Good Reduction of Puiseux Series and Complexity of the Newton-Puiseux Algorithm over Finite Fields

Adrien Poteaux, Marc Rybowicz
XLIM - DMI, UMR CNRS 6172
Université de Limoges
adrien.poteaux@xlim.fr, marc.rybowicz@xlim.fr

ABSTRACT

In [12], we sketched a numeric-symbolic method to compute Puiseux series with floating point coefficients. In this paper, we address the symbolic part of our algorithm. We study the reduction of Puiseux series coefficients modulo a prime ideal and prove a good reduction criterion sufficient to preserve the required information, namely Newton polygon trees. We introduce a convenient modification of Newton polygons that greatly simplifies proofs and statements of our results. Finally, we improve complexity bounds for Puiseux series calculations over finite fields, and estimate the bit-complexity of polygon tree computation.

Categories and Subjects Descriptors: I.1.2 [Symbolic and Algebraic Manipulation]: Algorithms; F.2.1 [Analysis of Algorithms and Problem Complexity]: Numerical Algorithms and Problems.

General Terms: Algorithms, Theory.

Keywords: Puiseux Series, Algebraic Functions, Modular Methods, Finite Fields, Complexity, Symbolic-Numeric Algorithms.

1. INTRODUCTION

Let K be a number field and $F(X,Y)$ be a squarefree bivariate polynomial in $K[X,Y]$, monic in Y, such that $\deg_Y(F) = d > 1$ and $\deg_X(F) = n > 0$. Denote by $\Delta_F(X)$ the discriminant of F with respect to Y. A root of Δ_F will be called a *critical point*. The equation $F(X,Y) = 0$ defines d 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 values of these functions in $\mathcal{D}$ can be obtained directly via truncated Puiseux series at $X = x_0$ (see Section 2). We have used this fact to devise an algorithm to compute the monodromy of the Riemann sphere covering defined by the curve $F(X,Y) = 0$ [12], a question that has numerous applications, including the determination of Galois groups, effective versions of Abel-Jacobi's Theorem [5], which in turn are useful in various context (see [5, 4]). Unfortunately, applying a floating point Newton-Puiseux algorithm (see Section 3) to compute Puiseux series 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 helpful. On the other hand, coefficient growth considerably slows down symbolic methods. Since the degree of Δ_F is in $O(nd)$, Puiseux series coefficients above x_0 belong to a finite extension of K whose degree over K may be in $O(d^2n)$. Moreover, when these coefficients are expressed as linear combination 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 [12]). Walsh [18] has shown that, for any $\epsilon > 0$, the singular part of Puiseux series can be computed using $O(d^{32+\epsilon}n^{4+\epsilon}\log h^{2+\epsilon})$ bit operations where h is the height of F. Although this bound is probably not sharp, it is not encouraging and tends to confirm experimental observations. To alleviate these problems, we introduced a symbolic-numeric approach : exact important information is first obtained by means of computations 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 unstability is reduced. Exact important data, such as ramification indices and intersection multiplicities of branches, are preserved. Experimental evidences reported in [12] seem to validate this approach. This paper presents several contributions :

- Section 3 introduces “generic Newton polygons” and “polygon trees”. The latter concept captures precisely the symbolic information needed for floating point computations. We explain how polygon trees can be obtained using modular arithmetic. For this task, generic Newton polygons are more convenient than classical ones (see Section 4).
- In Section 4, we study modular reduction of Puiseux series and provide a fully proved and easy to check criterion for choosing a “good prime”.
- Improved complexity bounds for the computation of rational Puiseux expansions over finite fields are given in Section 5. We also deduce bit-complexity estimates for a randomized version of the modular part of our symbolic-numeric method (Section 6).

Because of the lack of space, proofs and many comments

ISSAC'08, July 20–23, 2008, Hagenberg, Austria.

have been omitted. For proofs and details, the reader is refered to the extended version [13] available on the Internet.

The following notations and well-known facts will be used throughout the paper :

- If L is a field, $\overline{L}$ will denote an algebraic closure of L.
- 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 $tc(S)$ the trailing coefficient of S, namely $S = tc(S)X^{v_X(S)} +$ higher order terms.
- If $S = \sum_{k \geq l} \alpha_k X^{k/e}$ is an element of $L((X^{1/e}))$ and r is a rational number, $\widetilde{S}^r$ denotes the truncated power series $\widetilde{S}^r = \sum_{k=l}^{N} \alpha_k X^{k/e}$ where $N = \max\{k \in \mathbb{N} \mid \frac{k}{e} \leq r\}$.
- The discriminant of a univariate polynomial U is denoted by Δ_U. If U is a multivariate polynomial, the context will always allow to identify the variable.
- Let f be a polynomial in $L[T]$ with squarefree factorization $f = \prod_{i=1}^{r} f_i^{k_i}$. 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 $\deg f$.
- If $H \in L[X, Y]$, then H_X and H_Y are the formal partial derivatives of H.
- For $H(\underline{X}) = \sum_{\underline{k}} \alpha_{\underline{k}} \underline{X}^{\underline{k}} \in \mathbb{C}[\underline{X}] = \mathbb{C}[X_1, \ldots, X_n]$, where $\underline{k}$ is a multi-index, we denote $\|H\|_\infty = \max_{\underline{k}}\{|\alpha_{\underline{k}}|\}$.

2. PUISEUX SERIES

We need to state results over more general fields than K. Throughout this section, L denotes a field of characteristic $p \geq 0$ and F belongs to $L[X, Y]$. Otherwise, we keep the assumptions and notations of Section 1. We also impose the condition :

$$p = 0 \qquad \text{or} \qquad p > d = \deg_Y(F) \qquad (1)$$

After a change of variable $X \leftarrow X + x_0$, we may assume that the critical point is $X = 0$.

2.1 Classical Puiseux series

In this part, we review classical results about Puiseux series. We begin with :

Theorem 1 (Puiseux). *Let H be a squarefree polynomial of $L[X, Y]$ such that $\deg_Y(H) = d > 0$. If condition (1) is satisfied, there exist positive integers $e_1, \ldots, e_s$ satisfying $\sum_{i=1}^{s} e_i = d$ such that H, viewed as a polynomial in Y, has d distinct roots in $\overline{L((X))}$ which can be written :*

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

for $1 \leq i \leq s$ and $0 \leq j \leq e_i - 1$. Moreover, the set of coefficients $\{\alpha_{ik}\}$ is included in a finite algebraic extension of L.

Definition 1. *The d fractional Laurent series above 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 $X = 0$.

An arbitrary number of terms of all Puiseux series can be effectively computed using the Newton-Puiseux algorithm (see Section 3). For each positive integer $e \leq d$, hypothesis (1) implies that the Galois group $\mathbb{G}_e$ of $\overline{L}((X^{1/e}))/\overline{L}((X))$ is cyclic and generated by : $X^{1/e} \mapsto \zeta_e X^{1/e}$. Hence, $\mathbb{G}_{e_i}$ permutes cyclically the elements of $S_i = \{S_{ij}(X)\}_{0 \leq j \leq e_i - 1}$.

Definition 2. *We call S_i* a cycle of H above 0. *If an element of S_i (thus, all elements) vanishes 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 from any element of S_i, it is sufficient for our purposes to compute a set of representatives for the cycles of H.

Definition 3. *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 $(u, v) = (i, j)$. The truncated series $\widetilde{S_{ij}}^{\frac{r_{ij}}{e_i}}$ 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 $L[X, Y]$.

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 [11, 17]. 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 $1 \leq i \leq s$.

2.2 The characteristic of a Puiseux series

We derive relations between the discriminant of F and particular coefficients of its Puiseux series that we shall use to define a "good reduction" criterion. Let $S(X) = \sum_{i=0}^{\infty} \alpha_i X^{i/e}$ denote a Puiseux series of F with ramification index $e > 1$. We define a sequence $(B_0, R_0), \ldots, (B_g, R_g)$ of integer pairs as follows : $(B_0, R_0) = (0, e)$, and for $j > 0$, if $R_{j-1} > 1$ we set $B_j = \min\{i > B_{j-1} \mid \alpha_i \neq 0 \,\text{and}\, R_{j-1} \nmid i\}$ 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 $Q_j = R_{j-1}/R_j$, $M_j = B_j/R_j$ $(1 \leq j \leq g)$ and define H_j to be the largest nonnegative integer such that $B_j + H_j R_j < B_{j+1}$ for $0 \leq j \leq g - 1$. It is clear that $e = Q_1 Q_2 \cdots Q_g$ and M_j is an integer prime to Q_j.

With these notations, and up to a new indexing of the coefficients, S can be written in the form :

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

In the expression above, the monomials of S are ordered by increasing (rational) degree.

Definition 4 ([19, 1]). *The* characteristic *of S is the tuple of integers $(e; B_1, \ldots, B_g)$. The* characteristic coefficients *are the elements of $(\gamma_1, \ldots, \gamma_g)$ and the* characteristic monomials *are the corresponding monomials of S.*

Proposition 1. *Assume that hypothesis (1) is satisfied. 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. Then :*

- $tc(\Delta_G) = \pm\left(\prod_{i=1}^{g} Q_i^{R_i} \prod_{i=1}^{g} \gamma_i^{R_{i-1} - R_i}\right)^e$
- $v_X(\Delta_G) = \sum_{i=1}^{g} B_i(R_{i-1} - R_i)$.

2.3 Rational Puiseux expansions

In order to perform computations in the smallest possible extension of L and to take advantage of conjugacy over L, Duval introduced the notion of "rational Puiseux expansions over L" [6]. This arithmetical concept is irrelevant in the context of floating point computations, but will prove useful for expansions over finite fields.

Definition 5. *Let H be a polynomial in $L[X,Y]$ with $\deg_Y H > 0$. A* parametrization *$R(T)$ of H is a pair of non constant power series $R(T) = (X(T), Y(T)) \in \overline{L}((T))^2$ 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 :

$$\begin{array}{rrcl} \phi_R : & \mathcal{K} & \rightarrow & \overline{L}((T)) \\ & f(X,Y) & \mapsto & f(X(T), Y(T)) \end{array}$$

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 [2] and that $V_R = \{f \in \mathcal{K} \mid v_T(f) \geq 0\}$ is the corresponding V-ring of $\mathcal{K}$. We recall that $\mathfrak{P}_R$ is the unique maximal ideal of V_R and that the *residue field* of $\mathfrak{P}_R$ is $V_R/\mathfrak{P}_R$, which can be viewed as 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, to each place $\mathfrak{P}$ of $\mathcal{K}$ correspond a parametrization of H. Let us 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 6 (Rational Puiseux expansions).
- *Assume that H is irreducible in $L[X,Y]$. 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 :*

$$R_i(T) = (X_i(T), Y_i(T)) = (\gamma_i T^{e_i}, \sum_k \beta_{ik} T^k) \in \overline{L}((T))^2$$

with $e_i > 0$ such that :
(i) *Ψ is one-to-one from $\{R_i\}_{1 \leq i \leq r}$ to $\{\mathfrak{P}_i\}_{1 \leq i \leq r}$. We assume that the $\mathfrak{P}_i$ are numbered so that $\mathfrak{P}_i = \mathfrak{P}_{R_i} = \Psi(R_i)$.*
(ii) *The coefficient field of R_i is isomorphic to k_i.*
- *Assume that H is squarefree. 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 $L[X,Y]$.*

Definition 7. *If $Y_i \in \overline{L}[[T]]$, we say that R_i is* defined at $T = 0$ *and call $(X_i(0), Y_i(0))$ the* center *of R_i.*

The classical formula relating degrees of residue fields and ramification indices of an algebraic function field (see [2]) translates into :

Theorem 2. *Let H be squarefree polynomial of $L[X,Y]$, $\deg_Y H = d > 0$ and $\{R_i\}_{1 \leq i \leq r}$ be a system of L-rational Puiseux expansions above 0 for H. If f_i denotes the degree over L of the coefficient field of R_i, then $\sum_{i=1}^r e_i f_i = d$.*

Classical Puiseux series can readily be deduced from a system of rational Puiseux expansions (see [13]). Classical Puiseux series that are defined at $X = 0$ (resp. that vanish at $X = 0$) correspond to rational Puiseux expansions defined at $T = 0$ (resp. centered at $(0,0)$). Moreover, we note that 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 $\left(\gamma_i T^{e_i}, \sum_{k=-\infty}^{r_i} \beta_{ik} T^k\right)$, where r_i is the regularity index of a Puiseux series associated to R_i.

Since our initial polynomial F is monic, rational Puiseux expansions of F above zero are all defined at $T = 0$.

3. NEWTON-PUISEUX ALGORITHM

We describe an algorithm to compute singular parts of rational Puiseux expansions. We also briefly recall how to compute classical Puiseux series. Throughout Section 3, L denotes again a field of characteristic $p \geq 0$ and $F \in L[X,Y]$ is a polynomial such that condition (1) is satisfied. Moreover, we keep assumptions and notations of Section 1.

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.

3.1 Generic Newton polygons

Assume that $H(X,Y) = \sum_{i,j} a_{ij} X^j Y^i$ is a polynomial of $L[[X]][Y]$ such that $H(0,Y) \neq 0$.

Definition 8. *Denote by $\mathcal{I}(H)$ the nonnegative integer $v_Y(H(0,Y))$ and by $\mathcal{H}$ the convex hull of Supp$(H) = \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$. The* Newton Polygon *$\mathcal{N}(H)$ of H is the lower part of $\mathcal{H}$. Namely :*
- *If $H(X,0) \neq 0$, $\mathcal{N}(H)$ is formed by the sequence of edges of $\mathcal{H}$ closest to the origin and 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.*

We introduce a slightly different object, that we call *generic Newton polygon* for reasons explained in [13]. This variation allows a homogeneous treatment of finite series, clearer specifications for the algorithms and simplifies wording and proofs of results regarding modular reduction.

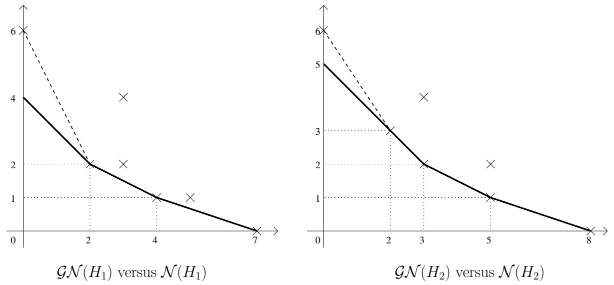
Definition 9. *The* generic Newton polygon *$\mathcal{GN}(H)$ is obtained by restricting $\mathcal{N}(H)$ to edges with slope no less than -1 and by joining the leftmost remaining point to the vertical axis with an edge of slope -1.*

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

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

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

Example 3. *Assume that $H_3(X,Y) = Y$. The classical polygon $\mathcal{N}(H_3)$ is the trivial polygon $(1,0)$. But $\mathcal{GN}(H_3)$ is formed of a unique edge joining $(0,1)$ to $(1,0)$.*



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

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

Figure 1: Generic versus classical polygons

Remark 1. *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 code is used to compute integral bases [16], but the implementation technique has not been published. In essence, Van Hoeij's implementation uses "local truncation orders", while Proposition 6 can be viewed as a "global truncation order". The latter allows to obtain complexity bounds. While local truncation orders may prove more efficient in practice, it is not clear that they lead to a better asymptotic behaviour.*

The algorithm first stage requires a special treatment. To this effect, we introduce the following definition :

Definition 10. *The exceptional Newton polygon $\mathcal{EN}(H)$ is the unique horizontal edge* $[(0,0),(\deg_Y H(0,Y),0)]$.

In particular, $\mathcal{EN}(F) = [(0,0),(d,0)]$ since F is monic. To an edge Δ of $\mathcal{GN}(H)$ (or $\mathcal{N}(H)$, $\mathcal{EN}(H)$) correspond three nonnegative integers q, m and l with 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 11. *We define the* characteristic polynomial *of Δ as $\phi_\Delta(T) = \sum_{(i,j)\in\Delta} a_{ij} T^{\frac{i-i_0}{q}}$, where i_0 is the smallest value 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 $\mathcal{GN}(H)$ allows such cancellation if Δ is a fictitious edge (or contains 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 the fictitious edge) added. For $\mathcal{EN}(H)$, 0 can also be a root of the characteristic polynomial.

The algorithm below performs successive changes of variable, determined by (q,m,l) and the roots of ϕ_Δ. It returns a set of triplets $\{(G_i(X,Y),P_i(X),Q_i(X,Y))\}_i$ such that :

- $G_i, P_i, Q_i \in \overline{L}[X,Y]$,
- $P_i(X)$ is a monomial of the form $\lambda_i X^{e_i}$,
- $Q_i(X,Y) = Q_{i0}(X) + Y\,X^{r_i}$, where r_i is the regularity index of the expansion and $(P_i(T),Q_{i0}(T))$ is the singular part of a parametrization of F,
- There exist nonnegative 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 $G_{iY}(0,0) \neq 0$.

3.2 Rational Newton-Puiseux algorithm

We present an algorithm due to Duval to compute singular parts of rational Puiseux expansions above 0 [7]. We also give differences between this algorithm and the classical one. We need two auxiliary algorithms, for which we only provide specifications :

```
Factor($L$,$\phi$)
 Input:   $L$ :   A field.
          $\phi$ :   A univariate polynomial in $L[T]$.
 Output:  A set of pairs $\{(\phi_i,k_i)\}_i$ so that $\phi_i$ is
          irreducible in $L[T]$ and $\phi = \prod_i \phi_i^{k_i}$.
Bezout($q$,$m$)
 Input:   $q, m$ :   Two coprime positive integers.
 Output:  A pair of integers $(u,v)$ so that $uq - mv = 1$.
          If $q = 1$, enforce $v = 0$ and $u = 1$.
```

```
Algorithm RNPuiseux($L$,$H$)
 Input:   $L$ :   A field.
          $H$ :   A squarefree polynomial of degree $d \geq 1$
                  in $L[X,Y]$, such that $H(0,Y) \neq 0$.
 Output:  A set of triplets $\{[G_i,P_i,Q_i]\}_i$, which form a
          set of representatives for :
          - $L$-rational Puiseux expansions of $H$ defined
          at $T = 0$ for the initial call,
          - $L$-rational Puiseux expansions of $H$ centered
          at $(0,0)$ for recursive calls.
Begin
   If in a recursive call then
      $\mathcal{P} \leftarrow \mathcal{GN}(H)$
      If $\mathcal{I}(H) = 1$ then Return $\{[H,X,Y]\}$ End
   else
      $\mathcal{P} \leftarrow \mathcal{EN}(H)$
   End
   $\mathcal{R} \leftarrow \{\}$
   For each side $\Delta$ of $\mathcal{P}$ do
      Compute $q$, $m$, $l$ and $\phi_\Delta$
      $(u,v) \leftarrow$ Bezout($q,m$)
      For each $(f,k)$ in Factor($L,\phi_\Delta$) do
         $\xi \leftarrow$ Any root of $f$
         $H'(X,Y) \leftarrow H(\xi^v X^q, X^m(\xi^u + Y))/X^l$
         For each $[G,P,Q]$ in RNPuiseux($L(\xi)$,$H'$) do
            $\mathcal{R} \leftarrow \mathcal{R} \cup \{[G, \xi^v\,P^q, P^m(\xi^u + Q)]\}$
         End
      End
   End
   Return $\mathcal{R}$
End.
```

Replacing L by $\overline{L}$ and (u,v) by $(1/q,0)$ in `RNPuiseux`, one obtains the classical algorithm, that we call `CNPuiseux`.

Example 4. *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 :*

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

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 :*

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

The first null coefficient of (P_1, Q_1) comes from the exceptional polygon $[(0,0),(0,7)]$. The second one corresponds to the fictitious edge of $\mathcal{GN}(F)$ introduced at the first recursive call. This may seem inefficient, but it has no impact on the complexity and clarifies arguments in Section 4.

3.3 Polygon trees

To a function call `RNPuiseux`(L, F) (see Section 3.2), we associate a labelled 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 is constructed recursively from the root vertex as follow (see Figure 2). Even depth vertices correspond to function calls.

- A vertex v of even depth l is labelled with the polygon $\mathcal{P}$, that is $\mathcal{EN}(H)$ for the root vertex ($l = 0$), and $\mathcal{GN}(H)$ for recursive calls ($l > 0$).
- To each Δ of $\mathcal{P}$ corresponds an edge from v to a depth $l+1$ vertex. Label the edge with Δ (represented by its end-point).
- A child (depth $l + 1$ vertex) is labelled with the corresponding integer partition $[\phi_\Delta]$ (see the end of Section 1).
- 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 labelled 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`$(L(\xi),\ H')$ where H' is the polynomial H' obtained for a choice of edge Δ and a choice of root ξ.

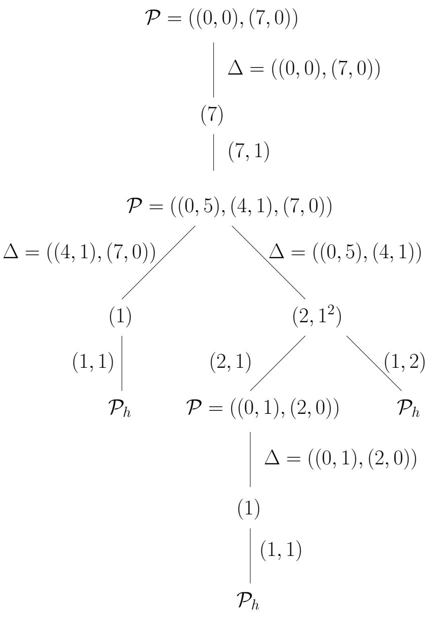


Figure 2: Polygon tree $\mathcal{RT}(\mathbb{Q}, F)$ for Example 4.

The leaves are even depth vertices labelled 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 squarefree factorization is a subproduct of the factorization over L, the labelled 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 labelled 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 labelled with a multiplicity k because the ground field is $\overline{L}$ and all field extension have degree 1.

Definition 12. *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 to achieve our goal.

Proposition 2. *The tree $\mathcal{T}(F)$ can easily be obtained from $\mathcal{RT}(L, F)$ as follow : duplicate f times each edge labelled (k, f) (together with the subtree rooted at this edge) and replace the tag (k, f) by the tag k.*

4. GOOD REDUCTION

We consider a polynomial F 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 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, $\mathfrak{p}$ a prime ideal of $\mathfrak{o}$ and $v_\mathfrak{p}$ 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 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 $\mathfrak{P}$ for a prime ideal of $\mathfrak{O}$, we introduce $\mathfrak{O}_\mathfrak{P} = \{\alpha \in L \mid v_\mathfrak{P}(\alpha) \geq 0\}$.

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 shall use the same notation $\overline{\alpha}$.

4.1 Modular reduction of Puiseux series

Our reduction strategy is based on the following definition :

Definition 13. *Let p be a prime number and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}$ dividing p. We say that F has* local (at $X = 0$) good reduction at $\mathfrak{p}$ *if : $F \in \mathfrak{o}_\mathfrak{p}[X, Y]$, $p > d = \deg_Y(F)$ and $v_\mathfrak{p}(tc(\Delta_F)) = 0$.*

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

Remark 2. *Applying our local criterion to all places of $K[X]$, we obtain that $[\Delta_F]$ must be equal to $[\Delta_{\overline{F}}]$ (preservation of the squarefree factorization). This test has 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 [15], publicly avalaible since Maple V.5. This condition was derived from proofs in ([9], 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 [10].*

A fundamental result for the reduction strategy is the following consequence of a theorem by Dwork and Robba [8] :

Theorem 3. *If F has local good reduction at $\mathfrak{p}$, then the Puiseux series coefficients of F above 0 are in $\mathfrak{O}_{\mathfrak{P}}$.*

We emphasize that this result holds for *any* $\mathfrak{P}$ dividing $\mathfrak{p}$.

Example 5. *Consider the case $F(X,Y) = Y^2 - X^3(p + X)$ with $p > 2$. Puiseux series above 0 are :*

$$\begin{aligned} S_{1j}(X) &= (-1)^j \sqrt{p} X^{3/2} \left(1 + \frac{X}{p}\right)^{1/2} \\ &= (-1)^j \sqrt{p} X^{3/2} (1 + \frac{X}{2p} - \frac{X^2}{8p^2} + \cdots). \end{aligned}$$

They are obviously not reducible modulo p, but the discriminant criteria of the theorem detects this deficiency.

Theorem 4. *Let $\{S_i\}_{1 \le i \le s}$ be a set of representatives for the cycles of F above 0. Assume that F has local good reduction at $\mathfrak{p}$. Then, $\{\overline{S_i}\}_{1 \le i \le s}$ is a set of representatives for the cycles of $\overline{F}$ above* 0.

However, annihiliation modulo $\mathfrak{P}$ of Puiseux series coefficients is not totally controlled by our good reduction criterion. If F is irreducible in $\overline{K}[[X]][Y]$, all non-characteristic coefficients may vanish modulo $\mathfrak{P}$, as shown by Proposition 1 (consider for instance the minimal polynomial over $\mathbb{Q}(X)$ of $S(X) = pX + X^{3/2}$). If F is not irreducible, our criterion will also detect cancellation of coefficients that "separate" cycles. This property is contained in Theorem 5.

4.2 Modular reduction of polygon trees

If $F \in \mathfrak{o}_{\mathfrak{p}}[X,Y]$ and $p > d$, algorithms of Section 3 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 obtain by means of modular computations the symbolic information required by the numerical algorithm in [12] :

Theorem 5. *If F has local good reduction at $\mathfrak{p}$, then :*
$$\mathcal{T}(F) = \mathcal{T}(\overline{F}).$$

The correspondence between $\mathcal{T}(F)$ and $\mathcal{T}(\overline{F})$ cannot be stated so simply if classical polygons are used instead of generic ones : Non-characteristic coefficients of Puiseux series may vanish upon modular reduction, yielding polygon modifications. Moreover, if the exceptional polygon is replaced by the generic polygon, the good reduction criterion does not detect the cancellation of $F(0,0)$, as shown by the example $F(X,Y) = (Y + p + X)(Y + 1 + X)$. But the criterion detects a change of root multiplicities. This example justifies the introduction of $\mathcal{EN}(F)$.

4.3 Choosing a good prime

This part is devoted to the choice of a prime ideal $\mathfrak{p}$ such that F has local good reduction at $\mathfrak{p}$.

Assume that $K = \mathbb{Q}(\gamma)$ and let M_γ be the minimal polynomial of γ over $\mathbb{Q}$. The 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 14. *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 num(P). The integer c is called the* denominator *of H and is written denom(P). We define the* size of *P as follow : $ht(P) = \max\{\log_2 c, \log_2 \|R\|_\infty\}$.*

Denoting $F_n = \text{num}(F)$ and $b = \text{denom}(F)$, we have $F(X,Y) = \frac{F_n(\gamma,X,Y)}{b}$. 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) $p > d$.
(C_2) p does not divide b.
(C_3) We can determine an explicit representation of a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ dividing p, so that a morphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_{p^t}$ can be effectively computed.
(C_4) $tc(\Delta_F) \not\equiv 0$ modulo $\mathfrak{p}$.

Condition (C_1) and (C_2) are easily checked out. We deal with condition (C_3) in a standard fashion. Let $\overline{M}$ be any irreducible factor of M_γ 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 $e_\gamma = [\mathfrak{o} : \mathbb{Z}(\gamma)]$ and if $\overline{M}$ is any irreducible factor of M_γ in $\mathbb{F}_p[T]$, then the ideal $\mathfrak{p} = (p, M(\gamma))$ of $\mathfrak{o}$ is prime [3]. Hence, elements of $\mathfrak{o}$ can be reduced by means of the morphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_p[T]/(\overline{M}) \cong F_{p^t}$, 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 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 reduce t, the case $t = 1$ being the most favorable.

As for (C_4), deterministic and randomized strategies are studied in the next subsections. In order to simplify the analysis, we replace condition (C_4) by the following stronger condition :
(C_4') $\text{Norm}_{K/\mathbb{Q}}(tc(\Delta_F)) \not\equiv 0$ modulo p.
If (C_1) to (C_4') are verified, then for all prime ideals $\mathfrak{p}$ dividing p, F has local good reduction at $\mathfrak{p}$. In practice, though, we do not recommand to use (C_4'). Finally, we introduce the notation $N_F = b \cdot |\text{Norm}_{K/\mathbb{Q}}(tc(\Delta_F))| \cdot |\Delta_{M_\gamma}|$. Conditions (C_1) to (C_4') are equivalent to :
(C_5) $p > d$ and $N_F \not\equiv 0$ modulo p.

4.3.1 Deterministic strategy

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

Lemma 1. *The discriminant $\Delta_{F_n} \in \mathbb{Z}[X,T]$ of F_n with respect to Y satisfies :*
$$\|\Delta_{F_n}\|_\infty \le (2d-1)!\, d^d \left[(w+1)(n+1)\right]^{2d-2} \|F_n\|_\infty^{2d-1}.$$

We denote by $R_F(T)$ the numerator of $tc(\Delta_F)$. Note that $\mathrm{denom}(tc(\Delta_F))$ is a power of b dividing b^{2d-1}.

Lemma 2. *Define :*

$$B_0 = \|\Delta_{F_n}\|_\infty(\|M_\gamma\|_\infty + 1)^{(w-1)(2d-1)-w+1},$$

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

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

Then, $|Norm_{K/\mathbb{Q}}(R_F(\gamma))| \le B_1$ *and* $e_\gamma \le |\Delta_{M_\gamma}| \le B_2$*.*

Proposition 3. *Set* $B = \max\{b, d+1, B_1, B_2\}$*. Then, for all* $p > B$*, condition* (C_5) *is verified. Moreover, there exists a prime* $p > B$ *with size* $ht(p)$ *in :*

$$O(wd(w\,ht(M_\gamma) + ht(F) + \log(wnd))).$$

4.3.2 Probabilistic strategies

We begin with a "Monte-Carlo" method, best described by the following algorithm. We need two auxiliary 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 $[A, C]$ (see [14], Section 7.5). The function `Nextprime` gives the smallest prime larger than the argument.

```
MCGoodPrime($d$,$B'$,$\epsilon$)
  Input:   $d$  :  The degree in $Y$ of the polynomial $F$.
           $B'$ :  A real number such that prime factors
                   of $N_F$ are less or equal to $B'$.
           $\epsilon$  :  A real number with $0 < \epsilon \le 1$.
  Output:  A prime number $p$ satisfying $(C_5)$ with
           probability at least $1 - \epsilon$.
Begin
   If $B' < 100$ then Return NextPrime($B'$) End
   $K \leftarrow 6\ln B'/(\epsilon \ln\ln B') + 2d/\ln d$
   $C \leftarrow \max\{2d, K(\ln K)^2\}$
   Return RandomPrime($d+1, C$)
End.
```

Proposition 4. `MCGoodPrime`*(d, B′, ϵ) returns a prime* p *satisfying* $ht(p) \in O(\log\log B' + \log d + \log \epsilon^{-1})$*. In particular, if* $B' = \max\{b, B_1, B_2\}$ *(see Lemma 2), then :* $ht(p) \in O(\log(dw\log n) + \log ht(F) + \log ht(M_\gamma) + \log \epsilon^{-1})$*. The probability that* p *does not satisfy* (C_5) *is less than* ϵ*.*

Finally, we consider a "Las Vegas" flavoured method :

```
LVGoodPrime($F$,$M_\gamma$)
  Input:   $F$   :  A polynomial as in Section 1.
           $M_\gamma$  :  A monic irreducible polynomial in $\mathbb{Z}[T]$.
Output: A prime number $p$ satisfying $(C_5)$.
Begin
   $d \leftarrow \deg_Y(F)$
   $N_F \leftarrow \mathrm{denom}(F) \cdot |\mathrm{Norm}_{K/\mathbb{Q}}(R_F(T))| \cdot |\mathrm{Disc}(M_\gamma)|$
   $B' \leftarrow \max\{\mathrm{denom}(F), |\mathrm{Norm}_{K/\mathbb{Q}}(R_F(T))|, |\mathrm{Disc}(M_\gamma)|\}$
   Repeat
      $p \leftarrow$ MCGoodPrime($d, B', 1/2$)
   until $p$ does not divide $N_F$ End
   Return $p$
End.
```

Proposition 5. `LVGoodPrime`*(F,M_γ) returns a prime* p *satisfying* $ht(p) \in O(\log(dw\log n) + \log ht(F) + \log ht(M_\gamma))$ *and* (C_5) *with an average number of iterations less than 2.*

The computation of B' and N_F may have a significant cost. In our monodromy context [12], though, we need to determine Δ_F anyway.

5. COMPLEXITY OVER A FINITE FIELD

In this section, L denotes a finite field and F belongs to $L[X, Y]$. Otherwise, we keep the notations and assumptions of Section 1. We denote by $p > d$ the characteristic of L. We also define $t_0 = [L : \mathbb{F}_p]$. This section is devoted to the proof of the following theorem :

Theorem 6. *Assuming that FFT-based polynomial multiplication over finite fields is used,* `RNPuiseux` *can compute singular parts of a system of rational Puiseux expansions above* 0 *of* F *in* $\tilde{O}(d^3n^2 + d^2nt_0\log p)$ *field operations in* L*.*

As usual, the notation $\tilde{O}$ hides logarithmic factors.

Remark 3. *This result improves the bound of [7], which is in* $O(d^6n^2)$ *field operations. Our estimates include factorization cost, while Duval relies on the D5 system to avoid factorizations. The gain comes from :*
- truncation of powers of X *in the course of the algorithm (see Proposition 6),*
- reducing transformations to shifts of univariate polynomials, for which fast methods are available (Proposition 7),
- a bound for δ_F *(see below and Proposition 9).*

We first introduce notations and make some assumptions :

- $\{R_i\}_{1\le i\le\rho}$ with $R_i(T) = (X_i(T), Y_i(T))$ stands for singular parts of a system of rational Puiseux expansions,
- (r_i, e_i, f_i), $1 \le i \le \rho$ are respectively the regularity index, the ramification index and the coefficient field degree over L of R_i.
- For each rational Puiseux expansion R_i, we can deduce e_if_i Puiseux series denoted $S_{ijk}(X), 1 \le k \le e_i, 1 \le j \le f_i$.
- We define $\delta_F = \sum_{i=1}^{\rho} f_ir_i$.
- L_t denotes an extension of degree t of L.
- $M(N)$ will denote the number of field operations in L_t needed to compute the product of two polynomials in $L_t[Z]$ of degree no larger than N. We recall that $M(N) \in O(N^2)$ for classical arithmetic and $M(N) \in O(N\log N\log\log N) \subset \tilde{O}(N)$ if FFT-based multiplication is used.
- A field operation in L_t can be done using $O(M(t)\log t)$ field operations in L.

We refer the reader to [17] for assertions regarding the complexity of operations over finite fields.

Remark 4. *It is worth noting that* δ_F *represents essentially the number of elements of* L *necessary to represent the* Y_i*. Indeed, each* Y_i *has at most* $r_i + 1$ *nonzero coefficients and each of those may be represented by at most* f_i *elements of* L*. Assume that a dense representation is used for the truncated power series* Y_i *(for instance, a vector of* $r_i + 1$ *elements of* L_{f_i}*) and assume in turn that the coefficients of* Y_i *are represented by vectors of* f_i *elements of* L*. Then, the size of the output is* $\delta_F + \sum_i f_i$*, which is bounded from below by* δ_F *and bounded from above by* $\delta_F + d$*.*

We split the proof into several results.

Proposition 6. *Systems of rational Puiseux expansions for* F *and* $\widetilde{F}^{\delta_F}$ *above 0 have the same singular parts (up to trivial changes of the parameter* T*). Moreover, singular parts of rational Puiseux expansions of* F *can be computed by applying* `RNPuiseux` *to* $\widetilde{F}^{\delta_F}$ *and truncating polynomials* H *modulo* X^{δ_F+1} *at each stage of the algorithm.*

Proposition 7. *The substitutions needed to compute the singular parts of a system of rational Puiseux expansions of* F *requires* $O\left(\delta_F^2 M(d)^2 \frac{\log d}{d}\right)$ *field operations in* L*.*

Proposition 8. *All factorizations of characteristic polynomials required by* `RNPuiseux` *can be computed with an expected number of* $O\left(\delta_F \log d \left[M(d^2) + t_0 \log p M(d) \log d\right]\right)$ *field operations in* L.

It is interesting to bound first the number of operations in L in terms of the output size, namely δ_F.

Theorem 7. *The number of operations in* L *required to compute singular parts of rational Puiseux expansions of* F *above 0 is in* $\tilde{O}\left(\delta_F M(d)\left[\delta_F \frac{M(d)}{d} + M(d) + t_0 \log p\right]\right)$.

Proposition 9. $\delta_F \leq v_X(\Delta_F) \leq n(2d-2)$

Theorem 6 is now a trivial consequence of the last two results.

6. BIT-COMPLEXITY

Let F be a polynomial of $K[X,Y]$, where K is an algebraic number field represented as in Section 4.3. We recall that $[K:\mathbb{Q}] = w$. We study the bit-complexity of the computation of $\mathcal{T}(F)$. We estimate only word operations generated by arithmetic operations in various coefficient fields. Assuming some care is taken in the implementation, (for instance, access to coefficients of polynomial should be achieved in constant time), results below should give a realistic upper bound for the behaviour of an actual computer program.

Our bounds for randomized algorithms do not include the cost of generating prime numbers, nor the cost of computing bounds given by our formula.

We assume that elements of $\mathbb{F}_p$ are represented by nonnegative integers. In order to simplify expressions, we assume that fast arithmetic is used for integer arithmetic as well as polynomial arithmetic over finite fields.

Theorem 8. *Given* ϵ *with* $0 < \epsilon \leq 1$, *there exists a probabilistic Monte Carlo algorithm that computes* $\mathcal{T}(F)$ *with an expected number of* $\tilde{O}(d^3 n^2 w^2 \log^2 \epsilon^{-1} [ht(M_\gamma) + ht(F)])$ *word operations and probability of error less than* ϵ.

7. CONCLUSION

This paper summarizes the results we have obtained in [13] regarding the symbolic part of our program towards a fast and reliable method to compute Puiseux series with floating point coefficients. In particular, the criterion ensuring preservation of polygon trees is essential. Along the path, we have derived improved complexity bounds for computations over finite fields. Although not optimal, these bounds are quite reasonable, i.e. quadratic in the output size, up to a factor d. Bit-complexity estimates for the Monte-Carlo version of the first step of our symbolic-numeric method confirm that the coefficient growth of pure symbolic Newton-Puiseux algorithm is avoided. Complexity bounds for the Las Vegas and deterministic version can be obtained similarly. Applying our reduction criterion for all places of $K[X]$ provides analogous bit-complexity bounds for the computation of the genus of an algebraic curve defined over an algebraic number field.

We are actively working on the numerical part of the algorithm, and in particular on error control, as well as on an improved implementation of both parts.

Acknowledgments

The authors would like to thank Mark van Hoeij for stimulating conversations and the referees for carefully proofreading the paper. We are also grateful to an anonymous referee of [12] for valuable suggestions.

8. REFERENCES

[1] E. Brieskorn and H. Knörrer. *Plane Algbebraic Curves.* Birkhaüser, 1986.

[2] C. Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*, volume 6 of *Mathematical Surveys.* AMS, 1951.

[3] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1993.

[4] B. Deconinck and M. S. Patterson. Computing the Abel Map. *preprint*, 2007.

[5] B. Deconinck and M. van Hoeij. Computing Riemann matrices of algebraic curves. *Phys. D*, 152/153:28–46, 2001.

[6] D. Duval. *Diverses questions relatives au calcul formel avec des nombres algébriques.* PhD thesis, Université de Grenoble, 1987. Thèse d'Etat.

[7] D. Duval. Rational Puiseux Expansions. *Compositio Mathematica*, 70:119–154, 1989.

[8] B. Dwork and P. Robba. On natural radii of p-adic convergence. *Trans. Amer. Math. Soc.*, 256:199–213, 1979.

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

[10] W. Fulton. Hurwitz Schemes and Irreducibility of Moduli of Algebraic Curves. *Annals of Mathematics*, 90:542–575, 1969.

[11] H. T. Kung and J. F. Traub. All algebraic functions can be computed fast. *J. ACM*, 25(2):245–260, 1978.

[12] A. Poteaux. Computing monodromy groups defined by plane algebraic curves. In *Proceedings of the 2007 International Workshop on Symbolic-numeric Computation*, pages 36–45, New-York, 2007. ACM.

[13] A. Poteaux and M. Rybowicz. Towards a Symbolic-Numeric Method to Compute Puiseux Series: The Modular Part, 2008. http://arxiv.org/abs/0803.3027.

[14] V. Shoup. *A Computational Introduction to Number Theory.* Cambridge University Press, 2005.

[15] B. M. Trager. *Integration of Algebraic Functions.* PhD thesis, Department of EECS MIT, 1984.

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

[17] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge University Press, Cambridge, 1999.

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

[19] O. Zariski. *Le problème des modules pour les branches planes.* Hermann, Paris, 1981.