



HAL
open science

Computing Riemann-Roch spaces via Puiseux expansions

Simon Abelard, Elena Berardini, Alain Couvreur, Grégoire Lecerf

► **To cite this version:**

Simon Abelard, Elena Berardini, Alain Couvreur, Grégoire Lecerf. Computing Riemann-Roch spaces via Puiseux expansions. 2021. hal-03281757v1

HAL Id: hal-03281757

<https://inria.hal.science/hal-03281757v1>

Preprint submitted on 8 Jul 2021 (v1), last revised 22 Jun 2022 (v2)

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

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

Computing Riemann–Roch spaces via Puiseux expansions*

SIMON ABELARD^{ab}, ELENA BERARDINI^{cd}, ALAIN COUVREUR^{ef}, GRÉGOIRE LECERF^{cg}

a. Thales SIX GTS France

c. Laboratoire d'informatique de l'École polytechnique (LIX)
CNRS, École polytechnique, Institut Polytechnique de Paris
Bâtiment Alan Turing, CS35003
1, rue Honoré d'Estienne d'Orves
91120 Palaiseau, France

e. Inria, France

b. Email: `sabelard@protonmail.com`

d. Email: `elena.berardini@lix.polytechnique.fr`

f. Email: `alain.couvreur@inria.fr`

g. Email: `gregoire.lecerf@lix.polytechnique.fr`

Preliminary version of July 8, 2021

Computing large Riemann–Roch spaces for plane projective curves still constitutes a major algorithmic and practical challenge. Seminal applications concern the construction of arbitrarily large algebraic geometry error correcting codes over alphabets with bounded cardinality. Nowadays such codes are increasingly involved in new areas of computer science such as cryptographic protocols and “interactive oracle proofs”. In this paper, we design a new probabilistic algorithm of Las Vegas type for computing Riemann–Roch spaces of smooth divisors, in characteristic zero, and with expected complexity exponent 2.373 (a feasible exponent for linear algebra) in terms of the input size.

KEYWORDS: Algebraic curves, Puiseux expansions, Riemann–Roch spaces, Complexity, Algorithms

1. INTRODUCTION

Let \mathbb{K} be an *effective* field and let $\bar{\mathbb{K}}$ denote an algebraic closure of \mathbb{K} . Here “effective” means that we can perform arithmetic operations and zero-tests in \mathbb{K} . The projective space of dimension 2 over $\bar{\mathbb{K}}$ is written \mathbb{P}^2 . The input projective curve C in \mathbb{P}^2 is given by its defining equation $F(x, y, z) = 0$, where $F \in \mathbb{K}[x, y, z]$ is homogeneous, absolutely irreducible, and of total degree $\delta \geq 1$.

The field $\mathbb{K}(C)$ denotes the set of rational functions of the form A/B where A and B are homogeneous polynomials of the same degree with B prime to F , and subject to the equivalence relation $A/B \sim A'/B' \iff AB' - A'B \in (F)$. For a given divisor D of C we are

*. This paper is part of a project of École polytechnique, that has received funding from the French “Agence de l’innovation de défense”. Simon Abelard was partially funded by this grant, when he was hosted at École polytechnique, Institut Polytechnique de Paris (91120 Palaiseau, France), from October 2019 to the end of December 2020.

interested in computing a basis of the Riemann–Roch space

$$\mathcal{L}(D) := \{h \in \mathbb{K}(C) \setminus \{0\} : \text{Div}(h) \geq -D\} \cup \{0\}.$$

The goal of the present paper is the design of a new efficient probabilistic algorithm of Las Vegas type to compute $\mathcal{L}(D)$ in the Brill–Noether fashion [13]. For the sake of simplicity, we focus on fields of characteristic zero. The actual restriction on the characteristic only concerns computations of Puiseux expansions, so our algorithm can be adapted to support positive characteristic whenever it is sufficiently large, namely greater than δ , or simply whenever the needed Puiseux expansions are well defined.

Riemann–Roch spaces intervene in various areas of applied algebra. For instance, they are pivotal to design efficient algebraic geometry error correcting codes, as introduced by Goppa [29, 30, 31]. These codes generalize the well known Reed–Solomon codes because they may be defined over smaller alphabets. Such codes are particularly suitable for new application areas such as “interactive oracle proofs” [8, 10], a construction itself involved in decentralized computations. In algebraic geometry, Riemann–Roch spaces intervene in arithmetic operations in Jacobians of curves [41, 45, 65].

Currently, in practice, algebraic curves used in coding theory are mostly limited to cases where Riemann–Roch spaces are explicitly known, such as Hermitian curves, Suzuki curves, or Giuletti–Korchmáros curves. For the sake of diversity it is relevant to handle more general situations which challenges our ability to efficiently compute Riemann–Roch spaces. For instance, known models of the curves introduced by Tsfasman, Vlăduț, and Zink [64] in order to construct codes asymptotically better than the Gilbert–Varshamov bound involve non-ordinary singularities [46], which are still not supported by the recent efficient algorithms of [2, 3, 49].

1.1. Brill–Noether in a nutshell

The present paper is in the vein of the seminal theory designed by Brill and Noether [13]. To the curve C is associated a so-called *adjoint divisor*, written A , related to the singularities of C ; see Section 4.2. Then D is decomposed into $D = D_+ - D_-$, where D_+ and D_- are *positive* (also called *effective*) divisors with disjoint supports; see the definition of divisors in Section 4. When $\deg D_+ < \deg D_-$, $\mathcal{L}(D)$ is $\{0\}$, so we freely assume that $\deg D_+ \geq \deg D_-$ in the rest of the paper. The Brill–Noether method mostly divides into two parts, as follows.

1. The first part consists in computing a homogeneous polynomial H that can serve as a common denominator of a basis of $\mathcal{L}(D)$. Brill and Noether showed that it is sufficient that H satisfies

$$\text{Div}(H) \geq D_+ + A. \tag{1.1}$$

Informally speaking, this means that the curve defined by $H = 0$ passes through the points of D and the singular locus of C with *ad hoc* multiplicities. Of course, for efficiency purposes, it is of practical interest to take H of degree as small as possible. In fact Condition (1.1) can be expressed in terms of a homogeneous linear system: the unknowns are the coefficients of H and the number of equations depends on $\deg D_+$ and $\deg A$. As soon as the number of unknowns is strictly larger than the number of equations, the system admits a non-zero solution. This is a standard way to determine a candidate for H .

2. Let $d := \deg H$ and let $l(D)$ denote the dimension of $\mathcal{L}(D)$. The second part of the Brill–Noether method consists in computing polynomials $G_1, \dots, G_{l(D)}$ of degree d such that $\{G_i/H\}_{i=1, \dots, l(D)}$ is a basis of $\mathcal{L}(D)$. These polynomials can be obtained as a basis of homogeneous polynomials G of degree d , “defined modulo F ”, that satisfy

$$\operatorname{Div}(G) \geq \operatorname{Div}(H) - D.$$

This condition can again be expressed in terms of a homogeneous linear system of equations in the coefficients of G , once $\operatorname{Div}(H)$ has been computed.

1.2. Computational model

For complexity analyses, we use an algebraic model over a general field \mathbb{K} (typically computation trees [14]), so we count the number of arithmetic operations and zero-tests performed by the algorithms. In order to simplify the presentation of complexity bounds, we use the established *soft-Oh* notation [28, Chapter 25, Section 7]: $f(n) = \tilde{O}(g(n))$ means that $f(n) = g(n) \log_2^{O(1)}(|g(n)| + 3)$. A function $f(n)$ is *softly linear* when $f(n) = \tilde{O}(n)$.

The vector space of polynomials of degree $< n$ in $\mathbb{K}[x]$ will be written $\mathbb{K}[x]_{<n}$. For polynomial arithmetic, we content ourselves with softly linear cost bounds for products, divisions, greatest common divisors, and products of several polynomials. We will freely use the known results presented in the textbook [28].

The constant ω will denote a real value between 2 and 3 such that two $n \times n$ matrices over a commutative ring can be multiplied with $O(n^\omega)$ ring operations. The current best known bound is $\omega < 2.37286$ [6]. The constant ϖ is another real value between 1.5 and $(\omega + 1)/2$ such that the product of a $n \times \sqrt{n}$ matrix by a $\sqrt{n} \times \sqrt{n}$ matrix takes $O(n^\varpi)$ operations. The current best known bound is $\varpi < 1.667$ [42, Theorem 10.1].

1.3. Related work

Adjoint curves. The notion of adjoint for plane curves was introduced by Brill and Noether [13] in 1874 for ordinary curves: they defined a curve to be adjoint to another curve \mathcal{C} if it passes with multiplicity at least $m - 1$ through any singular point of \mathcal{C} of multiplicity m . Since then, different notions of adjoint have been proposed.

In [32], Gorenstein presented an adjoint condition related to the conductor ideal of the curve. One century after the work of Brill and Noether, Keller proposed a notion of adjoint in terms of the “divisor of double points” of the curve; see [44] and [33, Definitions 2.12 and 2.13]. More recently in [7, Appendix A, Section 2] and then in [27], the adjoint condition has been defined in relation to the divisor of a differential form on the curve. The same definition is used by Campillo and Farrán [16, 17]. All these notions are proven to be equivalent when dealing with curves having only ordinary singularities: see [33, Corollary 4.16] and [26, Chapter 8, Section 5, Proposition 8]. In the case of non-ordinary singularities, Greco and Valabrega proved in [33, Theorem 4.6] that Gorenstein's and Keller's adjoint conditions are equivalent, and in [33, Theorem 4.13] that the Brill–Noether one is actually more restrictive. Following [27], one can also deduce the equivalence of the adjoint condition in terms of a differential form with Gorenstein's (and thus with Keller's) one.

The adjoint conditions listed above represent the mainstream in the literature. For the sake of completeness, we mention yet other definitions. In [5], Abhyankar and Sathaye proposed an adjoint notion depending on infinitely near singular points on the curve, while in [34] one can find another construction in terms of virtual multiplicities. Papers have been devoted to investigate these different definitions of adjoint and their relationships: we refer the reader to the work of Greco and Valabrega [33, 34], and also to [19] for a computational approach.

Algorithms. As said, the seminal Brill–Noether approach [13] to compute Riemann–Roch spaces was originally restricted to ordinary curves, and later extended to arbitrary plane curves by Le Brigand and Risler [48]. Although formulated in a slightly different manner Le Brigand and Risler revisited Keller's point of view for the adjoint conditions. In [35, 36, 37], Haché designed an algorithm along with a software implementation from [48]. Other algorithms in the vein of the Brill–Noether approach have been proposed by Huang and Ierardi [41] still for ordinary curves, and by Campillo and Farrán [16, 17] in combination with the theory of Hamburger–Noether expansions. An implementation of a Brill–Noether variant for general curves is available within the SINGULAR [61] computer algebra system.

More recently, fast algorithms have been designed for nodal curves [2, 49], leading to a complexity exponent as small as $(\omega + 1)/2$. Then, ordinary curves have been handled in [3] with the same complexity exponent. Comparisons between algorithms for ordinary curves can be found in [3].

In order to address general curves, one can also appeal to an alternate family of algorithms, often called “arithmetic”, that is different from the Brill–Noether approach. The state-of-the-art algorithm of this family is due to Hess [38] and is implemented both in the MAGMA [11] and SINGULAR [60] computer algebra systems.

1.4. Our contributions

In order to design fast algorithms from the Brill–Noether theory, one central problem is the definition and the efficient computation of the adjoint divisor A of the curve C .

Our first contribution is a new simple rewriting of the adjoint A of C in terms of the rational Puiseux expansions $(X_i(t), Y_i(t))$ centered at the singular points of C ; see Definitions 3.3 and 3.8. This condition is derived from the one based on differential forms [7, 27]. In this way, the adjoint condition $\text{Div}(H) \geq A$ for a homogeneous polynomial H is equivalent to the fact that the values of H at all the expansions $(X_i(t), Y_i(t))$ have sufficiently large valuations; see Section 4.2.

Our second contribution is an elementary proof of the following well known proposition via the Lagrange interpolation. Let P be a point of C and consider two homogeneous polynomials A and B that are prime to F : if $\text{Div}_P(B) \geq \text{Div}_P(A) + A_P$ then Noether's condition is satisfied by the triple (F, A, B) at P ; see Section 4.3. The Max Noether theorem and this proposition are the cornerstone of the *residue theorem* that summarizes the correctness of the Brill–Noether method; see Theorem 5.1. In other words, our approach avoids desingularizing C explicitly, nor determining sequences of conductor ideals. The practical interest is to benefit from fast algorithms recently developed for Puiseux expansions of algebraic germs of curves.

Once the Puiseux expansions of C have been computed at all the singular points with suitable orders, our third contribution is the reformulation of the linear systems for the above H and G_i in terms of structured linear algebra. On the one hand, we propose a relatively sharp bound for $\deg H$ that allows simplifications in the subsequent computation of $\text{Div}(H)$; see Section 5. On the other hand, we show that a “compressed representation” of the G_i is possible in terms of a basis of a $\mathbb{K}[x]$ -module; this is defined in Section 8.4.

In order to prove our main Theorem 8.8, we design a new probabilistic algorithm of Las Vegas type for computing Riemann–Roch spaces of smooth divisors, in characteristic zero, and with expected complexity exponent ω in terms of the input size. This algorithm makes use and extends ideas introduced in [3]. Its bottleneck relies in structured linear system solving, for which known algorithms are not as efficient as in the case of ordinary curves.

As a technical ingredient, we revisit the computation of the Puiseux expansions of C at all its singular points, truncated at suitable precisions, by means of the panoramic evaluation paradigm, that we adapt to randomized algorithms in Section 2.4. We rely on the complexity bound presented in [59, Theorem 1] for the singular parts of the Puiseux expansions of polynomials in $\mathbb{K}[[x]][y]$. Overall, Section 3.8 contains a streamlined alternative proof of [59, Theorem 2] in terms of total degrees. Further new technical ingredients also concern smooth divisors, for which we develop algorithms for their power series expansion representation in Section 4. Smooth and non-smooth divisors are finally represented by a unified data structure in the present paper.

For the sake of comparison, let us mention that the complexities of the algorithms implemented by Haché [35, 36, 37] have not been analyzed into details, to our best knowledge. Hess' algorithm achieves a polynomial complexity bound for general curves but the exact complexity exponent does not seem to have been analyzed so far, again to our best knowledge. At least, we know from [1] that the needed integral closures can be computed in softly quadratic time in terms of δ^2 (the dense size of the representation of F).

2. PRELIMINARIES

This section is mostly devoted to notations and well known algorithms in computer algebra. We also revisit the panoramic evaluation paradigm of [40] for randomized algorithms, that will be needed for computing Puiseux expansions in Section 3 and the adjoint divisor in Section 4.2. In this section, \mathbb{K} can have any characteristic.

2.1. Zariski closed sets

The projective space of dimension n over $\bar{\mathbb{K}}$ is denoted by \mathbb{P}^n . For a subset S of homogeneous polynomials in $\mathbb{K}[x_0, \dots, x_n]$, we write $\mathcal{U}_{\mathbb{P}}(S)$ for the Zariski closed set in the projective space \mathbb{P}^n defined as the common zeros of the elements of S , that is

$$\mathcal{U}_{\mathbb{P}}(S) := \{P \in \mathbb{P}^n : F(P) = 0, \forall F \in S\}.$$

The affine space of dimension n over $\bar{\mathbb{K}}$ is denoted by \mathbb{A}^n . For a set S of polynomials in $\mathbb{K}[x_1, \dots, x_n]$, we write $\mathcal{U}_{\mathbb{A}}(S)$ for the Zariski closed set in the affine space \mathbb{A}^n defined as the common zeros of the elements in S , that is

$$\mathcal{U}_{\mathbb{A}}(S) := \{P \in \mathbb{A}^n : f(P) = 0, \forall f \in S\}.$$

If $\mathbb{M} := \mathbb{K}[x_1, \dots, x_n]$ is a polynomial ring and P a point in \mathbb{A}^n , then \mathbb{M}_P will represent the local ring of the rational functions A/B in $\mathbb{K}(x_1, \dots, x_n)$ such that $B(P) \neq 0$.

2.2. Algorithms for polynomials

We first recall that a linear change of variables in a homogeneous polynomial takes softly linear time. If M is a 3×3 matrix over \mathbb{K} , then $F \circ M$ stands for the right composition of F with the linear map

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto M \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

LEMMA 2.1. [3, Lemma 2.5] *Let $F \in \mathbb{K}[x, y, z]$ be a homogeneous polynomial of degree δ and let M be a 3×3 matrix over \mathbb{K} . Then, $F \circ M$ can be computed with $\tilde{O}(\delta^2)$ operations in \mathbb{K} .*

Then, we recall a complexity result for modular composition, that will be used to evaluate rational functions at divisors. At present time no algorithm with softly linear cost is known for bivariate modular composition over a general field \mathbb{K} . We will content ourselves with the following statement.

LEMMA 2.2. *Let $f \in \mathbb{K}[x, y]$ be of total degree δ , let $\chi \in \mathbb{K}[t]$ and let $u, v \in \mathbb{K}[t]_{<\deg \chi}$ be such that $\lambda_x u(t) + \lambda_y v(t) = t \pmod{\chi(t)}$ holds for some $(\lambda_x, \lambda_y) \in \mathbb{K}^2$. Then $f(u(t), v(t)) \pmod{\chi(t)}$ can be computed with*

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg \chi\right)$$

operations in \mathbb{K} .

Proof. Up to permuting x and y , we may assume that $\lambda_y \neq 0$. We compute

$$g(x, t) := f(x, (t - \lambda_x x) / \lambda_y)$$

with $\tilde{O}(\delta^2)$ operations in \mathbb{K} via Lemma 2.1. Then we obtain $g(u(t), t) \pmod{\chi(t)}$ by means of [2, Lemma 2.1], that is a variant of an algorithm designed in [55]. \square

We also recall two well known propositions for multi-remaindering and Chinese remaindering [28, Chapter 10, Section 3].

PROPOSITION 2.3. *Let χ_1, \dots, χ_s be polynomials in $\mathbb{K}[x]$, and let $d := \deg \chi_1 + \dots + \deg \chi_s$. Given $f \in \mathbb{K}[x]$, the remainders $f \pmod{\chi_i}$ for $i = 1, \dots, s$ can be computed with $\tilde{O}(d + \deg f)$ operations in \mathbb{K} .*

PROPOSITION 2.4. *Let χ_1, \dots, χ_s be pairwise coprime polynomials in $\mathbb{K}[x]$, and let $d := \deg \chi_1 + \dots + \deg \chi_s$. Given $r_1, \dots, r_s \in \mathbb{K}[x]$ such that $\deg r_i < \deg \chi_i$, the unique polynomial $f \in \mathbb{K}[x]_{<d}$ satisfying $f \pmod{\chi_i} = r_i$ for $i = 1, \dots, s$ can be computed with $\tilde{O}(d)$ operations in \mathbb{K} .*

The last useful sub-algorithm concerns the computation of Taylor expansions of polynomials at algebraic numbers. Precisely, given a separable polynomial $\theta \in \mathbb{K}[s]$ and a positive integer m , we consider the map

$$\begin{aligned} \Gamma_{\theta, m}: \quad \mathbb{K}[s] / (\theta^m(s)) &\cong (\mathbb{K}[t] / (\theta(t)))[[S-t]] / (S-t)^m \\ s &\mapsto S. \end{aligned}$$

PROPOSITION 2.5. [39, simplified from Section 4.2] $\Gamma_{\theta, m}$ is an isomorphism. Both directions of $\Gamma_{\theta, m}$ can be computed in softly linear time, namely $\tilde{O}(m \deg \theta)$ operations in \mathbb{K} .

2.3. Panoramic evaluation

Panoramic evaluation necessitates a precise computational model in order to be presented accurately. We will use computation trees, and refer the reader to [14, Chapter 4, Section 4] or [40, Section 2.1] for the usual definitions. Informally speaking, a *computation tree* is a tree whose nodes represent input values, output values, arithmetic operations, or zero-tests that create branches.

We will consider computation trees that manipulate data in \mathbb{K} -algebras over an effective field \mathbb{K} , and only the following operations will be allowed:

- The binary arithmetic operations $+$, $-$, \times in the algebra.
- The unary operation of inversion, which is partially defined in the algebra.
- The unary zero-test.
- For each constant $c \in \mathbb{K}$, the nullary constant function $() \mapsto c$ and the unary function $x \mapsto cx$ of scalar multiplication by c .

The evaluation of a computation tree T with n inputs a in \mathbb{K} corresponds to the natural execution of the sequence of instructions over a path of the tree from the root to a leaf. The value in return is written $\mathcal{E}(T;a)$. The execution fails before reaching an output node in a leaf whenever the inverse of the zero element of \mathbb{K} occurs. In this case, we say that T is not *executable* at this input and the returned value is written not-executable.

Let \mathbb{A} be a \mathbb{K} -algebra. Given an input sequence a in \mathbb{A}^n , the *unpermissive evaluation* of T at a performs the usual evaluation as if \mathbb{A} were a field but it stops as soon as a non-trivial zero-divisor is discovered in the argument of a zero-test or an inversion; see [40, Section 3.2]. When a non-trivial zero-divisor is discovered, the returned value, written $\bar{\mathcal{E}}(T;a)$, is inconsistent and the zero-divisor is stored for subsequent use. Otherwise, $\bar{\mathcal{E}}(T;a)$ is $\mathcal{E}(T;a)$.

We say that a decomposition

$$\mathbb{A} \cong \mathbb{D}_1 \oplus \cdots \oplus \mathbb{D}_\ell$$

is a *panoramic splitting* of \mathbb{A} for the pair (T, a) if $\bar{\mathcal{E}}(T; \pi_{\mathbb{A} \rightarrow \mathbb{D}_i}(a)) \neq \text{inconsistent}$ for $i = 1, \dots, \ell$, where $\pi_{\mathbb{A} \rightarrow \mathbb{D}_i}$ stands for the projection from \mathbb{A} onto \mathbb{D}_i . A *panoramic value* of T at a is a set of pairs $\{(\mathbb{D}_1, b_1), \dots, (\mathbb{D}_\ell, b_\ell)\}$ such that $\mathbb{D}_1 \oplus \cdots \oplus \mathbb{D}_\ell$ is a panoramic splitting of \mathbb{A} and $b_i := \bar{\mathcal{E}}(T; \pi_{\mathbb{A} \rightarrow \mathbb{D}_i}(a))$ for $i = 1, \dots, \ell$; see the definition in [40, Section 3.3].

THEOREM 2.6. [40, Simplified from Theorem 1] *Let $\mathbb{A} = \mathbb{K}[x]/(\mu(x))$ be a separable extension of \mathbb{K} of degree $d := \deg \mu \geq 1$, and let T be a computation tree over \mathbb{K} -algebras, made of n inputs, $\leq m$ outputs, and of total cost $\leq \tau$. Then, computing a panoramic value of T over \mathbb{A} costs*

$$\tilde{O}((n + m + \tau) d)$$

operations in \mathbb{K} .

Panoramic evaluation can be implemented easily. In fact, we begin with running the unpermissive evaluation on the input data. If inconsistent is not returned then we are done. Otherwise a non-trivial zero-divisor v has been found and leads to a decomposition of \mathbb{A} into two sub-algebras \mathbb{A}_1 and \mathbb{A}_2 such that $\pi_{\mathbb{A} \rightarrow \mathbb{A}_1}(v)$ is zero and $\pi_{\mathbb{A} \rightarrow \mathbb{A}_2}(v)$ is invertible. Then, it suffices to restart the panoramic evaluation recursively and independently over \mathbb{A}_1 and \mathbb{A}_2 . This process ends with a correct panoramic value since \mathbb{A} is a finite product of fields.

The straightforward method described in the previous paragraph turns out to be sub-optimal. In fact, a special care is needed to avoid repeating calculations. The paradigm behind Theorem 2.6 is called *directed evaluation*, defined in [40, Section 3.5]. Roughly speaking, the directed evaluation performs the natural evaluation until a non-trivial zero-divisor v of \mathbb{A} is encountered as an argument of a zero-test or an inversion. When this happens, the current algebra \mathbb{A} is decomposed into two proper sub-algebras $\mathbb{A}_1 \oplus \mathbb{A}_2$ such that $\pi_{\mathbb{A} \rightarrow \mathbb{A}_1}(v)$ is zero and $\pi_{\mathbb{A} \rightarrow \mathbb{A}_2}(v)$ is invertible. This decomposition is stored and the directed evaluation is carried on over the one of \mathbb{A}_1 and \mathbb{A}_2 whose dimension is the largest (an arbitrary choice is made when the dimensions are equal). At the end of a directed evaluation, the returned value is obtained for the final current sub-algebra. Finally, a fast panoramic evaluation process first performs a directed evaluation, and then is recursively called over each resulting remaining sub-algebras.

2.4. Panoramic evaluation for randomized algorithms

Theorem 2.6 does not support randomized algorithms, that will intervene in this paper. In the next paragraphs we propose a way to handle randomization under mild assumptions.

Let ϵ be a fixed positive real value $\leq 1/2$. We consider a family of computation trees $(T_b)_{b \in \mathcal{B}}$ over \mathbb{K} -algebras, parametrized by a finite set \mathcal{B} . All the trees of the family have input size n , output size $\leq m$, and total cost $\leq \tau$. We endow \mathcal{B} with a uniform probability law.

Let \mathbb{L} denote an algebraic field extension of \mathbb{K} . For a given input in \mathbb{L}^n , we assume that a tree T_b of the family either evaluates to a correct result or returns wrong-random-choice with probability $\leq \epsilon$ for b taken at random in \mathcal{B} . Such a family of trees can be regarded as all the possible executions of a randomized algorithm.

For $k \geq 1$ and (b_1, \dots, b_k) in \mathcal{B}^k , we build the computation tree T_{b_1, \dots, b_k} that performs the successive evaluations of T_{b_1}, \dots, T_{b_k} at the given input while wrong-random-choice is encountered. Precisely, if $k = 1$ this tree is exactly T_{b_1} . If $k \geq 2$ then the evaluation of T_{b_1, \dots, b_k} performs first the evaluation of $T_{b_1, \dots, b_{k-1}}$ and returns the output value if it is not wrong-random-choice. Otherwise T_{b_k} is evaluated and its resulting value is returned. The probability that wrong-random-choice is returned after the evaluation of T_{b_1, \dots, b_k} is thus $\leq \epsilon^k$. The expected value of k that yields a correct result is

$$\leq \sum_{\kappa \geq 1} \kappa \epsilon^{\kappa-1} = \frac{1}{(1-\epsilon)^2}. \quad (2.1)$$

In other words, we can compute a correct result for a given input with an expected number of $O(\tau / (1-\epsilon)^2)$ operations in \mathbb{L} .

Now, let us consider l different input sets, with entries in different algebraic field extensions of \mathbb{K} . For (b_1, \dots, b_k) taken at random in \mathcal{B}^k , the probability that T_{b_1, \dots, b_k} does not end with wrong-random-choice for each of these l input sets is $\geq (1-\epsilon^k)^l$.

We revisit the proof of [40, Theorem 1] for \mathbb{K} -algebras of the form $\mathbb{A} = \mathbb{K}[x] / (\mu(x))$, where μ is separable; see [40, Section 4]. Let μ_1, \dots, μ_l represent the irreducible factors of μ , so \mathbb{A} writes as the product of fields

$$\mathbb{A} \cong \prod_{i=1}^l \mathbb{L}_i, \text{ where } \mathbb{L}_i := \mathbb{K}[x] / (\mu_i(x)).$$

An input of a computation tree T_{b_1, \dots, b_k} in \mathbb{A}^n in the unpermissive evaluation model can be regarded as a l -tuple of inputs in $\prod_{i=1}^l \mathbb{L}_i^n$ under the following assumption:

Hypothesis (H). For any input a in \mathbb{A}^n , and any $b \in \mathcal{B}$, if the evaluation of T_b at $\pi_{\mathbb{A} \rightarrow \mathbb{L}_i}(a)$ does not yield wrong-random-choice for all $i = 1, \dots, l$, then the unpermissive evaluation of T_b at a does not yield wrong-random-choice.

THEOREM 2.7. *Let $\mathbb{A} = \mathbb{K}[x] / (\mu(x))$ be a separable extension of \mathbb{K} of degree $d := \deg \mu \geq 1$, and let $(T_b)_{b \in \mathcal{B}}$ be a family of computation trees over \mathbb{K} -algebras made of n inputs, $\leq m$ outputs, of total cost $\leq \tau$, and satisfying Hypothesis (H). Then, a panoramic value of $(T_b)_{b \in \mathcal{B}}$ over \mathbb{A} can be computed with an expected number of $\tilde{O}((n + m + \tau)d)$ operations in \mathbb{K} .*

Proof. Thanks to Hypothesis (H), and according to the above discussion, T_{b_1, \dots, b_k} does not yield wrong-random-choice in the directed evaluation model over \mathbb{A} with probability $\geq (1 - \epsilon^k)^l$. While a directed evaluation yields a wrong-random-choice, we try another point (b_1, \dots, b_k) at random in \mathcal{B}^k . From (2.1), the expected number of trials is

$$\leq \frac{1}{(1 - \epsilon^k)^{2l}}.$$

We want this expected number of trials to be uniformly bounded by a constant $c > 1$, that is:

$$\frac{1}{(1 - \epsilon^k)^{2l}} \leq c.$$

Since $\epsilon \leq 1/2$, this condition is satisfied as soon as

$$l \epsilon^k \leq \log c.$$

Consequently, it suffices to take

$$k := \left\lceil \log \left(\frac{\log c}{l} \right) / \log \epsilon \right\rceil = O(\log l) = O(\log d).$$

By using this randomized directed evaluation in the proof of [40, Theorem 1], we obtain that the panoramic evaluation of $(T_b)_{b \in \mathcal{B}}$ in \mathbb{A} can be performed with an expected number of $\tilde{O}((n + m + \tau)d)$ operations in \mathbb{K} . \square

3. PUISEUX EXPANSIONS

This section gathers known facts and complexity results about Puiseux series. From now on and until the end of the paper, \mathbb{K} is assumed to have characteristic zero. For complexity results, we rely on recent papers by Poteaux and his collaborators [57, 58, 59], in which further details and historical references can be found. We recall that $\mathbb{K}[[x]]$ represents the ring of the power series in x . Its field of fractions, called the field of Laurent series, is written $\mathbb{K}((x))$.

Let $F \in \mathbb{K}((x))[y]$ be a monic separable polynomial of degree d_y in y . We write

$$F_y := \frac{\partial F}{\partial y}, \quad \text{Disc}_y F := (-1)^{d_y(d_y-1)/2} \text{Res}_y(F, F_y) \in \mathbb{K}((x)).$$

It is well known that F admits d_y distinct roots in the field of Puiseux series

$$\bar{\mathbb{K}}\langle\langle x \rangle\rangle := \bigcup_{e \geq 1} \bar{\mathbb{K}}\langle\langle x^{1/e} \rangle\rangle,$$

that are called its *Puiseux expansions*. From the seminal works of Newton and Puiseux, the field $\bar{\mathbb{K}}\langle\langle x \rangle\rangle$ is known to be algebraically closed. If F is monic in $\mathbb{K}[[x]][y]$, then its Puiseux expansions have nonnegative valuation in x .

3.1. Absolute factorization

Let $F \in \mathbb{K}\langle\langle x \rangle\rangle[y]$ be a monic *irreducible* polynomial of degree d_y in y . The *absolute factorization* of F means its factorization in $\bar{\mathbb{K}}\langle\langle x \rangle\rangle[y]$. Let $\mathfrak{F}_1, \dots, \mathfrak{F}_s$ denote the monic absolutely irreducible factors of F .

LEMMA 3.1. *With the above notation, for $i = 1, \dots, s$ the field \mathbb{E}_i generated by the coefficients of \mathfrak{F}_i over \mathbb{K} has degree d_y/s over \mathbb{K} . The fields $\mathbb{E}_1, \dots, \mathbb{E}_s$ are conjugated over \mathbb{K} .*

Proof. Let \mathbb{E}_1 be represented by $\mathbb{K}[a]/(\mu(a))$ with μ monic and irreducible. Let $\alpha_1 \in \bar{\mathbb{K}}$ be a root of μ such that $\mathbb{E}_1 = \mathbb{K}[\alpha_1]$; this defines an embedding of \mathbb{E}_1 into $\bar{\mathbb{K}}$. Then \mathfrak{F}_1 uniquely writes as $F(\alpha_1, x, y)$, where

$$F(\alpha, x, y) \in \mathbb{K}[a]\langle\langle x \rangle\rangle[y]$$

and such that F is monic in y and $\deg_a F < \deg \mu$. Let $\alpha_2, \dots, \alpha_{\deg \mu}$ denote the other roots of μ in $\bar{\mathbb{K}}$. Since \mathbb{E}_1 is generated over \mathbb{K} by the coefficients of \mathfrak{F}_1 , the $F(\alpha_i, x, y)$ are pairwise distinct irreducible factors of F in $\bar{\mathbb{K}}\langle\langle x \rangle\rangle[y]$. From

$$F(\alpha_1, x, y) \cdots F(\alpha_{\deg \mu}, x, y) = \text{Res}_a(\mu(a), F(a, x, y)) \in \mathbb{K}\langle\langle x \rangle\rangle[y]$$

and since F is irreducible, we have $F = \text{Res}_a(\mu(a), F(a, x, y))$, that implies

$$\{\mathfrak{F}_1, \dots, \mathfrak{F}_s\} = \{F(\alpha, x, y) : \mu(\alpha) = 0\},$$

whence $\deg_y \mathfrak{F}_i = d_y/s$ and $\deg \mu = s$. Finally, the \mathbb{E}_i are the different embeddings of $\mathbb{K}[a]/(\mu(a))$ into $\bar{\mathbb{K}}$. \square

In this paper, we prefer to avoid irreducible factorization of polynomials, because it cannot be computed in an algebraic complexity model for a general ground field [24, 25]. Of course, factorization is possible whenever \mathbb{K} is finitely and explicitly presented over \mathbb{Q} , but the bit costs are rather expensive in the worst cases. On the other hand it is usual that a set of absolutely irreducible factors $\mathfrak{F}_1, \dots, \mathfrak{F}_s$ in $\bar{\mathbb{K}}\langle\langle x \rangle\rangle[y]$ monic in y , of the same degree, and stable by conjugation over \mathbb{K} , can be represented by a pair (μ, F) such that:

- $\mu \in \mathbb{K}[a]$ is monic and separable of degree s ,
- $F(a, x, y) \in \mathbb{K}[a]\langle\langle x \rangle\rangle[y]$ is monic in y and satisfies $\deg_a F < \deg \mu$,
- $\{\mathfrak{F}_1, \dots, \mathfrak{F}_s\} = \{F(\alpha, x, y) : \mu(\alpha) = 0\}$.

With such a representation, μ is not required to be irreducible, while the $F(\alpha, x, y)$ are irreducible in $\bar{\mathbb{K}}\langle\langle x \rangle\rangle[y]$ for each root α of μ . This point of view is classical in the context of absolute factorization in $\mathbb{K}[x, y]$; see [20] for instance. In a similar fashion, we will parametrize families of Puiseux expansions in terms of roots of separable polynomials.

3.2. Rational Puiseux expansions

Let F denote an absolutely irreducible polynomial in $\mathbb{E}((x))[y]$ of degree d_y , where \mathbb{E} is the field generated by the coefficients of F over \mathbb{K} . Let $\varphi_1, \dots, \varphi_{d_y}$ denote the Puiseux expansions of F , so

$$F = \prod_{i=1}^{d_y} (y - \varphi_i).$$

Up to a permutation of indices, we may assume that φ_1 belongs to $\bar{\mathbb{K}}((x^{1/e}))$ with e taken minimal among the φ_i . In particular φ_1 writes as

$$\varphi_1 = \sum_{i=n}^{\infty} \beta_i x^{i/e},$$

with $\beta_n \neq 0$ (where $n \in \mathbb{Z}$) and there exists an integer m prime to e such that $\beta_m \neq 0$. Let ζ denote an e -th root of unity. From

$$F\left(x^{1/e}, \sum_{i=n}^{\infty} \beta_i (x^{1/e})^i\right) = 0$$

we observe that

$$F\left(\zeta x^{1/e}, \sum_{i=n}^{\infty} \beta_i (\zeta x^{1/e})^i\right) = 0,$$

which implies that

$$\psi_\zeta := \sum_{i=n}^{\infty} \beta_i (\zeta x^{1/e})^i$$

is also a root of F . Now, if ζ is a primitive e -th root of unity then $\psi_{\zeta^0} = \varphi_1, \dots, \psi_{\zeta^{e-1}}$ are also roots of F . If $0 \leq a < b < e$ then

$$\beta_m (\zeta^a x^{1/e})^m \neq \beta_m (\zeta^b x^{1/e})^m$$

because m is prime to e . It follows that $\psi_{\zeta^0}, \dots, \psi_{\zeta^{e-1}}$ are pairwise distinct. Let

$$G(x^{1/e}, y) := \prod_{k=0}^{e-1} (y - \psi_{\zeta^k}) \in \bar{\mathbb{K}}((x^{1/e}))[y].$$

By construction, we have $G(\zeta x^{1/e}, y) = G(x^{1/e}, y)$, whence $G(x^{1/e}, y) \in \bar{\mathbb{K}}((x))[y]$. Consequently G divides F , whence $G = F$. These observations are strengthened in the following statement that makes precise the algebraic extension in which the coefficients of the Puiseux expansions of F actually belong to.

THEOREM 3.2. [22, 23] *Let F be an absolutely irreducible polynomial in $\mathbb{E}((x))[y]$ of degree $d_y = e$. Then, there exists $\gamma \in \mathbb{E} \setminus \{0\}$ and $\sum_{i=n}^{\infty} \beta_i t^i \in \mathbb{E}((t))$ such that*

$$F = \prod_{k=0}^{e-1} \left(y - \sum_{i=n}^{\infty} \beta_i (\zeta^k (x/\gamma)^{1/e})^i \right),$$

where ζ stands for a primitive e -th root of unity.

Proof. These expansions appeared in [23, Section 1, p. 124], and their existence proof follows from a variant of the Newton polygon method [23, Section 4.4]. \square

This motivates the following definition, still extracted from [22, 23].

DEFINITION 3.3. Let $F \in \bar{\mathbb{K}}((x))[y]$ be an irreducible polynomial of degree e . Let \mathbb{E} represent the field generated by the coefficients of F over \mathbb{K} . A rational Puiseux expansion of F over \mathbb{K} is a pair $(X(t), Y(t)) \in \mathbb{E}((t))^2$, such that the following properties hold:

- $(X(t), Y(t)) = (\gamma t^e, \sum_{i=n}^{\infty} \beta_i t^i)$, with $n \in \mathbb{Z}$ and $\gamma \beta_n \neq 0$,
- $F(X(t), Y(t)) = 0$.

A rational Puiseux expansion represents the e following Puiseux series in $\bar{\mathbb{K}}((x^{1/e}))$, for $k=0, \dots, e-1$:

$$\varphi_k(x) := \sum_{i=n}^{\infty} \beta_i (\zeta^k (x/\gamma)^{1/e})^i,$$

where ζ is a primitive e -th root of unity. The common minimal polynomial over $\mathbb{E}((x))[y]$ of these series is

$$F = \prod_{k=0}^{e-1} (y - \varphi_k(x)).$$

It follows from the above discussion that no Puiseux expansion of F belongs to $\bar{\mathbb{K}}((x^{1/e'})$ with $e' < e$. The integer e is called the *ramification index* of the Puiseux expansions of F . More generally, a rational Puiseux expansion of a non necessarily absolutely irreducible polynomial $F \in \mathbb{K}((x))[y]$ will mean a rational Puiseux expansion of one of its absolutely irreducible factors.

3.3. Uniformizing parameters

Let F denote a monic irreducible polynomial in $\bar{\mathbb{K}}[[x]][y]$ of degree e , so

$$\bar{\mathbb{K}}[[x]][y]/(F(x, y))$$

is an integral domain, whose field of fractions is $\bar{\mathbb{K}}((x))[y]/(F(x, y))$. The rational Puiseux expansion of F over \mathbb{K} is written $(X(t), Y(t))$, as in Definition 3.3. The next proposition is well known and is often deduced from algorithms that compute Puiseux expansions. For completeness we include a standalone proof.

PROPOSITION 3.4. Let F denote a monic irreducible polynomial in $\bar{\mathbb{K}}[[x]][y]$. Then, $\bar{\mathbb{K}}((x))[y]/(F(x, y))$ is endowed with the unique discrete valuation that extends the valuation in x via the following isomorphism:

$$\begin{aligned} \Phi: \bar{\mathbb{K}}((x))[y]/(F(x, y)) &\cong \bar{\mathbb{K}}((t)) \\ x &\mapsto X(t) = \gamma t^e \\ y &\mapsto Y(t). \end{aligned}$$

Proof. The map Φ is injective because F is the minimal polynomial of $Y((x/\gamma)^{1/e})$ over $\bar{\mathbb{K}}((x))$, as seen in Section 3.2. Let us write $Y(t) = \sum_{i \geq 0} \beta_i t^i$ as before, and consider the morphism of $\bar{\mathbb{K}}((x))$ -algebras

$$\begin{aligned} \Psi: \bar{\mathbb{K}}((x))[y] &\longrightarrow \bar{\mathbb{K}}((x))[t]/(t^e - x/\gamma) \\ y &\longmapsto Y(t) = \sum_{k=0}^{e-1} \left(\sum_{i \geq 0} \beta_{ie+k} (x/\gamma)^i \right) t^k. \end{aligned}$$

The polynomial F is in $\ker \Psi$. Since F and $t^e - x/\gamma$ are irreducible over $\bar{\mathbb{K}}((x))$ and of the same degree e , the map

$$\begin{aligned} \bar{\Psi}: \bar{\mathbb{K}}((x))[y]/(F(x,y)) &\longrightarrow \bar{\mathbb{K}}((x))[t]/(t^e - x/\gamma) \\ y &\longmapsto Y(t). \end{aligned}$$

is an isomorphism. Finally we note that $\Phi(\bar{\Psi}^{-1}(t)) = t$, so Φ is surjective. \square

3.4. Singular parts

The computation of Puiseux series is usually presented in two steps. The first one concerns the expansions at the minimal precision that separates them; this is the purpose of the next definition. The second step mostly corresponds to the usual Newton operator that extends expansions to any requested finite precision.

DEFINITION 3.5. *The regularity index of a Puiseux expansion φ of F is the first rational number ρ such that no other Puiseux series of F has the same truncation up to degree ρ . The truncation of φ up to its regularity index is called the singular part of φ . By convention, if $\deg_y F = 1$ then the regularity index is set to $-\infty$.*

Remark 3.6. In [59, Definition 3] the regularity index is the quantity $e\rho$, where e is the ramification index of φ .

Since the Puiseux expansions represented by one rational Puiseux expansion share the same regularity index, the notions of regularity index and singular part naturally extend to rational Puiseux expansions.

LEMMA 3.7. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d_y in y , and let ψ be a Puiseux series that extends the singular part of a Puiseux expansion φ of F of ramification index e and regularity index ρ in F (namely $\text{val}_x(\psi - \varphi) > \rho$). Then, the following properties hold:*

1. $\text{val}_x(F_y(\psi)) = \text{val}_x(F_y(\varphi))$,
2. $\rho \leq \text{val}_x(F_y(\varphi))$,
3. $\text{val}_x(F(\psi)) \geq \rho + 1/e + \text{val}_x(F_y(\varphi))$.

Proof. Let $\varphi_1 = \varphi, \varphi_2, \dots, \varphi_{d_y}$ denote the Puiseux expansions of F . By definition of the regularity index, we have $\text{val}_x(\psi - \varphi_i) = \text{val}_x(\varphi - \varphi_i)$ for $i = 2, \dots, d_y$. It follows that

$$\text{val}_x(F_y(\psi)) = \text{val}_x\left(\prod_{i=2}^{d_y} (\psi - \varphi_i)\right) = \text{val}_x\left(\prod_{i=2}^{d_y} (\varphi - \varphi_i)\right) = \text{val}_x(F_y(\varphi)).$$

The two other properties are immediate. \square

3.5. Representation of rational Puiseux expansions

For algorithmic purposes and for avoiding irreducible polynomial factorization, we need to revisit Definition 3.3 in order to allow rational Puiseux expansions to be defined over products of fields.

DEFINITION 3.8. *A complete set of rational Puiseux expansions of a polynomial $F \in \mathbb{K}((x))[y]$ is a sequence of triples $(\mu_i(a), X_i(t), Y_i(t))$ for $i = 1, \dots, s$ such that:*

- $\mu_i \in \mathbb{K}[a]$ is monic and separable; we set $\mathbb{E}_i := \mathbb{K}[a]/(\mu_i(a))$,

- $(X_i(t) = \gamma_i t^{e_i}, Y_i(t)) \in \mathbb{E}_i((t))^2$,
- γ_i and the initial coefficient of Y_i are invertible in \mathbb{E}_i ,
- $\{1, \dots, s\} \times \mathcal{U}_{\mathbb{A}}(\mu_i)$ is in one-to-one correspondence with the absolutely irreducible factors of F . Precisely, for any $i \in \{1, \dots, s\}$ and any root α of μ_i , $(\pi_{\alpha}(X_i(t)), \pi_{\alpha}(Y_i(t)))$ is a rational Puiseux expansion (with the meaning of Definition 3.3) of an absolutely irreducible factor of F , where π_{α} stands for the natural projection from $\mathbb{E}_i[[t]]$ onto $\mathbb{K}[\alpha][[t]]$.

PROPOSITION 3.9. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d_y in y , and let $((\mu_i(a), X_i(t), Y_i(t)))_{i=1, \dots, s}$ represent the rational Puiseux expansions of F with the meaning of Definition 3.8. If the initial coefficient of $F_y(X_i(t), Y_i(t))$ is invertible modulo μ_i , for $i = 1, \dots, s$, then we have*

$$\text{val}_x(\text{Disc}_y F) = \sum_{i=1}^s \deg \mu_i \text{val}_t(F_y(X_i(t), Y_i(t))).$$

Proof. The multiplicative property of the resultant yields

$$\text{val}_x(\text{Disc}_y F) = \sum_{i=1}^{d_y} \deg \mu_i \sum_{k=0}^{e_i-1} \text{val}_x(F_y(x, Y_i(\zeta^k(x/\gamma_i)^{1/e_i}))).$$

On the other hand, for $k=0, \dots, e_i-1$ we verify that

$$\text{val}_x(F_y(x, Y_i(\zeta^k(x/\gamma_i)^{1/e_i}))) = \text{val}_t(F_y(X_i(t), Y_i(t))) / e_i. \quad \square$$

Concerning the singular parts, Definition 3.8 must be adapted in order to ensure that rational expansions with different regularity indices are distinguished.

DEFINITION 3.10. *The singular parts of a complete set of rational Puiseux expansions of a polynomial $F \in \mathbb{K}((x))[y]$ are a sequence of quadruples $(\mu_i(a), \hat{X}_i(t), \hat{Y}_i(t), \rho_i)$ for $i = 1, \dots, s$ such that:*

- $\mu_i \in \mathbb{K}[a]$ is monic and separable; we set $\mathbb{E}_i := \mathbb{K}[a] / (\mu_i(a))$, and let α_i be the class of a in \mathbb{E}_i ,
- $\rho_i \in \mathbb{Q}_{\geq 0} \cup \{-\infty\}$,
- $(\hat{X}_i(t) = \gamma_i t^{e_i}, \hat{Y}_i(t)) \in (\mathbb{E}_i((t)) / (t^{e_i \rho_i + 1}))^2$,
- γ_i and the initial coefficient of \hat{Y}_i are invertible in \mathbb{E}_i ,
- $\{1, \dots, s\} \times \mathcal{U}_{\mathbb{A}}(\mu_i)$ is in one-to-one correspondence with the absolutely irreducible factors of F . Precisely, for any $i \in \{1, \dots, s\}$ and any root α of μ_i , $(\pi_{\alpha}(\hat{X}_i(t)), \pi_{\alpha}(\hat{Y}_i(t)))$ is the singular part of a rational Puiseux expansion (with the meaning of Definition 3.3), with regularity index ρ_i , of an absolutely irreducible factor of F , where π_{α} stands for the natural projection from $\mathbb{E}_i[[t]]$ onto $\mathbb{K}[\alpha][[t]]$.

LEMMA 3.11. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d_y in y . Given the singular part $(\mu(a), \hat{X}(t), \hat{Y}(t), \rho)$ (with the meaning of Definition 3.10) of a rational Puiseux expansion $(\mu(a), X(t), Y(t))$ of F (with the meaning of Definition 3.8), if μ is irreducible, then we can compute $\text{val}_t(F_y(X(t), Y(t)))$ with*

$$\tilde{O}(d_y \deg \mu (\text{val}_t(F_y(X(t), Y(t))) + 1))$$

operations in \mathbb{K} .

Proof. Thanks to Lemma 3.7, the valuation of $F_y(X(t), Y(t))$ can be computed as the valuation of $F_y(\hat{X}(t), \hat{Y}(t))$. The evaluation of $F_y(\hat{X}(t), \hat{Y}(t))$ at precision $\eta > 1$ takes $\tilde{O}(d_y \eta)$ operations in $\mathbb{E} := \mathbb{K}[a]/(\mu(a))$, that amounts to $\tilde{O}(d_y \deg \mu \eta)$ operations in \mathbb{K} . The valuation $\text{val}_t(F_y(X(t), Y(t)))$ is obtained by evaluating $F_y(\hat{X}(t), \hat{Y}(t))$ successively at precisions $1, 2, 4, 8, \dots$ until a non-zero value is found. In this way, the final precision does not exceed $2 \text{val}_t(F_y(X(t), Y(t))) + 1$ and the number of evaluations is $O(\log(\text{val}_t(F_y(X(t), Y(t)))))$. \square

3.6. Computation of singular parts

For computing singular parts of rational Puiseux expansions we rely on the following complexity bound.

THEOREM 3.12. [59, simplified from Theorem 1] *Let $F \in \mathbb{K}[x][y]$ be monic and separable of degree d_y in y . There exists a probabilistic algorithm of Las Vegas type that computes the singular parts (with the meaning of Definition 3.10) of the rational Puiseux expansions of F regarded in $\mathbb{K}[[x]][y]$ with an expected number of*

$$\tilde{O}(d_y (\text{val}_x(\text{Disc}_y F) + 1))$$

operations in \mathbb{K} .

Remark 3.13. Let us mention that [59, Theorem 1] handles the more general case where $F \in \mathbb{K}[x][y]$ is not necessarily monic in y , and also where the characteristic of \mathbb{K} is positive and larger than d_y .

Example 3.14. Let us take $\mathbb{K} := \mathbb{Q}$ and

$$F(x, y) := y^7 - x(x^3 + y^2 + xy)^2.$$

We have $\text{val}_x(\text{Disc}_y F) = 33$. With the Newton polytope algorithm, we compute the singular parts of three rational Puiseux expansions with the representation of Definition 3.10:

- First singular part: $e_1 = 1, \rho_1 = 2$,

$$\begin{aligned} \mu_1(a) &:= a^2 - 2a + 2 \\ \hat{X}_1(t) &:= t \\ \hat{Y}_1(t) &:= -t + \alpha_1 t^2. \end{aligned}$$

- Second singular part: $e_2 = 3, \rho_2 = 1/3$,

$$\begin{aligned} \mu_2(a) &:= a \\ \hat{X}_2(t) &:= t^3 \\ \hat{Y}_2(t) &:= t. \end{aligned}$$

- Third singular part: $e_3 = 2, \rho_3 = 11/2$,

$$\begin{aligned} \mu_3(a) &:= a \\ \hat{X}_3(t) &:= -t^2 \\ \hat{Y}_3(t) &:= -t^4 + t^6 - 2t^8 + 5t^{10} + t^{11}. \end{aligned}$$

A Puiseux expansion $(\mu(a), X(t), Y(t))$ of $F \in \mathbb{E}[[x]][y]$ (with the meaning of Definition 3.8) is said to be *regular* if $F_y(0, Y(0))$ is invertible in $\mathbb{E} := \mathbb{K}[a] / (\mu(a))$. The regular parts can be easily computed as follows. For $\mu(a)$ we take the product of the factors of multiplicity 1 in $F(0, a)$, and if α denotes the class of a in $\mathbb{K}[a] / (\mu(a))$, then $(\mu(a), t, \alpha, 0)$ represents the singular part of the regular rational Puiseux expansions of F . From computing the squarefree factorization of $F(0, a)$, the regular Puiseux expansions can therefore be obtained in softly linear time.

PROPOSITION 3.15. *Let $F \in \mathbb{K}[x][y]$ be monic and separable of degree d_y in y . Given the singular parts of all the non-regular rational Puiseux expansions of F regarded in $\mathbb{K}[[x]][y]$ (with the meaning of Definition 3.10), we can compute another representation of the singular parts in the form $((\tilde{\mu}_i(a), \tilde{X}_i(t), \tilde{Y}_i(t), \tilde{\rho}_i))_{i=1, \dots, \tilde{s}}$ (still with the meaning of Definition 3.10) along with*

$$\tilde{\sigma}_i := \text{val}_t(F_y(\tilde{X}_i(t), \tilde{Y}_i(t)))$$

such that the coefficient of degree $\tilde{\sigma}_i$ in $F_y(\tilde{X}_i(t), \tilde{Y}_i(t))$ is invertible in $\tilde{\mathbb{E}}_i := \mathbb{K}[a] / (\tilde{\mu}_i(a))$. This new representation can be obtained with

$$\tilde{O}(d_y \text{val}_x(\text{Disc}_y F))$$

arithmetic operations in \mathbb{K} .

Proof. We let $((\mu_i(a), \hat{X}_i(t), \hat{Y}_i(t), \rho_i))_{i=1, \dots, s}$ represent the singular parts of the non-regular rational Puiseux expansions of F regarded in $\mathbb{K}[[x]][y]$.

If \mathbb{E}_i is a field, then Lemma 3.11 and Proposition 3.9 straightforwardly yield the claimed bound. Unfortunately, if \mathbb{E}_i is a finite product of fields, then panoramic evaluation does not conclude the proof, because the cost of the method described in the proof of Lemma 3.11 depends on the computed valuation for F_y . Consequently, we need to adapt the proof of Lemma 3.11.

Let $\mu_i^{[k]}$ denote the largest divisor of μ_i such that

$$\text{val}_t(F_y(\hat{X}_i(t) \bmod \mu_i^{[k]}, \hat{Y}_i(t) \bmod \mu_i^{[k]})) \geq 2^k - 1.$$

Note that $\mu_i^{[0]} := \mu_i$, and let K_i be the first value of k such that $\deg \mu_i^{[K_i]} = 0$.

If $\mu_i^{[k]}$ is known for some k with $0 \leq k < K_i$, then we use panoramic evaluation over $\mathbb{E}_i^{[k]} := \mathbb{K}[a] / (\mu_i^{[k]}(a))$ to test if $\text{val}_t(F_y(\hat{X}_i(t), \hat{Y}_i(t))) \geq 2^{k+1} - 1$ holds. Computing $\hat{X}_i(t) \bmod \mu_i^{[k]}$ and $\hat{Y}_i(t) \bmod \mu_i^{[k]}$ to precision $O(t^{2^{k+1}-1})$ takes

$$\tilde{O}(\deg \mu_i \min(e_i \rho_i + 1, 2^{k+1})),$$

where e_i is the ramification index of $(\hat{X}_i(t), \hat{Y}_i(t))$, and the panoramic evaluation then takes

$$\tilde{O}(d_y \deg \mu_i^{[k]} 2^k)$$

operations in \mathbb{K} by Theorem 2.6. As a result, we obtain pairwise coprime factors $\mu_{i,0}^{[k]}, \dots, \mu_{i,r_i,k}^{[k]}$ of $\mu_i^{[k]}$ such that $\mu_i^{[k]} = \mu_{i,0}^{[k]} \cdots \mu_{i,r_i,k}^{[k]}$ that

$$2^k - 1 \leq \text{val}_t(F_y(\hat{X}_i(t) \bmod \mu_{i,j}^{[k]}, \hat{Y}_i(t) \bmod \mu_{i,j}^{[k]})) < 2^{k+1} - 1 \text{ for } j \geq 1,$$

that the initial coefficient of $F_y(\hat{X}_i(t) \bmod \mu_{i,j}^{[k]}, \hat{Y}_i(t) \bmod \mu_{i,j}^{[k]})$ is invertible modulo $\mu_{i,j}^{[k]}$ for $j=1, \dots, r_{i,k}$, and that $\mu_i^{[k+1]} =: \mu_{i,0}^{[k]}$. The cost of these computations rewrites as

$$\begin{aligned} & \tilde{O}(\deg \mu_i e_i \rho_i + d_y \deg \mu_i^{[k]} 2^k) \\ &= \tilde{O}\left(\deg \mu_i e_i \rho_i + d_y \deg \mu_{i,0}^{[k]} 2^k + \sum_{j=1}^{r_{i,k}} d_y \deg \mu_{i,j}^{[k]} \operatorname{val}_t(F_y(\hat{X}_i(t) \bmod \mu_{i,j}^{[k]}, \hat{Y}_i(t) \bmod \mu_{i,j}^{[k]}))\right) \\ &= \tilde{O}(\deg \mu_i e_i \rho_i + d_y m_i), \end{aligned}$$

where

$$m_i := \sum_{\substack{\nu | \mu_i \\ \nu \text{ irreducible}}} d_y \deg \nu \operatorname{val}_t(F_y(\hat{X}_i(t) \bmod \nu, \hat{Y}_i(t) \bmod \nu)).$$

Thanks to Proposition 3.9, the sum of these costs for $k=0, \dots, K_i-1$ and $i=1, \dots, s$ is

$$\tilde{O}\left(d_y \operatorname{val}_x(\operatorname{Disc}_y F) \max_{i=1, \dots, s} K_i\right) = \tilde{O}(d_y \operatorname{val}_x(\operatorname{Disc}_y F)),$$

since $\max_{i=1, \dots, s} K_i = O(\log(\operatorname{val}_x(\operatorname{Disc}_y F)))$.

Finally, the reductions $(\hat{X}_i(t), \hat{Y}_i(t)) \bmod \mu_{i,j}^{[k]}$ for $i=1, \dots, s$, $j=1, \dots, r_{i,k}$, $k=0, \dots, K_i-1$, take softly linear time by Proposition 2.3. \square

Remark 3.16. The algorithm underlying [59, Theorem 1] may be implemented in a way to ensure that the initial coefficient of $F_y(\hat{X}_i(t), \hat{Y}_i(t))$ is invertible for all i . However, this property does not seem to be explicitly stated in the specifications of this algorithm, so we preferred to provide the reader with the details.

Example 3.17. (Continued from Example 3.14) Proposition 3.15 called with the singular parts of Example 3.14 does not refine the set of expansions. So

$$((\tilde{\mu}_i(a), \tilde{X}_i(t), \tilde{Y}_i(t), \tilde{\rho}_i))_{i=1, \dots, \tilde{s}} = ((\mu_i(a), \hat{X}_i(t), \hat{Y}_i(t), \rho_i))_{i=1, \dots, s},$$

and $\tilde{\sigma}_1 = 5$, $\tilde{\sigma}_2 = 6$, $\tilde{\sigma}_3 = 17$. By the way, we verify that the identity

$$\operatorname{val}_x(\operatorname{Disc}_y F) = \deg \mu_1 \tilde{\sigma}_1 + \deg \mu_2 \tilde{\sigma}_2 + \deg \mu_3 \tilde{\sigma}_3$$

holds as expected from Proposition 3.9.

3.7. Lifting a rational Puiseux expansion

In our main algorithm we will need to increase the precision of Puiseux expansions given by their singular parts, in order to obtain the adjoint divisor of a curve. Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d_y but not necessarily irreducible. Let $\varphi_1, \dots, \varphi_{d_y}$ denote the Puiseux expansions of F , so we have

$$F = \prod_{i=1}^{d_y} (y - \varphi_i).$$

LEMMA 3.18. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree $d_y \geq 2$ in y , and let \tilde{F} denote a monic polynomial of degree d_y such that $\operatorname{val}_x(F - \tilde{F}) > \operatorname{val}_x(\operatorname{Disc}_y F)$. Let $\hat{\varphi}$ be the singular part of a Puiseux expansion φ of F , with ramification index e and regularity index ρ in F . Then, the following properties hold:*

1. $\operatorname{val}_x(\tilde{F}(\hat{\varphi})) > \rho + \operatorname{val}_x(\tilde{F}_y(\hat{\varphi}))$.

2. If ψ is a Puiseux series truncated at precision $\rho + \eta$ for $\eta > 0$ such that

$$\begin{aligned} \psi &= \varphi + O(x^{\rho+1/e}), \\ \text{val}_x(\tilde{F}(\psi)) &\geq \rho + \eta + \text{val}_x(\tilde{F}_y(\hat{\varphi})), \end{aligned}$$

then there exists a unique Puiseux series $\tilde{\psi}$ of valuation $\geq \rho + \eta$ and truncated at precision $\rho + 2\eta$ such that $\text{val}_x(\tilde{F}(\psi + \tilde{\psi})) \geq \rho + 2\eta + \text{val}_x(\tilde{F}_y(\hat{\varphi}))$. This value of $\tilde{\psi}$ can be computed as

$$\tilde{\psi} := -\frac{\tilde{F}(\psi)}{\tilde{F}_y(\psi)} + O(x^{\rho+2\eta}),$$

where the evaluations of \tilde{F} and \tilde{F}_y need precision $\rho + 2\eta + \text{val}_x(\tilde{F}_y(\hat{\varphi}))$.

Proof. Let $m := \text{val}_x(\text{Disc}_y F)$ and assume that $\varphi = \varphi_1$. First, we observe that $\text{Disc}_y \tilde{F}$ and $\text{Disc}_y F$ coincide up to degree m , so they have the same valuation. In particular, \tilde{F} is separable in y .

Thanks to Lemma 3.7, part 1 holds because

$$\tilde{F}(\hat{\varphi}) = F(\hat{\varphi}) + O(x^{m+1/e}), \quad \text{val}_x(F(\hat{\varphi})) > \rho + \text{val}_x(F_y(\hat{\varphi})), \text{ and}$$

$$\begin{aligned} m &= \text{val}_x(F_y(\varphi)) + \sum_{i=2}^{d_y} \text{val}_x(F_y(\varphi_i)) \\ &= \text{val}_x(F_y(\varphi)) + \sum_{i=2}^{d_y} \sum_{j \neq i} \text{val}_x(\varphi_i - \varphi_j) \\ &\geq \text{val}_x(F_y(\varphi)) + \rho. \end{aligned}$$

As for part 2, again from Lemma 3.7, we know that

$$\text{val}_x(F_y(\psi)) = \text{val}_x(F_y(\varphi)) \leq m.$$

For any series $\tilde{\psi}$ of valuation $\geq \rho + \eta$, we consider the Taylor expansion

$$\tilde{F}(\psi + \tilde{\psi}) = \tilde{F}(\psi) + \tilde{F}_y(\psi) \tilde{\psi} + \sum_{k=2}^{d_y} \frac{1}{k!} \frac{\partial^k \tilde{F}}{\partial y^k}(\psi) \tilde{\psi}^k.$$

Then, we verify that

$$\frac{1}{k!} \frac{\partial^k \tilde{F}}{\partial y^k}(\psi) = \frac{1}{k!} \frac{\partial^k F}{\partial y^k}(\psi) + O(x^{m+1/e}) = \sum_{\substack{S \subseteq \{1, \dots, d_y\} \\ |S|=d_y-k}} \prod_{i \in S} (\psi - \varphi_i) + O(x^{m+1/e}).$$

A product $\prod_{i \in S} (\psi - \varphi_i)$ in $\frac{1}{k!} \frac{\partial^k F}{\partial y^k}(\psi)$ has valuation

$$\geq \text{val}_x(F_y(\psi)) - (k-1)\rho,$$

and this lower bound is $\leq m$. It follows that

$$\begin{aligned} \text{val}_x \left(\sum_{k=2}^{d_y} \frac{1}{k!} \frac{\partial^k \tilde{F}}{\partial y^k}(\psi) \tilde{\psi}^k \right) &\geq \min_{k=2, \dots, d_y} (k(\rho + \eta) + \text{val}_x(F_y(\psi)) - (k-1)\rho) \\ &\geq \min_{k=2, \dots, d_y} (k\eta + \text{val}_x(F_y(\psi)) + \rho) \\ &\geq \rho + 2\eta + \text{val}_x(F_y(\psi)), \end{aligned}$$

hence that

$$\tilde{F}(\psi + \tilde{\psi}) = \tilde{F}(\psi) + \tilde{F}_y(\psi) \tilde{\psi} + O(x^{\rho+2\eta+\text{val}_x(\tilde{F}_y(\psi))}).$$

Consequently, the condition

$$\text{val}_x(\tilde{F}(\psi + \tilde{\psi})) \geq \rho + 2\eta + \text{val}_x(\tilde{F}_y(\psi)) = \rho + 2\eta + \text{val}_x(F_y(\hat{\varphi}))$$

holds with $\tilde{\psi}$ uniquely determined at precision $O(x^{\rho+2\eta})$ by the claimed formula. \square

PROPOSITION 3.19. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d_y in y , and let \tilde{F} denote a truncation of F at a precision $>\text{val}_x(\text{Disc}_y F)$. Let $\hat{\varphi}$ be the singular part of a Puiseux expansion φ of F . Then, the Newton sequence $\psi_0 := \hat{\varphi}$ and*

$$\psi_{i+1} := \psi_i - \frac{\tilde{F}(\psi_i)}{\tilde{F}_y(\psi_i)} \text{ for } i \geq 0$$

converges to a root of \tilde{F} .

Proof. The convergence follows from Lemma 3.18. \square

PROPOSITION 3.20. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d_y in y , and let \tilde{F} denote a truncation of F at a precision $>\text{val}_x(\text{Disc}_y F)$. Then, the singular parts of F and \tilde{F} coincide.*

Proof. From Proposition 3.19 we know that each singular part of F can be extended into a root of F . It follows that the singular parts of F and \tilde{F} do coincide. \square

PROPOSITION 3.21. *Let $F \in \mathbb{K}[[x]][y]$ be monic and separable of degree d_y in y , and let $(\mu(a), \hat{X}(t), \hat{Y}(t), \rho)$ represent the singular part of a rational Puiseux expansion of F (with the meaning of Definition 3.10). If the initial coefficient of $F_y(\hat{X}(t), \hat{Y}(t))$ is invertible in $\mathbb{E} := \mathbb{K}[a] / (\mu(a))$, then the truncation at precision $N \geq 1$ of this rational Puiseux expansion can be computed with*

$$\tilde{O}(d_y \deg \mu(\text{val}_t(F_y(\hat{X}(t), \hat{Y}(t))) + N))$$

operations in \mathbb{K} . This computation can be achieved from the truncation of F in x at precision $\lceil (\text{val}_t(F_y(X(t), Y(t))) + N) / e \rceil$, where e represents the ramification index of the expansion.

Proof. This follows directly from Lemma 3.18. \square

3.8. Puiseux expansions for curves

In this subsection, F now represents a polynomial in $\mathbb{K}[x, y]$. We are interested in computing all the rational Puiseux expansions above the critical points of the projection $(x, y) \mapsto x$ from the curve $\mathcal{U}_{\mathbb{A}}(F)$ onto the x -axis.

PROPOSITION 3.22. *Let $F \in \mathbb{K}[x, y]$ be of total degree δ and of degree δ in y . We can compute the following data with a probabilistic algorithm of Las Vegas type that takes an expected number of $\tilde{O}(\delta^3)$ operations in \mathbb{K} :*

- $(\Delta_i, m_i)_{i=1, \dots, r}$; we set $\mathbb{L}_i := \mathbb{K}[b] / (\Delta_i(b))$, and let β_i represent the class of b in \mathbb{L}_i ;
- For $i = 1, \dots, r$, quintuples $((\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t), \rho_{i,j}, \sigma_{i,j}))_{j=1, \dots, s_i}$ with $\mu_{i,j}(a) \in \mathbb{L}_i[a]$, $\sigma_{i,j} \in \mathbb{N}_{\geq 0}$, and

$$(X_{i,j}(t), Y_{i,j}(t)) \in (\mathbb{E}_{i,j}[[t]] / (t^{\sigma_{i,j}+1}))^2,$$

where $\mathbb{E}_{i,j} := \mathbb{L}_i[a] / (\mu_{i,j}(a))$;

Such that the following properties hold:

- $\text{Disc}_y F = \Delta_1^{m_1} \cdots \Delta_r^{m_r}$, where the $\Delta_i \in \mathbb{K}[x]$ are pairwise separable coprime factors of $\text{Disc}_y F$ of multiplicity m_i (the m_i are not necessarily pairwise distinct), for $i = 1, \dots, r$;
- $\mu_{i,j}$ is monic and separable of degree ≥ 1 , for $i = 1, \dots, r$ and $j = 1, \dots, s_i$; here the separability of $\mu_{i,j}$ means that the discriminant of $\mu_{i,j}$ is invertible in \mathbb{L}_i ;
- $X_{i,j}$ writes as $\beta_i + \gamma_{i,j} t^{e_{i,j}}$, with $\gamma_{i,j}$ invertible in $\mathbb{E}_{i,j}$ and $e_{i,j} \geq 1$, for $i = 1, \dots, r$ and $j = 1, \dots, s_i$;
- The initial coefficient of $F_y(X_{i,j}(t), Y_{i,j}(t))$ is invertible in $\mathbb{E}_{i,j}$ and we have

$$\sigma_{i,j} = \text{val}_t(F_y(X_{i,j}(t), Y_{i,j}(t))),$$

for $i = 1, \dots, r$ and $j = 1, \dots, s_i$;

- For $i = 1, \dots, r$ and for all root β of Δ_i , let π_β stand for the natural projection $\mathbb{L}_i \rightarrow \mathbb{K}[\beta]$ (but also for its natural coefficient-wise extensions), then

$$((\pi_\beta(\mu_{i,j}(a)), \pi_\beta(X_{i,j}(t) - \beta_i), \pi_\beta(Y_{i,j}(t))))_{j=1, \dots, s_i}$$

are the truncations at precision $\sigma_{i,j} + 1$ of the rational Puiseux expansions of F regarded in $\mathbb{K}[\beta][[x - \beta]][y]$, with the meaning of Definition 3.8, and whose regularity index in F is $\rho_{i,j}$.

Proof. We compute the discriminant $\text{Disc}_y F$ with $\tilde{O}(\delta^3)$ operations in \mathbb{K} (by means of [50, Theorem 30] for instance) and then its squarefree factorization

$$\text{Disc}_y F = \tilde{\Delta}_1^{\tilde{m}_1} \cdots \tilde{\Delta}_{\tilde{r}}^{\tilde{m}_{\tilde{r}}},$$

with $\tilde{O}(\delta^2)$ operations in \mathbb{K} , where the $\tilde{\Delta}_i$ are squarefree, of degree ≥ 1 , pairwise coprime, and the $\tilde{m}_i \geq 1$ are pairwise distinct integers; see [28, Theorem 14.20]. By the classical Bézout theorem we have

$$\deg \Delta = \sum_{i=1}^{\tilde{r}} \tilde{m}_i \deg \tilde{\Delta}_i \leq \delta(\delta - 1); \quad (3.1)$$

see [3, Proposition 5.5] for instance. We write $\tilde{\mathbb{L}}_i := \mathbb{K}[b] / (\tilde{\Delta}_i(b))$, and let $\tilde{\beta}_i$ represent the class of b in $\tilde{\mathbb{L}}_i$. Note that $\text{val}_{x - \tilde{\beta}_i} \Delta = \tilde{m}_i$ is the valuation of the discriminant of F regarded in $\tilde{\mathbb{L}}_i[[x - \tilde{\beta}_i]][y]$.

By Proposition 2.3 we can compute $F(x, y) \text{rem } \tilde{\Delta}_i(x)^{\tilde{m}_i + 1}$ for $i = 1, \dots, \tilde{r}$ simultaneously, with $\tilde{O}(\delta^3)$ operations in \mathbb{K} . Thanks to Proposition 2.5, the Taylor expansion of $F(x, y) \text{rem } \tilde{\Delta}_i(x)^{\tilde{m}_i + 1}$ in

$$(\tilde{\mathbb{L}}_i[[x - \tilde{\beta}_i]] / (x - \tilde{\beta}_i)^{\tilde{m}_i + 1})[y]$$

can further be obtained in softly linear time.

If $\tilde{\Delta}_i$ is irreducible, then Proposition 3.20 ensures that we may appeal to Theorem 3.12 and Proposition 3.15 in order to obtain the singular parts of the rational Puiseux expansions of F regarded in $(\tilde{\mathbb{L}}_i[[x - \tilde{\beta}_i]] / (x - \tilde{\beta}_i)^{\tilde{m}_i + 1})[y]$. The expected cost is $\tilde{O}(\delta \tilde{m}_i)$ operations in $\tilde{\mathbb{L}}_i$, that amounts to an expected number of $\tilde{O}(\delta \tilde{m}_i \deg \tilde{\Delta}_i)$ operations in \mathbb{K} .

If $\tilde{\Delta}_i$ is not irreducible, then we apply the algorithm underlying Theorem 3.12 followed by the one of Proposition 3.15 in the context of a panoramic evaluation over $\tilde{\mathbb{L}}_i$. The former algorithm is randomized of Las Vegas type. Its internal probabilistic subroutine only concerns [59, Proposition 4] that calculates primitive element representations of algebraic towers of separable extensions of height two, precisely of the form

$$P_1(x_1) = P_2(x_1, x_2) = 0,$$

with P_2 monic in x_2 . A primitive element of $\mathcal{U}_{\mathbb{A}}(P_1, P_2)$ can be taken of the form $\lambda x_1 + x_2$, with $\lambda \in \mathbb{K}$; see the definition of a primitive element representation in Section 6.1. The number of values of λ in \mathbb{K} for which $\lambda x_1 + x_2$ is not primitive is

$$\leq \binom{\deg_{x_1} P_1 \deg_{x_2} P_2}{2} =: N.$$

Consequently, taking λ uniformly at random in a subset of \mathbb{K} of cardinality ηN does not lead to a primitive element with probability $\leq 1/\eta$. If a first random value of λ does not yield a primitive element then we can try another one, and so on. We assume that the number of such trials is fixed in the algorithm. With these arguments, the algorithm underlying Theorem 3.12, for a fixed value of δ , can be regarded as a family of computation trees $(T_b)_{b \in \mathcal{B}}$ where \mathcal{B} is the product of all the finite sets in which the γ are taken at random at every use of [59, Proposition 4]. And we can therefore assume that, for a given input, the probability that a tree T_b fails at finding primitive elements is $\leq 1/2$.

We are thus back in the context of Section 2.4. If P_1 and P_2 have their coefficients in a \mathbb{K} -algebra

$$\mathbb{A} \cong \prod_{i=1}^l \mathbb{F}_i, \text{ where the } \mathbb{F}_i := \mathbb{K}[x]/(\mu_i(x)) \text{ are fields,}$$

then $u := \lambda x_1 + x_2$ is primitive for

$$P_1(x_1) = P_2(x_1, x_2) = 0$$

if, and only if, $\text{Disc}_u(\text{Res}_{x_1}(P_1(x_1), P_2(x_1, u - \lambda x_1)))$ is invertible in \mathbb{A} . If so, it follows that u remains primitive for the projections of P_1 and P_2 onto each \mathbb{F}_i , for $i = 1, \dots, l$. Consequently, Hypothesis (H) is satisfied and Corollary 2.7 ensures that the panoramic evaluation of $(T_b)_{b \in \mathcal{B}}$ takes an expected cost $\tilde{O}(\delta \tilde{m}_i \deg \tilde{\Delta}_i)$. This process yields a panoramic decomposition of $\tilde{\mathbb{L}}_i$, that concretely means a partial factorization of $\tilde{\Delta}_i = \Delta_{i,1} \cdots \Delta_{i,r_i}$. For $j = 1, \dots, r_i$ we obtain the singular parts of the Puiseux expansions of F regarded in $\mathbb{L}_{i,j}[[x - \beta_{i,j}]][[y]]$ with the meaning of Definition 3.10 as if $\mathbb{L}_{i,j} := \mathbb{K}[b]/(\Delta_{i,j}(b))$ were a field, and where $\beta_{i,j}$ stands for the class of b in $\mathbb{L}_{i,j}$.

The correctness is ensured by Proposition 3.20. The expected cost is $\tilde{O}(\delta \tilde{m}_i \deg \tilde{\Delta}_i)$, by Theorem 3.12 and Proposition 3.15. The sum of these costs for $i = 1, \dots, \tilde{r}$ is $\tilde{O}(\delta^3)$ thanks to Inequality (3.1).

So far we have obtained the Δ_i along with the $\mu_{i,j}$ and $\sigma_{i,j}$ requested by the proposition, for $i = 1, \dots, r$ and $j = 1, \dots, s_i$, but the rational Puiseux expansions at our disposal are only singular parts, written $(\mu_{i,j}(a), \hat{X}_{i,j}(t), \hat{Y}_{i,j}(t), \rho_{i,j})$ as in Definition 3.10.

By Proposition 2.3 we can compute $F(x, y) \text{ rem } \Delta_i(x)^{2m_i+1}$ for $i = 1, \dots, r$ simultaneously, with $\tilde{O}(\delta^3)$ operations in \mathbb{K} . Thanks to Proposition 2.5, the Taylor expansion of $F(x, y) \text{ rem } \Delta_i(x)^{2m_i+1}$ in

$$(\mathbb{L}_i[[x - \beta_i]]/(x - \beta_i)^{2m_i+1})[[y]]$$

can be obtained in softly linear time. By Proposition 3.21 the lifting of a non-regular rational Puiseux expansion $(\mu_{i,j}(a), \hat{X}_{i,j}(t), \hat{Y}_{i,j}(t), \rho_{i,j})$ of F at precision $\sigma_{i,j} + 1$ is possible since F is known with precision $2m_i + 1$ in $x - \beta_i$. This lifting involves

$$\tilde{O}(\delta \deg \Delta_i \deg \mu_{i,j} (\text{val}_t(F_y(\hat{X}_{i,j}(t), \hat{Y}_{i,j}(t))) + 1))$$

operations in \mathbb{K} . If \mathcal{J}_i is the subset of indices j such that $(\mu_{i,j}(a), \hat{X}_{i,j}(t), \hat{Y}_{i,j}(t), \rho_{i,j})$ is non-regular, then Proposition 3.9 implies that

$$\tilde{O}\left(\sum_{j \in \mathcal{J}_i} \delta \deg \Delta_i \deg \mu_{i,j} \text{val}_t(F_y(\hat{X}_{i,j}(t), \hat{Y}_{i,j}(t)))\right) = \tilde{O}(\delta \deg \Delta_i m_i).$$

The sum of these costs for $i=1, \dots, r$ yields $\tilde{O}(\delta \deg \Delta) = \tilde{O}(\delta^3)$. Finally, the regular Puiseux series do not require to be lifted. \square

Proposition 3.22 is the main complexity result of this section, it will be used to compute adjoint divisors of curves in the next section. There, we will drop regular Puiseux expansions since only those centered at singular points intervene in adjoint divisors. We will see that the computation of the adjoint divisor is not the bottleneck of our main algorithm (underlying Theorem 8.8): a complexity bound $O(\delta^{2\omega})$ within Proposition 3.22 would suffice.

Example 3.23. (Continued from Example 3.17) Let us take $\mathbb{K} := \mathbb{Q}$ and

$$F(x, y) := y^7 - x(x^3 + y^2 + xy)^2,$$

that is absolutely irreducible. We illustrate the data occurring in Proposition 3.22. The equation $F=0$ defines a curve $\mathcal{U}_{\mathbb{A}}(F)$ of degree $\delta=7$. The discriminant of F in y is

$$\text{Disc}_y(F) = -\Delta_1^{m_1}(x) \Delta_2^{m_2}(x),$$

where

$$\begin{aligned} \Delta_1(b) &:= b \\ \Delta_2(b) &:= b^9 - \frac{345744}{823543} b^5 + \frac{377300}{823543} b^4 - \frac{122500}{823543} b^3 + \frac{19412}{823543} b^2 - \frac{3456}{823543} b + \frac{432}{823543} \end{aligned}$$

and $m_1 := 33$, $m_2 := 1$. So $r = 2$.

The unique singular point of $\mathcal{U}_{\mathbb{A}}(F)$ is $P := (0, 1)$. Let π represent the projection from the curve $\mathcal{U}_{\mathbb{A}}(F)$ onto the x -axis. The critical points of π are the roots of Δ_1 and Δ_2 .

The y -coordinates of the points of $\pi^{-1}(\beta_1)$ are the roots of $F(\beta_1, y) = y^7 = 0$, that is the singleton $\{0\}$. The singular parts of the rational Puiseux expansions of $F(x, y)$ regarded in $\mathbb{K}[[x]][[y]]$ have been presented in Example 3.17. After lifting these singular parts we obtain:

$$\begin{aligned} \mu_{1,1}(a) &:= a^2 - 2a + 2 \\ X_{1,1}(t) &:= t \\ Y_{1,1}(t) &:= -t + \alpha_{1,1} t^2 + \left(-\frac{3}{2} \alpha_{1,1} + 5\right) t^3 + \dots + \left(\frac{217}{8} \alpha_{1,1} - \frac{405}{8}\right) t^5 + O(t^6) \\ \sigma_{1,1} &:= 5 \\ \mu_{1,2}(a) &:= a \\ X_{1,2}(t) &:= t^3 \\ Y_{1,2}(t) &:= t + \frac{2}{3} t^3 - \frac{5}{9} t^5 + O(t^7) \\ \sigma_{1,2} &:= 6 \\ \mu_{1,3}(a) &:= a \\ X_{1,3}(t) &:= -t^2 \\ Y_{1,3}(t) &:= -t^4 + t^6 - 2t^8 + 5t^{10} + t^{11} - 14t^{12} + \dots - \frac{1615}{16} t^{17} + O(t^{18}) \\ \sigma_{1,3} &:= 17. \end{aligned}$$

The y -coordinates of the points of $\pi^{-1}(\beta_2)$ are the roots of $F(\beta_2, y) = 0$. We verify that 5 of these roots are simple and one is double: in fact $F(\beta_2, a)$ factorizes into $\mu_{2,1}(a) \mu_{2,2}^2(a)$ where $\mu_{2,1}$ has degree 5 and $\mu_{2,2}$ has degree 1. We deduce that

$$\begin{aligned} \mu_{2,1}(a) &:= a^5 + \left(-\frac{7524223091985523}{99075595293942} \beta_2^8 + \cdots + \frac{6356788317432}{16512599215657} \right) a^4 + \cdots \\ X_{2,1}(t) &:= \beta_2 + t \\ Y_{2,1}(t) &:= \alpha_{2,1} + O(t) \\ \sigma_{2,1} &:= 0 \\ \mu_{2,2}(a) &:= a + \frac{7524223091985523}{198151190587884} \beta_2^8 + \cdots - \frac{3178394158716}{16512599215657} \\ X_{2,2}(t) &:= \beta_2 + \gamma_{2,2} t^2 \\ Y_{2,2}(t) &:= \alpha_{2,2} + \gamma'_{2,2} t + O(t^2) \\ \sigma_{2,2} &:= 1, \end{aligned}$$

where $\gamma_{2,2}$ and $\gamma'_{2,2}$ are some elements in $\mathbb{E}_{2,2}$.

4. DIVISORS

From now on, F denotes an absolutely irreducible homogeneous polynomial in $\mathbb{K}[x, y, z]$ that defines a curve C in \mathbb{P}^2 . This section is devoted to the definition of places and divisors of C in terms of rational Puiseux expansions.

4.1. Places and valuations

A *place* \mathcal{D} of $\bar{\mathbb{K}}(C)$ in the affine chart $z = 1$ will be represented by a pair $(X(t), Y(t)) \in \bar{\mathbb{K}}[[t]]^2$ such that $(X(t) - X(0), Y(t))$ is a rational Puiseux expansion of $F(x, y, 1)$ regarded in $\mathbb{K}((x - X(0)))[y]$, as in Definition 3.3. The point $(X(0) : Y(0) : 1)$ of C is called the *center* of \mathcal{D} . From Proposition 3.4 a place \mathcal{D} induces a valuation as follows:

$$\text{val}_{\mathcal{D}}(A) := \text{val}_t(A(X(t), Y(t), 1)),$$

for any homogeneous polynomial A in $\bar{\mathbb{K}}[x, y, z]$.

Remark 4.1. This representation of places depends on ambient coordinates. For instance, a place \mathcal{D} centered at a regular point P of C has ramification index 1 if $F_y(P) \neq 0$, but ramification index ≥ 2 otherwise. However the valuation induced by a place does not depend on this representation.

A *divisor* D of a curve C is a symbolic sum of places multiplied by integers called *multiplicities*:

$$D = m_1 \mathcal{D}_1 + \cdots + m_s \mathcal{D}_s.$$

The *support* of D , denoted $\text{supp } D$, is the set of places which appear in the decomposition of D with non-zero multiplicities. A divisor D is *smooth* if the centers of the places of its support are regular points of the curve.

If \mathcal{E} is a finite subset of C , then $\mathcal{D}|\mathcal{E}$ will mean that \mathcal{D} is a place centered at a point of \mathcal{E} . If A is a homogeneous polynomial in $\bar{\mathbb{K}}[x, y, z]$ prime to F , then its associated divisor is

$$\text{Div}(A) = \sum_{\mathcal{D}|\mathcal{U}_{\mathbb{P}}(F,A)} \text{val}_{\mathcal{D}}(A) \mathcal{D}.$$

4.2. Adjoint divisor

Let us assume that the set of singular points of C , written $\text{Sing}(C)$, lies in the affine chart $z=1$. Let \mathcal{D} be a place represented by an expansion $(X(t), Y(t))$ as above. Following [7], the *local adjoint divisor* of C at a point $P \in \text{Sing}(C)$ is defined by

$$A_P := -\sum_{\mathcal{P}|P} \text{val}_t \left(\frac{e t^{e-1}}{F_y(X(t), Y(t), 1)} \right) \mathcal{P},$$

and the (*global*) *adjoint divisor* is

$$A := \sum_{P \in \text{Sing}(C)} A_P. \quad (4.1)$$

Remark 4.2. It is well known that A is positive. In fact, this can be seen from the following calculations. Let $((\mu_i(a), X_i(t) = \gamma_i t^{e_i}, Y_i(t)))_{i=1, \dots, s}$ represent the rational Puiseux expansions of F centered at a singular point P of C that we assume to be $(0:0:1)$ for simplicity. So the local factorization of F can be written

$$F(x, y, 1) = u(x, y) \prod_{i=1}^s \prod_{k=0}^{e_i-1} (y - Y_i(\zeta_i^k (x/\gamma_i)^{1/e_i})),$$

where u is invertible in $\mathbb{K}[[x, y]]$, and ζ_i is a primitive e_i -th root of unity. Then we calculate

$$\begin{aligned} & F_y(X_1(t), Y_1(t), 1) \\ &= u(X_1(t), Y_1(t)) \prod_{k=1}^{e_1-1} (Y_1(t) - Y_1(\zeta_1^k t)) \prod_{i \geq 2} \prod_{k=0}^{e_i-1} (Y_1(t) - Y_i(\zeta_i^k (\gamma_1 t^{e_1}/\gamma_i)^{1/e_i})) \end{aligned}$$

and we note that

$$\text{val}_t \left(\prod_{k=1}^{e_1-1} (Y_1(t) - Y_1(\zeta_1^k t^{e_1})) \right) \geq e_1 - 1,$$

which ensures that the multiplicity of the place $(X_1(t), Y_1(t))$ in A is positive.

Remark 4.3. It is usual to extend the valuation induced by a place \mathcal{D} to differential forms of C . The multiplicity of \mathcal{D} in the adjoint divisor is classically defined by

$$\text{val}_{\mathcal{D}} \left(\frac{dx}{F_y} \right) := \text{val}_t \left(\frac{e t^{e-1}}{F_y(X(t), Y(t), 1)} \right).$$

DEFINITION 4.4. A homogeneous polynomial $A \in \mathbb{K}[x, y, z]$ is adjoint to C if $\text{Div}_P(A) \geq A_P$ for all singular points P of C . It is said to be sharply adjoint to C if the inequalities are equalities for all singular points P .

Example 4.5. Let a and b be coprime positive integers such that $2 \leq a < b$, and take

$$F(x, y, z) := y^a z^{b-a} - x^b,$$

so $(0:0:1)$ is singular. $F(x, y, 1)$ is irreducible in $\bar{\mathbb{K}}[[x]][y]$. Its rational Puiseux expansion is

$$\begin{aligned} X(t) &= t^a \\ Y(t) &= t^b. \end{aligned}$$

Let \mathcal{D} denote the corresponding place. The regularity index of this expansion is b/a . We have $F_y(x, x^{b/a}, 1) = (a-1)x^{b(a-1)/a}$, $dx = at^{a-1} dt$, and

$$-\text{val}_t\left(\frac{at^{a-1}}{F_y(X(t), Y(t), 1)}\right) = -\text{val}_t\left(\frac{at^{a-1}}{(a-1)t^{b(a-1)}}\right) = b(a-1) - (a-1) = (b-1)(a-1),$$

that corresponds to valuation $(b-1)(a-1)/a$ in x . The latter is larger than the regularity index b/a in most cases.

Example 4.6. Let C be the curve defined by $y^2 - x^3 = 0$ in the affine chart $z = 1$. We recall that in [44] Keller proposed a notion of adjoint that is used in [48] for instance; see also [33, Definitions 2.12 and 2.13]. In order to compute Keller's adjoint divisor, we perform a single blow-up of equation $y = tx$. The strict transform \tilde{C} is defined by $t^2 - x = 0$. The exceptional divisor is defined by x : it intersects \tilde{C} at the origin with multiplicity $m = 2$. Consequently, the Keller adjoint divisor is:

$$\mathcal{A} = (m-1)m(0,0) = m(0,0).$$

Let

$$h := a(x) + b(x)y,$$

that rewrites

$$\tilde{h} := a(x) + xb(x)t,$$

in terms of the coordinates x, t . The condition $\text{Div}(h) \geq \mathcal{A}$ means that \tilde{h} vanishes at the origin with intersection multiplicity ≥ 2 . This is equivalent to

$$\text{val}_t(a(t^2) + b(t^2)t^3) \geq 2,$$

and then equivalent to $\text{val}_t(a(t^2)) \geq 1$.

On the other hand, the adjoint condition defined in (4.1) is obtained from the single place \mathcal{D} parametrized by $(X(t), Y(t)) = (t^2, t^3)$, that yields

$$\text{val}_{\mathcal{P}}\left(\frac{dx}{F_y}\right) = \text{val}_t\left(\frac{2t}{2t^3}\right) = -2.$$

It follows that h is adjoint if, and only if, $\text{val}_t(h(t^2, t^3)) \geq 2$. This is equivalent to $\text{val}_t(a(t^2)) \geq 2$. As expected, the adjoint condition (4.1) is the same as Keller's condition in this example.

4.3. Noether's condition

Let P be a singular point of C . Without loss of generality, up to a suitable linear change of coordinates, we may assume that $P = (0:0:1)$ and that the local equation of F in the neighborhood of P writes as follows:

$$F(x, y, 1) = u(x, y) \prod_{i=1}^m (y - \varphi_i(x)), \quad (4.2)$$

where $u \in \mathbb{K}[[x, y]]$ is invertible and where $\varphi_1, \dots, \varphi_m$ denote the Puiseux expansions of F regarded in $\mathbb{K}[[x]][y]$.

DEFINITION 4.7. (Noether's local condition) *Let F, G, H be homogeneous polynomials in $\mathbb{K}[x, y, z]$. When F and G are coprime, we say that Noether's condition is satisfied by the triple (F, G, H) at a point $P \in \mathbb{P}^2$ if H is in the ideal generated by F and G in $\bar{\mathbb{K}}[x, y, z]_P$.*

PROPOSITION 4.8. *Let P be a point of C , and consider two homogeneous polynomials A and B that are prime to F . If $\text{Div}_P(B) \geq \text{Div}_P(A) + A_P$ then Noether's condition is satisfied by the triple (F, A, B) at P .*

Proof. Without loss of generality we may assume that $P = (0:0:1)$ as above. Let $\varphi_1, \dots, \varphi_m$ denote the Puiseux expansions introduced in (4.2). By conjugation, the set $\{\varphi_1, \dots, \varphi_m\}$ is naturally partitioned into places $\mathcal{P}_1, \dots, \mathcal{P}_s$, with $s \leq m$. The ramification index of φ_i is written e_i . The assumption means that

$$\text{val}_{\mathcal{P}_i} \left(\frac{B}{A} \right) \geq -\text{val}_{\mathcal{P}_i} \left(\frac{dx}{F_y} \right),$$

for $i = 1, \dots, s$. For $i = 1, \dots, m$, this rewrites into

$$\text{val}_x \left(\frac{B}{A}(x, \varphi_i(x), 1) \right) - \text{val}_x(F_y(x, \varphi_i(x), 1)) \geq -\left(1 - \frac{1}{e_i}\right) > -1. \quad (4.3)$$

The Lagrange interpolation formula in

$$\bar{\mathbb{K}}\langle\langle x \rangle\rangle[y] / \left(\prod_{i=1}^m (y - \varphi_i(x)) \right)$$

gives

$$\left(\frac{B}{A} \right)(x, y, 1) \equiv c(x, y) \pmod{\prod_{i=1}^m (y - \varphi_i(x))}, \quad (4.4)$$

where

$$c(x, y) := \sum_{i=1}^m \frac{B(x, \varphi_i(x), 1)}{A(x, \varphi_i(x), 1)} \frac{\prod_{j \neq i} (y - \varphi_j(x))}{F_y(x, \varphi_i(x), 1)}. \quad (4.5)$$

Using that $\text{val}(a + b) \geq \min(\text{val}(a), \text{val}(b))$, Equation (4.3) implies

$$\text{val}_x(c(x, y)) \geq \min_i \text{val}_x \left(\frac{B}{A}(x, \varphi_i(x), 1) \frac{1}{F_y(x, \varphi_i(x), 1)} \right) > -1. \quad (4.6)$$

Since interchanging i and j in the right-hand side of Equation (4.5) leaves the expression of c unchanged, c is invariant under the action of transpositions, hence under any permutation of $\varphi_1, \dots, \varphi_m$. Consequently, c can be written as a polynomial in terms of elementary symmetric functions of $\varphi_1, \dots, \varphi_m$; see [47, Chapter IV, Section 6, Theorem 6.1] for instance. Since $\prod_{i=1}^m (y - \varphi_i(x)) \in \mathbb{K}[[x]][y]$ it follows that $c \in \mathbb{K}[[x]][y]$, hence that the left-hand side of Equation (4.6) is a nonnegative integer.

Equation (4.4) implies that $B(x, y, 1)$ belongs to the ideal $(F(x, y, 1), A(x, y, 1))$ regarded in $\mathbb{K}[[x]][y]$, that corresponds to Noether's condition at P . \square

The proof of Proposition 4.8 turns out to be remarkably elementary compared to other ones in the literature that appeal to desingularization trees or conductor ideals. Proposition 4.8 can be used in replacement of [3, Proposition 3.5] so that [3, Section 3] can be straightforwardly revisited into a complete elementary proof of the Brill–Noether method in characteristic zero.

4.4. Computation of the adjoint divisor

We conclude this section with a summary of the main results: the computation of the adjoint divisor and the rephrasing of the adjoint condition for the purpose of our main algorithm. But before it is useful to introduce an ad hoc definition for “generic coordinates”, that will occur several times in the sequel.

DEFINITION 4.9. *Let F and G be two coprime homogeneous polynomials in $\mathbb{K}[x, y, z]$. The coordinates x, y, z are said to be generic for F and G if the following conditions hold:*

- $\deg_y F = \deg F$,
- $R(x, z) := \text{Res}_y(F(x, y, z), G(x, y, z))$ has degree $\deg F \deg G$ in x .

We say the coordinates are generic for F if they are generic for F and F_y .

Note that $R(x, z)$ is always homogeneous of total degree $\deg F \deg G$. If the coordinates of F and G are generic, then $\mathcal{U}_{\mathbb{P}}(F, G)$ belongs to the affine chart $z = 1$.

Let us further recall that a linear form $\lambda(x, y)$ is said to be *primitive* for a finite set of points \mathcal{E} in \mathbb{A}^2 if it takes different values at different points of \mathcal{E} .

DEFINITION 4.10. *Let $F \in \mathbb{K}[x, y, z]$ be homogeneous, absolutely irreducible, and of total degree δ , such that the coordinates are generic for F , and that x is primitive for $\mathcal{U}_{\mathbb{A}}(F(x, y, 1), F_y(x, y, 1))$. Then, the series expansions of the adjoint divisor (4.1) are made of the following data:*

- $(\Delta_i)_{i=1, \dots, r}$ in $\mathbb{K}[b]$; we write $\mathbb{L}_i := \mathbb{K}[b] / (\Delta_i(b))$, and let β_i represent the class of b in \mathbb{L}_i ;
- For $i = 1, \dots, r$, $((\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t), \sigma_{i,j}))_{j=1, \dots, s_i})$ with $\mu_{i,j}$ of degree ≥ 1 in $\mathbb{L}_i[a]$, and

$$(X_{i,j}(t), Y_{i,j}(t)) \in (\mathbb{E}_{i,j}[[t]] / (t^{\sigma_{i,j}+1}))^2,$$

where $\mathbb{E}_{i,j} := \mathbb{L}_i[a] / (\mu_{i,j}(a))$;

Such that the following properties hold:

- The Δ_i are pairwise squarefree coprime factors of $\text{Disc}_y(F(x, y, 1))$ of multiplicity $m_i \geq 1$, for $i = 1, \dots, r$;
- $\mathcal{U}_{\mathbb{A}}(\Delta_1 \cdots \Delta_r)$ is the set of the abscissas of the singular locus of $\mathcal{U}_{\mathbb{A}}(F(x, y, 1))$;
- $\mu_{i,j}$ is monic and separable of degree ≥ 1 , for $i = 1, \dots, r$ and $j = 1, \dots, s_i$;
- $X_{i,j}(t) = \beta_i + \gamma_{i,j} t^{e_{i,j}}$, with $\gamma_{i,j}$ invertible in $\mathbb{E}_{i,j}$ and $e_{i,j} \geq 1$, for $i = 1, \dots, r$ and $j = 1, \dots, s_i$;
- The initial coefficient of $F_y(X_{i,j}(t), Y_{i,j}(t), 1)$ is invertible and we let

$$\sigma_{i,j} := \text{val}_t(F_y(X_{i,j}(t), Y_{i,j}(t), 1)),$$

for $i = 1, \dots, r$ and $j = 1, \dots, s_i$;

- For $i = 1, \dots, r$ and all root β of Δ_i , let π_{β} stand for the projection $\mathbb{L}_i \rightarrow \mathbb{K}[\beta]$, but also for its natural coefficient-wise extensions, then

$$((\pi_{\beta}(\mu_{i,j}(a)), \pi_{\beta}(X_{i,j}(t) - \beta_i), \pi_{\beta}(Y_{i,j}(t)))_{j=1, \dots, s_i})$$

are the truncations at precision $\sigma_{i,j} + 1$ of the rational Puiseux expansions of F regarded in $\mathbb{K}[\beta][[x - \beta]][[y]]$, with the meaning of Definition 3.8, and centered at the singular point of abscissa β .

PROPOSITION 4.11. *Let $F \in \mathbb{K}[x, y, z]$ be homogeneous, absolutely irreducible, and of total degree δ , such that the coordinates are generic for F , and that x is primitive for $\mathcal{U}_{\mathbb{A}}(F(x, y, 1), F_y(x, y, 1))$. Then, the series expansions of the adjoint divisor, defined in Equation (4.1) and represented as in Definition 4.10, can be computed with an expected number of $\tilde{O}(\delta^3)$ operations in \mathbb{K} .*

Proof. First we appeal to Proposition 3.22, which takes $\tilde{O}(\delta^3)$ operations in \mathbb{K} . Among the rational Puiseux expansions returned by Proposition 3.22, we drop the regular ones for free, using the fact that their regularity index is zero. We carry on the rest of the proof with the notation of Proposition 3.22 for simplicity.

Geometrically speaking, thanks to the assumptions, over each critical point β for the projection of the curve onto the x -axis, we retain only the expansions centered at the single point in $\mathcal{U}_{\mathbb{A}}(F(x, y, 1), F_y(x, y, 1), x - \beta)$.

Let $F_x := \frac{\partial F}{\partial x}$, we compute $F_x \bmod \Delta_i(x)$ for $i = 1, \dots, r$ with $\tilde{O}(\delta^3)$ operations thanks to Proposition 2.3. This yields $F_x(\beta_i, y, 1)$ for $i = 1, \dots, r$. The values $F_x(\beta_i, Y_{i,j}(0), 1)$ for $j = 1, \dots, s_i$ can be computed using Horner's method with

$$\tilde{O}\left(\delta \sum_{j=1}^{s_i} \deg \Delta_i \deg \mu_{i,j}\right) \quad (4.7)$$

operations in \mathbb{K} . By construction, the expansions $(\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t))$ occurring here are non-regular, so Proposition 3.9 yields the rough bound

$$\sum_{j=1}^{s_i} \deg \mu_{i,j} \leq m_i.$$

Consequently, the bound (4.7) simplifies to $\tilde{O}(\delta m_i \deg \Delta_i)$. The sum of these bounds for $i = 1, \dots, r$ is $\tilde{O}(\delta^3)$.

For $i = 1, \dots, r$ and $j = 1, \dots, s_i$ we consider the preimage $f_{i,j}(a)$ of $F_x(\beta_i, Y_{i,j}(0), 1)$ in $\mathbb{L}_i[a]_{<\deg \mu_{i,j}}$. Thanks to Theorem 2.6 applied to \mathbb{L}_i , the panoramic evaluation of the zero-tests of

$$\text{Res}_a(f_{i,j}(a), \mu_{i,j}(a)) \in \mathbb{L}_i$$

for $j = 1, \dots, s_i$ yields a partial factor decomposition of Δ_i into

$$\Delta_i = \Delta_{i,1} \cdots \Delta_{i,r_i}$$

such that

$$\text{Res}_a(f_{i,j}(a), \mu_{i,j}(a))$$

is invertible or zero modulo each $\Delta_{i,k}$ for $k = 1, \dots, r_i$. By Theorem 2.6 and Proposition 3.9, this panoramic evaluation takes

$$\tilde{O}\left(\deg \Delta_i \sum_{j=1}^{s_i} \deg \mu_{i,j}\right) = \tilde{O}(m_i \deg \Delta_i)$$

operations in \mathbb{K} . For each $j = 1, \dots, s_i$ we reduce $(\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t))$ modulo $\Delta_{i,1}, \dots, \Delta_{i,r_i}$ simultaneously in softly linear time by Proposition 2.3. We drop the expansions whose centers are not a root of F_x (because these expansions represent smooth germs of C). \square

With the notation of Definition 4.10, for $i = 1, \dots, r$ and $j = 1, \dots, s_i$, we introduce

$$\tau_{i,j} := \text{val}_i(F_y(X_{i,j}(t), Y_{i,j}(t), 1)) - (e_{i,j} - 1), \quad (4.8)$$

that corresponds to the common multiplicity of the places represented by $(\Delta_i(b), \mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t), \sigma_{i,j})$ in the support of the adjoint divisor \mathcal{A} . Since \mathcal{A} is positive, the $\tau_{i,j}$ are positive.

PROPOSITION 4.12. *Given A as in Definition 4.10, a homogeneous polynomial $A \in \mathbb{K}[x, y, z]$ is adjoint to the curve C defined by $F = 0$ if, and only if,*

$$\text{val}_t(A(X_{i,j}(t), Y_{i,j}(t), 1)) \geq \tau_{i,j} \quad (4.9)$$

for $i = 1, \dots, r$ and $j = 1, \dots, s_i$.

It is sharply adjoint to C if, and only if, Inequalities (4.9) are equalities and the coefficient of degree $\tau_{i,j}$ in $A(X_{i,j}(t), Y_{i,j}(t), 1)$ is invertible in $\mathbb{E}_{i,j}$, for $i = 1, \dots, r$ and $j = 1, \dots, s_i$.

Proof. This is a consequence of Definition 4.4 and the definition of divisors. \square

PROPOSITION 4.13. *Given A as in Definition 4.10, testing if a homogeneous polynomial $A \in \mathbb{K}[x, y, z]$ of degree $< \delta$ in y and total degree $\leq d$ is sharply adjoint to the curve C defined by $F = 0$ takes $\tilde{O}(\delta \max(d, \delta^2))$ operations in \mathbb{K} .*

Proof. We compute $A(x, y, 1) \bmod \Delta_i(x)^{m_i+1}$ for $i = 1, \dots, r$ thanks to fast multi-remaindering with $\tilde{O}(\delta \max(d, \delta^2))$ operations in \mathbb{K} , by Proposition 2.3. For $i = 1, \dots, s$, the image of A in

$$(\mathbb{L}_i[[x - \beta_i]] / (x - \beta_i)^{m_i+1})[y],$$

written A_i , can be computed in softly linear time by Proposition 2.5. Note that

$$\tau_{i,j} \leq \text{val}_t(F_y(X_{i,j}(t), Y_{i,j}(t), 1)) \leq m_i.$$

Via Horner's method, the evaluation of $A_i(X_{i,j}(t), Y_{i,j}(t), 1)$ at precision $\tau_{i,j} + 1$ takes time

$$\tilde{O}(\delta \deg \Delta_i \deg \mu_{i,j} (\tau_{i,j} + 1)) = \tilde{O}(\delta \deg \Delta_i \deg \mu_{i,j} \text{val}_t(F_y(X_{i,j}(t), Y_{i,j}(t), 1))).$$

The sum of these costs for $i = 1, \dots, s$ and $j = 1, \dots, s_i$ yields

$$\begin{aligned} \tilde{O} \left(\delta \sum_{i=1}^s \deg \Delta_i \sum_{j=1}^{s_i} \deg \mu_{i,j} \text{val}_t(F_y(X_{i,j}(t), Y_{i,j}(t), 1)) \right) &= \tilde{O} \left(\delta \sum_{i=1}^s m_i \deg \Delta_i \right) \\ &= \tilde{O}(\delta^3) \end{aligned}$$

operations in \mathbb{K} , thanks to Proposition 3.9. \square

Example 4.14. (Continued from Example 3.23) Let us take $\mathbb{K} := \mathbb{Q}$ and

$$F(x, y, z) := y^7 - x(x^3 + y^2z + xyz)^2,$$

that is absolutely irreducible. The point $(0:0:1)$ is the only singular point of the curve $C = \mathcal{U}_{\mathbb{P}}(F)$. The adjoint divisor is made of the rational Puiseux expansions computed in Example 3.23 that are centered at $(0:0:1)$.

5. DEGREE OF THE DENOMINATOR

Given a plane projective curve C and a smooth positive divisor D , this section deals with the existence of homogeneous polynomials $H \in \mathbb{K}[x, y, z]$ that are sharply adjoint to C , that satisfy $\text{Div}(H) \geq D$, and that have a total degree d as small as possible. Such polynomials will serve to build common denominators of Riemann–Roch spaces. Such a specific denominator will yield a simpler computation of $\text{Div}(H) - A$ in the context of the Brill–Noether method.

5.1. Residue theorem

In what follows we shall use the well known Residue Theorem in the algebraic framework, which is the cornerstone of the proof of the Brill–Noether method. In the literature, the Residue Theorem is often stated and proved for ordinary curves, see [26, Chapter 8], [48, Section 3], [3, Theorem 3.7]. A detailed proof in the general setting can be found in Haché’s PhD thesis [36, Théorème 2.6.10]. Here we state this theorem in the general context, without repeating a proof. However, we point out that the proof of [3, Theorem 3.7] for the ordinary case can be straightforwardly extended to the non-ordinary case, using our Proposition 4.8 instead of [3, Proposition 3.6].

We recall that two divisors D and D' of C are said to be *linearly equivalent*, written $D \equiv D'$, if there exists a rational function $h \in \mathbb{K}(C)$ such that $D = D' + \text{Div}(h)$.

THEOREM 5.1. (Residue Theorem) *Let D and D' be two divisors of the curve C defined by $F = 0$, such that $D \equiv D'$ and $D' \geq 0$. Suppose that H is a homogeneous polynomial prime to F such that $\text{Div}(H) = D + A + R$ for a positive divisor R . Then, there exists a homogeneous polynomial H' , prime to F , of the same degree as H , such that $\text{Div}(H') = D' + A + R$.*

We appeal to the Residue Theorem only once in this paper for the following lemma, that gives a condition for a function in $\mathbb{K}(C)$ to be regular in some affine chart.

LEMMA 5.2. *Let L be a homogeneous degree one polynomial such that $\text{Div}(L)$ is smooth. Then, for any positive integer d , any non-zero element of $\mathcal{L}(d \text{Div}(L) - A)$ admits a rational function representation in the form H/L^d , where H is a homogeneous polynomial of degree d .*

Proof. We set $D := d \text{Div}(L) - A$ and consider $h \neq 0$ in $\mathcal{L}(D)$ (if $\mathcal{L}(D) = \{0\}$ then the proof is trivial). By construction, we have

$$D' := D + \text{Div}(h) \geq 0.$$

We apply Theorem 5.1 to D' and the decomposition

$$\text{Div}(L^d) = d \text{Div}(L) = D + A + R,$$

where $R := 0$. This yields a homogeneous polynomial H of degree d prime to F such that

$$\text{Div}(H) = D' + A = D' - D + d \text{Div}(L).$$

Consequently, we have

$$\text{Div}(H/L^d) = D' - D = \text{Div}(h).$$

Then $\text{Div}((H/L^d)/h)$ is zero, whence $(H/L^d)/h$ is a constant, by [62, Corollary 1.3.4]. Finally, we have shown that h is a \mathbb{K} -multiple of H/L^d in $\mathbb{K}(C)$. \square

Let A be the adjoint divisor of C , defined in Equation (4.1), and recall that δ denotes the degree of the curve C . The genus g of C is

$$g := \frac{(\delta-1)(\delta-2) - \deg A}{2}. \tag{5.1}$$

This relation is proved in [32, Theorem 11] using the definition of the adjoint divisor in terms of conductor ideals. Since this definition is equivalent to the one in Equation (4.1) by [27, Section 4], this relation for the genus of the curve applies here. We also refer the reader to [35, Remark 4.9], where the same formula is given involving Keller’s notion of adjoint, and to [56], where the formula is stated in terms of differential forms.

5.2. Degree bound

Our degree bound for sharply adjoint denominators of Riemann–Roch spaces is presented in the following proposition.

PROPOSITION 5.3. *Assume that the cardinality of \mathbb{K} is infinite. Let D be a positive divisor of C , and let*

$$d \geq \frac{(\delta-1)(\delta-2) + \deg D}{\delta}.$$

Then, there exists a homogeneous polynomial H prime to F of degree d and such that

$$\operatorname{Div}(H) \geq D + A$$

and $\operatorname{Div}(H) - D - A$ is smooth.

Proof. Fix a homogeneous polynomial L of degree 1 such that $\operatorname{Div}(L)$ is smooth. By Bézout's theorem [26, Section 5.3] we have $\deg(\operatorname{Div}(L)) = \delta$. We set

$$E := D + A.$$

The assumption on d and Equation (5.1) lead to

$$\deg(d \operatorname{Div}(L) - E) = d\delta - \deg D - \deg A \geq (\delta-1)(\delta-2) - \deg A = 2g.$$

Let P_1, \dots, P_r denote the singular points of C and let $\mathcal{D}_{i,1}, \dots, \mathcal{D}_{i,s_i}$ be the places centered at P_i for $i = 1, \dots, r$. We can apply [26, Chapter 8, Corollary 3]: even if this corollary in [26] is stated for ordinary curves, it applies without change for curves with arbitrary singularities as explained in [27, Section 4]. Alternatively, we refer the reader to [18, Theorem 4.9.7]. We fit in a situation where the Riemann–Roch theorem is an equality, that is

$$\forall 1 \leq i \leq r, \forall 1 \leq j \leq s_i, \quad \dim \mathcal{L}(d \operatorname{Div}(L) - E - \mathcal{D}_{i,j}) = \dim \mathcal{L}(d \operatorname{Div}(L) - E) - 1.$$

Since $|\mathbb{K}|$ is infinite, there exist functions $h \in \mathcal{L}(d \operatorname{Div} L - E)$ which are not contained in any of the $\mathcal{L}(d \operatorname{Div} L - E - \mathcal{D}_{i,j})$ for any pair (i, j) . From Lemma 5.2 such a function h admits a rational function representation of the form $h = H/L^d$. By construction of h ,

$$\operatorname{Div}(H) - D - A = \operatorname{Div}(h) + d \operatorname{Div}(L) - E$$

is positive and smooth. □

5.3. Probability bound

If D is a smooth divisor (that will be the case in our main algorithm), then Proposition 5.3 ensures the existence of polynomials H such that $\operatorname{Div}(H) \geq D + A$ and H is sharply adjoint. The next lemma establishes that such polynomials H can be found with high probability in a suitable vector space.

LEMMA 5.4. *Let D be a smooth positive divisor of a curve $C = \mathcal{U}_{\mathbb{P}}(F)$ with F of total degree δ and such that the coordinates are generic for F . Let \mathcal{H} denote the \mathbb{K} -vector space of homogeneous polynomials $H \in \mathbb{K}[x, y, z]$ of total degree*

$$d := \left\lceil \frac{(\delta-1)(\delta-2) + \deg D}{\delta} \right\rceil,$$

of degree $< \delta$ in y , and such that $\text{Div}(H) \geq D + A$; by convention the zero polynomial is included in \mathcal{H} . Let H_1, \dots, H_l denote a basis of \mathcal{H} and let \mathcal{S} be a finite subset of \mathbb{K} . Then, for (a_1, \dots, a_l) taken at random in \mathcal{S}^l , the probability that $a_1 H_1 + \dots + a_l H_l$ is not sharply adjoint is

$$\leq \frac{(\delta-1)(\delta-2)}{|\mathcal{S}|}.$$

Proof. Set $H_a := a_1 H_1 + \dots + a_l H_l$. Let us write $A = \sum_{i=1}^s \tau_i \mathcal{D}_i$ into the sum of pairwise distinct places (with $\tau_i \geq 1$), and let $(X_i(t), Y_i(t))$ represent the rational Puiseux expansion of \mathcal{D}_i . If the a_i are regarded as variables, then H_a is sharply adjoint by Proposition 5.3, so the polynomial

$$\Sigma(a_1, \dots, a_l) := \prod_{i=1}^s \text{coeff}(H_a(X_i(t), Y_i(t), 1), \tau_i)$$

is non-zero, where $\text{coeff}(H_a(X_i(t), Y_i(t), 1), \tau_i)$ represents the coefficient of degree τ_i in $H_a(X_i(t), Y_i(t), 1)$.

Then, regarding the a_i as values in \mathcal{S} , the polynomial H_a is sharply adjoint if, and only if, $\Sigma(a_1, \dots, a_l) \neq 0$. The total degree of Σ in the a_i is

$$\leq s \leq \deg A \leq (\delta-1)(\delta-2).$$

The conclusion follows from the well known Schwartz–Zippel lemma; see [28, Lemma 6.44] for instance. \square

6. DATA STRUCTURES

Before presenting the main algorithm, it remains to describe the data structures for divisors, along with their main properties.

6.1. Primitive elements

A *primitive element representation* of a finite set \mathcal{E} of points in \mathbb{A}^2 is the data of:

- (λ_x, λ_y) in $\bar{\mathbb{K}}^2$ such that the linear form $\lambda := \lambda_x x + \lambda_y y$ separates the points of \mathcal{E} . This means that the form takes different values at different points of \mathcal{E} (as in Section 4.4).
- A polynomial θ in $\bar{\mathbb{K}}[t]$ whose roots are the values of λ at the points of \mathcal{E} , that is

$$\theta(t) := \prod_{P \in \mathcal{E}} (t - \lambda(P)).$$

So θ is monic and separable of degree $|\mathcal{E}|$.

- Polynomials u and v in $\bar{\mathbb{K}}[t]$ of degree $< |\mathcal{E}|$ such that

$$\mathcal{E} = \{(u(\zeta), v(\zeta)) : \theta(\zeta) = 0\}.$$

The form λ is said to be *primitive* for \mathcal{E} . Note that such a representation is uniquely determined by λ . If $(\lambda_x, \lambda_y) \in \mathbb{K}^2$ and if $\theta, u, v \in \mathbb{K}[t]$, then the primitive element representation is said to be *defined over* \mathbb{K} .

LEMMA 6.1. *Let \mathcal{S} be a finite subset of \mathbb{K} . The probability that a random matrix $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in \mathcal{S} does not make the linear form x primitive for $M(\mathcal{E})$ is $\leq \binom{|\mathcal{E}|}{2} / |\mathcal{S}|$.*

Proof. The proof is rather elementary and is detailed in [3, Lemma 4.1] for instance. \square

PROPOSITION 6.2. *Given a primitive element representation of \mathcal{E} over \mathbb{K} by $\lambda := \lambda_x x + \lambda_y y$, and polynomials u, v , and θ as above. Let $(\tilde{\lambda}_x, \tilde{\lambda}_y) \in \mathbb{K}^2$, let M denote a 3×3 invertible matrix, and let*

$$\mathcal{E}^\# := \{(a : b : 1) : (a, b) \in \mathcal{E}\} \subset \mathbb{P}^2.$$

We can check if $M(\mathcal{E}^\#)$ is in the affine chart $z = 1$ and if $\tilde{\lambda} := \tilde{\lambda}_x x + \tilde{\lambda}_y y$ is primitive for the set of points $\tilde{\mathcal{E}}$ representing $M(\mathcal{E}^\#)$ in \mathbb{A}^2 , and if so compute the corresponding primitive element representation of $\tilde{\mathcal{E}}$ with $O(|\mathcal{E}|^\omega)$ field operations.

Proof. The proof is essentially classical and is detailed in [3, Proposition 4.5]. \square

6.2. Smooth divisors

A smooth divisor will naturally be stored as the pair of the representations of D_- and D_+ , where D_- and D_+ are positive divisors whose sum is D . So we focus on the representation of a positive smooth divisor D defined over \mathbb{K} . Minimally, D can be represented by its centers (in one-to-one correspondence with the places in its support) and the respective multiplicities, that form a multi-set. If P is a center of D of multiplicity m , then the effective version of the implicit function theorem allows the computation of the power series expansions of the germ of curve defined by C at P at order m . The set of these expansions for each center of D constitutes a more detailed representation of D .

6.2.1. Multi-set representation

We will use the following representation of divisors, that is different from the one used in [2, 3], and turns out to be more flexible and efficient for practice because several computations can be performed independently of the multiplicities.

DEFINITION 6.3. *Let $\mathcal{E}_1, \dots, \mathcal{E}_s$ be pairwise disjoint sets in the affine chart $z = 1$ of C , defined over \mathbb{K} , parametrized by the same primitive element $\lambda_x x + \lambda_y y$, and such that*

$$\begin{vmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} \\ \lambda_x & \lambda_y \end{vmatrix}$$

is invertible at all the points of $\mathcal{E}_1 \cup \dots \cup \mathcal{E}_s$. Then, the set of pairs (\mathcal{E}_i, m_i) is a multi-set representation of the smooth positive divisor $D = m_1 \mathcal{E}_1 + \dots + m_s \mathcal{E}_s$.

For convenience, we will also write the support of D in terms of its centers, that is as

$$\text{supp } D := \mathcal{E}_1 \cup \dots \cup \mathcal{E}_s.$$

LEMMA 6.4. *Let \mathcal{S} be a finite subset of \mathbb{K} . Let D be a smooth positive divisor, let M be a 3×3 matrix with random entries in \mathcal{S} . If M is invertible then the probability that $M^{-1}(D)$ is not in the affine chart $z = 1$ or that x is not primitive for the corresponding affine part of $M^{-1}(D)$ is*

$$\leq \frac{3|\text{supp } D|^2}{|\mathcal{S}|}.$$

Proof. The proof is straightforward and the details can be found in [3, Lemma 4.14]. \square

LEMMA 6.5. Let $f \in \mathbb{K}[x, y]$ be of total degree δ , let $(\lambda_x, \lambda_y) \in \mathbb{K}^2$, and let $\chi_i \in \mathbb{K}[t]$ and $u_i, v_i \in \mathbb{K}[t]_{< \deg \chi_i}$ for $i = 1, \dots, s$ be such that $\lambda_x u_i(t) + \lambda_y v_i(t) = t \bmod \chi_i(t)$ holds and that the χ_i are pairwise coprime. Then, $f(u_i(t), v_i(t)) \bmod \chi_i(t)$ can be computed with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \sum_{i=1}^s \deg \chi_i\right)$$

operations in \mathbb{K} .

Proof. By Proposition 2.4 the polynomials $\chi := \chi_1 \cdots \chi_s$ and $u, v \in \mathbb{K}[t]_{< \deg \chi}$ such that $u \bmod \chi_i = u_i$ and $v \bmod \chi_i = v_i$ for $i = 1, \dots, s$, can be computed with $\tilde{O}(\deg \chi)$ operations in \mathbb{K} . Then $w := f(u, v) \bmod \chi$ is obtained with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg \chi\right)$$

further operations in \mathbb{K} by Lemma 2.2. Proposition 2.3 then yields $w \bmod \chi_i$ for $i = 1, \dots, s$ with $\tilde{O}(\deg \chi)$ further operations in \mathbb{K} . \square

PROPOSITION 6.6. Let D be a smooth positive divisor of C represented by a multi-set, let M denote an invertible 3×3 matrix over \mathbb{K} , and let $(\tilde{\lambda}_x, \tilde{\lambda}_y) \in \mathbb{K}^2$. We can test if $M(D)$ has its support in the affine chart $z = 1$, if $\tilde{\lambda}_x x + \tilde{\lambda}_y y$ is primitive for the affine part of $M(D)$, and if so compute the corresponding multi-set representation with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} |\text{supp } D| + |\text{supp } D|^\omega\right)$$

operations in \mathbb{K} .

Proof. With the notation of Definition 6.3, for $i = 1, \dots, s$ let \mathcal{E}_i be the sets of the centers of D , represented by $\lambda_x x + \lambda_y y$, u_i , v_i , and θ_i . Following the notation of Proposition 6.2, let $\mathcal{E}_i^\#$ denote the canonical image of \mathcal{E}_i in \mathbb{P}^2 , and let $\tilde{\mathcal{E}}_i$ denote the affine part of $M(\mathcal{E}_i^\#)$: we can check if $M(\mathcal{E}_i^\#)$ is in the affine chart $z = 1$, test if $\tilde{\lambda} = \tilde{\lambda}_x x + \tilde{\lambda}_y y$ is primitive for $\tilde{\mathcal{E}}_i$, and if so, compute the corresponding representation \tilde{u}_i , \tilde{v}_i , and $\tilde{\theta}_i$ with $O((\deg \theta_i)^\omega)$ operations.

In order to check if $\tilde{\lambda}$ is primitive for $\bigcup_{i=1}^s \tilde{\mathcal{E}}_i$, it suffices to verify that $\tilde{\theta} := \prod_{i=1}^s \tilde{\theta}_i$ is separable, that takes softly linear time.

Then, we evaluate $\lambda_y \frac{\partial F}{\partial x}(x, y, 1) - \lambda_x \frac{\partial F}{\partial y}(x, y, 1)$ at $(\tilde{u}_i, \tilde{v}_i)$ modulo $\tilde{\theta}_i$ for $i = 1, \dots, s$, and test if the result is prime to $\tilde{\theta}_i$, with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} |\text{supp } D|\right)$$

further operations in \mathbb{K} , by Lemma 6.5. \square

6.2.2. Expansions of multi-set representations

Given a regular point P of C , via the implicit function theorem, Newton's operator is a classical way to compute power series expansions of the germ of curve centered at P for any arbitrary truncation order. In the following paragraphs we analyze the complexity for computing D in terms of a list of series expansions.

DEFINITION 6.7. Given a subset of regular points \mathcal{E} of C defined over \mathbb{K} and represented by a primitive element $\lambda := \lambda_x x + \lambda_y y$ and polynomials θ, u, v . The series expansion of the divisor $D = m \mathcal{E}$ is the data of

$$(X(t), Y(t)) \in (\mathbb{L}[[t]] / (t^m))^2,$$

where

$$\mathbb{L} := \mathbb{K}[b] / (\theta(b)),$$

and such that $F(X(t), Y(t), 1) = O(t^m)$, $X(t) = u(\beta) + t$, $Y(0) = v(\beta)$, where F is the defining polynomial of the curve C and β denotes the class of b in \mathbb{L} .

For a general positive smooth divisor D of the form $m_1 \mathcal{E}_1 + \dots + m_s \mathcal{E}_s$ given by a multi-set, its corresponding series expansions are the set of the series expansions of $m_i \mathcal{E}_i$ for $i = 1, \dots, s$.

LEMMA 6.8. Let $f \in \mathbb{K}[x, y]$ be of total degree δ . Let $m_i \in \mathbb{N}_{>0}$, $\theta_i \in \mathbb{K}[b]$, $\mathbb{L}_i := \mathbb{K}[b] / (\theta_i(b))$,

$$(X_i(t), Y_i(t)) \in (\mathbb{L}_i[[t]] / (t^{m_i}))^2,$$

for $i = 1, \dots, s$ represent the series expansions of a positive smooth divisor D , as above. Then, $f(X_i(t), Y_i(t))$ for $i = 1, \dots, s$ can be computed with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\right)$$

operations in \mathbb{K} .

Proof. We follow the notation of Proposition 2.5, and compute $u_i(x) := \Gamma_{\theta_i, m_i}(X_i)$, $v_i(x) := \Gamma_{\theta_i, m_i}(Y_i)$ and $\chi_i := \theta_i^{m_i}$. Thanks to Lemma 6.5 we obtain $w_i := f(u_i(t), v_i(t)) \bmod \chi_i$, for $i = 1, \dots, s$, with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \sum_{i=1}^s \deg \chi_i\right) = \tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\right)$$

operations in \mathbb{K} . Then, we obtain $f(X_i(t), Y_i(t))$ as $\Gamma_{\theta_i, m_i}^{-1}(w_i)$. Evaluating Γ_{θ_i, m_i} and its inverse takes softly linear time by Proposition 2.5. \square

LEMMA 6.9. Let D be a smooth positive divisor given by series expansions. Series expansions of $2D$ can be computed with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\right)$$

operations in \mathbb{K} .

Proof. Let $D = m_1 \mathcal{E}_1 + \dots + m_s \mathcal{E}_s$ be as above. Let u_i, v_i, θ_i denote the parametrization of \mathcal{E}_i , and let $(X_i(t), Y_i(t)) \in (\mathbb{L}_i[[t]] / (t^{m_i}))^2$ with $\mathbb{L}_i := \mathbb{K}[b] / (\theta_i(b))$ stand for the expansion of $m_i \mathcal{E}_i$, for $i = 1, \dots, s$. Let $\lambda_x x + \lambda_y y$ denote the common primitive element of the \mathcal{E}_i .

The usual Newton iteration

$$\begin{pmatrix} \hat{X}_i \\ \hat{Y}_i \end{pmatrix} := \begin{pmatrix} X_i \\ Y_i \end{pmatrix} - \begin{pmatrix} \frac{\partial F}{\partial x}(X_i, Y_i) & \frac{\partial F}{\partial y}(X_i, Y_i) \\ \lambda_x & \lambda_y \end{pmatrix}^{-1} \begin{pmatrix} F(X_i, Y_i) \\ \lambda_x X_i + \lambda_y Y_i - t \end{pmatrix} + O(t^{2m_i})$$

yields the expansion of $2m_i \mathcal{E}_i$. The evaluations of F , $\frac{\partial F}{\partial x}$, and $\frac{\partial F}{\partial y}$ at $(X_i(t), Y_i(t))$ at precision $2m_i$, for $i = 1, \dots, s$, amount to

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\right)$$

operations in \mathbb{K} by Lemma 6.8. \square

PROPOSITION 6.10. Given a multi-set representation of a positive smooth divisor D , the corresponding series expansions can be computed with

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\right)$$

operations in \mathbb{K} .

Proof. We still write $D = m_1 \mathcal{E}_1 + \dots + m_s \mathcal{E}_s$ as above. Let K be the first integer such that $m_i < 2^{K+1}$ for $i = 1, \dots, s$. For $k = 1, \dots, K$, we introduce

$$D_k := \sum_{\substack{i=1 \\ 2^k \leq m_i < 2^{k+1}}}^s m_i \mathcal{E}_i.$$

The representation of the \mathcal{E}_i straightforwardly yields the series expansions of the smooth divisor

$$E_k := \sum_{\substack{i=1 \\ 2^k \leq m_i < 2^{k+1}}}^s \mathcal{E}_i.$$

Then, we compute $2E_k, 4E_k, \dots, 2^{k+1}E_k$ via Lemma 6.9. The series expansions of D_k are deduced from those of $2^{k+1}E_k$ by truncating the series at the precisions prescribed by the m_i . The total cost amounts to

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\right)$$

because $k = O(\log(\deg D))$. The sum of these costs for $k = 1, \dots, K$ yields the claimed bound since $K = O(\log(\deg D))$. \square

6.3. Sum and subtraction

In this subsection we consider two smooth positive divisors D_1 and D_2 represented by $((\theta_{1,i}, u_{1,i}, v_{1,i}, m_{1,i}))_{i=1, \dots, s_1}$ and $((\theta_{2,i}, u_{2,i}, v_{2,i}, m_{2,i}))_{i=1, \dots, s_2}$, as in Definition 6.3. In order to compute $D_1 + D_2$ and the positive part $[D_1 - D_2]_+$ of $D_1 - D_2$, we first treat separately the common points of the supports of D_1 and D_2 , and then the remaining points.

LEMMA 6.11. *Given two smooth positive divisors D_1 and D_2 in multi-set representation, sharing the same primitive element $\lambda := \lambda_x x + \lambda_y y$, and such that*

$$\prod_{i=1}^{s_1} \theta_{1,i} = \prod_{i=1}^{s_2} \theta_{2,i},$$

we can check if λ is primitive for $D := D_1 + D_2$, and, if so, compute the corresponding multi-set representation with

$$\tilde{O}(|\text{supp } D|)$$

operations in \mathbb{K} .

Proof. We proceed by induction on s_1 . If $s_1 = 1$, then we compute $u_{1,1} \bmod \theta_{2,i}$ and $v_{1,1} \bmod \theta_{2,i}$ for $i = 1, \dots, s_2$ in softly linear time by Proposition 2.3. The sum D can be parametrized by λ if, and only if, $u_{1,1} - u_{2,i} = 0 \bmod \theta_{2,i}$ and $v_{1,1} - v_{2,i} = 0 \bmod \theta_{2,i}$. A multi-set representation of D is obtained as

$$((\theta_{2,i}, u_{2,i}, v_{2,i}, m_{2,i} + m_{1,1}))_{i=1, \dots, s_2}.$$

If $s_1 \geq 2$ then we set $h := \lfloor s_1/2 \rfloor$. We define D_1^{lo} from $((\theta_{1,i}, u_{1,i}, v_{1,i}, m_{1,i}))_{i=1, \dots, h}$ and D_1^{hi} from $((\theta_{1,i}, u_{1,i}, v_{1,i}, m_{1,i}))_{i=h+1, \dots, s_1}$. We compute $\chi_1^{\text{lo}} := \prod_{i=1}^h \theta_{1,i}$ and $\chi_1^{\text{hi}} := \prod_{i=h+1}^{s_1} \theta_{1,i}$ in softly linear time.

Then $\theta_{2,i}^{\text{lo}} := \gcd(\chi_1^{\text{lo}}, \theta_{2,i})$ and $\theta_{2,i}^{\text{hi}} := \theta_{2,i} / \theta_{2,i}^{\text{lo}}$ for $i = 1, \dots, s_2$ can be computed in softly linear time via Proposition 2.3. We define D_2^{lo} to be

$$((\theta_{2,i}^{\text{lo}}, u_{2,i} \text{ rem } \theta_{2,i}^{\text{lo}}, v_{2,i} \text{ rem } \theta_{2,i}^{\text{lo}}, m_{2,i}))_{i=1, \dots, s_2}$$

and D_2^{hi} to be

$$((\theta_{2,i}^{\text{hi}}, u_{2,i} \text{ rem } \theta_{2,i}^{\text{hi}}, v_{2,i} \text{ rem } \theta_{2,i}^{\text{hi}}, m_{2,i}))_{i=1, \dots, s_2}.$$

Of course we discard tuples that represent empty sets. Finally, we compute $D_1^{\text{lo}} + D_2^{\text{lo}}$ and $D_1^{\text{hi}} + D_2^{\text{hi}}$ recursively, and concatenate the results. The claimed complexity bound follows from a classical induction. \square

PROPOSITION 6.12. *Given two smooth positive divisors D_1 and D_2 in multi-set representation, and sharing the same primitive element $\lambda := \lambda_x x + \lambda_y y$, one can check if λ is primitive for $D := D_1 + D_2$, and, if so, compute the corresponding multi-set representation with*

$$\tilde{O}(|\text{supp } D_1| + |\text{supp } D_2|)$$

operations in \mathbb{K} .

Proof. We compute $\chi_2 := \prod_{i=1}^{s_2} \theta_{2,i}$ and then $\chi_2 \bmod \theta_{1,i}$ for $i = 1, \dots, s_1$ with $\tilde{O}(|\text{supp } D_1| + |\text{supp } D_2|)$ operations in \mathbb{K} by Proposition 2.3. Then we deduce

$$\gamma_i := \gcd(\chi_2 \text{ rem } \theta_{1,i}, \theta_{1,i})$$

for $i = 1, \dots, s_1$ in softly linear time. For $i = 1, \dots, s_1$ we set $\check{\theta}_{1,i} := \theta_{1,i} / \gamma_i$, $\check{u}_{1,i} := u_{1,i} \text{ rem } \check{\theta}_{1,i}$ and $\check{v}_{1,i} := v_{1,i} \text{ rem } \check{\theta}_{1,i}$. The tuples

$$((\check{\theta}_{1,i}, \check{u}_{1,i}, \check{v}_{1,i}, m_{1,i}))_{i=1, \dots, s_1}$$

represent a smooth positive divisor written $\check{D}_1 \leq D_1$. The tuples

$$((\gamma_i, u_{1,i} \text{ rem } \gamma_i, v_{1,i} \text{ rem } \gamma_i, m_{1,i}))_{i=1, \dots, s_1}$$

represent another smooth positive divisor written $\hat{D}_1 \leq D_1$. Note that \hat{D}_1 and \check{D}_1 have disjoint support and that $D_1 = \hat{D}_1 + \check{D}_1$ holds. The total cost for computing this decomposition is $\tilde{O}(|\text{supp } D_1| + |\text{supp } D_2|)$.

Then, we compute $\gamma := \prod_{i=1}^{s_1} \gamma_i = \gcd(\chi_1, \chi_2)$ and $\delta_i := \gcd(\gamma, \theta_{2,i})$ for $i = 1, \dots, s_2$, in softly linear time, again via Proposition 2.3. For $i = 1, \dots, s_2$ we set $\check{\theta}_{2,i} := \theta_{2,i} / \delta_i$, $\check{u}_{2,i} := u_{2,i} \text{ rem } \check{\theta}_{2,i}$ and $\check{v}_{2,i} := v_{2,i} \text{ rem } \check{\theta}_{2,i}$. The tuples

$$((\check{\theta}_{2,i}, \check{u}_{2,i}, \check{v}_{2,i}, m_{2,i}))_{i=1, \dots, s_2}$$

represent a smooth positive divisor written $\check{D}_2 \leq D_2$. The tuples

$$((\delta_i, u_{2,i} \text{ rem } \delta_i, v_{2,i} \text{ rem } \delta_i, m_{2,i}))_{i=1, \dots, s_2}$$

represent a smooth positive divisor written $\hat{D}_2 \leq D_2$. Note that \hat{D}_2 and \check{D}_2 have disjoint support and that $D_2 = \hat{D}_2 + \check{D}_2$ holds.

Since \hat{D}_1 and \hat{D}_2 have the same product of defining polynomials, namely γ , Lemma 6.11 ensures that $\hat{D}_1 + \hat{D}_2$ can be computed with $\tilde{O}(|\text{supp } \hat{D}_1| + |\text{supp } \hat{D}_2|)$ operations in \mathbb{K} , unless it cannot be parametrized by λ . Finally, the multi-set representation of D is the union of the representations of \check{D}_1 , $\hat{D}_1 + \hat{D}_2$, and \check{D}_2 . \square

LEMMA 6.13. *Given two smooth positive divisors D_1 and D_2 in multi-set representation, sharing the same primitive element $\lambda := \lambda_x x + \lambda_y y$, and such that*

$$\prod_{i=1}^{s_1} \theta_{1,i} = \prod_{i=1}^{s_2} \theta_{2,i},$$

we can compute a multi-set representation $D := [D_1 - D_2]_+$ in terms of λ with

$$\tilde{O}(|\text{supp } D_1| + |\text{supp } D_2|)$$

operations in \mathbb{K} .

Proof. We proceed by induction on s_1 as in the proof of Lemma 6.11, from which we borrow the notation. If $s_1 = 1$, then we compute

$$\delta_i := \gcd(\theta_{2,i}, u_{1,1} - u_{2,i}, v_{1,1} - v_{2,i}) \text{ for } i = 1, \dots, s_2$$

via Proposition 2.3. We set

$$\check{\theta}_1 := \frac{\theta_{1,1}}{\prod_{i=1}^{s_2} \delta_i}.$$

A multi-set representation of D is made of the tuples

$$(\check{\theta}_1, u_{1,1} \text{ rem } \check{\theta}_1, v_{1,1} \text{ rem } \check{\theta}_1, m_{1,1})$$

and

$$(\delta_i, u_{2,i} \text{ rem } \delta_i, v_{2,i} \text{ rem } \delta_i, m_{1,1} - m_{2,i})$$

such that $m_{1,1} - m_{2,i} > 0$, for $i = 1, \dots, s_2$.

If $s_1 \geq 2$, then we compute $D_1^{\text{lo}}, D_1^{\text{hi}}, D_2^{\text{lo}}$, and D_2^{hi} as in the proof of Lemma 6.11. Then, we obtain $[D_1^{\text{lo}} - D_2^{\text{lo}}]_+$ and $[D_1^{\text{hi}} - D_2^{\text{hi}}]_+$ recursively, and merge the results. \square

PROPOSITION 6.14. *Given two smooth positive divisors D_1 and D_2 in multi-set representation, sharing the same primitive element $\lambda := \lambda_x x + \lambda_y y$, the multi-set representation of $[D_1 - D_2]_+$ in terms of λ can be computed with*

$$\tilde{O}(|\text{supp } D_1| + |\text{supp } D_2|)$$

operations in \mathbb{K} .

Proof. As in the proof of Proposition 6.12 we compute \check{D}_1, \hat{D}_1 , and \hat{D}_2 . We have

$$[D_1 - D_2]_+ = \check{D}_1 + [\hat{D}_1 - \hat{D}_2]_+,$$

so the conclusion follows from Lemma 6.13 used with \hat{D}_1 and \hat{D}_2 . \square

6.4. Equivalence with global representation

For the sake of comparison with previous works, we prove the equivalence between the series expansion representation with the “global representation” used in [2, 3, 49]. This equivalence is not necessary to the rest of the paper. We recall that the ambient curve \mathcal{C} in \mathbb{P}^2 is defined by the equation $F = 0$.

PROPOSITION 6.15. *Given a smooth positive divisor $D = m_1 P_1 + \dots + m_s P_s$ whose support is in the affine chart $z = 1$, and given a primitive element $\lambda_x x + \lambda_y y$ for D , there exist unique polynomials χ , u , and v in $\mathbb{K}[t]$ with the following properties:*

Div-H₀. χ is monic of degree $\deg D$, and u, v have degree $< \deg D$,

Div-H₁. $F(u(t), v(t), 1) = 0 \pmod{\chi(t)}$,

Div-H₂. $\lambda_x u(t) + \lambda_y v(t) = t$,

Div-H₃. $\lambda_y \frac{\partial F}{\partial x}(u(t), v(t), 1) - \lambda_x \frac{\partial F}{\partial y}(u(t), v(t), 1)$ is coprime with $\chi(t)$.

Proof. The proof can be found in [49, Section 3] or in [2, Proposition 3.1]. \square

A global representation of a smooth divisor D defined over \mathbb{K} is the data of $\lambda_x x + \lambda_y y$ and χ, u , and v in $\mathbb{K}[t]$, as occurring in Proposition 6.15.

PROPOSITION 6.16. *Given a smooth positive divisor D , the conversions between series expansions and global representations, for when x is the primitive element used in the representations, take softly linear time.*

Proof. Let $D = m_1 \mathcal{E}_1 + \dots + m_s \mathcal{E}_s$ be given by series expansions: we write θ_i, u_i, v_i for the parametrization of \mathcal{E}_i , and

$$(X_i(t), Y_i(t)) \in (\mathbb{L}_i[[t]] / (t^{m_i}))^2$$

for the series expansion of $m_i \mathcal{E}_i$, where $\mathbb{L}_i := \mathbb{K}[b] / (\theta_i(b))$. Let β_i stand for the class of b in \mathbb{L}_i . We introduce

$$\begin{aligned} \Gamma_{\theta_i, m_i}: \quad \mathbb{K}[t] / (\theta_i^{m_i}(t)) &\cong \mathbb{L}_i[[t]] / (t^{m_i}) \\ t &\mapsto \beta_i + t, \end{aligned}$$

and verify that

$$\Gamma_{\theta_i, m_i}^{-1}(X_i(t)) = \Gamma_{\theta_i, m_i}^{-1}(\beta_i + t) = t.$$

Then, $\theta_i^{m_i}, \Gamma_{\theta_i, m_i}^{-1}(X_i(t)), \Gamma_{\theta_i, m_i}^{-1}(Y_i(t))$ is the global representation of $m_i \mathcal{E}_i$ for the primitive element x . It can be obtained in softly linear time via Proposition 2.5. By Proposition 2.4 we recover the global representation of D in softly linear time by using Chinese remaindering.

Conversely, let $\chi(t), u(t) = t, v(t)$ denote a global representation of D in terms of x . In softly linear time we compute the squarefree factorization of $\chi = \theta_1^{m_1} \dots \theta_s^{m_s}$ where the m_i are pairwise distinct and the θ_i are squarefree and pairwise coprime. By Proposition 2.3, we obtain $u \pmod{\theta_i^{m_i}}$ and $v \pmod{\theta_i^{m_i}}$ for $i = 1, \dots, s$ with $\tilde{O}(\deg D)$ operations in \mathbb{K} . Then

$$\Gamma_{\theta_i, m_i}(u \pmod{\theta_i^{m_i}}) = \Gamma_{\theta_i, m_i}(t \pmod{\theta_i^{m_i}}) = \beta_i + t$$

and $\Gamma_{\theta_i, m_i}(v \pmod{\theta_i^{m_i}})$ represent the series expansion of $m_i \mathcal{E}_i$; this also incurs softly linear time via Proposition 2.5. \square

7. VANISHING POLYNOMIALS

This section is devoted to computing homogeneous polynomials that vanish at a divisor of a curve C defined by a homogeneous polynomial $F \in \mathbb{K}[x, y, z]$ of degree δ . We assume that F has degree δ in y and that the centers of this divisor are in the affine chart $z = 1$. The set of polynomials of total degree d that vanish at this divisor forms a vector space, that can be computed straightforwardly by Gaussian elimination. This straightforward approach is detailed in the first subsection. Then, we focus on a more promising approach that yields “compressed representations” of bases of Riemann–Roch spaces.

7.1. Vanishing conditions

So far, places occurring in the Brill–Noether algorithm have been separated into two families: those centered at singular points of the curve and those at regular points. However the representations of these places have been designed to be consistent in terms of families of series expansions parametrized by algebraic numbers. This motivates the following ad hoc definition.

DEFINITION 7.1. *A vanishing condition defined over \mathbb{K} is a quintuple $(\Delta(b), \mu(a), X(t), Y(t), m)$ such that:*

- $\Delta \in \mathbb{K}[b]$ is monic and separable, and β stands for the class of b in $\mathbb{L} := \mathbb{K}[b] / (\Delta(b))$;
- $\mu \in \mathbb{L}[a]$ is monic and separable, and α stands for the class of a in $\mathbb{E} := \mathbb{L}[a] / (\Delta(a))$; here separable means that the discriminant of μ is invertible in \mathbb{L} ;
- $m \in \mathbb{N}_{>0}$;
- $(X(t), Y(t)) \in (\mathbb{E}[[t]] / (t^m))^2$, with $X(t) = \beta + \gamma t^e$, γ invertible in \mathbb{E} , and e a positive integer.

We say that a polynomial $g \in \mathbb{K}[x, y]$ satisfies this vanishing condition when

$$\text{val}_t(g(X(t), Y(t))) \geq m.$$

With the representation of Definition 4.10 of the adjoint divisor A of C , and according to Definition 4.4, the adjoint condition can be regarded as a conjunction of vanishing conditions whose representations are

$$((\Delta_i(b), \mu_{i,j}(a), X_{i,j}(t) = \beta_{i,j} + \gamma_{i,j} t^{e_{i,j}}, Y_{i,j}(t), \tau_{i,j}))_{i=1, \dots, r, j=1, \dots, s_i})$$

where the $\tau_{i,j}$ are defined in Equation (4.8), and the $e_{i,j}$ are the ramification indices. In other words, a homogeneous polynomial $G \in \mathbb{K}[x, y, z]$ is adjoint to C if, and only if,

$$\text{val}_t(G(X_{i,j}(t), Y_{i,j}(t), 1)) \geq \tau_{i,j} \text{ for } i = 1, \dots, r, j = 1, \dots, s_i.$$

On the other hand, if $D = m\mathcal{E}$ is a smooth divisor given by series expansions as in Definition 6.7 and parametrized by x , its representation by $\theta(b)$, $u(b) = b$, $v(b)$, $X(t) = \beta + t$, $Y(t)$ gives rise to the following vanishing condition:

$$(\Delta(b) = \theta(b), \mu(a) = a, X(t), Y(t), m).$$

For a homogeneous polynomial $G \in \mathbb{K}[x, y, z]$, the condition $\text{Div}(G) \geq D$ is satisfied if, and only if,

$$\text{val}_t(G(X(t), Y(t), 1)) \geq m.$$

7.2. Straightforward linear solving

In this subsection we propose a solution based on classical linear algebra to the following problem: given vanishing conditions

$$((\Delta_i(b), \mu_i(a), X_i(t), Y_i(t), m_i))_{i=1, \dots, r})$$

as in Definition 7.1, find polynomials $g \in \mathbb{K}[x, y]$ of total degree $\leq d$, degree $< \delta$ in y and vanishing at all these conditions simultaneously. Vanishing conditions can be translated into a homogeneous linear system, where the unknowns are the coefficients of g and the number of equations is

$$\sigma := \sum_{i=1}^r m_i \deg \Delta_i \deg \mu_i. \quad (7.1)$$

Algorithm 7.1

Input. A sequence of vanishing conditions $((\Delta_i(b), \mu_i(a), X_i(t), Y_i(t), m_i))_{i=1, \dots, r}$ as in Definition 7.1 and integers $\delta, d \geq 1$.

Output. A basis of the polynomials $g \in \mathbb{K}[x, y]$ of total degree $\leq d$ and degree $< \delta$ in y that vanish simultaneously at all the input conditions.

1. Construct the matrix representing the \mathbb{K} -linear map Φ :

$$\begin{aligned} \{g \in \mathbb{K}[x, y] : \deg g \leq d, \deg_y g < \delta\} &\longrightarrow \prod_{i=1}^r \mathbb{E}_i[[t]] / (t^{m_i}) \\ g(x, y) &\longmapsto (g(X_i(t), Y_i(t)) \bmod t^{m_i} : i = 1, \dots, r). \end{aligned}$$

2. Compute and return a basis g_1, \dots, g_l of $\ker \Phi$.

PROPOSITION 7.2. *Algorithm 7.1 is correct and takes*

$$\tilde{O}((d\delta + \sigma)^\omega)$$

operations in \mathbb{K} , where σ has been defined in Equation (7.1).

Proof. For each $i = 1, \dots, r$ computing $X_i(t)^k Y_i(t)^l$ at precision m_i for $l = 0, \dots, \delta - 1$ and $k = 0, \dots, d - l$ takes

$$\tilde{O}(d\delta \deg \Delta_i \deg \mu_i m_i)$$

operations in \mathbb{K} . Taking the sum of these costs for $i = 1, \dots, r$, we deduce that $\tilde{O}(d\delta\sigma)$ operations in \mathbb{K} suffice to build the matrix of Φ . For the basis of the source space we take the monomials $x^k y^l$ for $l = 0, \dots, \delta - 1$ and $k = 0, \dots, d - l$. The basis of $\mathbb{E}_i[[t]] / (t^{m_i})$ in the target space is set to $\alpha_i^k \beta_i^l t^m$ for $k = 0, \dots, \deg \mu_i - 1$, $l = 0, \dots, \deg \Delta_i - 1$, and $m = 0, \dots, m_i - 1$. Consequently, the matrix of Φ has $O(d\delta)$ columns and σ rows. Computing a basis of $\ker \Phi$ costs

$$\tilde{O}((d\delta + \sigma)^\omega)$$

operations in \mathbb{K} ; see [9, Chapter 2], [63, Theorem 2.10], or [12, Chapitre 8, Théorème 8.4], for instance. \square

The straightforward approach developed in Algorithm 7.1 turns out to be sufficient to achieve the complexity bound of Theorem 8.8. Yet we believe that it is worth adapting the point of view previously introduced in [2, 3], because it yields more compact representations of Riemann–Roch spaces (see Section 8.4), and it could benefit from future improvements for computing the kernel of Φ . In fact, in the special case where \mathbb{K} is algebraically closed we will precisely achieve a lower complexity exponent in Section 8.7.

7.3. Popov form

Let $\mathbf{b}_1, \dots, \mathbf{b}_\delta$ be a basis of a free $\mathbb{K}[x]$ -submodule of rank δ of $\mathbb{K}[x]^\delta$, let $\mathbf{s} \in \mathbb{N}^\delta$ be a *shift vector*, we define

$$\deg_s \mathbf{b}_i := \max(\deg \mathbf{b}_{i,1} + s_1, \dots, \deg \mathbf{b}_{i,\delta} + s_\delta),$$

this is called the *s-degree* of \mathbf{b}_i . The *pivot index* of \mathbf{b}_i is the largest index j such that

$$\deg \mathbf{b}_{i,j} + s_j = \deg_s \mathbf{b}_i.$$

The basis $\mathbf{b}_1, \dots, \mathbf{b}_\delta$ is said to be in *s-Popov form* if the matrix made of the rows $\mathbf{b}_1, \dots, \mathbf{b}_\delta$ is in s-Popov form. In the present case this means that:

- the pivot index of \mathbf{b}_i equals i for $i = 1, \dots, \delta$,

- $\mathbf{b}_{i,i}$ is monic for $i = 1, \dots, \delta$,
- $\deg \mathbf{b}_{j,i} < \deg \mathbf{b}_{i,i}$ for $i = 1, \dots, \delta$, and $j \neq i$.

Given any basis, it is always possible to compute its *s*-Popov form. The Popov form will be needed for the following purpose.

PROPOSITION 7.3. [2, Proposition 4.2] *Let $\mathbf{b}_1, \dots, \mathbf{b}_\delta$ be a basis of a free $\mathbb{K}[x]$ -module M of rank δ in *s*-Popov form. Given an integer $d \geq 0$, the elements in M of *s*-degree $\leq d$ form a \mathbb{K} -vector space of basis $x^j \mathbf{b}_i$ for $i = 1, \dots, \delta$ such that $\deg_s \mathbf{b}_i \leq d$ and $j = 0, \dots, d - \deg_s \mathbf{b}_i$.*

Computing Popov forms of $m \times n$ matrices can be done by means of row operations only, with $\tilde{O}(mnr(\deg M)^2)$ operations in \mathbb{K} , where r is the rank of M and when s is zero [51, Theorem 7.1]. The current best known bound $\tilde{O}(m^{\omega-1}n \deg M)$ holds whenever $m \leq n$ [53, 54]. For more information about Popov forms we refer the reader to [52].

7.4. Syzygy module

Let \mathfrak{E} be a σ -dimensional \mathbb{K} -vector space, whose elements are regarded as column vectors. By choosing an endomorphism of \mathfrak{E} , represented by a $\sigma \times \sigma$ matrix J with entries in \mathbb{K} , we endow \mathfrak{E} with a structure of a $\mathbb{K}[x]$ -module defined by

$$p \cdot \mathbf{e} := p(J) \mathbf{e},$$

where $p \in \mathbb{K}[x]$ and $\mathbf{e} \in \mathfrak{E}$. In other words, J represents the matrix of the multiplication by x in \mathfrak{E} .

Given a vector $\mathbf{E} := (e_1, \dots, e_\delta)$ in \mathfrak{E}^δ , we consider the map

$$\begin{aligned} E_J: \mathbb{K}[x]^\delta &\longrightarrow \mathfrak{E} \\ \mathbf{p} := (p_1, \dots, p_\delta) &\longmapsto \mathbf{p} \cdot \mathbf{E} := p_1 \cdot e_1 + \dots + p_\delta \cdot e_\delta. \end{aligned} \quad (7.2)$$

The kernel of E_J forms a submodule of $\mathbb{K}[x]^\delta$ which is free of rank δ because it contains $\mu_J(x) \mathbb{K}[x]^\delta$, where μ_J stands for the minimal polynomial of J . The kernel $\ker E_J$ is usually called the (first) *syzygy* module of \mathbf{E} .

For the sake of efficiency, it is important to compute bases of $\ker E_J$ with small shifted degrees, for a shift vector $\mathbf{s} \in \mathbb{N}^\delta$ as above. The natural candidate bases are those in Popov form.

THEOREM 7.4. [43, simplified from Theorem 1.4] *With the notation as above, the basis in *s*-Popov form of $\ker E_J$ can be computed with $\tilde{O}(\sigma^\omega \lceil \delta / \sigma \rceil)$ operations in \mathbb{K} .*

7.5. Compressed bases

We come back to Algorithm 7.1: we will replace the straightforward kernel basis computation by Theorem 7.4. The complexity exponent will remain the same as in Proposition 7.2, but we will obtain special bases having a representation size in general smaller.

In this subsection, we are given vanishing conditions

$$((\Delta_i(b), \mu_i(a), X_i(t), Y_i(t), m_i))_{i=1, \dots, r}$$

as in Definition 7.1, an integer $\delta \geq 1$, and we search for polynomials $g \in \mathbb{K}[x, y]$ of degree $< \delta$ in y such that

$$\text{val}_t(g(X_i(t), Y_i(t))) \geq m_i \text{ for } i = 1, \dots, r.$$

We let

$$\mathfrak{E} := \bigoplus_{i=1}^r \mathbb{E}_i[[t]] / (t^{m_i}).$$

The basis considered for $\mathbb{E}_i[[t]] / (t^{m_i})$ is the set of the $\alpha_i^k \beta_i^l t^m$ for $k=0, \dots, \deg \mu_i - 1, l=0, \dots, \deg \Delta_i - 1, m=0, \dots, m_i - 1$. With σ defined by Equation (7.1), we have

$$\sigma = \dim_{\mathbb{K}} \mathfrak{E}.$$

Let J_i denote the matrix of the multiplication endomorphism by $X_i(t) = \beta_i + \gamma_i t^{e_i}$ in $\mathbb{E}_i[[t]] / (t^{m_i})$. Let J be the block diagonal matrix made of the blocks J_1, \dots, J_r . Let e_k denote the vector $(Y_1(t)^{k-1}, \dots, Y_r(t)^{k-1})$ regarded in \mathfrak{E} ; precisely the projection of e_k onto $\mathbb{E}_i[[t]] / (t^{m_i})$ is $Y_i(t)^{k-1}$.

LEMMA 7.5. *The matrices J_1, \dots, J_r and the vectors e_1, \dots, e_r can be computed with*

$$\tilde{O}((\delta + \sigma) \sigma)$$

operations in \mathbb{K} .

Proof. Fix i in $\{1, \dots, r\}$. Building the vector representation of $\alpha_i^k \beta_i^l t^m$ for $k=0, \dots, \deg \mu_i - 1$ does not require any operation in \mathbb{K} . Second, we precompute $\alpha_i^k \beta_i^l \gamma_i$ for $k=0, \dots, \deg \mu_i - 1$ and $l=0, \dots, \deg \Delta_i - 1$. This amounts to $\tilde{O}((\deg \Delta_i \deg \mu_i)^2)$ operations in \mathbb{K} .

Then, we note that

$$X_i(t) \alpha_i^k \beta_i^l t^m = \alpha_i^k \beta_i^{l+1} t^m + \alpha_i^k \beta_i^l \gamma_i t^{m+e_i},$$

so the coordinates of $X_i(t) \alpha_i^k \beta_i^l t^m$ are obtained without any further arithmetic operations. Computing $Y_i(t)^k$ for $k=0, \dots, \delta - 1$ takes $\tilde{O}(m_i \deg \Delta_i \deg \mu_i \delta)$ operations in \mathbb{K} . Summing these costs for $i=1, \dots, r$ yields

$$\tilde{O} \left(\sum_{i=1}^r ((\deg \Delta_i \deg \mu_i)^2 + m_i \deg \Delta_i \deg \mu_i \delta) \right) = \tilde{O}((\delta + \sigma) \sigma). \quad \square$$

PROPOSITION 7.6. *Let*

$$((\Delta_i(b), \mu_i(a), X_i(t), Y_i(t), m_i))_{i=1, \dots, r}$$

represent vanishing conditions as in Definition 7.1, let $\delta \geq 1$, and set $\mathbf{s} := (\delta - 1, \delta - 2, \dots, 1, 0)$ for the shift vector. Let g be the space of polynomials g of $\mathbb{K}[x, y]$ that vanish at all these conditions and such that $\deg_y g < \delta$. Then, g is a $\mathbb{K}[x]$ -module of rank δ , for which a basis in \mathbf{s} -Popov form can be computed with

$$\tilde{O}(\sigma^\omega \lceil \delta / \sigma \rceil + \delta \sigma)$$

operations in \mathbb{K} , where σ has been defined in Equation (7.1).

Proof. In this context, the map (7.2) is

$$E_J: \mathbb{K}[x]^\delta \longrightarrow \mathfrak{E} = \bigoplus_{i=1}^r \mathbb{E}_i[[t]] / (t^{m_i})$$

$$\mathbf{p} := (p_1, \dots, p_\delta) \longmapsto \mathbf{p} \cdot \mathbf{E} = (p_1(X_i(t)) + p_2(X_i(t)) Y_i(t) + \dots + p_\delta(X_i(t)) Y_i(t)^{\delta-1})_{i=1, \dots, r}.$$

Consequently, $\ker E_J$ can be regarded as the $\mathbb{K}[x]$ -module of the polynomials p in $\mathbb{K}[x][y]_{< \delta}$ such that

$$\text{val}_i(p(X_i(t), Y_i(t))) \geq m_i \text{ for } i=1, \dots, r,$$

that is exactly the definition of g . The combination of Lemma 7.5 with Theorem 7.4 yields the claimed cost. \square

7.6. Application to divisors

To conclude this section, we revisit Proposition 7.6 in terms of divisors.

PROPOSITION 7.7. *Let C be a projective curve of degree δ defined by $F=0$. We assume that the adjoint divisor A of C is represented as in Definition 4.10. Let D be a smooth positive divisor represented by series expansions as in Definition 6.7 and let $\mathbf{s} := (\delta-1, \delta-2, \dots, 1, 0)$ stand for a shift vector. Let \mathcal{G} be the space of homogeneous polynomials G of $\mathbb{K}[x, y, z]$ such that*

$$\deg_y G < \delta \text{ and } \text{Div}(G) \geq D + A.$$

Then, $\mathcal{G}(x, y, 1)$ is a $\mathbb{K}[x]$ -module of rank δ , for which a basis in \mathbf{s} -Popov form can be computed with

$$\tilde{O}((\delta^2 + \deg D)^\omega)$$

operations in \mathbb{K} .

Proof. Since D is smooth, the condition $\text{Div}(G) \geq D + A$ is equivalent to $\text{Div}(G) \geq D$ and $\text{Div}(G) \geq A$. As explained at the end of Section 7.1, these inequalities can straightforwardly be rephrased into vanishing conditions in the affine chart $z=1$. The inequality $\text{Div}(G) \geq D$ yields $\deg D$ linear equations in the coefficients of $G(x, y, 1)$, while the other inequality $\text{Div}(G) \geq A$ yields $\deg A = O(\delta^2)$ linear equations. Proposition 7.6 gives the claimed complexity bound since $\sigma = O(\delta^2 + \deg D)$. \square

8. COMPUTATION OF RIEMANN–ROCH SPACES

We are now ready to present our top level algorithm for computing Riemann–Roch spaces. For efficiency reasons, our method relies on random changes of coordinates. So we begin this section by studying the complexities related to this task.

8.1. Changes of coordinates

We first recall that generic coordinates (with the meaning of Definition 4.9) can be achieved after a random linear change of the variables with high probability.

LEMMA 8.1. *Let F and G be two coprime homogeneous polynomials in $\mathbb{K}[x, y, z]$, and let \mathcal{S} be a finite subset of \mathbb{K} . If M is an invertible 3×3 matrix taken at random with entries in \mathcal{S} , then the coordinates are not generic for $F \circ M$ and $G \circ M$ with probability*

$$\leq \frac{2 \deg F \deg G + \deg F}{|\mathcal{S}|}.$$

Testing if the coordinates are generic for F and G takes $\tilde{O}(\deg F + \deg G)$ operations in \mathbb{K} .

Proof. The proof is recalled briefly from [3, Lemma 5.2]. Let $(M_{i,j})_{1 \leq i, j \leq 3}$ denote the entries of M . The coefficient of $y^{\deg F}$ in $F \circ M$ is $F(M_{1,2}, M_{2,2}, M_{3,2})$, so it is generically non-zero and has degree $\deg F$ in the entries of M . Let C be the coefficient of $x^{\deg F \deg G}$ in the determinant R of the Sylvester matrix of $F \circ M$ and $G \circ M$ in y , where $F \circ M$ (resp. $G \circ M$) is regarded as a polynomial of degree $\deg F$ in y (resp. $\deg G$ in y).

The degree of C in the entries of M is $\leq 2 \deg F \deg G$. Once F is ensured to have degree $\deg F$ in y , then $R(x, z + cx)$ has degree $\deg F \deg G$ in x whenever $R(1, c) \neq 0$. This proves that C is not identically zero as a polynomial in the entries of M . The bound on the probability then follows directly from the aforementioned Schwartz–Zippel lemma.

Testing if the coordinates are generic involves determining the degree of F in y and computing $R(x, 0)$, that incur $\tilde{O}(\deg F + \deg G)$ arithmetic operations in \mathbb{K} . \square

LEMMA 8.2. *Let \mathcal{S} be a finite subset of \mathbb{K} and let F be a squarefree polynomial. If M is an invertible 3×3 matrix taken at random with entries in \mathcal{S} , then the coordinates are not generic for $F \circ M$ with probability*

$$\leq \frac{2(\deg F)^2}{|\mathcal{S}|}.$$

Testing if the coordinates are generic for F takes $\tilde{O}(\deg F)$ operations in \mathbb{K} .

Proof. Let $\delta := \deg F$. The proof is very similar to the one of Lemma 8.1. Let $(M_{i,j})_{1 \leq i, j \leq 3}$ denote the entries of M . The coefficient of y^δ in $F \circ M$ is $F(M_{1,2}, M_{2,2}, M_{3,2})$, so it is generically non-zero and has degree δ in the entries of M . Let C be the coefficient of $x^{\delta(\delta-1)}$ in the determinant R of the Sylvester matrix of $F \circ M$ and $\frac{\partial(F \circ M)}{\partial y}$ in y , where $F \circ M$ is regarded as a polynomial of degree δ in y .

The degree of C in the entries of M is $\leq \delta(2\delta - 1)$. Once F is ensured to have degree δ in y , then $R(x, z + cx)$ has degree $\delta(\delta - 1)$ in x whenever $R(1, c) \neq 0$. This proves that C is not identically zero as a polynomial in the entries of M . The rest of the proof is the same as for Lemma 8.1. \square

8.2. Modular change of coordinates

Next, we address the cost of the division by F with respect to the variable y . We write $G \operatorname{rem}_y F$ for the remainder in the division of G by F in $\mathbb{K}[x, z][y]$. This division is well defined whenever F is monic in y .

LEMMA 8.3. *Let $F \in \mathbb{K}[x, y, z]$ be homogeneous of degree $\delta \geq 1$ and of degree δ in y . Let G_1 and G_2 be homogeneous polynomials in $\mathbb{K}[x, y, z]$ of total degree d_1 and d_2 and degree $< \delta$ in y . Then, $G_1 G_2 \operatorname{rem}_y F$ can be computed with $\tilde{O}((d_1 + d_2)\delta)$ operations in \mathbb{K} .*

Proof. The product $P(x, y) := G_1(x, y, 1) G_2(x, y, 1)$ can be computed with $\tilde{O}((d_1 + d_2)\delta)$ by means of the Kronecker substitution method; see [28, Chapter 8, Section 4] for instance. If $d_1 + d_2 < \delta$ then no division by F in y is needed. Otherwise $P(x, y) \operatorname{rem}_y F(x, y, 1)$ can be computed in $(\mathbb{K}[[x]] / (x^{d_1 + d_2 + 1}))[[y]]$ with $\tilde{O}((d_1 + d_2)\delta)$ operations in \mathbb{K} . It remains to homogenize the latter remainder in degree d , unless it is zero. \square

LEMMA 8.4. *Let $F \in \mathbb{K}[x, y, z]$ be homogeneous of degree $\delta \geq 1$ and of degree δ in y . Let $G \in \mathbb{K}[x, y, z]$ be homogeneous of total degree d and degree $< \delta$ in y . Then, $G^n \operatorname{rem}_y F$ can be computed with $\tilde{O}(d\delta \log n)$ operations in \mathbb{K} .*

Proof. This bound follows from the usual modular binary powering algorithm and Lemma 8.3; see [28, Chapter 4, Section 3] for instance. \square

LEMMA 8.5. *Let $F \in \mathbb{K}[x, y, z]$ be homogeneous of degree $\delta \geq 1$ and of degree δ in y . Let $H \in \mathbb{K}[x, y, z]$ be homogeneous of total degree d and degree $< \delta$ in y , and let M be a 3×3 matrix over \mathbb{K} . Then, $H \circ M \operatorname{rem}_y F$ can be computed with $\tilde{O}(\delta^2 + d\delta)$ operations in \mathbb{K} .*

Proof. If $d \leq 2\delta$ then $H \circ M$ can be computed with $\tilde{O}(\delta^2)$ operations in \mathbb{K} , by Lemma 2.1. Then, $(H \circ M)(x, y, 1) \operatorname{rem}_y F(x, y)$ can be computed with $\tilde{O}(\delta^2)$ operations in \mathbb{K} by means of a fast division algorithm in $\mathbb{K}[[x]]/(x^{d+1})[y]$. The corresponding remainder can then be homogenized in degree d , unless it is zero.

If $d > 2\delta$, then we use the “divide and conquer” paradigm. We set $d_0 := \lfloor d/2 \rfloor$ and $d_1 := d - d_0$, and we note that $d_0 \geq \delta$ and $d_1 \geq \delta$. We decompose H into

$$H = z^{d_0} H_1 + G + x^{d_1} H_0,$$

where $\deg_z(G + x^{d_1} H_0) < d_0$, $\deg_x G < d_1$, and such that the supports of $z^{d_0} H_1$, G , and $x^{d_1} H_0$ are pairwise disjoint. Such a decomposition of H is uniquely determined by these conditions. In particular, we have

$$\deg H_0 = d_0, \quad \deg_y H_0 < \delta, \quad \deg H_1 = d_1, \quad \deg_y H_1 < \delta.$$

Then, we verify that

$$\begin{aligned} \deg_x(G + x^{d_1} H_0) &\geq d - \deg_z(G + x^{d_1} H_0) - \deg_y(G + x^{d_1} H_0) \\ &\geq d - (d_0 - 1) - (\delta - 1) \\ &= d_1 - \delta + 2, \end{aligned}$$

and that

$$\begin{aligned} \deg_z G &\geq d - \deg_x G - \deg_y G \\ &\geq d - (d_1 - 1) - (\delta - 1) \\ &= d_0 - \delta + 2. \end{aligned}$$

We set $\tilde{G} := G / (x^{d_1 - \delta + 2} z^{d_0 - \delta + 2})$, and deduce that

$$\begin{aligned} \deg_x \tilde{G} &\leq d_1 - 1 - (d_1 - \delta + 2) = \delta - 3 \\ \deg_z \tilde{G} &\leq d_0 - 1 - (d_0 - \delta + 2) = \delta - 3 \\ \deg_y \tilde{G} &\leq \delta - 1, \end{aligned}$$

so the decomposition of H rewrites as

$$H = z^{d_0} H_1 + x^{d_1 - \delta + 2} z^{d_0 - \delta + 2} \tilde{G} + x^{d_1} H_0.$$

By Lemma 8.4 the polynomials $(z \circ M)^{d_0} \operatorname{rem}_y F$, $(x \circ M)^{d_1 - \delta + 2} (z \circ M)^{d_0 - \delta + 2} \operatorname{rem}_y F$, and $(x \circ M)^{d_1} \operatorname{rem}_y F$, can be computed with $\tilde{O}(d\delta)$ operations in \mathbb{K} . In addition, $\tilde{G} \circ M \operatorname{rem}_y F$ can be computed with $\tilde{O}(\delta^2)$ operations in \mathbb{K} by Lemma 2.1. Thanks to Lemma 8.3 we obtain $H \circ M \operatorname{rem}_y F$ from $H_0 \circ M \operatorname{rem}_y F$ and $H_1 \circ M \operatorname{rem}_y F$ with $\tilde{O}(d\delta)$ operations in \mathbb{K} .

Let $\mathsf{T}(d)$ represent the cost for computing $H \circ M \operatorname{rem}_y F$ with $\deg H = d$. For $d > 2\delta$, we have shown that

$$\mathsf{T}(d) = \mathsf{T}(d_0) + \mathsf{T}(d_1) + \tilde{O}(d\delta).$$

This “divide and conquer” strategy ends when $d \leq 2\delta$, for which we have seen that $\mathsf{T}(d) = \tilde{O}(\delta^2)$.

The successive recursive calls of the algorithm are regarded as a tree. The sum of the total degree of the polynomials H occurring at depth h is $\leq d$. So the total cost of the computation nodes at depth h is $\tilde{O}(d\delta)$. The depth of the tree is $O(\log(d/\delta))$. The number of leaves is $O(d/\delta)$, and the contribution of each leaf is $\tilde{O}(\delta^2)$. Consequently, the computation of $H \circ M \operatorname{rem}_y F$ amounts to $\tilde{O}(\delta^2 + d\delta)$. \square

8.3. Computation of a common denominator

As recalled in Section 1.1, the first part of the Brill–Noether method is the computation of a common denominator of a basis of $\mathcal{L}(D)$. We are looking for homogeneous polynomials H of degree

$$d := \left\lceil \frac{(\delta-1)(\delta-2) + \deg D_+}{\delta} \right\rceil, \quad (8.1)$$

such that $\text{Div}(H) \geq D_+ + A$. Note that $d\delta = O(\delta^2 + \deg D_+)$. For the sake of complexity, we require that $\text{Div}(H)$ is sharply adjoint, which means that $\text{Div}(H) - A$ is smooth. The computation is summarized in the following algorithm.

Algorithm 8.1

Input. An absolutely irreducible plane projective curve C of degree δ , defined by the equation $F = 0$, and a smooth divisor D of C in multi-set representation.

Output. A homogeneous polynomial $H \in \mathbb{K}[x, y, z]$, of total degree d defined in (8.1), and degree $< \delta$ in y , such that $\text{Div}(H) \geq D_+ + A$ and $\text{Div}(H)$ is sharply adjoint, where A represents the adjoint divisor of C .

Assumption. \mathbb{K} has characteristic zero. The coordinates are generic for F . The centers of D are in the affine chart $z = 1$. The variable x is primitive for the union of the centers of D and $\mathcal{U}_{\mathbb{A}}(F(x, y, 1), F_y(x, y, 1))$.

1. Compute the series expansions of A using Proposition 4.11.
2. Expand the representation of D_+ using Proposition 6.10.
3. Let \mathcal{H} denote the space of homogeneous polynomials H of $\mathbb{K}[x, y, z]$ such that $\deg_y H < \delta$ and $\text{Div}(H) \geq D_+ + A$. Use Proposition 7.7 with D_+ in order to obtain a $\mathbb{K}[x]$ -module basis h_1, \dots, h_δ of $\mathcal{H}(x, y, 1)$.
4. Set $H(x, y, z) := z^d \sum_{i=1}^{\delta} a_i(x/z) h_i(x/z, y/z)$ with $a_i(x) \in \mathbb{K}[x]_{\leq d - \deg h_i}$ taken at random with coefficients in $\{1, \dots, 2^{\delta^2}\}$. Repeat this step until H is sharply adjoint.
5. Return H .

PROPOSITION 8.6. *Algorithm 8.1 is correct and takes an expected number of*

$$\tilde{O}((\delta^2 + \deg D_+)^{\omega})$$

operations in \mathbb{K} .

Proof. The assumptions are gathered in order to be able to apply Propositions 4.11, 6.10, and 7.7. By Proposition 5.3 the \mathbb{K} -vector subspace V of \mathcal{H} of homogeneous polynomials of degree d has positive dimension. Then, Proposition 7.3 ensures that the polynomials H generated in Step 4 are random elements of V . By Lemma 5.4, the expected number of iterations of this step is $O(1)$. Consequently, the algorithm finishes with a correct result.

Step 1 costs $\tilde{O}(\delta^3)$ operations in \mathbb{K} by Proposition 4.11. Step 2 contributes to

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D_+\right)$$

by Proposition 6.10. Then, Step 3 incurs $\tilde{O}((\delta^2 + \deg D_+)^{\omega})$ by Proposition 7.7. Finally, the construction of H in Step 4 takes $\tilde{O}(\delta d) = \tilde{O}(\delta^2 + \deg D_+)$ operations in \mathbb{K} . Testing if H is sharply adjoint further incurs

$$\tilde{O}(\delta \max(d, \delta^2)) = \tilde{O}(\delta^3 + \deg D_+)$$

by Proposition 4.13. □

8.4. Representation of Riemann–Roch bases

The $\mathbb{K}[x]$ -module approach of Section 7.5 naturally leads to the following representation of a Riemann–Roch space $\mathcal{L}(D)$ by:

- $M \in \mathrm{GL}_3(\mathbb{K})$,
- a homogeneous polynomial H in $\mathbb{K}[x, y, z]$,
- a sequence of homogeneous polynomials G_1, \dots, G_l in $\mathbb{K}[x, y, z]$ of respective degree d_1, \dots, d_l ,

such that

- $F \circ M$ has generic coordinates,
- $\deg_y H < \delta$, $\deg_y G_i < \delta$ for $i = 1, \dots, l$,
- the support of $M^{-1}(D)$ is in the affine chart $z = 1$,
- $\mathcal{U}_{\mathbb{P}}(F \circ M, H)$ is in the affine chart $z = 1$,
- $\left(\frac{x^j z^{d-d_i-j} G_i}{H} \right) \circ M^{-1}$ with $0 \leq j \leq d - d_i$ and $1 \leq i \leq l$ form a basis of $\mathcal{L}(D)$.

8.5. Computation of a numerator basis

We are now ready to detail the second step of the Brill–Noether method: a common denominator H of $\mathcal{L}(D)$ has been computed and it remains to obtain a basis of numerators. The way H has been determined does not a priori guarantee that the current coordinates will be sufficiently generic for $\mathrm{Div}(H)$ and for the subsequent computation of $\mathrm{Div}(H) - A - D$. Consequently, the first part of the following algorithm is dedicated to finding sufficiently generic coordinates with high probability. Although this part of the algorithm seems technical, its correctness will be proved routinely. Nevertheless, it would be further interesting to show that a single random change of the coordinates from the outset is sufficient to ensure all the needed genericity conditions with high probability. In fact, we previously developed this strategy in [3] for curves with ordinary singularities.

Algorithm 8.2

Input. An absolutely irreducible plane projective curve C defined by $F = 0$, a smooth divisor D of C in multi-set representation, a common denominator H of $\mathcal{L}(D)$ of total degree d and degree $< \delta$ in y .

Output. A representation of $\mathcal{L}(D)$ as defined in Section 8.4.

Assumption. \mathbb{K} has characteristic zero. The coordinates are generic for F . The centers of D are in the affine chart $z = 1$. The variable x is primitive for the union of the centers of D and the singular locus of C . $\mathrm{Div}(H)$ is sharply adjoint and satisfies $\mathrm{Div}(H) \geq D_+ + A$.

1. Take a 3×3 matrix M at random with entries in

$$\mathcal{S} := \{1, \dots, 60(\delta^2 + \deg D_+)^2\}$$

until M is invertible.

2. Compute $F \circ M$. If the coordinates are not generic for $F \circ M$, then go to Step 1.
3. Compute $H \circ M \operatorname{rem}_y F$ using Lemma 8.5.
4. Compute

$$\mathcal{E} := \mathcal{U}_{\mathbb{A}}(F \circ M(x, y, 1), (H \circ M \operatorname{rem}_y F)(x, y, 1))$$

by using [2, Lemma 2.4]. If the number of solutions counted with multiplicities is not $d\delta$ or if x is not primitive for \mathcal{E} , then go to Step 1.

Otherwise, write $\theta_i^H(x) = 0$ and $y = v_i^H(x)$ for the parametrization of the points of \mathcal{E} having intersection multiplicity i , for $i = 1, \dots, d\delta$.

5. Compute $M^{-1}(D)$ using Proposition 6.6. If the centers of $M^{-1}(D)$ are not in the affine chart $z = 1$, or if x is not a primitive element for $M^{-1}(D)$, then go to Step 1.
6. If x is not primitive for the union of the centers of $M^{-1}(D_-)$ and \mathcal{E} , then go to Step 1. If x is not primitive for $\mathcal{U}_{\mathbb{A}}\left(F \circ M(x, y, 1), \frac{\partial(F \circ M)}{\partial y}(x, y, 1)\right)$, then go to Step 1.
7. Replace F by $F \circ M$, H by $H \circ M$ $\text{rem}_y F$ and D by $M^{-1}(D)$, and compute the adjoint divisor A of C in the new coordinates, by using Proposition 4.11.
8. Compute the product Δ of the Δ_i of Definition 4.10. Compute

$$\theta := \prod_{i=1}^{d\delta} \theta_i^H \text{ and } \tilde{\theta} := \theta / \gcd(\theta, \Delta).$$

Then compute $\tilde{\theta}_i := \tilde{\theta} \bmod \theta_i^H$, $\tilde{\theta}_i := \gcd(\tilde{\theta}_i, \theta_i^H)$, $\tilde{v}_i := v_i^H \bmod \tilde{\theta}_i$ for $i = 1, \dots, d\delta$.

If some of the $F_y(x, \tilde{v}_i(x), 1)$ are not invertible modulo $\tilde{\theta}_i(x)$ then go to Step 1. Otherwise the $(\tilde{\theta}_i, \tilde{v}_i, i)$ for $i = 1, \dots, d\delta$ constitute a multi-set representation of the smooth divisor $\text{Div}(H) - A$.

9. Compute the multi-set representation of

$$R := ((\text{Div}(H) - A) - D_+) + D_-$$

by using Propositions 6.12 and 6.14 successively.

10. Expand the representation of R by means of Proposition 6.10.
11. Let \mathcal{G} denote the space of homogeneous polynomials G of $\mathbb{K}[x, y, z]$ such that $\deg_y G < \delta$ and $\text{Div}(G) \geq R + A$. Compute a basis g_1, \dots, g_δ of the $\mathbb{K}[x]$ -module $\mathcal{G}(x, y, 1)$ by means of Proposition 7.7 used with R . Sort the g_i by increasing total degrees and let l be maximal such that $\deg g_l \leq d$.
12. Return $M, H, z^{d_i} g_i(x/z, y/z)$, and d_i for $i = 1, \dots, l$.

PROPOSITION 8.7. *Algorithm 8.2 is correct and takes an expected number of*

$$\tilde{O}((\delta^2 + \deg D_+)^\omega).$$

operations in \mathbb{K} .

Proof. If the algorithm reaches Step 7, then the conditions of Proposition 4.11 are satisfied, so the adjoint divisor A can actually be computed. When entering Step 8 the variable x separates the centers of $\text{Div}(H)$ and $\text{Div}(H)$ is sharply adjoint. Since $\text{Div}(H) \geq D_+ + A$, the variable x also separates the centers of A (i.e. the singular points of C). Therefore if Step 8 does not return to Step 1, then it actually computes a multi-set representation of $\text{Div}(H) - A$. From Step 6 it is ensured that x is primitive for R so Step 9 works properly.

From the Brill–Noether theory, briefly recalled in Section 1.1, it is known that a polynomial H satisfying $\text{Div}(H) \geq D_+ + A$ is a suitable denominator for $\mathcal{L}(D)$. This means that a numerator basis is a basis of the space of polynomials G modulo F , of total degree d , and such that $\text{Div}(G) \geq \text{Div}(H) - D$; see [36, Chapitre 2, Théorème 2.7.1], or [37, Théorème 2.5], or [48, Section 4], for instance. Consequently, when Step 11 is reached, Propositions 7.3 and 7.7 ensure the correctness of the output.

Before analyzing probabilities, from the definition of d in (8.1), we note that

$$d\delta \leq \delta^2 + \deg D_+ - 2\delta. \quad (8.2)$$

The probability that a matrix M taken with random entries in \mathcal{S} is not invertible is

$$\leq \frac{3}{|\mathcal{S}|} \quad (8.3)$$

by the aforementioned Schwartz–Zippel lemma. In Step 2, the probability that the coordinates are not generic for $F \circ M$ is

$$\leq \frac{2\delta^2}{|\mathcal{S}|} \quad (8.4)$$

by Lemma 8.2. In Step 4, the probability that the coordinates are not generic for $F \circ M$ and $H \circ M$ or that x is not a suitable primitive element is

$$\leq \frac{2d\delta + \delta + \binom{d\delta}{2}}{|\mathcal{S}|} \leq \frac{3(\delta^2 + \deg D_+)^2}{|\mathcal{S}|} \quad (8.5)$$

by Lemmas 8.1 and 6.1 combined with Inequality (8.2). In Step 5, the probability that the conditions for $M^{-1}(D)$ are not met is

$$\leq \frac{3(\deg D_+ + \deg D_-)^2}{|\mathcal{S}|} \leq \frac{12(\deg D_+)^2}{|\mathcal{S}|}, \quad (8.6)$$

by Lemma 6.4. In Step 6, the probability that the algorithm goes back to Step 1 is

$$\begin{aligned} \frac{\binom{\deg D_- + |\mathcal{E}|}{2} + \binom{\delta(\delta-1)}{2}}{|\mathcal{S}|} &\leq \frac{(\deg D_+ + d\delta + \delta^2)^2}{|\mathcal{S}|} \\ &\leq \frac{4(\delta^2 + \deg D_+)^2}{|\mathcal{S}|} \end{aligned} \quad (8.7)$$

by Inequality (8.2) and Lemma 6.1 again. For the probability of Step 8 to return to Step 1, we apply Lemma 6.4 to the divisor made of the points of \mathcal{E} that are smooth on \mathcal{C} : the probability bound is

$$\leq \frac{3|\mathcal{E}|^2}{|\mathcal{S}|} \leq \frac{3(d\delta)^2}{|\mathcal{S}|} \leq \frac{3(\delta^2 + \deg D_+)^2}{|\mathcal{S}|}. \quad (8.8)$$

The sum of the right-hand sides of Inequalities (8.3) to (8.8) is $\leq 1/2$. Overall, the expected number of times the algorithm goes back to Step 1 is $O(1)$. We are done with the correctness.

The cost of Step 1 is negligible. Then Step 2 contributes to $\tilde{O}(\delta^2)$ by Lemmas 2.1 and 8.1. Step 3 takes

$$\tilde{O}(\delta^2 + d\delta) = \tilde{O}(\delta^2 + \deg D_+)$$

operations in \mathbb{K} by Lemma 8.5. By [2, Lemma 2.4] (or [3, Proposition 5.6]), the cost of Step 4 is

$$\tilde{O}(d\delta^2) = \tilde{O}(\delta^3 + \delta \deg D_+) = \tilde{O}((\delta^2 + \deg D_+)^2).$$

Step 5 costs

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D_+ + (\deg D_+)^{\omega}\right) = \tilde{O}((\delta^2 + \deg D_+)^2)$$

by Proposition 6.6.

Arriving at Step 6, x is primitive for the support of $M^{-1}(D_-)$ and for \mathcal{E} , so it suffices to verify that the defining polynomials are coprime, with

$$\tilde{O}(\deg D_- + |\mathcal{E}|) = \tilde{O}(d\delta + \deg D_+) = \tilde{O}(\delta^2 + \deg D_+)$$

operations in \mathbb{K} . Testing if x is primitive for $\mathcal{U}_A\left(F \circ M(x, y, 1), \frac{\partial(F \circ M)}{\partial y}(x, y, 1)\right)$ contributes to $\tilde{O}(\delta^3)$ by [2, Lemma 2.4] (or [3, Proposition 5.6]). The conditions of Proposition 4.11 are satisfied, so Step 7 costs $\tilde{O}(\delta^3)$.

For Step 8, Proposition 2.3 allows the computation of the $\tilde{\theta}_i, \tilde{v}_i$ for $i = 1, \dots, d\delta$ with

$$\tilde{O}(d\delta + \delta^2) = \tilde{O}(\delta^2 + \deg D_+)$$

operations in \mathbb{K} . The remaining evaluations of F_y and the consecutive invertibility tests of Step 8 amount to

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}}(d\delta)\right) = \tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}}(\delta^2 + \deg D_+)\right) = \tilde{O}((\delta^2 + \deg D_+)^2)$$

by Lemma 6.5.

By Propositions 6.12 and 6.14, Step 9 costs

$$\tilde{O}(\deg(\text{Div}(H)) + \deg D_+) = \tilde{O}(d\delta + \deg D_+) = \tilde{O}(\delta^2 + \deg D_+).$$

Step 10 then takes

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg R\right) = \tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}}(d\delta)\right) = \tilde{O}((\delta^2 + \deg D_+)^2)$$

operations in \mathbb{K} by Proposition 6.10. Finally Step 11 contributes to

$$\tilde{O}((\delta^2 + \deg R)^\omega) = \tilde{O}((\delta^2 + d\delta)^\omega) = \tilde{O}((\delta^2 + \deg D_+)^\omega)$$

by Proposition 7.7. □

8.6. Main complexity bound

By combining Algorithms 8.1 and 8.2, we finally achieve our main result.

THEOREM 8.8. *Let \mathbb{K} be an effective field of characteristic zero. Let $F \in \mathbb{K}[x, y, z]$ be a homogeneous and absolutely irreducible polynomial of degree δ , that defines a curve C . Let D be a smooth divisor of C given in multi-set representation (see Definition 6.3). Then, a representation of $\mathcal{L}(D)$ as in Section 8.4 can be computed with a probabilistic algorithm of Las Vegas type with an expected number of*

$$\tilde{O}((\delta^2 + \deg D_+)^\omega)$$

operations in \mathbb{K} .

Proof. After a random change of coordinates, the assumptions of Algorithm 8.1 hold with high probability, thanks to Lemmas 6.1, 6.4, and 8.2. Changing the coordinates in F and testing their genericity take $\tilde{O}(\delta^2)$ operations in \mathbb{K} by Lemmas 2.1 and 8.2. Changing the coordinates in D , verifying that the centers are in the affine chart $z = 1$, and that x is a primitive element takes

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}}(|\text{supp } D_+| + |\text{supp } D_+|^\omega)\right) = \tilde{O}((\delta^2 + \deg D_+)^\omega)$$

by Proposition 6.6. Let θ_D denote the corresponding minimal polynomial of x .

Testing if x is primitive for $\mathcal{U}_{\mathbb{A}}(F(x, y, 1), F_y(x, y, 1))$ and computing the corresponding parametrization requires $\tilde{O}(\delta^3)$ operations in \mathbb{K} by [2, Lemma 2.4] (or [3, Proposition 5.6]). Let θ_{F_y} denote the corresponding minimal polynomial of x .

The variable x is primitive for the union of the centers of D and $\mathcal{U}_{\mathbb{A}}(F(x, y, 1), F_y(x, y, 1))$ if, and only if, $\text{Res}(\theta_D, \theta_{F_y}) \neq 0$, whose computation takes negligible time. Finally, once the assumptions of Algorithm 8.1 are satisfied, we call this algorithm, followed by Algorithm 8.2. The total complexity bound is deduced from Propositions 8.6 and 8.7. \square

8.7. Towards a subquadratic complexity bound

To conclude this section we focus on the following unusual special case:

Hypothesis (C). \mathbb{K} is algebraically closed of characteristic zero and is endowed with a routine that computes the roots of any polynomial $\theta \in \mathbb{K}[x]$ in softly linear time.

In fact, our goal is only to show that the complexity exponent for computing Riemann–Roch spaces can be improved in this case, thanks to a faster algorithm for syzygy bases. Precisely, we will rely on the following statement that improves Theorem 7.4 in a particular case; we use the notation of Section 7.5.

THEOREM 8.9. [43, simplified from Theorem 1.5] *With the notation of Section 7.5, if J is a Jordan matrix, then the basis in s -Popov form of $\ker E_J$ can be computed with $\tilde{O}(\delta^{\omega-1}(\sigma + |s|))$ operations in \mathbb{K} , where $|s| := s_1 + \dots + s_\delta$.*

We deduce the following proposition in replacement of Proposition 7.7.

PROPOSITION 8.10. *Under Hypothesis (C), the complexity bound in Proposition 7.7 can be replaced by $\tilde{O}(\delta^{\omega-1}(\delta^2 + \deg D))$.*

Proof. Since \mathbb{K} is algebraically closed, by using root-finding, we can decompose any vanishing condition into a conjunction of vanishing conditions where each of them is still represented by $(\Delta(b), \mu(a), X(t), Y(t))$ as in Definition 7.1 but in the form $\Delta(b) := b - \beta$, $\mu(a) := a$ and $X(t) = \beta + t^e$. Such a rewriting takes softly linear time by Hypothesis (C) and Proposition 2.3.

For $j=0, \dots, e-1$, let v_j denote the largest integer v such that $ve + j \leq m-1$. In the basis of the \mathbb{K} -vector space $\mathbb{K}[[t]]/(t^m)$ made of the concatenation of

$$(t^{v_je+j}, t^{(v_j-1)e+j}, \dots, t^{e+j}, t^j) \text{ for } j=0, \dots, \min(e, m) - 1,$$

the matrix representing the multiplication by $X(t) = \beta + t^e$ is a Jordan matrix. Consequently, the cost of Lemma 7.5 becomes $\tilde{O}(\delta\sigma)$. Since $|s| = O(\delta^2)$, by combining this bound with Theorem 8.9, the complexity bound in Proposition 7.6 becomes $\tilde{O}(\delta^{\omega-1}(\delta^2 + \sigma))$. The conclusion follows as in the proof of Proposition 7.7. \square

In the future, we hope that the complexity bound in Proposition 8.10 will hold without Hypothesis (C). This might be made possible thanks to further advances in the so called *interpolation bases* algorithms; see [43, 52]. Let us now briefly assess the overall cost of our Brill–Noether variant in this framework.

THEOREM 8.11. *Under Hypothesis (C), the expected complexity bound in Theorem 8.8 can be replaced by*

$$\tilde{O}\left((\delta^2 + \deg D_+)^{\frac{\omega+1}{2}}\right).$$

Proof. Using Proposition 8.10 instead of Proposition 7.7, and revisiting complexity analyses step by step, the cost in Proposition 8.6 becomes $\tilde{O}(\delta^{\omega+1} + \delta^{\omega-1} \deg D_+)$. Then, the cost in Proposition 8.7 becomes

$$\tilde{O}(\delta^{\omega+1} + \delta^{\omega-1} \deg D_+ + (\deg D_+)^{\omega}).$$

It follows that the complexity bound in Theorem 8.8 can be replaced by

$$\tilde{O}(\delta^{\omega+1} + \delta^{\omega-1} \deg D_+ + (\deg D_+)^{\omega}) = \tilde{O}\left(\delta^{\omega+1} + \delta^{\omega-1} \deg D_+ + (\deg D_+)^{\frac{\omega+1}{2}}\right).$$

If $\deg D_+ \leq \delta^2$ then $\delta^{\omega-1} \deg D_+ = O(\delta^{\omega+1})$. Otherwise $\delta^2 < \deg D_+$ and we have

$$\delta^{\omega-1} \deg D_+ \leq (\deg D_+)^{\frac{\omega-1}{2}} \deg D_+ \leq (\deg D_+)^{\frac{\omega+1}{2}},$$

whence the claimed bound. \square

9. CONCLUSION

Our new algorithm for computing bases of Riemann–Roch spaces is subject to future improvements and extensions. A first extension concerns handling non necessarily smooth input divisors. Indeed our Proposition 5.3 supports this more general setting, so it would essentially suffice to focus on the algorithmic side.

Another challenging research direction would be to achieve the same complexity exponent in any characteristic. At present time the main difficulty resides in designing a suitable efficient replacement of Puiseux expansions. Some possibilities in this direction could be to exploit Hamburger–Noether expansions (introduced in [15] and previously used in the context of computing Riemann–Roch spaces in [16]), or to rely on the approximate roots theory initiated by Abhyankar [4, 21].

The bottleneck of our main algorithm is in the complexity bound of Theorem 7.4. Therefore, faster computations of syzygy bases related to the structured linear algebra problem occurring in Section 7.5 would improve the complexity exponent of our main algorithm, in a way similar to the framework of Section 8.7.

Finally, let us mention that, for practical efficiency, it would be also valuable to design an adjoint condition from the sole singular parts of the Puiseux expansions, because it would save the lifting procedure of Section 3.7. From [3, Section 7.1] this is already known to be possible for ordinary curves.

BIBLIOGRAPHY

- [1] S. Abelard. On the complexity of computing integral bases of function fields. In F. Boulier, M. England, T. M. Sadykov, and E. V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing. 22nd International Workshop, CASC 2020, Linz, Austria, September 14–18, 2020, Proceedings*, volume 12291 of *Lect. Notes Comput. Sci.*, pages 42–62. Cham, 2020. Springer International Publishing.
- [2] S. Abelard, A. Couvreur, and G. Lecerf. Sub-quadratic time for Riemann–Roch spaces: case of smooth divisors over nodal plane projective curves. In A. Mantzaflaris, editor, *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, ISSAC '20*, pages 14–21. New York, NY, USA, 2020. ACM.
- [3] S. Abelard, A. Couvreur, and G. Lecerf. Efficient computation of Riemann–Roch spaces for plane curves with ordinary singularities. Technical Report, HAL, 2021. <https://hal.archives-ouvertes.fr/hal-03110135>.

- [4] S. S. Abhyankar. *Lectures on expansion techniques in algebraic geometry*, volume 57 of *Lectures on mathematics and physics. Mathematics*. Bombay: Tata Institute of Fundamental Research, 1977.
- [5] S. S. Abhyankar and A. M. Sathaye. *Geometric theory of algebraic space curves*, volume 423 of *Lect. Notes Math*. Springer, Berlin, Heidelberg, 1974.
- [6] J. Alman and V. V. Williams. A refined laser method and faster matrix multiplication. In D. Marx, editor, *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 522–539. Philadelphia, PA, USA, 2021. SIAM.
- [7] E. Arbarello, M. Cornalba, P. Griffiths, and J. D. Harris. *Geometry of algebraic curves. Volume I*, volume 267 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag New York, 1985.
- [8] E. Ben-Sasson, A. Chiesa, A. Gabizon, M. Riabzev, and N. Spooner. Interactive oracle proofs with constant rate and query complexity. In *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017.
- [9] D. Bini and V. Y. Pan. *Polynomial and matrix computations. Vol. 1. Fundamental algorithms*. Progress in Theoretical Computer Science. Birkhäuser Boston, Inc., Boston, MA, 1994.
- [10] S. Bordage and J. Nardi. Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes. *Electronic colloquium on computational complexity*, 2020. TR20-165.
- [11] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [12] A. Bostan, F. Chyzak, M. Giusti, R. Lecomte, G. Lecerf, B. Salvy, and É. Schost. *Algorithmes Efficaces en Calcul Formel*. Frédéric Chyzak (self-published), Palaiseau, 2017. Electronic version available from <https://hal.archives-ouvertes.fr/AECF>.
- [13] A. Brill and M. Noether. Ueber die algebraischen Functionen und ihre Anwendung in der Geometrie. *Math. Ann.*, 7(2-3):269–310, 1874.
- [14] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, 1997.
- [15] A. Campillo. *Algebroid Curves in Positive Characteristics*, volume 813 of *Lect. Notes Math*. Springer-Verlag Berlin Heidelberg, 1980.
- [16] A. Campillo and J. I. Farrán. Symbolic Hamburger–Noether expressions of plane curves and applications to AG codes. *Math. Comp.*, 71(240):1759–1780, 2002.
- [17] A. Campillo and J. I. Farrán. Adjoints and codes. *Rendiconti del Seminario Matematico Università e Politecnico di Torino*, 62:209–223, 2004.
- [18] E. Casas-Alvero. *Algebraic Curves, the Brill and Noether Way*. Springer International Publishing, 2019.
- [19] M. Ceria. A computational approach to the theory of adjoints. *Atti della Accademia Peloritana dei Pericolanti-Classe di Scienze Fisiche, Matematiche e Naturali*, 94(2):7, 2016.
- [20] G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3):380–420, 2007.
- [21] V. Cossart and G. Moreno-Socías. Racines approchées, suites génératrices, suffisance des jets. *Annales de la Faculté des sciences de Toulouse : Mathématiques*, 6e série, 14(3):353–394, 2005.
- [22] D. Duval. *Diverses questions relatives au calcul formel avec des nombres algébriques*. PhD thesis, Université de Grenoble 1, 1987.
- [23] D. Duval. Rational Puiseux expansions. *Compos. Math.*, 70(2):119–154, 1989.
- [24] A. Fröhlich and J. C. Shepherdson. On the factorisation of polynomials in a finite number of steps. *Math. Z.*, 62:331–334, 1955.
- [25] A. Fröhlich and J. C. Shepherdson. Effective procedures in field theory. *Philos. Trans. Roy. Soc. London. Ser. A.*, 248:407–432, 1956.
- [26] W. Fulton. *Algebraic Curves – An Introduction to Algebraic Geometry*. Addison-Wesley, 1989.
- [27] W. Fulton. Adjoints and Max Noether’s Fundamentalsatz. In C. Christensen, A. Sathaye, G. Sundaram, and C. Bajaj, editors, *Algebra, Arithmetic and Geometry with Applications: Papers from Shreeram S. Abhyankar’s 70th Birthday Conference*, pages 301–313. Springer, Berlin, Heidelberg, 2004.
- [28] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013.
- [29] V. D. Goppa. Codes associated with divisors. *Probl. Peredachi Inf.*, 13(1):33–39, 1977. English translation: *Problems of Inform. Transmission*, 1977, 13(1), 22–27.
- [30] V. D. Goppa. Algebraico-geometric codes. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 46(4):762–781, 1982. English translation: *Mathematics of the USSR-Izvestiya*, 1983, 21(1):75–91.

- [31] V. D. Goppa. Codes and information. *Uspekhi Mat. Nauk*, 39(1(235)):77–120, 1984. English translation: *Russ. Math. Surv.*, 1984, 39(1), 87–141.
- [32] D. Gorenstein. An arithmetic theory of adjoint plane curves. *Trans. Am. Math. Soc.*, 72(3):414–436, 1952.
- [33] S. Greco and P. Valabrega. On the theory of adjoints. In K. Lonsted, editor, *Algebraic Geometry. Summer Meeting, Copenhagen, August 7-12, 1978*, volume 732 of *Lect. Notes Math.*, pages 98–123. Springer-Verlag Berlin Heidelberg, 1979.
- [34] S. Greco and P. Valabrega. On the theory of adjoints II. *Rendiconti del Circolo Matematico di Palermo*, 31(1):5–15, 1982.
- [35] G. Haché. Computation in algebraic function fields for effective construction of algebraic-geometric codes. In G. Cohen, M. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 262–278. Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.
- [36] G. Haché. *Construction Effective des Codes Géométriques*. PhD thesis, Université Paris 6, France, 1996.
- [37] G. Haché. L’algorithme de Brill–Noether appliqué aux courbes réduites. Technical Report, Rapport de recherche n° 1998-01, Laboratoire d’Arithmétique, de Calcul formel et d’Optimisation ESA - CNRS 6090, Université de Limoges, France, 1998. https://www.unilim.fr/laco/rapports/1998/R1998_01.pdf.
- [38] F. Hess. Computing Riemann–Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.
- [39] J. van der Hoeven and G. Lecerf. Composition modulo powers of polynomials. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '17*, pages 445–452. New York, NY, USA, 2017. ACM.
- [40] J. van der Hoeven and G. Lecerf. Directed evaluation. *J. Complexity*, 60:101498, 2020.
- [41] M.-D. Huang and D. Ierardi. Efficient algorithms for the Riemann–Roch problem and for addition in the Jacobian of a Curve. *J. Symbolic Comput.*, 18:519–539, 1994.
- [42] X. Huang and V. Y. Pan. Fast rectangular matrix multiplication and applications. *J. Complexity*, 14(2):257–299, 1998.
- [43] C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Computing minimal interpolation bases. *J. Symbolic Comput.*, 83:272–314, 2017.
- [44] O. H. Keller. *Vorlesungen über algebraische Geometrie*. Akademie Verlag Leipzig, 1974.
- [45] K. Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007.
- [46] A. Klyachko and O. Kara. Singularities of the modular curve. *Finite Fields Appl.*, 7(3):415–420, 2001.
- [47] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 3rd edition, 2002.
- [48] D. Le Brigand and J.-J. Risler. Algorithme de Brill–Noether et codes de Goppa. *Bulletin de la société mathématique de France*, 116(2):231–253, 1988.
- [49] A. Le Gluher and P.-J. Spaenlehauer. A fast randomized geometric algorithm for computing Riemann–Roch spaces. *Math. Comp.*, 89:2399–2433, 2020.
- [50] G. Lecerf. On the complexity of the Lickteig–Roy subresultant algorithm. *J. Symbolic Comput.*, 92:243–268, 2019.
- [51] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *J. Symbolic Comput.*, 35(4):377–401, 2003.
- [52] V. Neiger. *Bases of relations in one or several variables: fast algorithms and applications*. PhD thesis, École Normale Supérieure de Lyon (France) – University of Waterloo (Canada), 2016. <https://tel.archives-ouvertes.fr/tel-01431413>.
- [53] V. Neiger. Fast computation of shifted Popov forms of polynomial matrices via systems of modular polynomial equations. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '16*, pages 365–372. New York, NY, USA, 2016. ACM.
- [54] V. Neiger, J. Rosenkilde, and G. Solomatov. Computing Popov and Hermite forms of rectangular polynomial matrices. In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation, ISSAC '18*, pages 295–302. New York, NY, USA, 2018. ACM.
- [55] M. Nüsken and M. Ziegler. Fast multipoint evaluation of bivariate polynomials. In S. Albers and T. Radzik, editors, *Algorithms – ESA 2004. 12th Annual European Symposium, Bergen, Norway, September 14-17, 2004*, volume 3221 of *Lect. Notes Comput. Sci.*, pages 544–555. Springer Berlin Heidelberg, 2004.

- [56] D. Polemi, M. Hassner, O. Moreno, and C. J. Williamson. A computer algebra algorithm for the adjoint divisor. In *Proceedings. IEEE International Symposium on Information Theory. San Antonio, TX, USA*, pages 358–358. IEEE, 1993.
- [57] A. Poteaux. *Calcul de développements de Puiseux et application au calcul de groupe de monodromie d'une courbe algébrique plane*. PhD thesis, Université de Limoges, 2008.
- [58] A. Poteaux and M. Rybowicz. Improving complexity bounds for the computation of Puiseux series over finite fields. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC'15*, pages 299–306. ACM, 2015.
- [59] A. Poteaux and M. Weimann. Computing Puiseux series: a fast divide and conquer algorithm. Technical Report, arXiv:1708.09067, 2018. <https://arxiv.org/abs/1708.09067>. To appear in *Ann. Henri Lebesgue*.
- [60] I. Stenger. Hess.lib. A SINGULAR 4.1.2 library for Riemann–Roch space of divisors on function fields and curves. 2019. <http://www.singular.uni-kl.de>.
- [61] I. Stenger and J. Böhm. Brillnoether.lib. A SINGULAR 4.1.2 library for Riemann–Roch spaces of divisors on curves. 2019. <http://www.singular.uni-kl.de>.
- [62] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag Berlin Heidelberg, 2nd edition, 2009.
- [63] A. Storjohann. *Algorithms for matrix canonical forms*. PhD thesis, Swiss Federal Institute of Technology in Zürich (Switzerland), 2000.
- [64] M. A. Tsfasman, S. G. Vlăduț, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov–Gilbert bound. *Math. Nachr.*, 109(1):21–28, 1982.
- [65] E. J. Volcheck. Computing in the Jacobian of a plane algebraic curve. In L. M. Adleman and M.-D. Huang, editors, *Algorithmic Number Theory. First International Symposium, ANTS-I Ithaca, NY, USA, May 6–9, 1994. Proceedings*, volume 87 of *Lect. Notes Comput. Sci.*, pages 221–233. Springer Berlin Heidelberg, 1994.