Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities

Simon Abelard, Alain Couvreur, Grégoire Lecerf

Efficient computation of Riemann–Roch spaces for plane curves with ordinary singularities*

SIMON ABELARD[ab], ALAIN COUVREUR[cad], GRÉGOIRE LECERF[ae]

a. Laboratoire d'informatique de l'École polytechnique (LIX, UMR 7161)
CNRS, École polytechnique, Institut Polytechnique de Paris
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau, France

c. Inria

b. Email: simon.abelard@lix.polytechnique.fr
d. Email: alain.couvreur@inria.fr
e. Email: gregoire.lecerf@lix.polytechnique.fr

Preliminary version of January 14, 2021

We revisit the seminal Brill–Noether algorithm for plane curves with ordinary singularities. Our new approach takes advantage of fast algorithms for polynomials and structured matrices. We design a new probabilistic algorithm of type Las Vegas that computes a Riemann–Roch space in expected sub-quadratic time.

KEYWORDS: Algebraic curves, Riemann–Roch spaces, Complexity

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 divisor D of C we are interested in computing a 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 to derive a new efficient probabilistic algorithm of type Las Vegas from the Brill–Noether method for ordinary curves.

1.1. Motivation

Riemann–Roch spaces intervene in various areas of applied algebra. For instance they are the cornerstone of arithmetic operations in Jacobians of curves [37, 59], a task which was originally of cryptographic interest until it became clear that cryptographic curves

*. This paper is part of a project that has received funding from the French "Agence de l'innovation de défense".

should either be elliptic or of genus 2 [56], for which tailor-made algorithms and formulas are known. Nevertheless, performing arithmetic in Jacobians of curves retains its interest for applications in number theory and algebraic geometry.

From Goppa's seminal work [21, 22, 23], Riemann–Roch spaces are pivotal to design efficient algebraic geometry error correcting codes, where the encoding algorithm consists in evaluating a basis of such a space at points of an algebraic curve. These algebraic geometry codes extend the well known Reed–Solomon codes and may be defined over smaller alphabets. Currently in practice, algebraic curves and divisors used in coding theory are mostly limited to cases for which such bases are already explicitly known. In particular, most of the explicit examples in the literature concerns divisors supported by one or two points on Hermitian curves, Suzuki curves, or Giuletti–Kochmaros curves. For the sake of diversity it is relevant to handle more general curves and divisors.

Error correcting codes have recently revealed to be useful in new application areas such as IOP (*Interactive Oracle Proofs*) [3], a construction which is itself involved in decentralized computations. Algebraic geometry codes are particularly adapted to these applications that require codes of large length over a finite alphabet. The complexity of encoding also plays a role in the size of the proofs and the time needed by provers and verifiers; see [3, Lemma 7.2].

The practical construction of the best known algebraic geometry codes, as pioneered by Tsfasman, Vlăduţ, and Zink [58], still hides algorithmic challenges that go beyond the scope of the present paper because non-ordinary singularities are involved. Yet we hope that our contribution to the ordinary case will constitute a step towards the general case.

1.2. Hypotheses

Until the end of the paper, the degree of the curve C is written δ, and $\mathbb{K}$ is a sufficiently large field with the following restriction:

$\mathbb{K}$-H. $\mathbb{K}$ is either finite or has characteristic zero, and is therefore a perfect field.

We will further assume that the following hypotheses hold for C:

C-H$_1$. C is absolutely irreducible, that is irreducible over $\bar{\mathbb{K}}$;

C-H$_2$. C is *ordinary*: each germ of curve at a singular point of C splits into smooth germs with distinct tangent spaces; see Section 5.5.

Let us recall that absolute irreducibility can be tested efficiently by means of the algorithms of [13]. For testing the second hypothesis we will design a specific algorithm in Section 5.5. The restriction on the type of singularities involves major simplifications in the Brill–Noether algorithm [25, 40]: the desingularization of C requires to blow up each singular point only once, and the adjoint condition writes in a convenient manner.

We further focus on the following particular case of input divisors:

D-H. The input divisor D, for which we want a basis of the Riemann–Roch space, is *smooth* and defined over $\mathbb{K}$, which means that its support is made of regular points of C.

We will see that smooth divisors combine better with adjoint conditions, divisor intersections, and allow us to reduce the Brill–Noether method to a specific structured linear algebra problem, for which a fast algorithm is at our disposal.

We will often decompose a divisor D into $D = D_+ - D_-$, where D_+ and D_- are *positive* (also called *effective*) divisors with disjoint supports. 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.

1.3. Related work

The use of Riemann–Roch spaces to build error correcting codes goes back to Goppa [21, 22, 23]. Over the past forty years, a rich literature has addressed more and more efficient algorithms, relying both on theoretical breakthroughs and more sophisticated tools from computer algebra.

The seminal Brill–Noether approach [9] to compute Riemann–Roch spaces was originally restricted to ordinary curves. The extension to any plane curve and divisor is due to Le Brigand and Risler [40]. The algorithmic aspects were later detailed in the mid 90's in Haché's PhD thesis [25], who also achieved an implementation in the AXIOM programming language. At the same time, Huang and Ierardi [34] designed an algorithm to compute Riemann–Roch spaces for ordinary curves, whose complexity depends linearly in the size of the input divisor. With the use of Chow cycles to represent divisors, they were also able to avoid polynomial factorization in their algorithm.

The addition of divisors in Jacobians of curves involves the computation of particular Riemann–Roch spaces. In 1994, Volcheck [59] presented an algorithm based on the Brill–Noether theory to perform these additions with arbitrary singularities, using Puiseux expansions to obtain adjoint divisors. Puiseux expansions require assumptions on the characteristic of the base field. These assumptions were later removed by Campillo and Farrán [11] by means of Hamburger–Noether expansions. The family of algorithms derived from the Brill–Noether approach is often called "geometric".

Meanwhile, an alternate family of algorithms, called "arithmetic", involving ideals and integral closures in algebraic function fields, was initiated by Coates [14] and Davenport [16], based on earlier ideas of Dedekind and Weber [17], and on the proof of the Riemann–Roch theorem given by Hensel and Landberg [28] in 1902. The current state-of-the-art algorithm for this approach is due to Hess [29] and has been implemented in the MAGMA and SINGULAR computer algebra systems. Hess' algorithm handles all types of singularities, and does not involve generic changes of variables. However, this "arithmetic" strategy requires to compute integral closures of ad hoc orders in the input function field. Integral closures are in general costly: the quasi-optimal algorithm presented in [1] has a complexity higher than the fastest "geometric" approaches for computing Riemann–Roch spaces.

In 2007, Khuri-Makdisi [37] gave an algorithm for performing additions in the Jacobian of general genus-g curves in time $\tilde{O}(g^\omega)$, where $\tilde{O}$ hides logarithmic factors and $\omega \leqslant 3$ denotes an admissible complexity exponent for linear algebra; see notations in Section 2.1. However, Khuri-Makdisi's algorithm requires to precompute two Riemann–Roch spaces of divisors on the input curve whose degrees are in $O(g)$. The main idea is to represent divisors as vector spaces and to rephrase divisor operations in terms of linear algebra on matrices of size $\tilde{O}(g)$.

In 2018, Le Gluher and Spaenlehauer [42] designed an algorithm specific to nodal curves, in the vein of the Brill–Noether theory, while taking advantage of efficient tools from computer algebra: resultants and linear algebra. Up to logarithmic factors, their complexity bound is similar to Khuri-Makdisi's work in the worst case, but they provided a very efficient implementation which outperformed the previous standards.

Recently, we showed that under the same assumptions as in [42] it is possible to appeal to structured rather than generic linear algebra, by constructing Riemann–Roch spaces from suitable $\mathbb{K}[x]$-modules [2]. This point of view is already present in Hess' algorithm but, to the best of our knowledge, it had not been used before within "geometric" algorithms. Overall we designed the first subquadratic algorithm for computing Riemann–Roch spaces of smooth divisors of nodal curves [2].

1.4. Our contributions

Given an absolutely irreducible ordinary curve $\mathcal{C}$ and a smooth divisor D, our central contribution is a new probabilistic algorithm of type Las Vegas to compute the Riemann–Roch space $\mathcal{L}(D)$ with an expected number of

$$\tilde{O}(\delta^{\omega+1} + \delta^{\omega-1} \deg D_+) \tag{1.1}$$

operations in $\mathbb{K}$ if the characteristic is 0 or sufficiently large, and if the coordinates are "sufficiently generic" (δ still denotes the degree of $\mathcal{C}$); see Proposition 7.5. The overhead to achieve these "sufficiently generic" coordinates is analyzed in Theorem 7.7: the expected cost to compute $\mathcal{L}(D)$ then becomes

$$\tilde{O}\Big((\delta^2 + \deg D_+)^{\frac{\omega+1}{2}} \Big), \tag{1.2}$$

that is subquadratic in the dense size of the input. This turns out to be the first subquadratic complexity bound for ordinary curves. The complexity bound (1.2) matches the one of [2] for nodal curves. In positive characteristic we achieve similar complexity bounds by restricting to finite fields.

For the sake of comparison, Hess' algorithm achieves a polynomial complexity bound for general curves. It seems that its cost is $O(g^4)$ when restricted to the problem of arithmetic in Jacobians of curves, and where g denotes the genus of $\mathcal{C}$. But the dependency in $\deg D_+$ does not seem to have been analyzed so far, to our best knowledge. On the other hand, one algorithm of Huang and Ierardi takes $O((\delta \deg D_+)^{2\omega})$ operations in $\mathbb{K}$ in the particular case where $\mathcal{C}$ is smooth and the support of D only contains rational points [34, Section 4.2]. Another algorithm of them admits complexity $O(\delta^{6\omega} \deg D_+)$.

The paper is organized as follows. Section 2 is dedicated to preliminary results in computer algebra. Then, Section 3 revisits the proof of the Brill–Noether method from scratch and from a constructive point of view. It relies on elementary concepts from algebraic geometry: Nullstellensatz, resultants, linear algebra, and the Bézout theorem for plane curves. By the way we also provide the reader with a simple proof of this Bézout theorem in Section 5 (it mostly reduces to the Smith form of a suitable polynomial matrix). In fact this presentation of the Brill–Noether method aims at introducing the needed data structures and sub-algorithms. Let us say briefly here that this method divides into two main steps: first we compute a common denominator H of $\mathcal{L}(D)$, and then a basis of the corresponding numerators.

The representation of divisors is tackled in Section 4, where we revisit efficient algorithms for their sums, subtractions, and of changes of coordinates. Section 5 then focuses on algorithms for intersecting curves: they are necessary to obtain the singular locus of $\mathcal{C}$, the adjoint divisor $\mathcal{A}$ of $\mathcal{C}$, and the divisor of the common denominator H of $\mathcal{L}(D)$.

Section 6 shows how a "suitable" denominator H can be built in a randomized fashion with high probability. This constitutes a technical step to prove (1.2). As a byproduct we are able to show that the complexity bound (1.1) holds after a single random change of coordinates applied to F and D, with high probability. Heuristically this means that the bound (1.1) holds with "sufficiently generic" input F and D. The gap between (1.2) and (1.1) is mostly due to the random change of coordinates applied to D.

The top level algorithm is presented in Section 7. The final key ingredient is a new reformulation of the criteria ensuring that a curve is adjoint to another. Our reformulation allows us to benefit from Neiger's fast bivariate interpolation algorithm of [48] to solve the linear systems occurring in the Brill–Noether method.

2. PRELIMINARIES

For convenience this section gathers necessary notations and basic results from computational algebra.

2.1. Complexity model

For complexity analyses, we use an algebraic model over a general field $\mathbb{K}$ (typically computation trees [10]), so we count the number of arithmetic operations and zero tests performed by the algorithms. Over finite fields, we use RAM machines. In order to simplify the presentation of complexity bounds, we use the well established *soft-Oh* notation [20, Chapter 25, Section 7]: $f(n) \in \tilde{O}(g(n))$ means that $f(n) = g(n)\log_2^{O(1)}(|g(n)|+3)$.

The vector space of polynomials of degree $<n$ in $\mathbb{K}[x]$ is written $\mathbb{K}[x]_{<n}$. For integer and polynomial arithmetic, we content ourselves with softly linear cost bounds. We will freely use the known results presented in the text book [20].

The constant ω denotes 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 $\omega < 2.3728639$ [41]. The constant ϖ is another real value between 1.5 and $(\omega+1)/2$ such that the product of a $n \times \sqrt{n}$ matrix by a $\sqrt{n} \times \sqrt{n}$ matrix takes $O(n^\varpi)$ operations. The current best known bound is $\varpi < 1.667$ [35, Theorem 10.1].

2.2. Finite fields

A finite field $\mathbb{F}_q$ will be represented in the Kronecker style, that is $\mathbb{F}_p[t]/(\mu(t))$ where $\mu \in \mathbb{F}_p[t]$ is irreducible of degree $\kappa := \log q / \log p$. Elements in $\mathbb{F}_q$ are represented by polynomials in $\mathbb{F}_p[t]_{<\kappa}$.

Computing $e(t) := t^p \operatorname{rem} \mu(t)$ takes $\tilde{O}(\log q \log p)$ bit operations by binary exponentiation. Then, for any element $a(t) \bmod \mu(t)$, we may obtain $a(t)^p \operatorname{rem} \mu(t)$ as $(a \circ e) \operatorname{rem} \mu$. Until the end of the paper, $\epsilon > 0$ represents a fixed number, though to be close to zero. The latter modular composition can be implemented with $O(\log^{1+\epsilon} q)$ bit operations thanks to the Kedlaya–Umans algorithm [36]; see [32] for advances and for the complexity analysis for Turing machines.

PROPOSITION 2.1. *Given e as above, $a(t) \in \mathbb{F}_p[t]_{<\kappa}$ and $k \leqslant \kappa$, computing $a^{p^k} \operatorname{rem} \mu$ takes $O(\log^{1+\epsilon} q)$ bit operations.*

Proof. This follows from the usual "divide and conquer" approach:

$$t^{p^{2k}} \operatorname{rem} \mu(t) = t^{p^k} \circ t^{p^k} \operatorname{rem} \mu(t)$$

and $t^{p^{k+1}} \operatorname{rem} \mu(t) = e \circ t^{p^k} \operatorname{rem} \mu(t)$. Appealing to a cost $O(\log^{1+\epsilon/2} q)$ for modular composition, the total cost for $t^{p^k} \operatorname{rem} \mu$ is $O(\log^{1+\epsilon/2} q \log \kappa) = O(\log^{1+\epsilon} q)$. Then $a^{p^k} \operatorname{rem} \mu$ is obtained as $a\Big(t^{p^k} \operatorname{rem} \mu(t)\Big) \operatorname{rem} \mu(t)$, that incurs one extra modular composition. □

As a useful application of the latter lemma, the computation of p^k-th roots in $\mathbb{F}_q$ takes $O(\log^{1+\epsilon} q)$ bit operations. It is important to mention that when p remains small (that suits most applications to error correcting codes), p-th roots can be extracted fast in practice by means of the algorithm of [51], with $\tilde{O}(p\,\kappa)$ bit operations.

PROPOSITION 2.2. *The squarefree factorization of a polynomial $f \in \mathbb{F}_q[x]$ of degree d takes $\tilde{O}(d \log^{1+\epsilon} q)$ bit operations.*

Proof. First, the separable factorization of f is computed in time $\tilde{O}(d \log q)$; see [44, Section 4.1] for instance. If $p > d$ then the latter factorization corresponds to the squarefree one. Otherwise at most d p^k-th root extractions are further needed, that amount to

$$\tilde{O}(d \log^{1+\epsilon} q + \log q \log p) = \tilde{O}(d \log^{1+\epsilon} q)$$

bit operations by Proposition 2.1. □

2.3. Modular composition

Given three polynomials a, b, c in $\mathbb{K}[x]$, computing $a \circ b \operatorname{rem} c$ is called the (univariate) *modular composition* problem. If these polynomials have degree $\leqslant d$ then this computation can be done with $\tilde{O}(d^\varpi)$ operations in $\mathbb{K}$; see for instance [20, Chapter 12]. Achieving a complexity exponent close to one remains an important open problem. As said above, for finite fields, an asymptotically quasi-linear bit complexity bound has been discovered by Kedlaya and Umans [36]. For the purpose of the present paper, we will mostly use the exponent ϖ for modular composition over $\mathbb{K}$, except for p-th root extractions.

Assume that $\deg c = d$, $\deg a < d$, and $\deg b < d$. The right modular composition map with b modulo c is

$$\begin{aligned} \mathbb{K}[x]/(c) &\longrightarrow \mathbb{K}[x]/(c) \\ a &\longmapsto a \circ b \bmod c. \end{aligned}$$

It is a linear map, and the computation of its transpose

$$\begin{aligned} (\mathbb{K}[x]/(c) \to \mathbb{K}) &\longrightarrow \mathbb{K}^d \\ \lambda &\longmapsto \lambda(1), \lambda(b), \lambda(b^2 \bmod c), \ldots, \lambda(b^{d-1} \bmod c), \end{aligned}$$

is called the *power projection* problem. We refer to [10, Theorem 13.20] for the transposition of algorithms and to [8] for the practical aspects. The modular composition problem will also be needed in the following bivariate context.

LEMMA 2.3. *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 $f(u(t), v(t)) \operatorname{rem} \chi(t)$ 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 $\mathbb{K}$ by Lemma 2.5 below. Then we compute $g(u(t),t) \operatorname{rem} \chi(t)$ by means of [2, Lemma 2.1], that is a variant of [50]. □

2.4. Local expansion

Let μ be a separable polynomial in $\mathbb{K}[s]$, let m be a positive integer, and consider the map

$$\begin{array}{rccc} \Gamma\colon & \mathbb{K}[s]/(\mu^m(s)) & \cong & (\mathbb{K}[t]/(\mu(t)))[[S-t]]/(S-t)^m \\ & s & \longmapsto & S. \end{array}$$

PROPOSITION 2.4. [30, Section 4.2] *Γ is an isomorphism. Both directions of Γ can be computed in softly linear time, namely $\tilde{O}(m \deg \mu)$ operations in $\mathbb{K}$.*

If the μ-adic expansion of an element a modulo μ^m writes as

$$a = a_0 \mu + \cdots + a_{m-1} \mu^{m-1} \bmod \mu^m,$$

with $\deg a_i < \deg \mu$ for $i = 0, \ldots, m-1$, then the first integer k such that $a_k \neq 0$ equals the valuation of $\Gamma(a)$ in $S-t$.

2.5. Linear changes of variables

If $f \in \mathbb{K}[x]$ and $a \in \mathbb{K}$ then $f(x+a)$ can be computed with $\tilde{O}(\deg f)$ operations in $\mathbb{K}$ in a usual "divide and conquer" fashion; see for instance [4, Lemma 7]. This task is called a *univariate shift*. For a polynomial $F \in \mathbb{K}[x,y,z]$ and a 3×3 matrix M over $\mathbb{K}$ we write

$$(F \circ M)(x,y,z) := F((x,y,z)\, M^{\mathsf{T}}),$$

and we study the cost of this change of variables.

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

Proof. We compute the LU-decomposition of M in order to reduce the proof to triangular matrices. Now assume that $M = \begin{pmatrix} a & b & c \\ & d & e \\ & & f \end{pmatrix} \neq 0$ is upper triangular, so

$$F((x,y,z)\, M^{\mathsf{T}}) = F(ax + by + cz, dy + ez, fz)$$

is homogeneous of degree δ. We first simplify to

$$G(x,y) := F(x,y,f)$$

with $O(\delta^2)$ operations in $\mathbb{K}$, and we are led to compute

$$G(ax + by + c, dy + e).$$

With $\tilde{O}(\delta^2)$ operations in $\mathbb{K}$ (via univariate shifts) we can further reduce to the case where $c = 0$ and $e = 0$, and we are then led to compute

$$G(ax + by, dy).$$

We apply the latter change of variables to the homogeneous components of G independently. Each such homogeneous change of variables incurs a single univariate shift. Consequently, the total cost of the change of variables is $\tilde{O}(\delta^2)$. □

2.6. Zariski closed sets

For a subset S of homogeneous polynomials in $\mathbb{K}[x_0,...,x_n]$ 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

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

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 $\mathbb{M}_P$ represents the local ring of the rational functions A/B in $\mathbb{K}(x_1,\ldots,x_n)$ such that $B(P) \neq 0$.

2.6.1. Zero-dimensional sets

In this subsection, our point of view is geometric, meaning that points are considered over the algebraic closure $\bar{\mathbb{K}}$. In the affine case, an ideal I is *zero-dimensional* if $\mathcal{V}_{\mathbb{A}}(I)$ is finite; $\mathcal{V}_{\mathbb{A}}(I)$ is said to have dimension zero in this case. We recall the following classical result; see for instance [19, Chapter 2, Section 10, Proposition 6], [15, Chapter 4, Section 2], or [38, Chapter 4].

PROPOSITION 2.6. *Let I be a zero-dimensional ideal in $\mathbb{M} := \mathbb{K}[x_1,\ldots,x_n]$. Then, we have*

$$\mathbb{M}/I \cong \bigoplus_{P \in \mathcal{V}_{\mathbb{A}}(I)} \mathbb{M}_P/(I\,\mathbb{M}_P),$$

where each summand is a local $\mathbb{K}$-algebra of finite dimension.

Proof. Let $P_1,\ldots,P_D$ denote the points of $\mathcal{V}_{\mathbb{A}}(I)$. By the Nullstellensatz, a power of

$$\prod_{j=1}^{D} (x_i - x_i(P_j))$$

belongs to I for $i = 1,\ldots,n$, where $x_i(P_j)$ denotes the i-th coordinates of P_j. This shows that $\mathbb{M}/I$ is a $\mathbb{K}$-algebra whose dimension is finite.

Let M_i represent the multiplication endomorphism by x_i in $\mathbb{M}/I$ for $i = 1,\ldots,n$. Since these endomorphisms commute, it is well known that there exists a $\mathbb{K}$-algebra decomposition

$$\mathbb{M}/I \cong \bigoplus_{j=1}^{D} \mathbb{E}_j,$$

such that each $\mathbb{E}_j$ is stabilized by $M_1,\ldots,M_n$, the restriction of M_i to $\mathbb{E}_j$ admits $x_i(P_j)$ as a unique eigenvalue. Usually this decomposition is a consequence of the *generalized eigenspace decomposition*; see [38, Chapter 1, Theorem 1.1.7] for instance.

Let i be a coordinate where P_j and $P_{j'}$ differ for some $j \neq j'$. We have

$$(M_i - x_i(P_j)\,\mathrm{Id})^{\dim \mathbb{E}_j}\,\mathbb{E}_j = 0$$

in $\mathbb{M}/I$. For all $f \in \mathbb{E}_j$ we deduce that $(x_i - x_i(P_j))^{\dim \mathbb{E}_j} f \in I$, hence $f \in \mathbb{M}_{P_{j'}} I$. Consequently, $\mathbb{E}_j = \mathbb{M}_{P_j}/(I\,\mathbb{M}_{P_j})$ holds for $j = 1,\ldots,D$. □

The dimension $\dim_{\mathbb{K}}(\mathbb{M}_{P_j}/(I\,\mathbb{M}_{P_j}))$, written $\mathrm{mult}(P_j; I)$, is called the *multiplicity* of I at P_j, and $\dim_{\mathbb{K}}(\mathbb{M}/I)$ is the *degree* of I, written $\deg I$.

In particular, Proposition 2.6 tells us that a polynomial $h \in \mathbb{M}$ belongs to I if, and only if, its image h_j in $\mathbb{M}_{P_j}$ belongs to $I\,\mathbb{M}_{P_j}$ for $j = 1, \dots, D$. If P_j has multiplicity one, then h_j belongs to $I\,\mathbb{M}_{P_j}$ if, and only if, $h(P_j) = 0$. This means that if all points P_j have multiplicity 1, then h belongs to I if, and only if, it vanishes at P_j for $j = 1, \dots, D$. This is nothing else than the usual version of the Nullstellensatz when I is radical.

When working with local algebras as above, it will be sometimes convenient to regard polynomials as series, that is made possible thanks to the following well known lemma, for which we recall a standalone proof.

LEMMA 2.7. *Let I be a zero-dimensional ideal in $\mathbb{M} := \mathbb{K}[x_1, \dots, x_n]$. For all $P \in \mathcal{V}_{\mathbb{A}}(I)$, we have*

$$\mathbb{M}_P / (I\,\mathbb{M}_P) \cong \mathbb{K}[[x_1 - x_1(P), \dots, x_n - x_n(P)]] / I.$$

Proof. Without loss of generality we may assume that $P = 0$. Let m denote the multiplicity of I at P as above. We have seen in the proof of Proposition 2.6 that x_i^m is zero in $\mathbb{M}_P / (I\,\mathbb{M}_P)$, for $i = 1, \dots, n$, whence

$$J := (x_1^m, \dots, x_n^m) \subseteq I.$$

The map

$$\Phi: \quad \mathbb{M}_P / (I\,\mathbb{M}_P) \longrightarrow \mathbb{K}[[x_1, \dots, x_n]] / I$$

is well defined, and is surjective because any $h \in \mathbb{K}[[x_1, \dots, x_n]]$ defined modulo I can be truncated modulo J in order to yield a representative in $\mathbb{M}$.

Let $g_1, \dots, g_s$ denote generators of I in $\mathbb{M}$. Let $f \in \mathbb{M}$ be in the kernel of Φ, so there exist $h_1, \dots, h_s$ in $\mathbb{K}[[x_1, \dots, x_n]]$ such that $f = \sum_{i=1}^{s} h_i g_i$ holds. Let $\bar{h}_i$ denote the sum of the terms of h_i of partial degrees $< m$ in $x_1, \dots, x_n$. There exist $\tilde{h}_1, \dots, \tilde{h}_n$ in $\mathbb{K}[[x_1, \dots, x_n]]$ such that

$$f - \sum_{i=1}^{s} \bar{h}_i g_i = \sum_{i=1}^{n} \tilde{h}_i x_i^m. \tag{2.1}$$

If e denotes an upper bound on the total degree of $f - \sum_{i=1}^{s} \bar{h}_i g_i$, if $\tilde{h}_{i,\leqslant e-m}$ denotes the sum of the terms of $\tilde{h}_i$ of total degree $\leqslant e - m$, and if $\tilde{h}_{i,>e-m}$ denotes the sum of the terms of $\tilde{h}_i$ of total degree $> e - m$, then equation (2.1) rewrites into

$$f - \sum_{i=1}^{s} \bar{h}_i g_i - \sum_{i=1}^{n} \tilde{h}_{i,\leqslant e-m} x_i^m = \sum_{i=1}^{n} \tilde{h}_{i,>e-m} x_i^m.$$

It follows that both sides of the latter equality are zero, whence $f \in I$. Finally if $f \in \mathbb{M}_P$ is in the kernel of Φ, then it writes as $f = a/b$ with $a, b \in \mathbb{M}$ and $b(P) \neq 0$, so $\Phi(a) = 0$ holds, whence $f \in I\,\mathbb{M}_P$. In other words we have shown that Φ is injective. □

2.6.2. Plane curves

In the affine case, a plane curve is a Zariski closed set of the form $\mathcal{V}_{\mathbb{A}}(f)$ where f is a non-constant squarefree polynomial in $\mathbb{K}[x, y]$. In the homogeneous case it is of the form $\mathcal{V}_{\mathbb{P}}(F)$ where F is a non-constant homogeneous squarefree polynomial in $\mathbb{K}[x, y, z]$. A curve is absolutely irreducible if its defining polynomial is absolutely irreducible, that is irreducible over $\bar{\mathbb{K}}$.

PROPOSITION 2.8. *Let F and G be two homogeneous non-constant polynomials in $\mathbb{K}[x, y, z]$ that are coprime. Then $\mathcal{V}_{\mathbb{P}}(F, G)$ is zero-dimensional.*

Proof. Regarded in $\mathbb{K}[x,y][z]$, the resultant $\mathrm{Res}_z(F,G)$ is non-zero and belongs to the ideal (F,G). Doing so for permutations of the variables we have

$$\mathcal{U}_{\mathbb{P}}(F,G) \subseteq \mathcal{U}_{\mathbb{P}}(\mathrm{Res}_x(F,G), \mathrm{Res}_y(F,G), \mathrm{Res}_z(F,G)),$$

and the right-hand side is a finite set of points. □

2.7. Popov form

Let $\boldsymbol{b}_1,\dots,\boldsymbol{b}_\delta$ be a basis of a free $\mathbb{K}[x]$-submodule of rank δ of $\mathbb{K}[x]^\delta$. We introduce the *shift vector*

$$\boldsymbol{s} := (\delta-1, \delta-2, \dots, 1, 0), \tag{2.2}$$

and we let

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

denote the *shifted 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 $i=1,\dots,n$,
- $\boldsymbol{b}_{i,i}$ is monic for $i=1,\dots,n$,
- $\deg \boldsymbol{b}_{j,i} < \deg \boldsymbol{b}_{i,i}$ for $i=1,\dots,n$, 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 2.9. [2, 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 $\Delta \geqslant 0$, the elements in $\mathcal{M}$ of $\boldsymbol{s}$-degree $\leqslant \Delta$ form a $\mathbb{K}$-vector space of basis $x^j \boldsymbol{b}_i$ for $i=1,\dots,\delta$ such that $\deg_{\boldsymbol{s}} \boldsymbol{b}_i \leqslant \Delta$ and $j=0,\dots,\Delta-\deg_{\boldsymbol{s}} \boldsymbol{b}_i$.*

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 [46, Theorem 7.1]. The current best known bound $\tilde{O}(m^{\omega-1} n \deg M)$ holds whenever $m \leqslant n$ [48, 49]. For more information about the Popov form we refer the reader to [47].

3. THE BRILL–NOETHER METHOD FROM SCRATCH

This section is devoted to a proof of the Brill–Noether method, that computes Riemann–Roch spaces of plane curves. Because of complexity issues, we restrict to the case of a projective curve C defined over a perfect field $\mathbb{K}$ by the equation $F=0$, under the assumptions that F is absolutely irreducible and that all the singularities of C are ordinary. Our approach is down-to-earth: we use elementary arguments that will turn out to be constructive in the next sections.

3.1. Max Noether's theorem

This subsection is devoted to a proof of Max Noether's theorem that gives local algebraic conditions for a rational function to be regular over C. Let G and H denote non-zero homogeneous polynomials in $\mathbb{K}[x,y,z]$ such that G is prime to F. By Proposition 2.8, the set $\mathcal{U}_{\mathbb{P}}(F,G)$ is finite. If H vanishes at $\mathcal{U}_{\mathbb{P}}(F,G)$, then the Nullstellensatz theorem implies that some power of H belongs to the ideal (F,G). Max Noether's theorem focuses on stronger local criteria for ensuring that H does belong to the ideal (F,G).

The following classical definition says that H belongs to the ideal generated by F and G in a neighborhood of a point P.

DEFINITION 3.1. ***(Noether's local condition)*** *Let F,G,H be homogeneous polynomials in $\mathbb{K}[x,y,z]$. When F and G are coprime,* 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 $\bar{\mathbb{K}}[x,y,z]_P$.*

In other words, Noether's condition at P means the existence of A_P,B_P,C_P in $\bar{\mathbb{K}}[x,y,z]$ such that $C_PH=A_PF+B_PG$ and $C_P(P)\neq 0$. Since F,G,H are homogeneous, A_P,B_P,C_P can freely be taken homogeneous.

Now we are interested in situations where Noether's condition holds at any point $P\in\mathbb{P}^2$. First, we note that Noether's condition always holds at a point outside of $\mathcal{V}_{\mathbb{P}}(F,G)$: in fact if $F(P)\neq 0$ then we have $FH=HF+0\times G$, so we take $C_P=F$, $A_P=H$, and $B_P=0$; similarly if $G(P)\neq 0$ then we take $C_P=G$, $A_P=0$, and $B_P=H$. So Noether's conditions are satisfied everywhere if, and only if, they hold at the finite set $\mathcal{V}_{\mathbb{P}}(F,G)$.

Without loss of generality, and after an occasional algebraic extension of $\mathbb{K}$, we may apply a linear change of variables in order to ensure that $\mathcal{V}_{\mathbb{P}}(F,G)$ is included in the affine chart $z=1$. Under this assumption, for any point $P=(P_x:P_y:P_z)\in\mathcal{V}_{\mathbb{P}}(F,G)$ we may take $P_z=1$. Then Noether's condition at P is further equivalent to the belonging of $H(x,y,1)$ to the extension of

$$I:=(F(x,y,1),G(x,y,1))$$

to $\bar{\mathbb{K}}[x,y]_{(P_x,P_y)}$. Noether's local condition is satisfied at such a point P of $\mathcal{V}_{\mathbb{P}}(F,G)$ if, and only if, the image of $H(x,y,1)$ in $\bar{\mathbb{K}}[x,y]_{(P_x,P_y)}/(I\,\bar{\mathbb{K}}[x,y]_{(P_x,P_y)})$ is zero. By Proposition 2.6, this is further equivalent to the belonging of $H(x,y,1)$ to I. This observation extends to projective setting in the following seminal theorem.

THEOREM 3.2. ***(Max Noether's fundamental theorem)*** *Let F,G,H be homogeneous polynomials in $\mathbb{K}[x,y,z]$ such that F and G are coprime. The two following assertions are equivalent:*

1. *There exist homogeneous polynomials A and B in $\mathbb{K}[x,y,z]$ such that $H=AF+BG$ and*

$$\deg H=\deg A+\deg F=\deg B+\deg G.$$

2. *Noether's condition is satisfied by the triple (F,G,H) at all points of $\mathbb{P}^2$.*

Proof. It is clear that (1) implies (2). For the converse implication, we resume the above discussion, that has led us to $H(x,y,1)\in I$. In other words there exist a and b in $\mathbb{K}[x,y]$ such that

$$H(x,y,1)=a(x,y)\,F(x,y,1)+b(x,y)\,G(x,y,1).$$

After homogenization of the latter identity, we obtain another relation of the form

$$z^nH(x,y,z)=A(x,y,z)\,F(x,y,z)+B(x,y,z)\,G(x,y,z), \tag{3.1}$$

where $n\geqslant 0$ and A and B can be taken homogeneous. If $n=0$ then we are done. Otherwise $n\geqslant 1$ and the relation (3.1) rewrites into

$$z^nH(x,y,z)=(A(x,y,0)+z\tilde{A}(x,y,z))\,F(x,y,z)+(B(x,y,0)+z\tilde{B}(x,y,z))\,G(x,y,z),$$

where $\tilde{A}$ and $\tilde{B}$ are homogeneous polynomials. Since $n\geqslant 1$ this yields

$$0=A(x,y,0)\,F(x,y,0)+B(x,y,0)\,G(x,y,0).$$

Since $F(x,y,0)$ and $G(x,y,0)$ have no common root in $\mathbb{P}^1$, they are coprime. Therefore there exists a homogeneous $C(x,y)$ such that

$$\begin{aligned} A(x,y,0) &= C(x,y)\,G(x,y,0) \\ B(x,y,0) &= -C(x,y)\,F(x,y,0). \end{aligned}$$

Since $F(x,y,z)-F(x,y,0)$ and $G(x,y,z)-G(x,y,0)$ are multiples of z, we obtain polynomials $\hat{A}$ and $\hat{B}$ such that

$$\begin{aligned} A(x,y,0) &= C(x,y)\,G(x,y,z)+z\,\hat{A}(x,y,z) \\ B(x,y,0) &= -C(x,y)\,F(x,y,z)+z\,\hat{B}(x,y,z). \end{aligned}$$

Plugging the latter expressions into (3.1), we deduce that

$$\begin{aligned} z^n H(x,y,z) &= (C(x,y)\,G(x,y,0)+z\,(\hat{A}(x,y,z)+\tilde{A}(x,y,z)))\,F(x,y,z) \\ &\quad +(-C(x,y)\,F(x,y,0)+z\,(\hat{B}(x,y,z)+\tilde{B}(x,y,z)))\,G(x,y,z) \\ &= z\,((\hat{A}(x,y,z)+\tilde{A}(x,y,z))\,F(x,y,z)+(\hat{B}(x,y,z)+\tilde{B}(x,y,z))\,G(x,y,z)). \end{aligned}$$

This proves that $z^{n-1}H$ belongs to (F,G). Iterating this process n times shows that H does belong to (F,G). □

3.2. Ordinary singularities

Let P be a singular point of $\mathcal{C}$. Up to a suitable change of variables we may assume that $P=(0:0:1)$ and that no tangent of $\mathcal{C}$ at P is vertical. The point P is said to be an *ordinary singularity of multiplicity m* if the equation of $\mathcal{C}$ locally factorizes into

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

where $u\in\bar{\mathbb{K}}[[x,y]]$ is invertible, $\varphi_i(x)\in x\,\bar{\mathbb{K}}[[x]]$ for $i=1,\dots,m$, and such that $\varphi_i'(0)\neq\varphi_j'(0)$ for all $i\neq j$. This condition is equivalent to the following property: $F(x,y,1)$ has valuation m in $\mathbb{K}[[x,y]]$, and the homogeneous component of degree m of $F(x,y,1)$ is squarefree. This second formulation is independent of the set of coordinates.

3.3. Divisors

Let $P=(P_x,P_y)$ be a point in the affine chart $z=1$ of $\mathcal{C}$. The hypothesis that $\mathcal{C}$ has only ordinary singularities ensures that the germ of curve defined by $F=0$ in the neighborhood of P decomposes as follows, up to a sufficiently generic change of coordinates:

$$F(x,y,1)=u(x,y)\prod_{i=1}^{m}(y-\varphi_i(x)), \tag{3.3}$$

where $u\in\bar{\mathbb{K}}[[x-P_x,y-P_y]]$ is invertible, $\varphi_i\in P_y+(x-P_x)\,\mathbb{K}[[x-P_x]]$, and such that the $\varphi_i'(P_x)$ are pairwise distinct, for $i=1,\dots,m$.

The *local divisor* at P of a homogeneous polynomial $A\in\mathbb{K}[x,y,z]$ prime to F is defined as the set of pairs

$$\{((P_x+t,\varphi_i(t),1),\mathrm{val}_t(A(P_x+t,\varphi_i(t),1))) : i=1,\dots,m\}.$$

It is usual to write this set as a symbolic sum of the form

$$\mathrm{Div}_P(A):=\sum_{i=1}^{m}\mathrm{val}_t(A(P_x+t,\varphi_i(t),1))\;\mathcal{P}_i, \tag{3.4}$$

where $\mathcal{P}_i$ is a symbol that uniquely represents the germ of curve parametrized by φ_i, independently of the set of coordinates. For the usual terminology, $\mathcal{P}_i$ corresponds to the notion of a *place* of the function field $\bar{\mathbb{K}}(C)$.

The *(global) divisor* of A is the union, written as a symbolic sum, of its local divisors for all $P \in C$, that is

$$\mathrm{Div}(A) := \sum_{P \in C} \mathrm{Div}_P(A).$$

Since A is prime to F, $\mathcal{U}_{\mathbb{P}}(F,A)$ is finite, so the latter sum is finite. If A/B is a non-zero function in $\mathbb{K}(C) \setminus \{0\}$ then we define

$$\mathrm{Div}(A/B) := \mathrm{Div}(A) - \mathrm{Div}(B).$$

More generally, a divisor of C is a finite $\mathbb{Z}$-linear combination of places of C. The set of divisors is endowed with a partial order: we write $D_1 \leqslant D_2$ when the coefficient in D_1 of the place $\mathcal{P}$ is less than or equal to the coefficient in D_2 of $\mathcal{P}$, for all $\mathcal{P}$. The *support* of D is the set of places occurring in D with a non-zero coefficient.

3.4. Degree of a divisor

The *degree of a divisor* D, written $\deg D$, is defined as the sum of all its coefficients. Let A be a homogeneous polynomial prime to F of degree d. Up to a suitable change of coordinates we may assume that $\mathcal{U}_{\mathbb{P}}(F,A)$ is in the affine chart $z=1$. By Proposition 2.6 we have

$$\bar{\mathbb{K}}[x,y]/(F(x,y,1),A(x,y,1)) \;\cong \bigoplus_{P \in \mathcal{U}_{\mathbb{A}}(F(x,y,1),A(x,y,1))} \bar{\mathbb{K}}[x,y]_P/(F(x,y,1),A(x,y,1)).$$

By Lemma 2.7, we further have

$$\bar{\mathbb{K}}[x,y]_P/(F(x,y,1),A(x,y,1)) \;\cong\; \bar{\mathbb{K}}[[x-P_x,y-P_y]]/(F(x,y,1),A(x,y,1)).$$

Again, up to a suitable change of coordinates, F can be assumed to be monic in y and to factorize as in (3.3). From Proposition 5.4 below and since

$$\mathrm{Res}_y\left(\prod_{i=1}^{m}(y-\varphi_i(x)), A(x,y,1)\right)$$

is the determinant of the multiplication by $A(x,y,1)$ in

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

(see [6, Chapitre 6, Lemme 6.9] for instance), we obtain that

$$\begin{aligned}\dim(\bar{\mathbb{K}}[x,y]_P/(F(x,y,1),A(x,y,1))) &= \mathrm{val}_{x-P_x}\left(\mathrm{Res}_y\left(\prod_{i=1}^{m}(y-\varphi_i(x)), A(x,y,1)\right)\right)\\ &= \mathrm{val}_{x-P_x}\left(\prod_{i=1}^{m} A(x,\varphi_i(x),1)\right).\end{aligned}$$

It follows that the degree of $\mathrm{Div}_P(A)$ is the multiplicity of the ideal $(F(x,y,1),A(x,y,1))$ at P, and that the degree of $\mathrm{Div}(A)$ is the degree of the ideal (F,A).

PROPOSITION 3.3. *Let $A/B \in \mathbb{K}(C) \setminus \{0\}$. The divisor* $\mathrm{Div}(A/B)$ *is zero if, and only if, A/B is a constant in $\mathbb{K}$.*

Proof. If A/B is a constant then $\mathrm{Div}(A/B) = 0$ by definition. Conversely let us assume that $\mathrm{Div}(A/B) = 0$. Up to a sufficiently generic change of coordinates we may assume that the common zeros of A and F and of B and F are in the affine chart $z = 1$. Assume that A is not in $\mathbb{K}$. There exists a point $P = (P_x : P_y : 1)$ in $\mathcal{V}_{\mathbb{P}}(A,F)$ and we may consider a place parametrized by

$$x = P_x + t,\ y = \varphi(t) \in P_y + t\,\bar{\mathbb{K}}[[t]]$$

centered at this point. The assumption on $\mathrm{Div}(A/B)$ implies that the valuations of A and B coincide at this place, whence

$$k := \mathrm{val}_t(A(P_x + t, \varphi(t), 1)) = \mathrm{val}_t(B(P_x + t, \varphi(t), 1)).$$

Consequently there exists $\lambda \in \bar{\mathbb{K}}$ such that

$$\mathrm{val}_t((A - \lambda B)(P_x + t, \varphi(t), 1)) \geqslant k + 1.$$

At any other place $\mathcal{P}$ the valuation of $A - \lambda B$ is at least the valuation of A, that also coincides with the one of B. It follows that

$$\deg(\mathrm{Div}(A - \lambda B)) > \deg(\mathrm{Div}(A)).$$

By the Bézout theorem, namely our Proposition 5.5 below, the two latter degrees are equal to $\deg F \deg A$, that yields a contradiction. □

3.5. The residue theorem

If the local divisor of a rational function is "sufficiently large", then this function is locally regular, *i.e.* is regular at each germ of curve. The role of the adjoint divisor is to make precise the latter condition. This is formalized as follows.

DEFINITION 3.4. *The* local adjoint divisor *of C at P is $\mathcal{A}_P := (m-1)\sum_{i=1}^{m} \mathcal{P}_i$ (with the notation used in (3.4)). In particular $\mathcal{A}_P$ is zero at any regular point P of C. The* adjoint divisor $\mathcal{A}$ *of C is the sum of the $\mathcal{A}_P$ for all $P \in C$.*

PROPOSITION 3.5. *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.*

Proof. Without loss of generality we may assume that $P = (0:0:1)$ and that the local equation of F in the neighborhood of P writes as above:

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

where $u \in \mathbb{K}[[x, y]]$ is invertible. The condition $\mathrm{Div}_P(B) \geqslant \mathrm{Div}_P(A) + \mathcal{A}_P$ means that

$$\mathrm{val}(B(x, \varphi_i(x), 1)) \geqslant \mathrm{val}(A(x, \varphi_i(x), 1)) + m - 1, \text{ for } i = 1, \ldots, m.$$

Independently, Lagrange interpolation formula in $\mathbb{K}((x))[y] / (\prod_{i=1}^{m} (y - \varphi_i(x)))$ yields

$$\left(\frac{B}{A}\right)(x, y, 1) \equiv \sum_{i=1}^{m} \frac{B(x, \varphi_i(x), 1)}{A(x, \varphi_i(x), 1)} \frac{\prod_{j \neq i} (y - \varphi_j(x))}{\prod_{j \neq i} (\varphi_i(x) - \varphi_j(x))} \bmod \prod_{i=1}^{m} (y - \varphi_i(x)). \tag{3.5}$$

Since P is an ordinary singularity, for $i=1,\dots,m$, we have

$$\mathrm{val}_x\left(\prod_{j\neq i}(\varphi_i(x)-\varphi_j(x))\right)=m-1,$$

so the right-hand side of (3.5) yields a canonical representation of B/A in $\mathbb{K}[[x]][y]$ modulo $\prod_{i=1}^{m}(y-\varphi_i(x))$. We deduce that $B(x,y,1)$ belongs to the ideal $(F(x,y,1),A(x,y,1))$ regarded in $\mathbb{K}[[x,y]]$. By Lemma 2.7, $B(x,y,1)$ belongs to

$$(F(x,y,1),A(x,y,1))\,\mathbb{K}[x,y]_{(0,0)},$$

that corresponds to the claimed Noether condition. □

Combined with Max Noether's theorem, Proposition 3.5 can be "globalized" as follows.

PROPOSITION 3.6. *Consider two homogeneous polynomials A and B prime to F. If* $\mathrm{Div}(B)\geqslant \mathrm{Div}(A)+\mathcal{A}$ *then B belongs to (F,A).*

Proof. By Proposition 3.5, Noether's condition is satisfied by the triple (F,A,B) at all $P\in C$, so Theorem 3.2 concludes the proof. □

Two divisors D and $\tilde{D}$ of C are said to be *linearly equivalent* if there exists a rational function $A/B\in\bar{\mathbb{K}}(C)$ such that $D=\tilde{D}+\mathrm{Div}(A/B)$.

THEOREM 3.7. ***(Residue theorem)*** *Let D and $\tilde{D}$ be two linearly equivalent divisors of C with $\tilde{D}\geqslant 0$. If H is a homogeneous polynomial prime to F such that*

$$\mathrm{Div}(H)=D+\mathcal{A}+R,$$

for a positive divisor R, then there exists a homogeneous polynomial G prime to F of the same degree as H such that

$$\mathrm{Div}(G)=\tilde{D}+\mathcal{A}+R.$$

Proof. Let $A/B\in\mathbb{K}(C)$ be such that

$$D=\tilde{D}+\mathrm{Div}(A/B).$$

We have

$$\mathrm{Div}(BH)=\mathrm{Div}(B)+D+\mathcal{A}+R=\mathrm{Div}(A)+\tilde{D}+\mathcal{A}+R.$$

Since $\tilde{D}$ and R are positive we have $\mathrm{Div}(BH)\geqslant\mathrm{Div}(A)+\mathcal{A}$. By Proposition 3.6, BH belongs to the ideal (F,A), so there exists a homogeneous polynomial G such

$$AG-BH\in(F).$$

It follows that G is prime to F and that $\mathrm{Div}(AG)=\mathrm{Div}(BH)$, whence

$$\mathrm{Div}(G)=\mathrm{Div}(BH)-\mathrm{Div}(A)=\tilde{D}+\mathcal{A}+R.$$ □

3.6. The Brill–Noether method

Recall that the Riemann–Roch space $\mathcal{L}(D)$ of a divisor D of C is

$$\mathcal{L}(D):=\left\{\frac{A}{B}\in\mathbb{K}(C)\setminus\{0\}:\mathrm{Div}(A/B)\geqslant -D\right\}\cup\{0\}.$$

THEOREM 3.8. *Let C be an absolutely irreducible plane projective curve of equation $F=0$, let $\mathcal{A}$ be its adjoint divisor, and let D be a divisor of C. Let H be a non-zero homogeneous polynomial of degree d prime to F, such that* $\mathrm{Div}(H) \geqslant D + \mathcal{A}$. *Then we have*

$$\mathcal{L}(D) = \left\{ \frac{G}{H} \in \mathbb{K}(C) \setminus \{0\} : \mathrm{Div}(G/H) \geqslant -D \right\} \cup \{0\}.$$

Proof. The functions in the latter set clearly belong to $\mathcal{L}(D)$. Conversely, consider a non-zero function A/B in $\mathcal{L}(D)$. From the definition of $\mathcal{L}(D)$, the divisor

$$\tilde{D} := D + \mathrm{Div}(A) - \mathrm{Div}(B)$$

is positive. We apply Theorem 3.7 to $\tilde{D}$ and to the decomposition

$$\mathrm{Div}(H) = D + \mathcal{A} + R,$$

where $R := \mathrm{Div}(H) - D - \mathcal{A}$ is positive. This yields a homogeneous polynomial G of degree d such that

$$\mathrm{Div}(G) = \tilde{D} + \mathcal{A} + R = \tilde{D} - D + \mathrm{Div}(H).$$

Consequently, we have

$$\mathrm{Div}(G/H) = \tilde{D} - D = \mathrm{Div}(A/B).$$

Then $\mathrm{Div}((G/H)/(A/B))$ is zero, and $(G/H)/(A/B)$ is a constant by Proposition 3.3. Finally, we have shown that A/B writes as a $\mathbb{K}$-multiple of G/H in $\mathbb{K}(C)$. □

Theorem 3.8 is the cornerstone of the Brill–Noether method, summarized in the following algorithm.

Algorithm 3.1

Input. An absolutely irreducible plane projective curve C defined by the equation $F=0$, and a divisor D of C.

Output. A basis of $\mathcal{L}(D)$.

Assumption. The singularities of C are ordinary.

1. Compute the adjoint divisor $\mathcal{A}$ of C.
2. Find a homogeneous polynomial H prime to F such that $\mathrm{Div}(H) \geqslant D + \mathcal{A}$.
3. Compute $\mathrm{Div}(H) - D$.
4. Compute a basis $G_1, \ldots, G_l$ of the space of all homogeneous polynomials G of degree $\deg H$ such that $\mathrm{Div}(G) \geqslant \mathrm{Div}(H) - D$.
5. Return $G_1/H, \ldots, G_l/H$.

We will present further details on each intermediate step in dedicated sections.

3.7. Equivalence to usual definitions

The above definition of a divisor of C coincides with the usual one of [19], that is a $\mathbb{Z}$-linear combination of a finite set of points on a desingularization of C. The advantage of our present definition is precisely to avoid considering a desingularization of C but also to ease the presentation, because our algorithms will actually manipulate local divisors as power series.

Precisely, assume that $P=(0:0:1)$ is an ordinary singular point of $\mathcal{C}$ and consider the local factorization of F as in (3.2). For the blow-up parametrized by $y=tx$, the local equation of the desingularized germ of curve $\tilde{\mathcal{C}}$ in the coordinates x and t is

$$\prod_{i=1}^{m}(t-\tilde{\varphi}_i(x))=0,$$

where $\tilde{\varphi}_i(x):=\varphi_i(x)/x$. If $A(x,y,z)$ is homogeneous and prime to F then its intersection multiplicity with the branch $y=\varphi_i(x)$ is $\mathrm{val}_x(A(x,\varphi_i(x),1))$. With $\tilde{A}(x,t,z):=A(x,tx,z)$, the intersection multiplicity of $\tilde{A}$ with the regular germ of curve $t=\tilde{\varphi}_i(x)$ is

$$\mathrm{val}_x(\tilde{A}(x,\tilde{\varphi}_i(x),1))=\mathrm{val}_x(A(x,\varphi_i(x),1)).$$

The usual local adjoint divisor of $\mathcal{C}$ is defined as

$$\sum_{i=1}^{m}(m-1)\,(0,\tilde{\varphi}_i(0)).$$

It corresponds to intersection multiplicities $m-1$ at $(x,\tilde{\varphi}_i(x))$, that is valuation $m-1$ at the germ of curve defined by $y=\varphi_i(x)$, for $i=1,\dots,m$. Consequently the notion of adjoint introduced above is equivalent to the one of [19].

3.8. Notes

Nice expositions of the Max Noether theorem can be found in text books: for instance [19, Chapter 5, Section 5], [12, Chapter 3], etc.

The results presented in this section, along with their proofs, are not new. However, it is interesting to remark that the residue theorem (precisely Theorem 3.7) is generally stated for D and $\tilde{D}$ both positive, while only the positiveness of $\tilde{D}$ is actually needed. This weaker assumption intervenes in the efficiency of our algorithm: in fact it is crucial within the proof of Lemma 6.1 in order to guarantee the existence of denominators involving only smooth extra points. This refined version of the residue theorem was previously used by Haché [25, 26].

The elementary computational arguments used in the proof of Theorem 3.2 are borrowed from the proof of [12, Lemma 3.8.4]. Let us briefly mention a general argument from algebraic geometry that can be used instead. After a generic linear change of coordinates, the ring extension

$$\mathbb{K}[z]\hookrightarrow\mathbb{K}[x,y,z]/(F,G)$$

is integral. Since the ideal (F,G) is unmixed, $\mathbb{K}[x,y,z]/(F,G)$ has no $\mathbb{K}[z]$-torsion; see for instance [18, Proposition 1.22].

Proposition 3.5 is detailed in the more general context of any type of singularity in [25, Proposition 2.6.3]. Proposition 3.6 is extended in [25, Theorem 2.6.9]. Therefore Algorithm 3.1 works for any type of singularities [25, 26, 40].

4. DIVISORS

In order to turn the Brill–Noether method into practice, we need to specify how divisors are represented and how to operate on them.

4.1. Primitive element representations

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 $\lambda(x,y) := \lambda_x x + \lambda_y y$ *separates* the points of $\mathcal{E}$. This means that the form takes different values at different points of $\mathcal{E}$.
- 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 will be said *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* $\mathbb{K}$. It is worth noting that even if the annihilator ideal of $\mathcal{E}$ is generated by polynomials with coefficients in $\mathbb{K}$, a primitive element representation may not necessarily exist over $\mathbb{K}$ when $|\mathbb{K}|$ is too small.

LEMMA 4.1. *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. Let us write $\mathcal{E} = \{P_1, \ldots, P_{|\mathcal{E}|}\}$. We define

$$\Lambda(\lambda_x, \lambda_y) := \prod_{i<j} (\lambda_x x(P_i) + \lambda_y y(P_i) - (\lambda_x x(P_j) + \lambda_y y(P_j))). \tag{4.1}$$

It is a non-zero polynomial in $\bar{\mathbb{K}}[\lambda_x, \lambda_y]$ of total degree $\binom{|\mathcal{E}|}{2}$. If $\Lambda(a,b) \neq 0$ then x is primitive for $M(\mathcal{E})$. The probability bound follows from the well known Schwartz–Zippel lemma; for instance see [20, Lemma 6.44]. □

If $\mathbb{K}$ does not have sufficiently many elements to guarantee the existence of primitive element representations, then $\mathbb{K}$ may be replaced by a sufficiently large algebraic extension. We will not discuss these usual technical issues here, but instead, we will make explicit the conditions on the cardinality of $\mathbb{K}$ for each sub-algorithm.

By Proposition 2.6, if I is an ideal of dimension 0 of $\mathbb{K}[x,y]$ and if λ is primitive for $\mathcal{V}_{\mathbb{A}}(I)$, then the characteristic polynomial of the multiplication endomorphism by λ in $\mathbb{K}[x,y]/I$ is

$$\prod_{P\in\mathcal{V}_{\mathbb{A}}(I)} (t - \lambda(P))^{\mathrm{mult}(P;I)}.$$

In particular, the multiplicities of the points of $\mathcal{V}_{\mathbb{A}}(I)$ can be read off from this characteristic polynomial.

The change of primitive elements to represent sets of points, or more generally a basis of a quotient algebra of the form $\mathbb{K}[t]/(\theta(t))$, is a classical problem in computer algebra. The proof of the following lemma mostly gathers known techniques. Early ideas go back to Le Verrier [43], and fast algorithms have been designed and popularized by Shoup [54, 55]. Here, we slightly improve [2, Lemma 2.3].

LEMMA 4.2. *Let $\theta(t) \in \mathbb{K}[t]$ be a monic separable polynomial of degree n. 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*

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

is an isomorphism, with $O(n^\omega)$ field operations in characteristic zero or $>n$, or $\tilde{O}(n^\omega \log q)$ bit operations if $\mathbb{K} = \mathbb{F}_q$.

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 $\mu(z) := z^n \theta(1/z)$ stand for the reciprocal polynomial of θ, and we compute the power series expansion

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

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

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

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

We mentioned in Section 2.3 that this task is the transpose of modular composition, so it takes $O(n^\omega)$ operations in $\mathbb{K}$ by [20, Theorem 12.4].

Then, the generating series

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

satisfies the Newton–Girard formula

$$-\frac{\nu'(z)}{\nu(z)} = \tau(z) + O(z^n), \tag{4.2}$$

where $\nu(z) := z^n \tilde{\theta}(1/z)$ is the reciprocal of $\tilde{\theta}$. Therefore ν is recovered with $\tilde{O}(n)$ operations in characteristic zero or $>n$; for instance see [7, Corollary 1] or [24, Proposition 3]. In positive characteristic, the integration of (4.2) is more tedious in general, but in the special case $\mathbb{K} = \mathbb{F}_q$, it is possible with $\tilde{O}(n \log q)$ bit operations; see [24, Proposition 3].

Testing if $e(t)$ is primitive is equivalent to testing if $\tilde{\theta}$ is separable, which takes $\tilde{O}(n)$ operations in $\mathbb{K}$. If $e(t)$ is primitive then t can be written as

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

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

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

and verify that

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

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

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

is a polynomial of degree $\leqslant 2n-1$. Since $-z\nu'(z)+n\nu(z)$ has degree $\leqslant 2n-1$, we further obtain that σ has degree $\leqslant 2n-2$.

It follows that

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

whence that

$$z^{2n-1}\sigma(z^{-1}) = z\,\eta(z)\tilde{\theta}'(z)+\rho(z)\,z^{n+1}\nu(z^{-1}).$$

We may divide both sides of the latter identity by z, and deduce η as

$$\eta(z) = (z^{2n-2}\sigma(z^{-1}))\,/\,\tilde{\theta}'(z) \bmod \tilde{\theta}(z). \qquad \square$$

PROPOSITION 4.3. *Given a primitive element representation of $\mathcal{E}$ over $\mathbb{K}$ by $\lambda := \lambda_x x+\lambda_y y$, and given $(\tilde{\lambda}_x,\tilde{\lambda}_y)\in\mathbb{K}^2$, we can test if $\tilde{\lambda} := \tilde{\lambda}_x x+\tilde{\lambda}_y y$ is primitive for $\mathcal{E}$, and, if so, compute the corresponding representation of $\mathcal{E}$, along with $\eta(t)\in\mathbb{K}[t]_{<|\mathcal{E}|}$ such that*

$$\begin{aligned}\mathbb{K}[t]/(\theta(t)) &\cong \mathbb{K}[t]/(\tilde{\theta}(t)) \\ t &\longmapsto \eta(t) \\ \tilde{\lambda}_x v_x(t)+\tilde{\lambda}_y v_y(t) &\longleftarrow t\end{aligned}$$

is an isomorphism, with $O(|\mathcal{E}|^\omega)$ field operations in characteristic zero or $>|\mathcal{E}|$, or $\tilde{O}(|\mathcal{E}|^\omega\log q)$ bit operations if $\mathbb{K}=\mathbb{F}_q$.

Proof. This is a consequence of Lemma 4.2 applied to $e(t)=\tilde{\lambda}_x v_x(t)+\tilde{\lambda}_y v_y(t)$. $\square$

The next lemma concerns p-th root extraction. We state it here because it mostly follows from Lemma 4.2.

LEMMA 4.4. *Let $\theta(t)$ be a monic separable polynomial of degree n in $\mathbb{F}_q[t]$. The extraction of a p-th root in $\mathbb{F}_q[t]/(\theta(t))$ takes $O((n\log q)^{1+\epsilon})+\tilde{O}(n\log q\log p)$ bit operations.*

Proof. We compute $e(t) := t^p \bmod \theta(t)$ with $\tilde{O}(n\log q\log p)$ bit operations. Then, we adapt the proof of Lemma 4.2: the polynomial $e(t)$ now plays the role of the new primitive element, so we can compute the expression of t in terms of $e(t)$ modulo $\theta(t)$, namely

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

with $\eta\in\mathbb{F}_q[t]_{<n}$. If $q\geqslant n^{1+\epsilon}$ then the cost of a power projection in degree n over $\mathbb{F}_q$ is $(n\log q)^{1+\epsilon}$ by [36, Theorem 7.7, p. 1792]. Overall, η is obtained with $O((n\log q)^{1+\epsilon})+\tilde{O}(n\log q\log p)$ bit operations.

Once η is known, given $a \bmod \theta$ we compute $a\circ\eta \bmod \theta$ and note that

$$a(t) \bmod \theta(t) = (a\circ\eta \bmod \theta)(t^p).$$

Via Proposition 2.1 we extract the p-th roots of the coefficients of $a\circ\eta \operatorname{rem} \theta$ in order to deduce the p-th root of $a \bmod \theta$.

If $q < n^{1+\epsilon}$ then we set

$$l := \lceil (1+\epsilon) \log n / \log q \rceil = O(\log n),$$

so we have $q^l \geqslant n^{1+\epsilon}$. We compute an irreducible polynomial of degree l over $\mathbb{F}_q$ in time

$$\tilde{O}(\sqrt{q}\, l^{4+\epsilon}) = \tilde{O}(n \log q)$$

by [53, Theorem 4.1]. Finally, computing power projections over $\mathbb{F}_{q^l}$ instead of $\mathbb{F}_q$ is possible at the price of an additional logarithmic factor in the complexity bound. □

The final problem to be handled with primitive element representations concerns changes of coordinates in the projective setting.

PROPOSITION 4.5. *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 $O(n^\omega)$ field operations in characteristic zero or $>n$, or $\tilde{O}(n^\omega \log q)$ bit operations if $\mathbb{K} = \mathbb{F}_q$.

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 4.2 with $\mathbb{K}[t]/(\theta(t))$ and $e(t) := \tilde{\lambda}_x \tilde{u}(t) + \tilde{\lambda}_y \tilde{v}(t)$. □

4.2. Representation of smooth divisors

A divisor D of C is said to be *smooth* if its support is made of regular germs of curves of C. Since the regular germ of curve of C centered at P (that is a regular point) is uniquely determined by P, a smooth divisor D will be written in terms of the set of its centers $\mathcal{E} = \{P_1, \ldots, P_s\}$, also called its *support* for convenience, as follows:

$$D = m_1 P_1 + \cdots + m_s P_s,$$

with $m_i \neq 0$. We have $\deg D = m_1 + \cdots + m_s$.

Up to a linear change of coordinates we may assume that the support of D is in the affine chart $z=1$. In this case, a *primitive element* for D is a linear form $\lambda_x x + \lambda_y y$ that is primitive for its support, and satisfies the additional condition

$$\prod_{i=1}^{s} \begin{vmatrix} \frac{\partial F}{\partial x}(P_i) & \frac{\partial F}{\partial y}(P_i) \\ \lambda_x & \lambda_y \end{vmatrix} \neq 0.$$

Combined with condition (4.1) and using the Schwartz–Zippel lemma, as soon as

$$|\mathbb{K}| > \binom{\deg D_+ + \deg D_-}{2} + \deg D_+ + \deg D_- = \binom{\deg D_+ + \deg D_- + 1}{2}$$

then primitive elements can be found in $\mathbb{K}$.

PROPOSITION 4.6. *Given a smooth positive divisor $D = m_1P_1 + \cdots + m_sP_s$ whose support is in the affine chart $z = 1$, and given a primitive element $\lambda_x x + \lambda_y y$ for D, there exist unique polynomials χ, u, and v in $\bar{\mathbb{K}}[t]$ with the following properties:*

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

Div-H₁. *$F(u(t), v(t), 1) = 0 \bmod \chi(t)$,*

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

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

Proof. The proof can be found in [42, Section 3] or in [2, Proposition 3.1]. □

Remark 4.7. When the variable x is primitive for D, we omit λ_x, λ_y and $u(t) = t$, so that D is simply represented by the two polynomials χ and v.

Example 4.8. With $F(x, y, z) = x^2 + y^2 - z^2$, the divisor $D = 3\,(0:1:1)$ can be represented as above by taking $\lambda_x = 1$, $\lambda_y = 0$, $\chi(t) = t^3$, $u(t) = t$ and $v(t) = 1 - t^2/2$. We notice that $v(t)$ is nothing else than the power series expansion of the germ of C at $(0:1:1)$ that parametrizes y in terms of x at order 3. More generally, the divisor representation stated in Proposition 4.6 can be regarded as the glue of several germs of curves via Proposition 2.4 and Chinese remaindering.

4.3. Lifting divisors

The first operation to be useful is the doubling of a smooth divisor. Precisely we double its multiplicities by means of a suitable Newton iteration.

LEMMA 4.9. *Let D be a smooth positive divisor parametrized by $\lambda_x x + \lambda_y y$. The representation of $2D$ by $\lambda_x x + \lambda_y y$ can be computed with $\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\right)$ operations in $\mathbb{K}$.*

Proof. The proof is adapted from [2, Lemma 3.2]. We use the map

$$\Xi\colon \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} F(x, y, 1) \\ \lambda_x x + \lambda_y y - t \end{pmatrix}.$$

Let χ, u, v represent D, so $\Xi(u(t), v(t)) = 0 \bmod \chi(t)$. The Newton iteration of Ξ,

$$\begin{pmatrix} \tilde{u}(t) \\ \tilde{v}(t) \end{pmatrix} := \begin{pmatrix} u(t) \\ v(t) \end{pmatrix} - D\,\Xi(u(t), v(t))^{-1} \cdot \Xi(u(t), v(t)) \bmod \chi(t)^2,$$

yields $\Xi(\tilde{u}(t), \tilde{v}(t)) = 0 \bmod \chi(t)^2$. The underlying evaluations of F and of its partial derivatives at $(u(t), v(t), 1)$ modulo $\chi(t)^2$ take

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

operations in $\mathbb{K}$ by Lemma 2.3. The inverse of the determinant of $D\,\Xi(u(t), v(t))$ contributes to $\tilde{O}(\deg \chi)$. □

In Propositions 4.13 and 5.11 below we will need to reconstruct a smooth divisor from the data of its support and multiplicities. This is the purpose of the following proposition.

PROPOSITION 4.10. *Let $\mathcal{E}_1, \dots, \mathcal{E}_s$ be pairwise disjoint subsets of the smooth affine part of $\mathcal{C}$. The $\mathcal{E}_i$ can be occasionally empty, except $\mathcal{E}_s$. We assume that we are given a primitive element $\lambda = \lambda_x x + \lambda_y y$ for $\bigcup_{i=1}^{s} \mathcal{E}_i$ and we let u_i, v_i, and θ_i represent the corresponding parametrization of $\mathcal{E}_i$ over $\mathbb{K}$, for $i = 1, \dots, s$.*

Then, we can check if λ is primitive for

$$D := \sum_{i=1}^{s} i \sum_{P \in \mathcal{E}_i} P,$$

and if so compute the corresponding parametrization of D with

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

operations in $\mathbb{K}$.

Proof. Let k be an integer in the range $0, \dots, \lfloor \log_2 s \rfloor$. We proceed as follows:

1. We compute
$$\hat{\theta}_k := \prod_{i=2^k}^{\min(2^{k+1}-1, s)} \theta_i.$$
By Chinese remaindering we then compute $\hat{u}_k$ and $\hat{v}_k$ such that $\hat{u}_k \bmod \theta_i = u_i$ and $\hat{v}_k \bmod \theta_i = v_i$ for $i = 2^k, \dots, \min(2^{k+1}-1, s)$. This step takes $\tilde{O}(\deg \hat{\theta}_k + 2^k)$.
2. If $\lambda_y \frac{\partial F}{\partial x}(\hat{u}_k(t), \hat{v}_k(t), 1) - \lambda_x \frac{\partial F}{\partial y}(\hat{u}_k(t), \hat{v}_k(t), 1)$ is not coprime with $\hat{\theta}_k(t)$, then λ is not primitive for D. This test amounts to
$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg \hat{\theta}_k\Big)$$
operations in $\mathbb{K}$ by Lemma 2.3.
3. From now on we may assume that λ, $\hat{u}_k$, $\hat{v}_k$, and $\hat{\theta}_k$ represent the smooth divisor
$$\hat{D}_k := \sum_{i=2^k}^{\min(2^{k+1}-1, s)} \sum_{P \in \mathcal{E}_i} P.$$
4. We compute $2^{k+1} \hat{D}_k$ by a repeated use of Lemma 4.9 with cost
$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} 2^k \deg \hat{\theta}_k\Big).$$
Let λ, $\hat{u}_k$, $\hat{v}_k$, and $\hat{\theta}_k = \hat{\theta}_k^{2^{k+1}}$ denote the parametrization of $2^{k+1} \hat{D}_k$.
5. We compute
$$\chi_k := \prod_{i=2^k}^{\min(2^{k+1}-1, s)} \theta_i^i$$
with $\tilde{O}(\deg \chi_k + 2^k)$ operations in $\mathbb{K}$. The representation of
$$D_k := \sum_{i=2^k}^{\min(2^{k+1}-1, s)} i \sum_{P \in \mathcal{E}_i} P,$$
is λ, $\hat{u}_k \operatorname{rem} \chi_k$, $\hat{v}_k \operatorname{rem} \chi_k$ and χ_k.

Overall the computation of D_k amounts to

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1}+\delta^{\frac{\omega-1}{2}}2^k\deg\hat{\theta}_k+2^k\Big)=\tilde{O}\Big(\delta^{\frac{\omega}{2}+1}+\delta^{\frac{\omega-1}{2}}\deg D_k+2^k\Big)$$

operations in $\mathbb{K}$. Summing this bound over $k=0,\ldots,\lfloor\log_2 s\rfloor$ yields the claimed bound. □

4.4. Sum of divisors

The next operations on divisors concern the sum and the (partial) subtraction.

PROPOSITION 4.11. *Given two smooth positive divisors D_1 and D_2 parametrized by x. One can check if x is primitive for $D:=D_1+D_2$, and, if so, compute the corresponding parametrization with*

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1}+\delta^{\frac{\omega-1}{2}}(\deg D_1+\deg D_2)\Big)$$

operations in $\mathbb{K}$.

Proof. For $i=1,2$, let D_i be represented by χ_i and v_i, as in Remark 4.7. We compute

$$\hat{\chi}_1:=\gcd\left(\chi_2^{\deg\chi_1},\chi_1\right),\ \hat{v}_1:=v_1\operatorname{rem}\hat{\chi}_1,$$

that represents the largest part $\hat{D}_1$ of D_1 whose support is included in $\mathcal{V}_{\mathbb{A}}(\chi_2)$ regarded in $\mathbb{A}^2$. Similarly we compute

$$\hat{\chi}_2:=\gcd\left(\chi_1^{\deg\chi_2},\chi_2\right),\ \hat{v}_2:=v_2\operatorname{rem}\hat{\chi}_2,$$

that represents the largest part $\hat{D}_2$ of D_2 whose support is included in $\mathcal{V}_{\mathbb{A}}(\chi_1)$ regarded in $\mathbb{A}^2$. Checking that x is primitive for D then reduces to testing if

$$(\hat{v}_1-\hat{v}_2)^{\deg\hat{\chi}_1}=0\bmod\hat{\chi}_1,$$

that can be done in softly linear time via binary powering and fast gcd.

Then we further compute the parametrization of $\check{D}_i:=D_i-\hat{D}_i$ for $i=1,2$ as follows:

$$\check{\chi}_i:=\chi_i/\hat{\chi}_i,\ \check{v}_i:=v_i\operatorname{rem}\check{\chi}_i.$$

Let w_1 and w_2 be the cofactors in the Bézout relation $\gcd(\hat{\chi}_1,\hat{\chi}_2)=w_1\hat{\chi}_1+w_2\hat{\chi}_2$, then

$$\begin{aligned}\tilde{\chi}_3 &:= \operatorname{lcm}(\hat{\chi}_1,\hat{\chi}_2),\\ \tilde{v}_3 &:= \hat{v}_1w_2(\hat{\chi}_2/\gcd(\hat{\chi}_1,\hat{\chi}_2))+\hat{v}_2w_1(\hat{\chi}_1/\gcd(\hat{\chi}_1,\hat{\chi}_2))\operatorname{rem}\tilde{\chi}_3,\end{aligned}$$

is the parametrization of the divisor $\tilde{D}_3$ whose support is the common support of $\hat{D}_1$ and $\hat{D}_2$ and whose multiplicity at a point P is the maximum of the multiplicities of P in $\hat{D}_1$ and $\hat{D}_2$. The parametrization of $D_3:=\hat{D}_1+\hat{D}_2$ can be deduced from $2\tilde{D}_3$, that costs

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1}+\delta^{\frac{\omega-1}{2}}\deg\tilde{\chi}_3\Big)$$

by Lemma 4.9. Glueing $\check{D}_1+\check{D}_2+D_3$ to obtain D takes softly linear time by Chinese remaindering; see [2, Lemma 3.5] for instance. □

PROPOSITION 4.12. *Given two smooth positive divisors D_1 and D_2 parametrized by x, the parametrization of $[D_1-D_2]_+$ by x can be computed with*

$$\tilde{O}(\deg D_1+\deg D_2)$$

operations in $\mathbb{K}$.

Proof. For $i=1,2$, let D_i be represented by χ_i and v_i, as in Remark 4.7. We begin with computing

$$\hat{\chi}_2 := \gcd\left(\chi_1^{\deg\chi_2}, \chi_2\right),\ \hat{v}_2 := v_2 \operatorname{rem} \hat{\chi}_2,$$

that represents the largest part of D_2 whose support is in $\mathcal{V}_{\mathbb{A}}(\chi_1)$ regarded in $\mathbb{A}^2$. Then we compute

$$\tilde{\chi}_2(x) := \gcd\left((v_1(x)-\hat{v}_2(x))^{\deg\hat{\chi}_2}, \hat{\chi}_2(x)\right),\ \tilde{v}_2(x) := \hat{v}_2(x) \operatorname{rem} \tilde{\chi}_2(x),$$

that represents the largest part of D_2 whose support is included in the support of D_1. It follows that

$$\tilde{\chi}_1(x) := \chi_1 / \gcd(\chi_1, \tilde{\chi}_2),\ \tilde{v}_1(x) := v_1(x) \operatorname{rem} \tilde{\chi}_1(x)$$

parametrize $[D_1 - D_2]_+$ by x. □

4.5. Change of coordinates

Let D be a smooth positive divisor and let M be a 3×3 invertible matrix regarded as a change of coordinates in $\mathbb{P}^2$. We write $M(D)$ for the image of D in the new coordinates defined by M, as a divisor of the curve

$$M(C) := \left\{ M \begin{pmatrix} a \\ b \\ c \end{pmatrix} : (a:b:c) \in C \right\} = \mathcal{V}_{\mathbb{P}}(F \circ M^{-1}).$$

PROPOSITION 4.13. *Let D be a smooth positive divisor represented over $\mathbb{K}$ by λ, u, v, and χ as above, let M be a 3×3 invertible 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 $z=1$ and if $\tilde{\lambda}_x x + \tilde{\lambda}_y y$ is primitive for $M(D)$, and if so we can compute the corresponding parametrization with

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

field operations if $\mathbb{K}$ has characteristic zero or $>\deg D$, or

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

bit operations if $\mathbb{K} = \mathbb{F}_q$.

Proof. We compute the squarefree factorization of $\chi = \chi_1 \chi_2^2 \cdots \chi_n^n$, where the χ_i are pairwise coprime and squarefree, and where $\deg \chi_n \geqslant 1$ with $n \leqslant \deg D$. By Proposition 2.2, this takes $\tilde{O}(\deg D)$ field operations if $\mathbb{K}$ has characteristic 0 or $>\deg D$, or $\tilde{O}((\deg D \log q)^{1+\epsilon})$ bit operations if $\mathbb{K} = \mathbb{F}_q$.

By fast multi-remaindering [20, Chapter 10], we compute $u_i := u \operatorname{rem} \chi_i$ and $v_i := v \operatorname{rem} \chi_i$ with $\tilde{O}(\deg D)$ operations in $\mathbb{K}$. Let $\mathcal{E}_i$ stand for the set of points parametrized by λ, u_i, v_i, and χ_i, for $i=1,\ldots,n$. Following the notation of Proposition 4.5, we let $\mathcal{E}_i^{\#}$ denote the canonical image of $\mathcal{E}_i$ in $\mathbb{P}^2$, and $\tilde{\mathcal{E}}_i$ denote the affine part of $M(\mathcal{E}_i^{\#})$. From Proposition 4.5, we can check if $M(\mathcal{E}_i^{\#})$ is in the affine chart $z=1$, and test if $\tilde{\lambda} = \tilde{\lambda}_x x + \tilde{\lambda}_y y$ is primitive for $\tilde{\mathcal{E}}_i$. If so we can compute the corresponding representation $\tilde{u}_i$, $\tilde{v}_i$, and $\tilde{\chi}_i$ with $O((\deg \chi_i)^{\omega})$ field operations if $\mathbb{K}$ has characteristic zero of $>\deg \chi_i$, or $\tilde{O}((\deg \chi_i)^{\omega} \log q)$ bit operations if $\mathbb{K} = \mathbb{F}_q$.

In order to check that $\tilde{\lambda}$ is primitive for $\bigcup_{i=1}^{n} \mathcal{E}_i$, it suffices to verify that $\prod_{i=1}^{n} \tilde{\chi}_i$ is separable, that takes softly linear time. Finally we may try to reconstruct $M(D)$ via Proposition 4.10 with $\tilde{O}\Big(\delta^{\frac{\omega}{2}+1} + \delta^{\frac{\omega-1}{2}} \deg D\Big)$ further operations in $\mathbb{K}$. □

LEMMA 4.14. *Let $\mathcal{S}$ be a finite subset of $\mathbb{K}$. Let D be a smooth positive divisor, let M be a 3×3 random matrix with entries in $\mathcal{S}$. If M is invertible then the probability that $M^{-1}(D)$ is not in the affine chart $z=1$ or that x is not primitive for $M^{-1}(D)$ is*

$$\leqslant \frac{3\,(\deg D)^2}{|\mathcal{S}|}.$$

Proof. Let $P_1,\ldots,P_s$ 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

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

where $x(P_i)$ and $y(P_i)$ 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

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

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 $\mathcal{V}_{\mathbb{P}}\Big(\frac{\partial\,(F\circ M)}{\partial y}\Big)$ is $\leqslant s/|\mathcal{S}|$. □

5. INTERSECTION OF CURVES

The next ingredients necessary to turn the Brill–Noether method into practice concern algorithms to intersect curves, and to compute the singular locus of C.

5.1. Generic positions

In order to ease some computations and to benefit from fast algorithms, we often require that the coordinates are sufficiently generic. We shall begin with specifying genericities and with estimating the corresponding probability bounds.

DEFINITION 5.1. *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.*

Notice that $R(x,z)$ is 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 $z=1$. It will be convenient to apply Definition 5.1 to F and $\frac{\partial F}{\partial y}$: the coordinates will be said *generic* for $\mathcal{C}$ (or for F) when they are generic for F and $\frac{\partial F}{\partial y}$.

LEMMA 5.2. *Let $\mathcal{S}$ be a finite subset of $\mathbb{K}$. If M is a 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*

$$\leqslant \frac{2\deg F \deg G + \deg F + 3}{|\mathcal{S}|}.$$

Testing if the coordinates are generic 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 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.

We further need to ensure that $\det M \neq 0$, that yields a polynomial condition of degree 3. The bound on the probability then follows directly from the 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 $\mathbb{K}$. □

5.2. Resultant and characteristic polynomial

The following proposition is the cornerstone of the proof of the Bézout theorem presented below.

PROPOSITION 5.3. *Let $f \in \mathbb{K}[x][y]$ be monic of degree δ and let $g \in \mathbb{K}[x][y]$ be prime to f. The characteristic polynomial of the multiplication endomorphism by x in $\mathbb{K}[x,y]/(f,g)$ is a $\mathbb{K}$-multiple of the determinant of the multiplication endomorphism by g in $\mathbb{K}(x)[y]/(f)$.*

Proof. Let M denote the matrix with entries in $\mathbb{K}[x]$ of the multiplication endomorphism by g in $\mathbb{K}[x][y]/(f)$, for the canonical monomial basis. Since f is monic in y this matrix is well defined. The computation of the Smith form (see [39, Chapter III, Theorem 7.9] for instance) of M over $\mathbb{K}[x]$ yields two bases $a_1,\dots,a_\delta$ and $b_1,\dots,b_\delta$ of $\mathbb{K}[x][y]/(f)$ and monic polynomials $\chi_1,\dots,\chi_\delta$ in $\mathbb{K}[x]$ such that χ_i divides χ_{i+1} for $i=1,\dots,\delta-1$,

$$g a_i = \chi_i b_i \bmod f \text{ for } i=1,\dots,\delta,$$

and $\chi_1\cdots\chi_\delta$ is a $\mathbb{K}$-multiple of the determinant of M.

Let $n_i := \deg \chi_i$ and consider the following set of polynomials in $\mathbb{K}[x,y]$:

$$\mathcal{B} := \{x^{j-1} b_i : i=1,\dots,\delta, j=0,\dots,n_i-1\}.$$

Suppose that some $\mathbb{K}$-linear combination of the elements of $\mathcal{B}$ regarded in $\mathbb{K}[x,y]/(f,g)$ satisfies

$$r_1 b_1 + \cdots + r_\delta b_\delta \in (f,g)$$

where $r_i \in \mathbb{K}[x]$ has degree $< n_i$, for $i = 1, \ldots, \delta$. By construction there exist polynomials $q_1, \ldots, q_\delta$ in $\mathbb{K}[x]$ such that

$$r_1 b_1 + \cdots + r_\delta b_\delta + q_1 g a_1 + \cdots + q_\delta g a_\delta \in (f),$$

that rewrites into

$$(r_1 + q_1 \chi_1) b_1 + \cdots + (r_\delta + q_\delta \chi_\delta) b_\delta \in (f).$$

We deduce that $r_i + q_i \chi_i = 0$ and then that $r_i = 0$ for $i = 1, \ldots, \delta$. Consequently $\mathcal{B}$ is a free family of $\mathbb{K}[x,y]/(f,g)$.

An element in $\mathbb{K}[x,y]/(f,g)$ naturally writes as a $\mathbb{K}[x]$-linear combination of the b_i:

$$c_1 b_1 + \cdots + c_\delta b_\delta.$$

Then the Euclidean division $c_i = r_i + q_i \chi_i$ with $\deg r_i < n_i - 1$ yields

$$c_i b_i = r_i b_i + q_i b_i \chi_i = r_i b_i \bmod (f,g).$$

Consequently $\mathcal{B}$ is a generating family for $\mathbb{K}[x,y]/(f,g)$.

So far we have shown that $\mathcal{B}$ is a basis of $\mathbb{K}[x,y]/(f,g)$. The matrix of the multiplication endomorphism by x in this basis is block diagonal. The i-th block is the companion matrix of χ_i. Finally, the characteristic polynomial of x is the product of the χ_i. □

The next proposition is a local version of the previous one.

PROPOSITION 5.4. *Let $f \in \mathbb{K}[[x]][y]$ be monic of degree δ and let $g \in \mathbb{K}[[x]][y]$ be prime to f. Then the characteristic polynomial of the multiplication endomorphism by x in $\mathbb{K}[[x]][y]/(f,g)$ is a monomial whose degree equals the x-adic valuation of the determinant of the multiplication endomorphism by g in $\mathbb{K}[[x]][y]/(f)$.*

Proof. The proof is similar to the one of Proposition 5.3 by replacing $\mathbb{K}[x]$ by $\mathbb{K}[[x]]$. Both these rings are principal, so Smith forms behave similarly. However determinants of unimodular matrices over $\mathbb{K}[[x]]$ are not only invertible elements in $\mathbb{K}$ but may be any invertible series in $\mathbb{K}[[x]]$. □

5.3. Bézout's theorem

Let f and g be in $\mathbb{K}[x][y]$. Regarding $\mathrm{Res}_y(f,g)$ as the determinant of the Sylvester matrix of f and g, we have

$$\deg(\mathrm{Res}_y(f,g)) \leqslant \deg_x g \deg_y f + \deg_x f \deg_y g;$$

see [20, Theorem 6.22] for instance.

If f is monic in y, then it is well known that $\mathrm{Res}_y(f,g)$ is also the determinant of the multiplication endomorphism by g in $\mathbb{K}[x][y]/(f)$; see [6, Chapitre 6, Lemme 6.9] for instance. Then Proposition 5.3 yields $\deg I = \deg(\mathrm{Res}_y(f,g))$. Let us turn to the projective setting.

PROPOSITION 5.5. *Let F and G be homogeneous and coprime in $\mathbb{K}[x,y,z]$. If $\mathcal{U}_{\mathbb{P}}(F,G)$ is in the affine chart $z = 1$, then the ideal $(F(x,y,1), G(x,y,1))$ has degree $\deg F \deg G$.*

Proof. We may assume that $\mathbb{K}$ is algebraically closed. Up to a suitable linear change of coordinates, Lemma 5.2 allows us to assume that the coordinates are generic for F and G, so $R(x,z) := \mathrm{Res}_y(F(x,y,z), G(x,y,z))$ has degree $\deg F \deg G$ in x. From Proposition 5.3 we deduce that

$$\deg((F(x,y,1), G(x,y,1))) = \deg_x(R(x,z)) = \deg F \deg G. \qquad \square$$

The technique used here for the Bézout theorem is classical; see [18, Section 4] or [33, Section 5], for instance.

5.4. Computation of curve intersections

For computing intersections of curves, we will appeal to the following proposition, essentially based on polynomial resultants and gcds.

PROPOSITION 5.6. *Given f of total degree m and g of total degree n in $\mathbb{K}[x,y]$ such that $m \leqslant n$, such that f has degree m in y, and such that the solutions of*

$$f = g = 0$$

is a finite set $\mathcal{E}$. We can check if x is primitive for $\mathcal{E}$, and compute a partition $\mathcal{E}_1 \cup \cdots \cup \mathcal{E}_s$ of $\mathcal{E}$, where $\mathcal{E}_i$ contains points with the same intersection multiplicity m_i, with

$$\tilde{O}(n m^2 + n \deg_y g)$$

field operations in characteristic zero or $> mn$, or

$$\tilde{O}((n m^2 + n \deg_y g) \log q + (mn \log q)^{1+\epsilon})$$

bit operations if $\mathbb{K} = \mathbb{F}_q$.

Proof. The proof is revisited from the one of [2, Lemma 2.4], by taking Proposition 2.2 into account. Since $\deg_y f = \deg f$, the remainder $h := g \operatorname{rem} f$ regarded in $\mathbb{K}[x][y]$ has total degree $\leqslant n$. Therefore h can be computed with $\tilde{O}(n \deg_y g)$ operations in $\mathbb{K}$ by using fast division in $(\mathbb{K}[[x]]/(x^{n+1}))[y]$. Then, we obtain

$$\chi(x) := \mathrm{Res}_y(f(x,y), h(x,y))$$

with cost $\tilde{O}(n m^2)$ by [45, Corollary 31]. Since f has total degree m and h has total degree $\leqslant n$, it follows that χ has degree $\leqslant mn$: this can be verified by expanding the determinant of the Sylvester matrix of f and h.

The squarefree factorization $\chi =: \theta_1^{m_1} \cdots \theta_s^{m_s}$, with the θ_i squarefree and pairwise coprime, contributes to $\tilde{O}(mn)$ field operations in characteristic zero or $> mn$, or to $\tilde{O}(mn \log^{1+\epsilon} q)$ bit operations if $\mathbb{K} = \mathbb{F}_q$, by Proposition 2.2.

Then we use fast multi-remaindering to reduce f and h by $\theta_1, \ldots, \theta_s$ simultaneously [20, Chapter 10], with $\tilde{O}(n m^2)$ field operations. For now, assume that θ_i is irreducible and let ζ stand for a root of θ_i. We compute polynomials $q_i \in \mathbb{K}[x,y]$ with $\deg_x q_i < \deg \theta_i$ such that

$$q_i(\zeta, y) = \gcd(f(\zeta, y), h(\zeta, y)). \tag{5.1}$$

Then we further compute the separable factorization of q_i, with $\tilde{O}(m \deg \theta_i)$ operations in $\mathbb{K}$. If q_i is not a power of a degree 1 polynomial then x is not primitive and the algorithm raises an error. From now on let us further assume that q_i is a power of a degree 1 polynomial.

In characteristic zero, the separable factorization of q_i writes

$$q_i(\zeta, y) = (y - v_i(\zeta))^{e_i}$$

with $\deg v_i < \deg \theta_i$. In positive characteristic p, the separable factorization of q_i writes

$$q_i(\zeta, y) = \left(y^{p^{t_i}} - w_i(\zeta)\right)^{e_i}$$

with $\deg w_i < \deg \theta_i$ and e_i prime to p. By Lemma 4.4 computing the p^{t_i}-th root $v_i(\zeta)$ of $w_i(\zeta)$ takes time

$$(O((\deg \theta_i \log q)^{1+\epsilon}) + \tilde{O}(\deg \theta_i \log q \log m)) \log m$$

by taking $p^{t_i} \leqslant m$ into account.

In general we cannot assume that θ_i is irreducible, but we may appeal to the directed evaluation paradigm [31], that only involves a logarithmic overhead factor in complexities. This also yields an occasional decomposition $\theta_i =: \theta_{i,1} \cdots \theta_{i,s_i}$, and polynomials $v_{i,1}, \ldots, v_{i,s_i}$ such that $\deg v_{i,j} < \deg \theta_{i,j}$ for $j = 1, \ldots, s_i$: the only solution point of $f = h = 0$ with abscissa a root ζ of $\theta_{j,i}$ is $v_{i,j}(\zeta)$. Consequently the requested representation

$$\theta_i(x) = y - v_i(x) = 0$$

of $\mathcal{E}_i$ is deduced in softly linear time by Chinese remaindering via [2, Lemma 3.5], that contributes to $\tilde{O}(n\,m)$ further operations in $\mathbb{K}$. Finally, by Proposition 5.3, $\chi(x)$ is the characteristic polynomial of the multiplication by x in

$$\mathbb{K}[x, y] / (f(x, y), g(x, y)).$$ □

5.5. Adjoint divisor

If $a \in \mathbb{K}[[x, y]]$ is a bivariate power series, then its *initial form*, written $\mathrm{in}(a)$, is the homogeneous component of a of lowest degree. By convention we set $\mathrm{in}(0) := 0$.

We continue this section with the computation of the singular locus of $\mathcal{C}$ and the representation of the adjoint divisor $\mathcal{A}$ of $\mathcal{C}$. For completeness we begin with the following elementary result.

LEMMA 5.7. *At an m-ordinary singularity P of $\mathcal{C}$ the multiplicity of the ideal $\left(F, \frac{\partial F}{\partial y}\right)$ at P is $m(m-1)$.*

Proof. Without loss of generality we may assume that P is the origin and that the coordinates are sufficiently generic. In particular, from (3.2) that defines the φ_i as the local expansions of $\mathcal{C}$ at P, we obtain

$$\frac{\partial F}{\partial y}(x, \varphi_i, 1) \;=\; u(x, \varphi_i) \prod_{j \neq i} (\varphi_i - \varphi_j),$$

with $u(x, \varphi_i)$ invertible in $\mathbb{K}[[x]]$. Then Proposition 5.4 implies

$$\begin{aligned} \dim\left(\mathbb{K}[[x, y]] / \left(F(x, y, 1), \frac{\partial F}{\partial y}(x, y, 1)\right)\right) &= \mathrm{val}_x\left(\mathrm{Res}_y\left(\prod_{i=1}^{m} (y - \varphi_i(x)), \frac{\partial F}{\partial y}(x, y, 1)\right)\right) \\ &= \mathrm{val}_x\left(\prod_{i=1}^{m} \frac{\partial F}{\partial y}(x, \varphi_i, 1)\right) \\ &= m(m-1), \end{aligned}$$

whence the claimed intersection multiplicity. □

Given $\mathcal{C}$ with generic coordinates and such that x is primitive for $\mathcal{U}_{\mathbb{A}}\Big(F, \frac{\partial F}{\partial y}\Big)$, we wish to verify that $\mathcal{C}$ has only ordinary singularities, and if so, compute a univariate representation of the singular locus of $\mathcal{C}$.

LEMMA 5.8. *Let $\mathcal{S}$ be a finite subset of $\mathbb{K}$. With probability $\geqslant 1-4\,\delta^4/|\mathcal{S}|$ a matrix M taken with random entries in $\mathcal{S}$ is invertible and satisfies the following properties:*

- *The coordinates are generic for $F\circ M$,*
- *x is primitive for $\mathcal{E}_M := \mathcal{U}_{\mathbb{A}}\Big((F\circ M)(x,y,1), \frac{\partial\,(F\circ M)}{\partial y}(x,y,1)\Big)$.*

Proof. By the Bézout bound of Proposition 5.5 applied to $F=\frac{\partial F}{\partial y}=0$, we have

$$|\mathcal{E}_M| \leqslant \delta\,(\delta-1).$$

By Lemma 5.2 the coordinates are not generic for $F\circ M$ and $\frac{\partial\,(F\circ M)}{\partial y}$ with probability $\leqslant (2\,\delta\,(\delta-1)+\delta+3)/|\mathcal{S}|$. By Lemma 4.1, x is not primitive for the common roots of the latter polynomials with probability $\leqslant \frac{1}{2}\delta\,(\delta-1)\,(\delta\,(\delta-1)-1)/|\mathcal{S}|$. □

PROPOSITION 5.9. *Given F satisfying $\mathcal{C}$-H_1, we can check if*

- *the coordinates are generic for F,*
- *x is primitive for $\bar{\mathcal{E}} := \mathcal{U}_{\mathbb{A}}\Big(F(x,y,1), \frac{\partial F}{\partial y}(x,y,1)\Big)$,*
- *$\mathcal{C}$-H_2 holds,*

and, if so, compute a partition of the singular locus $\mathcal{E}$ of $\mathcal{C}$ into $\mathcal{E}_2,\dots,\mathcal{E}_\delta$, where $\mathcal{E}_i$ is the subset of points of multiplicity i and is parametrized by $\mu_i(x)=0$ and $y=v_i(x)$ for $i=2,\dots,\delta$, with $\tilde{O}(\delta^3)$ field operations in characteristic zero or $>\delta\,(\delta-1)$, or

$$\tilde{O}(\delta^3\log q + (\delta^2\log q)^{1+\epsilon})$$

bit operations if $\mathbb{K}=\mathbb{F}_q$.

Proof. Via Proposition 5.6, we may verify that the coordinates are generic for F and that x is primitive for $\bar{\mathcal{E}}$, and, if so, we compute a partition of $\bar{\mathcal{E}}$ into $\bar{\mathcal{E}}_1\cup\cdots\cup\bar{\mathcal{E}}_s$, where each $\bar{\mathcal{E}}_i$ is represented by $\bar{\mu}_i(x)=0$, $y=\bar{v}_i(x)$ for $i=1,\dots,s$ and such that the points in $\bar{\mathcal{E}}_i$ share the same intersection multiplicity l_i. By Proposition 5.6, this intersection costs $\tilde{O}(\delta^3)$ field operations in characteristic zero or $>\delta\,(\delta-1)$, or

$$\tilde{O}(\delta^3\log q + (\delta^2\log q)^{1+\epsilon})$$

bit operations if $\mathbb{K}=\mathbb{F}_q$. Note that

$$\sum_{i=1}^{s} l_i \deg\bar{\mu}_i = \delta\,(\delta-1) = O(\delta^2) \tag{5.2}$$

by combining Propositions 2.6 and 5.5.

Then, we compute $\bar{\mu} := \bar{\mu}_1\cdots\bar{\mu}_s$, and by fast Chinese remaindering [20, Chapter 10] we obtain $\bar{v}$ of degree $<\deg\bar{\mu}$ such that $\bar{v} \bmod \bar{\mu}_i = \bar{v}_i$ for $i=1,\dots,s$. In this way, $\bar{\mu}(x)=0$ and $y=\bar{v}(x)$ form a univariate representation of $\bar{\mathcal{E}}$ by x.

Then, we evaluate $a(x) := \frac{\partial F}{\partial x}(x, \bar{v}(x), 1) \bmod \bar{\mu}(x)$ with $\tilde{O}\left(\delta^{\frac{\omega+3}{2}}\right)$ operations in $\mathbb{K}$ by Lemma 2.3. With $\mu := \gcd(\bar{\mu}, a)$, the parametrization

$$\mu_i := \gcd(\bar{\mu}_i, \mu) = 0,\ y = v_i := \bar{v}_i \bmod \mu_i$$

represents the points of

$$\mathcal{E}_i := \bar{\mathcal{E}}_i \cap \mathcal{U}_{\mathbb{A}}\left(\frac{\partial F}{\partial x}(x, y, 1)\right).$$

Discarding the occasional empty $\mathcal{E}_i$, the sets $\mathcal{E}_1, \ldots, \mathcal{E}_s$ form a partition of the singular locus $\mathcal{E}$ of $\mathcal{C}$. The computation of the μ_i and the v_i can be done with $\tilde{O}(\delta^2)$ operations in $\mathbb{K}$ as follows: we compute the $\mu \bmod \bar{\mu}_i$ simultaneously and then use $\mu_i := \gcd(\bar{\mu}_i, \mu \bmod \bar{\mu}_i)$; see [20, Chapter 10] for instance.

If l_i does not write into the form $m_i(m_i - 1)$, then we know from Lemma 5.7 that the points of $\mathcal{E}_i$ are not ordinary. So, from now on, we assume that the m_i are known and satisfy $l_i = m_i(m_i - 1)$ for $i = 1, \ldots, s$. In this case, a singular point of multiplicity l_i in

$$\left(F(x, y, 1), \frac{\partial F}{\partial y}(x, y, 1)\right)$$

is ordinary if, and only if, the initial form of the local expansion of F is squarefree of degree m_i at all point of $\mathcal{E}_i$. In order to apply this criteria, we begin with computing $F(x, y, 1) \bmod \mu_i^{m_i+1}(x)$ simultaneously for $i = 1, \ldots, s$ with cost

$$\tilde{O}\left(\delta \sum_{i=1}^{s} m_i \deg \mu_i\right) = \tilde{O}(\delta^3),$$

thanks to (5.2). Then, obtaining

$$f_i(x, y) := F(x, y, 1) \bmod \mu_i^{m_i+1}(x) \bmod (y - v_i(x))^{m_i+1},$$

for $i = 1, \ldots, s$, also takes

$$\tilde{O}\left(\delta \sum_{i=1}^{s} m_i \deg \mu_i\right) = \tilde{O}(\delta^3)$$

operations in $\mathbb{K}$. For $i = 1, \ldots, s$ we set $\mathbb{K}[\alpha_i] := \mathbb{K}[s_i] / (\mu_i(s_i))$ and we regard f_i in

$$\mathbb{E}_i := \mathbb{K}[\alpha_i][[x - \alpha_i, y - v_i(\alpha_i)]] / ((x - \alpha_i)^{m_i+1}, (y - v_i(\alpha_i))^{m_i+1}).$$

The conversions of all the f_i take softly linear time via fast univariate polynomial shift and Proposition 2.4.

Then we compute the initial form $\mathrm{in}(f_i)$ of f_i via directed evaluation [31] over $\mathbb{E}_i$ with total cost

$$\tilde{O}\left(\sum_{i=1}^{s} m_i^2 \deg \mu_i\right) = \tilde{O}(\delta^2).$$

If the coefficients of f_i are zero up to total degree m_i then $\mathcal{C}$-H_2 is not satisfied. Otherwise $\mathrm{in}(f_i)$ has degree m_i. If $\mathrm{in}(f_i)$ is not squarefree then $\mathcal{C}$-H_2 is not satisfied. Thanks to Assumption $\mathbb{K}$-H, the polynomial $\mathrm{in}(f_i)$ is squarefree if, and only if, $\mathrm{in}(f_i)(1, y)$ has degree $m_i - 1$ or m_i and is separable. Doing so for $i = 1, \ldots, s$ allows us to check for $\mathcal{C}$-H_2. Using (5.2), the total cost amounts to $\tilde{O}(\sum_{i=1}^{s} m_i^2 \deg \mu_i) = O(\delta^2)$.

Note that directed evaluation occasionally causes a finer partition of the singular locus because factorizations of the μ_i might be discovered. Consequently, we obtain a new sequence $\mu_1, \dots, \mu_s$ along with the corresponding $v_1, \dots, v_s$, that describe the finer partition of $\mathcal{E}$ into $\mathcal{E}_1 \cup \cdots \cup \mathcal{E}_s$ where $\mathcal{E}_i$ is parametrized by $\mu_i(x) = 0$ and $y = v_i(x)$, and such that $\mathrm{in}(F(x,y,1))$ is squarefree of degree m_i in the neighborhood of all points of $\mathcal{E}_i$. We complete the algorithm by performing Chinese remaindering in order to recombine the parametrizations of the singular points that share the same multiplicity m_i. □

DEFINITION 5.10. *Following Proposition 5.9, given F satisfying C-H_1 and C-H_2, and such that*

- *the coordinates are generic for F,*
- *x is primitive for the singular locus $\mathcal{E}$ of F.*

The adjoint divisor $\mathcal{A}$ of C will be denoted by the sequence of parametrizations $y = v_m^{\mathcal{A}}(x) \bmod \mu_m^{\mathcal{A}}(x)$ representing the singular points $\mathcal{E}_m$ of C of multiplicity m, for $m = 2, \dots, \delta$.

For the complexity estimates below, we will need the following bound deduced from (5.2):

$$\deg \mathcal{A} = \sum_{m=2}^{\delta} m\,(m-1) \deg \mu_m^{\mathcal{A}} \leqslant \delta\,(\delta-1) = O(\delta^2). \tag{5.3}$$

5.6. Residual divisor

Following Algorithm 3.1, once a common denominator H of $\mathcal{L}(D)$ of degree d has been obtained, we need to compute the divisor $\mathrm{Div}(H)$. In fact we will show that H can be chosen such that $R := \mathrm{Div}(H) - \mathcal{A}$ is smooth, so we can actually compute a parametrization of R with the representation defined in Section 4. The method is summarized in the following algorithm, that takes care of checking if the coordinates are sufficiently generic and if R is actually smooth.

Algorithm 5.1

Input. $F \in \mathbb{K}[x,y,z]$, the adjoint divisor $\mathcal{A}$ of C, and a homogeneous polynomial H of degree $d \geqslant 0$.

Output. $\mathrm{Div}(H) - \mathcal{A}$ if the coordinates are generic for F and H, if $\mathrm{Div}(H) - \mathcal{A}$ is smooth, and if x is primitive for $\mathrm{Div}(H) - \mathcal{A}$. An error is raised otherwise.

Assumptions.

- C-H_1, C-H_2, and $\mathcal{A}$ is represented as in Definition 5.10,
- $\deg_y H < \delta$ and $\mathrm{Div}(H) \geqslant \mathcal{A}$.

1. Compute the solutions of $F = H = 0$ via Proposition 5.6. If the coordinates are not generic for F and H or if x is not primitive for $\mathcal{U}_{\mathbb{A}}(F(x,y,1), H(x,y,1))$ then raise an error to notify that the coordinates are not sufficiently generic.
   Write $\mu_i^H(x) = 0$ and $y = v_i^H(x)$ for the parametrization of the solutions of intersection multiplicity i, for $i = 1, \dots, d\,\delta$.
2. For $m = 2, \dots, \delta$ do:
   a. If $\mu_m^{\mathcal{A}}$ does not divide $\mu_{m(m-1)}^H$ then raise an error to notify that $\mathrm{Div}(H) - \mathcal{A}$ is not smooth.
   b. Replace $\mu_{m(m-1)}^H$ by $\mu_{m(m-1)}^H / \mu_m^{\mathcal{A}}$ and $v_{m(m-1)}^H$ by $v_{m(m-1)}^H \bmod (\mu_{m(m-1)}^H / \mu_m^{\mathcal{A}})$.

3. Apply Proposition 4.10 to the sets $\mathcal{E}_i^H$ parametrized by v_i^H and μ_i^H for $i=1,\dots,d\,\delta$, in order to recover the parametrization of $\mathrm{Div}(H)-\mathcal{A}$. Raise an error if x is not primitive for $\mathrm{Div}(H)-\mathcal{A}$.
4. Return the parametrization of $\mathrm{Div}(H)-\mathcal{A}$.

PROPOSITION 5.11. *Algorithm 5.1 is correct and takes*

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

operations in $\mathbb{K}$ in characteristic zero or $>d\,\delta$, or

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1}\log q+(d\,\delta^2\log q)^{1+\epsilon}\Big)$$

bit operations if $\mathbb{K}=\mathbb{F}_q$.

Proof. Let P be a singular point of C with multiplicity m. As in the proof of Lemma 5.7, and for sufficiently generic coordinates, since $\mathrm{Div}(H)\geqslant\mathcal{A}$, we obtain

$$\begin{aligned}\dim(\mathbb{K}[x,y]_P/(F(x,y,1),H(x,y,1))) &= \mathrm{val}_x(\mathrm{Res}_y(F(x,y,1),H(x,y,1)))\\ &= \mathrm{val}_x\left(\prod_{i=1}^{m}H(x,\varphi_i,1)\right)\\ &\geqslant m\,(m-1).\end{aligned}$$

Consequently $\mathrm{Div}(H)-\mathcal{A}$ is smooth if, and only if, the intersection multiplicity of (F,H) at every singular point P of C of multiplicity m is exactly $m\,(m-1)$.

Let us decompose $R:=\mathrm{Div}(H)-\mathcal{A}=R_1+\cdots+R_{d\delta}$, where R_i is supported by the points of multiplicity i in (F,H), while noting that $\deg R\leqslant\deg(\mathrm{Div}(H))=d\,\delta$. The role of step 2 is to verify that $\mathrm{Div}_P(H)=\mathcal{A}_P$ holds at all singular points P, and to compute parametrizations of the supports of the R_i. We are done with the correctness of the algorithm.

From Proposition 5.6, step 1 costs

$$\tilde{O}(d\,\delta^2)$$

field operations in characteristic zero or $>d\,\delta$, or

$$\tilde{O}((d\,\delta^2\log q)^{1+\epsilon})$$

bit operations if $\mathbb{K}=\mathbb{F}_q$. Step 2 takes $\tilde{O}(\max(d,\delta)\,\delta)$ operations in $\mathbb{K}$ in view of (5.3). By Proposition 4.10, step 3 contributes to

$$\tilde{O}\Big(\delta^{\frac{\omega}{2}+1}+d\,\delta^{\frac{\omega+1}{2}}\Big).$$ □

6. COMMON DENOMINATORS

Let us now turn to step 2 of Algorithm 3.1, that computes a common denominator, written H in the sequel, for all the elements of the requested Riemann–Roch space $\mathcal{L}(D)$. This section is dedicated to the choice of this common denominator H, still under the assumptions of Section 1.2. This choice is mostly driven by complexity purposes. It involves two types of requirements.

First, we require that the residual divisor $\mathrm{Div}(H) - \mathcal{A}$ is smooth in order to benefit from the algorithm of Section 5.6. And of course we would like H to have the smallest possible total degree. This problem is addressed in the first subsection.

The second type of requirements concerns *ad hoc* properties that H must satisfy after a random linear change of coordinates with high probability. These properties allow us to benefit from specific fast sub-algorithms, that finally lead to the complexity bound (1.1) which depends softly linearly in $\deg D_+$; see the algorithm in Section 7.3. Since we will require $\deg_y H < \delta$ to hold, such a change of coordinates introduces the following technical issue: the property $\deg_y H < \delta$ is not preserved under a generic change of coordinates whenever $d \geqslant \delta$.

6.1. Degree bound

The next two results provide a degree bound for H. In the vein of the first Bertini theorem, for an input smooth divisor D, we will show how to find H of relatively sharp degree such that $\mathrm{Div}(H) \geqslant D_+ + \mathcal{A}$ and $\mathrm{Div}(H) - \mathcal{A}$ is smooth with high probability. For the sake of generality, note that D does not need to be smooth in Proposition 6.2 below.

LEMMA 6.1. *Assume that the coordinates are generic for F. Let L be a homogeneous degree one polynomial such that $\mathcal{V}_{\mathbb{P}}(L,F)$ is in the affine chart $z=1$ and is disjoint of the singular locus of $\mathcal{C}$. Then, for any positive integer d, any non-zero element of $\mathcal{L}(d\,\mathrm{Div}(L) - \mathcal{A})$ has a rational function representation in the form H/L^d, where H is a homogeneous polynomial of degree d.*

Proof. We set $D := d\,\mathrm{Div}(L) - \mathcal{A}$. If $\mathcal{L}(D) \neq \{0\}$ we consider $A/B \neq 0$ in $\mathcal{L}(D)$. By construction we have

$$\tilde{D} := D + \mathrm{Div}(A) - \mathrm{Div}(B) \geqslant 0.$$

We apply Theorem 3.7 to $\tilde{D}$ 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

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

Consequently, we have

$$\mathrm{Div}(H/L^d) = \tilde{D} - D = \mathrm{Div}(A/B).$$

Then $\mathrm{Div}((H/L^d)/(A/B))$ is zero, whence $(H/L^d)/(A/B)$ is a constant, by Proposition 3.3. Finally, we have shown that A/B writes as a $\mathbb{K}$-multiple of H/L^d in $\mathbb{K}(\mathcal{C})$. □

With the notation of Definition 5.10, the genus g of $\mathcal{C}$ is

$$g = \frac{(\delta-1)(\delta-2)}{2} - \sum_{m=2}^{\delta} \frac{m(m-1)}{2} \deg \mu_m^{\mathcal{A}} = \frac{(\delta-1)(\delta-2) - \deg \mathcal{A}}{2}.$$

PROPOSITION 6.2. *Assume that $|\mathbb{K}|$ is infinite. Let D be a positive divisor of $\mathcal{C}$, and let*

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

Then, there exists a homogeneous polynomial H 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 of degree 1 such that $\mathrm{Div}(L)$ is smooth. By the Bézout theorem (Proposition 5.5) we have $\deg(\mathrm{Div}(L)) = \delta$. We set

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

The assumption on d ensures that

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

Let $P_1, \ldots, P_r$ denote the singular points of $\mathcal{C}$ and let $\mathcal{P}_{i,1}, \ldots, \mathcal{P}_{i,m_i}$ be the places above P_i. Following the discussion in Section 3.7, we may apply [19, Chapter 8, Corollary 3]: we fit in a situation where the Riemann–Roch theorem is an equality, that is

$$\forall 1 \leqslant i \leqslant r,\ \forall 1 \leqslant j \leqslant m_i, \quad \mathcal{L}(d\,\mathrm{Div}(L) - E - \mathcal{P}_{i,j}) = \mathcal{L}(d\,\mathrm{Div}(L) - E) - 1.$$

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 $\mathcal{L}(d\,\mathrm{Div}(L) - E - \mathcal{P}_{i,j})$ and this for any pair (i, j).

From Lemma 6.1 such a function h admits a rational function representation of the form $h = H / L^d$. It remains to notice that $\mathrm{Div}(H) - D - \mathcal{A} = \mathrm{Div}(h) + d\,\mathrm{Div}(L) - E$ is smooth. □

We do not claim that the degree bound of Proposition 6.2 is optimal, even in worst cases, but it is sufficient for our complexity bounds. In fact, experimentally this bound turned out to be suboptimal for a few examples that we examined.

6.2. Ad hoc coordinates

Until the end of the paper, for a given input divisor D, we set

$$d := \left\lceil \frac{(\delta-1)\,(\delta-2) + \deg D_+}{\delta} \right\rceil, \tag{6.1}$$

for the degree of the common denominator H of $\mathcal{L}(D)$ to be computed. This value for d is the smallest one that allows us to apply Proposition 6.2, hence to guarantee that such a denominator does exist. Note that

$$d\,\delta \leqslant (\delta-1)\,(\delta-2) + \deg D_+ + \delta - 1 \leqslant \delta^2 - 2\,(\delta-1) + \deg D_+ \leqslant \delta^2 + \deg D_+. \tag{6.2}$$

As said, *ad hoc* requirements on a common denominator H of $\mathcal{L}(D)$ are essential for efficiency reasons. In [2], our approach was to perform a new change of variables each time we fell into a non-generic situation and to provide bounds on the expected number of such changes of variables. For practical efficiency reasons, here we show that a single change of coordinates from the outset is sufficient for our Brill–Noether variant with high probability.

The key idea to study how changes of coordinates act on the space of the possible denominators of $\mathcal{L}(D)$ is to introduce the following auxiliary $\mathbb{K}$-vector space of polynomials that are precisely not reduced by F with respect to y:

$$\mathfrak{H} := \{H \in \mathbb{K}[x,y,z] : H \text{ homogeneous},\ \deg H = d,\ \mathrm{Div}(H) \geqslant D_+ + \mathcal{A}\} \cup \{0\}.$$

Let $\mathfrak{h}_1, \ldots, \mathfrak{h}_n$ stand for a basis of $\mathfrak{H}$, and let $\alpha_1, \ldots, \alpha_n$ be new indeterminates. We shall first state the *ad hoc* properties for $\mathfrak{h}_\alpha := \alpha_1 \mathfrak{h}_1 + \cdots + \alpha_n \mathfrak{h}_n$, and shall then show how they are preserved under changes of bases of $\mathfrak{H}$. Note that a change of coordinates in F and D is straightforwardly reflected in the same change of coordinates for the elements of $\mathfrak{H}$.

LEMMA 6.3. *Let $\mathcal{E}$ denote the singular locus of $\mathcal{C}$ and let $\mathcal{D}_-$ denote the support of D_-. Assume that the coordinates are generic for F, and that the following properties hold:*

$\mathfrak{h}_\alpha$-P_1. *The coordinates are generic for F and $\mathfrak{h}_\alpha := \alpha_1\mathfrak{h}_1 + \cdots + \alpha_n\mathfrak{h}_n$ over $\overline{\mathbb{K}(\alpha_1,\ldots,\alpha_n)}$,*

$\mathfrak{h}_\alpha$-P_2. *x is primitive for $\mathcal{D}_- \cup \mathcal{U}_{\mathbb{A}}(F(x,y,1), \mathfrak{h}_\alpha(x,y,1))$,*

$\mathfrak{h}_\alpha$-P_3. *$\mathcal{U}_{\mathbb{P}}(F,\mathfrak{h}_\alpha) \setminus \mathcal{E}$ is disjoint of $\mathcal{U}_{\mathbb{P}}\left(\frac{\partial F}{\partial y}\right)$.*

Let $\mathfrak{g}_1,\ldots,\mathfrak{g}_n$ be another basis of $\mathfrak{H}$ and let $\beta_1,\ldots,\beta_n$ be new indeterminates. Then, properties $\mathfrak{h}_\alpha$-P_1, $\mathfrak{h}_\alpha$-P_2, and $\mathfrak{h}_\alpha$-P_3 are satisfied for $\mathfrak{g}_\beta := \beta_1\mathfrak{g}_1 + \cdots + \beta_n\mathfrak{g}_n$ instead of $\mathfrak{h}_\alpha$.

Proof. There exists an invertible $n \times n$ matrix A over $\mathbb{K}$ such that

$$(\mathfrak{g}_1,\ldots,\mathfrak{g}_n) = (\mathfrak{h}_1,\ldots,\mathfrak{h}_n)\,A.$$

It follows that

$$\mathfrak{g}_\beta = (\mathfrak{h}_1,\ldots,\mathfrak{h}_n)\,A\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}.$$

Therefore $\mathbb{K}(\beta_1,\ldots,\beta_n)[x,y,z]/(F,\mathfrak{g}_\beta)$ is isomorphic to $\mathbb{K}(\alpha_1,\ldots,\alpha_n)[x,y,z]/(F,\mathfrak{h}_\alpha)$ via

$$\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix} \longmapsto A^{-1}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}.$$

Thanks to this isomorphism, the stated assumptions on $\mathfrak{h}_\alpha$ are transferred onto $\mathfrak{g}_\beta$. □

The property $\mathfrak{h}_\alpha$-P_1 ensures that the common zeros of F and $\mathfrak{h}_\alpha$ are in the affine space $z=1$. The properties $\mathfrak{h}_\alpha$-P_2 and $\mathfrak{h}_\alpha$-P_3 will contribute to allow us to parametrize the divisor $\mathrm{Div}(\mathfrak{h}_\alpha) - \mathcal{A} + D_-$ by x. The next lemma shows that these three properties can be achieved after a random linear change of coordinates with high probability.

LEMMA 6.4. *Let $\mathcal{E}$ denote the singular locus of $\mathcal{C}$, let $\mathcal{D}_-$ denote the support of D_-, and let $\mathcal{S}$ be a finite subset of $\mathbb{K}$. Let M be a 3×3 matrix with random entries in $\mathcal{S}$. If the coordinates are generic for $F\circ M$, then properties $\mathfrak{h}_\alpha$-P_1, $\mathfrak{h}_\alpha$-P_2, and $\mathfrak{h}_\alpha$-P_3 of Lemma 6.3 do not hold for $F\circ M$ and $\mathfrak{h}_\alpha \circ M$ instead of F and $\mathfrak{h}_\alpha$ with probability*

$$\leqslant \frac{9\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|},$$

whenever $\deg D_- \leqslant \deg D_+$.

Proof. By Lemma 5.2, the probability that the coordinates are not generic for $F\circ M$ and $\mathfrak{h}_\alpha \circ M$ regarded over $\mathbb{K}(\alpha_1,\ldots,\alpha_n)$ is

$$\leqslant \frac{2\,\delta d + \delta + 3}{|\mathcal{S}|} \leqslant \frac{6\,(\delta^2 + \deg D_+)}{|\mathcal{S}|},$$

by using (6.2).

By Lemma 4.1, the probability that x is not primitive for $M^{-1}(\mathcal{D}_-) \cup \mathcal{U}_{\mathbb{A}}((F\circ M)(x,y,1), (\mathfrak{h}_\alpha \circ M)(x,y,1))$ is

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

by using (6.2) again.

Let $(M_{i,j})_{1\leqslant i,j\leqslant 3}$ represent the entries of M. Then, for any point P we verify that:

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

By the Schwartz–Zippel lemma, the probability that $\mathcal{V}_{\mathbb{P}}(F\circ M, \mathfrak{h}_\alpha\circ M)\setminus M^{-1}(\mathcal{E})$ intersects $\mathcal{V}_{\mathbb{P}}\Big(\frac{\partial\,(F\circ M)}{\partial y}\Big)$ is therefore

$$\leqslant \frac{d\,\delta}{|\mathcal{S}|} \leqslant \frac{\delta^2+\deg D_+}{|\mathcal{S}|}. \qquad \square$$

6.3. Reduced denominators

In the rest of this section it remains to study how the results of the preceding subsection apply to the following sub-space $\mathfrak{H}_{<\delta}$ of $\mathfrak{H}$ made of "reduced" denominators, that means after division by F in $\mathbb{K}[x][y]$ (it is well defined because F is monic in y):

$$\mathfrak{H}_{<\delta} := \{H\in\mathfrak{H} : \deg_y H < \delta\}.$$

So we need to show that properties $\mathfrak{h}_\alpha$-P$_1$, $\mathfrak{h}_\alpha$-P$_2$, and $\mathfrak{h}_\alpha$-P$_3$ of Lemma 6.3 induce similar properties for $\mathfrak{H}_{<\delta}$.

LEMMA 6.5. *Let $\mathcal{E}$ denote the singular locus of $\mathcal{C}$, and let $\mathcal{D}_-$ denote the support of D_-. Assume that the coordinates are generic for F, and that properties $\mathfrak{h}_\alpha$-P$_1$, $\mathfrak{h}_\alpha$-P$_2$, and $\mathfrak{h}_\alpha$-P$_3$ of Lemma 6.3 hold. Let $H_1,\ldots,H_h$ be a basis of $\mathfrak{H}_{<\delta}$, and let $\gamma_1,\ldots,\gamma_h$ be new indeterminates. Then, the following properties hold:*

H_γ-P$_1$. *The coordinates are generic for F and $H_\gamma := \gamma_1 H_1 + \cdots + \gamma_h H_h$ over $\overline{\mathbb{K}(\gamma_1,\ldots,\gamma_h)}$,*

H_γ-P$_2$. *x is primitive for $\mathcal{D}_-\cup\mathcal{V}_{\mathbb{A}}(F(x,y,1),H_\gamma(x,y,1))$,*

H_γ-P$_3$. *$\mathcal{V}_{\mathbb{P}}(F,H_\gamma)\setminus\mathcal{E}$ is disjoint of $\mathcal{V}_{\mathbb{P}}\Big(\frac{\partial F}{\partial y}\Big)$.*

Proof. Thanks to Lemma 6.3, without loss of generality, we may consider another basis of $\mathfrak{H}$ from the outset such that

$$H_i = \mathfrak{h}_i \operatorname{rem}_y F, \text{ for } i=1,\ldots,h,$$

where rem_y denotes the remainder with respect to y. There exists a $h\times(n-h)$ matrix A over $\mathbb{K}$ such that

$$(\mathfrak{h}_{h+1}\operatorname{rem}_y F,\ldots,\mathfrak{h}_n\operatorname{rem}_y F) = (H_1,\ldots,H_h)\,A.$$

Then we have

$$(\mathfrak{h}_1\operatorname{rem}_y F,\ldots,\mathfrak{h}_n\operatorname{rem}_y F) = (H_1,\ldots,H_h)\,(\ \mathrm{Id}_h\ \ A\ ),$$

whence

$$\mathfrak{h}_\alpha\operatorname{rem}_y F = (H_1,\ldots,H_h)\,(\ \mathrm{Id}_h\ \ A\ )\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}.$$

We introduce the following linear forms in the α_i:

$$\begin{pmatrix}\Gamma_1\\ \vdots\\ \Gamma_h\end{pmatrix} := (\ \mathrm{Id}_h\ \ A\ )\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}.$$

In particular, all points P of $\mathcal{C}$ satisfy

$$(\Gamma_1 H_1 + \cdots + \Gamma_h H_h)(P) = (\alpha_1 \mathfrak{h}_1 + \cdots + \alpha_n \mathfrak{h}_n)(P). \tag{6.3}$$

Since F is monic in y, the resultant

$$R(x) := \mathrm{Res}_y(F(x,y,1), \mathfrak{h}_\alpha(x,y,1))$$

satisfies

$$\begin{aligned} R(x) &= \mathrm{Res}_y(F(x,y,1), \mathfrak{h}_\alpha(x,y,1) \operatorname{rem}_y F(x,y,1)) \\ &= \mathrm{Res}_y(F(x,y,1), \Gamma_1 H_1 + \cdots + \Gamma_h H_h). \end{aligned}$$

It follows that R belongs to $\mathbb{K}(\Gamma_1, \ldots, \Gamma_h)[x]$. On the other hand $\mathbb{K}(\Gamma_1, \ldots, \Gamma_h)$ is isomorphic to $\mathbb{K}(\gamma_1, \ldots, \gamma_h)$. Consequently $\mathfrak{h}_\alpha$-P$_1$ implies H_γ-P$_1$. Any irreducible factor R_i of R also belongs to $\mathbb{K}(\Gamma_1, \ldots, \Gamma_h)[x]$.

In positive characteristic p, for any irreducible factor R_i of R, the assumption $\mathfrak{h}_\alpha$-P$_2$ implies the existence of a polynomial v_i and integers t_i and e_i such that

$$\left(y^{p^{t_i}} - v_i(x)\right)^{e_i} = \gcd\left(F(x,y,1), \mathfrak{h}_\alpha(x,y,1)\right) \bmod R_i(x),$$

with $e_i \bmod p \neq 0$ and $\deg v_i < \deg R_i$. In the simpler case $p = 0$, we discard the latter exponent p^{t_i}. Therefore

$$\left(y^{p^{t_i}} - v_i(x)\right)^{e_i} = \gcd\left(F(x,y,1), \Gamma_1 H_1 + \cdots + \Gamma_h H_h\right) \bmod R_i(x),$$

is defined over $\mathbb{K}(\Gamma_1, \ldots, \Gamma_h)$. It follows that x is primitive for $\mathcal{U}_{\mathbb{A}}(F(x,y,1), H_\gamma(x,y,1))$.

From (6.3) a point $P \in \mathcal{D}_-$ belongs to $\mathcal{U}_{\mathbb{A}}(F(x,y,1), \mathfrak{h}_\alpha(x,y,1))$ if, and only if, it belongs to $\mathcal{U}_{\mathbb{A}}(F(x,y,1), H_\gamma(x,y,1))$. Let $P_1, \ldots, P_s$ denote the points of $\mathcal{D}_-$ that do not belong to $\mathcal{U}_{\mathbb{A}}(F(x,y,1), \mathfrak{h}_\alpha(x,y,1))$, we have that

$$\prod_{i=1}^{s} R(x(P_i)) \neq 0.$$

This concludes the proof of H_γ-P$_2$. If $P \in \mathcal{U}_{\mathbb{P}}\left(F, \frac{\partial F}{\partial y}\right) \setminus \mathcal{E}$ then $\mathfrak{h}_\alpha$-P$_3$ implies $\mathfrak{h}_\alpha(P) \neq 0$, so equality (6.3) yields $H_\gamma(P) \neq 0$, whence H_γ-P$_3$. □

In order to conclude this section, it remains to bound the probability that a random element of $\mathfrak{H}_{<\delta}$ satisfies the required properties. Recall that d has been defined in (6.1).

LEMMA 6.6. *Let $\mathcal{E}$ denote the singular locus of $\mathcal{C}$, let $\mathcal{D}_-$ denote the support of D_-, and let $H_1, \ldots, H_h$ be a basis of $\mathfrak{H}_{<\delta}$. Assume that the coordinates are generic for F, that $\deg D_- \leqslant \deg D_+$, and that properties H_γ-P$_1$, H_γ-P$_2$, and H_γ-P$_3$ of Lemma 6.5 hold.*

If $a_1, \ldots, a_h$ are random elements in $\mathcal{S}$, then with probability

$$\geqslant 1 - \frac{8\,\delta\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|}$$

the following properties hold:

- *the coordinates are generic for F and $H_a := a_1 H_1 + \cdots + a_h H_h$,*
- *x is primitive for $\mathcal{D}_- \cup \mathcal{U}_{\mathbb{A}}(F(x,y,1), H_a(x,y,1))$,*
- *$\mathcal{U}_{\mathbb{P}}(F, H_a) \setminus \mathcal{E}$ is disjoint of $\mathcal{U}_{\mathbb{P}}\left(\frac{\partial F}{\partial y}\right)$.*

Proof. Again, we consider the resultant

$$R(x) := \mathrm{Res}_y(F(x,y,1), (\gamma_1 H_1 + \cdots + \gamma_h H_h)(x,y,1)).$$

Its total degree in the γ_i is $\leqslant \delta$. In positive characteristic p, up to p-th root extractions, the irreducible factorization of R writes

$$R(x) = \rho \prod_{i=1}^{s} R_i(x^{q_i})^{m_i},$$

where

- the q_i are powers of p, and p does not divide the m_i,
- $\rho \in \mathbb{K}[\gamma_1, \ldots, \gamma_h]$ is the content of R, regarded in $\mathbb{K}[\gamma_1, \ldots, \gamma_h][x]$,
- $R_i(x^{q_i})$ and $R_j(x^{q_j})$ are coprime whenever $i \neq j$,
- R_i is separable, irreducible, primitive, and of positive degree, regarded in $\mathbb{K}[\gamma_1, \ldots, \gamma_h][x]$.

In characteristic zero, the situation is the same but with all the q_i set to 1. The assumption H_γ-P$_1$ implies that $\deg_x R = d\,\delta$ and, combined with H_γ-P$_2$, that there exists $w_i \in \mathbb{K}(\gamma_1, \ldots, \gamma_h)[x]$ such that

$$\left(y^{p^{t_i}} - w_i(x)\right)^{e_i} = \gcd\left(F(x,y,1), (\gamma_1 H_1 + \cdots + \gamma_h H_h)(x,y,1)\right) \bmod R_i(x), \tag{6.4}$$

with p prime to e_i. In the simpler case $p = 0$, we discard the latter exponent p^{t_i}.

We are to analyze the probability that an evaluation of $(\gamma_1, \ldots, \gamma_h)$ at a random point $(a_1, \ldots, a_h)$ commutes with the gcd of (6.4). But first we need to make sure that the factorization of R into the R_i remains well defined after this evaluation. For this purpose we introduce the following polynomial that belongs to $\mathbb{K}[\gamma_1, \ldots, \gamma_h]$:

$$\mathscr{R} := \rho \prod_{i=1}^{s} \mathrm{Res}(R_i(x^{q_i}), R(x)/R_i(x^{q_i})) \prod_{i=1}^{s} \mathrm{Res}(R_i, R_i').$$

By construction it is non-zero and we have

$$\deg \mathscr{R} \leqslant \delta + \sum_{i=1}^{s} \delta \deg R + \sum_{i=1}^{s} \delta\,(2 \deg R_i - 1) \leqslant 3 d^2 \delta^3.$$

Let $R_{|a}$ denote the specialization of R at $\gamma_1 = a_1, \ldots, \gamma_h = a_h$. If $\mathscr{R}(a_1, \ldots, a_h) \neq 0$ then $\deg R_{|a} = d\,\delta$ holds and the above factorization of $R(x)$ yields a separable decomposition of $R_{|a}$ into the specialized polynomials $R_{i|a}$, that are not necessarily irreducible.

Then, we express the gcd (6.4) as the non-zero subresultant polynomial of lowest degree, and invoke the specialization property of subresultants; see [20, Chapter 6] or [45] for instance, where subresultants are expressed in terms of determinants. Precisely let G_i denote the subresultant polynomial of degree $p^{t_i} e_i$ in y of $F(x,y,1)$ and $(\gamma_1 H_1 + \cdots + \gamma_h H_h)(x,y,1)$. It belongs to $\mathbb{K}[\gamma_1, \ldots, \gamma_h][x,y]$ and we have

$$G_i = \gcd\left(F(x,y,1), (\gamma_1 H_1 + \cdots + \gamma_h H_h)(x,y,1)\right) \bmod R_i(x).$$

Then, the specialization $G_{i|a}$ coincides with the subresultant polynomial of F and H_a of degree $p^{t_i} e_i$ in y. Let $g_i \in \mathbb{K}[\gamma_1, \ldots, \gamma_h][x]$ denote the coefficient of $y^{p^{t_i} e_i}$ in G_i and set

$$\mathscr{G}_1 := \prod_{i=1}^{s} \mathrm{Res}_x(g_i(x), R_i(x^{q_i})) \in \mathbb{K}[\gamma_1, \ldots, \gamma_h],$$

that is non-zero by construction. From $\deg_{\gamma_1,\dots,\gamma_h} G_i \leqslant \delta$ and $\deg_x g_i \leqslant 2d\delta$, we deduce that

$$\deg \mathcal{G}_1 \leqslant \sum_{i=1}^{s} (\delta \deg_x(R_i(x^{q_i})) + \delta \deg_x g_i) \leqslant d\delta^2 + d\delta^2(2d\delta) \leqslant 3d^2\delta^3.$$

If $\mathcal{G}_1(a_1,\dots,a_h) \neq 0$ then $G_{i|a} \bmod R_{i|a}$ is the gcd of F and H_a modulo any irreducible factor of $R_{i|a}$.

So far we have shown that $(\mathcal{R}\mathcal{G}_1)(a_1,\dots,a_h) \neq 0$ is sufficient to ensure that the coordinates are generic for F and H_a and that x is primitive for the corresponding intersection points.

From H_γ-P$_2$ we already know that x is primitive for $\mathcal{D}_-$. A point P in the support of $\mathcal{D}_-$ that cancels H_γ also cancels H_a. Let $P_1,\dots,P_s$ denote the points of $\mathcal{D}_-$ that do not belong to $\mathcal{U}_{\mathbb{A}}(F(x,y,1),H_\gamma(x,y,1))$. The assumption H_γ-P$_2$ further implies that

$$\mathcal{G}_2 := \prod_{i=1}^{s} R(x(P_i)) \in \mathbb{K}[\gamma_1,\dots,\gamma_h]$$

is a non-zero polynomial of total degree $\leqslant \delta \deg D_-$. If $(\mathcal{R}\mathcal{G}_1\mathcal{G}_2)(a_1,\dots,a_h) \neq 0$, then x is primitive for $\mathcal{D}_- \cup \mathcal{U}_{\mathbb{A}}(F(x,y,1),H_a(x,y,1))$.

By H_γ-P$_3$, the polynomial

$$\mathcal{H}(\gamma_1,\dots,\gamma_h) := \prod_{P \in \mathcal{U}_{\mathbb{P}}\left(F,\frac{\partial F}{\partial y}\right) \setminus \mathcal{U}_{\mathbb{P}}\left(\frac{\partial F}{\partial x}\right)} (\gamma_1 H_1 + \cdots + \gamma_h H_h)(P)$$

is not identically zero and has degree $\leqslant \delta(\delta-1)$. If $\mathcal{H}(a_1,\dots,a_h) \neq 0$ then $\mathcal{U}_{\mathbb{A}}(F(x,y,1), H_a(x,y,1))$ is disjoint of $\mathcal{U}_{\mathbb{P}}\left(F,\frac{\partial F}{\partial y}\right) \setminus \mathcal{U}_{\mathbb{P}}\left(\frac{\partial F}{\partial x}\right)$.

The probability bound thus follows from the Schwartz–Zippel lemma: H_a does not satisfy the properties with probability

$$\leqslant \frac{6d^2\delta^3 + \delta^2 + \delta \deg D_-}{|\mathcal{S}|} \leqslant \frac{8\delta(\delta^2 + \deg D_+)^2}{|\mathcal{S}|},$$

by using (6.2). □

7. COMPUTATION OF RIEMANN–ROCH SPACES

We are now ready to detail our algorithm adapted from the Brill–Noether method. The adjoint divisor $\mathcal{A}$ of $\mathcal{C}$ is represented as in Definition 5.10.

7.1. Rewriting the adjoint condition

The following proposition expresses the adjoint condition through more convenient valuative criteria, that will allow us to benefit from a fast structured linear algebra algorithm within Lemma 7.4 below.

PROPOSITION 7.1. *Assume that the coordinates are generic for F. Let H be homogeneous in $\mathbb{K}[x,y,z]$, let $P = (P_x : P_y : 1)$ be a singular point of multiplicity $m \geqslant 2$ on $\mathcal{C}$, and let $\mathcal{S} \subseteq \mathbb{K}$ be of cardinality $m-1$. Then, the following assertions are equivalent:*

i. $\mathrm{Div}_P(H) \geqslant \mathcal{A}_P$;

ii. $\mathrm{val}_{x-P_x,y-P_y}(H(x,y,1)) \geqslant m-1$;

iii. $\forall a \in \mathcal{S}$, $H(x, P_y + a\,x) = 0 \bmod (x-P_x)^{m-1}$.

Proof. Without loss of generality we may assume that $P=(0:0:1)$. The germs of curves of F at P are written $\varphi_1=a_1x+O(x^2),\dots,\varphi_m=a_mx+O(x^2)$. Since P is ordinary, the a_i are pairwise distinct.

Suppose that (i) holds, that is

$$\mathrm{val}_x(H(x,\varphi_i(x),1))\geqslant m-1 \text{ for } i=1,\dots,m. \tag{7.1}$$

Let us decompose $H(x,y,1)$ into the sum of its homogeneous components

$$H(x,y,1)=\sum_{j\geqslant 0} h_j(x,y),$$

where each h_j is homogeneous of degree j. If $m=2$, condition (7.1) implies that

$$H(x,\varphi_i(x),1)=h_0(1,a_i)+h_1(1,a_i)\,x+O(x^2),$$

whence $h_0=0$. For any $m\geqslant 2$ assume by induction that $h_0=\cdots=h_{j-1}=0$ for $j\leqslant m-2$. Then,

$$H(x,\varphi_i(x),1)=h_j(1,a_i)\,x^j+O(x^{j+1}),$$

so $h_j(1,a_i)=0$ for $i=1,\dots,m-1$, and therefore $h_j=0$. Assertion (ii) thus holds.

In order to prove that (iii) implies (ii), we verify that

$$H(x,a\,x,1)=\sum_{j\geqslant 0} h_j(1,a)\,x^j,$$

and conclude that $h_j=0$ for $j=0,\dots,m-2$. Finally we note that (ii) straightforwardly implies (i) and (iii). □

Instead of power series, we rephrase the adjoint condition in a way that avoids manipulating algebraic extensions of $\mathbb{K}$. For this purpose we fix a subset $\{a_1,\dots,a_{\delta-1}\}$ of $\mathbb{K}$, we keep the notation as in Definition 5.10 and make use of the isomorphism of Section 2.4:

$$\Gamma_m:\quad \mathbb{K}[x]/(\mu_m^{\mathcal{A}}(x))^{m-1}\ \cong\ (\mathbb{K}[z]/\mu_m^{\mathcal{A}}(z))[[x-z]]/(x-z)^{m-1}.$$

For $m\geqslant 2$ and $i=1,\dots,m-1$, we let

$$v_{m,i}^{\mathcal{A}}(x):=\Gamma_m^{-1}(v_m^{\mathcal{A}}(z)+a_i\,(x-z)).$$

The $\mu_i^{\mathcal{A}}$ being pairwise coprime, Chinese remaindering allows us to define and compute

$$\chi_i^{\mathcal{A}}:=(\mu_{i+1}^{\mathcal{A}})^i\cdots(\mu_\delta^{\mathcal{A}})^{\delta-1},\ y=w_i^{\mathcal{A}} \bmod \chi_i^{\mathcal{A}}$$

such that $w_i^{\mathcal{A}}=v_{m,i}^{\mathcal{A}} \bmod (\mu_m^{\mathcal{A}})^{m-1}$ for $m=i+1,\dots,\delta$.

PROPOSITION 7.2. *With the above notation, for a homogeneous polynomial H in $\mathbb{K}[x,y,z]$, the property* $\mathrm{Div}(H)\geqslant\mathcal{A}$ *is equivalent to*

$$H(x,w_i^{\mathcal{A}}(x),1)=0 \bmod \chi_i^{\mathcal{A}},\ \textit{for } i=1,\dots,\delta-1. \tag{7.2}$$

Proof. The property (7.2) is equivalent to

$$H(x,v_{m,i}^{\mathcal{A}}(x),1)=0 \bmod (\mu_m^{\mathcal{A}}(x))^{m-1},\ \text{for } i=1,\dots,\delta-1 \text{ and } m=i+1,\dots,\delta,$$

that rewrites via Γ_m to

$$H(x,v_m^{\mathcal{A}}(z)+a_i\,(x-z),1)=0 \bmod (x-z)^{m-1} \bmod \mu_m^{\mathcal{A}}(z),$$

for $m=2,\dots,\delta$ and $i=1,\dots,m-1$. The conclusion follows from part (iii) of Proposition 7.1. □

Proposition 7.1 previously occurred in [40, Section 2.3, Lemme b] and [19, Proposition 3]. However the adjoint condition given in Proposition 7.2 seems to be new and will be important for complexity purposes. Finally, using (5.3), we verify that

$$\begin{aligned}\sum_{i=1}^{\delta-1} \deg \chi_i^{\mathcal{A}} &= \sum_{i=1}^{\delta-1} \sum_{m=i+1}^{\delta} (m-1)\deg \mu_m^{\mathcal{A}} \\ &= \sum_{m=2}^{\delta} \sum_{i=1}^{m-1} (m-1)\deg \mu_m^{\mathcal{A}} \\ &= \sum_{m=2}^{\delta} (m-1)^2 \deg \mu_m^{\mathcal{A}} \leqslant \deg \mathcal{A} = O(\delta^2). \end{aligned} \tag{7.3}$$

LEMMA 7.3. *Assume $|\mathbb{K}| \geqslant \delta-1$. Given $\mathcal{A}$ as in Definition 5.10, we may compute the above polynomials $\chi_i^{\mathcal{A}}$ and $w_i^{\mathcal{A}}$ for $i=1,\dots,\delta-1$ with $\tilde{O}(\deg \mathcal{A}) = \tilde{O}(\delta^2)$ operations in $\mathbb{K}$.*

Proof. By Proposition 2.4 building each $v_{m,i}^{\mathcal{A}}$ takes $\tilde{O}((m-1)\deg \mu_m^{\mathcal{A}})$ operation in $\mathbb{K}$. The total cost for obtaining the $v_{m,i}^{\mathcal{A}}$ for $i=1,\dots,\delta-1$ and $m=i+1,\dots,\delta$ thus amounts to

$$\tilde{O}\left(\sum_{i=1}^{\delta-1} \sum_{m=i+1}^{\delta} (m-1)\deg \mu_m^{\mathcal{A}}\right) = \tilde{O}(\delta^2),$$

by using (7.3).

Then, for each $i=1,\dots,\delta-1$ the cost of Chinese remaindering to obtain $\chi_i^{\mathcal{A}}$ and $w_i^{\mathcal{A}}$ is $\tilde{O}(\deg \chi_i^{\mathcal{A}})$. The sum of the latter costs for $i=1,\dots,\delta-1$ is therefore $\tilde{O}(\deg \mathcal{A})$ by (7.3). □

7.2. Bivariate interpolation

The next lemma concerns the computation of bases of polynomials that have sufficiently large orders at a given divisor and that are adjoint to $\mathcal{C}$ as well. This is a key ingredient of our Brill–Noether variant. The constraints in terms of divisors will be expressed into vanishing conditions of bivariate polynomials, so the problem can be regarded as a bivariate interpolation. We use the notation of Section 2.7 about $\boldsymbol{s}$-shifted Popov forms.

LEMMA 7.4. *Let D be a smooth positive divisor of $\mathcal{C}$ with support in the affine chart $z=1$ and represented by $\chi^D(x)=0$ and $y=v^D(x)$. Assume that $\mathcal{A}$ is given as in Definition 5.10.*

Let $\mathcal{G}$ be the space of homogeneous polynomials G of $\mathbb{K}[x,y,z]$ such that

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

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

$$\tilde{O}(\delta^{\omega-1}(\deg D + \deg \mathcal{A}))$$

operations in $\mathbb{K}$.

Proof. We first appeal to Lemma 7.3, that involves $\tilde{O}(\deg \mathcal{A})$ operations in $\mathbb{K}$ to build polynomials $\chi_i^{\mathcal{A}}$ and $w_i^{\mathcal{A}}$ defined above for $i=1,\dots,\delta-1$. In softly linear time we then compute

$$c_j := (v^D)^j \operatorname{rem} \chi^D$$

for $j=0,\dots,\delta-1$. For $i=1,\dots,\delta-1$ we also compute $w_{i,j} := (w_i^{\mathcal{A}})^j \operatorname{rem} \chi_i^{\mathcal{A}}$ for $j=0,\dots,\delta-1$, that amounts to $\tilde{O}(\delta \deg \mathcal{A})$ from (7.3).

Then, we introduce the sub-module $\mathcal{M}$ of $\mathbb{K}[x]^\delta$ made of the vectors $(a_0,\dots,a_{\delta-1})$ that satisfy the following equations:

- $c_0 a_0 + \cdots + c_{\delta-1} a_{\delta-1} = 0 \bmod \chi^D$,
- $w_{i,0} a_0 + \cdots + w_{i,\delta-1} a_{\delta-1} = 0 \bmod \chi_i^{\mathcal{A}}$ for $i=1,\dots,\delta-1$.

Since $\mathbb{K}[x]$ is principal, $\mathcal{M}$ is free. Its rank is δ because it contains

$$(0,\dots,0,\chi^D \chi_1^{\mathcal{A}} \cdots \chi_{\delta-1}^{\mathcal{A}},0,\dots,0)$$

with $\chi^D \chi_1^{\mathcal{A}} \cdots \chi_{\delta-1}^{\mathcal{A}}$ at position i, for all $i=0,\dots,\delta-1$.

Using [48, Theorem 1.4] with the shift vector $\boldsymbol{s}$ of (2.2), $n=\delta$, and $m=\delta$: the nonsingular matrix in $\boldsymbol{s}$-Popov form whose rows are a basis of $\mathcal{M}$ can be computed with

$$\tilde{O}(\delta^{\omega-1} \deg(\chi^D \chi_1^{\mathcal{A}} \cdots \chi_{\delta-1}^{\mathcal{A}})) = \tilde{O}(\delta^{\omega-1}(\deg D + \deg \mathcal{A}))$$

operations in $\mathbb{K}$, by using (7.3) again.

Since D and $\mathcal{A}$ have disjoint support, the condition $\operatorname{Div}(G) \geqslant D + \mathcal{A}$ is equivalent to $\operatorname{Div}(G) \geqslant D$ and $\operatorname{Div}(G) \geqslant \mathcal{A}$. The former inequality corresponds to

$$G(x, v^D(x), 1) = 0 \bmod \chi^D(x),$$

and for the latter we appeal to Proposition 7.2. It follows that G belongs to $\mathcal{G}$ if, and only if, $G(x,y,1)$ belongs to $\mathcal{M}$. □

7.3. Riemann–Roch bases for sufficiently generic coordinates

We recall that D represents the input divisor, and that d, defined in (6.1), stands for the degree of the numerators and denominators of the basis of $\mathcal{L}(D)$ that we want to compute.

Once a common denominator H of degree d has been found, we compute $\operatorname{Div}(H) - D - \mathcal{A}$ as described in step 3 of Algorithm 3.1, and then we determine the space of polynomials G of the same degree d that satisfy $\operatorname{Div}(G) \geqslant \operatorname{Div}(H) - D$. Since $\operatorname{Div}(H) \geqslant D_+ + \mathcal{A}$, we are led to compute $\operatorname{Div}(H) - D_+ - \mathcal{A}$, that is positive. This yields the following algorithm dedicated to sufficiently generic coordinates.

Algorithm 7.1

Input. $F \in \mathbb{K}[x,y,z]$, the adjoint divisor $\mathcal{A}$ of $\mathcal{C}$, and a divisor D of $\mathcal{C}$.

Output. A denominator H of degree d defined in (6.1) of $\mathcal{L}(D)$ such that $\deg_y H < \delta$, and $G_1,\dots,G_l$ homogeneous of respective total degree $d_1,\dots,d_l$, of degree $<\delta$ in y, and such that

$$\frac{x^j z^{d-d_i-j} G_i}{H}$$

with $0 \leqslant j \leqslant d-d_i$ and $1 \leqslant i \leqslant l$ form a basis of $\mathcal{L}(D)$.

Assumptions.

- $\mathcal{C}$-H_1, $\mathcal{C}$-H_2, and $\mathcal{A}$ is represented as in Definition 5.10.

- D-H, the support of D is in the chart $z=1$, D is parametrized by x, and $\deg D_- \leqslant \deg D_+$.
- x is primitive for the union of the support of D and of the singular locus of $\mathcal{C}$.

1. 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 Lemma 7.4 with D_+ in order to obtain a $\mathbb{K}[x]$-module basis $h_1,\dots,h_\delta$ of $\mathcal{H}(x,y,1)$.
2. 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.
3. Let $\mathcal{E}$ denote the singular locus of $\mathcal{C}$. Call Algorithm 5.1 with H. If the algorithm raises an error notifying that the coordinates are not generic for F and H, or that x is not primitive for $\mathcal{V}_{\mathbb{A}}(F(x,y,1), H(x,y,1))$, or that $\mathcal{V}_{\mathbb{A}}(F(x,y,1), H(x,y,1)) \setminus \mathcal{E}$ intersects $\mathcal{V}_{\mathbb{A}}\Big(\frac{\partial F}{\partial y}(x,y,1)\Big)$ then raise an error. If Algorithm 5.1 raises an error to notify that $\mathrm{Div}(H) - \mathcal{A}$ is not smooth then go to step 2. Otherwise, Algorithm 5.1 actually returns $R := \mathrm{Div}(H) - \mathcal{A}$ parametrized by x.
4. Compute $R - D_+$ parametrized by x via Proposition 4.12.
5. If x is not primitive for $R - D = (R - D_+) + D_-$ then raise an error. Otherwise compute the univariate parametrization of $R - D$ in terms of x via Proposition 4.11.
6. Let $\mathcal{G}$ denote the space of homogeneous polynomials G of $\mathbb{K}[x,y,z]$ such that $\deg_y G < \delta$ and $\mathrm{Div}(G) \geqslant R - D + \mathcal{A}$. Compute a basis $g_1,\dots,g_\delta$ of the $\mathbb{K}[x]$-module $\mathcal{G}(x,y,1)$ by means of Lemma 7.4 called with $R - D$. Sort the g_i by increasing total degrees and let l be maximal such that $\deg g_l \leqslant d$.
7. Return H and $G_1 := z^{\deg g_1} g_1(x/z, y/z), \dots, G_l := z^{\deg g_l} g_l(x/z, y/z)$.

PROPOSITION 7.5. *Assume that $|\mathbb{K}| \geqslant 2\,\delta^3$. Algorithm 7.1 is correct and takes an expected number of*

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

operations in $\mathbb{K}$ in characteristic 0 or $> \delta d$, or an expected number of

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

bit operations when $\mathbb{K} = \mathbb{F}_q$.

Let $\mathcal{S}$ be a finite subset of $\mathbb{K}$ and assume that the $(a_i)_{1\leqslant i\leqslant \delta}$ in step 2 are taken with random coefficients in $\mathcal{S}$. If the hypotheses of Lemma 6.6 are satisfied, then the probability that Algorithm 7.1 raises an error is

$$\leqslant \frac{8\,\delta\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|}.$$

Proof. Proposition 2.9 ensures that the polynomials H built in step 2 are random elements of degree d in $\mathcal{H}$. And according to Theorem 3.8, the output of the algorithm is correct whenever the algorithm finishes normally.

Let us analyze the expected number of times the algorithm returns to step 2. If $|\mathbb{K}|$ is infinite then Proposition 6.2 already ensures the existence of a polynomial H such that $\mathrm{Div}_P(H) = \mathcal{A}_P$ for all singular point P of $\mathcal{C}$, so the algorithm finishes. Let us regard the coefficients of the polynomials $a_1,\dots,a_\delta$ as variables, written $a_{i,j}$ for short, and let

$$R := \mathrm{Res}_y(F(x,y,1), H(x,y,1)) \in \mathbb{K}[a_{i,j}][x],$$

The total degree of R in the $a_{i,j}$ is $\leqslant\delta$ and the degree in x is $d\,\delta$. Since $\mathrm{Div}(H)\geqslant\mathcal{A}$ the following division is exact:

$$S := R \Big/ \prod_{m=2}^{\delta} (\mu_m^{\mathcal{A}})^{m(m-1)} \in \mathbb{K}[a_{i,j}][x].$$

Let

$$\rho := \mathrm{Res}_x(\mu_2^{\mathcal{A}} \cdots \mu_\delta^{\mathcal{A}}, S) \in \mathbb{K}[a_{i,j}],$$

from (5.3) it has degree $\leqslant\delta \deg \mathcal{A} \leqslant \delta^3$, and it is not the zero polynomial by Proposition 6.2 used over $\bar{\mathbb{K}}$. Step 3 returns to step 2 if, and only if ρ vanishes at the actual values of the $a_{i,j}$. Consequently the Schwartz–Zippel lemma implies that the probability to return to step 2 is $\leqslant\delta^3/|\mathcal{S}|\leqslant 1/2$. In other words, the expected number of times the algorithm returns to step 2 is $O(1)$.

Let us now turn to the probability of failure of the algorithm. If the hypotheses of Lemma 6.6 are satisfied, then the algorithm returns a correct result. The claimed probability bound thus corresponds directly to the one of Lemma 6.6.

Concerning the cost of the algorithm, step 1 takes

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

operations in $\mathbb{K}$ by Lemma 7.4. Step 2 takes negligible time. By Proposition 5.11, step 3 costs

$$\tilde{O}\left(\delta^{\frac{\omega}{2}+1} + d\,\delta^2\right) = \tilde{O}(\delta^3 + \delta \deg D_+)$$

operations in $\mathbb{K}$ in characteristic zero or $>d\,\delta$, or

$$\tilde{O}(((\delta^3 + \delta \deg D_+)\log q)^{1+\epsilon})$$

bit operations if $\mathbb{K} = \mathbb{F}_q$.

By Proposition 4.12, step 4 also takes softly linear time. By Proposition 4.11, step 5 contributes to

$$\begin{aligned} & \tilde{O}\left(\delta^{\omega+\frac{1}{2}} + \delta^{\frac{\omega-1}{2}}(\deg D_- + d\,\delta)\right) \\ = \ & \tilde{O}\left(\delta^{\omega+\frac{1}{2}} + \delta^{\frac{\omega+3}{2}} + \delta^{\frac{\omega-1}{2}} \deg D_+\right) \\ = \ & \tilde{O}(\delta^{\omega+1} + \delta^{\omega-1} \deg D_+). \end{aligned}$$

Step 6 takes

$$\tilde{O}(\delta^{\omega-1}(\deg(R-D) + \deg \mathcal{A}))$$

operations in $\mathbb{K}$ by Lemma 7.4. Then we verify that

$$\begin{aligned} \deg(R-D) + \deg \mathcal{A} & \leqslant \deg D_- + \deg \mathcal{A} + d\,\delta - \deg \mathcal{A} - \deg D_+ \\ & \leqslant \deg D_- + (\delta-1)(\delta-2) + 1 \\ & = O(\delta^2 + \deg D_+). \end{aligned}$$

The total cost is deduced as the sum of the costs of each step. □

7.4. Main algorithm

The algorithmic point of view used to solve the interpolation problem in Section 7.2 reveals that Riemann–Roch spaces are endowed with a "compressed" algebraic structure, that we make precise in the following definition.

DEFINITION 7.6. *The Riemann–Roch space of D will be represented by*

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

such that

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

Algorithm 7.1 has been designed under several genericity assumptions, all concerning coordinates. In order to achieve a complete algorithm, it suffices to apply a random change of coordinates from the outset and to appeal to the results of Section 6.2. We are now ready to present our top level algorithm.

Algorithm 7.2

Input. $F \in \mathbb{K}[x,y,z]$ homogeneous defining the curve $\mathcal{C}$, a divisor D of $\mathcal{C}$.

Output. $\mathcal{L}(D)$ represented as in Definition 7.6 if $\mathcal{C}$-H_2 holds. An error is raised if $\mathcal{C}$-H_2 does not hold.

Assumptions. $\mathcal{C}$-H_1, D-H, $\deg D_- \leqslant \deg D_+$.

1. Pick a 3×3 invertible matrix M.
2. Replace F by $F \circ M$.
3. If the coordinates are not generic for F, or if x is not primitive for the singular locus of $\mathcal{C}$ then go to step 1.
4. If $\mathcal{C}$-H_2 does not hold then raise an error. Otherwise compute the adjoint $\mathcal{A}$ of $\mathcal{C}$ as in Definition 5.10.
5. Try to compute $M^{-1}(D)$ by means of Proposition 4.13. If the support of $M^{-1}(D)$ is not in the affine chart $z = 1$, or if x is not primitive for $M^{-1}(D)$ then go to step 1. Otherwise replace D by $M^{-1}(D)$.
6. Call Algorithm 7.1 in order to obtain a common denominator H and the polynomials $G_1,\dots,G_l$. If Algorithm 7.1 raises an error then go to step 1.
7. Return M, H and $G_1,\dots,G_l$.

THEOREM 7.7. *Assume that $|\mathbb{K}| \geqslant 66\,\delta\,(\delta^2 + \deg D_+)^2$. Algorithm 7.2 is correct and takes an expected number of*

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

operations in $\mathbb{K}$ in characteristic 0 or $> \max(d\delta, \delta(\delta-1), 2\deg D_+)$, or an expected number of

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

bit operations when $\mathbb{K} = \mathbb{F}_q$.

Proof. By Lemma 5.8, step 3 returns to step 1 with probability

$$\leqslant \frac{4\,\delta^4}{|\mathcal{S}|}. \tag{7.4}$$

By Lemma 4.14, the probability that $M^{-1}(D)$ is not in the affine chart $z=1$ or that x is not primitive for $M^{-1}(D)$ is

$$\leqslant \frac{3\,(\deg D_+ + \deg D_-)^2}{|\mathcal{S}|} \leqslant \frac{12\,(\deg D_+)^2}{|\mathcal{S}|}. \tag{7.5}$$

By Lemma 6.4, after the random change of coordinates properties $\mathfrak{h}_\alpha$-P$_1$, $\mathfrak{h}_\alpha$-P$_2$, and $\mathfrak{h}_\alpha$-P$_3$ of Lemma 6.3 do not hold with probability

$$\leqslant \frac{9\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|}. \tag{7.6}$$

If these properties hold, then Lemma 6.5 implies that the assumptions of Lemma 6.6 are satisfied. Therefore Algorithm 7.1 raises an error with probability

$$\leqslant \frac{8\,\delta\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|}, \tag{7.7}$$

by Proposition 7.5. Summing bounds (7.4) to (7.7), the probability that Algorithm 7.2 returns to step 1 is

$$\leqslant \frac{33\,\delta\,(\delta^2 + \deg D_+)^2}{|\mathcal{S}|} \leqslant \frac{1}{2}.$$

Consequently, the expected number of times that Algorithm 7.2 returns to step 1 is $O(1)$.

It remains to study the complexity of the algorithm. From Lemma 2.5, step 2 incurs $\tilde{O}(\delta^2)$ operations in $\mathbb{K}$. From Proposition 5.9, we know that steps 3 and 4 cost $\tilde{O}(\delta^3)$ field operations in characteristic zero or $>\delta\,(\delta-1)$, or

$$\tilde{O}(\delta^3 \log q + \delta^2 \log^{1+\epsilon} q) = \tilde{O}(\delta^{\omega+1} \log^{1+\epsilon} q).$$

bit operations if $\mathbb{K} = \mathbb{F}_q$.

By Proposition 4.13, step 5 takes

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

field operations if $\mathbb{K}$ has characteristic zero or $>2\deg D_+$, or

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

bit operations if $\mathbb{K} = \mathbb{F}_q$.

By Proposition 7.5 step 6 takes

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

operations in $\mathbb{K}$ in characteristic 0 or $>\delta d$, or

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

bit operations if $\mathbb{K} = \mathbb{F}_q$. Then we observe that $\delta^{\omega-1} \deg D_+ \leqslant \delta^{\omega+1}$ if $\deg D_+ \leqslant \delta^2$ and

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

otherwise. The total cost of the algorithm is deduced by summing the costs of the intermediate steps. □

7.5. Case of small finite fields

If $\mathbb{K}$ is the finite field $\mathbb{F}_q$ with a cardinality not sufficiently large to apply Algorithm 7.2, then we may build an extension $\mathbb{L} := \mathbb{F}_{q^e}$ of $\mathbb{F}_q$ such that

$$q^e \geqslant 66\,\delta\,(\delta^2 + \deg D_+)^2$$

in order to compute a basis of $\mathbb{L} \otimes \mathcal{L}(D)$ by running Algorithm 7.2 over $\mathbb{L}$; see the construction in the proof of Lemma 4.4. Since

$$e = O(\log(\delta + \deg D_+))$$

the overhead in the complexity bound of Theorem 7.7 is only a logarithmic factor. It remains to explain how to recover a basis of $\mathcal{L}(D)$ over $\mathbb{K}$ from one over $\mathbb{L}$.

In general, if q is too small, a compressed representation as in Definition 7.6 is no longer possible, so we are led to represent the basis over $\mathbb{L}$ directly by homogeneous polynomials $H, G_1, \ldots, G_l$ of degree d such that $\mathcal{L}(D)$ is spanned by $G_1/H, \ldots, G_l/H$. The total size of this representation is $O(l\,d^2)$, with $l = O(d^2)$. With the value of d of (6.1), we have $e = O(\log d)$. Note that in the worst case, when F cannot be made monic in any of the variables over $\mathbb{K}$, these polynomials are not "reduced modulo F" and the size of the dense representation exceeds the complexity bound of Theorem 7.7.

To deduce a $\mathbb{K}$-basis we may use the following relative trace map on the scalars:

$$\begin{array}{rccc} \mathrm{Tr}: & \mathbb{L} \otimes \mathcal{L}(D) & \longrightarrow & \mathcal{L}(D) \\ & \sum \lambda_i \otimes f_i & \longmapsto & \sum \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\lambda_i)\, f_i\,. \end{array}$$

Precisely, for $G = \sum_{i,j} g_{i,j} x^i y^j z^{d-i-j}$ let us write $G^{(q^k)} := \sum_{i,j} g_{i,j}^{q^k} x^i y^j d^{d-i-j}$, so if

$$\frac{G}{H} \in \mathbb{L} \otimes \mathcal{L}(D),$$

then we have

$$\mathrm{Tr}\left(\frac{G}{H}\right) = \sum_{k=0}^{e-1} \frac{G^{(q^k)}}{H^{(q^k)}}.$$

Note that if $a \in \mathbb{F}_{q^e}$ is a uniformly distributed random variable then $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(a)$ is uniformly distributed in $\mathbb{F}_q$. Therefore, drawing uniformly random elements $b_1, \ldots, b_l$ in $\mathbb{L} \otimes \mathcal{L}(D)$, the probability that $\mathrm{Tr}(b_1), \ldots, \mathrm{Tr}(b_l)$ is a $\mathbb{K}$-basis of $\mathcal{L}(D)$ equals the probability that a uniformly random $l \times l$ matrix over $\mathbb{K}$ is invertible, namely

$$\frac{(q^l - 1)\,(q^l - q) \cdots (q^l - q^{l-1})}{q^{l^2}} \geqslant \frac{1}{4}.$$

This method yields an efficient probabilistic algorithm to recover a basis over $\mathbb{K}$. Checking that a candidate basis is actually free over $\mathbb{K}$ usually costs $O(d^2\, l^{\omega-1})$ operations in $\mathbb{K}$; see for instance [5, Chapter 2] or [57, Theorem 2.10]. For small values of q the latter probability is far from 1, so it is worth generating a slightly larger set of uniformly random elements $b_1, \ldots, b_{l'}$ with $l' > l$ and then extract a basis from $\mathrm{Tr}(b_1), \ldots, \mathrm{Tr}(b_{l'})$ by Gaussian elimination.

In [34, Section 3.4], Huang and Ierardi proposed another deterministic method based on linear algebra. They compute $\bar{H} := H H^{(q)} \cdots H^{(q^{e-1})}$ and $\bar{G}_i := G_i H^{(q)} \cdots H^{(q^{e-1})}$ for $i = 1, \ldots, l$ with $\tilde{O}(l d^2 \log q)$ operations in $\mathbb{F}_q$. Since $\bar{H} \in \mathbb{K}[x, y, z]$ is homogeneous of degree $\tilde{O}(d)$, it remains to find linear combinations of the $\bar{G}_i$ that belong to $\mathbb{K}[x, y, z]$, that takes $\tilde{O}(d^2 l^{\omega-1})$ operations in $\mathbb{K}$.

Remark 7.8. Our bounds on both the probability of failure and on the size of $\mathbb{K}$ have been established through loose estimates, with negligible impact on asymptotic complexity bounds. However, for implementation purposes, it would be profitable to use sharper bounds instead of unnecessary extensions of the base field.

7.6. Notes

In order to make additional connections with the existing literature, we present a different and somehow more concise proof of Lemma 6.1 using sheaf cohomology. Let us denote by $Q_1, \ldots, Q_r$ the ordinary singularities of C and define $\nu : C' \longrightarrow C$ its desingularization map. For $i = 1, \ldots, r$, we denote by $Q_{i,1}, \ldots, Q_{i,m_i}$ the points of C' lying above Q_i.

Given a divisor D of C' whose support avoids the $Q_{i,j}$, we associate canonically a Weil divisor $\nu_* D$ on C'. According to Serre [52], one can define two Riemann–Roch spaces: one for C and one for C'. The space over C', written $\mathcal{L}_{C'}(D)$, is the usual one considered previously, namely

$$\mathcal{L}_{C'}(D) := \{f \in \mathbb{K}(C') \setminus \{0\} : \forall P \in C', v_P(f) \geqslant -v_P(D)\} \cup \{0\}.$$

The other space, defined on C, called the *singular Riemann–Roch space* and written $\mathcal{L}_C(D)$, is defined as:

$$\mathcal{L}_C(D) := \{f \in \mathcal{L}_{C'}(D) : \forall i \in \{1, \ldots, r\}, f(Q_{i,1}) = \cdots = f(Q_{i,m_i})\}.$$

From an embedded point of view, according to [52, § IV.2, eq. (13)], the latter space is the subspace of $\mathcal{L}_{C'}(D)$ of functions that belong to O_{C,Q_i} for any singular point Q_i. Lemma 6.1 reformulates as follows in this setting.

LEMMA 7.9. *Let $L \subseteq \mathbb{P}^2$ be a line defined over $\mathbb{K}$ and avoiding the singular points of C. Then, for any positive integer d, any non-zero element $f \in \mathcal{L}_C(d \operatorname{Div}(L))$ has a rational function representation as*

$$f = \frac{H}{L^d}$$

where H is a homogeneous polynomial of degree d.

Proof. The space $\mathcal{L}_C(d \operatorname{Div}(L))$ is isomorphic to the global section space of the sheaf $O_C(d \operatorname{Div}(L))$. We have the sheaf short exact sequence:

$$0 \longrightarrow \mathcal{I}_{\mathbb{P}^2, C}(dL) \longrightarrow O_{\mathbb{P}^2}(dL) \longrightarrow O_C(d \operatorname{Div}(L)) \longrightarrow 0, \tag{7.8}$$

where $\mathcal{I}_{\mathbb{P}^2, C}$ is the ideal sheaf of $O_{\mathbb{P}^2}$ of germs of functions vanishing on C. Since C has codimension 1 in $\mathbb{P}^2$, we get $\mathcal{I}_{\mathbb{P}^2, C} \simeq O_{\mathbb{P}^2}(-C)$ and hence,

$$\mathcal{I}_{\mathbb{P}^2, C}(dL) = \mathcal{I}_{\mathbb{P}^2, C} \otimes O_{\mathbb{P}^2}(dL) \simeq O_{\mathbb{P}^2}(dL - C).$$

The exact sequence (7.8) yields a long exact sequence in cohomology

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^0(\mathbb{P}^2, O_{\mathbb{P}^2}(dL - C)) &\longrightarrow \mathrm{H}^0(\mathbb{P}^2, O_{\mathbb{P}^2}(dL)) \\ &\longrightarrow \mathrm{H}^0(C, O_C(d \operatorname{Div}(L))) \longrightarrow \mathrm{H}^1(\mathbb{P}^2, O_{\mathbb{P}^2}(dL - C)). \end{aligned}$$

From [27, Th. III.5.1(b)] we know that $\mathrm{H}^1(\mathbb{P}^2, O_{\mathbb{P}^2}(dL - C)) = 0$, so the map

$$\mathrm{H}^0(\mathbb{P}^2, O_{\mathbb{P}^2}(dL)) \longrightarrow \mathrm{H}^0(C, O_C(d\,\mathrm{Div}(L)))$$

is surjective. In other words, any non-zero $f \in \mathcal{L}_C(d\,\mathrm{Div}(L)) \cong \mathrm{H}^0(C, O_C(d\,\mathrm{Div}(L)))$ has a rational function representation as H/L^d. □

8. CONCLUSION

From the theoretical point of view, the smoothness hypothesis on the input divisor D is not much restrictive thanks to the well known "moving lemma". In fact, if D is not smooth then we may compute a smooth divisor $\tilde{D}$ that is linearly equivalent to D, so $\mathcal{L}(\tilde{D})$ is isomorphic to $\mathcal{L}(D)$. From a practical point of view this approach is probably not the most efficient one whenever $\deg \tilde{D}_+$ is much larger than $\deg D_+$. Consequently, it might be more natural to extend our method in order to handle non-smooth divisors in a direct manner. But at present time it is not clear how to do so while preserving the fast bivariate interpolation technique used in Section 7.2.

Another challenging research direction concerns the extension of our method to any kind of singularities with a similar complexity exponent. Currently, the assumption that C is ordinary is required for our representation of divisors using power series, for our proof of Proposition 3.5, and to achieve efficient adjoint conditions. Of course, from [40] we know that general curves can still be handled in the Brill–Noether fashion. So the actual challenge concerns complexity and not feasability.

BIBLIOGRAPHY

[1] S. Abelard. On the complexity of computing integral bases of function fields. In F. Boulier, M. England, T. M. Sadykov, and E. V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing. 22nd International Workshop, CASC 2020, Linz, Austria, September 14–18, 2020, Proceedings*, volume 12291 of *Lect. Notes Comput. Sci.*, pages 42–62. Cham, 2020. Springer International Publishing.

[2] S. Abelard, A. Couvreur, and G. Lecerf. Sub-quadratic time for Riemann–Roch spaces: case of smooth divisors over nodal plane projective curves. In A. Mantzaflaris, editor, *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, ISSAC '20, pages 14–21. New York, NY, USA, 2020. ACM.

[3] 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.

[4] J. Berthomieu, G. Lecerf, and G. Quintin. Polynomial root finding over local rings and application to error correcting codes. *Appl. Alg. Eng. Comm. Comp.*, 24(6):413–443, 2013.

[5] 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.

[6] 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, 2017. Electronic version available from `https://hal.archives-ouvertes.fr/AECF`.

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

[8] A. Bostan, G. Lecerf, and É. Schost. Tellegen's principle into practice. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ISSAC '03, pages 37–44. New York, NY, USA, 2003. ACM.

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

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

[11] A. Campillo and J. Farrán. Symbolic Hamburger–Noether expressions of plane curves and applications to AG codes. *Math. Comp.*, 71(240):1759–1780, 2002.

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

[13] G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3):380–420, 2007.

[14] J. Coates. Construction of rational functions on a curve. *Math. Proc. Camb. Philos. Soc.*, 68(1):105–123, 1970.

[15] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2nd edition, 2005.

[16] J. H. Davenport. *On the Integration of Algebraic Functions*, volume 102 of *Lect. Notes Comput. Sci.* Springer-Verlag, Berlin Heidelberg GmbH, 1981.

[17] R. Dedekind and H. Weber. Theorie der algebraischen Functionen einer Veränderlichen. *J. für die Reine und Angew. Math.*, 92:181–290, 1882.

[18] C. Durvye and G. Lecerf. A concise proof of the Kronecker polynomial system solver from scratch. *Expo. Math.*, 26(2):101–139, 2008.

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

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

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] G. Haché. *Construction Effective des Codes Géométriques*. PhD thesis, Université Paris 6, France, 1996.

[26] 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`.

[27] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate texts in mathematics*. Springer Science & Business Media, 2013.

[28] K. Hensel and G. Landsberg. *Theorie der algebraischen Funktionen einer Variablen und ihre Anwendung auf algebraische Kurven und Integrale*. Teubner, 1902.

[29] F. Hess. Computing Riemann–Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[30] 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.

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

[32] J. van der Hoeven and G. Lecerf. Fast multivariate multi-point evaluation revisited. *J. Complexity*, 56:101405, 2020.

[33] J. van der Hoeven and G. Lecerf. On the complexity exponent of polynomial system solving. *Found. Comput. Math.*, 2020. `https://doi.org/10.1007/s10208-020-09453-0`.

[34] 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.

[35] X. Huang and V. Y. Pan. Fast rectangular matrix multiplication and applications. *J. Complexity*, 14(2):257–299, 1998.

[36] K. S. Kedlaya and C. Umans. Fast polynomial factorization and modular composition. *SIAM J. Comput.*, 40(6):1767–1802, 2011.

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

[38] M. Kreuzer and L. Robbiano. *Computational Linear and Commutative Algebra*. Springer International Publishing, 2016.

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

[40] 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.

[41] F. Le Gall. Powers of tensors and fast matrix multiplication. In K. Nabeshima, editor, *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pages 296–303. New York, NY, USA, 2014. ACM.

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

[43] 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.

[44] G. Lecerf. Fast separable factorization and applications. *Appl. Algebra Engrg. Comm. Comput.*, 19(2):135–160, 2008.

[45] G. Lecerf. On the complexity of the Lickteig–Roy subresultant algorithm. *J. Symbolic Comput.*, 92:243–268, 2019.

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

[47] 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`.

[48] 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.

[49] 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.

[50] 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.

[51] D. Panario and D. Thomson. Efficient pth root computations in finite fields of characteristic p. *Des. Codes Cryptogr.*, 50(3):351–358, 2009.

[52] J.-P. Serre. *Groupes algébriques et corps de classes*. Hermann, 1959.

[53] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Math. Comp.*, 54(189):435–447, 1990.

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

[55] 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.

[56] B. Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. In S. Nigel, editor, *Advances in Cryptology – EUROCRYPT 2008. 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, pages 163–180. Springer Berlin Heidelberg, 2008.

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

[58] 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.

[59] 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.