Fast computation of Riemann–Roch spaces for singular curves

Dounia Darkaoui Martin Weimann

LMNO, Université de Caen Normandie

dounia.darkaoui@unicaen.fr
martin.weimann@unicaen.fr

April 9, 2026

Abstract

Let $\mathscr{C}$ be a projective curve defined over a field k and let D be a divisor of $\mathscr{C}$. The Riemann–Roch space $\mathscr{L}(D)$ is the set of rational functions on $\mathscr{C}$ for which certain zeros are imposed and certain poles are allowed, with some multiplicities determined by D. Riemann–Roch spaces play a fundamental role in algebraic geometry due to the central place of the Riemann–Roch theorem. They have also important applications, such as coding theory or arithmetic of Jacobians of curves. In this article, we present what we believe is the fastest algorithm to date that computes a basis of a Riemann–Roch space for a curve with arbitrary singularities. Our algorithm is deterministic, works over any perfect field k, and works with no assumptions on the support of D.

1 Introduction

Let $\mathscr{C} \subset \mathbb{P}^2_k$ be an irreducible projective plane curve over a perfect field k, with function field $L = k(\mathscr{C})$. The Riemann–Roch space attached to a divisor D on $\mathscr{C}$ is

$$\mathscr{L}(D) = \{b \in L^\times \mid \operatorname{div}(b) \geq -D\} \cup \{0\}$$

where $\operatorname{div}(b)$ stands for the principal divisor of b. In other words, the elements of $\mathscr{L}(D)$ are rational functions of $\mathscr{C}$ that are allowed to have certain poles with prescribed multiplicities and are required to have certain zeros with prescribed multiplicities. This is a k-vector space of finite dimension.

The problem of computing Riemann–Roch spaces has attracted considerable interest since the 1980s, when Goppa [22, 23, 24] designed a new family of error-correcting codes (AG codes) obtained by evaluating functions of a Riemann–Roch space $\mathscr{L}(D)$ attached to a curve over a finite field (see [46] for a state of the art). The computation of particular Riemann–Roch spaces is also a cornerstone to perform operations in the Jacobian of the curve $\mathscr{C}$ [35, 67], with various applications in number theory and algebraic geometry. Among other applications of Riemann–Roch spaces, we can mention diophantine equations [18], integration of algebraic functions [19], parametrization of rational curves [66], or factorization of bivariate polynomials [68]. Due to its omnipresence in algebraic geometry and its various applications, the problem of computing

Riemann–Roch spaces became a fundamental task of computer algebra in the last four decades, as illustrated by an extensive literature, see e.g. [39, 31, 67, 21, 3, 4, 2, 32, 58, 9, 10, 16].

For curves with nodal or ordinary singularities, there are now probabilistic algorithms of Las Vegas type with a complexity which is closed to be quasi-optimal [3, 4]. In this article, we present what we believe is the fastest algorithm to date that computes a basis of a Riemann–Roch space for a curve with arbitrary singularities (Theorem 1.1). Our algorithm is deterministic, works over any perfect field k, with no assumptions on the support of D. We essentially follow Hess's algorithm [32], based on the computation of integral bases of fractional ideals of Dedekind rings and on reduction of $k[t]$-modules. We revisit this method, by taking into account the recent developments in algorithmic of local and global fields, a cornerstone being the OM algorithm which allows to compute, represent and manipulate efficiently prime ideals of Dedekind domains [50, 27, 28, 53].

Besides complexity issues, this article has a pedagogical focus. In particular, it intends to clear up the relations between the arithmetic point of view that we adopt here (divisors seen as a $\mathbb{Z}$-combination of prime ideals of Dedekind rings) and the geometric point of view that is often used in the literature (divisors seen as a $\mathbb{Z}$-combination of points on a smooth model of a curve). Although this gymnastics is classical for experts, we hope this effort will help the non-expert reader understand the various methods of computing Riemann–Roch spaces.

Main result. We use an algebraic RAM model as in [37], counting only the number of arithmetic operations and zero tests in k. We denote $\mathscr{O}(g(n))$ and $\tilde{\mathscr{O}}(g(n))$ to respectively hide constants and logarithmic factors with respect to n. We assume that fast multiplication of polynomials is used. We denote $2 \leq \omega \leq 3$ the constant of linear algebra, so that two $n \times n$ matrices over a commutative ring can be multiplied with $\mathscr{O}(n^\omega)$ ring operations. The best current bound is $\omega < 2.37286$ in [7]. We prove:

Theorem 1.1. *There exists a deterministic algorithm that, given a projective curve $\mathscr{C} \subset \mathbb{P}^2_k$ of degree n defined by an irreducible homogeneous polynomial $F \in k[X_0, X_1, X_2]$ monic and separable in X_2, and given a divisor $D \in \mathrm{Div}(\mathscr{C})$ of non negative degree with effective part D^+, computes a compressed basis of $\mathscr{L}(D)$ with*

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \delta(\mathscr{C}) + n)) \ \subset \ \tilde{\mathscr{O}}(n^\omega(\deg(D^+) + n^2))$$

operations in k, where $\delta(\mathscr{C}) = \frac{(n-1)(n-2)}{2} - g(\mathscr{C}) \in \mathbb{N}$, with $g(\mathscr{C})$ the geometric genus of $\mathscr{C}$.

Let us explain the data involved in the theorem. The divisor is represented as a $\mathbb{Z}$-combination of places of the function field $k(\mathscr{C})$, each place being given by an OM representation of a prime ideal of a suitable Dedekind subring (Definition 3.14). A compressed basis (Definition 5.4) is a list $(b_1, d_1), \ldots, (b_n, d_n)$ with $b_i \in k(t)[x]$ and $d_i \in \mathbb{Z}$ such that the k-vector space $\mathscr{L}(D)$ has basis

$$\left\{ b_i(t,x)t^j, \ i = 1, \ldots, n, \ j = 0, \ldots, d_i \right\},$$

where $t = X_1/X_0$ and $x = X_2/X_0$ are regarded modulo F. If $D_\infty = \mathrm{div}_\infty(t)$ is the divisor at infinity, we deduce for free the compressed basis of $\mathscr{L}(D + rD_\infty)$ for any integer $r \in \mathbb{Z}$ by simply replacing the integers d_i with $d_i + r$. The cost of writting down all elements of a basis of $\mathscr{L}(D)$ is estimated in Proposition 6.5.

The nonnegative integer $\delta(\mathscr{C})$ is the so-called delta-invariant. It measures how far is $\mathscr{C}$ from being smooth: the less singularities the curve $\mathscr{C}$ has, the smaller $\delta(\mathscr{C})$ gets and the faster our algorithm works. In particular, $\delta(\mathscr{C}) = 0$ if (and only if) $\mathscr{C}$ is nonsingular. If the singular

locus and the support of D do not contain points at infinity, we get a slightly better complexity $\tilde{\mathcal{O}}(n^\omega(\deg(D^+)+\delta(\mathscr{C}))$ (Theorem 6.4).

Up to our knowledge, Theorem 1.1 improves significantly the best current bound $\tilde{\mathcal{O}}((n^2+\deg(D^+))^\omega)$ for curves with arbitrary singularities [2]. Moreover, we stress that our algorithm is deterministic, works regardless of the characteristic of the base field, and does not require D to be supported at affine smooth points of $\mathscr{C}$, in contrast to [2]. If the curve has ordinary singularities, our bound is less good by a factor n than the (probabilistic) bound obtained in [3, 4]. Thus there is still room for improvements, a key point being that we represent elements of $\mathscr{L}(D)$ as rational functions with univariate denominators in contrast to [3, 4].

A more precise statement of Theorem 1.1 is given in Theorem 5.18, with a complexity expressed in terms of finner (and possibly much smaller) invariants than $\deg(D^+)$, which reflect how far is D from being of shape $\mathrm{div}(q)+rD_\infty$ with $q\in k(t)$ and $r\in\mathbb{Z}$ (Proposition 4.16).

Remark 1.2. *The hypothesis F monic and separable with respect to X_2 is not restrictive if $\mathrm{Card}(k)>n$ (Proposition 6.10). If $\mathrm{Card}(k)\leq n$, we may have to work over a finite extension k'/k of degree $\leq\log(n)$ to reduce to the separable monic case. We compute a k'-basis of $\mathscr{L}(D)\otimes k'$ with the same complexity up to a logarithmic factor. However, recovering a k-basis of $\mathscr{L}(D)$ from a k'-basis of $\mathscr{L}(D)\otimes k'$ may involve probabilistic routines (see [4] and Section 6.4 for details).*

Main lines of the proof. As said, we mainly follow Hess's algorithm [32] (see also Bauch's thesis [9]). The function field $k(\mathscr{C})$ is isomorphic to the finite extension $L=k(t)[X]/f$ where $f=F(1,t,X)\in k[t][X]$ is separable, irreducible, monic and of degree n. We can associate to D two fractional ideals $I=I(D)$ and $I_\infty=I_\infty(D)$ of the respective integral closures of $k[t]$ and $k[1/t]_{(1/t)}$ in L. The fractional ideal I is a free $k[t]$-module of rank n which represents the affine part of the Riemann–Roch space $\mathscr{L}(D)$, while I_∞ is a free $k[1/t]_{(1/t)}$-module of rank n which represents the part at infinity. We have $\mathscr{L}(D)=I\cap I_\infty$ and we are reduced to perform the following tasks:

- Step 1. Compute a $k[t]$-basis $\mathscr{B}$ of I and a $k[1/t]_{(1/t)}$-basis $\mathscr{B}_\infty$ of I_∞.
- Step 2. Compute a basis of the k-vector space $I\cap I_\infty$.

For the first step, we use the recent fast algorithm in [54] by Poteaux and the second author, following Okutsu's framework [47]. This algorithm is based on the combination of the fast OM algorithm in [53] by the same authors (factorization of polynomials over local fields), together with the remarkable MaxMin algorithm of Stainsby [61] which computes from an OM factorization a triangular p-basis of a given fractional ideal (see Section 4.3).

Each set $\mathscr{B}$ and $\mathscr{B}_\infty$ forms a basis of the $k(t)$-vector space L, and it is shown in [32] (see also [9]) that step 2 reduces to compute a row reduced form of the transition matrix $M\in k(t)^{n\times n}$ between $\mathscr{B}$ and $\mathscr{B}_\infty$. To this aim, we use fast algorithms for multiplying, inverting and reducing polynomial matrices of [44, 64], taking care of the particular shapes of the involved bases (see Section 5).

State of the art. Classical methods for computing bases of Riemann–Roch spaces are derived from the pioneer work of Brill and Noether which dates back to the second half of the 19th century. The Brill-Noether algorithm first computes a common denominator H for all elements of $\mathscr{L}(D)$, thought as quotients of homogeneous polynomials of same degrees regarded modulo F. Writing $D=D^+-D^-$ as a difference of effective divisors with disjoint supports, Brill and Noether showed that it is sufficient to consider $\mathrm{div}_0(H)\geq D^++\mathscr{A}$ where $\mathscr{A}$ is the so-called adjoint divisor. Given such an H, computing numerators amounts to compute a basis of the set of homogeneous polynomials $G \pmod F$ such that $\mathrm{div}_0(G)\geq\mathrm{div}_0(H)-D$. We have

$\mathrm{div}_0(H) - D \geq D^- + \mathscr{A} \geq 0$. Hence in both cases, we look for *polynomials with prescribed zeros*. The Riemann–Roch theorem gives upper bounds for the degrees of the polynomials G we are looking for, and after translating each condition $v_P(G) \geq n_P$ into a system of linear equations, the algorithm is mainly reduced to linear algebra. We usually talk about geometric methods, although *linear algebra methods* also seems to be an appropriate terminology.

A first drawback of the Brill-Noether aproach is that it was originally developed for curves with nodal singularities, in which case the adjoint divisor is easy to describe. Modern algorithms with good complexities have been developed for nodal curves in [21] using fast linear algebra, and improved in [3] using structured linear algebra based on $k[t]$-modules, leading to the best currently known complexity $\tilde{\mathcal{O}}((n^2 + \deg(D^+))^{\frac{\omega+1}{2}})$ for nodal curves. This result was then generalized in [4] to curves with ordinary singularities. These algorithms are probabilistic of Las-Vegas type since they require various generic change of coordinates in order to compute a univariate representation of the involved divisors. Considering nodal curves is theoretically sufficient since any curve is birationally equivalent to a plane nodal curve (possibly after extension of the base field). However, computing a nodal model of a singular curve is difficult and expensive. Moreover, considering curves with arbitrary (non ordinary) singularities led to the discovery of new AG-codes with excellent properties [39, 65, 46]. The Brill-Noether algorithm was thus extended to curves with arbitrary singularities by various authors [39, 31, 67, 16], using blow-ups or local parametrizations of places. These methods have been recently improved in [2] under the assumption that k has characteristic zero, in which case we can use the fast algorithm [52] to represent singular places by Puiseux expansions. The algorithm of [2] is probabilistic, with complexity $\tilde{\mathcal{O}}((n^2 + \deg(D^+))^{\omega})$. Up to our knowledge, this was up to now the best complexity for curves with arbitrary singularities (assuming characteristic zero).

A second drawback of the Brill-Noether method is that it supposes usually D to be supported at smooth points. The fast algorithms [21, 3, 4, 2] assume this. This hypothesis can not be dropped by a change of variable. Although this constraint is (up to our knowledge) not an issue for applications to AG codes, computing Riemann–Roch spaces attached to singular divisors is a relevant problem since various interesting divisors of a curve are precisely supported at singular places (different or co-different divisor, adjoint divisors, canonical divisor, etc.). For example, considering the canonical divisor has applications to integration of algebraic functions [19], to parametrization of rational curves [66], to factorization of bivariate polynomials [68], or to the computation of smooth canonical models of curves, from which one can extract various birational invariants such as the Clifford index or the gonality [57].

Some alternative approaches that overcome the drawbacks of Brill-Noether algorithms have been proposed, with a more arithmetic flavour. Arithmetic methods do not require generic position (except maybe monicity and separability of the input polynomial), do not require D to be supported at regular points, and do not make assumptions on the characteristic of the base field. They use integral bases of fractional ideals in function fields, in the spirit of the works of Coates [18] and Davenport [19]. There have been several contributions in the last decades [58, 42, 9, 32], Hess's algorithm [32] being a key reference since the years 2000s, implemented in the computer algebra systems Magma [13] and Singular [62, 12]. It is shown to run in polynomial time in [32], although no complexity estimates are provided. In 2014, Bauch obtained complexity estimates in his thesis [9], but the computation of integral bases in function fields was not yet competitive with the fastest linear algebra based algorithms of Brill-Noether type. Since then, there have been significant advances regarding computational aspects of function fields (and number fields). A key tool is the OM algorithm developed in 1999 by Montes [50], following one century of work by Ore [48, 49], MacLane [41, 40] and Okutsu [47] and many others, and developed further by Nart and its collaborators [11, 25, 26, 27, 29, 28, 30, 6] in the last two decades. Starting from a complete discrete rank one valued field K, a polynomial $f \in K[x]$ and the Gauss valuation

on $K[x]$, using Newton polygons and residual polynomials, the OM algorithm builds node after node a tree of valuations whose leaves correspond to the irreducible factors of f. It returns as a byproduct some extra data that allows to represent and manipulate effectively prime ideals in Dedekind domains. A version with quasi-optimal complexity has been recently developed in [53]. Among various applications, the OM algorithm led to new algorithms to compute integral bases of fractional ideals [10, 30, 61] and the quasi-optimal complexity estimates recently obtained in [54] opened the door to make arithmetic methods competitive with geometric methods, as the present paper intends to show.

Besides integral basis computations, an other feature of Hess's algorithm (and of fast Brill-Noether algorithms [3, 4, 2]) is to use basis reduction of free $k[t]$-modules, that is reduction of polynomial matrices. This problem of computer algebra has been considerably developed in the last two decades, and there are now fast algorithms for various tasks concerning polynomial matrices (multiplication, inversion, reduction, etc), see e.g. [64, 69, 44] and references therein. Some of these results are used in the present paper, and we believe there is still room to use more refined results to improve our complexity bounds.

Organization of the paper. In Section 2, we gently introduce divisors and Riemann–Roch spaces in the language of function fields. In Section 3, we explain the relations between places and prime ideals of Dedekind rings and we define the OM representation of divisors. We also mention some other classical representations of divisors. Section 4 is dedicated to the computation of the integral bases of the fractional ideals I and I_∞ mentioned above. The complexity is naturally expressed in terms of invariants attached to I and I_∞, and then expressed in terms of D. In the key Section 5, we compute the intersection $\mathscr{L}(D) = I \cap I_\infty$, a problem closely related to inversion and reduction of polynomial matrices. We prove Theorem 1.1 in Section 6, relating the delta invariant of the projective curve $\mathscr{C}$ in terms of indices of integral closures. For the sake of completeness, we add two appendices: we first recall basic facts about integral closures (Appendix A) and then explain why places of a function field $k(\mathscr{C})$ correspond bijectively to closed points of the normalization of $\mathscr{C}$ (Appendix B).

Acknowledgments. We thank Vincent Neiger for valuable discussions about reduction of polynomial matrices.

2 Divisors and Riemann–Roch spaces

A divisor on a smooth algebraic curve defined over an algebraically closed field is usually defined as a finite formal $\mathbb{Z}$-combination of points of the curve. However, we want to consider singular curves defined over non algebraically closed fields, in which case the notion of point has to be replaced by the more subtle notion of place.

We fix k a base field, assumed to be perfect. Typically k is a finite field or a number field. Classical references for what follows are [63, 20, 56, 59].

Definition 2.1. *A function field L over k (denoted L/k) is a finitely generated extension of k of transcendence degree one. A place of L/k is the maximal ideal P of a discrete valuation ring $\mathscr{O} \subset L$ containing k. We denote by V_L the set of places of L.*

Recall that a ring $\mathscr{O} \subset L$ is a valuation ring if for all $x \in L$, we have $x \in \mathscr{O}$ or $x^{-1} \in \mathscr{O}$. It is a local ring with maximal ideal $P = \mathscr{O} \setminus \mathscr{O}^\times$. The valuation ring $\mathscr{O}$ is discrete if moreover P is principal. Since L has transcendence degree one over k, all valuation rings of L containing k are discrete valuation rings [63, Thm 1.1.6].

Definition 2.2. *Let P be a place of L, with valuation ring $\mathcal{O}_P$.*

- *The residue field of P is $k_P = \mathcal{O}_P/P$. It is a finite extension of k.*
- *The degree of P over k is* $\deg(P) = [k_P : k]$.
- *A uniformizer of P is a generator of the principal ideal P.*

Definition 2.3. *A valuation on a function field L/k is a* surjective *map $v : L \to \mathbb{Z} \cup \{\infty\}$ wich vanishes on $k^\times$ and such that for all $b, b' \in L$, we have:*

1. $v(b) = \infty \iff b = 0$,
2. $v(bb') = v(b) + v(b')$
3. $v(b + b') \geq \min(v(b), v(b'))$ *with equality if* $v(b) \neq v(b')$.

We can associate to each place a valuation. Let $P \in V_L$ with valuation ring $\mathcal{O}$ with uniformizer π. Any $b \in L^\times$ writes uniquely as

$$b = u\pi^n, \quad u \in \mathcal{O}^\times, \quad n \in \mathbb{Z}.$$

The integer n does not depend on the choice of the generator π and the map $v_P(b) = n$ defines a valuation on L. Conversely, a valuation v on L defines a valuation ring and its maximal ideal,

$$\mathcal{O} = \{b \in L \mid v(b) \geq 0\} \qquad \text{and} \qquad P = \{b \in L \mid v(b) \geq 1\}$$

and we check that $v = v_P$. To summarize, there is a one-to-one correspondence between the places of L/k, the (discrete) valuation rings of L containing k and the valuations on L/k (see [63, Thm 1.1.13] for further details).

Definition 2.4. *A divisor D of L/k is a finite formal $\mathbb{Z}$-combination of places of L/k, that is,*

$$D = \sum_{P \in V_L} n_P \cdot P, \qquad n_P \in \mathbb{Z}, \quad n_P \neq 0 \text{ for finitely many } P.$$

We say that D is effective if $n_P \geq 0$ for all P, denoted $D \geq 0$.

- *The degree of D is* $\deg(D) = \sum_P n_P \deg(P)$.
- *The support of D is* $\mathrm{Supp}(D) = \{P \in V_L \mid n_P \neq 0\}$.

Remark 2.5. *A divisor of a curve $\mathscr{C}$ defined over k is simply a divisor of the field of rational functions $k(\mathscr{C})$ of $\mathscr{C}$ (which is indeed a function field), see Section 6 for details.*

We omit the dependency in the base field k and simply denote $\mathrm{Div}(L)$ the set of divisors of L/k. This is a group, namely the free abelian group generated by the set of places of L/k. This group admits a partial ordering by letting $E \geq D$ if $E - D \geq 0$.

Definition 2.6. *Let $b \in L^\times$. We have $v_P(b) \neq 0$ for finitely many places [63, Cor. 1.3.4]. The divisor of b is*

$$\mathrm{div}(b) = \sum_{P \in V_L} v_P(b) \cdot P.$$

We say that P is a zero of b if $v_P(b) > 0$ and that P is a pole of b if $v_P(b) < 0$. A divisor of shape $\mathrm{div}(b)$ *is called a principal divisor.*

For any $b \in \mathscr{O}_P$, we can "evaluate b at P" by setting

$$b(P) = b \bmod P \ \in k_P,$$

and P is a zero of b if and only if $b(P) = 0$. If $b \notin \mathscr{O}_P$, we have $v_P(b) < 0$ and we let $b(P) = \infty$. If k is algebraically closed, then $k_P \simeq k$ for all P, and any $b \in L$ defines a function $b : V_L \to k \cup \{\infty\}$. This explains the terminology "function field".

Definition 2.7. *The Riemann–Roch space of a divisor D is:*

$$\mathscr{L}(D) = \{b \in L^\times \mid \operatorname{div}(b) + D \geq 0\} \cup \{0\}.$$

It is a k-vector space of finite dimension and $\mathscr{L}(D) = \{0\}$ if $\deg(D) < 0$ [63, Prop. 1.4.9 and Cor. 1.4.12].

We can write uniquely D as a difference of effective divisors with disjoint support, namely

$$D = D^+ - D^-, \qquad \text{where} \quad D^+ = \sum_{n_P > 0} n_P \cdot P, \quad \text{and} \quad D^- = -\sum_{n_P < 0} n_P \cdot P.$$

Likewise, for an element $b \in L^\times$, we define $\operatorname{div}_0(b) = \operatorname{div}(b)^+$ *the zero divisor* of b and $\operatorname{div}_\infty(b) = \operatorname{div}(b)^-$ *the polar divisor* of b. We thus have

$$b \in \mathscr{L}(D) \iff \operatorname{div}_\infty(b) \leq D^+ \quad \text{and} \quad \operatorname{div}_0(b) \geq D^-.$$

In other words, we look for rational functions b with at most that many poles and at least that many zeros.

We want to compute a k-basis of $\mathscr{L}(D)$. The first questions are:

- How do we represent the field L and its elements ?
- How do we represent a place $P \in V_L$?
- How do we compute the valuation $v_P(b)$ of an element $b \in L$?

There are various possible answers to these questions, which depend on how we think a place. There are usually two main points of view. The geometric point of view considers places as closed points of the desingularization of a projective plane curve $\mathscr{C}$. In this setting, places are usually represented using blow-ups [39], Puiseux expansions [2, 58] or Hamburger-Noether expansions [16]. The arithmetic point of view, that we will adopt here, considers places as prime ideals of Dedekind rings. In this setting, places can be represented by generators of the prime ideal, by OM representation, or by expansions, as we will see in the next section. We refer the reader to Annex B for the relations between these two points of view.

3 Representation of places of a function field

We let $\operatorname{Spec} R$ be the set of prime ideals of a ring R. For $p \in \operatorname{Spec} R$, we let R_p be the localization of R at p, that is by the multiplicative subset $R \setminus \{p\}$.

3.1 Places of a rational function field.

Definition 3.1. *A function field K over k is rational if $K = k(t)$ for some $t \in K$.*

Let $K = k(t)$ be a rational function field. Let $A = k[t]$ and $p \in \operatorname{Spec} A$. Since A is integrally closed of dimension one, the local ring A_p is principal and integrally closed, hence is a discrete valuation rings of K, defining a place $P = pA_p$ of K. We say that P is a finite place (with respect to the choice of t). Note that p is generated by a unique monic irreducible polynomial of $k[t]$ (abusively still denoted p) and v_P coincides with the usual p-adic valuation v_p.

There is another valuation ring in K containing k, the local ring $A_\infty = k[1/t]_{(1/t)}$, whose maximal ideal $(1/t)$ is called the place at infinity, denoted $P = \infty$. The corresponding valuation v_∞ is the minus degree valuation (take care of sign)

$$v_\infty(g/h) = -\deg(g/h) = \deg(h) - \deg(g).$$

Proposition 3.2. *[63, Thm 1.2.2] The places of K/k are exactly the places $P = pA_p$ with $p \in \operatorname{Spec} A$ and the place at infinity $P = \infty$.*

There is thus a one-to-one correspondence between places of K and $\mathscr{P}_A = \operatorname{Spec} A \cup \{\infty\}$. Moreover, given $p \in \mathscr{P}_A$, the corresponding valuation v_p is easy to describe. Note that geometrically, we may think $\mathscr{P}_A$ to be the set of closed points of the projective line $\mathbb{P}^1_k = \mathbb{A}^1_k \cup \{\infty\}$.

3.2 Places vs prime ideals of Dedekind rings.

Let L/k be an arbitrary function field. Let $t \in L$ be transcendental over k. Thus L is a finite extension of the rational function field $K = k(t)$.

Lemma 3.3. *Let P be a place of L. The restriction $P' = P \cap K$ is a place of K. We say that P lies above P'.*

Proof. Clearly $\mathscr{O}_P \cap K$ is a valuation ring of K which contains k. The maximal ideal of $\mathscr{O}_P$ is $P = \{x \in L,\ x^{-1} \notin \mathscr{O}_P\}$ and the maximal ideal P' is the set $P' = \{x \in K,\ x^{-1} \notin \mathscr{O}_P \cap K\}$, that is $P' = P \cap K$. □

Definition 3.4. *We say that a place of L is finite if it lies above a finite place of K, and is infinite if it lies over ∞ (this notion depends on the choice of t).*

Let B and B_∞ be the respective integral closures of A and A_∞ in L (Definition A.1). We denote for short

$$\mathscr{P}_0 = \operatorname{Spec} B, \quad \mathscr{P}_\infty = \operatorname{Spec} B_\infty \quad \text{and} \quad \mathscr{P} = \mathscr{P}_0 \cup \mathscr{P}_\infty.$$

We call $\mathscr{P}$ the set of primes of L/K (note that maximal ideals and non zero prime ideals coincide in our context). We say that $\mathfrak{p} \in \mathscr{P}$ divides $p \in \mathscr{P}_A$ (or lies above p) if $p = \mathfrak{p} \cap K$, denoted $\mathfrak{p}|p$.

Proposition 3.5. *Places of L/k are in one-to-one correspondence with the primes of L/K. More precisely:*

1. *The set of finite places of L is $V_L(B) = \{\mathfrak{p}B_\mathfrak{p} \mid \mathfrak{p} \in \mathscr{P}_0\}$.*
2. *The set of infinite places of L is $V_L(B_\infty) = \{\mathfrak{p}B_{\infty,\mathfrak{p}} \mid \mathfrak{p} \in \mathscr{P}_\infty\}$.*
3. *The places $P \in V_L$ lying above $pA_p \in V_K$ are one-to-one with the primes $\mathfrak{p} \in \mathscr{P}$ lying above $p \in \mathscr{P}_A$.*

Proof. The rings B and B_∞ being integrally closed, their localizations at their maximal ideals are distinct valuation rings of L, hence define distinct places of L. Conversely, if $P \in V_L$ is a finite place, then $P \cap K$ is a finite place of K by Lemma 3.3, that is $\mathscr{O}_P \cap K = A_p$ for some prime $p \in \operatorname{Spec} A$ by Proposition 3.2. Thus $\mathscr{O}_P$ contains A, hence contains B since $\mathscr{O}_P$ is integrally closed. Let $\mathfrak{p} = P \cap B$. Then $\mathfrak{p} \cap A = p$ and thus $\mathscr{O}_P$ contains $B_\mathfrak{p}$. Since a discrete valuation ring is a maximal subring of its field of fractions, we get $\mathscr{O}_P = B_\mathfrak{p}$ and $P = \mathfrak{p}B_\mathfrak{p}$. The same reasoning applies for places at infinity. □

If $P \in V_L$, we let $\mathfrak{p} \in \mathscr{P}$ be the corresponding prime, called the prime of P. Conversely, if $\mathfrak{p} \in \mathscr{P}$, we let $P \in V_L$ be the corresponding place. We have

$$P = \mathfrak{p}B_\mathfrak{p} \quad \text{and} \quad \mathfrak{p} = P \cap B$$

for finite places and primes, and similarly for the places at infinity. Recall the following fact:

Lemma 3.6. *If $\mathfrak{p}, \mathfrak{q}$ are distinct maximal ideals of an integral ring R, then $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p}\mathfrak{q}$ and $\mathfrak{q}R_\mathfrak{p} = R_\mathfrak{p}$.*

Proof. As $\mathfrak{p}, \mathfrak{q}$ are distinct maximal ideals of R, we necessarily have $\mathfrak{p} + \mathfrak{q} = R$, i.e. $\mathfrak{p}$ and $\mathfrak{q}$ are coprime. Thus intersection and product coincide. Moreover, there exists $y \in \mathfrak{q}$ such that $y \notin \mathfrak{p}$. Thus y is invertible in $R_\mathfrak{p}$ and it follows that $1 \in \mathfrak{q}R_\mathfrak{p}$, that is $\mathfrak{q}R_\mathfrak{p} = R_\mathfrak{p}$. □

The ring B is integrally closed of dimension one, hence is a Dedekind ring [8, thm 9.3]. Thus all fractional ideals of B are invertible [8, thm 9.8], the set of fractional ideals of B is the free abelian multiplicative group generated by the primes $\mathfrak{p} \in \mathscr{P}_0$ [8, Cor. 9.8], and any fractional ideal I of B admits a unique factorization [8, Cor 9.4]

$$I = \prod_{\mathfrak{p} \in \mathscr{P}_0} \mathfrak{p}^{n_\mathfrak{p}}, \qquad \text{with } n_\mathfrak{p} \in \mathbb{Z} \text{ and } n_\mathfrak{p} = 0 \text{ for almost all } \mathfrak{p}.$$

We define $v_\mathfrak{p}(I) = n_\mathfrak{p}$, with convention $v_\mathfrak{p}(0) = \infty$. This induces the $\mathfrak{p}$-adic valuation

$$v_\mathfrak{p} : L \to \mathbb{Z} \cup \{\infty\}, \quad v_\mathfrak{p}(b) = v_\mathfrak{p}(bB).$$

In the same way, B_∞ is a Dedekind ring, and we define analogously the $\mathfrak{p}$-adic valuation attached to any prime $\mathfrak{p} \in \mathscr{P}_\infty$.

Lemma 3.7. *Let $P \in V_L$ with prime $\mathfrak{p} \in \mathscr{P}$. The valuations v_P and $v_\mathfrak{p}$ coincide.*

Proof. By Lemma 3.6, $v_\mathfrak{p}(b)$ coincides with the largest integer n such that $b \in \mathfrak{p}^n$, and with the largest integer such that $b \in \mathfrak{p}^n B_\mathfrak{p}$. As $\mathfrak{p}B_\mathfrak{p} = P$, the claim follows. □

Let us conclude this section with few classical definitions and results.

Definition 3.8. *Let $\mathfrak{p} \in \mathscr{P}$ be a finite place and let $p = \mathfrak{p} \cap K$.*

- *The degree of $\mathfrak{p}$ is $\deg(\mathfrak{p}) = [B/\mathfrak{p}B : k]$.*
- *The residual degree of $\mathfrak{p}/p$ is $f_\mathfrak{p} = [B/\mathfrak{p}B : A/pA]$.*
- *The index of ramification of $\mathfrak{p}/p$ is $e_\mathfrak{p} = v_\mathfrak{p}(p)$.*

We extend trivially this definition for places at infinity, replacing A, B by A_∞, B_∞. Note that in such a case, $p = \infty$ and $A_\infty/pA_\infty = k$. Thus, degree and residual degree coincide. If p is finite, we identify p with its unique monic generator $p \in A = k[t]$.

Proposition 3.9. *Let P be a finite place of L with prime $\mathfrak{p}$ lying above $p \in \operatorname{Spec} A$. We have*

$$\deg(P) = \deg(\mathfrak{p}) = f_{\mathfrak{p}} \deg(p).$$

Proof. First equality is immediate since $\mathscr{O}_P/P = B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \simeq B/\mathfrak{p}B$. Second equality follows from the multiplicative property $[B/\mathfrak{p}B : k] = [B/\mathfrak{p}B : A/pA][A/pA : k]$ together with $[A/pA : k] = \deg(p)$. □

The following result is known as the fundamental inequality [20, Thm 3.3.4 and Thm. 3.3.5]:

Proposition 3.10. *We have $\sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}} \leq [L : K]$, and equality holds if the extension is separable.*

3.3 OM-representations of places

We assume from now on that $L = K[X]/(f)$ for some irreducible monic separable polynomial $f \in A[X]$. We let $n = \deg(f) = [L : K]$. Denoting $x = X \mod f$, we can write

$$L = K(x) = k(t, x) = k(t)[x]$$

and any $b \in L$ writes uniquely as $b = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, with $a_i \in k(t)$.

By Proposition 3.5, the places of L/k can be represented by the primes of L/K. Given $p \in \mathscr{P}_A$, we denote $\widehat{A}_p$ the p-adic completion of A_p.

Proposition 3.11. *There is a one-to-one correspondence between the primes $\mathfrak{p}$ dividing p and the monic irreducible factors $F_{\mathfrak{p}}$ of f in $\widehat{A}_p[X]$.*

Proof. This follows from [45, Prop. 8.2] combined with Proposition 3.5. □

Given any $p \in \mathscr{P}_A$, the OM-algorithm allows to compute the factors $F_{\mathfrak{p}}$ up to an arbitrary p-adic precision. This powerful algorithm has been developed by Montes [50] in the continuation of the pioneer work of Ore [48, 49], MacLane [41, 40] and Okutsu [47]. In the last decade, it has been improved and generalized in various papers, see e.g. [26, 27, 28, 30, 11, 29, 53, 6].

Briefly speaking, the OM-algorithm detects at each iteration a partial factorization of f on a higher order Newton polygon and on a higher order residual polynomial (double dissection process), until the factorization is complete. It returns as a byproduct *a type* $t_{\mathfrak{p}}$ (also called Okutsu frame, or OM-representation) attached to each prime $\mathfrak{p}$. This object is a sequence

$$t_{\mathfrak{p}} = [p, \phi_1, \ldots, \phi_{r_{\mathfrak{p}}}, \phi_{\mathfrak{p}}] \tag{1}$$

where $p = \mathfrak{p} \cap A$ and where the $\phi_i \in A[X]$ are some particular irreducible monic polynomials of strictly increasing degrees $d_1 | \cdots | d_{r_{\mathfrak{p}}}$, called key polynomials. The last key polynomial $\phi_{\mathfrak{p}}$ is a p-adic approximation of $F_{\mathfrak{p}}$ with a high enough precision which allows to distinguish $F_{\mathfrak{p}}$ from the remaining factors $F_{\mathfrak{q}}$ of f, see e.g. [11, Sec.3] for details.

Remark 3.12. *Key polynomials have been introduced by Mac Lane in the 1930s [41, 40]. When k has characteristic zero or large enough, some appropriate "approximate roots" of f may play the role of key polynomials. Approximate roots were originally introduced by Abhyankhar [5] to study germs of complex plane curves without using Puiseux series (see e.g. [51] for a nice survey on this topic).*

Let us give two simple examples.

Example 3.13. • *Let $f = X^3 - X^2 + t^2$ and let $p = (t)$. The completion of $k[t]$ at p is the ring of formal power series $k[[t]]$. We assume that* $\mathrm{char}(k) \neq 2$. *The factorization of f in $k[[t]][X]$ is $f = f_1 f_2 f_3$ with $f_1 = X - t + O(t^2)$, $f_2 = X + t + O(t^2)$ and $f_3 = X - 1 + O(t^2)$. Some OM-representations of the primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ lying above (t) are given by*

$$t_{\mathfrak{p}_1} = [t, X - t], \qquad t_{\mathfrak{p}_2} = [t, X + t], \qquad t_{\mathfrak{p}_3} = [t, X - 1].$$

• *Let $f = (X^2 + 1)^2 + tX + t + t^2$. This polynomial is irreducible in $k[[t]][X]$. Hence, there is a unique prime $\mathfrak{p}$ lying above (t). An OM-representation is*

$$t_{\mathfrak{p}} = [t, X, X^2 + 1, (X^2 + 1)^2 + t].$$

In practice, the types $t_{\mathfrak{p}}$, $\mathfrak{p}|p$ come together with extra numerical data which allows to calculate various arithmetic quantities (e.g. ramification, residual degree, index, intersection multiplicities), see e.g. [28]. An important fact for us is that these data allow for a fast computation of the valuation $v_{\mathfrak{p}}(b)$ of any $b \in L$. Concretely, this task is reduced to compute the $(\phi_1, \ldots, \phi_{r_{\mathfrak{p}}})$-multiadic expansion of b, which can be achieved in quasi-linear time. Another important feature of the OM-representation is that it allows also for a quick computation of an integral basis of a fractional ideal (see [30, 54] and Section 4), which is a key point to compute Riemann–Roch spaces using arithmetic approach.

Let us insist that an OM-representation of $\mathfrak{p}$ is given *a priori* at small precision. If needed, we can compute the $\phi_{\mathfrak{p}}$'s up to an arbitrary precision using a single-factor lifting procedure [29] or a multi-factor lifting procedure [53], the latter approach having a quasi-linear complexity thanks to a valuated Hensel's lemma. Higher precisions are required for various tasks such as computing valuations, computing two-elements representation of ideals, or computing integral bases of fractional ideals.

The OM-algorithm has been improved in [53]. This fast version computes an OM-representation of all primes $\mathfrak{p}$ dividing p with $\tilde{\mathscr{O}}(n\delta_p)$ operations in the residue field k_p if the residual characteristic is zero or high enough – this is quasi-linear in the size of the output –, or $\tilde{\mathscr{O}}(n\delta_p + \delta_p^2)$ operations in k_p otherwise, where $\delta_p \leq v_p(\mathrm{disc}(f))$ is the so-called Okutsu invariant ([54]). We refer the reader to [11, 53, 54] for more details about complexity issues.

3.4 OM-representation of divisors

Definition 3.14. *Let $D = \sum_P n_P \cdot P$ be a divisor of L. An OM-representation of D is a list*

$$t_D = \{(t_P, n_P),\ P \in \mathrm{Supp}(D)\}$$

where $t_P = t_{\mathfrak{p}}$ is an OM-representation (a type as in (1)) of the prime $\mathfrak{p} \in \mathscr{P}$ associated to P.

Let us insist on the fact that the computation of the Riemann–Roch space $\mathscr{L}(D)$ does not involve only the places $P \in \mathrm{Supp}(D)$: we need also to control that $v_P(b) \geq 0$ at all remaining places $P \notin \mathrm{Supp}(D)$. In particular, this requires to compute an OM-representation of all places centered at singular points of the projective curve defined by f. We do not assume that this data is given. However, this task has to be done only once if we need to compute Riemann–Roch spaces attached to several divisors.

Remark 3.15. *In many interesting situations, we may want to compute the OM-representation of a divisor D of L which is of particular interest, and simply defined by its intrinsic properties. For instance the canonical divisor of a curve, the adjoint divisor of a curve, the conductor of L/K, the different, the codifferent, etc. For such divisors, there are explicit formula for the values $v_{\mathfrak{p}}(D)$ in terms of the OM-invariants of f (see e.g. [43]), and it follows from [53] that we can compute an OM-representation of D in quasi-linear time.*

3.5 Other usual representations of places

For the sake of completeness, let us mention two other representations of places which are classically used in the literature.

3.5.1 Representation of places by Puiseux expansions.

This representation of places is widely used in algebraic geometry, in particular for computing Riemann–Roch spaces [2]. Geometrically, the irreducible factor $F_\mathfrak{p}$ of f gives the local equation of a branch $C_\mathfrak{p}$ of the affine plane curve C defined by f. In this setting, the valuation $v_\mathfrak{p}$ corresponds to the intersection multiplicity with $F_\mathfrak{p}$, which is usually computed by means of resultants. Namely:

Proposition 3.16. *Let $h \in L = K[x]$ non-zero. The $\mathfrak{p}$-adic valuation of h is given by*

$$v_\mathfrak{p}(h) = \frac{v_p(\mathrm{Res}(h, F_\mathfrak{p}))}{f_\mathfrak{p}} \in \mathbb{Z}, \tag{2}$$

where we still denote by h the canonical lifting of h to $K[X]$.

Proof. Let θ be a root of $F_\mathfrak{p}$ in a fixed algebraic closure $\mathbb{K}$ of the p-adic completion of K. By the henselian property, the valuation v_p extends uniquely to a valuation $\bar{v}$ on $\mathbb{K}$, and we have the equality $v_\mathfrak{p}(h) = e_\mathfrak{p}\bar{v}(h(\theta))$ (see e.g. [45, p.165]). Let $d_\mathfrak{p} = \deg F_\mathfrak{p}$ and let $\theta_1 = \theta, \theta_2, \ldots, \theta_{d_\mathfrak{p}}$ be the roots of $F_\mathfrak{p}$. Since $F_\mathfrak{p}$ is monic, the Poisson formula for the resultant gives $v_p(\mathrm{Res}(h, F_\mathfrak{p})) = \sum_{i=1}^{d_\mathfrak{p}} \bar{v}(h(\theta_i)) = d_\mathfrak{p}\bar{v}(h(\theta))$ and we conclude thanks to the equality $d_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p}$. □

However, using resultant is not convenient in practice. An alternative way is to represent the prime $\mathfrak{p}$ by a *rational parametrization* of the corresponding branch $C_\mathfrak{p}$, that is by a pair $(a, b) \in k_\mathfrak{p}((u))$ (which is truncated in practice) such that $F_\mathfrak{p}(a(u), b(u)) = 0$. If the characteristic of k is zero or big enough, such a parametrization can be given by a "rational Puiseux expansion" of shape $(\lambda u^e, S(u))$. The equality (2) becomes

$$v_\mathfrak{p}(h) = \mathrm{ord}_u\, h(\lambda u^e, S(u)), \tag{3}$$

which can be calculated quickly by Horner's rule [2]. Representing places as Puiseux expansions is particularly convenient for computing Riemann–Roch spaces since they allow to translate the conditions $v_\mathfrak{p}(h) \geq n_\mathfrak{p}$ into a finite system of linear equations over k once we have a bound on the total degree of h (see e.g. [2]). However, the complexity of the linear system solving is higher than our complexity bound for general singular curves. Nevertheless, using some extra $k[t]$-module structures (as we will do in this paper) it is shown in [21, 3, 4] that we can fasten the computations for nodal or ordinary curves in general position.

Remark 3.17. *If the characteristic of k is small, we can replace Puiseux expansions by Hamburger-Noether parametrizations [15, 16]. However, we are not aware of any implementations and complexity estimates for this task.*

Remark 3.18. *The OM-algorithm computes the truncated factors $F_\mathfrak{p}$, but not a parametrization of the corresponding branch. We believe that this is a nice open problem.*

3.5.2 Two-elements representation of a place.

It is based on the following classical result:

Lemma 3.19. *Any prime ideal $\mathfrak{p} \subset B$ can be generated by two elements $\mathfrak{p} = (p, q)$ where $p \in A$ is the monic generator of $\mathfrak{p} \cap A$ and $q \in B$. If $\mathfrak{p} \subset B_\infty$, there exists $q \in B_\infty$ such that $\mathfrak{p} = (1/t, q)$.*

This is probably the most classical way to represent prime ideals in function fields or number fields, as used for instance in the computer algebra systems SageMath or PariGP.

Definition 3.20. *The pair (p, q) is called a two-elements representation of the prime $\mathfrak{p}$.*

The $\mathfrak{q}$-adic valuation of a fractional ideal equals the minimal valuation of its generator. In particular, if $\mathfrak{p} = (p, q)$, we have $\min(v_\mathfrak{p}(p), v_\mathfrak{p}(q)) = v_\mathfrak{p}(\mathfrak{p}) = 1$ so p or q has to be a uniformizer of the place $P = P_\mathfrak{p}$. However, this condition is not sufficient. Indeed, the generator $q \in L$ needs to ensure that all conditions

$$v_\mathfrak{p}(\mathfrak{p}) = 1 \quad \text{and} \quad v_\mathfrak{q}(\mathfrak{p}) = 0 \ \ \forall\ \mathfrak{q} \in \mathscr{P}_0,\ \ \mathfrak{q} \neq \mathfrak{p}$$

are satisfied. This imposes conditions on q which involve *a priori* all finite places of L.

Example 3.21. *Let $f = X^3 - X^2 + t^2$ as in example 3.13, with factors $f_1 = X - t + O(t^2)$, $f_2 = X + t + O(t^2)$ and $f_3 = X - 1 + O(t^2)$ above $p = (t)$. We claim that*

$$\mathfrak{p}_1 = (t, q) \qquad \text{where} \qquad q = (x - 1 + t)(x - t)/t.$$

Let $\mathfrak{p} = (t, q)$. We have $v_\mathfrak{q}(\mathfrak{p}) = \min(v_\mathfrak{q}(t), v_\mathfrak{q}(q))$ for all finite primes $\mathfrak{q}$. We need to check that $v_{\mathfrak{p}_1}(\mathfrak{p}) = 1$ and $v_\mathfrak{q}(\mathfrak{p}) = 0$ for all $\mathfrak{q} \neq \mathfrak{p}_1$. If $\mathfrak{q} \nmid t$, then $v_\mathfrak{q}(q) \geq 0$ (since $x \in B \subset B_\mathfrak{q}$ as f is monic) and $v_\mathfrak{q}(t) = 0$. Hence, $v_\mathfrak{q}(\mathfrak{p}) = 0$. If $\mathfrak{q} = \mathfrak{p}_i$, we have $v_{\mathfrak{p}_i}(t) = 1$. Let us compute $v_{\mathfrak{p}_i}(q)$. For $i = 1$, we compute f_1 with a higher precision $f_1 = X - t - t^2/2 + O(t^3)$. Proposition 3.16 gives

$$v_{\mathfrak{p}_1}(q) = v_p\left(\mathrm{Res}((X - 1 + t)(X - t), X - t - t^2/2 + O(t^3)\right) - 1 = 2 - 1 = 1.$$

Hence $v_{\mathfrak{p}_1}(\mathfrak{p}) = 1$. For $i = 2, 3$ we find that

$$v_{\mathfrak{p}_2}(q) = v_p(\mathrm{Res}((X - 1 + t)(X - t), X + t + O(t^2)) - 1 = 1 - 1 = 0$$

and similarly $v_{\mathfrak{p}_3}(q) = 0$. Hence $v_{\mathfrak{p}_2}(\mathfrak{p}) = v_{\mathfrak{p}_3}(\mathfrak{p}) = 0$ as required. In a similar way, we would obtain the two-elements representations $\mathfrak{p}_2 = (t, (x - 1 + t)(x + t)/t)$ and $\mathfrak{p}_3 = (t, x - 1)$.

More generally, we can deduce easily a two-elements representation of a prime $\mathfrak{p}$ from its OM-representation, see [28]. However, two-elements representations are not suitable for rapid calculation of the $\mathfrak{p}$-adic valuation and do not contain enough information to compute integral bases. For this reason, we prefer OM-representations, although we do not exclude that mixing both representations could be of interest for various tasks, such as computing the integral basis of a product of two fractional ideals.

4 From divisors to integral bases

We keep notations of previous section. We still assume that $L = K[X]/(f)$ for some irreducible monic separable polynomial $f \in A[X]$ of degree n.

4.1 Divisors as pairs of fractional ideals

Let $D = \sum_{P \in V_L} n_P \cdot P \in \mathrm{Div}(L/k)$. Denote $\mathfrak{p} \in \mathscr{P}$ the prime of P and let $n_\mathfrak{p} = n_P$. We define

$$I(D) = \prod_{\mathfrak{p} \in \mathscr{P}_0} \mathfrak{p}^{-n_\mathfrak{p}} \qquad \text{and} \qquad I_\infty(D) = \prod_{\mathfrak{p} \in \mathscr{P}_\infty} \mathfrak{p}^{-n_\mathfrak{p}}. \tag{4}$$

Thus $I(D) \subset L$ is a fractional ideal of B and $I_\infty(D)$ is a fractional ideal of B_∞. Let $\mathscr{I}$ (resp. $\mathscr{I}_\infty$) stand for the multiplicative groups of fractional ideals of B (resp. B_∞), and let $\mathscr{I} \times \mathscr{I}_\infty$ be their direct product.

Proposition 4.1. *[32] The map $D \mapsto (I(D), I_\infty(D))$ is a group isomorphism from $\mathrm{Div}(L)$ to $\mathscr{I} \times \mathscr{I}_\infty$. Moreover, we have*

$$\mathscr{L}(D) = I(D) \cap I_\infty(D).$$

Proof. First point is clear from Proposition 3.5 together with the fact that $\mathscr{I}$ (resp. $\mathscr{I}_\infty$) is the free abelian group generated by $\mathscr{P}_0$ (resp. $\mathscr{P}_\infty$). For the second point, we remark that $\mathscr{L}(D) = \bigcap_{P \in V_L} P^{-n_P}$ by definition. By Proposition A.6, we have $B = \bigcap_{\mathfrak{p} \in \mathscr{P}_0} B_\mathfrak{p}$ and $B_\infty = \bigcap_{\mathfrak{p} \in \mathscr{P}_\infty} B_{\infty,\mathfrak{p}}$. It thus follows from Lemma 3.5 that $\mathscr{L}(D)$ is the intersection of the fractional ideal $\bigcap_{\mathfrak{p} \in \mathscr{P}_0} \mathfrak{p}^{-n_\mathfrak{p}}$ of B with the fractional ideal $\bigcap_{\mathfrak{p} \in \mathscr{P}_\infty} \mathfrak{p}^{-n_\mathfrak{p}}$ of B_∞. By Lemma 3.6, these intersections can be replaced by a product. □

We want to compute a basis of $\mathscr{L}(D)$ using Proposition 4.1. The first step is to compute an integral basis of the fractional ideals $I(D)$ and $I_\infty(D)$. To this aim, we use recent results of [53].

4.2 Triangular bases of fractional ideals

Let $R = A = k[t]$ or $R = A_\infty = k[1/t]_{(1/t)}$.

Definition 4.2. *Let $M, N \subset L$ be free R-modules of rank n. We denote $[M : N]$ the fractional ideal of R generated by the determinant of the transition matrix of an R-basis of N to an R-basis of M. It is called the index ideal of M over N.*

The definition does not depend on the choice of the bases since the determinant varies by a unit of R. The index ideal obeys to the following classical properties (see e.g. [59]):

Lemma 4.3. *Let L, M and N be free R-modules of rank n. We have*

1. *$[L : N] = [L : M][M : N]$ and $[M : N] = [N : M]^{-1}$,*
2. *If $N \subset M$, then there exists $a_1, \dots, a_n \in R$ such that $a_1 | \cdots | a_n$ and*

$$M/N \cong R/a_1R \times \cdots \times R/a_nR.$$

We have then $[M : N] = (a_1 \cdots a_n) \subset R$ and $N = M$ if and only if $[M : N] = R$.

Let $\overline{R} \subset L = k(t)[x]$ be the integral closure of R in L (so $\overline{R} = B$ or $\overline{R} = B_\infty$). Thus $\overline{R}$ is a Dedekind ring. As L/K is assumed to be separable, all fractional ideals of $\overline{R}$ are free R-module of rank $n = [L : K]$. We refer to [60, Thm.1.16] for the following result:

Proposition 4.4. *A fractional ideal I of $\overline{R}$ admits an R-basis $\mathscr{B} = (q_0, q_1h_1(x), \dots, q_{n-1}h_{n-1}(x))$ such that the following conditions are satisfied:*

1. *For all $0 \leq i < n$, $q_i \in K$ and $h_i(x) \in R[x]$ is monic of degree i (in particular $h_0 = 1$).*
2. *We have inclusions $q_0R \subset q_1R \subset \cdots \subset q_{n-1}R$ of fractional ideals of R.*

We say that $\mathscr{B}$ is a triangular R-basis of I. The elements q_i are uniquely determined up to multiplication by a unit of R and we have

$$[I : R[x]] = (q_0 \cdots q_{n-1})^{-1}R.$$

Remark 4.5. *Any free R-module $I \subset L$ of rank n admits an R-basis satisfying the first condition by Gaussian elimination, but the second condition may not be satisfied. It turns out that if I is a fractional ideal of a Dedekind ring, then condition 2 follows automatically from condition 1.*

Notation. For $R = A$ or $R = A_\infty$, any fractional ideal J of R is principal, hence generated by a unique element $h = a/b$ with $a, b \in k[t]$ monic and coprime. We then write for short

$$\deg(J) = \deg(h) = \deg(a) - \deg(b).$$

4.3 Computing triangular bases over finite places

We consider here $R = A = k[t]$. We want to compute an integral basis of a fractional ideal I of B. The index of I does not reflect well the size of I, and we will rather express the complexity of our algorithm in terms of the index of a normalized ideal of I.

Definition 4.6. *Let I be a fractional ideal of B. Let $q_I \in K$ such that $I \cap K = q_I A$.*

- *The normalized ideal of I is $I^* = q_I^{-1} I$.*
- *The normalized index of I is $\delta_I = \deg [I^* : A[x]]$.*
- *The normalized exponent of I is $\exp(I) = \min\{\deg(a) \mid a \in A, aI^* \subset A[x]\}$.*

Lemma 4.7. *We have $A[x] \subset B \subset I^*$. In particular, $0 \leq \delta_B \leq \delta_I$ and $0 \leq \exp(B) \leq \exp(I)$. Moreover,*

$$\exp(I) \leq \delta_I \leq n \exp(I).$$

Proof. As f is monic, x is integral over A, hence $A[x] \subset B$. Let $q = q_I$. We have $I \cap K = qA$, hence $I^* \cap K = q^{-1}qA = A$. Thus $1 \in I^*$ and $B \subset I^*$. From these inclusions, we deduce $0 \leq \exp(B) \leq \exp(I)$, and the inequality $0 \leq \delta_B \leq \delta_I$ follows from Lemma 4.3, using $[I^* : A[x]] = [I^* : B][B : A[x]]$ and $A[x] \subset B \subset I^*$. Still from Lemma 4.3, we get a decomposition $I^*/A[x] \simeq A/a_1A \times \cdots \times A/a_nA$ with $a_i \in A$ and $a_i | a_{i+1}$. We deduce that $\exp(I) = \deg a_n$. Moreover, $[I^* : A[x]] = a_1 \cdots a_n A$, hence $\delta_I = \deg a_1 + \cdots + \deg a_n$. Since $\deg a_i \leq \deg a_{i+1}$, the last claim follows. □

Computing integral bases in function fields is a classical task of computer algebra and there are several algorithms to do this. There are geometric approaches based on Puiseux series (see [1] for a state-of-the art in the case $I = B$) and there are arithmetic approaches ([10, 30, 61, 54] and references therein) which rather follow Okutsu's framework [47] and use the OM-algorithm as we do here. This latter approach has the advantage to work in any characteristic and applies *mutatis mutandis* to the case of number fields.

Let us briefly summarize the main steps. Let $I = \prod_{\mathfrak{p} \in \mathscr{P}_0} \mathfrak{p}^{n_\mathfrak{p}}$ be a fractional ideal of B.

1. For each finite prime $p \in \mathscr{P}_A$, we compute a triangular A_p-basis of the free A_p-module $I_p = I \otimes_A A_p$. If p does not divide the index $[B : A[x]]$ and $n_\mathfrak{p} = 0$ for all $\mathfrak{p} | p$, then a triangular basis is $1, x, \ldots, x^{n-1}$. Otherwise:
   (a) We run the OM-algorithm [53] above p to compute an OM-representation of each $\mathfrak{p} | p$ with high enough precision (i.e. a list of key polynomials of the prime factor $F_\mathfrak{p} \in \widehat{A}_p[x]$ of f).

(b) We apply the beautiful MaxMin algorithm of Stainsby [61] to detect (for free) for each $i = 0, \dots, n-1$ a degree i multiplicative combination h_i of key polynomials which maximizes the semi-valuation $w_{I,p}(h) = \min_{\mathfrak{p}|p}(v_{\mathfrak{p}}(h) - n_{\mathfrak{p}})/e_{\mathfrak{p}}$. Then $h_0/p^{\lfloor w_{I,p}(h_0)\rfloor}, \dots, h_{n-1}/p^{\lfloor w_{I,p}(h_{n-1})\rfloor}$ is a triangular A_p-basis of I_p, see [61, Thm.3.4].

2. We use the Chinese Remainder Theorem to glue together all A_p-bases, resulting in a triangular A-basis of I (we use here the fact that the A_p-bases are triangular).

We use notations $\mathscr{O}_\epsilon(g(n)) = \mathscr{O}(g(n)^{1+\epsilon(n)})$ with $\epsilon(n) \to 0$. We denote for short $\delta = \delta_B$. We obtain the following complexity estimate:

Theorem 4.8. *[54, Thm.7] Suppose f separable and monic. Let $I = \prod \mathfrak{p}^{n_\mathfrak{p}}$ be a fractional ideal of B, the primes $\mathfrak{p}$ being given in OM-representation. There is a deterministic algorithm which computes a triangular A-basis of I with*

- *$\mathscr{O}_\epsilon(n\delta_I)$ operations in k if $char(k) = 0$ or $char(k) > n$,*
- *$\mathscr{O}_\epsilon(n\delta_I + \delta^2)$ operations in k if $char(k) \leq n$.*

The returned basis is given as a pair $\mathscr{B} = (q, \mathscr{B}^*)$, with $q = q_I \in k(t)$ as in Definition 4.6 and $\mathscr{B} = q\mathscr{B}^*$, where

$$\mathscr{B}^* = \left(1, \frac{g_1(t,x)}{p_1(t)}, \dots, \frac{g_{n-1}(t,x)}{p_{n-1}(t)}\right) \tag{5}$$

is an A-basis of the normalized ideal I^* such that:
(i) $p_i \in k[t]$ is monic, $p_1|p_2|\cdots|p_{n-1}$.
(ii) $g_i \in k[t][x]$ is monic of degree i in x and $\deg_t(g_i) < \deg(p_i)$.

The p_i's are uniquely determined. The quantities introduced in Definition 4.6 satisfy $\delta_I = \deg(p_1) + \cdots + \deg(p_{n-1})$ and $\exp(I) = \deg(p_{n-1})$. Not taking into account the factor q, the output has arithmetic dense size $\sum_{i=1}^{n-1} i\deg(p_i) = \mathscr{O}(n\delta_I)$, and this bound is sharp. Thus the algorithm has a quasi-linear complexity in characteristic zero or high enough. The element $q = q_I$ is given as a product of primes $q = \prod_{p\in\mathscr{P}_A} p^{-m_p}$ (not computed), with the m_p's explicitly determined by I, see below.

Remark 4.9. *Theorem 7 of [54] requires to know the set of primes $p \in \mathscr{P}_A$ dividing $[I^* : A[x]]$. A part of these primes is deduced for free from the OM-representation of I (which is given). The remaining primes are the prime divisors of $[B : A[x]]$. They can be deduced from the irreducible factorization in $k[t]$ of the discriminant of f. Using dynamic evaluation [34], it's in fact sufficient to compute the square-free factors of the discriminant, whose cost fits in the aimed bound.*

4.4 Computing triangular bases at infinity

We now specialize Proposition 4.4 to the case $R = A_\infty = k[1/t]_{(1/t)}$. We want to compute a triangular A_∞-basis of a fractional ideal I_∞ of B_∞. We need to take care that $A_\infty[x]$ is usually not contained in B_∞. Let $f = \sum_{i=0}^n c_i X^i$ with $c_i \in A = k[t]$. Following [32], we consider

$$y = xt^{-\lambda} \qquad \text{where} \qquad \lambda = \lambda(f) = \max_{i<n}\left(\left\lceil \frac{\deg(c_i)}{n-i}\right\rceil\right). \tag{6}$$

Lemma 4.10. *The element $y \in L$ is integral over A_∞.*

Proof. The polynomial $f_\infty(Y) = t^{-n\lambda} f(t^\lambda Y)$ is a monic polynomial of degree n which by (6) belongs to $k[t^{-1}][Y]$. Since $f_\infty(y) = t^{-n\lambda} f(x) = 0$ and $k[t^{-1}] \subset A_\infty$, we conclude. □

Let us denote $u = t^{-1}$. Note that $\deg_u(a) = -\deg(a)$ for all $a \in K$. The ideal $I_\infty \cap K$ is now a fractional ideal of $A_\infty = k[u]_{(u)}$.

Definition 4.11. *Let I_∞ be a fractional ideal of B_∞ and let $m_{I_\infty} \in \mathbb{Z}$ such that $I_\infty \cap K = u^{m_{I_\infty}} A_\infty$.*

- *The normalized ideal of I_∞ is $I_\infty^* = u^{-m_{I_\infty}} I_\infty$.*
- *The normalized index of I_∞ is $\delta_{I_\infty} = \deg_u [I_\infty^* : A_\infty[y]]$.*
- *The normalized exponent of I_∞ is $\exp(I_\infty) = \min\{\deg_u(a) \mid a \in A_\infty, aI^* \subset A_\infty[y]\}$.*

Lemma 4.12. *We have $A_\infty[y] \subset B_\infty \subset I_\infty^*$. In particular, $0 \le \delta_{B_\infty} \le \delta_{I_\infty}$ and $0 \le \exp(B_\infty) \le \exp(I_\infty)$. Moreover,*

$$\exp(I_\infty) \le \delta_{I_\infty} \le n \exp(I_\infty).$$

Proof. Similar to the proof of Lemma 4.7, except that we work over the ring $A_\infty = k[u]_{(u)}$. □

We denote for short $\delta_\infty = \delta_{B_\infty}$. Analogously to Theorem 4.8, we deduce from [54]:

Theorem 4.13. *Let I_∞ be a fractional ideal of B_∞ given by OM-representation. There is a deterministic algorithm which computes a triangular A_∞-basis of I_∞ with:*

- *$\mathscr{O}_\epsilon(n\delta_{I_\infty})$ operations in k if $char(k) = 0$ or $char(k) > n$,*
- *$\mathscr{O}_\epsilon(n\delta_{I_\infty} + \delta_\infty^2)$ operations in k if $char(k) \le n$.*

The returned basis has shape $\mathscr{B}_\infty = u^m \mathscr{B}_\infty^*$ with $m = m_{I_\infty} \in \mathbb{Z}$ as in Definition 4.11 and where

$$\mathscr{B}_\infty^* = \left(1, \frac{h_1(u,y)}{u^{m_1}}, \dots, \frac{h_{n-1}(u,y)}{u^{m_{n-1}}}\right) \tag{7}$$

is an A_∞-basis of the normalized ideal I_∞^* which satisfies:
(i) $0 \le m_1 \le m_2 \cdots \le m_{n-1}$.
(ii) $h_i \in k[u][y]$ is monic of degree i in y and $\deg_u(h_i) < m_i$.

The m_i's are uniquely determined. We have $\delta_{I_\infty} = m_1 + \cdots + m_{n-1}$ and $\exp(I_\infty) = m_{n-1}$. The complexity is again quasi-linear with respect to the size of the output.

4.5 Various bounds for the exponents

We will need upper bounds for the exponents $\exp(I)$ and $\exp(I_\infty)$ in terms of the divisor D. A key point is the following explicit formula.

Lemma 4.14. *Let $I = \prod_{\mathfrak{p} \in \mathscr{P}_0} \mathfrak{p}^{-n_\mathfrak{p}}$ and $I_\infty = \prod_{\mathfrak{p} \in \mathscr{P}_\infty} \mathfrak{p}^{-n_\mathfrak{p}}$. For $p \in \mathscr{P}_A = \operatorname{Spec} A \cup \{\infty\}$, we let $m_p = \min\left\{\left\lfloor \frac{n_\mathfrak{p}}{e_\mathfrak{p}} \right\rfloor \mid \mathfrak{p} | p\right\}$. With notations of Definition 4.6 and Definition 4.11:*

1. *We have $q_I = \prod_{p \in \operatorname{Spec} A} p^{-m_p}$ and $I^* = \prod_{p \in \operatorname{Spec} A} \prod_{\mathfrak{p}|p} \mathfrak{p}^{e_\mathfrak{p} m_p - n_\mathfrak{p}}$*
2. *We have $m_{I_\infty} = -m_\infty$ and $I_\infty^* = \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{e_\mathfrak{p} m_\infty - n_\mathfrak{p}}$.*

Proof. This follows from [54, Lem.2]. □

For $q = a/b \in K = k(t)$ with $a, b \in k[t]$ coprime, we denote $h(q) = \deg(a) + \deg(b)$ the height of q.

Proposition 4.15. *Let $D \in \mathrm{Div}(L)$ and let $I = I(D)$ and $I_\infty = I_\infty(D)$. We have*

$$\exp(B) + \exp(B_\infty) \;\leq\; \exp(I) + \exp(I_\infty) \;\leq\; \deg(D^+) + \deg(D^-) + \exp(B) + \exp(B_\infty) \quad (8)$$

and $h(q_I) + |m_{I_\infty}| \leq \deg(D^+) + \deg(D^-)$.

Proof. We first prove the second point. We have $h(q_I) + |m_{I_\infty}| = \sum_{p \in \mathscr{P}_A} |m_p| \deg p$ from Lemma 4.14 (with convention $\deg \infty = 1$). Let $p \in \mathscr{P}_A$ and let $\mathfrak{p}_0 | p$ such that $m_p = \left\lfloor \frac{n_{\mathfrak{p}_0}}{e_{\mathfrak{p}_0}} \right\rfloor$.

- If $n_{\mathfrak{p}_0} > 0$ then $0 < n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \leq n_{\mathfrak{p}_0}$. Hence, $0 \leq \lfloor n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \rfloor \leq n_{\mathfrak{p}_0}$ and $|m_p| \leq |n_{\mathfrak{p}_0}|$.
- If $n_{\mathfrak{p}_0} < 0$, then $0 > n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \geq n_{\mathfrak{p}_0}$. Hence, $0 \geq \lfloor n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \rfloor \geq n_{\mathfrak{p}_0}$ and $|m_p| \leq |n_{\mathfrak{p}_0}|$.

As $\deg p \leq \deg \mathfrak{p}_0$ by Proposition 3.9, we get $|m_p| \deg p \leq |n_{\mathfrak{p}_0}| \deg \mathfrak{p}_0 \leq \sum_{\mathfrak{p}|p} |n_\mathfrak{p}| \deg \mathfrak{p}$. Summing over all $p \in \mathscr{P}_A$, we get as required:

$$h(q_I) + |m_{I_\infty}| \leq \sum_{\mathfrak{p} \in \mathscr{P}_A} |n_\mathfrak{p}| \deg \mathfrak{p} = \deg(D^+) + \deg(D^-).$$

We prove now inequality (8). Since $A[x] \subset B \subset I^*$, clearly $\exp(B) \leq \exp(I)$. Let $a, b \in A$ such that $aI^* \subset B$ and $bB \subset A[x]$. We have $abI^* \subset A[x]$. Hence, $\exp(I) \leq \deg(a) + \deg(b)$. Considering b of minimal degree, we obtain $\exp(I) \leq \deg(a) + \exp(B)$ and we are left to bound $\deg a$ in terms of D. Let us first construct such an a. Denote $l_p = \max\{\lceil n_\mathfrak{p}/e_\mathfrak{p} \rceil \mid \mathfrak{p}|p\}$ for $p \in \mathrm{Spec}_A$ and consider $a = \prod_{p \in \mathrm{Spec}\, A} p^{l_p - m_p}$. Since $l_p \geq m_p$, we have $a \in A$. For all $\mathfrak{p}|p$, we have $v_\mathfrak{p}(p) = e_\mathfrak{p}$ (Definition 3.8) and Lemma 4.14 gives

$$v_\mathfrak{p}(aI^*) = e_\mathfrak{p}(l_p - m_p) + e_\mathfrak{p} m_p - n_\mathfrak{p} = e_\mathfrak{p} l_p - n_\mathfrak{p} \geq 0.$$

It follows that $aI^* \subset B$ and we are left to bound $\deg a$. We have

$$l_p \leq \max_{\mathfrak{p}|p, n_\mathfrak{p} > 0} \left\lceil \frac{n_\mathfrak{p}}{e_\mathfrak{p}} \right\rceil \leq \max_{\mathfrak{p}|p, n_\mathfrak{p} > 0} n_\mathfrak{p} \qquad \text{and} \qquad m_p \geq \min_{\mathfrak{p}|p, n_\mathfrak{p} < 0} \left\lfloor \frac{n_\mathfrak{p}}{e_\mathfrak{p}} \right\rfloor \geq \min_{\mathfrak{p}|p, n_\mathfrak{p} < 0} n_\mathfrak{p}.$$

Using again $\deg p \leq \deg \mathfrak{p}$ for all $\mathfrak{p}|p$, we get

$$\deg(a) = \sum_{p \in \mathrm{Spec}\, A} (l_p - m_p) \deg(p) \leq \sum_{\mathfrak{p} \in \mathscr{P}_0 | n_\mathfrak{p} > 0} n_\mathfrak{p} \deg \mathfrak{p} - \sum_{\mathfrak{p} \in \mathscr{P}_0 | n_\mathfrak{p} < 0} n_\mathfrak{p} \deg \mathfrak{p} = \deg(D_0^+) + \deg(D_0^-)$$

where D_0 is the finite part of D. Hence $\exp(I) \leq \deg(D_0^+) + \deg(D_0^-) + \exp(B)$. We show in the same way that $\exp(I_\infty) \leq \deg(D_1^+) + \deg(D_1^-) + \exp(B_\infty)$ where D_1 is the infinite part of D. As $D = D_0 + D_1$, the claim follows. □

The upper bounds of Proposition 4.15 are sharp in some cases, but quite bad in some other cases. Let us provide another estimate in terms of the divisor defined by the normalized ideals.

Proposition 4.16. *Let D^* be the divisor defined by the pair of normalized fractional ideals (I^*, I_∞^*) following Proposition 4.1.*

1. *We have $D^* \geq 0$ and $D^* = D + \mathrm{div}(q) + rD_\infty$ for some $q \in K = k(t)$ and some $r \in \mathbb{Z}$.*
2. *We have $q = q_I$ and $r = m_{I_\infty} + \deg q_I$.*
3. *If $D_0^* \neq D^*$ satisfies point 1 for some q_0, r_0, then $D_0^* > D^*$, $r < r_0$ and $q_0/q \in k[t] \setminus k$.*
4. *The following inequality holds:*

$$\exp(I) + \exp(I_\infty) \leq \deg(D^*) + \exp(B) + \exp(B_\infty) \quad (9)$$

Proof. Point 1. Since $B \subset I^*$ and $B_\infty \subset I^*_\infty$ by respectively Lemma 4.7 and Lemma 4.12, each $\mathfrak{p}$ appears with negative exponents in I^* and I^*_∞, and we deduce from (4) that $D^* \geq 0$. Let us consider $q = q_I$ and $m = m_{I_\infty}$. We have $I(D) = I = qI^* = qI(D^*) = I(D^* - \mathrm{div}(q))$, the second equality by Definition 4.6, the third equality by definition of D^* and the fourth equality by (4). Hence,

$$D = D^* - \mathrm{div}(q) + D' \tag{10}$$

for some D' supported at infinity by (4). In the same way, $I_\infty = u^m I^*_\infty = t^{-m} I^*_\infty$ (Definition 4.11) implies that $I_\infty(D) = I_\infty(D^* + \mathrm{div}(t^m))$, hence

$$D = D^* + \mathrm{div}(t^m) + D'' \tag{11}$$

for some D'' supported at finite places. Let $D_\infty = \mathrm{div}_\infty(t) = \mathrm{div}_0(t^{-1}) \geq 0$ be the divisor at infinity. Since $q \in K$, the infinite part of $-\mathrm{div}(q)$ is exactly $\deg(q) D_\infty$ while the infinite part of $\mathrm{div}(t^m)$ is $-mD_\infty$. By equating the parts at infinity in (10) and (11), we deduce that $D' = -(m + \deg q) D_\infty$. Using (10) again, we get $D^* = D + \mathrm{div}(q) + rD_\infty$, with $r = m + \deg q$. This shows point 1 together with the fact that $q = q_I$ and $m = m_{I_\infty}$ are solutions. We show points 2 and 3 simultaneously. We keep notations $q = q_I$ and $m = m_{I_\infty}$ and $r = m + \deg q$. Let $D^*_0 = D + r_0 D_\infty + \mathrm{div}(q_0)$ with $D^*_0 \geq 0$, $q_0 \in K$ and $m_0 \in \mathbb{Z}$. Thus

$$q_0 \in \mathscr{L}(D + r_0 D_\infty) \cap K. \tag{12}$$

By Proposition 4.1, we get in particular $q_0 \in I(D + r_0 D_\infty) \cap K = I(D) \cap K = qA$, the first equality by (4) since $r_0 D_\infty$ is supported at infinity, and the second equality by Definition 4.6 of $q = q_I$. Thus $q_0 = aq$ for some $a \in A = k[t]$. In particular, a has no poles at finite places and $\mathrm{div}(q_0) - \mathrm{div}(q) = \mathrm{div}(a) = \mathrm{div}_0(a) - \deg(a) D_\infty$. We get

$$D = D^*_0 - r_0 D_\infty - \mathrm{div}(q_0) = D^* - rD_\infty - \mathrm{div}(q) \quad \Longrightarrow \quad D^*_0 = D^* + \mathrm{div}_0(a) + (r_0 - r - \deg a) D_\infty. \tag{13}$$

On the other hand, (12) and Proposition 4.1 give $q_0 \in I_\infty(D + r_0 D_\infty) \cap K$. Since $r_0 D_\infty$ is the infinite part of $\mathrm{div}(t^{-r_0})$, we get

$$I_\infty(D + r_0 D_\infty) \cap K = I_\infty(D + \mathrm{div}(t^{-r_0})) \cap K = t^{r_0} I_\infty(D) \cap K = t^{r_0 - m} A_\infty,$$

the last equality by Definition 4.11 since $m = m_{I_\infty}$. Hence $q_0 t^{m - r_0} \in A_\infty$, that is $\deg q_0 + m - r_0 \leq 0$. As $m = r - \deg(q)$, we get $r_0 - r - \deg a \geq 0$. Combined with (13), we deduce that $D^*_0 \geq D^*$, with equality if and only if $a \in k$ and $r = r_0$. This proves points 2 and 3. Finally, we have $\exp(I) = \exp(I^*)$ by Definition 4.6 and $I(D^*) = I^*$ by definition of D^*. Hence, $\exp(I) = \exp(I(D^*))$ and similarly at infinity. Point 4 thus follows from Proposition 4.15 applied to the effective divisor D^*. □

In short, Proposition 4.16 says that:

- The divisor D^* is the effective divisor of minimal degree which is K-linearly equivalent to D modulo D_∞.
- The quantity $\exp(I) + \exp(I_\infty)$ measures the defect of K-principality of D modulo D_∞.
- The quantity $r_D = \deg(q_I) + m_{I_\infty}$ obeys to the following relation:

$$\deg D^* = \deg D + n r_D \qquad \text{and} \qquad r_D = \min\left\{ r \in \mathbb{Z},\ \mathscr{L}(D + rD_\infty) \cap K \neq \{0\} \right\},$$

first equality by point 1 since $\deg(\mathrm{div}(q)) = 0$ and $\deg D_\infty = n$ and second equality by combining points 1, 2, 3.

Remark 4.17. *The bound (9) is possibly much better than (8). In particular, if $D = \mathrm{div}(q) + rD_\infty$ for some $q \in K$ and some $r \in \mathbb{Z}$, then $D^* = 0$ and (9) gives the minimal possible value $\exp(I) + \exp(I_\infty) = \exp(B) + \exp(B_\infty)$ which does not depend on $\deg(D)$, while the upper bound (8) can be arbitrarily large when $h(q)$ increases.*

On the other hand, if D is negative and far from being K-principal modulo D_∞, the bound (8) is better. An example is $D = -N\mathfrak{p}$ with $N > 0$, $e_\mathfrak{p} = f_\mathfrak{p} = 1$. We get $\deg D = -N$, $r_D = \deg q_I + m_{I_\infty} = N$ by Lemma 4.14, hence $\deg D^* = \deg D + nr_D = (n-1)N > N = \deg D^+ + \deg D^-$.

5 From integral bases to Riemann–Roch spaces

Given some integral bases of $I(D)$ and $I_\infty(D)$, we want now to compute a k-basis of $\mathscr{L}(D) = I(D) \cap I_\infty(D)$. We follow the algorithm of Hess [32] (see also Bauch's thesis [9]), in the vein of the pioneer work of Schmidt [58]. Recall that the divisor at infinity is $D_\infty = \mathrm{div}_\infty(t)$. It is supported at infinite places. We will compute a k-basis of $\mathscr{L}(D + rD_\infty)$ for any integer r.

5.1 Hess's algorithm

A key point is the notion of reduced basis, that we will rather express in terms of row reduced matrices. For $b \in k(t)^n$, we let $\deg(b)$ be the maximal degree of the entries of b.

Definition 5.1. *Let $b_0, \dots, b_{n-1} \in k(t)^n$. We denote $\mathbf{M} = (b_0, \dots, b_{n-1}) \in k(t)^{n\times n}$ the matrix with rows b_i.*

- *The row-degree of $\mathbf{M}$ is $\mathrm{rdeg}(\mathbf{M}) = (\deg(b_0), \dots, \deg(b_{n-1})) \in \mathbb{Z}^n$.*
- *We say that $\mathbf{M}$ is row reduced if $\deg\left(\sum \lambda_i b_i\right) = \max_i \deg\left(\lambda_i b_i\right)$ for all $\lambda_i \in k(t)$.*

Lemma 5.2. *Let $\mathbf{M} \in k(t)^{n\times n}$ be non singular.*

- *The matrix $\mathbf{M}$ is row reduced if and only if $\deg\det(\mathbf{M}) = |\mathrm{rdeg}(\mathbf{M})|$.*
- *There exists $\mathbf{U} \in k[t]^{n\times n}$ unimodular such that $\mathbf{UM}$ is row reduced.*

Proof. This is standard, see e.g. [36, Ch.6.3], [69, Sec.2.7] or [32, Lem.4.1]. □

As in the previous section, we assume that $L = k(t)[X]/(f)$ for some irreducible monic separable polynomial f of degree n. Thus $L = k(t)[x]$ is a $k(t)$-vector space of dimension n. Here is the key result of [32].

Proposition 5.3. *[32] Let $D \in \mathrm{Div}(L)$. Let $\mathscr{B} = (b_0, \dots, b_{n-1})$ be an A-basis of $I(D)$ and let $\mathscr{B}_\infty$ be an A_∞-basis of $I_\infty(D)$.*

- *Both $\mathscr{B}$ and $\mathscr{B}_\infty$ form a basis of L as a $k(t)$-vector space.*
- *Let $\mathbf{P} \in k(t)^{n\times n}$ be the matrix of the basis $\mathscr{B}$ expressed in the basis $\mathscr{B}_\infty$. If $\mathbf{P}$ is row reduced, then for all $r \in \mathbb{Z}$, the Riemann–Roch space $\mathscr{L}(D + rD_\infty)$ has k-basis*

$$(b_i t^j,\ 0 \le i \le n-1,\ 0 \le j \le d_i + r)$$

where $(d_0, \dots, d_{n-1}) = -\mathrm{rdeg}(\mathbf{P})$.

- *The integers $d_i \in \mathbb{Z}$ are uniquely determined (up to permutation) by the subring $A \subset L$ and the divisor D.*

Proof. This follows from [32, Thm.5.1 and Algo.6.1] (with the minor difference that we deal here with row vectors while [32] deals with column vectors). The key point is that $\mathbf{P}$ being row reduced, there exists a unimodular matrix $\mathbf{V} \in A_\infty^{n\times n}$ such that $\mathbf{PV}$ is diagonal with entries $(t^{-d_0}, \dots, t^{-d_{n-1}})$ [32, Cor.4.3]. The set $\mathbf{V}^{-1}\mathscr{B}_\infty$ is a new A_∞-basis $(v_0, \dots, v_{n-1})$ of $I_\infty(D)$ and we have now $b_i = t^{-d_i}v_i$ for all i. Let $h \in L$. By Proposition 4.1, we have $h \in \mathscr{L}(D + rD_\infty)$ if and only if $h \in I(D + rD_\infty)$ and $h \in I_\infty(D + rD_\infty)$. As $I(D + rD_\infty) = I(D)$, the first condition is equivalent to h being of shape $h = \sum a_i b_i$ with $a_i \in k[t]$. Since $I_\infty(D + rD_\infty) = t^r I_\infty(D)$ and $h = \sum a_i t^{-d_i} v_i$, the second condition is equivalent to $a_i t^{-r-d_i} \in A_\infty$, that is $\deg(a_i) \le d_i + r$, as required. □

Definition 5.4. *A family $((b_0, d_0), \dots, (b_{n-1}, d_{n-1}))$ as in Proposition 5.3 is called a compressed basis of $\mathscr{L}(D)$.*

Remark 5.5. *Note that a compressed basis exists even if $\mathscr{L}(D) = \{0\}$, which corresponds to the case $d_i < 0$ for all i. Computing a compressed basis in such a case makes sense if we want to compute $\mathscr{L}(D + rD_\infty)$ for some $r \in \mathbb{Z}$.*

In what follows, we freely identify $b \in L = k(t)[x]$ with the row vector of its coefficients in the basis $1, x, \dots, x^{n-1}$ of the $k(t)$-vector space L. We are led to the following algorithm:

Algorithm 1 Hess's algorithm

Input: $L = k(t)[X]/(f)$ with $f \in k[t][X]$ monic and separable, and $D \in \mathrm{Div}(L)$.
Output: A compressed basis of $\mathscr{L}(D)$.
1: Compute $\mathbf{M}$ with rows an A-basis $\mathscr{B}$ of $I(D)$.
2: Compute $\mathbf{N}$ with rows an A_∞-basis $\mathscr{B}_\infty$ of $I_\infty(D)$.
3: Compute $\mathbf{U} \in k[t]^{n\times n}$ unimodular such that $\mathbf{UMN}^{-1}$ is row reduced.
4: Compute $\mathbf{UM}$, say $\mathbf{UM} = (b_0, \dots, b_{n-1})$.
5: **return** $((b_i, d_i),\ 0 \le i \le n-1)$ where $(d_0, \dots, d_{n-1}) = -\mathrm{rdeg}(\mathbf{UMN}^{-1})$.

Theorem 5.6. *This algorithm is correct.*

Proof. The existence of $\mathbf{U}$ is ensured by Lemma 5.2. Since $\mathbf{U} \in k[t]^{n\times n} = A^{n\times n}$ is unimodular, the rows of $\mathbf{UM}$ still form an A-basis $\mathscr{B}'$ of $I(D)$. The matrix of $\mathscr{B}'$ in the basis $\mathscr{B}_\infty$ is given by $\mathbf{P} = \mathbf{UMN}^{-1}$, which is row reduced. The result thus follows from Proposition 5.3. □

Complexity of steps 1 and 2 have been analyzed in the previous section. We need to study the complexity of the remaining steps. A delicate point is that the computation of $\mathbf{MN}^{-1}$ and $\mathbf{UM}$ is too expensive if we consider the matrix $\mathbf{N}$ of the triangular A_∞-basis of $I_\infty(D)$ given by (7). We will need to compute first a suitable normal form of $\mathbf{N}$.

Let us first state some auxiliary complexity results about polynomial matrices.

5.2 Multiply, invert and reduce polynomial matrices

In what follows, the degree of a matrix is the maximal degree of its entries.

Proposition 5.7. *Let $\mathbf{E}, \mathbf{F} \in k[t]^{n\times n}$ and let $d = \deg \mathbf{E}$ and $e = \deg \mathbf{F}$. Then:*

1. $\deg(\mathbf{EF}) \le d + e$.
2. *We can compute $\mathbf{EF}$ in time $\mathscr{O}_e(n^\omega(d + e + 1))$.*

Proof. By considering $\mathbf{E}, \mathbf{F}$ as polynomials in t with coefficients in $k^{n\times n}$, the inequality $\deg(\mathbf{EF}) \leq d+e$ is clear. The second point follows from [17]. □

Next, we need to estimate the cost of computing a row reduced form (Definition 5.1) of a polynomial matrix.

Proposition 5.8. *Let $\mathbf{E} \in k[t]^{n\times n}$ of degree d. We can compute a row reduced form $\mathbf{E}_{\mathrm{red}}$ of $\mathbf{E}$ in time $\tilde{\mathcal{O}}(n^\omega(d+1))$. We have then $\deg \mathbf{E}_{\mathrm{red}} \leq \deg \mathbf{E}$.*

Proof. First point follows for instance from [44, Thm 1.4]. We have $\overline{\mathrm{rdeg}(\mathbf{E})} \geq \overline{\mathrm{rdeg}(\mathbf{E}_{\mathrm{red}})}$, see [69, Lem 2.14], where $\overline{a}$ is the list of the entries of $a \in \mathbb{Z}^n$ sorted in increasing order. Particularly, it implies $\deg(\mathbf{E}_{\mathrm{red}}) \leq \deg(\mathbf{E})$. □

Finally, we will use the following key fact concerning the inversion of a polynomial matrix:

Proposition 5.9. *Let $\mathbf{F} \in k[t]^{n\times n}$ be a row reduced matrix and let $d \in \mathbb{N}$ such that:*

$$\deg \mathbf{F} \leq d \qquad \text{and} \qquad t^d\mathbf{F}^{-1} \in k[t]^{n\times n}.$$

Then $\deg(t^d\mathbf{F}^{-1}) \leq d$ and $\mathbf{F}^{-1}$ can be computed in time $\mathcal{O}_\epsilon(n^\omega d)$.

Proof. We follow [55]. Using the determinant formula, the cofactor matrix of $\mathbf{F}$ satisfies $\deg({}^t\mathrm{com}(\mathbf{F})) \leq |\mathrm{rdeg}(\mathbf{F})|$. Since $\mathbf{F}$ is row reduced, we have $\deg(\det(\mathbf{F})) = |\mathrm{rdeg}(\mathbf{F})|$ (Lemma 5.2). Using $\mathbf{F}^{-1} = {}^t\mathrm{com}(\mathbf{F})/\det(\mathbf{F})$, we obtain $\deg(\mathbf{F}^{-1}) \leq 0$. Hence $t^d\mathbf{F}^{-1}$ has degree at most d. The cost estimate follows by combining [55, Lemma 3.8] and [55, Lemma 3.6] (first condition is expressed in [55] in terms of column degree, but this has no matter for our purpose up to transpose). The strategy is as follows: we compute $\mathbf{F}^{-1}$ modulo $(t-1)$ and use fast high order lifting [64] to deduce $\mathbf{F}^{-1}$ modulo $(t-1)^{d+1}$. We deduce $t^d\mathbf{F}^{-1}$ modulo $(t-1)^{d+1}$ and we use fast radix conversion to deduce the t-adic expansion of $t^d\mathbf{F}^{-1}$. □

Remark 5.10. *There exist finner complexity results about multiplication and reduction of polynomials matrices, which take into account the average degree of the rows (or columns) of the input matrices (see e.g. [44]). We don't need these improvements for our purpose.*

5.3 Revisiting Hess's algorithm

From now on, we denote $I = I(D)$ and $I_\infty = I_\infty(D)$ and we let $\mathscr{B}, \mathscr{B}^*$ and $\mathscr{B}_\infty, \mathscr{B}^*_\infty$ the triangular basis respectively defined by (5) and (7). We denote for short

$$d = \exp(I) \qquad \text{and} \qquad e = \exp(I_\infty). \tag{14}$$

(see Definition 4.6 and Definition 4.11). We thus have $d = \deg p_{n-1}$ and $e = m_{n-1}$ with notations (5) and (7).

Lemma 5.11. *Let $\mathbf{M}^*$ be the matrix of the basis $\mathscr{B}^*$ expressed in the basis $1, x, \ldots, x^{n-1}$. The matrix $\mathbf{M}^*$ is lower triangular and we have*

$$p_{n-1}\mathbf{M}^* = \tilde{\mathbf{M}}, \quad \tilde{\mathbf{M}} \in k[t]^{n\times n}, \quad \deg(\tilde{\mathbf{M}}) = d.$$

Proof. This follows straightforwardly from (5) and (14). □

Recall that we denote $u = t^{-1}$. Hence $\deg_u = -\deg_t$.

Lemma 5.12. *Let $\mathbf{N}^*$ be the matrix of the basis $\mathscr{B}_\infty^*$ expressed in the basis $1, x, \ldots, x^{n-1}$ and let λ as in (6). We have*

$$u^e \mathbf{N}^* = \tilde{\mathbf{N}} \quad \text{where} \quad \tilde{\mathbf{N}} \in k[u]^{n\times n}, \quad \deg_u(\tilde{\mathbf{N}}) \leq e + n\lambda.$$

Moreover, we have $u^{e+n\lambda}\tilde{\mathbf{N}}^{-1} \in k[u]^{n\times n}$.

Proof. Let $\mathbf{N}'$ be the matrix of $\mathscr{B}_\infty^*$ in the basis $1, y, \ldots, y^{n-1}$. As $y = xu^\lambda$, the matrix of $\mathscr{B}_\infty^*$ in the basis $1, x, \ldots, x^{n-1}$ is $\mathbf{N}^* = \mathbf{N}'\mathbf{D}$ where $\mathbf{D} = \mathrm{diag}(1, u^\lambda, \ldots, u^{(n-1)\lambda})$. It follows straightforwardly from (7) and (14) that $u^e\mathbf{N}' \in k[u]^{n\times n}$, $\deg_u(u^e\mathbf{N}') = e$. Hence, $\tilde{\mathbf{N}} = u^e\mathbf{N}'\mathbf{D} \in k[u]^{n\times n}$ and $\deg_u \tilde{\mathbf{N}} \leq \deg_u(u^e\mathbf{N}') + \deg_u \mathbf{D} \leq e + n\lambda$, as required. For the second point, we have $u^{e+n\lambda}\tilde{\mathbf{N}}^{-1} = u^{n\lambda}\mathbf{D}^{-1}\mathbf{N}'^{-1}$. Since $u^{n\lambda}\mathbf{D}^{-1} \in k[u]^{n\times n}$, we are reduced to show that $\mathbf{N}'^{-1} \in k[u]^{n\times n}$. We deduce from (7) that $\mathbf{N}' = \mathbf{D}'\mathbf{T}$ where $\mathbf{T} \in k[u]^{n\times n}$ is lower triangular with ones on the diagonal (in particular, $\mathbf{T}$ is unimodular) and where $\mathbf{D}'$ is a diagonal matrix with entries in $k[u^{-1}]$. Thus both $\mathbf{T}^{-1}$ and $\mathbf{D}'^{-1}$ lie in $k[u]^{n\times n}$ and $\mathbf{N}'^{-1} \in k[u]^{n\times n}$ as required. □

Lemma 5.13. *Let $\tilde{\mathbf{N}}_{\mathrm{red}} \in k[u]^{n\times n}$ be a row reduced form of $\tilde{\mathbf{N}}$. We have:*

(i) $\deg_u(\tilde{\mathbf{N}}_{\mathrm{red}}) \leq e + n\lambda$

(ii) $u^{e+n\lambda}\tilde{\mathbf{N}}_{\mathrm{red}}^{-1} \in k[u]^{n\times n}$

(iii) $\deg_u(u^{e+n\lambda}\tilde{\mathbf{N}}_{\mathrm{red}}^{-1}) \leq e + n\lambda$.

Given $\tilde{\mathbf{N}}$, we can compute both the matrix $\tilde{\mathbf{N}}_{\mathrm{red}}$ and its inverse $\tilde{\mathbf{N}}_{\mathrm{red}}^{-1}$ in time $\tilde{\mathscr{O}}(n^\omega(e + n\lambda))$.

Proof. Item (i) and the complexity of computing $\tilde{\mathbf{N}}_{\mathrm{red}}$ follow from Lemma 5.12 and Proposition 5.8. We have $\tilde{\mathbf{N}}_{\mathrm{red}} = \mathbf{U}\tilde{\mathbf{N}}$ with $\mathbf{U} \in k[u]^{n\times n}$ unimodular, thus $\tilde{\mathbf{N}}_{\mathrm{red}}^{-1} = \tilde{\mathbf{N}}^{-1}\mathbf{U}^{-1}$ with $\mathbf{U}^{-1} \in k[u]^{n\times n}$ and (ii) follows from Lemma 5.12. Finally (iii) and the complexity of computing $\tilde{\mathbf{N}}_{\mathrm{red}}^{-1}$ follow from (i), (ii) and Proposition 5.9. □

In the following two lemmas, we come back to the coordinate $t = u^{-1}$.

Lemma 5.14. *Let $\mathbf{P} = \tilde{\mathbf{M}}\tilde{\mathbf{N}}_{\mathrm{red}}^{-1}$. Then $\mathbf{P} \in k[t]^{n\times n}$ and $\deg_t \mathbf{P} \leq d + e + n\lambda$. We can compute $\mathbf{P}$ in time $\tilde{\mathscr{O}}(n^\omega(d + e + n\lambda))$.*

Proof. By Lemma 5.11, we have $\tilde{\mathbf{M}} \in k[t]^{n\times n}$, $\deg_t \tilde{\mathbf{M}} = d$. From Lemma 5.13 (ii) and (iii) we deduce that $\tilde{\mathbf{N}}_{\mathrm{red}}^{-1} \in k[u^{-1}]^{n\times n} = k[t]^{n\times n}$ and $\deg_t \tilde{\mathbf{N}}_{\mathrm{red}}^{-1} \leq e + n\lambda$. The result thus follows from Proposition 5.7. □

Lemma 5.15. *We can compute a row reduced form $\mathbf{P}_{\mathrm{red}} \in k[t]^{n\times n}$ of $\mathbf{P}$ in time $\tilde{\mathscr{O}}(n^\omega(d+e+n\lambda))$. We have $\deg_t(\mathbf{P}_{\mathrm{red}}) \leq d + e + n\lambda$.*

Proof. This follows from Proposition 5.8 and Lemma 5.14. □

Lemma 5.16. *Let $\mathbf{U} \in k[t]^{n\times n}$ be the unimodular matrix such that $\mathbf{P}_{\mathrm{red}} = \mathbf{U}\mathbf{P}$. We can compute $\tilde{\mathbf{M}}_{\mathrm{red}} = \mathbf{U}\tilde{\mathbf{M}} \in k[t]^{n\times n}$ in time $\tilde{\mathscr{O}}(n^\omega(d + e + n\lambda))$.*

Proof. By definition of $\mathbf{P}$ in Lemma 5.14, we have $\mathbf{U}\tilde{\mathbf{M}} = \mathbf{U}\mathbf{P}\tilde{\mathbf{N}}_{\mathrm{red}} = \mathbf{P}_{\mathrm{red}}\tilde{\mathbf{N}}_{\mathrm{red}}$. By Lemma 5.13 (i) and since $u = t^{-1}$, we deduce that $t^{e+n\lambda}\tilde{\mathbf{N}}_{\mathrm{red}} \in k[t]^{n\times n}$ has degree at most $e + n\lambda$ in t. Hence computing $t^{e+n\lambda}\mathbf{P}_{\mathrm{red}}\tilde{\mathbf{N}}_{\mathrm{red}}$ fits in the aimed bound by Lemma 5.15 and Proposition 5.7. There remains to divide the resulting matrix by $t^{e+n\lambda}$, which can be done for free. □

Remark 5.17. *Clearly, we could have studied more carefully the complexity of the various steps taking into account in particular that* $\tilde{\mathbf{N}}_{\mathrm{red}}$ *is a left multiple of the diagonal matrix* $\mathbf{D} = (1, u^{\lambda}, \ldots, u^{(n-1)\lambda})$. *This would not improve the overall cost estimate in general, but this leads to a slight improvement when the index at infinity is zero, see Subsection 5.4.*

We can now revisit Hess algorithm to get complexity estimates.

Algorithm 2 Riemann–Roch

Input: $L = k(t)[X]/(f)$ with $f \in k[t][X]$ monic and separable, and $D \in \mathrm{Div}(L)$ given by OM-representation.

Output: A compressed basis of $\mathscr{L}(D)$.

1: Compute $\tilde{\mathbf{M}} \in k[t]^{n\times n}$ as in Lemma 5.11 using Theorem 4.8.
2: Compute $\tilde{\mathbf{N}} \in k[u]^{n\times n}$ as in Lemma 5.12 using Theorem 4.13.
3: Compute a row reduced form $\tilde{\mathbf{N}}_{\mathrm{red}}$ of $\tilde{\mathbf{N}}$ in $k[u]^{n\times n}$ and compute $\tilde{\mathbf{N}}_{\mathrm{red}}^{-1}$ with Lemma 5.13.
4: Compute $\mathbf{P} = \tilde{\mathbf{M}}\tilde{\mathbf{N}}_{\mathrm{red}}^{-1} \in k[t]^{n\times n}$ with Lemma 5.14.
5: Compute a row reduced form $\mathbf{P}_{\mathrm{red}} = \mathbf{U}\mathbf{P}$ in $k[t]^{n\times n}$ with Lemma 5.15.
6: Compute $\tilde{\mathbf{M}}_{\mathrm{red}} = \mathbf{U}\tilde{\mathbf{M}}$ in $k[t]^{n\times n}$ with Lemma 5.16.
7: Compute $\mathbf{M}_{\mathrm{red}} = \frac{q}{p_{n-1}}\tilde{\mathbf{M}}_{\mathrm{red}} \in k(t)^{n\times n}$, with $q \in k(t)$ and $p_{n-1} \in k[t]$ as in (5).
8: Let $\delta = m_{n-1} - m - \deg(q/p_{n-1})$ with $m_{n-1} \in \mathbb{N}$ and $m \in \mathbb{Z}$ as in (7).
9: **return**

$$((b_i, d_i),\ 0 \le i \le n-1)$$

where $(b_0, \ldots, b_{n-1}) = \mathbf{M}_{\mathrm{red}}$ and $(d_0, \ldots, d_{n-1}) = -\operatorname{rdeg}\mathbf{P}_{\mathrm{red}} + (\delta, \ldots, \delta)$.

Recall that $b_i \in k(t)^n$ is identified with an element of $k(t)[x]$ at step 9. Using notations of Definition 4.6 and Definition 4.11, we get:

Theorem 5.18. *This algorithm returns a correct answer. It performs at most*

- $\tilde{\mathscr{O}}(n^{\omega}(\exp(I) + \exp(I_{\infty}) + n\lambda) + n^2 h(q_I))$ *operations in* k *if* $\mathrm{char}(k) = 0$ *or* $\mathrm{char}(k) > n$,
- $\tilde{\mathscr{O}}(n^{\omega}(\exp(I) + \exp(I_{\infty}) + n\lambda) + n^2 h(q_I) + \delta^2 + \delta_{\infty}^2)$ *operations in* k *otherwise.*

Proof. Correctness. Let $\mathbf{M}$ and $\mathbf{N}$ be the respective matrices of $\mathscr{B}$ and $\mathscr{B}_{\infty}$ in the canonical basis $1, x, \ldots, x^{n-1}$. With notations (5) and (7) and notations of Lemma 5.11 and Lemma 5.12, we thus have

$$\mathbf{M} = q\mathbf{M}^* = \frac{q}{p_{n-1}}\tilde{\mathbf{M}} \qquad \text{and} \qquad \mathbf{N} = u^m\mathbf{N}^* = u^{m-e}\tilde{\mathbf{N}}. \tag{15}$$

By construction, $\tilde{\mathbf{N}}_{\mathrm{red}} = \mathbf{V}\tilde{\mathbf{N}}$ for some unimodular matrix $\mathbf{V} \in k[u]^{n\times n}$. So $\mathbf{V}$ is unimodular over $A_{\infty} = k[u]_u$ and the rows of $\mathbf{N}_{\mathrm{red}} = u^{m-e}\tilde{\mathbf{N}}_{\mathrm{red}} = \mathbf{V}\mathbf{N}$ still form an A_{∞}-basis of $\mathscr{B}_{\infty}$. The matrix $\mathbf{P}_{\mathrm{red}} = \mathbf{U}\tilde{\mathbf{M}}\tilde{\mathbf{N}}_{\mathrm{red}}^{-1}$ being row reduced at step 5 (with respect to $\deg_t$), we deduce from Definition 5.1 that the matrix $\mathbf{P}_0 = \mathbf{U}\mathbf{M}\mathbf{N}_{\mathrm{red}}^{-1}$ is row reduced too since it is a K-multiple of $\mathbf{P}_{\mathrm{red}}$. It follows from Algorithm 1 and Theorem 5.6 that a compressed basis of $\mathscr{L}(D)$ is given by $(b_0, \ldots, b_{n-1}) = \mathbf{U}\mathbf{M}$ together with $(d_0, \ldots, d_{n-1}) = -\operatorname{rdeg}(\mathbf{P}_0)$. Using (15) together with $e = \exp(I_{\infty}) = m_{n-1}$ (by (7)) and $u = t^{-1}$, we get

$$\mathbf{U}\mathbf{M} = \frac{q}{p_{n-1}}\mathbf{U}\tilde{\mathbf{M}} = \mathbf{M}_{\mathrm{red}} \qquad \text{and} \qquad \mathbf{P}_0 = \frac{qt^{m-m_{n-1}}}{p_{n-1}}\mathbf{P}_{\mathrm{red}},$$

hence $(b_0, \ldots, b_{n-1}) = \mathbf{M}_{\mathrm{red}}$ and $(d_0, \ldots, d_{n-1}) = -\operatorname{rdeg}\mathbf{P}_{\mathrm{red}} + (\delta, \ldots, \delta)$ with $\delta = m_{n-1} - m - \deg(q/p_{n-1})$, as returned by Algorithm 2.

Complexity. We compute $\mathbf{M}^*$ and $\mathbf{N}^*$ in the aimed bound thanks to Theorem 4.8 and Theorem 4.13 combined with the inequalities $n\delta_I \leq n^2 \exp(I)$ and $n\delta_{I_\infty} \leq n^2 \exp(I_\infty)$ by respectively Lemma 4.7 and Lemma 4.12. Since $\deg p_{n-1} = \exp(I)$ and the n^2 entries of $\mathbf{M}^*$ have height $\mathscr{O}(\exp(I))$, we compute $\tilde{\mathbf{M}} = p_{n-1}\mathbf{M}^*$ in the aimed bound. We compute $\tilde{\mathbf{N}}$ from $\mathbf{N}^*$ for free (multiplication by a power of t). The complexity of steps 3, 4, 5, 6 fits in the aimed bound from respectively Lemma 5.13, Lemma 5.14, Lemma 5.15 and Lemma 5.16. The polynomial matrix $\tilde{\mathbf{M}}_{\text{red}}$ has degree at most $\exp(I) + \exp(I_\infty) + n\lambda$ by (the proof of) Lemma 5.16. Since $q = q_I$ and $\deg p_{n-1} = \exp(I)$, we deduce that computing $\mathbf{M}_{\text{red}}$ at step 7 fits in the aimed bound. □

Again, we could have been more careful when looking at the complexity of the various multiplications of matrices by elements of $K = k(t)$. However, this would not improve the overall cost estimate.

Remark 5.19. *Instead of performing the product at step 7, we may also return a list of (non expanded) product* $(q\tilde{b}_0, q\tilde{b}_1/p_1, \ldots, q\tilde{b}_{n-1}/p_{n-1})$ *where the* $\tilde{b}_i$ *are given by the rows of* $\tilde{\mathbf{M}}_{\text{red}}$*. In such a case, we do not need the extra term* $h(q_I)$ *in the complexity estimate. This is particularly relevant if* $\exp(I) << h(q_I)$*, that is when* D *is closed to be* K*-principal modulo* D_∞ *(see Remark 4.17).*

5.4 The case of trivial exponent at infinity

If we assume that $\exp(I_\infty) = 0$, the annoying extra term $n\lambda$ disappears in the complexity estimate of Theorem 5.18:

Theorem 5.20. *Suppose that* $\exp(I_\infty) = 0$*. We can compute a compressed basis of* $\mathscr{L}(D)$ *with*

- $\tilde{\mathscr{O}}(n^\omega \exp(I) + n^2 h(q_I))$ *operations in* k *if* $\text{char}(k) = 0$ *or* $\text{char}(k) > n$*,*
- $\tilde{\mathscr{O}}(n^\omega \exp(I) + n^2 h(q_I) + \delta^2)$ *operations in* k *otherwise.*

The proof requires to use shifted reduction of matrices instead of the usual degree reduction.

Definition 5.21. *Let* $\vec{s} = (s_0, \ldots, s_{n-1}) \in \mathbb{Z}^n$ *be a shift and* $\mathbf{E} \in k(t)^{n\times n}$*. The matrix* $\mathbf{E}$ *is said to be row* $\vec{s}$*-reduced if* $\mathbf{ED}$ *is row reduced, where* $\mathbf{D} = \text{diag}(t^{s_0}, \ldots, t^{s_{n-1}})$*.*

The shift is used as column weights.

Theorem 5.22 ([44])**.** *Let* $\mathbf{E} \in k[t]^{n\times n}$ *of degree* d*. We can compute a row* $\vec{s}$*-reduced form of* $\mathbf{E}$ *in time* $\tilde{\mathscr{O}}(n^\omega d)$*.*

It is remarkable that the complexity estimate does not depend on the shift $\vec{s}$.

Proof of Theorem 5.20. The hypothesis $\exp(I_\infty) = 0$ is equivalent to $\delta_{I_\infty} = 0$ thanks to Lemma 4.12, that is $\deg[A_\infty[y] : I^*_\infty] = 0$ by Definition 4.11. Since, $A_\infty[y] \subset I^*_\infty$, we get $A_\infty[y] = I^*_\infty$ by Lemma 4.3. Hence $\tilde{\mathbf{N}} = \mathbf{D} = \text{diag}(1, u^\lambda, \ldots, u^{(n-1)\lambda})$ is diagonal (hence reduced), so the algorithm simplifies. The matrix $\tilde{\mathbf{M}}_{\text{red}}$ of step 6 in Algorithm 2 coincides with the row $\vec{s}$-reduced form of $\tilde{\mathbf{M}}$ where $\vec{s} = (1, \lambda, \ldots, (n-1)\lambda)$, and we may replace steps 3, 4, 5, 6 by simply computing the row $\vec{s}$-reduced form of $\tilde{\mathbf{M}}$, with complexity $\tilde{\mathscr{O}}(n^\omega \exp(I))$ by Theorem 5.22. Note that $\tilde{\mathbf{N}}_{\text{red}} = \mathbf{D}$, hence $\mathbf{P}_{\text{red}} = \tilde{\mathbf{M}}_{\text{red}}\mathbf{D}^{-1}$. Thus $\text{rdeg}\,\mathbf{P}_{\text{red}} = \text{rdeg}\,\tilde{\mathbf{M}}_{\text{red}} + (1, \lambda, \ldots, (n-1)\lambda)$ is deduced for free from the row-degree of $\tilde{\mathbf{M}}_{\text{red}}$. □

5.5 An example

Let us illustrate Algorithm 2 on a concrete example. Let $f = X^3 - X^2 + t^2 \in \mathbb{F}_5(t)[X]$ as in Example 3.13.

• Let $p = tA$. We saw in Example 3.13 that there are three primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ lying above p, with OM-representation $t_{\mathfrak{p}_1} = [t, x-t]$, $t_{\mathfrak{p}_2} = [t, x+t]$ and $t_{\mathfrak{p}_3} = [t, x-1]$. We have for instance $tB = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ and $(x-1)B = \mathfrak{p}_3^2$.

• Let $p' = (t-1)A$. There are exactly two primes $\mathfrak{p}'_1, \mathfrak{p}'_2$ lying above p', with OM-representation $t_{\mathfrak{p}'_1} = [t-1, x+3]$ and $t_{\mathfrak{p}'_2} = [t-1, x, x^2+x+2]$. We have $(t-1)B = \mathfrak{p}'_1\mathfrak{p}'_2$.

• Let $p_\infty = t^{-1}A_\infty$. Following (6), we have $\lambda = 1$, $y = xt^{-1}$ and $y^3 - t^{-1}y^2 + t^{-1} = 0$. There is a unique prime $\mathfrak{p}_\infty$ above p_∞, with OM-representation $\mathfrak{p}_\infty = [t^{-1}, y, y^3 + t^{-1}]$. We have $t^{-1}B_\infty = \mathfrak{p}_\infty^3$ and $yB_\infty = \mathfrak{p}_\infty$.

Let us compute the Riemann–Roch space associated to the divisor $D = 2\mathfrak{p}_1 + 3\mathfrak{p}_2 - \mathfrak{p}'_1 - \mathfrak{p}'_2 + \mathfrak{p}_\infty \in \mathrm{Div}(\mathbb{F}_5(t)[X]/f)$.

Step 1. We have $I = I(D) = \mathfrak{p}_1^{-2}\mathfrak{p}_2^{-3}\mathfrak{p}'_1\mathfrak{p}'_2$. Using the computer algebra system SageMath, we find that this fractional ideal has basis

$$\mathscr{B} = (t-1)\mathscr{B}^*, \qquad \text{with} \qquad \mathscr{B}^* = \left(1, \frac{x-1}{t^2}, \frac{x^2 - (t+1)x + t(1+t-t^2)}{t^4}\right).$$

We have $I^* = \mathfrak{p}_1^{-2}\mathfrak{p}_2^{-3}$, $q = t-1$, $p_{n-1} = t^4$ and

$$\tilde{\mathbf{M}} = \begin{pmatrix} t^4 & 0 & 0 \\ -t^2 & t^2 & 0 \\ t(1+t-t^2) & -(t+1) & 1 \end{pmatrix}.$$

Step 2. We have $I_\infty = I_\infty(D) = \mathfrak{p}_\infty^{-1}$. This fractional ideal is normalized and has basis

$$\mathscr{B}_\infty = \mathscr{B}_\infty^* = \left(1, y, ty^2\right) = \left(1, \frac{x}{t}, \frac{x^2}{t}\right).$$

We have $m = 0$, $m_{n-1} = 1$ and

$$\tilde{\mathbf{N}} = \begin{pmatrix} 1/t & 0 & 0 \\ 0 & 1/t^2 & 0 \\ 0 & 0 & 1/t^2 \end{pmatrix}.$$

Step 3. The matrix $\tilde{\mathbf{N}}$ is diagonal, thus row reduced, and the inverse of $\tilde{\mathbf{N}} = \tilde{\mathbf{N}}_{\mathrm{red}}$ is obvious.

Step 4. We compute

$$\mathbf{P} = \tilde{\mathbf{M}} \times \tilde{\mathbf{N}}^{-1} = \begin{pmatrix} t^5 & 0 & 0 \\ -t^3 & t^4 & 0 \\ t^2(1+t-t^2) & -t^2(t+1) & t^2 \end{pmatrix}.$$

Step 5. The matrix $\mathbf{P}$ is not row reduced. Indeed, $\deg(\det(\mathbf{P})) = 11 < |\mathrm{rdeg}(\mathbf{P})| = 13$. We compute a row reduced form of $\mathbf{P}$:

$$\mathbf{P}_{\mathrm{red}} = \begin{pmatrix} t^3 + t^2 & -2t^3 - t^2 & t^2(t+1) \\ -t^3 & t^4 & 0 \\ 0 & -t^4 & t^4 + t^2 \end{pmatrix}.$$

Step 6. We compute the product $\tilde{\mathbf{M}}_{\text{red}} = \mathbf{P}_{\text{red}} \times \tilde{\mathbf{N}}$:

$$\tilde{\mathbf{M}}_{\text{red}} = \begin{pmatrix} t^2+t & -2t-1 & t+1 \\ -t^2 & t^2 & 0 \\ 0 & -t^2 & t^2+1 \end{pmatrix}.$$

Step 7. We obtain the following elements, corresponding to the lines of $\mathbf{M}_{\text{red}} = \frac{q}{p_{n-1}}\tilde{\mathbf{M}}_{\text{red}}$:

$$b_0 = \frac{t^2-1}{t^2} + x\frac{(3t-1)(t-1)}{t^4} + x^2\frac{t^2-1}{t^4},\ b_1 = \frac{1-t}{t^2} + x\frac{t-1}{t^2} \text{ and } b_2 = x\frac{1-t}{t^2} + x^2\frac{(t^2+1)(t-1)}{t^4}.$$

Step 8. We have $\delta = 4$ and $\text{rdeg}(\mathbf{P}_{\text{red}}) = (3,4,4)$, hence $(d_0, d_1, d_2) = (1,0,0)$.

Result: A k-basis of $\mathscr{L}(D)$ is (b_0, tb_0, b_1, b_2).

6 Arithmetic vs Geometry (proof of Theorem 1.1)

The complexity given in Theorem 1.1 is stated in terms of the delta invariant of a projective plane curve. To this aim, we need to relate curves and function fields. More details are given in Appendix B.

6.1 Curves vs function fields

Let $\mathscr{C} \subset \mathbb{P}^2_k$ be a degree n irreducible projective plane curve defined by a degree n homogeneous polynomial $F \in k[X_0, X_1, X_2]$. We denote $k(\mathscr{C})$ the field of rational functions of $\mathscr{C}$. The elements of $k(\mathscr{C})$ are quotients G/H of homogeneous polynomials of the same degrees, with $H \mod F \neq 0$, and modulo the equivalence relation $G/H \sim G'/H'$ if $GH' - G'H = 0 \mod F$. The field $k(\mathscr{C})$ is a function field over k (and every function field arises in such a way).

Definition 6.1. *A divisor of $\mathscr{C}$ is a divisor of the function field $k(\mathscr{C})$ of $\mathscr{C}$.*

Equivalently, a divisor of $\mathscr{C}$ can be seen as a $\mathbb{Z}$-combination of closed points of the normalization $\overline{\mathscr{C}}$ of $\mathscr{C}$ (Theorem B.10). If $\mathscr{C}$ is smooth and k is algebraically closed, a divisor is simply a $\mathbb{Z}$-combination of points on a curve, the usual way to think a divisor.

Let us assume that $F \neq X_0$. Denoting $t = X_1/X_0$ and $X = X_2/X_0$, the restriction of $\mathscr{C}$ to the affine chart $U_0 = \{X_0 \neq 0\} \simeq \mathbb{A}^2_k$ can be identified with the affine curve $C \subset \mathbb{A}^2_k$ defined by

$$C = \operatorname{Spec} k[t,X]/(f) \quad \text{where} \quad f(t,X) = F(1,t,X) \in k[t,X].$$

The coordinate ring of C is $k[C] = k[t,X]/(f)$ and its function field is $k(C) = \operatorname{Frac} k[C]$. With notations $A = k[t]$, $K = k(t)$ and $x = X \mod f$ used in the previous sections, we thus have

$$k[C] = A[x] \quad \text{and} \quad k(C) = K(x).$$

Dehomogenization induces an isomorphism $k(\mathscr{C}) \simeq k(C)$. It identifies closed points of $\mathscr{C} \cap U_0$ with closed points of C and induces isomorphisms of local rings $\mathscr{O}_{\mathscr{C},P} \simeq \mathscr{O}_{C,P}$ for such points. Note that a closed point $P \in C$ is by definition a maximal ideal of $k[C]$ and the local ring of C at P is $\mathscr{O}_{C,P} = k[C]_P$ (see Section B.1).

6.2 Bounds for the indices of B and B_∞

In order to prove Theorem 1.1, there remains to relate the indices $\delta = \deg[B : A[x]]$ and $\delta_\infty = \deg[B_\infty : A_\infty[y]]$ of f as defined in Definition 4.6 and Definition 4.11 with the delta-invariant of the input projective plane curve $\mathscr{C}$ (Definition B.14). We denote $\overline{\mathscr{O}_{\mathscr{C},P}}$ the integral closure of $\mathscr{O}_{\mathscr{C},P}$.

Proposition 6.2. *Suppose F monic and separable in X_2. With notations as above, we have:*

1. $\delta = \sum_{P \in \mathscr{C} \cap U_0} \dim_k \overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}$.
2. $\delta_\infty = \sum_{P \in \mathscr{C} \setminus \mathscr{C} \cap U_0} \dim_k \overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}$.

Note that according to Proposition B.2, $\overline{\mathscr{O}_{\mathscr{C},P}} = \mathscr{O}_{\mathscr{C},P}$ if and only if P is a regular point of $\mathscr{C}$, hence the sums hold over the finite set of singular points of $\mathscr{C}$.

Proof. Let us show point 1. Let B be the integral closure of A in $L = k(C)$. As $A \subset A[x] = k[C]$, we have $B \subset \overline{k[C]}$. By hypothesis, $f(t, X) = F(1, t, X)$ is monic and separable in X. Hence x is integral over A which forces $A[x] \subset B$, that is $k[C] \subset B$. As B is integrally closed, it follows that $\overline{k[C]} \subset B$, hence $\overline{k[C]} = B$. In other words, B coincides with the coordinate ring of the normalization $\overline{C}$ of C. We thus have

$$\delta = \deg[B : A[x]] = \dim_k(B/A[x]) = \dim_k(\overline{k[C]}/k[C]). \tag{16}$$

A closed point $P \in \mathscr{C} \cap U_0 \simeq C$ is by definition a maximal ideal of $k[C] = A[x]$ and we have $\mathscr{O}_{\mathscr{C},P} \simeq k[C]_P = A[x]_P$ (localization at P). As integral closure commutes with localization, we have an isomorphism of semi-local ring $\overline{\mathscr{O}_{\mathscr{C},P}} \simeq \overline{k[C]}_P = B_P$ and we get

$$\dim_k(\overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}) = \dim_k(B_P/A[x]_P). \tag{17}$$

We now follow the proof of [38, Thm.4.17]. Let $a \in A[x]$ such that $aB \subset A[x]$. Thus $aA[x]$ and aB are both ideals of $A[x]$, and we have an inclusion $aA[x] \subset aB$. The k-algebra $A[x]/aA[x]$ being finitely generated and zero-dimensional, it has a finite number of maximal ideals. Thus, the Chinese remainder theorem (see [38, Cor.D.4]) ensures that

$$A[x]/aA[x] = \prod_{P \in \operatorname{Spec} A[x]} A[x]_P/aA[x]_P$$

and $aB/aA[x]$ identifies with $\prod_{P \in \operatorname{Spec} A[x]} aB_P/aA[x]_P$. Recall that $C = \operatorname{Spec} A[x]$. We obtain

$$\dim_k(B/A[x]) = \dim_k(aB/aA[x]) = \sum_{P \in C} \dim_k(aB_P/aA[x]_P) = \sum_{P \in C} \dim_k(B_P/A[x]_P)$$

which combined with (16) and (17) concludes for the first point.

Let us show point 2. Since F is monic in X_2, we have $F(0 : 0 : 1) \neq 0$. Thus $(0 : 0 : 1) \notin \mathscr{C}$ and all points of $\mathscr{C} \setminus \mathscr{C} \cap U_0 = \mathscr{C} \cap (X_0 = 0)$ (the points at infinity) belong to the affine chart $U_1 = \{X_1 \neq 0\}$. Denoting $u = X_0/X_1 = t^{-1}$ and $Y = X_2/X_1 = Xt^{-1}$, the affine equation of $\mathscr{C}$ in the chart $U_1 \simeq \mathbb{A}^2_k$ is given by the polynomial

$$f_\infty \in k[u, Y], \quad f_\infty(u, Y) = u^n f(u^{-1}, u^{-1}Y).$$

The residue class y of Y modulo f_∞ satisfies $y = xt^{-1}$ in $L = k(t, x) = k(u, y)$. As f has total degree n, the integer $\lambda = \lambda(f)$ defined in (6) satisfies $\lambda = 1$ and Definition 4.11 becomes

$$\delta_\infty = \deg[B_\infty : A_\infty[y]],$$

where $u = t^{-1}$, $y = xt^{-1}$, $A_\infty = k[u]_{(u)}$ and B_∞ is the integral closure of A_∞ in L. The line at infinity $X_0 = 0$ has local equation $u = 0$ and the points of $\mathscr{C} \setminus \mathscr{C} \cap U_0 = \mathscr{C} \cap (X_0 = 0)$ are in one-to-one correspondence with the maximal ideals of $k[u, y]$ containing u, hence with the maximal ideals P of $A_\infty[y]$. By the same reasoning as above, we get

$$\dim_k(B_\infty/A_\infty[y]) = \sum_{P \in \mathscr{C} \setminus \mathscr{C} \cap U_0} \dim_k(B_{\infty,P}/A_\infty[y]_P).$$

and we conclude thanks to the isomorphisms $A_\infty[y]_P \simeq \mathscr{O}_{\mathscr{C},P}$ and $B_{\infty,P} \simeq \overline{\mathscr{O}_{\mathscr{C},P}}$. □

Denote by $\delta(\mathscr{C})$ the delta invariant of $\mathscr{C}$ and by $g(\mathscr{C})$ its geometric genus, as defined in Section B.6. We get:

Corollary 6.3. *Suppose F monic and separable in X_2. Then $\delta + \delta_\infty = \delta(\mathscr{C}) = \frac{(n-1)(n-2)}{2} - g(\mathscr{C})$.*

Proof. First equality follows from Proposition 6.2 and Definition B.14. Second equality follows from the genus formula (Corollary B.16). □

6.3 Proof of Theorem 1.1

Theorem 1.1 follows immediately from the slightly more general result.

Theorem 6.4. *Let $\mathscr{C} \subset \mathbb{P}^2(k)$ be an irreducible curve of degree n defined by an homogeneous polynomial F monic and separable in X_2. Let $D \in Div(\mathscr{C})$. There exists a deterministic algorithm which computes a compressed basis (Definition 5.4) of $\mathscr{L}(D)$ with*

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \deg(D^-) + \delta(\mathscr{C}) + n)) \subset \tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \deg(D^-) + n^2))$$

arithmetic operations in k. If $\deg D \geq 0$, the complexity becomes

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \delta(\mathscr{C}) + n)).$$

If moreover the singular locus of $\mathscr{C}$ and the support of D are contained in the affine chart $X_0 \neq 0$, the complexity becomes

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \delta(\mathscr{C}))).$$

Proof. We have $\lambda(f) = 1$ in this setting. Hence, the first result follows straightforwardly from Theorem 5.18 combined with Proposition 4.15 and Corollary 6.3. The second statement (that is Theorem 1.1) follows immediately since $\deg D \geq 0$ implies $\deg D^- + \deg D^+ \leq 2 \deg D^+$. The last estimate follows from Theorem 5.20. □

We may want to store all elements of a k-basis of $\mathscr{L}(D)$. We get the following size estimate.

Proposition 6.5. *Suppose $\mathscr{C}$ irreducible over $\bar{k}$. Given a compressed basis of $\mathscr{L}(D)$, we can compute (meaning we can store) a k-basis of $\mathscr{L}(D)$ in time*

$$\mathscr{O}(n(\deg(D) + 1)(\deg(D^+) + \delta(\mathscr{C}) + n))$$

(that is zero cost if $\deg D < 0$).

Proof. The complexity is that of writting all elements of the set $\{t^j b_i \,|\, 0 \leq j \leq d_i, 0 \leq i \leq n-1\}$. This set has cardinality $\ell(D) = \dim \mathscr{L}(D)$. If $\ell(D) = 0$, there is nothing to do. Otherwise, $\deg D \geq 0$, hence $\deg D^+ + \deg D^- \leq 2 \deg D^+$. Thus each element $t^j b_i \in \mathscr{L}(D)$ has arithmetic size $n(\deg D^+ + \delta(\mathscr{C}) + n)$ by (the proof) of Theorem 5.18 and Corollary 6.3. The assumption $\mathscr{C}$ irreducible over $\bar{k}$ is equivalent to k is algebraically closed in L. In such a case, it is well known that $\ell(D) \leq \deg(D) + 1$ (see e.g. [63, Prop.1.4.9 and Eq.1.21]), which concludes the proof. □

Remark 6.6. *If $\mathscr{C}$ is only irreducible over k, its number of irreducible factors over $\bar{k}$ is $\rho = [k_0 : k] = \dim \mathscr{L}(0)$ where $k \subset k_0 \subset L$ is the field of constants, algebraic closure of k in L. In such a case, we have the inequality $\ell(D) \leq \deg D + \rho$ by (the proof of) [63, Prop.1.4.9] and we have to replace the factor $\deg D + 1$ by $\deg D + \rho$ in Proposition 6.5. For instance, the curve defined by $f = X^2 - 2t^2$ is irreducible over $\mathbb{Q}$, but has $\rho = 2$ irreducible components over $\bar{\mathbb{Q}}$. The space of constant functions is $\mathscr{L}(0) = k_0 \simeq k(\sqrt{2})$, with k-basis $(1, x/t)$ and dimension $\ell(0) = 2$.*

6.4 Reduction to the monic separable case

For the sake of completeness, let us explain how one can reach the monic and separable assumption of Theorem 6.4 given an arbitrary projective plane curve.

Lemma 6.7. *Let $F \in k[X_0, X_1, X_2]$ irreducible, homogeneous of degree $n > 0$. Suppose that $\mathrm{Card}(k) > n$. We can compute two distinct rational points $P, P' \in \mathbb{P}^2(k)$ such that $F(P) \neq 0$ and $F(P') \neq 0$ in time $\mathscr{O}(n^2)$.*

Proof. Let $f(t, X) = F(1, t, X)$. We can write $f = \sum f_i(t) X^i$ with $\deg f_i \leq n - i$. Evaluating f_i at $t = 0$ and $t = 1$ with Horner's rule costs $\mathscr{O}(n)$ operations. Summing over i, we compute $f(0, X)$ and $f(1, X)$ in time $\mathscr{O}(n^2)$. Let $\alpha_0, \ldots, \alpha_n$ be distinct elements of k. Evaluating $f(0, X)$ and $f(1, X)$ at $\alpha_0, \ldots, \alpha_n$ costs $\tilde{\mathscr{O}}(n)$ operations using fast multi-point evaluation. Since each polynomial has degree at most n, there exists $\alpha = \alpha_i$ and $\alpha' = \alpha_j$ such that $f(0, \alpha) \neq 0$ and $f(1, \alpha') \neq 0$. The points $P = (1 : 0 : \alpha)$ and $P' = (1 : 1 : \alpha')$ satisfy the required assumptions. □

Lemma 6.8. *Let P, P' as above. There exists a projective automorphism $\tau : \mathbb{P}^2_k \to \mathbb{P}^2_k$ which sends $(0, 1, 0)$ to P and $(0, 0, 1)$ to P'. We can compute $\tilde{F} = F \circ \tau$ in time $\tilde{\mathscr{O}}(n^2)$. The polynomial $\tilde{F}$ is homogeneous of degree n, irreducible, and monic (up to multiplication by a non zero scalar) of degree n both with respect to X_1 and X_2*

Proof. First claim is clear: this amounts to find an invertible linear map from $\mathbb{A}^3 \to \mathbb{A}^3$ which maps two given non zero vectors to two given non zero vectors. Computing τ is negligible and the second claim is proved for instance in [4, Lem.2.5]. Of course, $\tilde{F}$ remains homogeneous of degree n and irreducible. By construction, we have $\tilde{F}(0, 1, 0) = F(P) \neq 0$ and $\tilde{F}(0, 0, 1) = F(P') \neq 0$. This exactly means that the monomials X_1^n and X_2^n appear in $\tilde{F}$ with a non zero coefficient. □

Lemma 6.9. *Let $F \in k[X_0, X_1, X_2]$ be homogeneous of degree $n > 0$, irreducible, and monic of degree n in X_1 and X_2. If k is perfect, then F is separable with respect to X_1 or separable with respect to X_2.*

Proof. Suppose on the contrary that F is not separable w.r.t X_1 and X_2. Since F is irreducible, we thus have $\partial_{X_1} F = \partial_{X_2} F = 0$. Since F is monic of degree n in X_1, this forces $p = \mathrm{char}(k)$ to divide n and the Euler formula $\sum X_i \partial_{X_i} F = nF = 0$ forces $\partial_{X_0} F = 0$. Finally, we get $F = G(X_0^p, X_1^p, X_2^p)$ for some G. Since k is perfect, this leads to $F = G^p$, contradicting that F is irreducible. □

We are led to the following result.

Proposition 6.10. *Let $F \in k[X_0, X_1, X_2]$ irreducible, homogeneous of degree $n > 0$. If $\mathrm{Card}(k) > n$, we can compute in time $\tilde{\mathscr{O}}(n^2)$ a polynomial $f \in k[t, X]$ of total degree n, separable and monic of degree n with respect to X such that $k(\mathscr{C}) \simeq k(t)[X]/(f)$.*

Proof. We compute P, P' as in Lemma 6.7 and consider $\tilde{F}$ as in Lemma 6.8. Following Lemma 6.9, we let $f(t, X) = \tilde{F}(1, t, X)$ if $\tilde{F}$ is separable with respect to X_2 or $f = \tilde{F}(1, X, t)$ if $\tilde{F}$ is separable with respect to X_1. □

If $\mathrm{Card}(k) < n$, we may have $F(P) = 0$ for all $P \in \mathbb{P}^2_k$ (filling curves), in which case Lemma 6.7 can consider a finite extension k' of k such that $\mathrm{Card}(k') > n$ and $[k' : k] \in O(\log(n))$. Since F is irreducible over k, its irreducible factors over k' are conjugate over k and it's straightforward to check that Lemma 6.9 still holds in this context. Thus we are led to compute a basis of

$$\mathscr{L}(D) \otimes k' \simeq \mathscr{L}(D')$$

where D' is the divisor of the curve $\mathscr{C}' = \mathscr{C} \otimes k'$ defined by a degree n homogeneous polynomial $G \in k'[X_0, X_1, X_2]$ which is separable and monic of degree n in X_2. The curve $\mathscr{C}'$ is not necessarily irreducible over k' but the all algorithm works exactly in the same way. The cost estimate is multiplied at most by a logarithmic factor $O(\log(n))$. In order to recover a basis of $\mathscr{L}(D)$ from a basis of $\mathscr{L}(D) \otimes k'$ we can use for instance the relative trace map

$$\mathrm{Tr}_{k'/k} : \mathscr{L}(D) \otimes k' \to \mathscr{L}(D).$$

A choice of a random basis of $\mathscr{L}(D) \otimes k'$ will lead to a k-basis of $\mathscr{L}(D)$ with probability $\geq 1/4$. We refer to [4, Sec.7.5] for details (see also [35] for a deterministic approach).

Remark 6.11. *Since $A = k[t]$ is a k-algebra of finite type, the fractional ideals of B are always free A-module of rank $n = [L : K]$ by [14, Ch.V,§2,no2, thm.2]. This suggests that the hypotheses monic and separable could be dropped. This would require to adapt the OM algorithm and the computation of integral bases in this larger context, which is beyond the scope of this paper. This would be of deep interest, since then our algorithm would work for any irreducible polynomial F, avoiding any change of coordinates and any base field extension.*

A Appendix: valuation rings and integral closures

A common ingredient of geometric and arithmetic approaches is the notion of integral closure. Let us briefly remind the main properties we need.

Definition A.1. *Let S be a ring and $R \subset S$ a subring. An element $x \in S$ is integral over R if it is the root of a* monic *polynomial $f \in R[X]$. The set of integral elements of S over R is called the integral closure of R in S. We say that R is integrally closed in S if it coincides with its integral closure in S. If R is integrally closed in its total ring of fractions, we say simply that R is integrally closed.*

Proposition A.2. *[8, Cor 5.3 and Cor. 5.5] Let S be a ring and let $R \subset S$ be a subring. The integral closure of R in S is a subring of S that contains R and that is integrally closed in S.*

For a ring R, we denote Spec R the set of maximal ideals of R. For $\mathfrak{p} \in \mathrm{Spec}\, R$, we let $R_{\mathfrak{p}}$ be the localization of R at $\mathfrak{p}$ (i.e. at the multiplicative subset $R \setminus \{\mathfrak{p}\}$). It is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.

Proposition A.3. *[8, Prop 5.13] An integral domain R is integrally closed if and only if all local rings $R_{\mathfrak{p}}$, $\mathfrak{p} \in \mathrm{Spec}\, R$ are integrally closed.*

Connection between integral closures and valuation rings starts with the following elementary result:

Lemma A.4. *A valuation ring is integrally closed.*

Proof. Let $\mathscr{O}$ be a valuation ring. Let $x \in \mathrm{Frac}(\mathscr{O})$ such that $x^n = a_{n-1}x^{n-1} + \cdots + a_0$, where $a_i \in \mathscr{O}$. If $x \notin \mathscr{O}$, then $x^{-1} \in \mathscr{O}$ by definition of a valuation ring. Dividing by x^{n-1}, we get $x = a_{n-1} + \cdots + a_0 x^{1-n} \in \mathscr{O}$, a contradiction. □

The following result gives a characterization of the discrete valuation rings of a function field:

Proposition A.5. *[8, Prop.9.2] Let $\mathscr{O}$ be a Noetherian local ring of dimension one. Then $\mathscr{O}$ is a discrete valuation ring if and only if it is integrally closed.*

Integrally closed rings are of particular importance for our purpose, due to the following results (see e.g. [8, Cor 5.22]):

Proposition A.6. *The integral closure of a subring R of a field L is the intersection of all valuation rings of L containing R.*

Let us assume now that R is a subring of a function field L/k, with $k \subset R$. The previous proposition says that $b \in L$ is integral over R if and only if $v(b) \geq 0$ for all valuations v of L which are positive on R.

Proposition A.7. *The integral closure $\overline{R}$ of R in L is a finite R-module and the map*

$$\mathrm{Spec}\,\overline{R} \to \mathrm{Spec}\,R, \quad \mathfrak{p} \mapsto \mathfrak{p} \cap R$$

is well-defined, surjective, and finite. Moreover this map is one-to-one above (at least) all $\mathfrak{m} \in \mathrm{Spec}\,R$ such that $R_{\mathfrak{m}}$ is a valuation ring (i.e. integrally closed).

Proof. If R is a field, then $\overline{R}$ is a field which is a finite extension of R and the proposition is obvious in such a case. If R is not a field, then R is a finitely generated k-algebra of Krull dimension one, and $\overline{R}$ is again a finite R-module by the finiteness theorem (see e.g. [56, Thm.9, p.267]). The claims then follow from [38, Lem.F.9 and Thm.F.10] □

Definition A.8. *The* center *of a place $P \in V_L$ on R is the set $\mathfrak{p} = P \cap R$, that is the set of "functions" $b \in R$ which vanish at P.*

The center of a place is a prime ideal of R. In what follows, we say that a subring $S \subset L$ lies over R if $R \subset S$.

Proposition A.9. *Suppose that R is not a field. Let $\overline{R}$ be the integral closure of R in L and let $P \in V_L$. The following conditions are equivalent:*

(a) The center $\mathfrak{p} = P \cap R$ is not the zero ideal;
(b) The center $\mathfrak{p} = P \cap R$ is a maximal ideal of R;
(c) The valuation ring $\mathscr{O}_P$ lies over R;
(d) The valuation ring $\mathscr{O}_P$ lies over $\overline{R}$.

We say then that P is centered on R and that P lies over $\mathfrak{p}$.

Proof. $a) \Leftrightarrow b)$ follows from the fact that R has Krull dimension one since $k \subset R \subset L$ is not a field. $d) \Rightarrow c)$ is clear since $R \subset \overline{R}$. Let us show $c) \Rightarrow d)$. If $R \subset \mathscr{O}_P$, then any element of L which is integral over R is a fortiory integral over $\mathscr{O}_P$, hence $\overline{R} \subset \overline{\mathscr{O}_P}$. But $\overline{\mathscr{O}_P} = \mathscr{O}_P$ by Lemma A.4. We recall that $\mathscr{O}_P = \{a \in L \mid a^{-1} \notin P\}$. Let us prove $c) \Rightarrow a)$. Let $R \subset \mathscr{O}_P$. If $P \cap R = \{0\}$, then $a^{-1} \in \mathscr{O}_P$ for all nonzero $a \in R$ which leads to $L \subset \mathscr{O}_P$. It is not possible, so $P \cap R$ is not the zero ideal. At last, we show $b) \Rightarrow c)$. Suppose that there exists $a \in R$ such that $a \notin \mathscr{O}_P$. In particular, $a \notin \mathfrak{p}$. Since $\mathfrak{p}$ is a maximal ideal of R there exists $b \in R$ satisfying $ab - 1 \in \mathfrak{p}$. However, $a \notin \mathscr{O}_P$ so $b \notin \mathscr{O}_P^\times$, hence $b \in \mathfrak{p}$ follows. This leads to $1 \in \mathfrak{p}$, which is absurd, so no such element a exists. □

Proposition A.10. *Let $V_L(R)$ be the set of places centered on R. Suppose that* $\mathrm{Frac}(R) = L$. *The map*

$$V_L(R) \to \mathrm{Spec}\, \overline{R}, \quad P \mapsto \mathfrak{p} = P \cap \overline{R}$$

is bijective, and we have $\mathscr{O}_P = \overline{R}_{\mathfrak{p}}$ and $P = \mathfrak{p}\overline{R}_{\mathfrak{p}}$.

Proof. We have $V_L(R) = V_L(\overline{R})$ by items (c) and (d) of Proposition A.9, hence we may suppose that $R = \overline{R}$. The result follows from [63, Prop.3.2.9]. □

B Appendix: places vs closed points on curves

Warning: we denote here by P or Q closed points of curves, which are not to be confused with places of function fields.

B.1 Affine curves and closed points

Let k be a perfect field and $\bar{k}$ be an algebraic closure. Let $R = k[X_1, \ldots, X_n]$ be the polynomial ring in n variables and let us consider the affine n-space

$$\mathbb{A}^n_k = \mathrm{Spec}\ R.$$

A closed point $P \in \mathbb{A}^k_n$ is by definition a maximal ideal of R. Alternatively, we can think P as the set of points in $\bar{k}^n$ at which all functions in P vanish: this set is a Galois orbit of a point in $\bar{k}^n$ under $\mathrm{Gal}(\bar{k}/k)$. Conversely, given a Galois orbit in $\bar{k}^n$, the set of all polynomials in R vanishing at any (thus all) points of the orbit is a maximal ideal of R (Nullstellensatz). An affine curve over k is a one-dimensional integral subscheme $C \subset \mathbb{A}^k_n$, that is

$$C = \mathrm{Spec}\ R/I$$

where $I \subset R$ is a prime ideal of height $n-1$. A closed point of C is now a maximal ideal of R/I, or equivalently a maximal ideal of R containing I by the correspondence theorem. Again, a closed point $P \in C$ can be thought as a Galois orbit of a point of the variety (the geometric curve)

$$C(\bar{k}) = \{a \in \bar{k}^n,\ f(a) = 0\ \forall\ f \in I\}.$$

The ring of regular functions on C, or coordinate ring of C, is

$$k[C] = R/I.$$

As I is assumed to be prime, $k[C]$ is an integral domain. We call its field of fractions the field of rational functions of C, denoted by $k(C)$. It is a function field and every function field is isomorphic to a field of shape $k(C)$. The local ring of C at a closed point $P \in C$ is the localization $k[C]_P$ of $k[C]$ at the maximal ideal P, usually denoted $\mathscr{O}_{C,P}$. We thus have inclusions

$$k[C] \subset \mathscr{O}_{C,P} \subset k(C).$$

The field $k_P = \mathscr{O}_{C,P}/P\mathscr{O}_{C,P} \simeq k[C]/(P)$ is the residue field of P, which is a finite extension of k. If $h \in \mathscr{O}_{C,P}$, we say that h is regular at P. This terminology is justified by the fact that the evaluation map

$$ev_P : \mathscr{O}_{C,P} \to k_P, \quad ev_P(h) = h \mod P$$

is well defined. We write also $h(P) = ev_P(h)$. We say that h vanishes at P if $h(P) = 0$, that is if $h \in P$. Note that if $k = \bar{k}$ then $P = (X_1 - a_1, \ldots, X_n - a_n)$ can be identified with $a = (a_1, \ldots, a_n) \in C(\bar{k})$ and $h(P)$ is canonically identified with $h(a)$, usual evaluation of a function at a point.

Remark B.1. *The scheme C is endowed with a topology: the closed subsets of C are C itself or finite unions of closed points. It comes also with a structural sheaf $\mathscr{O}_C$ on the topological space C, where for an open set $U \subset C$, $\mathscr{O}_C(U) \subset k(C)$ is the subring of functions regular at all $P \in U$. The stalk at P is the local ring $\mathscr{O}_{C,P}$. These are crucial data, especially to define morphisms between schemes. However, we deliberately don't go into these details here, and we mainly consider poorly C as a set. See any book of algebraic geometry for more details.*

B.2 Regular and singular points.

The local rings $\mathscr{O}_{C,P}$ are not necessarily valuation rings. Indeed, we have the following classical characterization [8, Prop.9.2, p.94]:

Proposition B.2. *Let $P \in C$ be a closed point. The following assertions are equivalent:*
(a) The ring $\mathscr{O}_{C,P}$ is a discrete valuation ring.
(b) The ring $\mathscr{O}_{C,P}$ is integrally closed.
(c) If $I = (f_1, \ldots, f_r)$, the partial derivatives of the f_i's do not all vanish at P.

We say that P is a *regular point* of C if it satisfies one of these conditions. Otherwise, we say that P is a singular point. By (c), P is a regular point if and only if the geometric curve $C(\bar{k})$ is smooth (in the usual sense) at all points of the Galois orbit defined by P. A closed point is singular if it's not regular. A curve C is regular (or smooth) if it has no singular points. Otherwise, we say that C is singular. The set of singular points on a curve C is finite. By combining Proposition A.3 and Proposition B.2, we get the classical result:

Proposition B.3. *An affine curve C is smooth if and only if $k[C]$ is integrally closed.*

Note that a regular point $P \in C$ defines in particular a discrete rank one valuation $v_P : k(C) \to \mathbb{Z} \cup \{\infty\}$. Thus it makes sense to talk about the vanishing order or the pole order of a rational function $h \in k(C)$ at a regular point.

B.3 Normalization of singular curves.

The local ring of a curve at a singular point is not a valuation ring. In such a case, the notion of vanishing order or pole order of a function at P does not make sense anymore. We need to desingularize, or normalize, the curve C.

Definition B.4. *The normalization of C is the curve $\overline{C} = \operatorname{Spec} \overline{k[C]}$ where $\overline{k[C]}$ stands for the integral closure of $k[C]$ in $k(C)$.*

The fact that $\overline{C}$ is a curve follows from the finiteness theorem (which is itself a consequence of Noether's normalization theorem) which ensure that $\overline{k[C]}$ is a one-dimensional integral k-algebra (Proposition A.7). That is, $\overline{k[C]} \simeq k[Z_1, \ldots, Z_m]/J$ where J is a prime ideal of height $m-1$. Thus $\overline{C}$ is indeed an affine curve in a (possibly larger) affine space $\mathbb{A}^m_k$.

Example B.5. *Consider the affine plane curve $C = \operatorname{Spec} k[T,X]/(X^2 - T^2 - T^3)$. There is only one singular point $P = (T, X)$ (corresponding to the geometric point $(0,0)$). Denote t and x the residue classes of T and X. Thus $k[C] = k[t,x]$ where $x^2 = t^2 - t^3$. The rational function $y = x/t \in k(C)$ satisfies $y^2 - t - 1 = 0$, thus is integral over $k[C]$. Adjoining this element to the ring $k[C]$ leads to the bigger ring*

$$k[t, x, x/t] = \frac{k[T,X,Y]}{(X^2 - T^2 - T^3, X - TY, Y^2 - T - 1)} \simeq k[Y].$$

As $k[Y]$ is integrally closed, we deduce that $\overline{k[C]} = k[t, x, x/t] \simeq k[Y]$ and $\overline{C}$ is isomorphic to the affine line $\mathbb{A}^1_k = \operatorname{Spec} k[Y]$ (note however that $\overline{C}$ is naturally embedded in $\mathbb{A}^3_k$ here).

By Proposition B.3, the affine curve $\overline{C}$ is smooth, and $\overline{C} = C$ if and only if C is smooth. We have inclusions $k[C] \subset \overline{k[C]} \subset k(C)$ so the curves C and $\overline{C}$ have same function field $k(C) = k(\overline{C})$. Two curves with isomorphic function fields are said to be birationally equivalent. By Proposition A.7, we have a surjective map (in fact a morphism of k-schemes)

$$\pi : \overline{C} \twoheadrightarrow C, \quad \pi(Q) = Q \cap k[C]$$

which is finite, and one-to-one except above a finite number of closed points of C, these points being contained in the singular locus of C. If P is singular, there may be several points or not lying above Q.

Example B.6. *(Example B.5 continued) The fiber of $\pi : \overline{C} \to C$ above $P = (T, X)$ consists of the maximal ideals $Q \subset k[T, X, Y]$ containing $P + (X^2 - T^2 - T^3, X - TY, Y^2 - T - 1) = (T, X, Y^2 - 1)$. Assuming $\operatorname{char}(k) \neq 2$, the fiber thus consists of two closed points, given by the maximal ideal $Q_1 = (T, X, Y - 1)$ and $Q_2 = (T, X, Y + 1)$, corresponding to the geometric points $(0, 0, \pm 1)$ (this is an example of a blow-up of a plane curve at a nodal point). If $\operatorname{char}(k) = 2$ then $Y^2 - 1 = (Y - 1)^2$ and there is a unique point Q lying above P, given by the maximal ideal $(T, X, Y - 1)$.*

We say that a place of $k(C)$ is centered on C if it is centered on $k[C]$ (Proposition A.9). We can reformulate Proposition A.10 in this context:

Theorem B.7. *Let C be an affine curve. There is a one-to-one correspondence between the places of $k(C)$ centered on C and the closed points of $\overline{C}$.*

The underlying map is $\tilde{Q} \mapsto Q = \tilde{Q} \cap k[\overline{C}]$. The center on C of the place $\tilde{Q}$ is $P = \tilde{Q} \cap k[C] = \pi(Q) \in C$. If the curve C is smooth, we may thus identify places centered on C and closed points of C.

B.4 Places and branches of plane curves.

Suppose that $C = \operatorname{Spec} k[T, X]/(f)$ is a plane curve defined by an irreducible polynomial $f \in R = k[T, X]$ and let $P \in C$ be a closed point. We can describe the places centered at P as follows. Let $\widehat{R}_P$ be the completion of R with respect to the P-adic topology. Typically, $P = (T, X)$ and $\widehat{R}_P = k[[T, X]]$. The germ of the curve C at P is

$$(C, P) = \operatorname{Spec} \widehat{R}_P/(f).$$

The local irreducible factorization $f = f_1 \cdots f_r \in \widehat{R}_P$ leads to the decomposition

$$\widehat{R}_P/(f) = \widehat{R}_P/(f_1) \oplus \cdots \oplus \widehat{R}_P/(f_r)$$

where each summand is now an integral local ring (but not integrally closed in general). The irreducible germ of curve (C_i, P) defined by f_i is called *a branch* of (C, P). We have

$$(C, P) = (C_1, P) \cup \cdots \cup (C_r, P).$$

The following result is the local counterpart of Proposition 3.11 and Proposition 3.16.

Proposition B.8. *There is a one-to-one correspondence between the places Q_i of $k(C)$ with center P and the branches (C_i, P) of the germ of curve (C, P). The valuation v_{Q_i} is induced by the intersection multiplicity at P with f_i. More precisely, if $h \in \mathscr{O}_{C,P}$, we have the equality*

$$v_{Q_i}(h) = \frac{1}{[k_P : k]} \dim_k \frac{\widehat{R}_P}{(f_i, h)}.$$

where we still denote $h \in R_P \subset \widehat{R}_P$ an arbitrary lifting of h.

This point of view allows to represent a place Q_i by the (truncated) local equation f_i of the corresponding branch, and the intersection multiplicity can be computed by means of resultants or local parametrizations, as detailled in Section 3.5.1.

B.5 Places at infinity and compactification.

Unfortunately, the closed points of $\overline{C}$ do not allow to describe all places of $k(C)$. In other words, there are some remaining places which are not centered on C. These are the places "at infinity" of the affine curve C.

Example B.9. *Consider the regular curve $C = \operatorname{Spec} k[T, X]/(TX - 1)$, with coordinate ring $k[C] = k[t, x]$, where $tx = 1$. Thus $k[C] = k[t, 1/t]$ and $k(C) = k(t)$. Consider the two places P_1 and P_2 given respectively by the maximal ideals (t) and $(1/t)$ of the discrete valuation rings $k[t]_{(t)}$ and $k[1/t]_{(1/t)}$ of $k(C)$. We check that $P_1 \cap k[C] = \{0\}$ and $P_2 \cap k[C] = \{0\}$, thus P_1 and P_2 are not centered on C (Proposition A.9).*

In order to give a geometric meaning of the places at infinity, we need to "compactify" C. A classical compactification is the projective closure. For the sake of completeness, let us briefly (and roughly) detail the construction. The projective n-space over k is

$$\mathbb{P}^n_k = \operatorname{Proj} k[X_0, \ldots, X_n].$$

Set theoretically, $\mathbb{P}^n_k$ is the set of homogeneous prime ideals of $R' = k[X_0, X_1, \ldots, X_n]$ of height n whose radical is not equal to the irrelevant ideal $(X_0, \ldots, X_n)$. The underlying variety is the usual projective n-space over $\bar{k}$, that is

$$\mathbb{P}^n(\bar{k}) = (\bar{k}^{n+1} \setminus 0)/\sim$$

where $\sim$ is the collinearity relation of equivalence. The hyperplane at infinity of $\mathbb{P}^n_k$ is

$$H_0 = \operatorname{Proj} R'/(X_0) \simeq \operatorname{Proj} k[X_1, \ldots, X_n] \simeq \mathbb{P}^{n-1}_k,$$

denoted for short $H_0 = \{X_0 = 0\}$. The closed points of H_0 corresponds to the closed points of $\mathbb{P}^n_k$ containing (X_0). The remaining points of $\mathbb{P}^n_k$ are one-to-one with the maximal ideal of $R = k[X_1, \ldots, X_n]$ by dehomogeneization, that is, by letting $X_0 = 1$. We get in such a way a bijection

$$\iota_0 : U_0 = \mathbb{P}^n_k \setminus H_0 \longrightarrow \mathbb{A}^n_k.$$

The reverse map ι_0^{-1} consists of homogeneization of maximal ideals $P \subset k[X_1, \ldots, X_n]$ with respect to X_0, a generator f of P being sent to the homogeneous polynomial

$$f(X_1, \ldots, X_n) \mapsto F(X_0, \ldots, X_n) = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$$

where $d = \deg(f) = \deg(F)$. Note that for each $i = 0, \ldots, n$, dehomogeneization with respect to X_i leads to an isomorphism $\iota_i : U_i = \mathbb{P}^n_k \setminus H_i \simeq \mathbb{A}^k_n$ where $H_i = \{X_i = 0\}$. Moreover, the charts U_i cover the all space $\mathbb{P}^n_k$, thus we can work locally in $\mathbb{P}^n_k$ as in the usual affine n-space.

Let $I' \subset R'$ be the homogeneization of the ideal $I \subset R$ defining the affine curve C. The closed points of

$$\mathscr{C} = \operatorname{Proj} R'/I'$$

are the homogeneous prime ideals of R' of height n containing I' and whose radical is not equal to $(X_0, \ldots, X_n)$. We have a natural inclusion $\mathscr{C} \subset \mathbb{P}^n_k$ and the dehomogenization map ι_0 induces an isomorphism

$$\iota_0 : \mathscr{C} \cap U_0 \longrightarrow C,$$

hence an isomorphism $\mathscr{O}_{\mathscr{C},P} \simeq \mathscr{O}_{C,\iota_0(P)}$ for all $P \in \mathscr{C} \cap U_0$. The remaining set of points of $\mathscr{C}$ is $H_0 \cap \mathscr{C}$ (the points "at infinity"), and there are finitely many such points. We say that $\mathscr{C}$ is *the projective closure* of C. For each chart U_i, the ideal of the affine curve $C_i = \iota_i(\mathscr{C} \cap U_i)$ is easily deduced from the ideal of C. In the plane case $C = \operatorname{Spec} k[X_1, X_2]/(f)$ with f of total degree d, we have

$$\mathscr{C} = \operatorname{Proj} k[X_0, X_1, X_2]/(F)$$

with F the homogeneization of f. We get $C_1 = \operatorname{Spec} k[X_0, X_2]/(f_1)$ and $C_2 = \operatorname{Spec} k[X_0, X_1]/(f_2)$ where

$$f_1(X_0, X_2) = X_0^d f(1/X_0, X_2/X_0) \quad \text{and} \quad f_2(X_0, X_1) = X_0^d f(1/X_0, X_1/X_0).$$

The curve $\mathscr{C}$ is naturally isomorphic to the abstract curve obtained by gluing the affine curves C_i along their intersection. Each affine curve $C_i \subset \mathbb{A}^n_k$ admits a normalization $\overline{C}_i$ as described in the previous paragraph. The affine curves $\overline{C}_i$ can be glued again together and the resulting curve $\overline{\mathscr{C}}$ is a *smooth projective curve*, called the normalization of $\mathscr{C}$.

Theorem B.10. *Let $C \subset \mathbb{A}^n_k$ be an affine curve with projective closure $\mathscr{C} \subset \mathbb{P}^n_k$. There is a one-to-one correspondence between the places of $k(C)$ and the closed points of the normalization $\overline{\mathscr{C}}$ of $\mathscr{C}$.*

The places of $k(C)$ which are centered on C are called the affine places. The remaining places are centered on the points at infinity of $\mathscr{C} \setminus C = \mathscr{C} \cap (X_0 = 0)$, and are called the places at infinity of C. Take care that the normalization of the projective closure $\overline{\mathscr{C}}$ is usually not the projective closure of the affine normalization $\overline{C}$. This is the case if and only if the points at infinity of C are regular points of $\mathscr{C}$.

Example B.11. *(Example B.9 continued). The homogeneization of $f = TX - 1$ with respect to a new variable Z is $F = TX - Z^2$, and $\mathscr{C} = \operatorname{Proj} k[Z, T, X]/(F)$. The intersection of $\mathscr{C}$ with the line at infinity $Z = 0$ is $\operatorname{Proj} k[Z, T, X]/(F, Z) \simeq \operatorname{Proj} k[T, X]/(TX)$, which consists of two closed points $P_1 = (Z, T)$ and $P_2 = (Z, X)$ (corresponding respectively to the geometric points $(0 : 0 : 1)$ and $(0 : 1 : 0)$). These two points correspond to the two places at infinity described in Example B.9. Note that we need here two distinct affine charts $X = 1$ and $T = 1$ to describe the local rings of these points.*

Remark B.12. *There are various ways of compactifying an affine curve. For instance, we can consider its closure in a product of projective spaces or in proper toric varieties. For instance, considering a plane curve defined by a polynomial f with $\lambda(f) > 1$ (as defined in (6)) suggests to consider the Zariski closure $\mathscr{C}$ of the affine plane curve of f in some well-chosen weighted projective compactification of $\mathbb{A}^2_k$.*

Affine places versus finite places. Let $C = \operatorname{Spec} k[T,X]/(f)$ be an affine plane curve and let $\mathscr{C} \subset \mathbb{P}^2_k$ be the projective compactification of C. Denoting $K = k(T)$ and $L = K[X]/(f)$ as in Section 3, we may identify $L = k(\mathscr{C})$. In this context, affine places of L/k (i.e. centered on C) and finite places of L/K (Definition 3.4) do not necessarily coincide. Indeed:

Proposition B.13. *The set of places centered on C is contained in the set of finite places of L/K. These two sets coincide if and only if f is monic in X.*

Proof. By Proposition A.9 (d), a place P is centered on C if and only if $\mathscr{O}_P$ contains $\overline{k[C]}$, while P is finite if and only if $\mathscr{O}_P$ contains the integral closure B of $A = k[t]$ in $L = k(t,x)$. Since $A \subset k[C]$, we have $B \subset \overline{k[C]}$, thus any place centered on C is a finite place. If f is monic, then $x \in B$, hence $B = \overline{k[C]} = \overline{A[x]}$ and affine places coincide with finite places. If f is not monic, then $x \notin B$ and $B \subsetneq \overline{k[C]} = \overline{A[x]}$. Since both rings are integrally closed, we deduce from Proposition A.6 that there exists a place P such that $\mathscr{O}_P$ contains B and does not contain $\overline{k[C]}$, that is P is finite, but not centered on C. □

For instance, in Exemple B.11, the place with center $P_1 = (Z,T)$ is not an affine place, but is a finite place.

B.6 Delta invariant and the genus formula

Let $\mathscr{C}$ be a projective curve defined over k. Let $P \in \mathscr{C}$ be a closed point, with local ring $\mathscr{O}_{\mathscr{C},P}$. The normalization $\overline{\mathscr{O}_{\mathscr{C},P}}$ is a semi-local ring, whose maximal ideals correspond to the closed points of the normalization $\overline{\mathscr{C}}$ lying over P. It is a finite $\mathscr{O}_{\mathscr{C},P}$-module (Proposition A.7), thus $\overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}$ is a finite k-dimensional vector space.

Definition B.14. *The delta-invariant of $\mathscr{C}$ at a closed point $P \in \mathscr{C}$ is*

$$\delta_P(\mathscr{C}) = \dim_k \overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}.$$

The global delta-invariant of $\mathscr{C}$ is $\delta(\mathscr{C}) = \sum_{P \in \mathscr{C}} \delta_P(\mathscr{C})$.

Note that $\delta_P(\mathscr{C}) = 0$ if and only if P is a regular point (Proposition B.2). Thus the sum holds over the finite set of singular points and the global delta-invariant is well-defined. It measures how singular the curve $\mathscr{C}$ is. If $\mathscr{C}$ is a nodal curve, its delta-invariant is simply the number of nodes (over $\bar{k}$), and is called sometimes the "double points number".

Denoting $\mathscr{O}_{\mathscr{C}}$ the structural sheaf of $\mathscr{C}$, the arithmetic genus of $\mathscr{C}$ is defined as

$$p_a(\mathscr{C}) = 1 - \dim_k H^0(\mathscr{C}, \mathscr{O}_{\mathscr{C}}) + \dim_k H^1(\mathscr{C}, \mathscr{O}_{\mathscr{C}}).$$

If $\mathscr{C}$ is irreducible over $\bar{k}$, this is $p_a(\mathscr{C}) = H^1(\mathscr{C}, \mathscr{O}_{\mathscr{C}})$. By definition, the geometric genus $g(\mathscr{C})$ is the arithmetic genus of the normalization of $\mathscr{C}$. In contrast to the arithmetic genus which depends on the embedding of $\mathscr{C}$, the geometric genus is a birational invariant.

The next result due to Hironaka [33] is known as the genus formula. It relates the delta invariant, the arithmetic genus, and the geometric genus of a projective curve.

Proposition B.15. *[33, Thm 2] Let $\mathscr{C} \subset \mathbb{P}^r_k$ be a projective curve. We have $g(\mathscr{C}) = p_a(\mathscr{C}) - \delta(\mathscr{C})$.*

For a projective plane curve of degree n, the genus degree formula states that

$$p_a(\mathscr{C}) = \frac{(n-1)(n-2)}{2}.$$

Combined with Proposition B.15, we get:

Corollary B.16. *Let $\mathscr{C} \subset \mathbb{P}^2_k$ be a projective plane curve of degree n. Then*

$$g(\mathscr{C}) = \frac{(n-1)(n-2)}{2} - \delta(\mathscr{C}).$$

References

[1] S. Abelard. On the complexity of computing integral bases of function fields. In *Computer Algebra in Scientific Computing*, pages 42–62. Springer International Publishing, 2020.

[2] S. Abelard, E. Berardini, A. Couvreur, and G. Lecerf. Computing riemann–roch spaces via puiseux expansions. *Journal of Complexity*, 73:101666, 2022.

[3] S. Abelard, A. Couvreur, and G. Lecerf. Sub-quadratic time for riemann-roch spaces: case of smooth divisors over nodal plane projective curves. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, ISSAC '20, page 14–21, New York, NY, USA, 2020. Association for Computing Machinery.

[4] S. Abelard, A. Couvreur, and G. Lecerf. Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities. *Applicable Algebra in Engineering, Communication and Computing*, Dec. 2022.

[5] S. S. Abhyankar. Irreducibility criterion for germs of analytic functions of two complex variables. *Advances in Mathematics*, 74(2):190 – 257, 1989.

[6] M. Alberich-Carramiñana, J. Guàrdia, E. Nart, A. Poteaux, J. Roé, and M. Weimann. Polynomial factorization over henselian fields. *Foundations of Computational Mathematics*, 25(2):631–681, 2022.

[7] J. Alman and V. V. Williams. *A Refined Laser Method and Faster Matrix Multiplication*, pages 522–539.

[8] M. F. Atiyah and I. G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1969.

[9] J.-D. Bauch. *Lattices over Polynomial Rings and Applications to Function Fields*. PhD thesis, Universitat Autonoma de Barcelona, 2014.

[10] J.-D. Bauch. Computation of integral bases. *Journal of Number Theory*, 165:382–407, 2016.

[11] J.-D. Bauch, E. Nart, and H. Stainsby. Complexity of the om-factorizations of polynomials over local fields. *LMS Journal of Computation and Mathematics*, 16:139–171, 2013.

[12] J. Böhm and I. Stenger. Brillnoether.lib. a singular 4.1.2 library for riemann–roch spaces of divisors on curves, 2019. http://www.singular.uni-kl.de.

[13] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[14] Bourbaki. *Algèbre commutative, Chapitres 5 à 7*. Springer Berlin, Heidelberg, 2006.

[15] A. Campillo. *Algebroid Curves in Positive Characteristic*, volume 378 of *LNCS*. Springer-Verlag, 1980.

[16] A. Campillo and J. I. Farrán. Symbolic hamburger-noether expressions of plane curves and applications to ag codes. *Math. Comput.*, 71(240):1759–1780, 2002.

[17] D. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Informatica*, 28(7):693–701, 1990.

[18] J. Coates. Construction of rational functions on a curve. *Mathematical Proceedings of the Cambridge Philosophical Society*, 68(1):105–123, 1970.

[19] J. H. Davenport. On the integration of algebraic functions. *Lect. Notes Comput. Sci.*, 102, 1981.

[20] A. J. Engler and A. Prestel. *Valued Fields*. Springer Monographs in Mathematics. Springer Berlin, Heidelberg, 2005.

[21] A. L. Gluher and P.-J. Spaenlehauer. A fast randomized geometric algorithm for computing riemann-roch spaces. *Mathematics of Computation*, 89:2399–2433, 2020.

[22] V. D. Goppa. Codes associated with divisors. *Probl. Peredachi Inf.*, 13(1):33–39, 1977.

[23] V. D. Goppa. Algebraico-geometric codes. *Math. USSR, Izv.*, 21:75–91, 1983.

[24] V. D. Goppa. Codes and information. *Russ. Math. Surv.*, 39(1):87–141, 1984.

[25] J. Guàrdia, J. Montes, and E. Nart. Okutsu invariants and Newton polygons. *Acta Arithmetica*, 145:83–108, 2010.

[26] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *Journal de Théorie des Nombres de Bordeaux*, 23(3):667–696, 2011.

[27] J. Guàrdia, J. Montes, and E. Nart. Newton polygons of higher order in algebraic number theory. *Transactions of the American Mathematical Society*, 364:361–416, 2012.

[28] J. Guàrdia, J. Montes, and E. Nart. A new computational approach to ideal theory in number fields. *Foundations of Computational Mathematics*, 13(5):729–762, 2013.

[29] J. Guàrdia, E. Nart, and S. Pauli. Single-factor lifting and factorization of polynomials over local fields. *Journal of Symbolic Computation*, 47(11):1318 – 1346, 2012.

[30] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons and integral bases. *Journal of Number Theory*, 147:549–589, 2015.

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

[32] F. Hess. Computing riemann–roch spaces in algebraic function fields and related topics. *Journal of Symbolic Computation*, 33(4):425–445, 2002.

[33] H. Hironaka. On the arithmetic genera and the effective genera of algebraic curves. *Mem. College Sci. Univ. Kyoto Ser. A Math.*, 30(2):177–195, 1957.

[34] J. v. d. Hoeven and G. Lecerf. Directed evaluation. *Journal of Complexity*, 60:101498, 2020.

[35] M.-D. Huang and D. Ierardi. Efficient algorithms for the riemann-roch problem and for addition in the jacobian of a curve. *Journal of Symbolic Computation*, 18(6):519–539, 1994.

[36] T. Kailath. *Linear Systems*. Prentice-Hall, Englewood Cliffs, 1980.

[37] E. Kaltofen. Greatest common divisors of polynomials given by straight-line programs. *J. ACM*, 35(1):231–264, 1988.

[38] E. Kunz. *Introduction to plane algebraic curves*. Birkauser, 2005.

[39] D. Le Brigand and J. Risler. Algorithme de brill-noether et codes de goppa. *Bulletin de la Société Mathématique de France*, 116(2):231–253, 1988.

[40] S. Mac Lane. A construction for prime ideals as absolute values of an algebraic field. *Duke Math. J.*, 2(3):492–510, 1936.

[41] S. MacLane. A construction for absolute values in polynomial rings. *Trans. Amer. Math. Soc.*, 40(3):363–395, 1936.

[42] R. Matsumoto and S. Miura. Finding a basis of a linear system with pairwise distinct discrete valuations on an algebraic curve. *Journal of Symbolic Computation*, 30(3):309–324, 2000.

[43] E. Nart. Local computation of differents and discriminants. *Mathematics of Computation*, 83(287):1513–1534, 2014.

[44] V. Neiger and T. X. Vu. Computing Canonical Bases of Modules of Univariate Relations. In *ISSAC '17 - 42nd International Symposium on Symbolic and Algebraic Computation*, page 8, Kaiserslautern, Germany, July 2017.

[45] J. Neukirch. *Algebraic number theory*. Springer-Verlag, Berlin, 1999.

[46] H. Niederreiter and F. Özbudak. *Asymptotically Good Codes*, pages 181–220. 2008.

[47] K. Okutsu. Construction of integral basis, i. *Proc. Japan Acad. Ser. A Math. Sci.*, 58(1):47–49, 1982.

[48] Ö. Ore. Zur Theorie der Algebraischen Körper. *Acta Mathematica*, 44(none):219 – 314, 1923.

[49] Ö. Ore. Newtonsche Polygone in der Theorie der algebraischen Körper. *Mathematische Annalen*, 99:84–117, 1928.

[50] J. M. Peral. *Polígonos de Newton de orden superior y aplicaciones aritméticas*. PhD thesis, Universitat de Barcelona, 1999.

[51] P. Popescu-Pampu. Approximate roots. *Fields Institute Communiations*, 33:1–37, 2002.

[52] A. Poteaux and M. Weimann. Computing puiseux series: a fast divide and conquer algorithm. *Annales Henri Lebesgue*, 4:1061–1102, 2021.

[53] A. Poteaux and M. Weimann. Local polynomial factorisation: Improving the montes algorithm. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22, page 149–157, New York, NY, USA, 2022. Association for Computing Machinery.

[54] A. Poteaux and M. Weimann. Fast integral bases computation. In *Computer Algebra in Scientific Computing: 26th International Workshop, CASC 2024, Rennes, France, September 2–6, 2024, Proceedings*, page 292–313, Berlin, Heidelberg, 2024. Springer-Verlag.

[55] J. Rosenkilde and A. Storjohann. Algorithms for simultaneous hermite–padé approximations. *Journal of Symbolic Computation*, 102:279–303, 2021.

[56] P. Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[57] J. Schicho, F.-O. Schreyer, and M. Weimann. Computational aspects of gonal maps and radical parametrization of curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(5):313–341, Nov. 2013.

[58] W. M. Schmidt. Construction and estimation of bases in function fields. *Journal of Number Theory*, 39(2):181–224, 1991. In Memory of Theodor Schneider.

[59] J. P. Serre. *Local fields*. Springer-Verlag New York, 2nd corr. print. edition, 1995.

[60] H. D. Stainsby. *Triangular bases of integral closures*. PhD thesis, 2014.

[61] H. D. Stainsby. Triangular bases of integral closures. *Journal of Symbolic Computation*, 87:140–175, 2018.

[62] I. Stenger. Hess.lib. a singular 4.1.2 library for riemann–roch space of divisors on function fields and curves, 2019. http://www.singular.uni-kl.de.

[63] H. Stichtenoth. *Algebraic function fields and codes*. Springer-Verlag, Berlin, 2009.

[64] A. Storjohann. High-order lifting and integrality certification. *Journal of Symbolic Computation*, 36(3):613–648, 2003. ISSAC 2002.

[65] M. A. Tsfasman, S. G. Vlădutx, and T. Zink. Modular curves, shimura curves, and goppa codes, better than varshamov-gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.

[66] M. van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *Journal of Symbolic Computation*, 23(2-3):209–227, 1997.

[67] E. J. Volcheck. Computing in the jacobian of a plane algebraic curve. In L. M. Adleman and M.-D. Huang, editors, *Algorithmic Number Theory*, pages 221–233, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[68] M. Weimann. Factoring bivariate polynomials using adjoints. *Journal of Symbolic Computation*, 58:77–98, 2013.

[69] W. Zhou. *Fast Order Basis and Kernel Basis Computation and Related Problems*. PhD thesis, 2013.