Good Reduction of Puiseux Series and Applications

Adrien Poteaux, Marc Rybowicz

XLIM - UMR 6172
Université de Limoges/CNRS
Department of Mathematics and Informatics
123 Avenue Albert Thomas
87060 Limoges Cedex - France

Abstract

We have designed a new symbolic-numeric strategy to compute efficiently and accurately floating point Puiseux series defined by a bivariate polynomial over an algebraic number field. In essence, computations modulo a well chosen prime number p are used to obtain the exact information needed to guide floating point computations. In this paper, we detail the symbolic part of our algorithm: First of all, we study modular reduction of Puiseux series and give a good reduction criterion to ensure that the information required by the numerical part is preserved. To establish our results, we introduce a simple modification of classical Newton polygons, that we call "generic Newton polygons", which turns out to be very convenient. Finally, we estimate the size of good primes obtained with deterministic and probabilistic strategies. Some of these results were announced without proof at ISSAC '08.

Key words: Puiseux Series, Algebraic Functions, Finite Fields, Symbolic-Numeric Algorithm.

1. Introduction

Let K be a number field (finite extension of $\mathbb{Q}$, the field of rational numbers), and $F(X,Y)$ be a bivariate polynomial in $K[X,Y]$ such that:
- $d_Y = \deg_Y(F) > 0$ and $d_X = \deg_X(F) > 0$,
- F is squarefree and primitive with respect to Y.

If $R_F(X)$ denotes the resultant of F and F_Y, its derivative with respect to Y, then a root of R_F is called a *critical point*. Critical points can also be defined as the set of numbers x_0 such that $F(x_0,Y)$ has less than d_Y roots. Non-critical points will be called *regular*.

Email addresses: adrien.poteaux@unilim.fr (Adrien Poteaux), marc.rybowicz@xlim.fr (Marc Rybowicz).

At $X = x_0$, the d_Y roots of F, viewed as a univariate polynomial in Y, can be represented by fractional Laurent series in $(X - x_0)$ called *Puiseux series*; see Section 3. If x_0 is regular, Puiseux series reduce to classical Laurent series.

Puiseux series are fundamental objects of the theory of algebraic curves (Walker, 1950; Brieskorn and Knörrer, 1986) and provide important information: They give ramification indices of the X-plane covering defined by F, they can be used to compute the genus of the curve defined by F using Riemann-Hurwitz formula, or to compute integral bases and linear spaces associated to divisors on the curve (Bliss, 1933; Duval, 1987; van Hoeij, 1994), which in turn have many applications, such as the determination of parametrizations of genus 0 curves (van Hoeij, 1997), the integration of algebraic functions (Trager, 1984; Bronstein, 1990), or the absolute factorization of polynomials (Duval, 1991).

Moreover, the equation $F(X, Y) = 0$ defines d_Y algebraic functions of the variable X, which are analytic in any simply connected domain $\mathcal{D} \subset \mathbb{C}$ free of critical points. If $\mathcal{D}$ is included in a sufficiently small disc centered at a critical point x_0, it is well-known that numerical approximations of these functions in $\mathcal{D}$ can be obtained directly via truncated Puiseux series at $X = x_0$.

We have used this fact to devise an algorithm to compute the monodromy of the X-plane covering defined by the curve $F(X, Y) = 0$ (Poteaux, 2007). The algorithm follows paths along a minimal spanning tree for the set of critical points; expansions above critical point are used to bypass them. Our ultimate goal was to build an effective version of the celebrated Abel-Jacobi Theorem (Miranda, 1995; Forster, 1981), which requires the integration of algebraic functions along paths on the Riemann Surface defined by F (see Deconinck and van Hoeij (2001) for instance). Again, in this context, Puiseux series are definitely useful (Deconinck and Patterson, 2008).

We know of three methods to compute Puiseux series:

Differential Equation. It has been known for a long time (Comtet, 1964) that Puiseux series can be efficiently computed using the differential equation satisfied by the algebraic functions. More recently, (Chudnovsky and Chudnovsky, 1986, 1987; van der Hoeven, 1999, 2005) have advocated this approach and designed asymptotically fast algorithms, in terms of truncation order and precision required. In our monodromy context, though, we do not need a high precision since we just need enough information to separate functions. Moreover, no differential equation is known a priori; the minimal order differential equation may have high degree coefficients and its determination may be a bottleneck. Bostan et al. (2007) have recenlty proposed a method to reduce the degrees of the coefficients, but this leads to a higher order differential equation. Hence, it is not clear that these asymptotically fast methods are relevant.

Generalized Hensel constructions. Cohn (1984) has proposed a matrix analogue of Hensel's Lemma that gives an alternative proof of Puiseux's Theorem (Theorem 1 below). Diaz-Toca and Gonzalez-Vega (2002) deduced an algorithm that can be viewed as an iterative method to compute the Jordan normal form of a matrix whose eigenvalues are the roots of F, i.e. Puiseux series. But computations are performed in algebraic extensions of K larger than residue fields (see Section 3.3) and there is no evidence that, in its current setting, this approach is competitive.

Hensel lifting has also been extended by several authors to compute factorizations of F in $K[[X]][Y]$ when $X = 0$ is a critical point; see Sasaki and Inaba (2000), who consider the case where X is a multi-variable, and references therein. This method could be used to compute Puiseux series, if there is no ramification or if ramification indices

are known in advance, which is not our case. Moreover, we have found no information on the efficiency and complexity of the method, nor any implementation.

Newton-Puiseux Algorithm. This method is based on Newton polygons and is well-established (Walker, 1950; Brieskorn and Knörrer, 1986). A variant that allows to perform all computations in the residue fields, called "Rational Newton-Puiseux Algorithm", was introduced by Duval (1989). An implementation due to Mark Van Hoeij is available in the Maple library since release V; see also the Magma implementation (Bosma et al., 1997). Our approach is based on the Newton-Puiseux algorithm and its rational version; we shall give details in Section 4.

Unfortunately, applying a floating point Newton-Puiseux algorithm above a critical point is doomed to failure. Indeed, if the critical point x_0 is replaced with an approximation, expansion algorithms return approximate series with very small convergence discs and do not retain important information, such as ramification indices. Therefore, the output is not aidful.

On the other hand, coefficient growth considerably slows down symbolic methods. Since the degree of R_F may be equal to $d_X(2d_Y - 1)$, a critical point x_0 may be an algebraic number with large degree. Furthermore, Puiseux series coefficients above x_0 may belong to a finite extension of degree d_Y over $K(x_0)$: For $d_Y = d_X = 10$, the degree over K may already be excessively large for practical computations. Moreover, when these coefficients are expressed as linear combinations over $\mathbb{Q}$, the size of the rational numbers involved may also be overwhelming. Floating point evaluation of such coefficients must, in some cases, be performed with a high number of digits because spectacular numerical cancellations occur; see examples in (Poteaux, 2007). For instance, the degree 6 polynomial $F(X,Y) = (Y^3 - X)\,((Y-1)^2 - X)\,(Y - 2 - X^2) + X^2\,Y^5$ has a resultant $R_F(X) = X^3\,P(X)$, where $P(X)$ is an irreducible polynomial of degree 23 over $\mathbb{Q}$. Rational Puiseux series (see Section 3.3) above roots of $P(X)$ have coefficients in a degree 23 extension of $\mathbb{Q}$. Rational numbers with 136 digits appear in the first term of the expansions. Walsh (2000) has shown that, for any $\epsilon > 0$, the singular part of Puiseux series can be computed using $O(d_Y^{32+\epsilon} d_X^{4+\epsilon} \log h^{2+\epsilon})$ bit operations, where h is the height of F. Although this bound is probably not sharp, it is not encouraging and tends to confirm fast coefficient growth.

To alleviate these problems, we have introduced a symbolic-numeric approach: exact relevant information is first obtained by means of computation modulo a well chosen prime number p, then this information is used to guide floating point computations. The coefficient size is therefore kept under control while numerical instability is reduced. Experimental evidences reported in Poteaux (2007) seem to validate this approach. Exact important data, such as ramification indices, Puiseux pairs and intersection multiplicities of branches, are preserved by our reduction criterion; as a byproduct, we also obtain a modular method to compute the genus of a plane curve and the topological type of its singularities (Zariski, 1981; Campillo, 1980).

This paper presents several contributions:

- We introduce "generic Newton polygons" and "polygon trees" (Section 4). The latter captures precisely the symbolic information needed for floating point computations and other aplications.
- We study modular reduction of Puiseux series and rational Puiseux expansions. This leads to a fully proved and easy to check criteria for the choice of a "good prime" p such that polygon trees can be obtained using modular arithmetic (Section 5). We rely on technical results that are proven or recalled in Section 3 and 4.

- Finally, we study deterministic and probabilistic methods to obtain such a prime and give estimates for the size of p (Section 6). It turns out that probabilistic methods yield primes with logarithmic size, with respect to the size of F.

Many of these results were announced without proofs by Poteaux and Rybowicz (2008) at ISSAC '08, and only for F monic. This paper is an extended and (almost) self-contained version that includes all proofs and additional material such as the non monic case, which requires some care, as well as a global good reduction criterion.

In (Poteaux and Rybowicz, 2009), we study how to efficiently implement the rational Newton-Puiseux algorithm over finite fields and deduce improved arithmetic complexity bounds. Combined with our results herein about the size of a good prime, they give estimates for the bit-complexity of the symbolic part of our symbolic-numeric method, as well as bit-complexity estimates for the computation of the genus and similar problems.

Obtaining floating point Puiseux series from polygon trees is not a trivial task. A first method was briefly described in (Poteaux, 2007) and experimental results were provided. A more elegant and more appropriate approach based on Singular Value Decomposition is given in (Poteaux, 2008); this will be the topic of a forthcoming article.

Finally, we remark that modular methods are extensively used in Computer Algebra to avoid intermediate coefficient swell, via Hensel lifting or the Chinese Remainder Theorem; see for instance von zur Gathen and Gerhard (1999). However, a "reduce mod p and lift" or "reduce mod p_i and combine" method would not help much in this case since we are not facing an intermediate coefficient growth problem, but an intrinsically large symbolic output. Modular methods are much less common when it comes to directly obtaining numerical results. We therefore claim some originality with this approach.

2. Notations and assumptions

We collect herein a number of notations and assumptions that will be used throughout the paper. We also recall well-known facts.

- In this paper, all fields are commutative. Moreover, for each field L considered, there exists an algorithm to factorize polynomials with coefficients in L.
- If L is a field, $\overline{L}$ will denote an algebraic closure of L and $L^* = L \setminus \{0\}$.
- For each positive integer e, ζ_e is a primitive e-th root of unity in $\overline{L}$. Primitive roots are chosen so that $\zeta_{ab}^b = \zeta_a$.
- v_X denotes the X-adic valuation of the fractional power series field $L((X^{1/e}))$, normalized with $v_X(X) = 1$. If $S \in L((X^{1/e}))$, we denote by $\mathrm{tc}(S)$ the trailing coefficient of S, namely $S = \mathrm{tc}(S)X^{v_X(S)} + \text{terms of higher order}$.
- The degree and leading coefficient of a polynomial U in the variable X are respectively denoted by $d_X(U)$ and $\mathrm{lc}_X(U)$. For our input polynomial F, we use the shortcuts $d_X = d_X(F), d_Y = d_Y(F)$. The derivative with respect to a variable X is denoted U_X.
- If $S = \sum_k \alpha_k X^{k/e}$ is a fractional power series in $L((X^{1/e}))$ and r is a rational number, $\widetilde{S}^r$ denotes the truncated power series $\widetilde{S}^r = \sum_k^N \alpha_k X^{k/e}$ where $N = \max\{k \in \mathbb{N} \mid \frac{k}{e} \leq r\}$. We generalize this notation to elements of $L((X^{1/e}))[Y]$ by applying it coefficient-wise. In particular, if $H \in L[[X]][Y]$ is defined as $H = \sum_i (\sum_{k\geq 0} \alpha_{ik} X^k) Y^i$, then $\widetilde{H}^r = \sum_i (\sum_{k=0}^{\lfloor r \rfloor} \alpha_{ik} X^k) Y^i$.
- If U is a univariate polynomial, then Δ_U denotes the discriminant of U and R_U denotes the resultant of U and its derivative. If U is a multivariate polynomial, the context will always allow to identify the variable.

- If $U(T)$ (resp. $V(T)$) is a separable univariate polynomial of degree r (resp. s) with roots $\{u_1, \ldots, u_r\}$ (resp. $\{v_1 \ldots, v_s\}$) and leading coefficient u (resp. v), then:

$$\Delta_U = \pm u^{2r-2} \prod_{\substack{1 \le i,j \le r \\ i \ne j}} (u_i - u_j) \qquad \text{Resultant}(U,V) = u^s v^r \prod_{\substack{1 \le i \le r \\ 1 \le j \le s}} (u_i - v_j). \tag{1}$$

- If U is a univariate polynomial that admits a factorization into a product of polynomials $U = \prod_{i=1}^{r} U_i$, then:

$$\Delta_U = \prod_{i=1}^{r} \Delta_{U_i} \prod_{\substack{1 \le i,j \le r \\ i \ne j}} \text{Resultant}(U_i, U_j). \tag{2}$$

- For each i with $0 \le i \le e-1$, we denote $[i,e]$ the automorphism:

$$\begin{aligned} [i,e] \ : \overline{L}((X^{1/e})) &\to \overline{L}((X^{1/e})) \\ X^{1/e} &\mapsto \zeta_e^i X^{1/e} \end{aligned}$$

  When the ramification index can be deduced from the context, we shall simply write $[i]$ instead of $[i,e]$. If $S \in \overline{L}((X^{1/e})$, the image of S under $[i]$ is denoted by $S^{[i]}$. This notation extends naturally to any polynomial with coefficient in $\overline{L}((X^{1/e})$. It is obvious that elements of the subfield $\overline{L}((X))$ are invariant under $[i]$.
- Let f be a polynomial in $L[T]$ with squarefree factorization $f = \prod_{i=1}^{r} f_i^{k_i}$; that is, the k_i are pairwise distinct positive integers and the f_i are relatively prime polynomials with positive degrees. We associate to f the partition of $\deg f$ denoted $[f] = (k_1^{\deg f_1} \ldots k_r^{\deg f_r})$. Namely, the multiplicity k_i is repeated $\deg f_i$ times in the decomposition of $\deg f$. We shall call this partition the *multiplicity structure of* f.
- For a multivariate polynomial $H(\underline{X}) = \sum_{\underline{k}} \alpha_{\underline{k}} \underline{X}^{\underline{k}} \in \mathbb{C}[\underline{X}] = \mathbb{C}[X_1, \ldots, X_n]$, where $\underline{k}$ is a multi-index, we introduce: $\|H\|_\infty = \max_{\underline{k}} \{|\alpha_{\underline{k}}|\}$.

3. Puiseux series

We need to state results over more general fields than K. Throughout the section, L stands for a field of characteristic $p \ge 0$. If H is a polynomial of $L[X,Y]$, we shall say that *L and H satisfy the characteristic condition* if:

$$p = 0 \quad \text{or} \quad p > d_Y(H) \tag{3}$$

Up to a change of variable $X \leftarrow X + x_0$, we assume that $X = 0$ is a critical point and we begin by reviewing a number of classical results regarding Puiseux series above 0.

3.1. Classical Puiseux series

Theorem 1 (Puiseux)**.** *Let H be a squarefree polynomial of $L[X,Y]$ with $d_Y(H) > 0$.*

- *If condition (3) is satisfied by H, there exist positive integers $e_1, \ldots, e_s$ satisfying $\sum_{i=1}^{s} e_i = d_Y(H)$ such that H (viewed as a polynomial in Y) has $d_Y(H)$ distinct roots in $\overline{L((X))}$ that can be written:*

$$S_{ij}(X) = \sum_{k=n_i}^{+\infty} \alpha_{ik}\, \zeta_{e_i}^{jk}\, X^{\frac{k}{e_i}}$$

where $1 \leq i \leq s$, $0 \leq j \leq e_i - 1$, $n_i \in \mathbb{Z}$ *and* $\alpha_{in_i} \neq 0$ *if* $S_{ij} \neq 0$*; if* $S_{ij} = 0$*, we set* $n_i = 0$ *and* $e_i = 1$*. Moreover, the set of coefficients* $\{\alpha_{ik}\}$ *is included in a finite algebraic extension of* L*.*

- *If* $p = 0$*, then:*

$$\overline{L(X)} \subset \overline{L((X))} = \bigcup_{e \in \mathbb{N}^*} \overline{L}((X^{1/e}))$$

Proof. If $p = 0$, see Brieskorn and Knörrer (1986); Eichler (1966); Walker (1950) or most textbooks about algebraic functions. For $p > 0$, condition (3) ensures that there is no obstruction to the existence of the S_{ij}; see Chevalley (1951, Chap. IV, Sec. 6). □

Definition 2. These $d_Y(H)$ fractional Laurent series are called *Puiseux series of* H *above 0*. The integer e_i is the *ramification index* of S_{ij}. If $e_i > 1$, then S_{ij} is *ramified*. If $S_{ij} \in \overline{L}[[X^{1/e_i}]]$, we say that S_{ij} *is defined at* $X = 0$. If $S_{ij}(0) = 0$, we say that S_{ij} *vanishes at* $X = 0$.

For each positive integer $e \leq d_Y(H)$, condition (3) implies that the Galois group $\mathbb{G}_e$ of $\overline{L}((X^{1/e}))/\overline{L}((X))$ is cyclic and generated by $[1] : X^{1/e} \mapsto \zeta_e X^{1/e}$. Hence, $\mathbb{G}_{e_i}$ permutes cyclically the elements of the set $S_i = \{S_{ij}(X)\}_{0 \leq j \leq e_i - 1}$.

Definition 3. We call S_i *a cycle of* H *above 0*. If elements of S_i vanish at $X = 0$, we say that *the cycle vanishes at* $X = 0$.

Since the S_{ij} $(0 \leq j \leq e_i - 1)$ can be quickly recovered, both symbolically and numerically, from any element of S_i, it is sufficient for our purposes to compute a set of representatives for the cycles of H.

Definition 4. The *regularity index* r_{ij} *of* S_{ij} *in* H is the least integer N such that $\widetilde{S_{ij}}^{\frac{N}{e_i}} = \widetilde{S_{uv}}^{\frac{N}{e_i}}$ implies $(u, v) = (i, j)$; $\widetilde{S_{ij}}^{\frac{r_{ij}}{e_i}}$ is called the *singular part of* S_{ij} *in* H.

In other words, r_{ij} is the smallest number of terms necessary to distinguish S_{ij} from the other Puiseux series above 0. It is worth noting that r_{ij} depends not only on S_{ij}, but also on H since H is not assumed irreducible in $L[X, Y]$; see examples in Section 4.2.

If the singular part of a Puiseux series is known, a change of variable yields a bivariate polynomial for which remaining terms of the series can be computed "fast" using quadratic Newton iterations (Kung and Traub, 1978; von zur Gathen and Gerhard, 1999). Newton iterations can be applied to series with floating point coefficients, therefore we focus on the computation of the singular parts of the S_{ij}. Since it can be shown that all elements of a cycle S_i have the same regularity index, that we denote r_i, the problem reduces to the determination of the singular part of a representative of S_i for $1 \leq i \leq s$.

When $L \subset \mathbb{C}$, the S_{ij} converge in the pointed disc $\mathring{D}(0, \rho) = \{x \in \mathbb{C} \mid 0 < |x| < \rho\}$ where ρ is equal to the distance from 0 to the nearest (nonzero) critical point (Markushevich, 1967). If we choose a determination for the e_i-th root functions, the S_{ij} define $d_Y(H)$ analytic functions in any domain $\mathcal{D}$ that is included in this convergence pointed disc and does not intersect the branch cut. To evaluate accurately these functions in $\mathcal{D}$, we need to:

- Control truncation orders of Puiseux series; bounds are given in Poteaux (2007).

- Compute efficiently floating point approximation of the truncated S_{ij}; this is the goal of our symbolic-numeric method and the point where the present work about good reduction comes into play (Poteaux, 2008).
- Give error bounds for the approximations of the α_{ik} and study the algorithm numerical stability. This topic has not been addressed yet, but experimental results obtained with our Maple prototype are promising.

3.2. The characteristic of a Puiseux series

We now derive relations between particular coefficients of a Puiseux series $S(X) = \sum_{i=n}^{\infty} \alpha_i X^{i/e} \in L((X^{1/e}))$ with ramification index $e > 1$ and the discriminant of its minimal polynomial, that we shall use to define our good reduction criterion.

We define a finite sequence $(B_0, R_0), (B_1, R_1), \ldots, (B_g, R_g)$ of integer pairs as follows:

- $R_0 = e$, $B_0 = -\infty$.
- If $R_{j-1} > 1$, we define $B_j = \min\{i > B_{j-1} \mid \alpha_i \neq 0 \,\text{and}\, i \not\equiv 0 \bmod R_{j-1}\}$ and $R_j = |\gcd(B_j, R_{j-1})|$. If $R_{j-1} = 1$, we stop and set $g = j - 1$. Note that $g \geq 1$ and $R_g = 1$.

Finally, we set $Q_j = R_{j-1}/R_j > 1$, $M_j = B_j/R_j$ for $1 \leq j \leq g$, $M_0 = n/e$ and define H_j to be the largest integer such that $H_j + M_j < M_{j+1}/Q_{j+1}$. It is clear that $e = Q_1 Q_2 \cdots Q_g$ and M_j is an integer prime to Q_j.

After a change of coefficient indices, S can be written:

$$\begin{aligned} S(X) = & \textstyle\sum_{j=0}^{H_0} \alpha_{0,j} X^{M_0+j} \\ & + \gamma_1 X^{\frac{M_1}{Q_1}} && + \textstyle\sum_{j=1}^{H_1} \alpha_{1,j} X^{\frac{M_1+j}{Q_1}} \\ & + \gamma_2 X^{\frac{M_2}{Q_1 Q_2}} && + \textstyle\sum_{j=1}^{H_2} \alpha_{2,j} X^{\frac{M_2+j}{Q_1 Q_2}} \\ & + \cdots && + \cdots \\ & + \gamma_g X^{\frac{M_g}{Q_1 Q_2 \cdots Q_g}} && + \textstyle\sum_{j=1}^{\infty} \alpha_{g,j} X^{\frac{M_g+j}{Q_1 Q_2 \cdots Q_g}} \end{aligned} \tag{4}$$

In (4), monomials of S are ordered by strictly increasing (rational) degree.

Definition 5 (Zariski (1981); Brieskorn and Knörrer (1986))**.** The *characteristic* of S is the tuple of integers $(e; B_1, \ldots, B_g)$. The *characteristic coefficients* (resp.*monomials*) are the elements of the sequence $(\gamma_1, \ldots, \gamma_g)$ (resp. corresponding monomials of S).

Proposition 6. *Let $G(X, Y)$ be the minimal polynomial over $\overline{L}((X))$ of a ramified Puiseux series $S \in \overline{L}((X^{1/e}))$ as above. Let $\Delta_G(X)$ be the discriminant of G with respect to Y. Assume that hypothesis (3) is satisfied for G. Then:*

$$\mathrm{tc}(\Delta_G) = \pm\Big(\prod_{i=1}^{g} Q_i^{R_i} \prod_{i=1}^{g} \gamma_i^{R_{i-1}-R_i}\Big)^e \tag{5}$$

$$v_X(\Delta_G) = \sum_{i=1}^{g} B_i(R_{i-1} - R_i) \tag{6}$$

Proof. We first introduce the notations $v = v_X(\Delta_G)$ and $\theta = \mathrm{tc}(\Delta_G)$. The conjugates of S over $\overline{L}((X))$ are $\{S^{[i]}\}_{0 \leq i \leq e-1}$, therefore:

$$\Delta_G = \pm \prod_{\substack{0 \leq i,j \leq e-1 \\ i \neq j}} (S^{[i]} - S^{[j]}).$$

From this relation and (4), we note that v depends only on the contribution of terms $X^{B_i/e} = X^{M_i/(Q_1 \cdots Q_i)}$. Hence, if we consider the γ_i as unknowns, v is determined by the exponent of γ_i in θ. Therefore, if (5) is true, so is (6) since:

$$v = \sum_{i=1}^{g} e\,(R_{i-1} - R_i)\frac{B_i}{e} = \sum_{i=1}^{g} B_i(R_{i-1} - R_i).$$

In order to prove (5), we proceed by induction on g. For each positive integer r let δ_r be the discriminant of $X^r - 1$, that is $\delta_r = \pm r^r$.

If $g = 1$, the expansion of Δ_G in increasing fractional powers of X is:

$$\begin{aligned}\Delta_G &= \prod_{\substack{0 \le i,j \le e-1 \\ i \ne j}} \left(\gamma_g(\zeta_e^{M_g i} - \zeta_e^{M_g j})X^{M_g/Q_g} + \cdots\right) \\ &= \gamma_g^{e(e-1)} \left(\prod_{\substack{0 \le i,j \le e-1 \\ i \ne j}} (\zeta_e^{M_g i} - \zeta_e^{M_g j})\right) X^{e(e-1)M_g/Q_g} + \cdots\end{aligned}$$

Since M_g is prime to Q_g and $Q_g = e$, $\zeta_e^{M_g}$ is a primitive e-th root of unity. We obtain $\theta = \delta_e \gamma_g^{e(e-1)} = \pm Q_g^{Q_g} \gamma_g^{e(R_{g-1} - R_g)}$ as expected.

We now assume that $g > 1$. To simplify notations, we set $Q = Q_1$ and $R = R_1 = Q_2 \cdots Q_g$. We define $H \in \overline{L}((X^{1/Q}))[Y]$ as follows:

$$H = \prod_{i=0}^{R-1} (Y - S^{[i\,Q]}).$$

Since $[Q] = [Q, e]$ generates the Galois group of $\overline{L}((X^{1/e}))$ over $\overline{L}((X^{1/Q}))$, H is the minimal polynomial of S over $\overline{L}((X^{1/Q}))$. Moreover, the factorization of G over $\overline{L}((X^{1/Q}))$ is given by:

$$G = \prod_{i=0}^{Q-1} H^{[i]}.$$

Using relation (2), we obtain $\Delta_G = \Pi_1 \Pi_2$ where:

$$\Pi_1 = \prod_{i=0}^{Q-1} \Delta_{H^{[i]}} \qquad \Pi_2 = \prod_{\substack{0 \le i,j \le Q-1 \\ i \ne j}} \text{Resultant}(H^{[i]}, H^{[j]}).$$

We need to evaluate the contribution to θ of Π_1 and Π_2. We first consider Π_1. Let $U(X, Y) = H(X^Q, Y)$ be the minimal polynomial of $S(X^Q)$ over $\overline{L}((X))$. Since U has characteristic $(R; B_2, \ldots, B_g)$, our induction hypothesis yields:

$$\Delta_U = (\pm \prod_{i=2}^{g} Q_i^{R_i} \prod_{i=2}^{g} \gamma_i^{R_{i-1} - R_i})^R X^u + \cdots$$

for some positive integer u. Therefore:

$$\Delta_{H^{[j]}} = \zeta_e^{uRj} (\pm \prod_{i=2}^{g} Q_i^{R_i} \prod_{i=2}^{g} \gamma_i^{R_{i-1} - R_i})^R X^{\frac{u}{Q}} + \cdots$$

Since $Q\,R = e$ and $\zeta_e^{uR\,j} = \zeta_Q^{u\,j}$ the contribution of Π_1 to θ is:

$$\pm(\prod_{i=2}^{g} Q_i^{R_i} \prod_{i=2}^{g} \gamma_i^{R_{i-1}-R_i})^e \tag{7}$$

We now estimate the contribution of Resultant$(H^{[i]}, H^{[j]})$. Each difference of roots in the product defining the resultant has the form:

$$\gamma_1(\zeta_Q^{M_1 i} - \zeta_Q^{M_1 j})(X^{M_1/Q_1} + \dots)$$

and there are R^2 such differences. Since there are $Q(Q-1)$ resultants in the product and $\zeta_Q^{M_1}$ is a primitive Q-th root of unity, we conclude that the contribution of Π_2 to θ is:

$$\gamma_1^{R^2Q(Q-1)}(\prod_{\substack{0\le i,j\le Q-1\\ i\neq j}} \zeta_Q^{M_1 i} - \zeta_Q^{M_1 j})^{R^2} = \gamma_1^{R^2Q(Q-1)}\delta_Q^{R^2} = \pm Q_1^{eR_1}\gamma_1^{e\,(R_0-R_1)}$$

Combining the last expression with (7) gives (5). □

The expression for $v_X(\Delta_G)$ is well-known; see for instance Zariski (1981). It can be expressed as the sum of a differential exponent and of a conductor degree. In Singularity Theory, it also has an interpretation in terms of "infinitely near point" multiplicities (Brieskorn and Knörrer, 1986). However, the expression for $\mathrm{tc}(\Delta_G)$ seems knew.

3.3. Rational Puiseux expansions

In order to perform computations in the smallest possible extension of L and to take advantage of conjugacy over L, Duval (1987) introduced "rational Puiseux expansions over L". This arithmetical concept is irrelevant in the context of floating point computations, but will prove useful for expansions over finite fields.

Remark 7. Slightly different definitions of "rational Puiseux expansions over L" appeared in Duval (1989) and Walsh (1999). The definition given therein corresponds to "rational Puiseux expansions over $\overline{L}$" in the sense of Duval (1987) and in the sense of the present article.

Definition 8. Let H be a polynomial in $L[X,Y]$. A *parametrization* $R(T)$ of H is a pair $R(T) = (X(T), Y(T)) \in \overline{L}((T))^2$ such that $H(X(T), Y(T)) = 0$ in $\overline{L}((T))$. The parametrization is *irreducible* if there is no integer $u > 1$ such that $R(T) \in \overline{L}((T^u))^2$. The *coefficient field* of $R(T)$ is the extension of L generated by the coefficients of $X(T)$ and $Y(T)$.

Assume for a moment that H is irreducible in $L[X,Y]$ so that $\mathcal{K} = L(X)[Y]/(H)$ is an algebraic function field. A parametrization $R(T) = (X(T), Y(T))$ induces a field morphism:

$$\begin{aligned} \phi_R \;:\quad & \mathcal{K} \to \overline{L}((T)) \\ & f(X,Y) \mapsto f(X(T), Y(T)) \end{aligned}$$

Composing ϕ_R with the valuation v_T of $\overline{L}((T))$, we obtain a valuation of $\mathcal{K}$ that we denote again by v_T. It is easily seen that the set $\mathfrak{P}_R = \{f \in \mathcal{K} \,|\, v_T(f) > 0\}$ is a *place* of $\mathcal{K}$ in the sense of Chevalley (1951) and that $V_R = \{f \in \mathcal{K} \,|\, v(f) \ge 0\}$ is the corresponding V-ring

of $\mathcal{K}$. We recall that $\mathfrak{P}_R$ is the unique maximal ideal of V_R. The *residue field* $V_R/\mathfrak{P}_R$ of $\mathfrak{P}_R$ is a finite algebraic extension of L. Therefore, we obtain a mapping Ψ from the set of parametrizations of F onto the set of places of $\mathcal{K}$. Reciprocally, parametrizations of H can be associated to each place $\mathfrak{P}$.

We denote by $\{\mathfrak{P}_i\}_{1\leq i\leq r}$ the places of $\mathcal{K}$ dividing X and by k_i the residue field of $\mathfrak{P}_i$.

Definition 9 (Rational Puiseux expansions)**.**

- Assume that H is irreducible in $L[X,Y]$, with $d_Y(H) > 0$. A *system of L-rational Puiseux expansions above 0 of H* is a set of irreducible parametrizations $\{R_i\}_{1\leq i\leq r}$ of the form:
$$R_i(T) = (X_i(T), Y_i(T)) = \left(\gamma_i T^{e_i}, \sum_{k=n_i}^{+\infty} \beta_{ik} T^k\right) \in \overline{L}((T))^2$$
with $e_i > 0, n_i \in \mathbb{Z}$ such that:
(i) Ψ is one-to-one from $\{R_i\}_{1\leq i\leq r}$ to $\{\mathfrak{P}_i\}_{1\leq i\leq r}$
(ii) the coefficient field of R_i is isomorphic to k_i, assuming the $\mathfrak{P}_i$ indexed so that $\mathfrak{P}_i = \Psi(R_i)$.
- Assume that H is squarefree, with $d_Y(H) > 0$. A *system of L-rational Puiseux expansions above 0 of H* is the union of systems of L-rational Puiseux expansions for the irreducible factors of H in $L[X,Y]$ with positive degree in Y.

Definition 10. We say that R_i is *defined at* $T = 0$ if $Y_i \in \overline{L}[[T]]$. In this case, the *center* of R_i is the pair $(X_i(0), Y_i(0)) \in \overline{L}^{\,2}$.

The classical formula relating degrees of residue fields and ramification indices of an algebraic function field (Chevalley, 1951) translates into:

Theorem 11. *Let $H \in L[X,Y]$ be squarefree and $d_Y(H) > 0$. Let $\{R_i\}_{1\leq i\leq r}$ be a system of L-rational Puiseux expansions above 0 for H. Let f_i stand for $[k_i : L]$. Then:*
$$\sum_{i=1}^{r} e_i\, f_i = d_Y(H)$$

Classical Puiseux series can readily be deduced from a system of rational Puiseux expansions:

(1) R_i has exactly f_i conjugates over L, that we denote R_i^σ $(1 \leq \sigma \leq f_i)$.
$$R_i^\sigma(T) = (X_i^\sigma(T), Y_i^\sigma(T)) = \left(\gamma_i^\sigma T^{e_i}, \sum_{k=n_i}^{\infty} \beta_{ik}^\sigma T^k\right)$$
(2) Each R_i^σ yields a Puiseux series $Y_i^\sigma((X/\gamma_i^\sigma)^{1/e_i})$. The set of all such series form a set of representatives for set of cycles $\{S_l\}_{1\leq l\leq s}$ of H above 0.
(3) The d_Y Puiseux series are finally obtained using the action of $\mathbb{G}_{e_i}$, $1 \leq i \leq s$.

In particular, classical Puiseux series defined at $X = 0$ (resp. vanishing at $X = 0$) correspond to rational Puiseux expansions defined at $T = 0$ (resp. centered at $(0,0)$).

Regularity indices for all Puiseux series corresponding to the same rational Puiseux expansion are equal. Therefore, we define the singular part of a rational Puiseux expansion

R_i to be the pair:

$$\left(\gamma_i T^{e_i}, \sum_{k=n_i}^{r_i} \beta_{ik} T^k\right)$$

where r_i is the regularity index of a Puiseux series associated to R_i.

It is worth noting that, unlike classical Puiseux series, rational Puiseux expansions are not canonically defined. Replacing T by γT in $R_i(T) = (X_i(T), Y_i(T))$ with γ chosen in the coefficient field of R_i yields another rational Puiseux expansion corresponding to the same place. The choice of γ_i can have dramatic consequences on coefficient size and algorithm performance; see Section 6.3 for more comments.

4. The Newton-Puiseux algorithm

In this section, we focus on Duval's variant of Newton-Puiseux's algorithm to compute singular parts of rational Puiseux expansions, and view as a particular case the classical version that computes Puiseux series. Both methods are used by our symbolic-numeric strategy: Duval's rational method is used for finite fields, while the numeric part is based on the classical algorithm. We also explain how coefficients computed by the two methods are related; this will prove useful to understand modular reduction of rational Puiseux expansions.

Newton polygons and characteristic polynomials are the crucial tools. We first recall well-known definitions and introduce a variant that will prove more convenient and powerful. Throughout the section, L stands again for a field of characteristic $p \geq 0$.

4.1. Generic Newton polygons and characteristic polynomials

Assume that $H(X, Y) = \sum_{i,j} a_{ij} X^j Y^i$ is a polynomial of $L[[X]][Y]$ satisfying characteristic condition (3) and $H(0, Y) \neq 0$. The Newton polygon of H is classically defined as follow:

Definition 12. For each pair (i, j) of $\mathrm{Supp}(H) = \{(i, j) \in \mathbb{N}^2 \,|\, a_{ij} \neq 0\}$, define $Q_{ij} = \{(i', j') \in \mathbb{R}^2 \mid i' \geq i \text{ and } j' \geq j\}$. The *Newton Polygon* $\mathcal{N}(H)$ of H is the set of finite edges of the convex hull $\mathcal{H}$ of $Q(H) = \cup_{(i,j)\in \mathrm{Supp}(H)} Q_{ij}$.

In particular, vertical and horizontal edges of $\mathcal{H}$, which are infinite, do not belong to $\mathcal{N}(H)$ and slopes of $\mathcal{N}(H)$ edges are all negative. If $\mathcal{I}(H)$ denotes the nonnegative integer $v_Y(H(0, Y))$, we can alternatively describe the Newton polygon as follow:

- If $H(X, 0) \neq 0$, $\mathcal{N}(H)$ is formed by the sequence of edges of $\mathcal{H}$ joining $(0, v_X(H(X, 0)))$ to $(\mathcal{I}(H), 0)$.
- If $H(X, 0) = 0$, $(0, v_X(H(X, 0)))$ is replaced by the leftmost point of $\mathcal{H}$ with smallest j-coordinate.

The Newton polygon may consist of a single point. For instance $H(X, Y) = Y$ yields the trivial polygon $(1, 0)$.

We now introduce a slightly different object, that we call *generic Newton polygon* for reasons explained in Remark 27. This variant allows a homogeneous treatment of finite series, clearer specifications for algorithms and simplifies wording and proofs of results regarding modular reduction.

Definition 13. The *generic Newton polygon* $\mathcal{GN}(H)$ is obtained by restricting $\mathcal{N}(H)$ to edges with slope no less than -1 and by joining the leftmost remaining point to the vertical axis with an edge of slope -1.

In other words, we add a fictitious point $(0, j_0)$ to $\mathrm{Supp}(H)$ so as to mask edges with slope less than -1.

Example 14. Consider $H_1(X,Y) = Y^7 + XY^5 + XY^4 + (X^4 + X^2)Y^3 + X^2Y^2 + X^6$. In Figure 1, the support of H_1 is represented by crosses, $\mathcal{GN}(H_1)$ is drawn with plain lines while the masked edge of $\mathcal{N}(H_1)$ is represented by a dotted line.

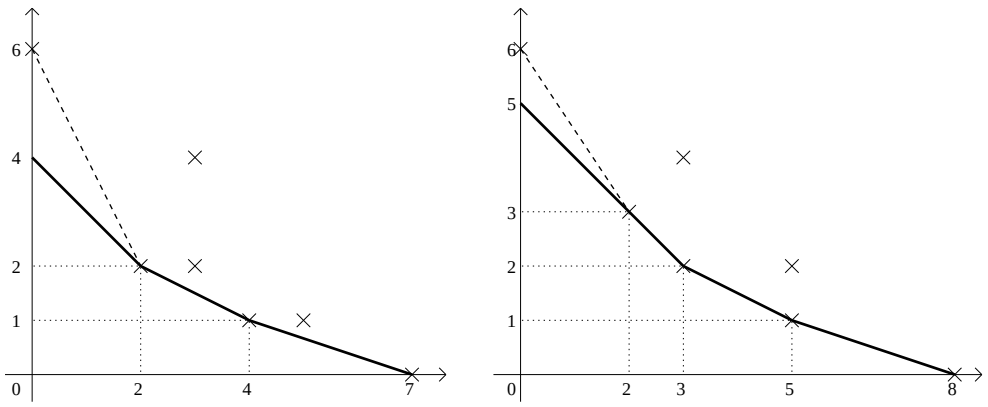
Example 15. Consider $H_2(X,Y) = Y^8 + (X^2 + X)Y^5 + (X^4 + X^2)Y^3 + X^3Y^2 + X^6$ and Figure 1 again. The edge with slope -1 is prolongated until the vertical axis.

Example 16. Assume that $H_3(X,Y) = Y$. Then $\mathcal{GN}(H_3)$ consists of a unique edge joining $(0,1)$ to $(1,0)$.

Remark 17. Mark Van Hoeij pointed out to us that his implementation of the Newton-Puiseux algorithm, available since Maple V.5 (`algcurves[puiseux]`), implicitely uses the concept of generic polygons. His motivation was to improve efficiency: At each recursive step, it is possible to compute modulo a well-chosen power of X so as to precisely obtain the generic polygon of the next step. This program was developed to compute integral bases (van Hoeij, 1994), but this implementation technique has not been published.

Generic Newton polygons enable us to compute Puiseux series that vanish at $X = 0$. To compute all Puiseux series of F above 0, the first stage of the algorithm requires a special treatment: Edges with positive slopes must be taken into account and edges with negative slopes must now be "hidden" by an horizontal edge.

Definition 18. The exceptional Newton polygon $\mathcal{EN}(H)$ is the lower part of the convex hull of $\mathrm{Supp}(H) \cup \{(0,0)\}$.



$\mathcal{GN}(H_1)$ versus $\mathcal{N}(H_1)$ $\mathcal{GN}(H_2)$ versus $\mathcal{N}(H_2)$

Fig. 1. Generic versus classical polygons

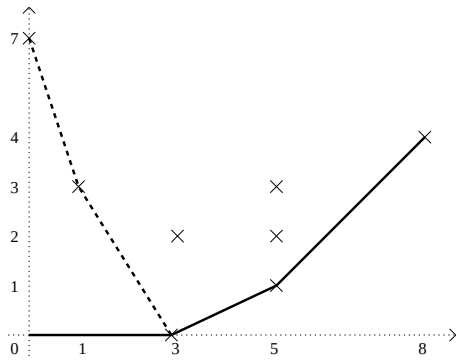


Fig. 2. $\mathcal{EN}(H_4)$ versus $\mathcal{N}(H_4)$

In other words, it consists of the edge $[(0,0),(\mathcal{I}(H),0)]$, followed by a sequence of edges with positive slopes that join $(\mathcal{I}(H),0)$ to $(d_Y(H), v_X(\mathrm{lc}_Y(H))$. In particular, $\mathcal{EN}(H) = [(0,0),(d_Y(H),0)]$ if H is monic.

Example 19. Let $H_4(X,Y) = X^4Y^8 + (X^3+X^2+X)Y^5 + (1+X^2)Y^3 + X^3Y + X^7$. In picture 2, $\mathcal{EN}(H_4)$ is drawn with plain lines while the masked edges of $\mathcal{N}(H_4)$ are represented by dotted lines.

To an edge Δ of $\mathcal{GN}(H)$ (resp. $\mathcal{N}(H)$, $\mathcal{EN}(H)$) corresponds three integers q, m and l with $q > 0$, q and m coprime, such that Δ is on the line $q\,j + m\,i = l$. If Δ is the horizontal edge of $\mathcal{EN}(H)$, $m = l = 0$ and we choose $q = 1$.

Definition 20. We define the *characteristic polynomial* ϕ_Δ:

$$\phi_\Delta(T) = \sum_{(i,j)\in\Delta} a_{ij} T^{\frac{i-i_0}{q}}$$

where i_0 is the smallest value of i such that (i,j) belongs to Δ.

Note that if $\mathcal{N}(H)$ is used, $\phi_\Delta(T)$ cannot vanish at $T = 0$, while $\mathcal{GN}(H)$ and $\mathcal{EN}(H)$ allow such cancellation if Δ is a fictitious edge (or contain a fictitious part). In this case, the multiplicity of 0 as a root of $\phi_\Delta(T)$ is the length of the fictitious edge (or portion of edge) added.

The next two lemmas recall the relation between Newton polygons of H and Newton polygons of its factors in $L[[X]][Y]$:

Lemma 21. *If H is an irreducible polynomial of $L[[X]][Y]$ and $H(0,0) = 0$, then $\mathcal{GN}(H)$ has a unique edge Δ. Moreover, if L is algebraically closed, ϕ_Δ has a unique root.*

Proof. This is well-known for classical Newton polygons (Brieskorn and Knörrer, 1986). The extension to generic polygons is straightforward. □

Lemma 22. *Let H_1 and H_2 be elements of $L[[X]][Y]$. Then, $\mathcal{GN}(H_1H_2)$ results from joining together the different edges of $\mathcal{GN}(H_1)$ and $\mathcal{GN}(H_2)$, suitably translated. Moreover, the characteristic polynomial of an edge Δ with slope $-m/q$ of $\mathcal{GN}(H_1H_2)$ is the*

product of the characteristic polynomials associated with edges of $\mathcal{GN}(H_1)$ and $\mathcal{GN}(H_2)$ with slope $-m/q$. In particular, if $H_1(0,0) \neq 0$, so that $\mathcal{GN}(H_1)$ is reduced to the point $(0,0)$, then $\mathcal{GN}(H_1H_2) = \mathcal{GN}(H_2)$.

Proof. For classical Newton polygons, see Brieskorn and Knörrer (1986). For generic Newton polygons, proceed as follow: If necessary, add a monomial cX^{n_1} (resp. cX^{n_2}) to H_1 (resp. H_2), where c is an indeterminate, so that $\mathcal{GN}(H_i) = \mathcal{N}(H_i)$. Then, apply the result for the classical case and set $c = 0$ to recover $\mathcal{GN}(H_1H_2)$. □

4.2. Rational Newton-Puiseux Algorithm

Duval's algorithm below performs successive changes of variables, determined by triplets (q, m, l) and roots of ϕ_Δ; see Section 4.1. It returns a set of triplets

$$\{(G_i(X,Y), P_i(X), Q_i(X,Y))\}_{1\leq i\leq r}$$

such that:
- $G_i \in \overline{L}[X,Y]$,
- $P_i(X)$ is a monomial of the form $\lambda_i X^{e_i}$,
- $Q_i(X,Y) = Q_{0i}(X) + Y\,X^{r_i}$, where r_i is the regularity index of the expansion and $(P_i(T), Q_{0i}(T))$ is the singular part of a parametrization of F,
- There exist integers L_i such that $G_i(X,Y) = F(P_i(X), Q_i(X,Y))/X^{L_i}$, $G_i(0,0) = 0$ and $G_{iY}(0,0) \neq 0$.

By the formal Implicit Function Theorem, the latter conditions ensure that there exists a unique power series S such that $G_i(X, S(X)) = 0$ and $S(0) = 0$. The corresponding parametrization o F is therefore $R_i(T) = (P_i(T), Q_i(T, S(T)))$. The power series S can be computed using "fast" techniques (Kung and Traub, 1978). It may also happen that Y divides G_i, in which case the expansion is finite. Therefore, we will consider that such a triplet represents a rational Puiseux expansion.

We need two auxiliary algorithms, for which we only provide specifications:

`Algorithm Factor(`L`,`ϕ`)`

`Input:`

L : *A field.*
ϕ : *A univariate polynomial in $L[T]$.*

`Output:` *A set of pairs $\{(\phi_i, k_i)\}_i$ so that ϕ_i is irreducible in $L[T]$ and $\phi = \prod_i \phi_i^{k_i}$.*

`Algorithm Bézout(`q`,`m`)`

`Input:`

q, m : *Two positive integers.*

`Output:` *A pair of integers (u, v) such that $u\,q - m\,v = 1$, with $(u, v) = (1, 0)$ when $q = 1$.*

The first (non recursive) call to the main function below must be treated differently since $\mathcal{EN}(H)$ must be used instead of $\mathcal{GN}(H)$, in order to treat expansions not defined at $X = 0$ and for reasons explained in Section 5.2. We assume that a mechanism is available to distinguish the initial call from recursive calls; adding a Boolean argument would work.

```
Algorithm RNPuiseux(L,H)
Input:
```
L : *A field of characteristic $p \geq 0$.*
H : *A squarefree polynomial in $L[X,Y]$ with $d_Y(H) \geq 2$ and $H(0,Y) \neq 0$. H satisfies the characteristic condition (3).*

`Output:` *A set of triplets $\{[G_i, P_i, Q_i]\}_i$, which form a set of representatives for:*
- L-rational Puiseux expansions of H above 0 for the initial call,
- L-rational Puiseux expansions of H centered at $(0,0)$ for recursive calls.

```
Begin
  If in a recursive call then
    N ← GN(H)
    If I(H) = 1 then Return {[H, X, Y]} End
  else
    N ← EN(H)
  End
  R ← {}
  For each side Δ of N do
    Compute q, m, l and φ_Δ
    (u, v) ← Bézout(q, m)
    For each (f, k) in Factor(L, φ_Δ) do
      ξ ← Any root of f
      H_0(X, Y) ← H(ξ^v X^q, X^m(ξ^u + Y))/X^l
      For each [G, P, Q] in RNPuiseux(L(ξ), H) do
        R ← R ∪ {[G, ξ^v P^q, P^m(ξ^u + Q)]}
      End
    End
  End
  Return R
End.
```

Since generic polygons are used, when $q = 1$, ξ may be null; in this case, the specific choice of $(u, v) = (1, 0)$ in `Bézout` ensures that the first variable of H is not cancelled and that no division by zero occurs.

Replacing L by $\overline{L}$ and (u, v) by $(1/q, 0)$ in `RNPuiseux`, one obtains an instance of the classical algorithm (Walker, 1950), where only one representative of each cycle is returned and conjugacy over the ground field is not taken into account; we call it `CNPuiseux`. In this case, factors f of ϕ_Δ have degree 1 and `CNPuiseux` runs through *all* roots of ϕ_Δ.

Duval (1989) suggested that the D5 system (Della Dora et al., 1985) should be used to avoid factorization. In our case, though, since efficient algorithms are known for factoring polynomials over finite fields, and small primes p can be used (see Section 5), factorization does not dominate the complexity of our symbolic-numeric method (Poteaux and Rybowicz, 2009; Poteaux, 2008).

Example 23. Set $F(X,Y) = (Y^3 - X^5)(X^2Y^3 - 1) \in \mathbb{Q}[X,Y]$. Applying `RNPuiseux` yields two triplets:

$$(P_1, Q_1) = (X^3, X^{-2}(1+Y)) = (X^3, X^{-2} + X^{-2}Y)$$
$$(P_2, Q_2) = (X^3, X^0(0 + X^3(0 + X^2(1+Y)))) = (X^3, X^5 + X^5Y)$$

The first null coefficient of $Q_2(X,Y)$ comes from the horizontal edge of the exceptional polygon $[(0,0),(0,3),(2,6)]$. The second one correspond to the fictious edge of $\mathcal{GN}(F)$ introduced at the first recursive call. This may seem inefficient, but these tricks have no impact on the complexity and clarifies arguments in Section 5. In practice, one may still use classical Newton polygons if necessary.

Example 24. Consider $F(X,Y) = (Y - 1 - 2X - X^2)(Y - 1 - 2X - X^7) \in \mathbb{Q}[X,Y]$. We obtain two triplets with:

$$(P_1, Q_1) = (X, X^0(1 + X(2 + X(1 + Y))) = (X, 1 + 2X + X^2 + X^2Y)$$
$$(P_2, Q_2) = (X, X^0(1 + X(2 + X(0 + Y))) = (X, 1 + 2X + X^2Y)$$

Note that the generic Newton polygon allows to obtain immediately the regularity index of the series $X + X^7$ in F, which is 2. The classical polygon does not provide directly this information; this causes difficulties to describe precisely the ouput of Duval's algorithm.

Example 25. Let F be the product of the minimal polynomials over $\mathbb{Q}(X)$ of the series $X^{5/6} + X$ and $X^{5/6} + X^{11/12}$. We obtain two triplets with:

$$(P_1, Q_1) = (X^6, X^0(0 + X^5(1 + X(1 + Y)))) = (X^6, X^5 + X^6 + X^6Y)$$
$$(P_2, Q_2) = (X^{12}, X^0(0 + X^{10}(1 + X(1 + Y)))) = (X^{12}, X^{10} + X^{11} + X^{11}Y)$$

The regularity indices in F are indeed 6 and 11.

Example 26. Let $F(X,Y) = (Y^2 - 2X^3)(Y^2 - 2X^2)(Y^3 - 2X) \in \mathbb{Q}[X,Y]$. Applying `RNPuiseux` over $\mathbb{Q}$ yields three expansions:

$$(P_1, Q_1) = (2X^2, X^0(0 + 2X^2(0 + X(2 + Y)))) = (2X^2, 4X^3 + 2X^3Y)$$
$$(P_2, Q_2) = (4X^3, X^0(0 + X(2 + Y))) = (4X^3, 2X + 2XY)$$
$$(P_3, Q_3) = (X, X^0(0 + X(\sqrt{2} + Y))) = (X, \sqrt{2}X + XY)$$

The first two expansions have residue field $\mathbb{Q}$ and ramification index 2 and 3. The third one corresponds to a place with residue field isomorphic to $\mathbb{Q}(\sqrt{2})$. Applying `RNPuiseux` over $\mathbb{Q}(\sqrt{2})$ will result in one more expansion:

$$(P_4, Q_4) = (X, X^0(0 + X(-\sqrt{2} + Y))) = (X, -\sqrt{2}X + XY).$$

Finally, applying `CNPuiseux` gives:

$$(P_1, Q_1) = (X^2, \sqrt{2}X^3 + \frac{\sqrt{2}}{2}X^3Y)$$
$$(P_2, Q_2) = (X^3, \sqrt[3]{2}X + \sqrt[3]{2}XY)$$
$$(P_3, Q_3) = (X, \sqrt{2}X + XY)$$
$$(P_4, Q_4) = (X, -\sqrt{2}X + XY)$$

In the first two expansions, unecessary algebraic extensions are introduced. The last two expansions show that conjugacy over $\mathbb{Q}$ is not taken into account.

Remark 27. For any irreducible $F(X,Y) \in \overline{L}[[X]][Y]$, at each step of `RNPuiseux`, the polygon $\mathcal{N}$ has exactly one edge and the characteristic polynomial has a unique root. Moreover, the sequence of generic Newton polygons encountered depends only on the characteristic terms of the Puiseux series (see Section 3.2), and not on the other terms. In this sense, these polygons are truly "generic", since all polynomials with the same characteristic yield the same sequence of generic polygons.

For floating point computation, `CNPuiseux` should be used since conjugagy over L is meaningless. Although it is not the topic of this paper, we briefly explain our symbolic-numeric strategy since it was our original motivation.

The data q, m, l come directly from the polygons. They need to be computed exactly, since for instance q will contribute to the ramification index, which has to be obtained exactly. It is obvious that if ξ is replaced by a numerical approximation, the change of variable in `CNPuiseux` will almost always produce a polynomial H_0 with trivial Newton polygon, namely reduced to the unique point $(0,0)$. It will not be easy to recover the correct polygon, since we will have to decide which coefficients are approximations of 0 and should be ignored. Moreover:

Proposition 28. *Let H be a polynomial satisfying the input hypotheses of* `RNPuiseux`.
- *The integer $\mathcal{I}(H)$ is the number of Puiseux series of H above 0 vanishing at $X = 0$.*
- *The integer $\mathcal{I}(H_0)$ (see the algorithm) is equal to the multiplicity of ξ in ϕ_Δ.*

Proof. Duval (1989). □

The second assertion of Proposition 28 tells us that ϕ_Δ is not squarefree in general. In the presence of approximations, determining the distinct roots of ϕ_Δ and their multiplicity may be difficult. However, if we assume that all Newton polygons (and thus root multiplicities) are obtained by some other means, such as computation modulo a prime number, then we can:

(1) Extract the approximate coefficients of H which are meaningful to compute $\mathcal{GN}(H)$. The coefficients below $\mathcal{GN}(H)$ should be equal to 0; just discard them.
(2) Deduce an approximate ϕ_Δ.
(3) Find clusters of approximate roots of ϕ_Δ with the expected multiplicities.
(4) For each cluster, deduce an approximate value of ξ, apply the numerical change of variable to obtain an approximation of H_0 and proceed with the recursive call.

Again, the reader is refered to Poteaux (2007, 2008) for more details.

4.3. Polygon trees

To a function call `RNPuiseux`(L, F) (see Section 4), we associate a labeled rooted tree. By definition, the *depth* of a vertex v is the number of edges on the path from the root to v. In particular, the root vertex has depth 0. The tree vertices of even depth are labeled with polygons, while vertices of odd depth are labeled with integer partitions. Similarly, tree edges are labeled alternatively with edges of polygons and integer pairs (k, f) where

k is the multiplicity of a root ξ and $f = [L(\xi) : L]$. A tree edge corresponds either to the choice of a polygon edge or to the choice of a root. More precisely, the tree is constructed recursively from the root vertex as follow (even depth vertices correspond to function calls; see Figure 3):

- A vertex v of even depth l is labeled with the polygon $\mathcal{N}$, that is $\mathcal{EN}(H)$ for the root vertex ($l = 0$), and $\mathcal{GN}(H)$ for recursive calls ($l > 0$).
- To each Δ of $\mathcal{N}$ corresponds an edge from v to a depth $l + 1$ vertex. Label the edge with Δ (represented by its endpoint).
- A child (depth $l + 1$ vertex) is labeled with the corresponding integer partition $[\phi_\Delta]$ (see the end of Section 1 for this notation).
- To each choice of root ξ of ϕ_Δ made by the algorithm corresponds an edge from a depth $l + 1$ vertex to a depth $l + 2$ vertex. The edge is labeled with the pair (k, f), where k is the multiplicity of ξ of and $f = [L(\xi) : L]$.
- Then, we proceed recursively: A depth $l + 2$ vertex is the root vertex of the tree corresponding to the function call `RNPuiseux`$(L(\xi), H_0)$ where H_0 is the polynomial obtained for a choice of edge Δ and a choice of root ξ.

The leaves are even depth vertices labeled with polygons that have only one side $\mathcal{P}_h = [(0, 1), (1, 0)]$. Note that the roots ξ are not part of the tree. Since the square-free factorization is a sub-product of the factorization over L, the labeled tree can be obtained at no significant cost. If l is the depth of the function call tree generated by `RNPuiseux`(L,F), then the labeled tree constructed has depth $2l$.

For a function call `CNPuiseux`(F), we define a similar tree, but in this case, an edge from a partition to a polygon is only labeled with a multiplicity k because the ground field is $\overline{L}$ and all field extensions have degree 1.

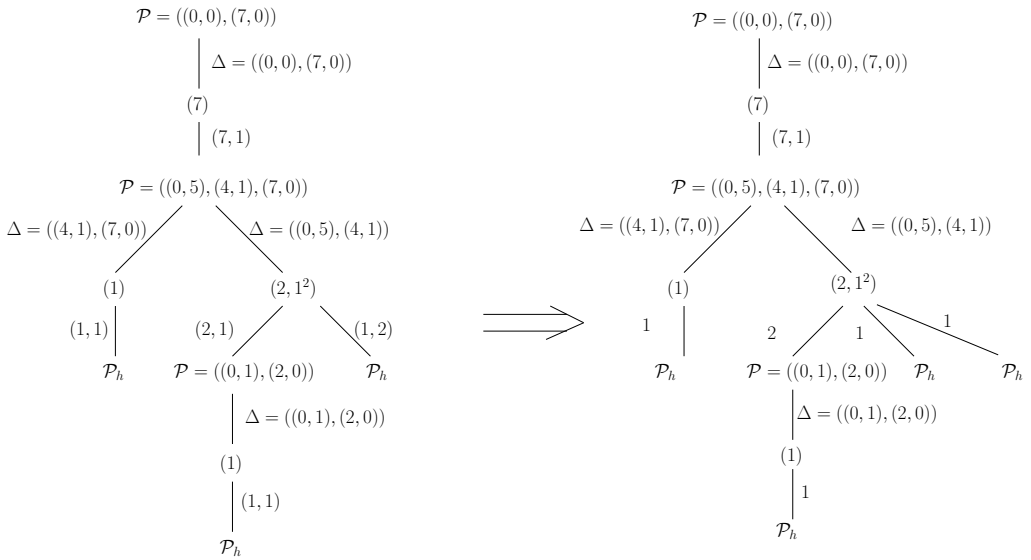


Fig. 3. Polygon trees $\mathcal{RT}(\mathbb{Q}, F)$ and $\mathcal{T}(F)$ for Example 26.

Definition 29. We denote by $\mathcal{RT}(L,F)$ (resp. $\mathcal{T}(F)$) a tree associated to the function call `RNPuiseux`(L,F) (resp. `CNPuiseux`(F)). In both cases, the tree is called *the polygon tree* associated to the function call.

It turns out that $\mathcal{T}(F)$ is precisely the symbolic information required for our symbolic-numeric method (Poteaux, 2007, 2008) and applications mentioned in Section 1.

Proposition 30. *The tree $\mathcal{T}(F)$ can easily be obtained from $\mathcal{RT}(L,F)$ as follow: duplicate f times each edge labeled (k,f) (together with the sub-tree rooted at this edge) and replace tag (k,f) by tag k.*

Proof. Trivials, since $\mathcal{T}(F) = \mathcal{RT}(\overline{L},F)$; see Section 4.4. □

This process is illustrated in Figure 3.

4.4. From classical Puiseux series to rational Puiseux expansions

Following Duval (1989), we remark that Newton polygons and root multiplicities obtained along the computation with `RNPuiseux` or `CNPuiseux` are the same. This remark easily extends if generic Newton polygons are used. However, in general, nonzero roots of characteristic polynomials obtained with the two algorithms differ.

Studying relations between coefficients of rational Puiseux expansions and classical coefficients has a number of benefits: it provides a better understanding of the rational algorithm, insight about the coefficient growth and a reduction criterion for rational Puiseux expansions (see Theorem 43).

Let $(\xi_1,m_1,q_1)\dots(\xi_h,m_h,q_h)$ be the sequence of triplets encountered along the computation of a single rational Puiseux expansion using `RNPuiseux`, where ξ_i is a root of the i-the characteristic polynomial and $-m_i/q_i$ is the slope of an edge of the corresponding generic Newton Polygon. We denote by (u_i,v_i), $1\leq i\leq h$ the pairs of integers returned by the `Bézout` algorithm.

On the other hand, let $(\alpha_1,m_1,q_1)\dots(\alpha_h,m_h,q_h)$ be the sequence of triplets encountered along the computation of a classical Puiseux series using `CNPuiseux`. Here, α_i is a q_i-th root of the i-th characteristic polynomial. The output of `CNPuiseux` is:

$$\begin{aligned} P(X) &= X^{q_1q_2\cdots q_h} = X^e \\ Q(X,Y) &= X^{m_1q_2\cdots q_h}(\alpha_1 + X^{m_2q_3\cdots q_h}(\alpha_2 + \cdots + X^{m_h}(\alpha_h + Y)\cdots)) \end{aligned}$$

so that an element of the corresponding cycle can be written:

$$S(X) = X^{\frac{m_1}{q_1}}(\alpha_1 + X^{\frac{m_2}{q_1q_2}}(\alpha_2 + \cdots + X^{\frac{m_h}{q_1q_2\cdots q_h}}(\alpha_h + \cdots)\cdots)) \tag{8}$$

Since we have used generic and exceptional Newton polygons, some of the ξ_i and α_i may be null. If $\xi_i = \alpha_i = 0$, we have $q_i = 1$ because ξ_i is associated with an edge of slope -1 or 0 and therefore, $v_i = 0$ (see procedure `Bézout`). In the sequel, we define $0^0 = 1$ so that $\xi_i^{v_i} = \alpha_i^{v_i} = 1$ and all expressions involved make sense and are correct.

Proposition 31. *There exists a classical Puiseux series as above and a set of integers* $\{e_{ij}\}_{1\le j<i\le h}$ *such that:*

$$\xi_i = \alpha_i^{q_i} \prod_{j=1}^{i-1} \alpha_j^{v_j e_{ij}}.$$

Proof. We set $X_0 = X$, $Y_0 = Y$, and consider transformations performed by `RNPuiseux`:

$$\begin{aligned} X_{i-1} &= \xi_i^{v_i} X_i^{q_i} \\ Y_{i-1} &= X_i^{m_i}(\xi_i^{u_i} + Y_i) \end{aligned}$$

We define (any choice of e-th root is acceptable):

$$\mu_i = \prod_{j=1}^{i} \xi_j^{-\frac{v_j}{q_j q_{j+1}\cdots q_i}} \qquad 1 \le i \le h,$$

so that we can write:

$$X_i = \mu_i X^{\frac{1}{q_1 q_2 \cdots q_i}}.$$

The truncated series computed by algorithm `RNPuiseux` can be expressed as follow:

$$Q(X,0) = X_1^{m_1}(\xi_1^{u_1} + X_2^{m_2}(\xi_2 + X_3^{m_3}(\xi_3^{u_3} + \dots X_{h-1}^{m_{h-1}}(\xi_{h-1}^{u_{h-1}} + X_h^{m_h}\xi_h^{u_h})\cdots))).$$

Using the above expression for X_i and identifying coefficients with those of expression (8) shows that there exists a classical Puiseux series verifying:

$$\alpha_i \alpha_{i-1}^{-1} = \xi_{i-1}^{-u_{i-1}} \xi_i^{u_i} \mu_i^{m_i} \qquad 1 \le i \le h$$

where we have chosen $\alpha_0 = \xi_0 = 1$. It is convenient to introduce $\theta_i = \alpha_i \alpha_{i-1}^{-1} \xi_{i-1}^{u_{i-1}}$. Hence, we have:

$$\begin{aligned} \mu_i^{q_i} &= \mu_{i-1} \xi_i^{-v_i} \\ \theta_i &= \xi_i^{u_i} \mu_i^{m_i} \end{aligned}$$

Raising the second equality to the power q_i and applying relation $u_i q_i - m_i v_i = 1$, we obtain:

$$\xi_i = \theta_i^{q_i} \mu_{i-1}^{-m_i}.$$

Raising the first equality to the power u_i and the second one to the power v_i, Bézout relation gives:

$$\mu_i = \theta_i^{-v_i} \mu_{i-1}^{u_i}.$$

The recurrence given by the last equality easily yields:

$$\begin{aligned} \mu_i &= \theta_i^{-v_i} \theta_{i-1}^{-v_{i-1}u_i} \theta_{i-2}^{-v_{i-2}u_{i-1}u_i} \cdots \theta_1^{-v_1 u_2 u_3 \cdots u_i} \\ \xi_i &= \theta_i^{q_i} \left(\theta_{i-1}^{v_{i-1}} \theta_{i-2}^{v_{i-2}u_{i-1}} \cdots \theta_1^{v_1 u_2 u_3 \cdots u_{i-1}}\right)^{m_i} \end{aligned} \tag{9}$$

Finally, the proposition is proved by induction on i, together with the following assertion: There exists a set of integers $\{f_{ij}\}_{1\le j<i\le h}$ such that:

$$\theta_i = \alpha_i \prod_{j=1}^{i-1} \alpha_j^{v_j f_{ij}} \tag{10}$$

The case $i = 1$ is trivial. Assume that $i > 1$. The induction hypothesis about ξ_{i-1} gives:

$$\theta_i = \alpha_i \alpha_{i-1}^{-1} \xi_{i-1}^{u_{i-1}} = \alpha_i \alpha_{i-1}^{-1} \alpha_{i-1}^{q_{i-1} u_{i-1}} \prod_{j=1}^{i-2} \alpha_j^{v_j e_{i-1,j} u_{i-1}}$$

Setting $f_{ij} = e_{i-1,j} u_{i-1}$ for $1 \leq j \leq i-2$ and $f_{i,i-1} = m_{i-1}$ we obtain (10). The expression for ξ_i in the proposition then follows directly from the formula for ξ_i in (9). □

Remark 32. Assuming that the v_i are chosen in $\mathbb{N}$, it is easily seen that the e_{ij} and f_{ij} are also in $\mathbb{N}$.

Remark 33. Using relation (9) and the definition of θ_i, it is easy to express recursively the ξ_i in terms of the α_i, but there is no simple formula. On the other hand, the α_i can be easily expressed as follow: For $1 \leq i \leq j \leq h$, define $s_{ji} = \sum_{k=j}^{i} \frac{m_k}{q_j \cdots q_k}$. Then:

$$\alpha_i = \xi_i^{u_i} \prod_{j=1}^{i} \xi_j^{-v_j s_{ji}}.$$

To conclude this part, we rewrite coefficients returned by `RNPuiseux` in terms of the ξ_i. In order to simplify expressions, we introduce the following notation for $0 \leq i \leq h-1$:

$$\xi_{(i)} = \xi_{i+1}^{v_{i+1}} \xi_{i+2}^{v_{i+2} q_{i+1}} \xi_{i+3}^{v_{i+3} q_{i+1} q_{i+2}} \cdots \xi_h^{v_h q_{i+1} \cdots q_{h-1}}.$$

We also define $\xi_{(h)} = 1$.

We deduce the parametrization:

$$\begin{aligned} X(T) &= \xi_{(0)} T^e \\ Y(T) &= \xi_1^{u_1} \xi_{(1)}^{m_1} T^{m_1 q_2 \cdots q_h} + \\ &\quad \xi_2^{u_2} \xi_{(1)}^{m_1} \xi_{(2)}^{m_2} T^{m_1 q_2 \cdots q_h + m_2 q_3 \cdots q_h} + \\ &\quad \cdots \\ &\quad \xi_h^{u_h} \xi_{(1)}^{m_1} \xi_{(2)}^{m_2} \cdots \xi_{(h)}^{m_h} T^{m_1 q_2 \cdots q_h + m_2 q_3 \cdots q_h + \cdots + m_h} + \cdots \end{aligned} \tag{11}$$

5. Good reduction

We consider a polynomial $F(X,Y) = \sum_{k=0}^{d_Y} A_k(X) Y^k$ with coefficients in an algebraic number field K and discuss how to choose a prime number p so that the computation of rational Puiseux expansions modulo a prime ideal $\mathfrak{p}$ dividing p provides enough information to guide floating point computations of Puiseux series, namely $\mathcal{T}(F)$.

We denote by $\mathfrak{o}$ the ring of algebraic integers of K. If $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$, then $v_\mathfrak{p}$ is the corresponding valuation of K. Finally, we define:

$$\mathfrak{o}_\mathfrak{p} = \{\alpha \in K \mid v_\mathfrak{p}(\alpha) \geq 0\}.$$

Let L be the finite extension generated over K by the Puiseux series coefficients of F. Note that by Proposition 31, L also contains the coefficients of rational Puiseux

expansions computed by `RNPuiseux`. If $\mathfrak{O}$ stands for the ring of algebraic integers of L and $\mathfrak{P}$ a prime ideal of $\mathfrak{O}$, we introduce:

$$\mathfrak{O}_{\mathfrak{P}} = \{\alpha \in L \,|\, v_{\mathfrak{P}}(\alpha) \geq 0\}.$$

In the sequel, $\mathfrak{P}$ will always denote a prime ideal of $\mathfrak{O}$ dividing $\mathfrak{p}$.

The reduction modulo $\mathfrak{P}$ of $\alpha \in \mathfrak{O}_{\mathfrak{P}}$ is represented by $\overline{\alpha}$. We extend this notation to polynomials and fractional power series with coefficients in $\mathfrak{O}_{\mathfrak{P}}$. If $\alpha \in \mathfrak{o}_{\mathfrak{p}}$, since $\mathfrak{P}$ divides $\mathfrak{p}$, reduction modulo $\mathfrak{P}$ and $\mathfrak{p}$ coincide and we will also use notation $\overline{\alpha}$.

5.1. Modular reduction of Puiseux series

Our reduction strategy is based on the following definition:

Definition 34. Let p be a prime number and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}$ dividing p. If the three conditions below are verified:
- $F \in \mathfrak{o}_{\mathfrak{p}}[X, Y]$,
- $p > d_Y$,
- $v_{\mathfrak{p}}(\mathrm{tc}(R_F)) = 0$,

then we say that F has *local (at X=0) good* $\mathfrak{p}$*-reduction*. Moreover, we say that F has *local good* $\mathfrak{p}$*-reduction at* $X = x_0$ if $F(X + x_0, Y)$ does at $X = 0$.

Note that if F has good $\mathfrak{p}$-reduction at $\mathfrak{p}$, since $\mathfrak{P}$ divides $\mathfrak{p}$, then $v_{\mathfrak{P}}(\mathrm{tc}(R_F)) = 0$ and F also has good $\mathfrak{P}$-reduction. We shall use this fact freely in the sequel.

We also remark that if F has a good $\mathfrak{p}$-reduction, then $\overline{F}$ is squarefree and $d_Y(\overline{F}) = d_Y$; indeed, since Δ_F and $= A_{d_Y}\mathrm{lc}_Y(F)$ have coefficients in $\mathfrak{o}_{\mathfrak{p}}$, relation $R_F = \pm A_{d_Y}\Delta_F$ implies that $v_{\mathfrak{p}}(\mathrm{tc}(A_{d_Y})) = 0$ and $v_{\mathfrak{p}}(\mathrm{tc}(\Delta_F)) = 0$. We shall also use these facts later.

We now derive a fundamental result for our reduction strategy (Theorem 38) from a theorem by Dwork and Robba. Let $\mathbb{C}_p$ be the field of p-adic numbers and let $|\cdot|_p$ denote its absolute value; see Robert (2000) for an introduction to p-adic analysis. We consider L as a subfield of $\mathbb{C}_p$ by means of its $\mathfrak{P}$-adic completion, so that we can write:

$$\mathfrak{O}_{\mathfrak{P}} = \{\alpha \in L \,|\, |\alpha|_p \leq 1\}.$$

Finally, for all $\rho \in \mathbb{R}^{+*}$, we define $D(0, \rho^-) = \{x \in \mathbb{C}_p \mid |x|_p < \rho\}$ and $\mathring{D}(0, \rho^-) = \{x \in \mathbb{C}_p \mid 0 < |x|_p < \rho\}$

Theorem 35. *If $F \in \mathfrak{o}_{\mathfrak{p}}[X, Y]$, $p > d_Y$ and R_F has no root in $\mathring{D}(0, 1^-)$, then Puiseux series of F above 0 converge p-adically in $D(0, 1^-)$.*

Proof. Dwork and Robba (1979, Theorem 2.1). □

Proposition 36. *Let $S(X) = \sum_{i=n}^{\infty} \beta_i X^{i/e} \in \mathbb{C}_p[[X]]$ be a p-adically convergent and bounded Puiseux series in $D(0, 1^-)$. Then:*

$$\sup_{x \in D(0,1^-)} |S(x)|_p = \sup_{i \geq 0} |\beta_i|_p$$

Proof. See for instance Robert (2000, Section 4.6). □

Lemma 37. *Let $P(X) = X^m(c_0 + \cdots + c_r X^r) \in \mathfrak{o}_\mathfrak{p}[X]$ be a polynomial such that $|c_0|_p = 1$. Then P has no root in $\mathring{D}(0, 1^-)$.*

Proof. Assume that $x \in \mathbb{C}_p^*$ satisfies $|x|_p < 1$ and $P(x) = 0$. Since $P \in \mathfrak{o}_\mathfrak{p}[X]$, $|c_i x^i|_p < 1$ for $1 \leq i \leq r$. But $|a + b|_p = \max\{|a|_p, |b|_p\}$ if $|a|_p \neq |b|_p$; hence $|c_0 + \cdots + c_r x^r| = 1$. This is impossible because $c_0 + \cdots + c_r x^r = 0$. □

We deduce the fundamental following result:

Theorem 38. *If F has local good $\mathfrak{p}$-reduction, then coefficients of Puiseux series of F above 0 are in $\mathfrak{O}_\mathfrak{P}$.*

Proof. Let $S(X) = \sum_{i=n}^{\infty} \alpha_i X^{i/e}$ be any of the Puiseux series S_{ij}. Since coefficients of R_F are in $\mathfrak{O}_\mathfrak{P}$ and $|\mathrm{tc}(R_F)|_p = 1$, Lemma 37 asserts that R_F has no root in $\mathring{D}(0, 1^-)$; hence, Theorem 35 ensures that S converges in $D(0, 1^-)$.

We define $v = v_X(A_{d_Y})$. Then, the polynomial $F_0(X, Y) = X^{(d_Y-1)v} F(X, Y/X^v) \in \mathfrak{o}_\mathfrak{p}[X, Y]$ has a leading coefficient $A(X) = A_{d_Y}(X)/X^v$ such that $|A(0)|_p = 1$, and therefore $|A(x)|_p = 1$ for $|x|_p < 1$ (see proof of Lemma 37). Moreover, $S_0(X) = X^v S(X)$ is a Puiseux series of F_0 that also converges in $D(0, 1^-)$. We now show that S_0 is bounded by 1 on $D(0, 1^-)$: Indeed, if for some $x \in D(0, 1^-)$, we have $|S_0(x)|_p > 1$, then $S_0(x)$ cannot satisfy the equation $F_0(x, S_0(x)) = A(x)S_0(x)^{d_Y} + A_{d_Y-1}(x)S(x)^{d_Y-1} + \cdots + x^{(d_Y-1)v} A_0(x) = 0$ because $|A(x)|_p = 1$, so that the first term of the sum cannot be cancelled by the others. By Proposition 36, coefficients of S_0 (and S) are in $\mathfrak{O}_\mathfrak{P}$. □

It is worth insisting on the fact that this result holds for *any* $\mathfrak{P}$ dividing $\mathfrak{p}$.

Example 39. Consider the case $F(X, Y) = Y^2 - X^3(p + X)$ with $p > 2$. Puiseux series above 0 are:

$$S_{1j}(X) = (-1)^j \sqrt{p} X^{3/2} (1 + \frac{X}{p})^{1/2} = (-1)^j \sqrt{p} X^{3/2} (1 + \frac{X}{2\,p} - \frac{X^2}{8\,p^2} + \cdots).$$

They are obviously not reducible modulo p, but the criterion detects this deficiency. It is interesting to note, however, that a system of rational Puiseux expansions is given by $\{X = pT^2, Y = p^2T^3 + \frac{1}{2}p^2T^5 + \dots\}$. This parametrization is reducible modulo p, but the reduction $\{X = 0, Y = 0\}$ is trivial and hardly useful. On the other hand, $\{X = T^2/p, Y = T^3/p + \frac{1}{2}T^5/p^3 + \dots\}$ is also a (non reducible) system of rational Puiseux expansions.

Example 40. Let $F(X, Y) = X\,(p + X)\,Y^2 + Y + X$. Puiseux series above 0 are:

$$S_1(X) = -X - pX^3 - X^4 + \dots \qquad S_2(X) = -\frac{1}{p\,X} + \frac{1}{p^2} + \frac{p^3 - 1}{p^3} X + \dots$$

The discriminant of F with respect to Y is $\Delta_F = -4\,X^3 - 4p\,X^2 + 1$. Its trailing coefficient does not vanish modulo p, but the trailing coefficient of $\mathrm{lc}_Y(F)$ does. The resultant condition detects correctly the problem in S_2; compare to Poteaux and Rybowicz (2008), which dealt only with the monic case.

Corollary 41. *If F has local good $\mathfrak{p}$-reduction, then $\mathfrak{P}$-adic valuations of characteristic coefficients of all ramified Puiseux series of F above 0 are equal to zero. In other words, reduction modulo $\mathfrak{P}$ preserves the characteristic of ramified cycles of F above 0.*

Proof. First of all, we show that if F has good $\mathfrak{p}$-reduction, then any monic factor G of F in $\overline{K}((X))[Y]$ satisfies $v_{\mathfrak{P}}(\mathrm{tc}(\Delta_G)) = 0$. Let $F = GH$. Relation (2) shows that $\mathrm{tc}(\Delta_F) = \mathrm{tc}(\Delta_G)\mathrm{tc}(\Delta_H)\mathrm{tc}(\mathrm{Resultant}(G,H))^2$. From Theorem 38, coefficients of G and H are in $\mathfrak{O}_{\mathfrak{P}}$, and so are these three numbers; therefore, their $\mathfrak{P}$-adic valuation must be zero. Apply this result to all monic irreducible factors of F in $\overline{K}((X))[Y]$: Proposition 6 yields the corollary, because all integers $(R_{i-1} - R_i)$, R_i and Q_i involved are positive. □

It is important to note, however, that annihilation modulo $\mathfrak{P}$ of Puiseux series coefficients is not totally controlled by this criterion. If F is irreducible in $\overline{K}[[X]][Y]$, all non-characteristic coefficients may vanish modulo $\mathfrak{P}$, as shown by Proposition 6: consider for instance the minimal polynomial over $\mathbb{Q}(X)$ of $S(X) = pX + X^{3/2}$, which satisfies the criterion. However, we shall see in Section 5.2 that if F is not irreducible, our criterion also detects cancellation of coefficients that "separate" cycles; see Theorem 48.

Theorem 42. *Let $\{S_i\}_{1\leq i\leq s}$ be a set of representatives for the cycles of F above 0. Assume that F has local good $\mathfrak{p}$-reduction. Then, $\{\overline{S_i}\}_{1\leq i\leq s}$ form a set of representatives for the cycles of $\overline{F}$ above 0.*

Proof. Since $R_{\overline{F}} = \overline{R_F} \neq 0$, formula (1) shows that the $\overline{S_i}$ are pairwise distinct roots of $\overline{F}$. By Corollary 41, the ramification index of $\overline{S_i}$ is equal to the ramification index of S_i, namely e_i. Since $\sum_{i=1}^{s} e_i = d_Y$, they form a complete set of representatives. □

We now show that parametrizations computed by `RNPuiseux` yield meaningful results when reduced modulo $\mathfrak{P}$ (see Example 39). It is obviously not the case for all rational Puiseux expansions, even if F satisfies the criterion.

Theorem 43. *Denote by $R(T) = (\gamma T^e, \sum_{i=0}^{r} \beta_i T^{a_i})$ (with $\beta_i \neq 0$) a parametrization given by* `RNPuiseux`*(K, F). If F has local good $\mathfrak{p}$-reduction, then β_i belongs to $\mathfrak{O}_{\mathfrak{P}}$ and $v_{\mathfrak{P}}(\gamma) = 0$. Moreover, if a_i is a characteristic exponent, then $v_{\mathfrak{P}}(\beta_i) = 0$.*

Proof. We use the notations of Section 4.4. If α_j is a characteristic coefficient, then Corollary 41 shows that $v_{\mathfrak{P}}(\alpha_j) = 0$. If α_j is not a characteristic coefficient, it is the root of a characteristic polynomial of a Newton polygon edge with integer slope. Hence, $q_j = 1$, $v_j = 0$ and $u_j = 1$ (see procedure `Bézout`). From Proposition 31 we deduce that $v_{\mathfrak{P}}(\xi_i) = q_i v_{\mathfrak{P}}(\alpha_i)$ for all $1 \leq i \leq h$. The same argument proves that $v_{\mathfrak{P}}(\xi_{(i)}) = 0$ for $0 \leq i \leq h$. In particular, $\gamma = \xi_{(0)}$ and $v_{\mathfrak{P}}(\gamma) = 0$. Finally, (11) shows that $v_{\mathfrak{P}}(\beta_i) = u_i q_i v_{\mathfrak{P}}(\alpha_i)$. If α_i is a characteristic coefficient, the latter valuation is zero, otherwise it is equal to $q_i v_{\mathfrak{P}}(\alpha_i) \geq 0$ since $u_i = 1$ in this case. □

Finally, we can apply the local criterion to each relavant place of $K[X]$. This leads to the following global criterion:

Definition 44. Let p be a prime number and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}$ dividing p. If the conditions below are verified:
- $F \in \mathfrak{o}_\mathfrak{p}[X, Y]$,
- $p > d_Y$,
- $[R_F] = [R_{\overline{F}}]$, i.e. the multiplicity structure of R_F is preserved (see Section 2),

then we say that F has *global good* $\mathfrak{p}$*-reduction.*

Remark 45. This criterion has already been used by the second author as a genus preservation condition (good reduction, in a classical sense) in his implementation of Trager's algorithm for the integration of algebraic functions (Trager, 1984), publicly available since Maple V.5. This condition was derived from proofs in Eichler (1966, Section III.6), using elementary considerations. This test was also brought to the attention of the Computer Algebra community by Trager (unpublished document), as a consequence of a more sophisticated theorem by Fulton (Fulton, 1969).

Proposition 46. *If F has global good $\mathfrak{p}$-reduction, then for each critical point $x_0 \in \overline{K}$ of F, and for each prime ideal $\mathfrak{P}$ of $K(x_0)$ dividing $\mathfrak{p}$, $F(X + x_0, Y)$ has local good $\mathfrak{P}$-reduction.*

Proof. Let x_0 be a critical point of F. Since the resultant multiplicity structure is preserved by $\mathfrak{p}$-reduction, we have $d_X(R_F) = d_X(R_{\overline{F}})$. Thus, $v_\mathfrak{p}(\mathrm{lc}_X(R_F)) = 0$ and x_0 is integral over $\mathfrak{o}_\mathfrak{p}$; therefore, the coefficients of $F(X + x_0, Y)$ can be reduced modulo $\mathfrak{P}$.

Let $R_F = c \prod_i R_i^{k_i}$ be the monic squarefree factorization of R_F (i.e. the R_i are monic). Since $v_\mathfrak{p}(c) = 0$, we have $R_i \in \mathfrak{o}_\mathfrak{p}[x]$, by Gauss Lemma. If we define $S = \prod_i R_i$, then the equality $[R_F] = [R_{\overline{F}}]$ is equivalent to $v_\mathfrak{p}(\Delta_S) = 0$. Thus, $v_\mathfrak{P}(\Delta_S) = 0$, and so $v_\mathfrak{P}(\Delta_{S(X+x_0)}) = 0$, since the discriminant is unchanged by a shift. The last equality implies $[R_{F(X+x_0,Y)}] = [R_{\overline{F(X+x_0,Y)}}]$, and in particular $v_\mathfrak{P}(\mathrm{tc}(R_{F(X+x_0,Y)})) = 0$. □

Moreover, the global criterion ensures local good reduction at $X = \infty$:

Proposition 47. *If F has a global good $\mathfrak{p}$-reduction, then $X^{d_X} F(1/X, Y)$ has a local good $\mathfrak{p}$-reduction.*

Proof. Note that $\mathrm{tc}(R_{X^{d_X} F(1/X,Y)}) = \mathrm{lc}_X(R_F)$; but $v_\mathfrak{p}(\mathrm{lc}_X(R_F)) = 0$. □

5.2. Modular reduction of polygon trees

If $F \in \mathfrak{o}_\mathfrak{p}[X, Y]$ and $p > d_Y$, algorithms of Section 4 can be applied to the reduction $\overline{F}$ of F modulo $\mathfrak{p}$, so that the notations $\mathcal{T}(\overline{F})$ and $\mathcal{RT}(\mathbb{F}_{p^t}, \overline{F})$ make sense. The computed expansions have coefficients in a finite extension of $\mathbb{F}_p$.

The following result is crucial. It allows to compute by means of modular computations the symbolic information required:

Theorem 48. *If F has local good $\mathfrak{p}$-reduction, then $\mathcal{T}(F) = \mathcal{T}(\overline{F})$.*

Note that the correspondence between $\mathcal{T}(F)$ and $\mathcal{T}(\overline{F})$ cannot be stated so simply if classical Newton polygons are used instead of generic ones: non-characteristic coefficients of Puiseux series may vanish under modular reduction, yielding polygon modifications.

To prove Theorem 48, we proceed as follow: We first show that a number of convenient properties are preserved by each recursive call to `RNPuiseux` (Lemma 49), then we prove that, when these properties are satisfied, Newton polygons and multiplicity structures are preserved by modular reduction (Lemmas 50 and 51) and we complete the proof.

Lemma 49. *Assume that H satisfies:*
(i) $H \in \mathfrak{O}_\mathfrak{P}[X,Y]$,
(ii) *H has no multiple roots,* $d_Y(H) > p$, $H(0,0) = 0$, $H(0,Y) \neq 0$,
(iii) *the roots of H are in* $\cup_{e>0}\mathfrak{O}_\mathfrak{P}((X^{1/e}))$,
(iv) $v_\mathfrak{P}(\mathrm{tc}(R_H)) = 0$.
Let (m,q,l) be integers associated to an edge Δ of $\mathcal{GN}(H)$ and let ξ be a root of ϕ_Δ. Then, $H_0(X,Y) = H(X^q, X^m(\xi+Y))/X^l$ also satisfies the conditions (i) to (iv).

Proof. Conditions $H_0(0,0) = 0$ and $H_0(0,Y) \neq 0$ follow from properties of `CNPuiseux`. If $\{Y_i(X)\}_{1\leq i\leq d_Y(H)}$ denotes the roots of H, the roots of H_0 are $\{Y_i(X)/X^m - \xi\}_{1\leq i\leq d_Y(H)}$; they are obviously distinct. Since ξ is in $\mathfrak{O}_\mathfrak{P}$, so are the coefficients of H_0 and the coefficients of its roots. Finally, if $A(X) = \mathrm{lc}_Y(H)$, the term $A(X)Y^{d_Y(H)}$ becomes $A(X^q)X^{md-l}(Y+\xi)^{d_Y(H)}$. The coefficient of Y^{d_Y} is $A(X^q)X^{md-l}$, which has the same trailing coefficient as $A(X)$. Therefore, since the resultant is, up to a power of the leading coefficient, a product of root differences, its trailing coefficient does not change under the transformation. □

Lemma 50. *Assume that H satisfies conditions (i) to (iv) of Lemma 49. Then:*
(a) $\mathcal{GN}(H) = \mathcal{GN}(\overline{H})$.
(b) *Let Δ be a edge of $\mathcal{GN}(H)$. The characteristic polynomial ϕ_Δ (resp. $\overline{\phi_\Delta}$) of Δ in H (resp. $\overline{H}$) satisfy $[\phi_\Delta] = [\overline{\phi_\Delta}]$ (equality of multiplicity structures; see Section 2).*

Proof. Denote $\{S_i\}_{1\leq i\leq w}$ the cycles of H that vanish at $X=0$, $\{e_i\}_{1\leq i\leq w}$ their ramification indices and $\{H_i\}_{1\leq i\leq w}$ their minimal polynomials over $\overline{K}((X))$. The irreducibility of H_i yields $e_i = \deg_Y H_i$. Our assumptions about roots of H induce that H_i belongs to $\mathfrak{O}_\mathfrak{P}[[X]][Y]$. Hypothesis *(iv)* implies that S_i can be reduced modulo $\mathfrak{P}$. By Corollary 41, S_i and $\overline{S_i}$ have the same characteristic, and therefore the same algebraic degree; in particular, $\overline{H_i}$ must be the minimal polynomial of $\overline{S_i}$ and is thus irreducible in $\overline{\mathbb{F}_p}[[X]][Y]$.

We define $V = \prod_{i=1}^w H_i$, so that V is a monic polynomial with coefficients in $\mathfrak{O}_\mathfrak{P}$. Write $H = UV$ with U in $\mathfrak{O}_\mathfrak{P}[[X]][Y]$. By Proposition 28, $\mathcal{I}(H) = \mathcal{I}(V)$, thus $U(0,0) \neq 0$; Lemma 22 shows that $\mathcal{GN}(H) = \mathcal{GN}(V)$.

We now show that $\mathcal{GN}(\overline{H}) = \mathcal{GN}(\overline{V})$, which is equivalent to $v_\mathfrak{P}(U(0,0)) = 0$ by Lemma 22 again. From relation (2), we get:

$$\mathrm{tc}(\Delta_H) = \pm\mathrm{tc}(\Delta_V)\,\mathrm{tc}(\Delta_U)\,\mathrm{tc}(\mathrm{Resultant}(U,V))^2.$$

But V is monic, hence the latter resultant is $\pm\prod_i U(X,v_i)$, where v_i runs through the roots of V; since $v_i(0) = 0$, its trailing coefficient is a power of $U(0,0)$. We deduce that $\mathrm{tc}(\Delta_H)$ is the product of a power of $U(0,0)$ with an element of $\mathfrak{O}_\mathfrak{P}$. Hypothesis (iv) yields $v_\mathfrak{P}(\mathrm{tc}(\Delta_H)) = 0$ and $v_\mathfrak{P}(U(0,0)) = 0$. Therefore, $\mathcal{GN}(\overline{H}) = \mathcal{GN}(\overline{V})$.

To prove *(a)*, it remains to show that $\mathcal{GN}(V) = \mathcal{GN}(\overline{V})$. By Lemma 22, this is equivalent to $\mathcal{GN}(H_i) = \mathcal{GN}(\overline{H_i})$. If $\mathcal{I}(H_i) = 1$, then $\mathcal{I}(\overline{H_i}) = 1$ because H_i is monic. Therefore, both $\mathcal{GN}(H_i)$ and $\mathcal{GN}(\overline{H_i})$ are reduced to the unique edge $[(0,1),(1,0)]$. Assume $\mathcal{I}(H_i) > 1$. Since $\overline{H_i}$ is irreducible in $\overline{\mathbb{F}_p}[[X]][Y]$, $\mathcal{GN}(\overline{H_i})$ has a single edge Δ, with a characteristic polynomial of the form $(T-\xi)^m$ for some positive integer m and element ξ of $\overline{K}$; see Lemma 21. If the unique edge of $\mathcal{GN}(H_i)$ has slope -1, so does the unique edge of $\mathcal{GN}(\overline{H_i})$ since the vanishing modulo $\mathfrak{P}$ of $\mathrm{tc}(H_i(X,0))$ leads to the same (fictitious) edge. If the unique edge has a slope greater than -1, $\mathrm{tc}(H_i(X,0))$ is a nonnegative power of ξ. But ξ is a nonnegative power of a characteristic coefficient, which cannot vanish modulo $\mathfrak{P}$ by Corollary 41. In both cases, $\mathcal{GN}(H_i) = \mathcal{GN}(\overline{H_i})$.

To address *(b)*, let Δ be a common edge of $\mathcal{GN}(H)$ and $\mathcal{GN}(\overline{H})$. If Δ corresponds to irreducible polynomials H_i and $\overline{H_i}$, ϕ_Δ and $\overline{\phi_\Delta}$ have a unique root with the same multiplicity, since they have the same degree, and we are done. Assume that Δ corresponds to at least two irreducible polynomials H_1 and H_2 associated to the roots ξ_1 and ξ_2 of ϕ_Δ. In order to demonstrate *(b)*, we just need to show that if $\xi_1 \neq \xi_2$, then $\overline{\xi_1} \neq \overline{\xi_2}$. If m and q are relatively prime integers such that $-m/q$ is the slope of Δ, we set $\alpha_i = \xi_i^{1/q}$ (any choice of q-th root is suitable). The cycle associated to H_i can be represented by the series $\alpha_i X^{m/q} + \cdots$. By (1), there exists $\delta \in \mathfrak{O}_\mathfrak{P}$ such that $\mathrm{tc}(\Delta_H) = (\alpha_1 - \alpha_2)\delta$. From hypothesis *(iv)*, $v_\mathfrak{P}(\alpha_1 - \alpha_2) = 0$, so that $\overline{\alpha_1} \neq \overline{\alpha_2}$, which in turn gives $\overline{\xi_1} \neq \overline{\xi_2}$. □

Lemma 51. *Assume that F has local good $\mathfrak{p}$-reduction. Then:*

(a) $\mathcal{EN}(F) = \mathcal{EN}(\overline{F})$.

(b) Let Δ be an edge of $\mathcal{EN}(F)$. The characteristic polynomial ϕ_Δ (resp. $\overline{\phi_\Delta}$) of Δ in F (resp. $\overline{F}$) satisfies $[\phi_\Delta] = [\overline{\phi_\Delta}]$.

Proof. We denote $\Delta_0, \ldots, \Delta_{s-1}$ the sequence of edges of the exceptional Newton polygon $\mathcal{EN}(F)$, sorted by decreasing slope. By definition of $\mathcal{EN}(F)$, if $\Delta_k = [(i_k, j_k), (i_{k+1}, j_{k+1})]$, then we have $(i_0, j_0) = (0,0)$ and $(i_s, j_s) = (d_Y, v)$, where $v = v_X(A_{d_Y})$ is the X-adic valuation of the leading coefficient of F.

If $F(X,Y) = \sum_{i,j} a_{ij} X^j Y^i$, since $(0,0)$ belongs to $\mathcal{EN}(F)$ and $\mathcal{EN}(\overline{F})$ by construction, assertion *(a)* is equivalent to:

$$v_\mathfrak{p}(a_{i_k j_k}) = 0 \text{ for all } 1 \leq k \leq s \tag{12}$$

A trivial consequence of the reduction criterion is $v_\mathfrak{p}(\mathrm{tc}(A_{d_Y})) = v_\mathfrak{p}(a_{i_s j_s}) = 0$. We now consider an integer k satisfying $1 \leq k \leq s-1$, if such an integer exists, and suppose that $v_\mathfrak{p}(a_{i_{k+1} j_{k+1}}) = 0$. If $-\frac{m_k}{q_k}$ denotes the slope of the edge Δ_k, and ξ_k a root of the characteristic polynomial ϕ_{Δ_k}, then there is a Puiseux series S_{k,ξ_k} of F which has $\xi_k^{1/q_k} x^{m_k/q_k}$ as first term. Moreover, since $k \geq 1$, we have $\frac{m_k}{q_k} < \frac{m_0}{k_0}$. Therefore, if S_0 is a Puiseux series associated to the edge Δ_0, then $\mathrm{tc}(S_{k,\xi_k} - S_0) = \xi_k^{1/q_k}$. But we can deduce from $v_\mathfrak{p}(R_F) = 0$ and relation (1) that $v_\mathfrak{P}(\mathrm{tc}(S_{k,\xi_k} - S_0)) = 0$ and so $v_\mathfrak{P}(\xi_k) = 0$ for all $\mathfrak{P}$ dividing $\mathfrak{p}$. Finally, as $a_{i_k j_k}$ is, up to the sign, the product of $a_{i_{k+1} j_{k+1}}$ and the roots of ϕ_{Δ_k}, we conclude that $v_\mathfrak{p}(a_{i_k j_k}) = 0$, which proves (12) by induction.

Concerning (b), we proceed as in the proof of (b), Lemma 50. □

Remark 52. The assertion (i) of Lemma 51 does not hold if the exceptional polygon is replaced by the generic polygon, as shown by the example $F(X,Y) = (Y + p + X)(Y + 1 + X)$. The good reduction criterion does not detect the cancellation of $F(0,0)$, but does detect a change of root multiplicities. This remark justifies the introduction of $(0,0)$ in the support of F to define $\mathcal{EN}(F)$.

Proof. (of Theorem 48) By Lemma 51, the root vertex, depth one vertices and edges down to depth 2 vertices of $\mathcal{T}(\overline{F})$ are correctly labelled.

Let Δ be an edge of $\mathcal{EN}(F)$, $mi + qj = l$ be the line containing Δ, ξ be a root of ϕ_Δ and $H(X,Y) = F(X^q, X^m(Y+\xi))/X^l$. Assumptions of Lemma 49 are obviously satisfied for H because $\xi \in \mathfrak{O}_\mathfrak{P}$ and $\mathrm{tc}(R_H) = \mathrm{tc}(R_F)$. Denote by $\mathcal{T}_0(H)$ the sub-tree of $\mathcal{T}(F)$ corresponding to the recursive function call `CNPuiseux`(H).

We show that, for all H satisfying hypotheses of Lemma 49, $\mathcal{T}_0(H) = \mathcal{T}_0(\overline{H})$. We proceed by induction on the number c of function calls to `CNPuiseux` necessary to compute $\mathcal{T}_0(H)$.

If $c = 1$, then $\mathcal{I}(H) = 1$ and $\mathcal{T}_0(H)$ is reduced to a single vertex labelled with $\mathcal{GN}(H)$, which consists of the unique edge $[(0,1),(1,0)]$. Lemma 50 gives $\mathcal{T}_0(H) = \mathcal{T}_0(\overline{H})$.

Suppose now that $c > 1$. Lemma 50 shows that the root vertex, the depth 1 vertices and all edges from the root to depth 2 vertices of $\mathcal{T}_0(H)$ and $\mathcal{T}_0(\overline{H})$ coincide and are labelled identically. Let H_0 denote a polynomial obtained from H in `CNPuiseux`. The number of function calls necessary to compute $\mathcal{T}_0(H_0)$ is less than c. Lemma 49 ensures that the induction hypotheses can be applied to H_0. Hence, $\mathcal{T}_0(H_0) = \mathcal{T}_0(\overline{H_0})$. By construction of polygon trees, $\mathcal{T}_0(H) = \mathcal{T}_0(\overline{H})$ □

6. Size of a good prime

This part is devoted to the choice of a prime ideal $\mathfrak{p}$ such that F has good reduction at $\mathfrak{p}$. Assume that $K = \mathbb{Q}(\gamma)$ and let M_γ be the minimal polynomial of γ over $\mathbb{Q}$. Elements of K are represented as polynomials in γ of degree less than $w = [K : \mathbb{Q}]$ with coefficients in $\mathbb{Q}$. Up to a change of variable in M_γ and the coefficients of F, we suppose that γ belongs to $\mathfrak{o}$, namely $M_\gamma \in \mathbb{Z}[T]$.

Definition 53. Let P be a multivariate polynomial of $K[\underline{X}]$. There exists a unique pair (H,c) with $H \in \mathbb{Z}[T,\underline{X}]$, $c \in \mathbb{N}$, $\deg_T(H) < w$ and $P(\underline{X}) = H(\gamma,\underline{X})/c$, where c is minimal. The polynomial H is called the *numerator of* P and is denoted $\mathrm{num}(P)$. The integer c is called the *denominator* of H and is written $\mathrm{denom}(P)$. We define the *size of* P as follows: $\mathrm{ht}(P) = \max\{\log c, \log \|H\|_\infty\}$.

Defining $F_n = \mathrm{num}(F)$ and $b = \mathrm{denom}(F)$, we have: $F(X,Y) = F_n(\gamma,X,Y)/b$.

6.1. Local reduction

We are left with the problem of finding a prime number p and a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ dividing p such that:

(C_1) $p > d_Y$;

(C_2) p does not divide b;

(C_3) we can determine an explicit representation of $\mathfrak{p}$ such that a morphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p} \simeq \mathbb{F}_{p^t}$ can effectively be computed;

(C_4) $\mathrm{tc}(R_F) \not\equiv 0$ modulo $\mathfrak{p}$.

Conditions (C_1) and (C_2) are easily verified. We deal with condition (C_3) in a standard fashion: Let $\overline{M}$ be any irreducible factor of $\overline{M_\gamma}$ in $\mathbb{F}_p[T]$ and M be a lifting of $\overline{M}$ in $\mathbb{Z}[T]$. It is well-known that if p is a prime number not dividing the index $e_\gamma = [\mathfrak{o} : \mathbb{Z}[\gamma]]$, then the ideal $\mathfrak{p} = (p, M(\gamma))$ of $\mathfrak{o}$ is prime (Cohen, 1993). Hence, elements of $\mathfrak{o}$ can be reduced by means of the morphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p} \simeq \mathbb{F}_p[T]/(\overline{M}) \simeq \mathbb{F}_{p^t}$ where $t = \deg \overline{M}$. Computing e_γ is a non-trivial task, and so is the computation of generators of prime ideals dividing p when p divides e_γ. If e_γ is unknown, it is sufficient to choose p so that it does not divide the discriminant Δ_{M_γ}, since e_γ divides Δ_{M_γ}. In practice, $\overline{M}$ is chosen amongst the factors of $\overline{M_\gamma}$ of smallest degree. Moreover, it is worth trying a few primes p in order to decrease t, the case $t = 1$ being the most favorable.

In order to simplify the analysis, we replace condition (C_4) by the stronger condition:

(C_4') $\mathrm{Norm}_{K/\mathbb{Q}}(\mathrm{tc}(R_F)) \not\equiv 0$ modulo p.

If (C_1) to (C_4') are verified, then for all prime ideals $\mathfrak{p}$ dividing p, F has good $\mathfrak{p}$-reduction. In practice, though, we do not recommend to use (C_4'). Finally, we introduce the notation:

$$N_F = b|\mathrm{Norm}_{K/\mathbb{Q}}(\mathrm{tc}(R_F))\Delta_{M_\gamma}|.$$

Conditions (C_1) to (C_4') are induced by:

(C_5) $p > d_Y$ and $N_F \not\equiv 0$ modulo p.

6.1.1. Deterministic strategy

We determine a bound B such that, for all prime numbers $p > B$, condition (C_5) is satisfied. We first prove two lemmas:

Lemma 54. *The resultant $R_{F_n} \in \mathbb{Z}[T, X]$ of F_n and F_{nY} satisfies:*

$$\|R_{F_n}\|_\infty \leq (2d_Y - 1)!\, d_Y^{d_Y}\, [(w+1)(d_X+1)]^{2d_Y-2}\, \|F_n\|_\infty^{2d_Y-1}$$

Proof. Let $A_i(T, X)$ be the cofficient of Y^i in F_n. Expanding the determinant of the Sylvester matrix of F_n and F_{nY}, we see that there exists a sequence $(i_j)_{1\leq j\leq 2d_Y-1}$ of indices in $[0, d_Y]$ such that:

$$\begin{aligned}\|R_{F_n}\|_\infty &\leq (2d_Y-1)!\, \| \prod_{j=1}^{dy-1} A_{i_j}(T,X) \prod_{j=d_y}^{2d_y-1} i_j A_{i_j}(T,X)\|_\infty \\ &\leq (2d_Y-1)!\, {d_Y}^{d_Y} \| \prod_{j=1}^{2d_Y-1} A_{i_j}(T,X)\|_\infty.\end{aligned}$$

The bound follows recursively from $\|A_iC\|_\infty \leq (w+1)(d_X+1)\|A_i\|_\infty\|C\|_\infty$ for all $C(T, X) \in \mathbb{Z}[T, X]$ and the inequality $\|A_i\|_\infty \leq \|F_n\|_\infty$. □

Lemma 55. *Define:*

$$B_0 = \|R_{F_n}\|_\infty(\|M_\gamma\|_\infty + 1)^{(w-1)(2d_Y-2)} \tag{13}$$
$$B_1 = (w+1)^{(2w-1)/2}\|M_\gamma\|_\infty^{w-1}B_0^w \tag{14}$$
$$B_2 = w^w(w+1)^{(2w-1)/2}\|M_\gamma\|_\infty^{2w-1}. \tag{15}$$

If $c \in \mathbb{Z}[T]$ denotes the numerator of a coefficient of $R_{F_n(\gamma,X,Y)}$, then we have $\|c\|_\infty \leq B_0$, $|\operatorname{Norm}_{K/\mathbb{Q}}(c)| \leq B_1$ and $|\Delta_{M_\gamma}| \leq B_2$. In particular, $\|R_{F_n(\gamma,X,Y)}\|_\infty \leq B_0$.

Proof. Since the leading coefficient of F_n in Y does not vanish by evaluation at $T = \gamma$, evaluation and resultant commute: $R_{F_n(\gamma,X,Y)} = R_{F_n}(\gamma, X)$. Let $C_i(T) \in \mathbb{Z}[T]$ be the coefficient of X^i in $R_{F_n}(T, X)$ and $c_i(T) \in \mathbb{Z}[T]$ be the numerator of the coefficient of X^i in $R_{F_n}(\gamma, X)$. It is clear that $c_i(\gamma) = C_i(\gamma)$. Since M_γ is monic, Euclidean division yields $Q_i \in \mathbb{Z}[T]$ such that $C_i = Q_iM_\gamma + c_i$. Since $\deg_T C_i \leq (2d_Y - 1)(w - 1)$, one can show that:

$$\|c_i\|_\infty \leq \|C_i\|_\infty(\|M_\gamma\|_\infty + 1)^{(w-1)(2d_Y-2)}.$$

The latter inequality gives the bound for c. From $\operatorname{Norm}_{K/\mathbb{Q}}(c(\gamma)) = \operatorname{Resultant}_T(M_\gamma, c)$, Hadamard's inequality and trivial comparison of norms yield the second inequality. The third one is obtained similarly. □

Finally, we have the following result, for which we do not claim optimality:

Proposition 56. *Define $B = \max\{b, B_1, B_2\}$ (see (14) and (15)). Then, for all $p > B$, condition (C_5) is verified. Moreover, B is effectively computable and there exists a prime $p > B$ with size $\operatorname{ht}(p) \in O(wd_Y[w\operatorname{ht}(M_\gamma) + \operatorname{ht}(F) + \log(wd_Xd_Y)])$.*

Proof. For $d_Y > 1$, we have $B_1 > d_Y$ and $p > d_Y$. Lemma 55 applied to $c(\gamma) = \operatorname{tc}(R_{Fn(\gamma,X,Y)})$ shows that if p is a prime greater than B, (C_5) is verified. Taking logarithms and using Stirling's formula in the definition of B_1 and B_2, it is readily seen that B has the announced asymptotic size. Since there is always a prime between B and $2B$ (Bertrand's Theorem), the proposition follows. □

6.1.2. Probabilistic strategies

We now give two probabilistic algorithms to find a prime p such that (C_5) is satisfied: A Monte Carlo method and a Las Vegas one. Both use an intermediary function, that we first describe. To this end, we rely on two other procedures:

- The function call `RandomPrime(A,C)` returns a random prime number in the real interval $[A, C]$. We assume that the primes returned are uniformly distributed in the set of primes belonging to the interval $[A, C]$; see for instance Shoup (2005, Section 7.5).
- The function `Nextprime` gives the smallest prime larger than the argument.

`Algorithm Draw-p`(B, d, ϵ)
`Input:`

B : *A positive real number.*

d : *An integer greater than 1.*

ϵ : *A real number with* $0 < \epsilon \leq 1$.

`Output:` *A prime number p satisfying:*
- *$p > d$,*
- *for each $N \in \mathbb{N}$ with $d \leq N \leq B$, p divides N with probability less than ϵ.*

`Begin`
`If` $B < 3$ `then Return Nextprime(`d`) End`
$K \leftarrow 2 \ln B / (\epsilon \ln \ln B) + 2d / \ln d$
$C \leftarrow \max\{2d, K(\ln K)^2\}$
`Return RandomPrime`$(d+1, C)$
`End.`

Proposition 57. *Algorithm* `Draw-p` *is correct and* `Draw-p`(B, d, ϵ) *returns a prime p satisfying* $\mathrm{ht}(p) \in O(\log\log B + \log d + \log \epsilon^{-1})$.

Proof. Note that condition $p > d$ is automatically verified. Moreover, if $B < 3$, the algorithm returns a prime greater than B with size $O(\log d)$; indeed, since $d > 1$, there always exists a prime between d and $2d$. Thus, we now assume $B \geq 3$. If n is a positive integer, $\omega(n)$ is classically the number of primes dividing n. For a positive real number x, we use the notation $\pi(x)$ for the number of primes less or equal to x. Estimates of Bach and Shallit (1996, Section 8.8) give:

$$\frac{x}{\ln x} < \pi(x) \quad (x \geq 17), \qquad \pi(x) < \frac{2x}{\ln x} \quad (x > 1), \qquad \omega(n) < \frac{2\ln n}{\ln\ln n} \ (n \geq 3).$$

Let $h(x) = \frac{2\ln x}{\ln\ln x}$. We first show that for all integer N with $d \leq N \leq B$, we have $\omega(N) \leq h(B)$. The function $h(x)$ has a minimum on $[3, +\infty[$ equal to $2e$ and reached at $x = e^e < 16$. Thus, if $N < e^e$, $\omega(N) \leq 2 \leq 2e \leq h(B)$. For $x > e^e$, the function $h(x)$ is increasing, such that we also have $\omega(N) \leq h(B)$ if $N > e^e$.

Let C be a number greater than $2d$ and τ be the probability that a prime given by `RandomPrime(`$d+1$`,`C`)` divides N. We just have to determine a C large enough so that $\tau \leq \epsilon$. But there is always a prime number between d and $2d$ if $d > 1$, thus $\pi(C) - \pi(d) \geq 1$. Since `RandomPrime` has a uniform behavior, we search for a C such that, for all integer $d \leq N \leq B$, we have:

$$\tau = \frac{\omega(N)}{\pi(C) - \pi(d)} \leq \epsilon. \tag{16}$$

Since $B \geq 3$ and $d > 1$, estimates above show that it is sufficient to find C with:

$$\pi(C) \geq K = \frac{2\ln B}{\epsilon \ln\ln B} + \frac{2d}{\ln d}.$$

Setting $C = K(\ln K)^2$, we find $C/\ln C = K(\ln K)^2/(\ln K + 2\ln\ln K)$. For $B \geq 3$ and $d \geq 2$, K is greater than $4e$, and therefore $(\ln K)^2/(\ln K + 2\ln\ln K) \geq 1$ (increasing

function on $[4e, +\infty[$. Moreover $C \geq 17$, hence:

$$\pi(C) \geq \frac{C}{\ln C} \geq K,$$

and (16) holds. The algorithm returns a prime p with $\mathrm{ht}(p) = \max\{\log C, \log 2d\}$. Since $\log C = \log K + 2\log\log K \in O(\log\log B + \log d + \log \epsilon^{-1})$, the result follows. □

We begin with the Monte Carlo version:

`Algorithm MCGoodPrime(`F`,`M_γ`,`ϵ`)`
`Input:`

F : *A squarefree polynomial of* $K[X,Y]$ *with degree* $d_Y > 1$.

M_γ : *A monic irreducible polynomial in* $\mathbb{Z}[T]$.

ϵ : *A real number with* $0 < \epsilon \leq 1$.

`Output:` *A prime number* p *satisfying* (C_5) *with probability at least* $1 - \epsilon$.
`Begin`

$(d_X, d_Y, w) \leftarrow (\deg_X(F), \deg_Y(F), \deg_T(M_\gamma))$

$F_n \leftarrow \mathrm{num}(F)$

$R \leftarrow (2d_Y - 1)!\, {d_Y}^{d_Y}\, [(w+1)(d_X+1)]^{2d_Y-1}\, \|F_n\|_\infty^{2d_Y-1}$

$B_0 \leftarrow R\, (\|M_\gamma\|_\infty + 1)^{(w-1)(2d_Y-2)}$

$B_1 \leftarrow (w+1)^{(2w-1)/2} \|M_\gamma\|_\infty^{w-1} B_0^w$

$B_2 \leftarrow w^w (w+1)^{(2w-1)/2} \|M_\gamma\|_\infty^{2w-1}$

$B \leftarrow \max\{\mathrm{denom}(F), B_1, B_2\}$

`Return Draw-p(`$B, d_Y, \epsilon/3$`)`
`End.`

Proposition 58. `MCGoodPrime(`F`,`M_γ`,`ϵ`)` *returns a prime* p *satisfying:*

$$\mathrm{ht}(p) \in O(\log(d_Y w \log d_X) + \log \mathrm{ht}(F) + \log \mathrm{ht}(M_\gamma) + \log \epsilon^{-1}).$$

Moreover, the probability that p *does not satisfy* (C_5) *is less than* ϵ.

Proof. From proposition 57, p divides each integer $\mathrm{denom}(F)$ and Δ_{M_γ} with a probability less than $\epsilon/3$. The result is the same for the remaining factor of condition (C_5), because F is squarefree and the resultant is nonzero. Thus, p divides the product with a probability less than ϵ. For the size of p, apply Proposition 57 with the estimate of B given by Proposition 56. □

Finally, we consider a Las Vegas flavored method:

`Algorithm LVGoodPrime(`F`,`M_γ`)`
`Input:`

F : *A squarefree polynomial of* $K[X,Y]$ *with degree* $d_Y > 1$.

M_γ : *A monic irreducible polynomial in* $\mathbb{Z}[T]$.

`Output:` *A prime number* p *satisfying* (C_5).

```
Begin
   d_Y ← deg_Y(F)
   R ← num(tc(Resultant_Y(F, F_Y)))
   N_1 ← |Norm_{K/Q}(R(γ))|
   N_2 ← |Δ_{M_γ}|
   L ← {denom(F), N_1, N_2}
   B' ← max L
   Repeat
      p ← Draw-p(B', d_Y, 1/6)
   until p does not divide any element of L
   Return p
End.
```

Proposition 59. `LVGoodPrime`*(F, M_γ) returns a prime p satisfying:*

$$\mathrm{ht}(p) \in O(\log(d_Y w \log d_X) + \log \mathrm{ht}(F) + \log \mathrm{ht}(M_\gamma)).$$

and the average number of iterations is at most 2.

Proof. Similar to Proposition 58. Moreover, each candidate p satisfies (C_5) with probability at least $1/2$. □

The computation of $\mathrm{tc}(R_F)$ may have a significant cost. In our monodromy context, though, we need to determine R_F anyway. Moreover, in practice, we do not compute the norm of R_F's trailing coefficient, but perform reduction modulo $\mathfrak{p} = (p, \overline{M})$ instead.

6.2. Global good reduction

In this section, we extend our bounds to find a prime number p and a prime ideal $\mathfrak{p}$ dividing p such that F has a global good $\mathfrak{p}$-reduction. Thus, we want to find p and $\mathfrak{p}$ such that conditions (C_1), (C_2) and (C_3) (see the beginning of Section 6) are satisfied, and verifying:

(GC_4) The multiplicity structure of $R_F(X)$ is preserved by reduction modulo the prime ideal $\mathfrak{p}$ defined by condition (C_3).

Let $S(X)$ denote the *monic* squarefree part of $R_{F_n(\gamma,X,Y)}$, i.e. the monic squarefree polynomial of highest degree dividing $R_{F_n(\gamma,X,Y)}$. Set $S_n = \mathrm{num}(S) \in \mathbb{Z}[T, X]$ and $S_d = \mathrm{denom}(S)$, so that $\mathrm{lc}_X(S_n) = S_d$. We define $R_{S_n} = \mathrm{Resultant}_X(S_n, S_{nX}) \in \mathbb{Z}[T]$. Since $\mathrm{lc}_X(S_n)$ does not vanish at $T = \gamma$, $R_{S_n}(\gamma) = R_{S_n(\gamma,X)}$. In order to simplify the analysis, we define as in the previous part:

$$N_S = b|\mathrm{Norm}_{K/\mathbb{Q}}(\mathrm{lc}_X(R_{F_n(\gamma,X,Y)}))\mathrm{Norm}_{K/\mathbb{Q}}(R_{S_n(\gamma,X)})\Delta_{M_\gamma}|.$$

Lemma 60. *The following condition implies (C_1), (C_2), (C_3) and (GC_4) :*

(GC_5) *$p > d_y$ and $N_S \not\equiv 0$ modulo p.*

Proof. From a result of Weinberger and Rothschild (1976) (see also Encarnación (1995, Theorem 3.1)), S_d, and therefore $\mathrm{lc}_X(S_n)$, divides $\mathrm{Norm}_{K/\mathbb{Q}}(\mathrm{lc}_X(R_{F_n(\gamma,X,Y)}))\Delta_{M_\gamma}$ in $\mathbb{Z}$. If (GC_5) is verified, $\mathrm{lc}_X(S_n)$ does not vanish modulo $\mathfrak{p}$. We deduce that $\overline{R_{S_n}} = 0$ if and only if $R_{\overline{S_n}} = 0$. Thus, (GC_5) implies that $\overline{S_n}$ does not have multiple roots, and that its degree is the same as S_n's. In the same way, the degree and the number of distinct roots of $R_{F_n(\gamma,X,Y)}$ are preserved by reduction modulo $\mathfrak{p}$, so is its multiplicity structure, as well as R_F's. □

6.2.1. Deterministic strategy

We search for a bound B_G such that for all primes $p > B_G$, condition (GC_5) is verified. Lemma 55 gives $\mathrm{Norm}_{K/\mathbb{Q}}(\mathrm{lc}_X(R_{F_n(\gamma,X,Y)})) \leq B_1$ and $|\Delta_{M_\gamma}| \leq B_2$; thus, we just need to bound $|\mathrm{Norm}_{K/\mathbb{Q}}(R_{S_n(\gamma,X)})|$. We introduce $\delta = d_X(R_F)$, that we will use as a bound for the degree of S.

Lemma 61.

$$\|S_n\|_\infty \leq 2^{w+\delta}(\delta+1)^{\frac{1}{2}}(w+1)^{\frac{7w}{2}}\|R_{F_n(\gamma,X,Y)}\|_\infty^\delta \|M_\gamma\|_\infty^{4\delta}.$$

Proof. We have $\|S_n\|_\infty \leq |\mathrm{Norm}_{K/\mathbb{Q}}(\mathrm{lc}_X(R_{F_n(\gamma,X,Y)}))\Delta_{M_\gamma}|\|S\|_\infty$ from Weinberger and Rothschild (1976). The inequality then comes from Encarnación (1995, Lemma 4.1)). □

Lemma 62. *$R_{S_n} = Resultant_X(S_n, S_{nX}) \in \mathbb{Z}[T]$ verifies:*

$$\|R_{S_n}\|_\infty \leq (2\delta-1)!\,\delta^\delta(w+1)^{2\delta-2}\|S_n\|_\infty^{2\delta-1}.$$

Proof. Obvious from Lemma 54. □

Lemma 63. *Let*

$$B_3 = \|R_{S_n}\|_\infty(\|M_\gamma\|_\infty+1)^{(w-1)(2\delta-2)} \tag{17}$$

$$B_4 = (w+1)^{(2w-1)/2}\|M_\gamma\|_\infty^{w-1}B_3^w \tag{18}$$

Then $\|R_{S_n(\gamma,X)}\|_\infty \leq B_3$ and $|\mathrm{Norm}_{K/\mathbb{Q}}(R_{S_n(\gamma,X)})| \leq B_4$.

Proof. Similar to Lemma 55. □

Proposition 64. *Let $B_G = \max\{b, B_4\}$ (see (18)), then for all primes $p > B_G$, condition (GC_5) is satisfied. Moreover, B_G can be effectively computed, and there is a prime $p > B_G$ with size:*

$$\mathrm{ht}(p) \in O(w^2 d_X^2 d_Y^3\,[\mathrm{ht}(M_\gamma) + \mathrm{ht}(F) + \log(w d_X d_Y)]).$$

Proof. Since $d_Y > 1$, we have $B_1 > d_Y$. Then, $B_0 \leq B_3$ leads to $B_1 \leq B_4$. Therefore, we do not need to consider B_1. The inequality $B_2 \leq B_4$ is also easily verified. If p is a prime greater than B_G, then condition (GC_5) is true. Taking the logarithm of B_4, and using bounds of previous lemmas, we get:

$$\mathrm{ht}(p) \in O(w^2\delta \log(w\delta) + w\delta^2 d_Y\,[w\mathrm{ht}(M_\gamma) + \mathrm{ht}(F) + \log(wd_X d_Y)]).$$

Inequality $\delta \leq d_X(2d_Y - 1)$ and trivial estimates yield the result. To conclude, we note as usual that there is always a prime between B_G and $2B_G$. □

6.2.2. Probabilistic strategies

As for the local case, bound B_G of Proposition 64 leads to two probabilistic algorithms to find a prime p satisfying (GC_5), that we call `GMCGoodPrime` and `GLVGoodPrime`. The construction of these algorithms and related proofs are straigthforward; therefore, we shall only provide results. We just remark that there are now four factors to avoid instead of three. Hence, in `GMCGoodPrime`, the function `Draw-p` must be called with $\epsilon/4$ instead of $\epsilon/3$, while in `GLVGoodPrime`, `Draw-p` must be called with $1/8$ instead of $1/6$.

Proposition 65. `GMCGoodPrime`(F, M_γ, ϵ) *returns a prime p satisfying:*

$$\mathrm{ht}(p) \in O(\log(wd_X d_Y) + \log \mathrm{ht}(F) + \log \mathrm{ht}(M_\gamma) + \log \epsilon^{-1}).$$

Proposition 66. `GLVGoodPrime`*(F, M_γ) returns a prime p satisfying:*

$$\mathrm{ht}(p) \in O(\log(wd_X d_Y) + \log \mathrm{ht}(F) + \log \mathrm{ht}(M_\gamma)).$$

and the average number of iterations is less than 2.

6.3. Practical considerations

It is not our purpose to give a detailed complexity analysis herein, since it would require a more precise description of algorithm `RNPuiseux`; the reader is refered to Poteaux and Rybowicz (2009), and to Poteaux (2008) for F monic. We shall however briefly comment on the above bounds for p.

Deterministic bounds of Proposition 56 and 64 are mainly of theoretical interest. Indeed, they show that a good prime p of polynomial size can be deterministically chosen, while Walsh (1999) claims (without proof) that coefficients computed by `RNPuiseux` may have exponential size in characteristic 0. But from a practical point of view, these bounds are far too large. To illustrate this problem, we consider as in the introduction the polynomial $F(X,Y) = (Y^3 - X)\,((Y-1)^2 - X)\,(Y - 2 - X^2) + X^2\,Y^5$. For global good reduction, the number of digits given by Proposition 64 is 120084. For local good reduction above roots of the degree 23 irreducible factor of R_F, Proposition 56 (applied to the appropriate translation of F) yields a prime with 5304 digits. Although our estimates are probably not optimal, it is unlikely that they can be improved sufficiently so as to give acceptable figures.

On the other hand, probabilistic strategies give satisfactory results. For this example $(\epsilon = 10^{-8})$, `GMCGoodPrime` returns a prime with less than 17 digits, while `GLVGoodPrime` yields primes with at most 5 digits, the smallest prime with global good reduction being $p = 11$.

In many situations, computing the resultant R_F will be necessary anyway; for these cases, the Las Vegas approach is of course recommended. Finally, no matter which method

is chosen, it is usually worth trying a few good prime in order to reduce the coefficient field degree.

We illustrate the benefits of modular computation with a last example: Let a and h be positive integers and consider the following parametrization, introduced in a different context (Henry and Merle, 1987):

$$X(T) = T^{2^h}, Y(T) = \sum_{k=1}^{h} a\, T^{3\cdot 2^h(1-1/2^k)} \tag{19}$$

We define $d = 2^h$ and $F_d(X,Y) = \text{Resultant}_T(X - X(T), Y - Y(T))$, so that $d_Y(F_d) = d$ and $d_X(F_d) = 3(d-1)$. There is a unique place above 0 for F_d and therefore, a system of rational Puiseux expansions contains a unique parametrization.

Choosing $(u,v) = (2,1)$ in subroutine `Bézout` at each recursive call, and using results of Section 4.4, it can be shown that coefficients returned by `RNPuiseux` have size larger than $\frac{d^3}{2}\log_{10} a$. Since probabilistic strategies give primes with size logarithmic with respect to d, they allow to decrease significantly the coefficient size. For instance, `RNPuiseux` returns for F_{16}:

$$\begin{aligned} X(T) &= a^{3072}T^{16} \\ Y(T) &= a^{4609}T^{24} + a^{6913}T^{36} + a^{8065}T^{42} + a^{8641}T^{45} \end{aligned}$$

Setting $a = 2$, coefficients of the rational Puiseux expansion above 0 have up to 2602 digits, while Proposition 56 gives deterministic primes with 374 digits, `LVGoodPrime` (resp. `MCGoodPrime` with $\epsilon = 10^{-8}$) gives primes with less than 5 digits (resp. 14 digits).

The Maple 13 implementation of the rational Newton-Puiseux algorithm gives even worse results (`algcurves[puiseux]` command):

$$\begin{aligned} X(T) &= a^{24672}T^{16} \\ Y(T) &= a^{37009}T^{24} + a^{55513}T^{36} + a^{64765}T^{42} + a^{69391}T^{45} \end{aligned}$$

Setting $a = 2$ again, the coefficients have up to 20888 digits.

This example also illustrates a drawback of `RNPuiseux`: As remarked by Duval (1989), the choice of u and v has a significant influence on the coefficient size. Moreover, optimal output is not always reachable by this algorithm, no matter how u and v are chosen, even for simple cases. Transformations different than that of `RNPuiseux` may be necessary. In this example, reduction of powers of a in the course of the computation by substitutions of the form $T = U/a^s$ result in smaller coefficients, but it is not clear how efficient this workaround may be in general.

7. Summary and conclusion

We have presented the symbolic part of our symbolic-numeric strategy for efficiently computing floating point Puiseux series over critical points of $F \in K[X,Y]$, with K algebraic number field. The symbolic information required to guide floating point computations is encoded in a so called "polygon tree" $\mathcal{T}(F)$, or its rational counterpart $\mathcal{RT}(L,F)$. Our investigation of modular reduction of Puiseux series yields a criterion to ensure that F and $\overline{F}$, its reduction modulo $\mathfrak{p}$, have the same polygon tree. The symbolic part may therefore be summarized as follow:

(1) find a prime ideal $\mathfrak{p}$, by means of deterministic or probabilistic methods, such that F has (local or global) good $\mathfrak{p}$-reduction,
(2) determine a finite field $\mathbb{F}_{p^t}$ isomorphic to $\mathfrak{o}/\mathfrak{p}$ and compute $\overline{F}$, image of F under this isomorphism,
(3) compute $\mathcal{RT}(\mathbb{F}_{p^t}, \overline{F})$ using `RNPuiseux`, the rational Newton Puiseux algorithm due to Duval, using generic Newton polygons instead of classical ones,
(4) deduce $\mathcal{T}(\overline{F})$ using Proposition 30, at the cost of a tree traversal,
(5) by Theorem 48, $\mathcal{T}(F) = \mathcal{T}(\overline{F})$.

The generic Newton polygons that we introduced are crucial to prove invariance of polygon trees under good reduction; they also provide regularity indices of Puiseux series. Information such as the genus of the curve defined by F or the topological type of its singularities can also be extracted from polygon trees; we therefore obtain a modular method to compute them.

Finally, we have shown that good primes of polynomial size (with respect to the size of F) can be deterministically obtained, while Monte Carlo and Las Vegas approaches yield good primes with logarithmic size that may effectively be used to avoid expression swell.

Complexity estimates for the symbolic part of our method are proven in (Poteaux and Rybowicz, 2009). The description of the numeric part is left to forthcoming papers; preliminary results can be found in (Poteaux and Rybowicz, 2008; Poteaux, 2008, 2007).

Finally, we remark that, although Walsh (1999) proved that rational Puiseux expansions over K with polynomial size coefficient exist, an algorithm to compute rational Puiseux expansions with provably small coefficient size is still unknown; see end of Section 6.3.

Acknowledgements

The authors would like to thank Mark van Hoeij and Grégoire Lecerf for stimulating conversations.

References

Bach, E., Shallit, J., 1996. Algorithmic Number Theory: Efficient Algorithms. Vol. 1. The MIT Press.

Bliss, G. A., 1933. Algebraic functions. AMS.

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma Algebra System I : The User Language. Journal of Symbolic Computation 24 (3-4), 235–265.

Bostan, A., Chyzak, F., Lecerf, G., Salvy, B., Schost, E., 2007. Differential Equations for Algebraic Functions. In: Brown, C. W. (Ed.), ISSAC'07: Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation. ACM Press, pp. 25–32.

Brieskorn, E., Knörrer, H., 1986. Plane Algebraic Curves. Birkhaüser.

Bronstein, M., 1990. Integration of Elementary Functions. Journal of Symbolic Computation 9 (2), 117–173.

Campillo, A., 1980. Algebroid Curves in Positive Characteristic. Vol. 378 of LNCS. Springer-Verlag.

Chevalley, C., 1951. Introduction to the Theory of Algebraic Functions of One Variable. Vol. 6 of Mathematical Surveys. AMS.

Chudnovsky, D. V., Chudnovsky, G. V., 1986. On Expansion of Algebraic Functions in Power and Puiseux Series. I. Journal of Complexity 2 (4), 271–294.

Chudnovsky, D. V., Chudnovsky, G. V., 1987. On Expansion of Algebraic Functions in Power and Puiseux Series. II. Journal of Complexity 3 (1), 1–25.

Cohen, H., 1993. A Course in Computational Algebraic Number Theory. Springer-Verlag.

Cohn, P. M., 1984. Puiseux's Theorem Revisited. Journal of Pure and Applied Algebra 24, 1–4.

Comtet, L., 1964. Calcul pratique des coefficients de Taylor d'une fonction algébrique. L'Enseignement Mathématique 2 (10), 267–270.

Deconinck, B., Patterson, M. S., 2008. Computing the Abel Map. Physica D: Nonlinear Phenomena 237, 3214–3232.

Deconinck, B., van Hoeij, M., 2001. Computing Riemann Matrices of Algebraic Curves. Phys. D 152/153, 28–46.

Della Dora, J., Dicrescenzo, C., Duval, D., 1985. About a New Method for Computing in Algebraic Number Fields. In: EUROCAL 85. Springer-Verlag LNCS 204.

Diaz-Toca, G., Gonzalez-Vega, L., Sep. 2002. Determining Puiseux Expansions by Hensel's Lemma and Dynamic Evaluation. In: Ganzha, V., Mayr, E., Vorozhtsov, E. (Eds.), Computer Algebra in Scientific Computing, CASC 2002. Technische Universität München, Germany.

Duval, D., 1987. Diverses questions relatives au calcul formel avec des nombres algébriques. Université de Grenoble, Thèse d'État.

Duval, D., 1989. Rational Puiseux Expansions. Compositio Math. 70 (2), 119–154.

Duval, D., 1991. Absolute Factorization of Polynomials. SIAM Journal on Computing 20 (1), 1–21.

Dwork, B., Robba, P., 1979. On natural radii of p-adic convergence. Trans. Amer. Math. Soc. 256, 199–213.

Eichler, M., 1966. Introduction to the Theory of Algebraic Numbers and Functions. Academic Press.

Encarnación, M. J., 1995. Computing GCDs of Polynomials over Algebraic Number Fields. Journal of Symbolic Computation 20, 299–313.

Forster, O., 1981. Lectures on Riemann Surfaces. Graduate Text in Mathematics. Springer Verlag, New-York, Berlin.

Fulton, W., 1969. Hurwitz Schemes and Irreducibility of Moduli of Algebraic curves. Annals of Mathematics, 90:542–575 90, 542–575.

Henry, J.-P., Merle, M., 1987. Complexity of Computation of Embedded Resolution of Algebraic Curves. In: Proceedings Eurocal 87. No. 378 in Lecture Notes in Computer Science. Springer-Verlag, pp. 381–390.

Kung, H. T., Traub, J. F., 1978. All Algebraic Functions Can Be Computed Fast. J. ACM 25 (2), 245–260.

Markushevich, A. I., 1967. Theory of Functions of a Complex Variable. Vol. III. Prentice-Hall, Englewood Cliffs, N. J.

Miranda, R., 1995. Algebraic Curves and Riemann Surfaces. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI.

Poteaux, A., 2007. Computing Monodromy Groups Defined by Plane Algebraic Curves. In: Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation. ACM, New-York, pp. 36–45.

Poteaux, A., 2008. Calcul de développements de puiseux et application au calcul de groupe de monodromie d'une courbe algébrique plane. Ph.D. thesis, Université de Limoges.

Poteaux, A., Rybowicz, M., 2008. On the Good Reduction of Puiseux Series and the Complexity of the Newton-Puiseux Algorithm over Finite Fields. In: ISSAC'08: Proceedings of the 2008 International Symposium on Symbolic and Algebraic Computation. ACM Press, pp. 239–246.

Poteaux, A., Rybowicz, M., 2009. Complexity Bounds for the Rational Newton-Puiseux Algorithm over Finite Fields. Submitted to Applicable Algebra in Engineering, Communication and Computing.

Robert, A. M., 2000. A Course in p-adic Analysis. Vol. 198 of Graduate Texts in Mathematics. Springer-Verlag, New York.

Sasaki, T., Inaba, D., 2000. Hensel Construction of $f(x, u_1, \ldots, u_l)$ at a Singular Point and its Application. Sigsam Bulletin 1, 9–17.

Shoup, V., 2005. A Computational Introduction to Number Theory. Cambridge University Press.

Trager, B. M., 1984. Integration of Algebraic Functions. Ph.D. thesis, Department of EECS MIT.

van der Hoeven, J., 1999. Fast Evaluation of Holonomic Functions. Theoretical Computer Science 210 (1), 199–215.

van der Hoeven, J., 2005. Effective Analytic Functions. Journal of Symbolic Computation 39 (3-4), 433–449.

van Hoeij, M., 1994. An Algorithm for Computing an Integral Basis in an Algebraic Function Field. Journal of Symbolic Computation 18, 353–363.

van Hoeij, M., 1997. Rational Parametrizations of Algebraic Curves using a Canonical Divisor. Journal of Symbolic Computation 23, 209–227.

von zur Gathen, J., Gerhard, J., 1999. Modern Computer Algebra. Cambridge University Press, Cambridge.

Walker, R. J., 1950. Algebraic Curves. Springer-Verlag.

Walsh, P. G., 1999. On the Complexity of Rational Puiseux Expansions. Pacific Journal of Mathematics 188, 369–387.

Walsh, P. G., 2000. A Polynomial-time Complexity Bound for the Computation of the Singular Part of an Algebraic Function. Mathematics of Computation 69, 1167–1182.

Weinberger, P. J., Rothschild, L. P., 1976. Factoring Polynomial over Algebraic Number Fields. Transactions on Mathematical Software 2, 335–350.

Zariski, O., 1981. Le problème des modules pour les branches planes. Hermann, Paris.