$ is allowed) and extend Theorem 2 by considering approximate roots in the larger ring $\mathbb{K}((x))[y]$. However, it turns out that this option is not compatible with our $PGL_2(\mathbb{K})$-invariant point of view when F defines a germ centered at $(0, \infty)$, and Theorem 2 would require some slight modifications to hold in this larger context.

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 $d = \deg_y(F)$, the well known upper bound $\delta \leq 2nd$ leads to a complexity estimate $\tilde{\mathcal{O}}(nd)$ which is quasi-linear with respect to the arithmetic size of the input. Moreover, up to perform a slight modification of the algorithm, there is no need to assume F square-free in this "algebraic" case (see again [20] for details).

5.4 Some examples

Example 4 (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 root 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 (30), we update $V = (1, 1, 1)$ and $\Lambda = (1, z_1, 3z_1^2 - 1)$. Note that $\mathcal{N}(F)$ is not straight. In particular, F is reducible in $\mathbb{Q}[[x]][y]$.

Step 1. The 2^{th}-approximate root of F is $\psi_1 = y^3 - \frac{3}{2}x^3y - x^2y$ and F has Ψ-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 (32) are ψ_1^2 (for $j = 2$) and $-3\psi_0^2\psi_{-1}^5$ and ψ_{-1}^7 (for $j = 0$). We deduce from (33) 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 edge data $(q_2, m_2, P_2, N_2) = (2, 1, Z_2 - \alpha, 1)$. As $N_2 = 1$, we deduce that F is balanced with $g = 2$.

Conclusion. We deduce from Theorem 2 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 (9), 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 5 (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 root 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 4, 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 (30), 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 Ψ-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 (32) are ψ_1^2 (for $j = 2$) and $-4\psi_{-1}^6\psi_0^2$ (for $j = 0$). We deduce from (33) 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 α 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 factorise F, we would need at this stage to split the algorithm accordingly to the discovered factorisation $P_1 = Z_1(Z_1^2 - 1)$ before continuing the process, as described in [19].

Example 6 (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 root 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 (32), the monomials involved in the lower edge of H_0 are $\psi_0^6, -2\psi_0^4, \psi_0^2$. We deduce from (33) 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 (30), we update $V = (1,0,0)$ and $\Lambda = (1, z_1, 3z_1^2 - 1)$.

Step 1 The $N_1 = 2^{th}$ approximate root of F is $\psi_1 = (y+1)^3 - 3/2x^3(y+1) - (y+1)$ and F has Ψ-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 (32) are ψ_1^2 (for $j = 2$) and $-\psi_{-1}^3$, $-3\psi_{-1}^3\psi_0^2$ (for $j = 0$). We deduce from (33) 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 edge 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 2 (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 (9), we compute $B_0 = e = 2$, $B_1 = 0$, $B_2 = 3$ and $M_1 = 0$, $M_2 = 6$. By Theorem 2, 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.

References

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

[2] A. Campillo. *Algebroid Curves in Positive Characteristic*, volume 378 of *LNCS*. Springer-Verlag, 1980.

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

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

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

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

[9] G.-M. Greuel, C. Lossen, and E. Shustin. *Introduction to singularities and deformation.* Monographs in Mathematics. Springer, 2007.

[10] M. Hodorog, B. Mourrain, and J. Schicho. A symbolic-numeric algorithm for computing the Alexander polynomial of a plane curve singularity. In *Proceedings of the 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 21–28, 2010.

[11] M. Hodorog, B. Mourrain, and J. Schicho. An adapted version of the Bentley-Ottmann algorithm for invariants of plane curve singularities. In *Proceedings of 11th International Conference on Computational Science and Its Applications*, volume 6784, pages 121–131. Springer, 2011.

[12] M. Hodorog and J. Schicho. A regularization method for computing approximate invariants of plane curves singularities. In *Proceedings of the 2011 International Workshop on Symbolic-Numeric Computation*, pages 44–53. SNC, 2011.

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

[14] T.-S. Nguyen, Hong-Duc; Pham and P.-D. Hoang. Topological invariants of plane curve singularities: Polar quotients and lojasiewicz gradient exponents, 2017. arXiv:1708.08295v1.

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

[16] 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.

[17] 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.

[18] 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.

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

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

[21] A. Poteaux and M. Weimann. Using approximate roots for irreducibility and equi-singularity issues in $\mathbb{K}[[x]][y]$, 2019. Preprint arXiv:1904.00286v2.

[22] A. Sommese and C. Wampler. Numerical Solution of Polynomial Systems Arising in Engineering and Science. *World Scientific*, 2005.

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

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

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

[26] 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.

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

[28] O. Zariski. Studies in equisingularity i: Equivalent singularities of plane algebroid curves. *American J. Math*, 87:507–535, 1965.

[29] O. Zariski. Studies in equisingularity ii: Equisingularity in codimension 1 (and characteristic zero). *American J. Math*, 87:972–1006, 1965.

[30] O. Zariski. Studies in equisingularity iii: Saturation of local rings and equisingularity. *American J. Math*, 90:961–1023, 1968.

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