Computing Riemann-Roch spaces via Puiseux expansions

Simon Abelard, Elena Berardini, Alain Couvreur, Grégoire Lecerf

Computing Riemann–Roch spaces via Puiseux expansions*

SIMON ABELARD[ab], ELENA BERARDINI[cd], ALAIN COUVREUR[ecf], 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

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 $\delta\geqslant 1$.

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 $\mathbb{K}$-rational divisor D

*. 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. Elena Berardini has also received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 899987.

of C we are interested in computing a $\mathbb{K}$-basis of the Riemann–Roch space

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

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 [15]. 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 [28, 29, 30]. 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" [9, 11], a construction itself involved in decentralized computations. In algebraic geometry, Riemann–Roch spaces intervene in arithmetic operations in Jacobians of curves [44, 47, 71].

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, Vlăduţ, and Zink [70] in order to construct codes asymptotically better than the Gilbert–Varshamov bound involve non-ordinary singularities [48], which are still not supported by the recent efficient algorithms of [3, 4, 52].

1.1. Brill–Noether in a nutshell

The present paper is in the vein of the seminal theory designed by Brill and Noether [15]. To the curve C is associated a so-called *adjoint divisor*, written $\mathcal{A}$, related to the singularities of C; see Section 3.2. Then the input $\mathbb{K}$-rational divisor 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 3. When $\deg D_+ < \deg D_-$, $\mathcal{L}(D)$ is $\{0\}$, so we freely assume that $\deg D_+ \geqslant \deg D_-$ 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 $\mathbb{K}$-basis of $\mathcal{L}(D)$. Brill and Noether showed that it is sufficient that $H \in \mathbb{K}[x, y, z]$ satisfies

$$\mathrm{Div}(H) \geqslant D_+ + \mathcal{A}. \tag{1.1}$$

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 $\deg \mathcal{A}$. 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 $\ell(D)$ denote the dimension of $\mathcal{L}(D)$. The second part of the Brill–Noether method consists in computing polynomials $G_1, \ldots, G_{\ell(D)}$ of degree d such that $\{G_i/H\}_{i=1,\ldots,\ell(D)}$ is a basis of $\mathcal{L}(D)$. These polynomials can be obtained as a basis of homogeneous polynomials $G \in \mathbb{K}[x,y,z]$ of degree d, "defined modulo F", that satisfy

$$\mathrm{Div}(G) \geqslant \mathrm{Div}(H) - D.$$

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

1.2. Computational model

For complexity analyses, we use an algebraic model over a general field $\mathbb{K}$ (typically computation trees [16]), 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 [27, 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 [27].

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 $\omega < 2.37286$ [7]. 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 $\varpi < 1.629$ [51, Table 2, half of the upper bound for $\omega(2)$] (combined with the tensor permutation lemma [43, Corollary 7]).

1.3. Related work

Adjoint curves. The notion of adjoint for plane curves was introduced by Brill and Noether [15] 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 [31], 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 [46] and [32, Definitions 2.12 and 2.13]. More recently in [8, Appendix A, Section 2] and then in [26], 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 [18, 19]. All these notions are proven to be equivalent when dealing with curves having only ordinary singularities: see [32, Corollary 4.16] and [25, Chapter 8, Section 5, Proposition 8]. In the case of non-ordinary singularities, Greco and Valabrega proved in [32, Theorem 4.6] that Gorenstein's and Keller's adjoint conditions are equivalent, and in [32, Theorem 4.13] that the Brill–Noether one is actually more restrictive. Examples of an adjoint in the sense of Gorenstein (equivalently of Keller) that is not an adjoint in the sense of Brill and Noether can be found in [32, Example 4.5] and [33, Example 2.5]. Following [26], one can further 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 [6], Abhyankar and Sathaye proposed an adjoint notion depending on infinitely near singular points on the curve, while in [33] 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 [32, 33], and also to [21] for a computational approach.

Algorithms. As said, the seminal Brill–Noether approach [15] to compute Riemann–Roch spaces was originally restricted to ordinary curves, and later extended to arbitrary plane curves by Le Brigand and Risler [50]. 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 [50]. Other algorithms in the vein of the Brill–Noether approach have been proposed by Huang and Ierardi [44] still for ordinary curves, and by Campillo and Farrán [18, 19] in combination with the theory of Hamburger–Noether expansions. An implementation of a Brill–Noether variant for general curves is available within the SINGULAR [67] computer algebra system.

More recently, fast algorithms have been designed for nodal curves [3, 52], leading to a complexity exponent as small as $(\omega+1)/2$. Then, ordinary curves have been handled in [4] with the same complexity exponent. Comparisons between algorithms for ordinary curves can be found in [4].

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, and that makes use of integral bases. The state-of-the-art algorithm of this family is due to Hess [38] and is implemented both in the MAGMA [12] and SINGULAR [66] 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 $\mathcal{A}$ of the curve C.

Our first contribution is a new simple rewriting of the adjoint $\mathcal{A}$ of C in terms of the rational Puiseux expansions $(X_i(t), Y_i(t))$ centered at the singular points of C; see Definitions 2.8 and 2.9. This condition is derived from the one based on differential forms [8, 26]. In this way, the adjoint condition $\mathrm{Div}(H) \geqslant \mathcal{A}$ 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 3.2.

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 $\mathrm{Div}_P(B) \geqslant \mathrm{Div}_P(A) + \mathcal{A}_P$ then Noether's condition is satisfied by the triple (F, A, B) at P; see Section 3.3. 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 4.1. In other words, our approach avoids both desingularizing C explicitly and 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 $\mathrm{Div}(H)$; see Section 4. 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 7.4.

In order to prove our main Theorem 7.8, 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 [4]. Its bottleneck lies in linear system solving. The exponent ω is achieved by means of a generic solver, but we also develop a more promising alternative approach via the aforementioned $\mathbb{K}[x]$-modules.

Further new technical ingredients also concern divisors, for which we develop efficient algorithms for their power series expansion representation in Section 3. This representation is more convenient than the global one used in [3, 4] because it fits both smooth and non-smooth divisors.

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 [38] also uses $\mathbb{K}[x]$-modules to represent and compute Riemann–Roch spaces, and achieves a polynomial complexity bound for general curves but the exact complexity exponent does not seem to have been analyzed so far, still 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. PREREQUISITES

This section is mostly devoted to notations, to well known algorithms in computer algebra, and to Puiseux expansions.

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 $\mathbb{K}[x_0, \ldots, x_n]$, we write $\mathcal{V}_{\mathbb{P}}(S)$ for the Zariski closed set in the projective space $\mathbb{P}^n$ defined as the common zeros of the elements of S, that is

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

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

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

If $\mathbb{M} := \mathbb{K}[x_1, \ldots, x_n]$ 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 $\mathbb{K}(x_1, \ldots, x_n)$ 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

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

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

Proof. The case $|\mathbb{K}|\geqslant \delta+1$ corresponds to [42, Proposition 9]. It will be sufficient for the main result of the paper. The general case is proved in [4, Lemma 2.5]. □

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 $\lambda_x u(t)+\lambda_y v(t)=t \bmod \chi(t)$ holds for some $(\lambda_x,\lambda_y)\in\mathbb{K}^2$. Then $f(u(t),v(t)) \bmod \chi(t)$ can be computed with*

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

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 $g(u(t),t) \bmod \chi(t)$ by means of [3, Lemma 2.1], that is a variant of an algorithm designed in [58]. □

We also recall two well known propositions for multi-remaindering and Chinese remaindering [27, Chapter 10, Section 3].

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

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

The change of primitive elements for quotient algebras of the form $\mathbb{K}[t]/(\theta(t))$ is a classical problem in computer algebra. The proof of the following lemma gathers efficient known techniques: early ideas go back to Le Verrier [53], and fast algorithms have been designed and popularized by Shoup [63, 64]. Here, we slightly improve [3, Lemma 2.3].

LEMMA 2.5. *Let $\theta(t) \in \mathbb{K}[t]$ be a monic separable polynomial of degree d. Given $e(t)$ in $\mathbb{K}[t]/(\theta(t))$ we can test if $e(t)$ is primitive for $\mathbb{K}[t]/(\theta(t))$ and, if so, compute its minimal polynomial $\tilde{\theta}$ along with $\eta(t) \in \mathbb{K}[t]_{<d}$ such that*

$$\begin{array}{rcl} \mathbb{K}[t]/(\theta(t)) & \cong & \mathbb{K}[t]/(\tilde{\theta}(t)) \\ t & \longmapsto & \eta(t) \\ e(t) & \longmapsto & t \end{array}$$

is an isomorphism, with $O(d^{\omega})$ field operations, whenever $\mathbb{K}$ has characteristic zero or $>d$.

Proof. Let Tr denote the trace map of $\mathbb{K}[t]/(\theta(t))$. To obtain the vector representation of Tr in the canonical basis of the powers of x, we use the well known Newton–Girard formula. In fact we let $\mu(z) := z^d \theta(1/z)$ stand for the reciprocal polynomial of θ, and we compute the power series expansion

$$-\frac{\mu'(z)}{\mu(z)} = \mathrm{Tr}(t) + \mathrm{Tr}(t^2)\, z + \cdots + \mathrm{Tr}(t^{d-1})\, z^{d-1} + O(z^d)$$

with $\tilde{O}(d)$ operations in $\mathbb{K}$.

Let $\tilde{\theta}$ be the characteristic polynomial of the multiplication by $e(t)$ endomorphism in this algebra. Le Verrier's method consists in computing

$$\mathrm{Tr}(e(t)^i), \text{ for } i = 1, \ldots, d.$$

This task is the transpose of modular composition (for instance see [64, Section 2], or [40, Section 1.2]), so it takes $O(d^{\omega})$ operations in $\mathbb{K}$ by combining [27, Theorem 12.4] with [16, Theorem 13.20]. Then, the generating series

$$\tau(z) := \sum_{i \geqslant 0} \mathrm{Tr}(e(t)^{i+1})\, z^i$$

satisfies the Newton–Girard formula

$$-\frac{\nu'(z)}{\nu(z)} = \tau(z) + O(z^d), \tag{2.1}$$

where $\nu(z) := z^d \tilde{\theta}(1/z)$ is the reciprocal of $\tilde{\theta}$. Therefore ν is recovered with $\tilde{O}(d)$ operations in characteristic zero or $>d$; for instance see [14, Corollary 1] or [34, Proposition 3]. Testing if $e(t)$ is primitive is equivalent to testing if $\tilde{\theta}$ is separable, which takes $\tilde{O}(d)$ operations in $\mathbb{K}$. If $e(t)$ is primitive then t can be written as

$$t = \eta(e(t)) \bmod \theta(t),$$

where $\eta = \eta_0 + \eta_1 t + \cdots + \eta_{d-1} t^{d-1} \in \mathbb{K}[t]$. We write Λ for the linear form

$$\begin{array}{rccl} \Lambda\colon & \mathbb{K}[t]/(\theta(t)) & \longrightarrow & \mathbb{K} \\ & a(t) & \longmapsto & \mathrm{Tr}(t\, a(t)), \end{array}$$

and verify that

$$\begin{aligned} \sum_{i \geqslant 0} \Lambda(e(t)^i)\, z^i &= \sum_{j=0}^{d-1} \eta_j \sum_{i \geqslant 0} \mathrm{Tr}(e(t)^{i+j})\, z^i \\ &= \eta(z^{-1})\,(z\,\tau(z) + d) + z^{-1}\rho(z^{-1}), \end{aligned}$$

where $\rho \in \mathbb{K}[z]$ has degree $<d-2$, so

$$\begin{aligned}\sigma(z) &:= z^{d-1}\nu(z)\sum_{i\geqslant 0}\Lambda(e(t)^i)\,z^i \\ &= z^{d-1}\eta(z^{-1})(-z\,\nu'(z)+d\,\nu(z))+z^{d-2}\rho(z^{-1})\,\nu(z)\end{aligned}$$

is a polynomial of degree $\leqslant 2d-1$. Since $-z\,\nu'(z)+d\,\nu(z)$ has degree $\leqslant 2d-1$, we further obtain that σ has degree $\leqslant 2d-2$. Again, using the transpose algorithm of the modular composition, the computation of $\Lambda(e(t)^i)$ for $i=0,\ldots,n-1$, hence of σ, takes $O(d^\omega)$ operations in $\mathbb{K}$ by [27, Theorem 12.4].

It follows that

$$z^{2d-1}\sigma(z^{-1}) = \eta(z)(-z^{d-1}\nu'(z^{-1})+dz^d\nu(z^{-1}))+\rho(z)\,z^{d+1}\nu(z^{-1}),$$

whence that

$$\begin{aligned}z^{2d-1}\sigma(z^{-1}) &= z\,\eta(z)\tilde{\theta}'(z)+\rho(z)\,z^{d+1}\nu(z^{-1}) \\ &= z\,\eta(z)\tilde{\theta}'(z)+\rho(z)\,z\,\tilde{\theta}(z).\end{aligned}$$

At this point $\tilde{\theta}$ has been computed, we may divide both sides of the latter identity by z, and deduce η as

$$\eta(z) = (z^{2d-2}\sigma(z^{-1}))\,/\,\tilde{\theta}'(z) \text{ rem } \tilde{\theta}(z),$$

in softly linear time. □

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

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

PROPOSITION 2.6. [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. Rational Puiseux expansions

From now and until the end of the section we gather known facts and complexity results about Puiseux series. It is assumed that $\mathbb{K}$ has characteristic zero. We rely on recent papers by Poteaux and his collaborators [60, 61, 62], 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

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

where $\mathrm{Res}_y(F,F_y)$ represents the resultant of F and F_y regarded in the main variable y. It is well known that F admits d_y distinct roots in the field of Puiseux series

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

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.

PROPOSITION 2.7. [23, 24] *Let F be an absolutely irreducible polynomial in $\mathbb{K}((x))[y]$ of degree $d_y = e$. Then, there exists $\gamma \in \mathbb{K} \setminus \{0\}$ and $\sum_{i=n}^{\infty} \beta_i t^i \in \mathbb{K}((t))$ 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 [24, Section 1, p. 124], and the proof of their existence follows from a variant of the Newton polygon method [24, Section 4.4]. □

This proposition motivates the following definition, still extracted from [23, 24].

DEFINITION 2.8. *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 $k = 0, \ldots, e-1$:

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

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

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

The integer e is called the *ramification index* of the Puiseux expansions of F: no Puiseux expansion of F belongs to $\bar{\mathbb{K}}((x^{1/e'}))$ with $e' < e$. 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.

For algorithmic purposes and for avoiding irreducible polynomial factorization, we need to revisit Definition 2.8 in order to allow rational Puiseux expansions to be defined over products of fields.

DEFINITION 2.9. *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 $i = 1, \ldots, s$ such that:*

- *$\mu_i \in \mathbb{K}[a]$ is monic and separable; we set $\mathbb{E}_i := \mathbb{K}[a]/(\mu_i(a))$ and α_i will represent the class of a in $\mathbb{E}_i$,*
- *$(X_i(t) = \gamma_i t^{e_i}, Y_i(t)) \in \mathbb{E}_i((t))^2$,*
- *γ_i and the initial coefficients of Y_i and $F_Y(X_i(t), Y_i(t))$ are invertible in $\mathbb{E}_i$,*
- *$\{1, \ldots, s\} \times \mathcal{V}_{\mathbb{A}}(\mu_i)$ is in one-to-one correspondence with the absolutely irreducible factors of F. Precisely, for any $i \in \{1, \ldots, s\}$ 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 2.8) of an absolutely irreducible factor of F, where π_α stands for the natural projection from $\mathbb{E}_i[[t]]$ onto $\mathbb{K}[\alpha][[t]]$.*

Example 2.10. Let us take $\mathbb{K} := \mathbb{Q}$ and

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

We have $\mathrm{val}_x(\mathrm{Disc}_y F) = 33$. With the Newton polytope algorithm, we compute three rational Puiseux expansions with the representation of Definition 2.9:

$$\begin{array}{lll}
\mu_1(a) := a^2-2a+2 & \mu_2(a) := a & \mu_3(a) := a \\
X_1(t) := t & X_2(t) := t^3 & X_3(t) := -t^2 \\
Y_1(t) := -t+\alpha_1 t^2+O(t^3) & Y_2(t) := t+O(t^2) & Y_3(t) := -t^4+t^6-2\,t^8+5\,t^{10}+ \\
 & & \quad t^{11}+O(t^{12})
\end{array}$$

PROPOSITION 2.11. *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 2.9. Then, we have*

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

Proof. Let ζ_i stand for a primitive e_i-th root of unity. The multiplicative property of the resultant yields

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

On the other hand, for $k = 0,\dots,e_{i-1}$ we verify that

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

2.4. Puiseux expansions at ramified points

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

$$\begin{array}{rcl}
\mathcal{V}_{\mathbb{A}}(F) & \longrightarrow & \bar{\mathbb{K}} \\
(x,y) & \longmapsto & x.
\end{array}$$

The following proposition is a consequence of the proof of [62, Theorem 1.2].

PROPOSITION 2.12. *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 $\mathbb{L}_i := \mathbb{K}[b]/(\Delta_i(b))$; β_i will represent the class of b in $\mathbb{L}_i$;*
- *For $i = 1,\dots,r$, quadruples $((\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t), \sigma_{i,j}))_{j=1,\dots,s_i}$ with $\mu_{i,j}(a) \in \mathbb{L}_i[a]$, $\sigma_{i,j} \in \mathbb{N}_{\geqslant 0}$, and*

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

  where $\mathbb{E}_{i,j} := \mathbb{L}_i[a]/(\mu_{i,j}(a))$; $\alpha_{i,j}$ will represent the class of a in $\mathbb{E}_{i,j}$;

Such that the following properties hold:

- *$\mathrm{Disc}_y F = \Delta_1^{m_1} \cdots \Delta_r^{m_r}$, where the $\Delta_i \in \mathbb{K}[x]$ are pairwise separable coprime factors of $\mathrm{Disc}_y F$ 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 $\geqslant 1$, and its non-zero coefficients are invertible in $\mathbb{L}_i$, 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 β_i zero or invertible in $\mathbb{L}_i$, $\gamma_{i,j}$ invertible in $\mathbb{E}_{i,j}$ and $e_{i,j}\geqslant 1$, for $i=1,\dots,r$ and $j=1,\dots,s_i$;*
- *The non-zero coefficients of $Y_{i,j}$ are invertible in $\mathbb{E}_{i,j}$, 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*

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

for $i=1,\dots,r$ and $j=1,\dots,s_i$;
- *For $i=1,\dots,r$ and for any root β of Δ_i, let π_β stand for the natural projection $\mathbb{L}_i\to\mathbb{K}[\beta]$ (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 2.9.

Proof. We assume that the reader is familiar with [62], especially with Sections 5 and 6. We compute the "D5-desingularisation" of F, with the meaning of [62, Definition 6.1, based on Definition 5.10], and with an expected number of $\tilde{O}(\delta^3)$ operations in $\mathbb{K}$ by [62, Proposition 6.2]. As a result, we directly obtain all the needed data and properties but the following ones, which require a closer look at the internal calculations:

- The truncation of the parametrization $(X_{i,j}(t),Y_{i,j}(t))$ is computed at precision $>2\sigma_{i,j}\geqslant\sigma_{i,j}+1$. This is not explicitly stated in [62], that focuses on singular parts. But this is a byproduct of [62, Proposition 3.14], that is passed on Step 5 of algorithm MonicRNP3. This internal precision is indeed required by the Hensel lifting subroutine.
- The valuation of $F_y(X_{i,j}(t),Y_{i,j}(t))$ is determined by the successive internal Newton polygons leading to $(X_{i,j}(t),Y_{i,j}(t))$ during the calculations; see [62, Lemma 3.16]. On the other hand all the Puiseux expansions represented by the pair $(X_{i,j}(t),Y_{i,j}(t))$ share the same sequence of Newton polygons: this is ensured by Step 2 of [62, Algorithm Polygon-Data]. Consequently, the initial coefficient of $F_y(X_{i,j}(t),Y_{i,j}(t))$ is invertible. □

Proposition 2.12 will play a part in computing adjoint divisors of curves in the next section. This computation will not be the bottleneck of our main algorithm (underlying Theorem 7.8): a complexity bound $O(\delta^{2\omega})$ within Proposition 2.12 would suffice for Theorem 7.8.

Example 2.13. (Continued from Example 2.10) 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 2.12. The equation $F=0$ defines a curve $\mathcal{U}_{\mathbb{A}}(F)$ of degree $\delta=7$. The discriminant of F in y is

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

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

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

Here β_1 is the class of b in $\mathbb{L}_1 := \mathbb{K}[b]/(\Delta_1(b))$. The y-coordinates of the points of $\Pi_x^{-1}(\beta_1)$ are the roots of $F(\beta_1, y) = y^7 = 0$, that is the singleton $\{0\}$. We obtain the following truncations for the Puiseux expansions (recall that $\alpha_{1,1}$ represents a root of $\mu_{1,1}$):

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

The y-coordinates of the points of $\Pi_x^{-1}(\beta_2)$ 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 of $\mathbb{E}_{2,2}$.

Remark 2.14. The first preprint version [2] of the present paper contains another proof of Proposition 2.12 independent of Sections 5 and 6 of [62]. It relies on the combination of [62, Theorem 1.1] and the directed evaluation paradigm [41]. The resulting algorithm is expected to be easier to implement than the one in [62].

2.5. 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 2.8. The next proposition is well known and is often deduced from algorithms that compute Puiseux expansions. For completeness we include a standalone proof based on the definitions.

PROPOSITION 2.15. *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:*

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

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 2.3. Let us write $Y(t)=\sum_{i\geqslant 0}\beta_i t^i$ as before, and consider the morphism of $\bar{\mathbb{K}}((x))$-algebras

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

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

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

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

3. DIVISORS

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

3.1. Places and valuations

A *place* $\mathcal{P}$ of $\bar{\mathbb{K}}(\mathcal{C})$ 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 2.8. The point $(X(0):Y(0):1)$ of $\mathcal{C}$ is called the *center* of $\mathcal{P}$. From Proposition 2.15 a place $\mathcal{P}$ induces a valuation as follows:

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

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

Remark 3.1. This representation of places depends on ambient coordinates. For instance, a place $\mathcal{P}$ centered at a regular point P of $\mathcal{C}$ has ramification index 1 if $F_y(P)\neq 0$, but ramification index $\geqslant 2$ otherwise. However the valuation induced by a place does not depend on the coordinates.

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

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

The *support* of D, denoted by $\operatorname{supp} D$, 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. The *degree* of D is defined by

$$\deg D := m_1 + \cdots + m_s.$$

If $\mathcal{E}$ is a finite subset of C, then $\mathcal{P}|\mathcal{E}$ will mean that $\mathcal{P}$ 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

$$\operatorname{Div}(A) = \sum_{\mathcal{P}|\mathcal{V}_{\mathbb{P}}(F,A)} \operatorname{val}_{\mathcal{P}}(A)\, \mathcal{P}.$$

3.2. Adjoint divisor

Let us assume that the set of singular points of C, written $\operatorname{Sing}(\mathcal{C})$, lies in the affine chart $z=1$. Let $\mathcal{P}$ be a place represented by an expansion $(X(t), Y(t))$ as above. Following [8], the *local adjoint divisor* of C at a point $P \in \operatorname{Sing}(\mathcal{C})$ is defined by

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

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

$$\mathcal{A} := \sum_{P \in \operatorname{Sing}(\mathcal{C})} \mathcal{A}_P. \tag{3.1}$$

Remark 3.2. It is well known that $\mathcal{A}$ is positive. In fact, this can be seen from the following calculations. Let $((\mu_i(a), X_i(t) = \gamma_i t^{e_i}, Y_i(t)))_{i=1,\ldots,s}$ 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

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

and we note that

$$\operatorname{val}_t\left(\prod_{k=1}^{e_{i-1}} (Y_1(t) - Y_1(\zeta_i^k t^{e_i}))\right) \geqslant e_i - 1,$$

which ensures that the multiplicity of the place $(X_1(t), Y_1(t))$ in $\mathcal{A}$ is nonnegative.

Remark 3.3. It is usual to extend the valuation induced by a place $\mathcal{P}$ to differential forms of $\mathcal{C}$. The multiplicity of $\mathcal{P}$ in the adjoint divisor is classically defined by

$$\mathrm{val}_{\mathcal{P}}\left(\frac{\mathrm{d}x}{F_y}\right) := \mathrm{val}_t\left(\frac{e\,t^{e-1}}{F_y(X(t),Y(t),1)}\right).$$

DEFINITION 3.4. *A homogeneous polynomial $A \in \mathbb{K}[x,y,z]$ is* adjoint *to $\mathcal{C}$ if* $\mathrm{Div}_P(A) \geqslant \mathcal{A}_P$ *for all singular points P of $\mathcal{C}$. It is said to be* sharply adjoint *to $\mathcal{C}$ if the inequalities are equalities for all singular points P.*

Example 3.5. Let $\mathcal{C}$ be the curve defined by $y^2 - x^3 = 0$ in the affine chart $z = 1$. We recall that in [46] Keller proposed a notion of adjoint that is used in [50] for instance; see also [32, Definitions 2.12 and 2.13]. In order to compute Keller's adjoint divisor, we perform a single blow-up of equation $y = t\,x$. The strict transform $\tilde{\mathcal{C}}$ is defined by $t^2 - x = 0$. The exceptional divisor is defined by x: it intersects $\tilde{\mathcal{C}}$ at the origin with multiplicity $m = 2$. Consequently, the Keller adjoint divisor is:

$$\mathcal{A} = (m-1)\,m\,(0,0) = 2\,(0,0).$$

Let $h := a(x) + b(x)\,y$, that rewrites $\tilde{h} := a(x) + x\,b(x)\,t$, in terms of the coordinates x, t. The condition $\mathrm{Div}(h) \geqslant \mathcal{A}$ means that $\tilde{h}$ vanishes at the origin with intersection multiplicity $\geqslant 2$. This is equivalent to

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

and then equivalent to $\mathrm{val}_t(a(t^2)) \geqslant 2$.

On the other hand, the adjoint condition defined in (3.1) is obtained from the single place $\mathcal{P}$ parametrized by $(X(t),Y(t)) = (t^2,t^3)$, that yields

$$\mathrm{val}_{\mathcal{P}}\left(\frac{\mathrm{d}x}{F_y}\right) = \mathrm{val}_t\left(\frac{2\,t}{2\,t^3}\right) = -2.$$

It follows that h is adjoint if, and only if, $\mathrm{val}_t(h(t^2,t^3)) \geqslant 2$. This is equivalent to $\mathrm{val}_t(a(t^2)) \geqslant 2$. As expected, the adjoint definition (3.1) is the same as Keller's one in this example.

3.3. Noether's condition

Let $P \in \mathbb{P}^2$ be a singular point of $\mathcal{C}$. 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:

$$F(x,y,1) = u(x,y) \prod_{i=1}^{m} (y - \varphi_i(x)), \tag{3.2}$$

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

DEFINITION 3.6. (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 3.7. *Let P be a point of $\mathcal{C}$, and consider two homogeneous polynomials A and B in $\mathbb{K}[x,y,z]$ that are prime to F. If $\mathrm{Div}_P(B) \geqslant \mathrm{Div}_P(A) + \mathcal{A}_P$ 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 $\varphi_1, \ldots, \varphi_m$ denote the Puiseux expansions introduced in (3.2). By conjugation, the set $\{\varphi_1,\ldots,\varphi_m\}$ is naturally partitioned into places $\mathcal{P}_1, \ldots, \mathcal{P}_s$, with $s \leqslant m$. The ramification index of φ_i is written e_i. The assumption means that

$$\mathrm{val}_{\mathcal{P}_i}\left(\frac{B}{A}\right) \geqslant -\mathrm{val}_{\mathcal{P}_i}\left(\frac{\mathrm{d}x}{F_y}\right),$$

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

$$\mathrm{val}_x\left(\frac{B}{A}(x,\varphi_i(x),1)\right) - \mathrm{val}_x(F_y(x,\varphi_i(x),1)) \geqslant -\left(1-\frac{1}{e_i}\right) > -1. \tag{3.3}$$

The Lagrange interpolation formula in

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

gives

$$\left(\frac{B}{A}\right)(x,y,1) \equiv c(x,y) \bmod \prod_{i=1}^{m} (y-\varphi_i(x)), \tag{3.4}$$

where

$$c(x,y) := \sum_{i=1}^{m} \frac{B(x,\varphi_i(x),1)}{A(x,\varphi_i(x),1)} \frac{\prod_{j\neq i} (y-\varphi_j(x))}{F_y(x,\varphi_i(x),1)}. \tag{3.5}$$

Using that $\mathrm{val}(a+b) \geqslant \min(\mathrm{val}(a), \mathrm{val}(b))$, Equation (3.3) implies

$$\mathrm{val}_x(c(x,y)) \geqslant \min_i \mathrm{val}_x\left(\frac{B}{A}(x,\varphi_i(x),1)\,\frac{1}{F_y(x,\varphi_i(x),1)}\right) > -1. \tag{3.6}$$

Since interchanging i and j in the right-hand side of Equation (3.5) leaves the expression of c unchanged, c is invariant under the action of transpositions, hence under any permutation of $\varphi_1, \ldots, \varphi_m$. Consequently, c can be written as a polynomial in terms of elementary symmetric functions of $\varphi_1,\ldots,\varphi_m$; see [49, 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 (3.6) is a nonnegative integer.

Equation (3.4) 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. □

The proof of Proposition 3.7 turns out to be remarkably elementary compared to other ones in the literature that appeal to desingularization trees or conductor ideals. Proposition 3.7 can be used in replacement of [4, Proposition 3.5] so that [4, Section 3] can be straightforwardly revisited into a complete elementary proof of the Brill–Noether method in characteristic zero.

3.4. 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 3.8. *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:*

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

We say that 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 $\mathcal{V}_{\mathbb{P}}(F,G)$ 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 $\mathcal{E}$.

From a geometric point of view, x is primitive for $\mathcal{V}_{\mathbb{A}}(F(x,y,1),F_y(x,y,1))$ if, and only if, the following projection is injective:

$$\begin{aligned}\mathcal{V}_{\mathbb{A}}(F(x,y,1),F_y(x,y,1)) &\longrightarrow \bar{\mathbb{K}}\\ (x,y) &\longmapsto x.\end{aligned}$$

DEFINITION 3.9. *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 $\mathcal{V}_{\mathbb{A}}(F(x,y,1),F_y(x,y,1))$. Then, the* series expansions *of the adjoint divisor (3.1) 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 $i=1,\dots,r$, quadruples $((\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t), \sigma_{i,j}))_{j=1,\dots,s_i}$ with $\mu_{i,j}$ of degree $\geqslant 1$ 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 $\mathbb{E}_{i,j} := \mathbb{L}_i[a]/(\mu_{i,j}(a))$; The class of a in $\mathbb{E}_{i,j}$ will be written $\alpha_{i,j}$;

Such that the following properties hold:

- *The Δ_i are pairwise squarefree coprime factors of $\mathrm{Disc}_y(F(x,y,1))$ of multiplicity $m_i \geqslant 1$ (the m_i are not necessarily distinct), for $i=1,\dots,r$;*
- *$\mathcal{V}_{\mathbb{A}}(\Delta_1 \cdots \Delta_r)$ is the set of abscissas of the singular locus of $\mathcal{V}_{\mathbb{A}}(F(x,y,1))$;*
- *$\mu_{i,j}$ is monic and separable of degree $\geqslant 1$, and its non-zero coefficients are invertible in $\mathbb{L}_i$, for $i=1,\dots,r$ and $j=1,\dots,s_i$;*
- *$X_{i,j}$ writes as $\beta_i + \gamma_{i,j} t^{e_{i,j}}$, with β_i zero or invertible in $\mathbb{L}_i$, $\gamma_{i,j}$ invertible in $\mathbb{E}_{i,j}$ and $e_{i,j} \geqslant 1$, for $i=1,\dots,r$ and $j=1,\dots,s_i$;*
- *The non-zero coefficients of $Y_{i,j}$ are invertible in $\mathbb{E}_{i,j}$, 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 have*

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

  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 $\mathbb{L}_i \to \mathbb{K}[\beta]$, 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 2.9, and centered at the singular point of abscissa β.

In the following proposition, the series expansions of the adjoint divisor (3.1) are computed via Proposition 2.12. Informally speaking, among all the Puiseux expansions occurring in this proposition, it suffices to keep only those which are centered at singular points of the curve defined by F.

PROPOSITION 3.10. *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 $\mathcal{V}_{\mathbb{A}}(F(x,y,1), F_y(x,y,1))$. Then, the series expansions of the adjoint divisor, defined in Equation (3.1) and represented as in Definition 3.9, can be computed by an algorithm of Las Vegas type with an expected number of $\tilde{O}(\delta^3)$ operations in $\mathbb{K}$.*

Proof. Let us first recall a simple criterion to decide if a given point of $\mathcal{V}_{\mathbb{A}}(F(x,y,1))$ is regular from the knowledge of Puiseux expansions. Without loss of generality we can assume this point to be the origin. Regarded in $\bar{\mathbb{K}}[[x,y]]$, the polynomial $F(x,y,1)$ factorizes into $u(x,y)\,G(x,y)$ where u is invertible and $G \in \bar{\mathbb{K}}[[x]][y]$ is monic. The origin is a regular point if, and only if, $G_x(0,0) \neq 0$ or $G_y(0,0) \neq 0$. Let us assume that $G_y(0,0) = 0$. In this case, the condition $G_x(0,0) \neq 0$ becomes equivalent to the fact that the Newton polygon of G starts at the point $(0,1)$. Since this polygon ends at $(\deg_y G, 0)$, it admits a single edge. Consequently, the origin is regular if, and only if, G has a single rational Puiseux expansion of the form $X(t) = \gamma t^e$, $Y(t) = \rho t + O(t^2)$, where $e := \deg_y G$ and γ, ρ are non-zero elements of $\mathbb{K}$. Informally speaking in the neighborhood of the origin $G(x,y)$ approximates to $y^e - \rho^e x/\gamma$.

Then, we consider the data computed by the algorithm underlying Proposition 2.12, and we aim at discarding from them the rational Puiseux expansions centered at regular points of the curve $\mathcal{V}_{\mathbb{A}}(F(x,y,1))$. First, it is clear that we can discard all the quadruples $(\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t), \sigma_{i,j})$ satisfying $\sigma_{i,j} = 0$. Second, following the criterion of the preceding paragraph, and according to the assumptions on the coordinates, the remaining Puiseux expansions centered at regular points are the ones corresponding to indices i satisfying the following property: it remains a single quadruple $(\mu_{i,j}(a), X_{i,j}(t), Y_{i,j}(t), \sigma_{i,j})$ such that $\deg \mu_{i,j} = 1$ and $Y'_{i,j}$ is non-zero in $\mathbb{E}_{i,j}$ (hence invertible). These expansions are dropped, so the remaining ones are those centered at singular points of $\mathcal{V}_{\mathbb{A}}(F(x,y,1))$. □

Example 3.11. (Continued from Example 2.13) Let us take $\mathbb{K} := \mathbb{Q}$ and

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

that is absolutely irreducible. The point $(0:0:1)$ is the only singular point of the curve $\mathcal{C} = \mathcal{V}_{\mathbb{P}}(F)$. The adjoint divisor is made of the rational Puiseux expansions computed in Example 2.13 that are centered at $(0:0:1)$.

With the notation of Definition 3.9, for $i = 1, \ldots, r$ and $j = 1, \ldots, s_i$, we introduce

$$\tau_{i,j} := \mathrm{val}_t(F_y(X_{i,j}(t), Y_{i,j}(t), 1)) - (e_{i,j} - 1), \tag{3.7}$$

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 3.12. *Given $\mathcal{A}$ as in Definition 3.9, a homogeneous polynomial $A \in \mathbb{K}[x,y,z]$ is adjoint to the curve $\mathcal{C}$ defined by $F = 0$ if, and only if,*

$$\mathrm{val}_t(A(X_{i,j}(t), Y_{i,j}(t), 1)) \geqslant \tau_{i,j} \tag{3.8}$$

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

It is sharply adjoint to $\mathcal{C}$ if, and only if, Inequalities (3.8) 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 3.4 and the definition of divisors. □

PROPOSITION 3.13. *Given $\mathcal{A}$ as in Definition 3.9, testing if a homogeneous polynomial $A\in\mathbb{K}[x,y,z]$ of degree $<\delta$ in y and total degree $\leqslant d$ is sharply adjoint to the curve $\mathcal{C}$ defined by $F=0$ takes $\tilde{O}(\delta\max(d,\delta^2))$ operations in $\mathbb{K}$.*

Proof. We compute $A(x,y,1)\operatorname{rem}\Delta_i(x)^{m_i+1}$ for $i=1,...,r$ 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 2.6. Note that

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

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

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

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

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

operations in $\mathbb{K}$, thanks to Proposition 2.11. Finally, testing if the coefficient of degree $\tau_{i,j}$ in $A_i(X_{i,j}(t),Y_{i,j}(t),1)$ is non-zero takes softly linear time. □

4. DEGREE OF THE DENOMINATOR

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

4.1. 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 [25, Chapter 8], [50, Section 3], [4, 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 [4, Theorem 3.7] for the ordinary case can be straightforwardly extended to the non-ordinary case, using our Proposition 3.7 instead of [4, 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 $D = D' + \mathrm{Div}(h)$.

THEOREM 4.1. (Residue Theorem) *Let D and D' be two $\mathbb{K}$-rational divisors of the curve C defined by $F = 0$, such that $D \equiv D'$ and $D' \geqslant 0$. Suppose that $H \in \mathbb{K}[x,y,z]$ is a homogeneous polynomial prime to F such that $\mathrm{Div}(H) = D + \mathcal{A} + R$ for a positive $\mathbb{K}$-rational divisor R. Then, there exists a homogeneous polynomial $H' \in \mathbb{K}[x,y,z]$, prime to F, of the same degree as H, such that $\mathrm{Div}(H') = D' + \mathcal{A} + R$.*

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 4.2. *Let $L \in \mathbb{K}[x,y,z]$ be a homogeneous degree one polynomial such that $\mathrm{Div}(L)$ is smooth. Then, for any positive integer d, any non-zero element of $\mathcal{L}(d\,\mathrm{Div}(L) - \mathcal{A})$ admits a rational function representation in the form H/L^d, where $H \in \mathbb{K}[x,y,z]$ is a homogeneous polynomial of degree d.*

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

$$D' := D + \mathrm{Div}(h) \geqslant 0.$$

We apply Theorem 4.1 to D' and the decomposition

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

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

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

Consequently, we have

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

Then $\mathrm{Div}((H/L^d)/h)$ is zero, whence $(H/L^d)/h$ is a constant, by [68, Corollary 1.3.4]. Finally, we have shown that h is a $\mathbb{K}$-multiple of H/L^d in $\mathbb{K}(C)$. □

Let $\mathcal{A}$ be the adjoint divisor of C, defined in Equation (3.1), and recall that δ denotes the degree of the curve C. The genus g of C is

$$g := \frac{(\delta-1)(\delta-2) - \deg \mathcal{A}}{2}. \tag{4.1}$$

This relation is proved in [31, Theorem 11] using the definition of the adjoint divisor in terms of conductor ideals. Since this definition is equivalent to the one in Equation (3.1) by [26, 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 [59], where the formula is stated in terms of differential forms.

4.2. Degree bound

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

PROPOSITION 4.3. *Assume that the cardinality of $\mathbb{K}$ is infinite. Let D be a positive $\mathbb{K}$-rational divisor of C, and let*

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

Then, there exists a homogeneous polynomial $H \in \mathbb{K}[x,y,z]$ prime to F of degree d and such that

$$\mathrm{Div}(H) \geqslant D + \mathcal{A}$$

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

Proof. Fix a homogeneous polynomial $L \in \mathbb{K}[x,y,z]$ of degree 1 such that $\mathrm{Div}(L)$ is smooth. By Bézout's theorem [25, Section 5.3] we have $\deg(\mathrm{Div}(L)) = \delta$. We set

$$E := D + \mathcal{A}.$$

The assumption on d and Equation (4.1) lead to

$$\deg(d\,\mathrm{Div}(L) - E) = d\,\delta - \deg D - \deg \mathcal{A} \geqslant (\delta-1)(\delta-2) - \deg \mathcal{A} = 2g.$$

Let $P_1, \ldots, P_r$ denote the singular points of C and let $\mathcal{P}_{i,1}, \ldots, \mathcal{P}_{i,s_i}$ be the places centered at P_i for $i = 1, \ldots, r$. We can apply [25, Chapter 8, Section 8.6, Corollary 3]: even if this corollary in [25] is stated for ordinary curves, it applies without change for curves with arbitrary singularities as explained in [26, Section 4]. Alternatively, we refer the reader to [20, Theorem 4.9.7]. We fit in a situation where the Riemann–Roch theorem for $\bar{\mathbb{K}}(C)$ is an equality, that is

$$\dim_{\bar{\mathbb{K}}} \mathcal{L}_{\bar{\mathbb{K}}}(d\,\mathrm{Div}(L) - E - \mathcal{P}_{i,j}) = \dim_{\bar{\mathbb{K}}} \mathcal{L}_{\bar{\mathbb{K}}}(d\,\mathrm{Div}(L) - E) - 1,$$

for $i = 1, \ldots, r$ and $j = 1, \ldots, s_i$. By [65, Chapter II, Section 5, Proposition 5.8] we have

$$\mathcal{L}_{\bar{\mathbb{K}}}(d\,\mathrm{Div}(L) - E) = \bar{\mathbb{K}} \otimes \mathcal{L}(d\,\mathrm{Div}(L) - E).$$

Consequently, since $|\mathbb{K}|$ is infinite, there exist functions $h \in \mathcal{L}(d\,\mathrm{Div}(L) - E)$ which are not contained in any of the $\mathcal{L}_{\bar{\mathbb{K}}}(d\,\mathrm{Div}(L) - E - \mathcal{P}_{i,j})$ for any pair (i,j). From Lemma 4.2 such a function h admits a rational function representation of the form $h = H / L^d$. By construction of h,

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

is positive and smooth. □

4.3. Probability bound

If D is a smooth $\mathbb{K}$-rational divisor (that will be the case in our main algorithm), then Proposition 4.3 ensures the existence of polynomials $H \in \mathbb{K}[x,y,z]$ such that $\mathrm{Div}(H) \geqslant D + \mathcal{A}$ 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 4.4. *Let D be a smooth positive $\mathbb{K}$-rational divisor of a curve $C = \mathcal{V}_{\mathbb{P}}(F)$ 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 $\mathrm{Div}(H) \geqslant D + \mathcal{A}$*; by convention the zero polynomial is included in $\mathcal{H}$. Let $H_1, \ldots, H_l$ denote a basis of $\mathcal{H}$ and let $\mathcal{S}$ be a finite subset of $\mathbb{K}$. Then, for $(a_1, \ldots, a_l)$ taken at random in $\mathcal{S}^l$, the probability that $a_1 H_1 + \cdots + a_l H_l$ is not sharply adjoint is*

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

Proof. Set $H_a := a_1 H_1 + \cdots + a_l H_l$. Let us write $\mathcal{A} = \sum_{i=1}^{s} \tau_i \mathcal{P}_i$ into the sum of pairwise distinct places (with $\tau_i \geqslant 1$), and let $(X_i(t), Y_i(t))$ represent the rational Puiseux expansion of $\mathcal{P}_i$. If the a_i are regarded as variables, then H_a is sharply adjoint by Proposition 4.3, so the polynomial

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

is non-zero, where $\mathrm{coeff}(H_a(X_i(t), Y_i(t), 1), \tau_i)$ 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, $\Sigma(a_1, \ldots, a_l) \neq 0$. The total degree of Σ in the a_i is

$$\leqslant s \leqslant \deg \mathcal{A} \leqslant (\delta-1)(\delta-2).$$

The conclusion follows from the well known Schwartz–Zippel lemma; see [27, Lemma 6.44] for instance. □

5. DATA STRUCTURES

Before presenting the main algorithm, it still remains to describe the data structures for divisors, along with their main properties. We design specific data structures to represent divisors by local expansions and to operate on them efficiently. The present approach differs from the global representation of divisors used in [3, 4, 52]; the comparison is addressed at the end of the section. It yields a unified way to represent smooth and non-smooth divisors that will be useful in Section 6. As a benefit we can operate faster on the supports of the divisors and perform less multi-remaindering and Chinese remaindering (the inverse task of multi-remaindering).

5.1. Primitive elements

We recall usual terminologies.

DEFINITION 5.1. *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 3.4).*
- *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 $\mathbb{K}$. *In the sequel we will also say that λ* parametrizes *$\mathcal{E}$.*

With the notation of Definition 5.1, note that $\lambda_x u(t) + \lambda_y v(t) = t \bmod \theta(t)$ holds.

LEMMA 5.2. *Let $\mathcal{S}$ be a finite subset of $\mathbb{K}$. The probability that a random matrix $M := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with entries in $\mathcal{S}$ does not make the linear form x primitive for $M(\mathcal{E})$ is $\leqslant \binom{|\mathcal{E}|}{2} / |\mathcal{S}|$.*

Proof. The proof is rather elementary. For instance, it results from the combination of [52, Lemma 7] with the aforementioned Schwartz–Zippel lemma; see details in [4, Lemma 4.1] for instance. □

PROPOSITION 5.3. *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, whenever $\mathbb{K}$ has characteristic zero or $>|\mathcal{E}|$.

Proof. We compute

$$\begin{pmatrix} w_x \\ w_y \\ w_z \end{pmatrix} = M \begin{pmatrix} u \\ v \\ 1 \end{pmatrix}.$$

Then, $M(\mathcal{E}^{\#})$ is in the affine chart $z = 1$ if, and only if, w_z is invertible modulo θ. If so we can compute $\tilde{u} := w_x / w_z \bmod \theta$ and $\tilde{v} := w_y / w_z \bmod \theta$. Then we appeal to Lemma 2.5 with $\mathbb{K}[t]/(\theta(t))$ and $e(t) := \tilde{\lambda}_x \tilde{u}(t) + \tilde{\lambda}_y \tilde{v}(t)$. □

5.2. 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 with disjoint supports and whose difference 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.

5.2.1. Multi-set primitive representation

We will represent smooth divisors in a different manner from [3, 4, 52], that turns out to be more flexible and efficient for practice because several computations can be performed independently of the multiplicities. Informally speaking, a smooth divisor D will involve a primitive representation of its support, as detailed in the following definition.

DEFINITION 5.4. *Let $\mathcal{E}_1,\dots,\mathcal{E}_s$ be pairwise disjoint finite sets in the affine chart $z=1$ of $\mathcal{C}$, defined over $\mathbb{K}$, parametrized by the same primitive element $\lambda := \lambda_x x + \lambda_y y$, 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 $\mathcal{E}_1 \cup \cdots \cup \mathcal{E}_s$. Then, λ and the set of pairs $(\mathcal{E}_i, m_i)$ form a multi-set primitive representation *of the smooth positive divisor $D = m_1\mathcal{E}_1 + \cdots + m_s\mathcal{E}_s$. The form λ is said to be an* unramified primitive element *for D.*

Given λ and a pair $(\mathcal{E}_i, m_i)$ as in Definition 5.4, there exists a unique primitive element representation θ_i, u_i, v_i of $\mathcal{E}_i$. For convenience, we will write the support of a smooth divisor D in terms of its centers, that is as

$$\operatorname{supp} D := \mathcal{E}_1 \cup \cdots \cup \mathcal{E}_s.$$

LEMMA 5.5. *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 an unramified primitive element for the affine part of $M^{-1}(D)$ is*

$$\leqslant \frac{3\,|\operatorname{supp} D|^2}{|\mathcal{S}|}.$$

Proof. Let $P_1,\dots,P_s$ represent the support of D. Let $(M_{i,j})_{1\leqslant i,j\leqslant 3}$ denote the entries of M, and let $(N_{i,j})_{1\leqslant i,j\leqslant 3}$ denote the entries of $N := \det(M)\,M^{-1}$. The $N_{i,j}$ are polynomials of total degree 2 in the entries of M. If

$$\prod_{i=1}^{s} \left(N_{3,1}\,x(P_i) + N_{3,2}\,y(P_i) + N_{3,3}\,z(P_i)\right) \neq 0,$$

where $x(P_i)$, $y(P_i)$ and $z(P_i)$ represent the coordinates of P_i, then $M^{-1}(D)$ is in the affine chart $z=1$. As a straightforward application of the Schwartz–Zippel lemma, the probability that $M^{-1}(D)$ is not in this affine chart is $\leqslant 2s/|\mathcal{S}|$. If

$$\prod_{1\leqslant i<j\leqslant s} \left(N_{1,1}\,(x(P_i)-x(P_j)) + N_{1,2}\,(y(P_i)-y(P_j)) + N_{1,3}\,(z(P_i)-z(P_j))\right) \neq 0$$

then x is primitive for the support of $M^{-1}(D)$. So the probability that x is not primitive for the support of $M^{-1}(D)$ is $\leqslant 2\binom{s}{2}/|\mathcal{S}|$. Then we verify that

$$\frac{\partial(F\circ M)}{\partial y}(M^{-1}(P_i)) = M_{1,2}\frac{\partial F}{\partial x}(P_i) + M_{2,2}\frac{\partial F}{\partial y}(P_i) + M_{3,2}\frac{\partial F}{\partial z}(P_i).$$

Therefore, the probability that the support of $M^{-1}(D)$ intersects $\mathcal{V}_{\mathbb{P}}\left(\frac{\partial\,(F\circ M)}{\partial y}\right)$ is $\leqslant s/|\mathcal{S}|$, again by the Schwartz–Zippel lemma. □

LEMMA 5.6. *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 $u \operatorname{rem} \chi_i = u_i$ and $v \operatorname{rem} \chi_i = v_i$ for $i = 1, \ldots, s$, can be computed with $\tilde{O}(\deg \chi)$ operations in $\mathbb{K}$. Then $f(u,v) \operatorname{rem} \chi$ is obtained with

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

further operations in $\mathbb{K}$ by Lemma 2.2. Proposition 2.3 then yields $f(u,v) \operatorname{rem} \chi_i$ for $i = 1, \ldots, s$ with $\tilde{O}(\deg \chi)$ further operations in $\mathbb{K}$. □

PROPOSITION 5.7. *Let D be a smooth positive $\mathbb{K}$-rational divisor of $\mathcal{C}$ represented as in Definition 5.4, 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 an unramified primitive element for the affine part of $M(D)$, and if so compute the corresponding multi-set primitive representation with*

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} |\operatorname{supp} D| + |\operatorname{supp} D|^{\omega}\Big)$$

operations in $\mathbb{K}$, whenever $\mathbb{K}$ has characteristic zero or $> |\operatorname{supp} D|$.

Proof. With the notation of Definition 5.4, for $i = 1, \ldots, s$ 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. In the context of Proposition 5.3, 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 by Proposition 5.3.

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 $i = 1, \ldots, s$, and test if the result is prime to $\tilde{\theta}_i$, with

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} |\operatorname{supp} D|\Big)$$

further operations in $\mathbb{K}$, by Lemma 5.6. □

5.2.2. Expansions of multi-set primitive representations

Given a regular point P of $\mathcal{C}$, 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 5.8. *Given a subset of regular points $\mathcal{E}$ of $\mathcal{C}$ 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 $\mathcal{C}$ and β denotes the class of b in $\mathbb{L}$.

For a general positive smooth $\mathbb{K}$-rational divisor D of the form $m_1\mathcal{E}_1+\cdots+m_s\mathcal{E}_s$ represented as in Definition 5.4, its corresponding series expansions *are the set of the series expansions of $m_i\mathcal{E}_i$ for $i=1,\ldots,s$.*

LEMMA 5.9. *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 $i=1,\ldots,s$ represent the series expansions of a positive smooth divisor D (as in Definition 5.8). Then, $f(X_i(t),Y_i(t))$ for $i=1,\ldots,s$ can be computed with

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

operations in $\mathbb{K}$.

Proof. We follow the notation of Proposition 2.6, and compute $u_i(t):=\Gamma_{\theta_i,m_i}(X_i(t))$, $v_i(t):=\Gamma_{\theta_i,m_i}(Y_i(t))$ and $\chi_i:=\theta_i^{m_i}$. Thanks to Lemma 5.6 we obtain $f(u_i(t),v_i(t))\operatorname{rem}\chi_i$, for $i=1,\ldots,s$, with

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

operations in $\mathbb{K}$. Then, we obtain $f(X_i(t),Y_i(t))$ as $\Gamma^{-1}_{\theta_i,m_i}(f(u_i(t),v_i(t))\operatorname{rem}\chi_i)$. Evaluating Γ_{θ_i,m_i} and its inverse takes softly linear time by Proposition 2.6. □

LEMMA 5.10. *Let D be a smooth positive $\mathbb{K}$-rational divisor given by series expansions. Series expansions of $2D$ can be computed with*

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

operations in $\mathbb{K}$.

Proof. Let $D=m_1\mathcal{E}_1+\cdots+m_s\mathcal{E}_s$ 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 $i=1,\ldots,s$. 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 $i=1,\ldots,s$, amount to

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

operations in $\mathbb{K}$ by Lemma 5.9. □

PROPOSITION 5.11. *Given a multi-set primitive representation of a positive smooth $\mathbb{K}$-rational divisor D, the corresponding series expansions can be computed with*

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

operations in $\mathbb{K}$.

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

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

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

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

Then, we compute $2E_k, 4E_k, \ldots, 2^{k+1}E_k$ via Lemma 5.10. 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

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

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

5.3. Addition and subtraction

In this subsection we consider two smooth positive divisors D_1 and D_2 represented by $((\theta_{1,i}, u_{1,i}, v_{1,i}, m_{1,i}))_{i=1,\ldots,s_1}$ and $((\theta_{2,i}, u_{2,i}, v_{2,i}, m_{2,i}))_{i=1,\ldots,s_2}$, as in Definition 5.4. 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 5.12. *Given two smooth positive divisors D_1 and D_2 in multi-set primitive representation, parametrized by the same unramified 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 an unramified primitive element for $D := D_1 + D_2$, and, if so, compute the corresponding multi-set primitive representation with

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

operations in $\mathbb{K}$.

Proof. The form λ is an unramified primitive element for $D := D_1 + D_2$ if, and only if, D_1 and D_2 have the same support. In this case the multi-set primitive representation of D is obtained by computing a common factor basis for $(\theta_{1,i})_{i=1,\ldots,s_1}$ and $(\theta_{2,i})_{i=1,\ldots,s_2}$.

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

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

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

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

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

and D_2^{hi} to be

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

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

PROPOSITION 5.13. *Given two smooth positive divisors D_1 and D_2 in multi-set primitive representation as in Definition 5.4, sharing the same unramified primitive element $\lambda := \lambda_x x + \lambda_y y$, one can check if λ is an unramified primitive element for $D := D_1 + D_2$, and, if so, compute the corresponding multi-set primitive representation with*

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

operations in $\mathbb{K}$.

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

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

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

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

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

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

represent another smooth positive divisor written $\hat{D}_1 \leqslant D_1$. 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 $\tilde{O}(|\operatorname{supp} D_1| + |\operatorname{supp} D_2|)$.

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 $i = 1, \ldots, s_2$, in softly linear time, again via Proposition 2.3. For $i = 1, \ldots, s_2$ we set $\check{\theta}_{2,i} := \theta_{2,i} / \delta_i$, $\check{u}_{2,i} := u_{2,i} \operatorname{rem} \check{\theta}_{2,i}$, and $\check{v}_{2,i} := v_{2,i} \operatorname{rem} \check{\theta}_{2,i}$. The tuples

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

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

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

represent a smooth positive divisor written $\hat{D}_2 \leqslant D_2$. 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 5.12 ensures that $\hat{D}_1 + \hat{D}_2$ can be computed with $\tilde{O}(|\operatorname{supp} \hat{D}_1| + |\operatorname{supp} \hat{D}_2|)$ operations in $\mathbb{K}$, unless λ is not an unramified primitive element. Finally, the multi-set primitive representation of D is the union of the representations of $\check{D}_1$, $\hat{D}_1 + \hat{D}_2$, and $\check{D}_2$. □

LEMMA 5.14. *Given two smooth positive divisors D_1 and D_2 in multi-set primitive representation as in Definition 5.4, sharing the same unramified 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 primitive representation $D := [D_1 - D_2]_+$ in terms of λ with

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

operations in $\mathbb{K}$.

Proof. We proceed by induction on s_1 as in the proof of Lemma 5.12, from which we borrow the notation. If $s_1 = 1$, then we compute

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

via Proposition 2.3. We set

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

A multi-set primitive representation of D is made of λ and the tuples

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

and

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

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

If $s_1 \geqslant 2$, then we compute D_1^{lo}, D_1^{hi}, D_2^{lo}, and D_2^{hi} as in the proof of Lemma 5.12. Finally, we obtain $[D_1^{\mathrm{lo}} - D_2^{\mathrm{lo}}]_+$ and $[D_1^{\mathrm{hi}} - D_2^{\mathrm{hi}}]_+$ recursively, and merge the results. □

PROPOSITION 5.15. *Given two smooth positive divisors D_1 and D_2 in multi-set primitive representation, sharing the same unramified primitive element $\lambda := \lambda_x x + \lambda_y y$, the multi-set primitive representation of $[D_1 - D_2]_+$ in terms of λ can be computed with*

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

operations in $\mathbb{K}$.

Proof. As in the proof of Proposition 5.13 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 5.14 used with $\hat{D}_1$ and $\hat{D}_2$. □

5.4. Equivalence with global representation

For the sake of comparison with previous work, for smooth divisors, we prove the equivalence between the series expansion representation and the "global representation" used in [3, 4, 52]. This equivalence is not necessary to the rest of the paper. As a benefit, multiset primitive representations are cheaper for sums and partial subtractions since Hensel lifting is not needed. We recall that the ambient curve C in $\mathbb{P}^2$ is defined by the equation $F=0$.

PROPOSITION 5.16. *Given a smooth positive divisor $D=m_1P_1+\cdots+m_sP_s$ whose support is in the affine chart $z=1$, and given an unramified primitive element $\lambda_x x+\lambda_y y$ for D, there exist unique polynomials χ, u, and v in $\bar{\mathbb{K}}[t]$ with the following properties:*

Div-H$_0$. *χ is monic of degree* $\deg D$*, and u, v have degree* $<\deg D$*,*

Div-H$_1$. $F(u(t),v(t),1) \operatorname{rem} \chi(t)=0$*,*

Div-H$_2$. $\lambda_x u(t)+\lambda_y v(t)=t$*,*

Div-H$_3$. $\lambda_y \frac{\partial F}{\partial x}(u(t),v(t),1)-\lambda_x \frac{\partial F}{\partial y}(u(t),v(t),1)$ *is coprime with $\chi(t)$,*

Div-H$_4$. *The roots of χ are $\lambda(P_1),\ldots,\lambda(P_s)$, with respective multiplicities $m_1,\ldots,m_s$, and $\{(u(\zeta), v(\zeta)) : \chi(\zeta)=0\}=\{P_1,\ldots,P_s\}$ holds.*

Proof. The proof can be found in [52, Section 3] or in [3, Proposition 3.1]. □

A *global representation* of a smooth $\mathbb{K}$-rational divisor D is the data of $\lambda_x x+\lambda_y y\in\mathbb{K}[x, y]$ and χ, u, and v in $\mathbb{K}[t]$, as occurring in Proposition 5.16.

PROPOSITION 5.17. *Given a smooth positive $\mathbb{K}$-rational divisor D for which x is an unramified primitive element, the conversions between the series expansions and the global representation of D in terms of x take softly linear time.*

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

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

for the series expansion of $m_i\mathcal{E}_i$, where $\mathbb{L}_i:=\mathbb{K}[b]/(\theta_i(b))$, β_i represents the class of b in $\mathbb{L}_i$, and γ_i is invertible in $\mathbb{L}_i$. Up to replacing t by t/γ_i (that incurs linear time), we may assume that $\gamma_i=1$. We introduce

$$\begin{array}{rccc}\Gamma_{\theta_i,m_i}\colon & \mathbb{K}[t]/(\theta_i^{m_i}(t)) & \cong & \mathbb{L}_i[[t]]/(t^{m_i})\\ & t & \longmapsto & \beta_i+t,\end{array}$$

and verify that

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

Then, $\theta_i^{m_i},\Gamma^{-1}_{\theta_i,m_i}(X_i(t)),\Gamma^{-1}_{\theta_i,m_i}(Y_i(t))$ 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 2.6. By Proposition 2.4 we recover the global representation of D in softly linear time by Chinese remaindering.

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

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

and $\Gamma_{\theta_i,m_i}(v \operatorname{rem} \theta_i^{m_i})$ represent the series expansion of $m_i\mathcal{E}_i$; this also incurs softly linear time thanks to Proposition 2.6. □

6. VANISHING POLYNOMIALS

This section is devoted to computing homogeneous polynomials that vanish at a divisor of a curve $\mathcal{C}$ 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 approach is detailed in the first subsection. Then, we focus on a more promising method that yields "compressed representations" of bases of Riemann–Roch spaces.

6.1. 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 6.1. *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;* β *will represent the class of* b *in* $\mathbb{L} := \mathbb{K}[b]/(\Delta(b))$*;*
- $\mu \in \mathbb{L}[a]$ *is monic and separable; here separable means that the discriminant of* μ *is invertible in* $\mathbb{L}$*;* α *will represent the class of* a *in* $\mathbb{E} := \mathbb{L}[a]/(\Delta(a))$*;*
- $m \in \mathbb{N}_{>0}$*;*
- $(X(t), Y(t)) \in (\mathbb{E}[[t]]/(t^m))^2$*, 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*

$$\operatorname{val}_t(g(X(t), Y(t))) \geqslant m.$$

With the representation of Definition 3.9 of the adjoint divisor $\mathcal{A}$ of $\mathcal{C}$, and according to Definition 3.4, the adjoint condition can be regarded as a conjunction of vanishing conditions whose representations are

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

where the $\tau_{i,j}$ are defined in Equation (3.7), 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 $\mathcal{C}$ if, and only if,

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

On the other hand, if $D = m\mathcal{E}$ is a smooth divisor given by series expansions as in Definition 5.8 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 $\mathrm{Div}(G) \geqslant D$ is satisfied if, and only if,

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

6.2. Straightforward linear solving

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

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

as in Definition 6.1, find polynomials $g \in \mathbb{K}[x,y]$ of total degree $\leqslant d$, degree $< \delta$ in y and vanishing at all these conditions simultaneously. Vanishing conditions can be translated into a homogeneous $\mathbb{K}$-linear system, where the unknowns are the coefficients of g and the number of equations is

$$\sigma := \sum_{i=1}^{r} m_i \deg \Delta_i \deg \mu_i. \tag{6.1}$$

Algorithm 6.1

Input. A sequence of vanishing conditions $((\Delta_i(b), \mu_i(a), X_i(t), Y_i(t), m_i))_{i=1,\ldots,r}$ as in Definition 6.1 and integers $\delta, d \geqslant 1$.

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

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

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

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

PROPOSITION 6.2. *Algorithm 6.1 is correct and takes*

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

operations in $\mathbb{K}$, where σ has been defined in Equation (6.1).

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

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

operations in $\mathbb{K}$. Taking the sum of these costs for $i = 1, \ldots, r$, 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 $l = 0, \ldots, \delta - 1$ and $k = 0, \ldots, d - l$. 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 $k = 0, \ldots, \deg \mu_i - 1$, $l = 0, \ldots, \deg \Delta_i - 1$, and $m = 0, \ldots, m_i - 1$. 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 [10, Chapter 2], [69, Theorem 2.10], or [13, Chapitre 8, Théorème 8.4], for instance. □

The straightforward approach developed in Algorithm 6.1 turns out to be sufficient to achieve the complexity bound of Theorem 7.8. Yet we believe that it is worth adapting the point of view previously introduced in [3, 4], because it yields more compact representations of Riemann–Roch spaces (see Section 7.4), 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 7.7.

6.3. Popov form

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

$$\deg_{\boldsymbol{s}} \boldsymbol{b}_i := \max\left(\deg \boldsymbol{b}_{i,1} + \boldsymbol{s}_1, \dots, \deg \boldsymbol{b}_{i,\delta} + \boldsymbol{s}_\delta\right),$$

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

$$\deg \boldsymbol{b}_{i,j} + \boldsymbol{s}_j = \deg_{\boldsymbol{s}} \boldsymbol{b}_i.$$

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

- the pivot index of $\boldsymbol{b}_i$ equals i for $i = 1, \dots, \delta$,
- $\boldsymbol{b}_{i,i}$ is monic for $i = 1, \dots, \delta$,
- $\deg \boldsymbol{b}_{j,i} < \deg \boldsymbol{b}_{i,i}$ for $i = 1, \dots, \delta$, and $j \neq i$.

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

PROPOSITION 6.3. [3, Proposition 4.2] *Let $\boldsymbol{b}_1, \dots, \boldsymbol{b}_\delta$ be a basis of a free $\mathbb{K}[x]$-module $\mathcal{M}$ of rank δ in* $\boldsymbol{s}$-Popov form. *Given an integer $d \geqslant 0$, the elements in $\mathcal{M}$ of $\boldsymbol{s}$-degree $\leqslant d$ form a $\mathbb{K}$-vector space of basis $x^j \boldsymbol{b}_i$ for $i = 1, \dots, \delta$ such that $\deg_{\boldsymbol{s}} \boldsymbol{b}_i \leqslant d$ and $j = 0, \dots, d - \deg_{\boldsymbol{s}} \boldsymbol{b}_i$.*

Computing Popov forms of $m \times n$ matrices can be done by means of row operations only, with $\tilde{O}(m\, n\, r (\deg M)^2)$ operations in $\mathbb{K}$, where r is the rank of M and when $\boldsymbol{s}$ is zero [54, Theorem 7.1]. The current best known bound $\tilde{O}(m^{\omega-1}\, n \deg M)$ holds whenever $m \leqslant n$ [56, 57]. For more information about Popov forms we refer the reader to [55].

6.4. 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

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

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

Given a vector $\boldsymbol{E} := (\boldsymbol{e}_1, \dots, \boldsymbol{e}_\delta)$ in $\mathfrak{E}^\delta$, we consider the map

$$\begin{aligned} \boldsymbol{E}_J\colon \quad \mathbb{K}[x]^\delta &\longrightarrow \mathfrak{E} \\ \boldsymbol{p} := (p_1, \dots, p_\delta) &\longmapsto \boldsymbol{p} \cdot \mathbf{E} := p_1 \cdot \boldsymbol{e}_1 + \cdots + p_\delta \cdot \boldsymbol{e}_\delta. \end{aligned} \tag{6.2}$$

The kernel of $\boldsymbol{E}_J$ 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 $\ker \boldsymbol{E}_J$ is usually called the (first) *syzygy* module of $\boldsymbol{E}$.

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

THEOREM 6.4. [45, simplified from Theorem 1.4] *With the notation as above, the basis in $\boldsymbol{s}$-Popov form of* $\ker \boldsymbol{E}_J$ *can be computed with $\tilde{O}(\sigma^\omega \lceil \delta/\sigma \rceil)$ operations in $\mathbb{K}$.*

6.5. Compressed bases

We come back to Algorithm 6.1: we will replace the straightforward kernel basis computation by Theorem 6.4. The complexity exponent will remain the same as in Proposition 6.2, 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 6.1, an integer $\delta \geqslant 1$, and we search for polynomials $g \in \mathbb{K}[x,y]$ of degree $< \delta$ in y such that

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

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 (6.1), 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 $\boldsymbol{e}_k$ denote the vector $(Y_1(t)^{k-1}, \dots, Y_r(t)^{k-1})$ regarded in $\mathfrak{E}$; precisely the projection of $\boldsymbol{e}_k$ onto $\mathbb{E}_i[[t]]/(t^{m_i})$ is $Y_i(t)^{k-1}$.

LEMMA 6.5. *The matrices $J_1, \dots, J_r$ and the vectors $\boldsymbol{e}_1, \dots, \boldsymbol{e}_r$ can be computed with*

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

operations in $\mathbb{K}$.

Proof. Fix i in {1,...,r}. Building the vector representation of $\alpha_i^k \beta_i^{\deg \Delta_i}$ for $k = 0,\dots,\deg \mu_i - 1$ does not require any operation in $\mathbb{K}$. Second, we compute $\alpha_i^k \beta_i^l \gamma_i$ 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

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

PROPOSITION 6.6. *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 6.1, let $\delta \geqslant 1$, *and set* $\boldsymbol{s} := (\delta-1, \delta-2, \dots, 1, 0)$ *for the shift vector. Let* $\mathcal{G}$ *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,* $\mathcal{G}$ *is a free* $\mathbb{K}[x]$*-module of rank* δ, *for which a basis in* $\boldsymbol{s}$*-Popov form can be computed with*

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

operations in $\mathbb{K}$, *where* σ *has been defined in Equation* (6.1).

Proof. In this context, the map (6.2) is

$$\begin{aligned} \boldsymbol{E}_J\colon \quad \mathbb{K}[x]^\delta &\longrightarrow \mathfrak{E} = \bigoplus_{i=1}^{r} \mathbb{E}_i[[t]] / (t^{m_i}) \\ \boldsymbol{p} := (p_1, \dots, p_\delta) &\longmapsto \boldsymbol{p} \cdot \mathbf{E} = (p_1(X_i(t)) + p_2(X_i(t))\, Y_i(t) + \cdots + p_\delta(X_i(t))\, Y_i(t)^{\delta-1})_{i=1,\dots,r}. \end{aligned}$$

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

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

that is exactly the definition of $\mathcal{G}$. The combination of Lemma 6.5 with Theorem 6.4 yields the claimed cost. □

6.6. Application to divisors

To conclude this section, we revisit Proposition 6.6 in terms of divisors.

PROPOSITION 6.7. *Let* $\mathcal{C}$ *be a projective curve of degree* δ *defined by* $F = 0$. *We assume that the adjoint divisor* $\mathcal{A}$ *of* $\mathcal{C}$ *is represented as in Definition 3.9. Let* D *be a smooth positive* $\mathbb{K}$*-rational divisor represented by series expansions as in Definition 5.8 and let* $\boldsymbol{s} := (\delta-1, \delta-2, \dots, 1, 0)$ *stand for a shift vector. Let* $\mathcal{G}$ *be the space of homogeneous polynomials* G *of* $\mathbb{K}[x,y,z]$ *such that*

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

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

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

operations in $\mathbb{K}$.

Proof. Since D is smooth, the condition $\mathrm{Div}(G) \geqslant D + \mathcal{A}$ is equivalent to $\mathrm{Div}(G) \geqslant D$ and $\mathrm{Div}(G) \geqslant \mathcal{A}$. As explained at the end of Section 6.1, these inequalities can straightforwardly be rephrased into vanishing conditions in the affine chart $z = 1$. The inequality $\mathrm{Div}(G) \geqslant D$ yields $\deg D$ linear equations in the coefficients of $G(x,y,1)$, while the other inequality $\mathrm{Div}(G) \geqslant \mathcal{A}$ yields $\deg \mathcal{A} = O(\delta^2)$ linear equations. Proposition 6.6 gives the claimed complexity bound since $\sigma = O(\delta^2 + \deg D)$. □

7. 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 with studying the complexities related to this task.

7.1. Changes of coordinates

We first recall that generic coordinates (with the meaning of Definition 3.8) can be achieved after a random linear change of the variables with high probability.

LEMMA 7.1. *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*

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

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

Proof. Let $(M_{i,j})_{1\leqslant i,j\leqslant 3}$ 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 $\leqslant 2\deg F\deg G$. 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 $\mathbb{K}$. □

LEMMA 7.2. *Let $\mathcal{S}$ be a finite subset of $\mathbb{K}$ and let F be a squarefree polynomial in $\mathbb{K}[x,y,z]$. 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*

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

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 7.1 but we need to take into account that the change of variables does not commute with the differentiation in y. Let $(M_{i,j})_{1\leqslant i,j\leqslant 3}$ 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 $\leqslant\delta\,(2\delta-1)$. 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 7.1. □

7.2. 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 7.3. *Let $F \in \mathbb{K}[x,y,z]$ be homogeneous of degree $\delta \geqslant 1$ 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 [27, 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_1+d_2, unless it is zero. □

LEMMA 7.4. *Let $F \in \mathbb{K}[x,y,z]$ be homogeneous of degree $\delta \geqslant 1$ 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 $\tilde{O}(n\,d\,\delta)$ operations in $\mathbb{K}$.*

Proof. This bound follows from the usual modular binary powering algorithm and Lemma 7.3; see [27, Chapter 4, Section 3] for instance. □

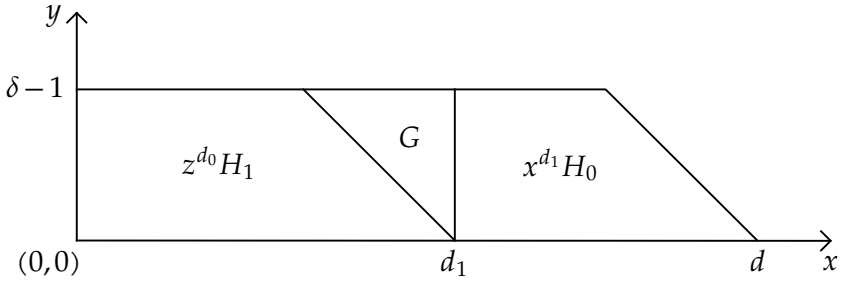
LEMMA 7.5. *Let $F \in \mathbb{K}[x,y,z]$ be homogeneous of degree $\delta \geqslant 1$ and of degree δ in y. Let $H \in \mathbb{K}[x,y,z]$ be homogeneous of total degree d and degree $<\delta$ in y, and let M be a 3×3 matrix over $\mathbb{K}$. Then, $H \circ M \operatorname{rem}_y F$ can be computed with $\tilde{O}(\delta^2 + d\,\delta)$ operations in $\mathbb{K}$.*

Proof. If $d \leqslant 2\,\delta$ 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 $d_0 \geqslant \delta$ and $d_1 \geqslant \delta$. 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. The supports of these polynomials specialized at $z=1$ can be sketched as follows:



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

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

and that

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

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

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

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 7.4, 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 7.3, 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 $d \leqslant 2\delta$, 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 $\leqslant d$. 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 $\tilde{O}(\delta^2 + d\,\delta)$. □

7.3. 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 $H \in \mathbb{K}[x,y,z]$ of degree

$$d := \left\lceil \frac{(\delta-1)(\delta-2)+\deg D_+}{\delta} \right\rceil, \tag{7.1}$$

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

Algorithm 7.1

Input. An absolutely irreducible plane projective curve $\mathcal{C}$ of degree δ, defined by the equation $F = 0$, and a smooth $\mathbb{K}$-rational divisor D of $\mathcal{C}$ in multi-set primitive representation.

Output. A homogeneous polynomial $H \in \mathbb{K}[x,y,z]$, of total degree d defined in (7.1), and degree $< \delta$ in y, such that $\operatorname{Div}(H) \geqslant D_+ + \mathcal{A}$ and $\operatorname{Div}(H)$ is sharply adjoint, where $\mathcal{A}$ represents the adjoint divisor of $\mathcal{C}$.

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 $\mathcal{V}_{\mathbb{A}}(F(x,y,1),F_y(x,y,1))$.

1. Compute the series expansions of $\mathcal{A}$ using Proposition 3.10.
2. Expand the representation of D_+ using Proposition 5.11.
3. Let $\mathcal{H}$ denote the space of homogeneous polynomials H of $\mathbb{K}[x,y,z]$ such that $\deg_y H<\delta$ and $\mathrm{Div}(H)\geqslant D_+ + \mathcal{A}$. Use Proposition 6.7 with D_+ in order to obtain a $\mathbb{K}[x]$-module basis $h_1,\dots,h_\delta$ 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 $a_i(x)\in\mathbb{K}[x]_{\leqslant d-\deg h_i}$ taken at random with coefficients in $\{1,\dots,2\,\delta^2\}$. Repeat this step until H is sharply adjoint.
5. Return H.

PROPOSITION 7.6. *Algorithm 7.1 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 3.10, 5.11, and 6.7. By Proposition 4.3 the $\mathbb{K}$-vector subspace V of $\mathcal{H}$ of homogeneous polynomials of degree d has positive dimension. Then, Proposition 6.3 ensures that the polynomials H generated in Step 4 are uniformly random elements of V. By Lemma 4.4, 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 3.10. Step 2 contributes to

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

by Proposition 5.11. Then, Step 3 incurs $\tilde{O}((\delta^2+\deg D_+)^\omega)$ by Proposition 6.7. 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 3.13. □

7.4. Representation of Riemann–Roch bases

The $\mathbb{K}[x]$-module approach of Section 6.5 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 $z=1$,

- $\mathcal{V}_{\mathbb{P}}(F\circ M, H)$ is in the affine chart $z=1$,
- $\left(\dfrac{x^j z^{d-d_i-j} G_i}{H}\right)\circ M^{-1}$ with $0\leqslant j\leqslant d-d_i$ and $1\leqslant i\leqslant l$ form a basis of $\mathcal{L}(D)$.

7.5. 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 $\mathrm{Div}(H)-\mathcal{A}-D$. 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 [4] for curves with ordinary singularities.

Algorithm 7.2

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

Output. A representation of $\mathcal{L}(D)$ as defined in Section 7.4.

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 $\mathcal{C}$. $\mathrm{Div}(H)$ is sharply adjoint and satisfies $\mathrm{Div}(H)\geqslant D_+ + \mathcal{A}$.

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 7.5.
4. Compute
$$\mathcal{E} := \mathcal{V}_{\mathbb{A}}(F\circ M(x,y,1), (H\circ M \operatorname{rem}_y F)(x,y,1))$$
by using [3, 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 $\theta_i^H(t)=0$, $x=u_i^H(t)=t \operatorname{rem}\theta_i^H(t)$ and $y=v_i^H(t)$ 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 5.7. If the centers of $M^{-1}(D)$ are not in the affine chart $z=1$, or if x is not an unramified 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 $\mathcal{V}_{\mathbb{A}}\left(F\circ M(x,y,1), \frac{\partial(F\circ M)}{\partial y}(x,y,1)\right)$, then go to Step 1.

7. Replace F by $F \circ M$, H by $H \circ M \operatorname{rem}_y F$ and D by $M^{-1}(D)$, and compute the adjoint divisor $\mathcal{A}$ of $\mathcal{C}$ in the new coordinates, by using Proposition 3.10.
8. Compute the product Δ of the Δ_i of Definition 3.9. Compute
$$\theta := \prod_{i=1}^{d\delta} \theta_i^H \text{ and } \tilde{\theta} := \theta / \Delta.$$
Then compute $\tilde{\theta}_i := \tilde{\theta} \operatorname{rem} \theta_i^H$, $\tilde{\theta}_i := \gcd(\tilde{\theta}_i, \theta_i^H)$, $\tilde{u}_i := t \operatorname{rem} \tilde{\theta}_i(t)$, $\tilde{v}_i := v_i^H \operatorname{rem} \tilde{\theta}_i$, for $i = 1, \ldots, d\delta$.
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 $(\tilde{\theta}_i, \tilde{u}_i, \tilde{v}_i, i)$ for $i = 1, \ldots, d\delta$ constitute a multi-set primitive representation of the smooth divisor $\operatorname{Div}(H) - \mathcal{A}$ in terms of x.
9. Compute the multi-set primitive representation of
$$R := ((\operatorname{Div}(H) - \mathcal{A}) - D_+) + D_-$$
in terms of x by using Propositions 5.15 and 5.13 successively.
10. Expand the representation of R by means of Proposition 5.11.
11. Let $\mathcal{G}$ denote the space of homogeneous polynomials G of $\mathbb{K}[x, y, z]$ such that $\deg_y G < \delta$ and $\operatorname{Div}(G) \geqslant R + \mathcal{A}$. Compute a basis $g_1, \ldots, g_\delta$ of the $\mathbb{K}[x]$-module $\mathcal{G}(x, y, 1)$ by means of Proposition 6.7 used with R. Sort the g_i by increasing total degrees and let l be maximal such that $\deg g_l \leqslant d$.
12. Return M, H, $z^{d_i} g_i(x/z, y/z)$, and d_i for $i = 1, \ldots, l$.

PROPOSITION 7.7. *Algorithm 7.2 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 3.10 are satisfied, so the adjoint divisor $\mathcal{A}$ can actually be computed. When entering Step 8 the variable x separates the centers of $\operatorname{Div}(H)$ and $\operatorname{Div}(H)$ is sharply adjoint. Since $\operatorname{Div}(H) \geqslant D_+ + \mathcal{A}$, the variable x also separates the centers of $\mathcal{A}$ (i.e. the singular points of $\mathcal{C}$). Consequently Δ divides θ in Step 8. Therefore if Step 8 does not return to Step 1, then it actually computes a multi-set primitive representation of $\operatorname{Div}(H) - \mathcal{A}$. From Step 6 it is ensured that x is an unramified primitive element 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 $\operatorname{Div}(H) \geqslant D_+ + \mathcal{A}$ 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 $d = \deg H$, and such that $\operatorname{Div}(G) \geqslant \operatorname{Div}(H) - D$; see [36, Chapitre 2, Théorème 2.7.1], or [37, Théorème 2.5], or [50, Section 4], for instance. Consequently, when Step 11 is reached, Propositions 6.3 and 6.7 ensure the correctness of the output.

Before analyzing probabilities, from the definition of d in (7.1), we note that
$$d\delta \leqslant \delta^2 + \deg D_+ - 2\delta. \tag{7.2}$$
The probability that a 3×3 matrix M taken with random entries in $\mathcal{S}$ is not invertible is
$$\leqslant \frac{3}{|\mathcal{S}|} \tag{7.3}$$

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

$$\leqslant \frac{2\,\delta^2}{|\mathcal{S}|} \tag{7.4}$$

by Lemma 7.2. 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

$$\leqslant \frac{2\,d\,\delta + \delta + \binom{d\,\delta}{2}}{|\mathcal{S}|} \leqslant \frac{3\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|} \tag{7.5}$$

by Lemmas 7.1 and 5.2 combined with Inequality (7.2). In Step 5, the probability that the conditions for $M^{-1}(D)$ are not met is

$$\leqslant \frac{3\,(\deg D_+ + \deg D_-)^2}{|\mathcal{S}|} \leqslant \frac{12\,(\deg D_+)^2}{|\mathcal{S}|}, \tag{7.6}$$

by Lemma 5.5. In Step 6, the probability that the algorithm goes back to Step 1 is

$$\begin{aligned} \frac{\binom{\deg D_- + |\mathcal{E}|}{2} + \binom{\delta\,(\delta-1)}{2}}{|\mathcal{S}|} &\leqslant \frac{(\deg D_+ + d\,\delta + \delta^2)^2}{|\mathcal{S}|} \\ &\leqslant \frac{4\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|} \end{aligned} \tag{7.7}$$

by Inequality (7.2) and Lemma 5.2 again.

In Step 8 the abscissas of the centers of the places of $\mathrm{Div}(H)$ which belong to $\mathcal{A}$ are precisely the roots of Δ: we discard those places by dividing each θ_i^H by $\gcd(\theta_i^H, \Delta)$ and we update the parametrization u_i^H and v_i^H in order to obtain the candidate representation of $\mathrm{Div}(H) - \mathcal{A}$. Then, we check whether x is an unramified primitive element for $\mathrm{Div}(H) - \mathcal{A}$. For the probability of Step 8 to return to Step 1, we apply Lemma 5.5 to the divisor made of the points of $\mathcal{E}$ that are smooth on C: the probability bound is

$$\leqslant \frac{3\,|\mathcal{E}|^2}{|\mathcal{S}|} \leqslant \frac{3\,(d\,\delta)^2}{|\mathcal{S}|} \leqslant \frac{3\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|}. \tag{7.8}$$

The sum of the right-hand sides of Inequalities (7.3) to (7.8) is $\leqslant 1/2$. 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 7.1. Step 3 takes

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

operations in $\mathbb{K}$ by Lemma 7.5. By [3, Lemma 2.4] (or [4, 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

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

by Proposition 5.7.

Arriving at Step 6, x is an unramified primitive element 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 $\mathcal{U}_{\mathbb{A}}\Big(F\circ M(x,y,1), \frac{\partial(F\circ M)}{\partial y}(x,y,1)\Big)$ contributes to $\tilde{O}(\delta^3)$ by [3, Lemma 2.4] (or [4, Proposition 5.6]). The conditions of Proposition 3.10 are satisfied, so Step 7 costs $\tilde{O}(\delta^3)$.

For Step 8, Proposition 2.3 allows the computation of the $\tilde{\theta}_i$, $\tilde{u}_i$, $\tilde{v}_i$ 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

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

by Lemma 5.6.

By Propositions 5.13 and 5.15, Step 9 costs

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

Step 10 then takes

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

operations in $\mathbb{K}$ by Proposition 5.11. 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 6.7. □

7.6. Main complexity bound

By combining Algorithms 7.1 and 7.2, we finally achieve our main result.

THEOREM 7.8. *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 $\mathcal{C}$. Let D be a smooth $\mathbb{K}$-rational divisor of $\mathcal{C}$ given in multi-set primitive representation (see Definition 5.4). Then, a representation of $\mathcal{L}(D)$ as in Section 7.4 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 7.1 hold with high probability, thanks to Lemmas 5.2, 5.5, and 7.2. Changing the coordinates in F and testing their genericity takes $\tilde{O}(\delta^2)$ operations in $\mathbb{K}$ by Lemmas 2.1 and 7.2. Changing the coordinates in D, verifying that the centers are in the affine chart $z=1$, and that x is an unramified primitive element takes

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1}+\delta^{\frac{\omega-1}{2}}|\mathrm{supp}\,D_+|+|\mathrm{supp}\,D_+|^\omega\Big)=\tilde{O}((\delta^2+\deg D_+)^\omega)$$

by Proposition 5.7. 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 [3, Lemma 2.4] (or [4, Proposition 5.6]). Let θ_{F_y} denote the corresponding minimal polynomial of x.

The variable x is an unramified primitive element 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, $\mathrm{Res}(\theta_D,\theta_{F_y})\neq 0$, whose computation takes negligible time. Finally, once the assumptions of Algorithm 7.1 are satisfied, we call this algorithm, followed by Algorithm 7.2. The total complexity bound is deduced from Propositions 7.6 and 7.7. □

7.7. 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 6.4 in a particular case; we use the notation of Section 6.5.

THEOREM 7.9. [45, simplified from Theorem 1.5] *With the notation of Section 6.4, if J is a Jordan matrix, then the basis in $\boldsymbol{s}$-Popov form of* $\ker \boldsymbol{E}_J$ *can be computed with $\tilde{O}(\delta^{\omega-1}(\sigma+|\boldsymbol{s}|))$ operations in $\mathbb{K}$, where $|\boldsymbol{s}|:=s_1+\cdots+s_\delta$.*

We deduce the following proposition in replacement of Proposition 6.7.

PROPOSITION 7.10. *Under Hypothesis (C), the complexity bound in Proposition 6.7 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 6.1 but in the form of $\Delta(b):=b-\beta$, $\mu(a):=a$ and $X(t)=\beta+\gamma t^e$. Such a rewriting takes softly linear time by Hypothesis (C) and Proposition 2.3. By computing a e-th root of γ we can further reduce to the case where $\gamma=1$, that is $X(t)=\beta+t^e$, in softly linear time.

For $j=0,\ldots,e-1$, let ν_j denote the largest integer ν such that $\nu e+j\leqslant m-1$. In the basis of the $\mathbb{K}$-vector space $\mathbb{K}[[t]]/(t^m)$ made of the concatenation of

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

the matrix representing the multiplication by $X(t)=\beta+t^e$ is a Jordan matrix. Consequently, the cost of Lemma 6.5 becomes $\tilde{O}(\delta\sigma)$: building the J_i is straightforward, and $e_1,\ldots,e_r$ still contribute to $\tilde{O}(\delta\sigma)$.

Since $|\boldsymbol{s}|=O(\delta^2)$, by combining this bound with Theorem 7.9, the complexity bound in Proposition 6.6 becomes $\tilde{O}(\delta^{\omega-1}(\delta^2+\sigma))$. The conclusion follows as in the proof of Proposition 6.7. □

In the future, we hope that the complexity bound in Proposition 7.10 will hold without Hypothesis (C). This might be made possible thanks to further advances in the so called *interpolation bases* algorithms; see [45, 55]. Let us now briefly assess the overall cost of our Brill–Noether variant in this framework.

THEOREM 7.11. *Under Hypothesis (C), the expected complexity bound in Theorem 7.8 can be replaced by*

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

Proof. Using Proposition 7.10 instead of Proposition 6.7, and revisiting complexity analyses step by step, the cost in Proposition 7.6 becomes $\tilde{O}(\delta^{\omega+1} + \delta^{\omega-1}\deg D_+)$. Then, the cost in Proposition 7.7 becomes

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

It follows that the complexity bound in Theorem 7.8 can be replaced by

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

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

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

whence the claimed bound. □

The complexity bound of Theorem 7.11 is similar to the one obtained in [4] for ordinary curves without Hypothesis (C): in this case another fast algorithm from [56] is used for syzygy bases.

8. 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 4.3 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 [17] and previously used in the context of computing Riemann–Roch spaces in [18]), or to rely on the approximate roots theory initiated by Abhyankar [5, 22].

Finally, the bottleneck of our main algorithm is in the complexity bound of Theorem 6.4. Therefore, faster computations of syzygy bases related to the structured linear algebra problem occurring in Section 6.5 would improve the complexity exponent of our main algorithm, in a way similar to the framework of Section 7.7.

Acknowledgments. We thank the anonymous referees for their useful comments.

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, E. Berardini, A. Couvreur, and G. Lecerf. Computing Riemann–Roch spaces via Puiseux expansions. Technical Report, HAL, 2021. `https://hal.archives-ouvertes.fr/hal-03281757`, version 1.

[3] 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.

[4] 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`, version 1.

[5] 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.

[6] S. S. Abhyankar and A. M. Sathaye. *Geometric theory of algebraic space curves*, volume 423 of *Lect. Notes Math.* Springer, Berlin, Heidelberg, 1974.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] S. Bordage and J. Nardi. Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes. *Electronic colloquium on computational complexity*, 2020. TR20-165.

[12] 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).

[13] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, and É. Schost. *Algorithmes Efficaces en Calcul Formel*. Frédéric Chyzak (self-published), Palaiseau, France, 2017. Electronic version available from `https://hal.archives-ouvertes.fr/AECF`.

[14] A. Bostan, Ph. Flajolet, B. Salvy, and É. Schost. Fast computation of special resultants. *J. Symbolic Comput.*, 41(1):1–29, 2006.

[15] A. Brill and M. Noether. Ueber die algebraischen Functionen und ihre Anwendung in der Geometrie. *Math. Ann.*, 7(2-3):269–310, 1874.

[16] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, 1997.

[17] A. Campillo. *Algebroid Curves in Positive Characteristics*, volume 813 of *Lect. Notes Math.* Springer-Verlag Berlin Heidelberg, 1980.

[18] 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.

[19] A. Campillo and J. I. Farrán. Adjoints and codes. *Rendiconti del Seminario Matematico Università e Politecnico di Torino*, 62:209–223, 2004.

[20] E. Casas-Alvero. *Algebraic Curves, the Brill and Noether Way*. Springer International Publishing, 2019.

[21] 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.

[22] V. Cossart and G. Moreno-Socías. Racines approchées, suites génératrices, suffisance des jets. *Annales de la Faculté des sciences de Toulouse 6^{e} série*, 14(3):353–394, 2005.

[23] D. Duval. *Diverses questions relatives au calcul formel avec des nombres algébriques*. PhD thesis, Université de Grenoble 1, France, 1987.

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

[25] W. Fulton. *Algebraic Curves – An Introduction to Algebraic Geometry*. Addison-Wesley, 1989.

[26] 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.

[27] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013.

[28] 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.

[29] 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.

[30] V. D. Goppa. Codes and information. *Uspekhi Mat. Nauk*, 39(1(235)):77–120, 1984. English translation: *Russ. Math. Surv.*, 1984, 391(1), 87–141.

[31] D. Gorenstein. An arithmetic theory of adjoint plane curves. *Trans. Am. Math. Soc.*, 72(3):414–436, 1952.

[32] 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.

[33] S. Greco and P. Valabrega. On the theory of adjoints II. *Rendiconti del Circolo Matematico di Palermo*, 31(1):5–15, 1982.

[34] B. Grenet, J. van der Hoeven, and G. Lecerf. Deterministic root finding over finite fields using Graeffe transforms. *Appl. Algebra Engrg. Comm. Comput.*, 27(3):237–257, 2016.

[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. Accelerated tower arithmetic. *J. Complexity*, 55:101402, 2019.

[41] J. van der Hoeven and G. Lecerf. Directed evaluation. *J. Complexity*, 60:101498, 2020.

[42] J. van der Hoeven and G. Lecerf. On the complexity exponent of polynomial system solving. *Found. Comput. Math.*, 21:1–57, 2021.

[43] J. Hopcroft and J. Musinski. Duality applied to the complexity of matrix multiplication and other bilinear forms. *SIAM J. Comput.*, 2(3):159–173, 1973.

[44] 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.

[45] C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Computing minimal interpolation bases. *J. Symbolic Comput.*, 83:272–314, 2017.

[46] O. H. Keller. *Vorlesungen über algebraische Geometrie*. Akademie Verlag Leipzig, 1974.

[47] K. Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007.

[48] A. Klyachko and O. Kara. Singularities of the modular curve. *Finite Fields Appl.*, 7(3):415–420, 2001.

[49] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 3rd edition, 2002.

[50] 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.

[51] F. Le Gall and F. Urrutia. Improved rectangular matrix multiplication using powers of the Coppersmith–Winograd tensor. In A. Czumaj, editor, *Proceedings of the 2018 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1029–1046. Philadelphia, PA, USA, 2018. SIAM.

[52] A. Le Gluher and P.-J. Spaenlehauer. A fast randomized geometric algorithm for computing Riemann–Roch spaces. *Math. Comp.*, 89:2399–2433, 2020.

[53] U. Le Verrier. Sur les variations séculaires des éléments elliptiques des sept planètes principales : Mercure, Vénus, la Terre, Mars, Jupiter, Saturne et Uranus. *Journal de Mathématiques Pures et Appliquées*, 1:220–254, 1840.

[54] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *J. Symbolic Comput.*, 35(4):377–401, 2003.

[55] 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`.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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, France, 2008.

[61] A. Poteaux and M. Rybowicz. Improving complexity bounds for the computation of Puiseux series over finite fields. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC'15, pages 299–306. New York, NY, USA, 2015. ACM.

[62] A. Poteaux and M. Weimann. Computing Puiseux series: a fast divide and conquer algorithm. *Ann. Henri Lebesgue*, 5:1061–1102, 2021.

[63] V. Shoup. Fast construction of irreducible polynomials over finite fields. *J. Symbolic Comput.*, 17(5):371–391, 1994.

[64] V. Shoup. Efficient computation of minimal polynomials in algebraic extensions of finite fields. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation*, ISSAC '99, pages 53–58. New York, NY, USA, 1999. ACM.

[65] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, New York, NY, 2nd edition, 2009.

[66] 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`.

[67] 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`.

[68] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag Berlin Heidelberg, 2nd edition, 2009.

[69] A. Storjohann. *Algorithms for matrix canonical forms*. PhD thesis, Swiss Federal Institute of Technology in Zürich (Switzerland), 2000.

[70] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov–Gilbert bound. *Math. Nachr.*, 109(1):21–28, 1982.

[71] 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.