Solving the p-Riccati Equations and Applications to the Factorisation of Differential Operators.

Raphaël Pagès

SOLVING THE p-RICCATI EQUATION AND APPLICATIONS TO THE FACTORISATION OF DIFFERENTIAL OPERATORS

RAPHAËL PAGÈS

ABSTRACT. The solutions of the equation $f^{(p-1)} + f^p = h^p$ in the unknown function f over an algebraic function field of characteristic p are very closely linked to the structure and factorisations of linear differential operators with coefficients in function fields of characteristic p. However, while being able to solve this equation over general algebraic function fields is necessary even for operators with rational coefficients, no general resolution method has been developed. We present an algorithm for testing the existence of solutions in polynomial time in the "size" of h and an algorithm based on the computation of Riemann-Roch spaces and the selection of elements in the divisor class group, for computing solutions of size polynomial in the "size" of h in polynomial time in the size of h and linear in the characteristic p, and discuss its applications to the factorisation of linear differential operators in positive characteristic p.

1. INTRODUCTION

This article deals with some algorithmic questions related to the factorisation of linear differential operators in positive characteristic p. Let K be a field equipped with an additive map $a \mapsto a'$ verifying the Leibniz rule $(ab)' = a'b + ab'$. Such a map is called a derivation on K and K is called a differential field. An example of such a field is $k(x)$, where k is any field, equipped with the derivation $\frac{\mathrm{d}}{\mathrm{d}x}$. We can consider the field $K\langle\partial\rangle$ of linear differential operators with coefficients in K, whose elements are polynomials in the variable ∂ of the form

$$a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_1\partial + a_0$$

with $a_i \in K$, and where the (noncommutative) multiplication verifies the commutation rule $\partial a = a\partial + a'$ for any $a \in K$. For operators with coefficients in $K = \mathbb{C}(x)$ or $K = \overline{\mathbb{Q}}(x)$, the problem of factorisation has been well studied and several algorithms have been proposed over the years [6, 10, 24]. The question of factorisation for operators with coefficients in $\mathbb{F}_p(x)$ has also been studied in the perspective of developing modular algorithms to factor operators in $\mathbb{Q}(x)\langle\partial\rangle$ [21, 7] after van der Put published in [20] a full classification of finite dimensional differential modules in characteristic p which serves as the basis of all factorisation algorithms for operators in $\mathbb{F}_p(x)\langle\partial\rangle$. The most remarkable difference between operators in characteristic 0 and in characteristic p is the size of the field of constants. Indeed, whereas it is reduced to $\mathbb{C}$ over $\mathbb{C}(x)$, the field of constants of $\mathbb{F}_p(x)$ is $\mathbb{F}_p(x^p)$ over which the field of rational functions $\mathbb{F}_p(x)$ is of finite dimension p. As a consequence, any operator $L \in \mathbb{F}_p(x)\langle\partial\rangle$ is a divisor of an element $N \in \mathbb{F}_p(x^p)[\partial^p]$, the center of $\mathbb{F}_p(x)\langle\partial\rangle$. Factoring those central elements is much easier as they behave as bivariate polynomials. Furthermore, the factorisation of central multiples of L can be used to recover information on the factorisations of L. This allows to reduce the problem of factorisation over $\mathbb{F}_p(x)\langle\partial\rangle$ to the factorisation of divisors of some $N(\partial^p)$ where N is an irreducible polynomial over $\mathbb{F}_p(x^p)$. In the case where N is of the form $Y - a$ with $a \in \mathbb{F}_p(x^p)$, it was shown [20, 7] that finding irreducible factors of $\partial^p - a$ is equivalent to solving the equation

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}f + f^p = a$$

over $\mathbb{F}_p(x)$. This result generalizes to higher degrees of N. For the sake of simplicity we shall assume N to be separable. Let y_N be a root of N in a separable closure of $\mathbb{F}_p(x^p)$. If $N(\partial^p)$ is not itself irreducible, then irreducible factors of $N(\partial^p)$ with coefficients in $\mathbb{F}_p(x)$ are in bijection with the solutions of

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}f + f^p = y_N \tag{1}$$

in $\mathbb{F}_p(x)[y_N]$. We call this equation the p-Riccati equation relative to N. Furthermore, if L is a divisor of $N(\partial^p)$ (not necessarily irreducible) then the solutions of the p-Riccati equation can be used to recover irreducible divisors of L. One way of doing that is to notice that if f is a solution of the p-Riccati equation relative to N then $L(\partial - f)$ has an algebraic solution $b \in \mathbb{F}_p(x)[y_N]$. It follows that an irreducible divisor of L is given by the smallest left multiple of $\partial - f - \frac{b'}{b}$ in $\mathbb{F}_p(x)\langle\partial\rangle$. The "size" of the irreducible divisor of L that this method returns thus depends at least in part on the "size" of the solution to the p-Riccati equation used. In particular, while it is not sufficient it is important in the perspective of developing modular methods for factorisation that the "size" of the solution to the p-Riccati equation is independent from p.
Finally the existence of solutions to the p-Riccati equation acts as an irreducibility test for $N(\partial^p)$.

1.1. **State of the art.** An algorithm to solve the p-Riccati equation was proposed [23, §13.2.1] in the rational case. In that setting, the p-Riccati equation can be written as

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f + f^p = g^p$$

with $g \in \mathbb{F}_p(x)$. This method consists in showing that if rational solutions exists then one of them has the same denominator as g and a numerator of degree at most the maximum of the degrees of the numerator and the denominator of g. Finding this solution is now an easy task since the map $f \mapsto \frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f + f^p$ is $\mathbb{F}_p$-linear. This method returns a solution of degree polynomial (in fact linear here) in that of g and a naive computational approach outputs the result in polynomial time in the degree of g and linear time in p.

Over a general algebraic function field, the only known method was presented in an unpublished manuscript of van der Put [22]. If L is a nontrivial divisor of $N(\partial^p)$ then one can consider $L_* = \gcd(L, \partial^p - y_N)$. By writing

$$L_* = \partial^m + b_{m-1}\partial^{m-1} + \cdots + b_1\partial + b_0$$

it can be shown that $-\frac{b_{m-1}}{m}$ is a solution to the p-Riccati equation relative to N.
This method can only be used if one already knows a nontrivial divisor of $N(\partial^p)$. In particular if nothing else is known it cannot be used as an irreducibility test for $N(\partial^p)$. Furthermore, computing the greatest common divisor of L with an operator of order p yields an operator whose coefficients are of linear "size" in p. Thus the solution to the p-Riccati equation that this method returns has linear size in p as well.

The case of the factorisation of central operators of the form $N(\partial^p)$ has been ignored by the previous works on factorisation. However, this case is highly nontrivial as we will see.

1.2. **Contribution.** We present two new algorithms regarding the p-Riccati equation on algebraic curves of characteristic p. The first is a polynomial time irreducibility test for differential operators of the form $N(\partial^p)$ where N is an irreducible polynomial over $\mathbb{F}_q(x^p)$ (with q being a power of p). Precisely, we show the following result.

Theorem 1.1. *Let $q \in \mathbb{N}^*$ be a power of p and $N_* \in \mathbb{F}_q[x, Y]$ be an irreducible bivariate polynomial of degree d_x with respect to x and d_y with respect to Y. There exists an algorithm testing the irreducibility of $N_*^p(\partial)$ in polynomial time in d_x, d_y and $\log(q)$.*

We then use this irreducibility test to design a resolution algorithm of the p-Riccati equation relative to N and discuss its implications for the factorisation of differential operators.

Theorem 1.2. *Let $q \in \mathbb{N}^*$ be a power of p and let $N_* \in \mathbb{F}_q[x, Y]$ be an irreducible polynomial of degree d_x with respect to x and d_y with respect to Y. We denote by $N \in \mathbb{F}_q[x^p, Y]$ the unique polynomial such that $N_*^p(Y) = N(Y^p)$.*

- *There exists a solution to the p-Riccati equation relative to N of size polynomial in d_x and d_y and an algorithm taking N_* as input and outputting this solution in linear time in p and polynomial time in d_x and d_y.*
- *$N(\partial^p)$ has irreducible factors in $\mathbb{F}_q(x)\langle\partial\rangle$ of size polynomial d_x and d_y. There exists an algorithm taking N_* as input and outputting such a factor in linear time in p and polynomial time in d_x and d_y.*

Remark 1.3. It should be noted that while we limit, for the sake of simplicity, our complexity study to the case of operators whose coefficients are rational functions over $\mathbb{P}^1$, all of the aforementioned algorithms can in fact be designed for factoring operators whose coefficients are rational functions over an algebraic curve $\mathcal{C}$.

Complexity basics. We use the soft-O notation $\tilde{O}$ which indicates that polylogarithmic factors are not displayed. More precisely, if $\lambda, \mu : \mathbb{N} \to \mathbb{R}_+$ are increasing functions, saying that $\lambda(n) = \tilde{O}(\mu(n))$ means that there exists an integer $k \in \mathbb{N}$ such that $\lambda(n) = O(\mu(n)\log^k(\mu(n)))$. We will also locally use the notation O_ε. With the same notations, saying that $\lambda(n) = O_\varepsilon(\mu(n))$ means that for any $\varepsilon > 0$, $\lambda_n = O(\mu(n)^{1+\varepsilon})$.
We denote by $2 \leqslant \omega \leqslant 3$ a feasible exponent for matrix multiplication, that is, by definition, a real number for which we are given an algorithm that computes the product of two m-by-m matrices over a ring R for a cost of $O(m^\omega)$ operations in R. From [1], we know that we can take $\omega < 2.3728596$. We shall also need estimates on the cost of computing characteristic polynomials. Let denote $\Omega \in \mathbb{R}_+^*$ such that the computation of the characteristic polynomial of a square matrix of size m with coefficients in a ring R can be done in $\tilde{O}(m^\Omega)$ arithmetic operations in R. From [13, Section 6], we know that it is theoretically possible to take $\Omega \simeq 2.697263$. Finally, we assume that any two polynomials of degree d over a ring R (resp. integers of bit size n) can be multiplied in $\tilde{O}(d)$ operations in R (resp. $\tilde{O}(n)$ bit operations); FFT-like algorithms allow for these complexities [5, 12].

We begin by recalling some facts about differential operators in characteristic p.

2. Prolegomena

In this section we will work on differential operators with coefficients in a differential field (K, ∂) of characteristic p verifying the following hypothesis:

Hypothesis 2.1. Let C be the subfield of constants of K. We assume:
(1) $[K : C] = p$.
(2) There exists $x \in K$ such that $\partial(x) = 1$.

Remark 2.2. Since we will work on operators in $K\langle\partial\rangle$, ∂ will denote both a formal operator and a derivation on K. For the sake of simplicity we will write

$$f' := \partial(f) \text{ and } f^{(k)} := \partial^k(f)$$

for any $f \in K$.

Notation 2.3. Let $L \in K\langle\partial\rangle$. We denote

$$\mathcal{D}_L := {}^{K\langle\partial\rangle}\!/_{K\langle\partial\rangle L}$$

and for any right divisor L_* of L,

$$\mathcal{D}_L L_* := {}^{K\langle\partial\rangle L_*}\!/_{K\langle\partial\rangle L}$$

The quotient module $\mathcal{D}_L$ is important because of its relation to the factors of L.

Proposition 2.4. *The map*

$$L_* \mapsto \mathcal{D}_L L_*$$

is a bijection between the set of monic right divisors of L and the set of submodules of $\mathcal{D}_L$.

Proof. See [23, Section 2.2, page 47] □

As we previously mentioned, we restrain our study to operators $L \in K\langle\partial\rangle$ for which there exists a separable irreducible polynomial $N \in C[Y]$ such that L is a divisor of $N(\partial^p)$. For the rest of this section we suppose that N is fixed.

Notation 2.5. We denote by $C_N := {}^{C[Y]}\!/_{N(Y)}$ the splitting field of N over C and by y_N the image of Y in C_N. We also set $K_N = K[y_N]$.

Proposition 2.6. *i) For any $f \in K$, $f^{(p)} = 0$.*
ii) $K\langle\partial\rangle$ is a free algebra of dimension p^2 over its center $C[\partial^p]$.

iii) $\mathcal{D}_{N(\partial^p)}$ *is a central simple* C_N*-algebra of dimension* p^2 *(by identifying* $C_N := {}^{C[Y]}/_{N(Y)}$ *with* ${}^{C[\partial^p]}/_{N(\partial^p)} \subset \mathcal{D}_{N(\partial^p)}$*).*

iv) $\mathcal{D}_{N(\partial^p)}$ *is either a division algebra or is isomorphic to* $M_p(C_N)$*.*

v) If $N(\partial^p)$ *is a division algebra then* $N(\partial^p)$ *is irreducible. If* $\mathcal{D}_{N(\partial^p)}$ *is isomorphic to* $M_p(C_N)$ *then all irreducible divisors of* $N(\partial^p)$ *are of order* $\deg(N)$*.*

Proof. (i) and (ii) are done in [20, Lemma 1.1]. (iii) is [20, Lemma 1.2] and (iv) is [20, Corollary 1.3].
Suppose that $\mathcal{D}_{N(\partial^p)}$ is a division algebra. Then in particular it has no nontrivial zero divisor. Thus $N(\partial^p)$ has no nontrivial divisor.
Suppose now that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$ and let L be an irreducible divisor of $N(\partial^p)$. Then $\mathcal{D}_L$ is a simple $K\langle\partial\rangle$-module. We can apply [20, Proposition 1.7.1] to $\mathcal{D}_L$. Since $\mathcal{D}_L$ is simple we must have $\mathcal{D}_L \simeq I(N)$ (with the notations of [20, Proposition 1.7. 1]). In particular, $\dim_{C_N} \mathcal{D}_L = p$ and $\operatorname{ord}(L) = \dim_K \mathcal{D}_L = \frac{[C_N:C]}{[K:C]} \dim_{C_N} \mathcal{D}_L = \deg(N)$. □

We now show how the p-Riccati equation appears when N is a polynomial of degree 1.

Proposition 2.7. *Let* $a \in C$*. If* $\partial^p - a$ *is not irreducible then its monic irreducible divisors are the operators of the form* $\partial - f$ *with* f *verifying*

$$f^{(p-1)} + f^p = a$$

Proof. Let us suppose that $\partial^p - a$ is not irreducible. Then $\mathcal{D}_{\partial^p - a}$ is isomorphic to $M_p(C)$. Let L be a monic irreducible divisor of $\partial^p - a$. From Proposition 2.6 (v) we know that L is of order 1 so it is of the form $\partial - b$. We consider the K-linear endomorphism ψ_p^L of $\mathcal{D}_L$ given by $\psi_p^L : M \mapsto \partial^p \cdot M$. Since ∂^p is central in $K\langle\partial\rangle$, this is indeed a K-linear map. Furthermore, $\mathcal{D}_L$ is isomorphic to K as a K-vector space so there exists $g \in K$ such that ψ_p^L is the multiplication by g. Then we have

$$\begin{aligned} \partial &\equiv \partial \cdot \partial^p \pmod{L} \\ &\equiv \partial^p \cdot \partial \pmod{L} \\ &\equiv g\partial \pmod{L} \end{aligned}$$

Thus $\partial g - g\partial = 0 \pmod{L}$. Since $\partial g - g\partial = g'$, it follows that $g' = 0$ and $g \in C$. Moreover, $Y - g$ is the characteristic polynomial of ψ_p^L, so $\psi_p^L - g\mathrm{Id} = 0$. In particular $\partial^p - g = 0 \pmod{L}$. Thus L is a common divisor of both $\partial^p - a$ and $\partial^p - g$. This is possible only if $g = a$. According to [20, Lemma 1.4.2], $g = b^{(p-1)} + b^p$.
Conversely if L is of the form $\partial - b$ with $b^{(p-1)} + b^p = a$ then from what precedes it is a divisor of $\partial^p - b^{(p-1)} - b^p = \partial^p - a$. □

It follows that $\partial^p - a$ is irreducible in $K\langle\partial\rangle$ if and only if the equation $f^{(p-1)} + f^p = a$ has no solution in K. We now extend this result to polynomials N of higher degree.

Proposition 2.8. *i)* K_N *verifies Hypothesis 2.1 and* $[K_N : K] = \deg(N)$*.*

ii) The canonical morphism $\mathcal{D}_{N(\partial^p)} \to {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ *is an isomorphism of* C_N*-algebras.*

iii) $\mathcal{D}_{N(\partial^p)}$ *is isomorphic to* $M_p(C_N)$ *if and only if the p-Riccati equation relative to* N *has a solution in* K_N*.*

Proof. i) Let $x \in K$ be such that $x' = 1$. Since $[K : C] = p$, we have $K = C[x]$. Furthermore, noticing that $x^p \in C$, we find that $Y^p - x^p$ is the minimal polynomial of x over C. In particular, since N is supposed to be separable, $x \notin C_N$. Thus we also have $K_N = C_N[x]$. Furthermore, since the minimal polynomial of x over C is inseparable, that must also be the case of its minimal polynomial over C_N. Thus we have $[K_N : C_N] = p$. Furthermore, we have $[K_N : C] = [K_N : C_N][C_N : C] = [K_N : K][K : C]$ so $[K_N : K] = \frac{p\deg(N)}{p} = \deg(N)$.

ii) Let $\varphi_N : \mathcal{D}_{N(\partial^p)} \to {}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ be the canonical morphism. We first show that φ_N is injective.
Let $\overline{L} \in \ker(\varphi_N)$ and $L \in K\langle\partial\rangle$ be a lift of $\overline{L}$. We can write $L = \sum_{0 \leqslant i,j \leqslant p-1} l_{i,j}(\partial^p) x^i \partial^j$ with the $l_{i,j} \in C[Y]$. Since K_N verifies Hypothesis 2.1, we deduce that the family $(x^i\partial^j)_{0 \leqslant i,j \leqslant p-1}$ is a C_N-basis of ${}^{K_N\langle\partial\rangle}/_{\partial^p - y_N}$. This means that for all $i, j \in [\![0; p-1]\!]$, $Y - y_N$ divides $l_{i,j}$.
Thus y_N is a root of all $l_{i,j}$. But since the $l_{i,j}$ all have coefficients in C and N is the

minimal polynomial of y_N over C, it follows that N divides all $l_{i,j}$.
Thus the ideal generated by $N(\partial^p)$ is precisely the kernel of the considered map. It follows that φ_N is injective. Observe finally that $\dim_{C_N}(\mathcal{D}_{N(\partial^p)}) = p^2$ and $\dim_{C_N}({}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}) = p \cdot [K_N : C_N] = p^2$. It follows that φ_N is also surjective by dimensional analysis.

iii) $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$ if and only if ${}^{K_N\langle\partial\rangle}/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_N)$ which to say that $\partial^p - y_N$ admits an irreducible divisor of order 1 in $K_N\langle\partial\rangle$. From Proposition 2.7, this is equivalent to the p-Riccati equation with respect to N having a solution in K_N.

□

Notation 2.9. If $N \in C[Y]$ is an irreducible separable polynomial, we denote by S_N the set of elements $f \in K_N$ verifying

$$f^{(p-1)} + f^p = y_N.$$

Lemma 2.10. *Let $N \in C[Y]$ be an irreducible separable polynomial and $f \in S_N$. Then $S_N = \{f - \frac{g'}{g} | g \in K_N\}$.*

Proof. Let h be an element of K_N. The element h is in S_N if and only if $h - f$ verifies $(h-f)^{(p-1)} + (h-f)^p = 0$, which is the same as requiring that $\partial - (h-f)$ is a divisor of ∂^p. Since $\frac{\mathrm{d}^p}{\mathrm{d}x^p}(K_N) = 0$, this is further equivalent to saying that $\partial - (h-f)$ has a solution $g \in K_N$ and is its minimal vanishing operator, that is to say is equal to $\partial - \frac{g'}{g}$. Thus $h \in S_N$ if and only if $h - f$ is of the form $h = \frac{g'}{g}$. □

In Section 4, we will also see how to use the solutions of the p-Riccati equation to compute irreducible divisors of $N(\partial^p)$.

3. Polynomial time irreducibility test

We now present an irreducibility test for operators of the form $N(\partial^p)$ with N being an irreducible polynomial over C. We restrict ourselves to the case where K is a finite separable extension of $\mathbb{F}_p(x)$.

Lemma 3.1. *If K is a finite separable field extension of $\mathbb{F}_p(x)$ equipped with the derivation $\frac{\mathrm{d}}{\mathrm{d}x}$ then K verifies Hypothesis 2.1. Furthermore its constants are the p-th powers of elements of K.*

Proof. Let C be the field of constants of K. $\mathbb{F}_p(x)$ does verify Hypothesis 2.1 and its field of constant is $\mathbb{F}_p(x^p)$. Since K is a finite separable extension of $\mathbb{F}_p(x)$, there exists $F \in \mathbb{F}_p[x, Y]$ irreducible and a root r of F in a separable closure of $\mathbb{F}_p(x)$ such that $K = \mathbb{F}_p(x)[r]$. But then $r^p \in C$, thus $\mathbb{F}_p(x^p)[r^p] \subset C$. Let Φ denote the Frobenius endomorphism on $\mathbb{F}_p(x)$. The element r^p is a root of $\Phi(F)$ so $[\mathbb{F}_p(x^p)[r^p] : \mathbb{F}_p(x^p)] = [K : \mathbb{F}_p(x)]$. We have $[K : \mathbb{F}_p(x^p)] = [K : \mathbb{F}_p(x)][\mathbb{F}_p(x) : \mathbb{F}_p(x^p)] = [K : \mathbb{F}_p(x^p)[r^p]][\mathbb{F}_p(x^p)[r^p] : \mathbb{F}_p(x^p)]$ which is to say that $[K : \mathbb{F}_p(x^p)[r^p]] = \frac{\deg(F)p}{\deg(F)} = p$. Since $\mathbb{F}_p(x^p)[r^p] \subset C \subset K$, and $K \neq C$ $(x \in K)$ we have $C = \mathbb{F}_p(x^p)[r^p]$ and $[K : C] = p$. Furthermore the elements of $C = \mathbb{F}_p(x^p)[r^p]$ are exactly the p-th powers of elements of $K = \mathbb{F}_p(x)[r]$. □

Notation 3.2. Let N be an irreducible polynomial over C. For any place $\mathfrak{P}$ of K_N we denote by $K_{N,\mathfrak{P}}$ the completion of K_N with regard to the associated valuation $\nu_{\mathfrak{P}}$. We also denote $\mathcal{G}_{\mathfrak{P}}$ the residue class field of K_N. Finally we will usually use the notation $t_{\mathfrak{P}}$ to refer to a prime element of $\mathfrak{P}$ in K_N.
For any place of $\mathfrak{P}'$ of C_N, we denote by $C_{N,\mathfrak{P}'}$ the completion of $(C_N, \nu_{\mathfrak{P}'})$.
For any algebraic function field F we denote by $\mathbb{P}_F$ the set of places of F and by $\mathrm{Div}(F)$ the group of divisors of F; we recall that it is the free $\mathbb{Z}$-module generated by the elements of $\mathbb{P}(F)$. If f is an nonzero element of F, we denote by (f) the principal divisor of f, by $(f)_0$ its divisor of zeros and by $(f)_\infty$ its divisor of poles. If D is a divisor over F, we write $\mathcal{L}(D) = \{f \in F | (f) \geqslant -D\}$ for the Riemann-Roch space associated to D.
We denote by $\mathrm{Diff}(K_N/K)$ (or just $\mathrm{Diff}(K_N)$) the different divisor of K_N over K.
Finally if k is a field, we denote by $\mathrm{Br}(k)$ the Brauer group of k.

The basis for our irreducibility test is the following proposition

Proposition 3.3. *Let N be an irreducible polynomial over C. Then, $N(\partial^p)$ is reducible in $K\langle\partial\rangle$ if and only if the p-Riccati equation*

$$f^{(p-1)} + f^p = y_N$$

has a solution in $K_{N,\mathfrak{P}}$ for all $\mathfrak{P} \in \mathbb{P}_{K_N}$.

Proof. We know that $N(\partial^p)$ is reducible in $K\langle\partial\rangle$ if and only if $\mathcal{D}_{N(\partial^p)} \simeq {}^{K_N\langle\partial\rangle}\!/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_N)$, which amounts to saying that ${}^{K_N\langle\partial\rangle}\!/_{(\partial^p - y_N)}$ vanishes in the $\mathrm{Br}(C_N)$. We know that $D \mapsto \bigoplus_{\mathfrak{P}\in\mathbb{P}_{C_N}} D \otimes_{C_N} C_{N,\mathfrak{P}}$ induces an injective group morphism [9, Corollary 6.5.4]

$$\mathrm{Br}(C_N) \hookrightarrow \bigoplus_{\mathfrak{P}\in\mathbb{P}_{C_N}} \mathrm{Br}(C_{N,\mathfrak{P}}).$$

In particular this means that ${}^{K_N\langle\partial\rangle}\!/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_N)$ if and only if

$${}^{K_N\langle\partial\rangle}\!/_{(\partial^p - y_N)} \otimes_{C_N} C_{N,\mathfrak{P}}$$

is isomorphic to $M_p(C_{N,\mathfrak{P}})$ for all $\mathfrak{P} \in \mathbb{P}_{C_N}$.

Besides we know that ${}^{K_N\langle\partial\rangle}\!/_{(\partial^p - y_N)} \otimes_{C_N} C_{N,\mathfrak{P}}$ is isomorphic to ${}^{K_{N,\kappa^{-1}(\mathfrak{P})}\langle\partial\rangle}\!/_{(\partial^p - y_N)}$. Thus ${}^{K_N\langle\partial\rangle}\!/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_N)$ if and only if ${}^{K_{N,\mathfrak{P}}\langle\partial\rangle}\!/_{(\partial^p - y_N)}$ is isomorphic to $M_p(C_{N,\kappa(\mathfrak{P})})$ for all $\mathfrak{P} \in \mathbb{P}_{K_N}$.

Lastly $K_{N,\mathfrak{P}}$ is of the form $\mathbb{F}_q((t_\mathfrak{P}))$ for q some power of p. In particular it is a field verifying Hypothesis 2.1. Thus it is isomorphic to $M_p(C_{N,\mathfrak{P}})$ if and only if the equation

$$f^{(p-1)} + f^p = y_N$$

has a solution in $K_{N,\mathfrak{P}}$. □

We now want to find a criteria for the p-Riccati equation relative to N to have a solution in $\mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$. Over fields of Laurent series we can apply a Newton iteration to find solutions to a higher precision from a given seed as illustrated by the following proposition.

Proposition 3.4. *Let $f_0 \in \mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$ and $n \in \mathbb{Z}$ be such that*

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f_0 + f_0^p = y_N + O(t_\mathfrak{P}^{pn}).$$

We set $e_\mathfrak{P} := 1 - \nu_\mathfrak{P}(t'_\mathfrak{P})$. There exists $f_1 \in \mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$ such that $f_1 = f_0 + O(t_\mathfrak{P}^{pn+(p-1)e_\mathfrak{P}})$ and

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f_1 + f_1^p = y_N + O(t_\mathfrak{P}^{p(pn+(p-1)e_\mathfrak{P})}).$$

Proof. Let $g := \frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f_0 + f_0^p - y_N$. For any $f \in \mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$, $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f$ is a constant since $\frac{\mathrm{d}^p}{\mathrm{d}x^p} = 0$. Since $y_N \in C_N$ is also a constant, it follows that $\frac{\mathrm{d}g}{\mathrm{d}x} = 0$. Thus there exists $\mathcal{I}(f_0) \in \mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$ such that $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} \mathcal{I}(f_0) = g$. Furthermore, we claim that we can take $\mathcal{I}(f_0)$ such that $\nu_\mathfrak{P}(I(f_0)) = pn + (p-1)e_\mathfrak{P}$.
Indeed, let $h \in \mathrm{Im}\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)$ and $H = \sum_{k=\nu_\mathfrak{P}(H)}^{\infty} h_k t_\mathfrak{P}^k \in \mathcal{G}_\mathfrak{P}((t_\mathfrak{P}))$ such that $\frac{\mathrm{d}}{\mathrm{d}x} H = h$. Then we set $H_1 := H - \sum_{k\in\mathbb{Z}} h_{pk} t_\mathfrak{P}^{pk}$. We have $\frac{\mathrm{d}}{\mathrm{d}x} H_1 = \frac{\mathrm{d}}{\mathrm{d}x} H = h$. Furthermore p does not divide $\nu_\mathfrak{P}(H_1)$. But we also have

$$\frac{\mathrm{d}}{\mathrm{d}x} H_1 = t'_\mathfrak{P} \frac{\mathrm{d}}{\mathrm{d}t_\mathfrak{P}} \left(\sum_{k=\nu_\mathfrak{P}(H_1)}^{\infty} h_k t_\mathfrak{P}^k \right) = t'_\mathfrak{P} \sum_{k=\nu_\mathfrak{P}(H_1)-1} (k+1) h_{k+1} t_\mathfrak{P}^k.$$

It follows that $\nu_\mathfrak{P}(h) = \nu_\mathfrak{P}(H_1) - 1 + \nu_\mathfrak{P}(t'_\mathfrak{P})$ which is to say that h admits a primitive H_1 verifying $\nu_\mathfrak{P}(H_1) = \nu_\mathfrak{P}(h) + e_\mathfrak{P}$. Applying this result $p-1$ times, we conclude that we can take $\mathcal{I}(f_0)$ such that $\nu_\mathfrak{P}(I(f_0)) = pn + (p-1)e_\mathfrak{P}$.

Next, we consider $f_1 := f_0 - \mathcal{I}(f_0)$. By definition $f_1 = f_0 + O(t_\mathfrak{P}^{pn+(p-1)e_\mathfrak{P}})$ and

$$\begin{aligned}
\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f_1 + f_1^p &= \frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f_0 + f_0^p - \frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} \mathcal{I}(f_0) - \mathcal{I}(f_0)^p \\
&= g + y_N - g - \mathcal{I}(f_0)^p \\
&= y_N + O(t_\mathfrak{P}^{p(pn+(p-1)e_\mathfrak{P})})
\end{aligned}$$

□

Corollary 3.5. *The p-Riccati equation relative to N admits a solution in $K_{N,\mathfrak{P}} = \mathcal{G}_{\mathfrak{P}}((t_{\mathfrak{P}}))$ if and only if there exists $f \in \mathcal{G}_{\mathfrak{P}}((t_{\mathfrak{P}}))$ such that*

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f + f^p = y_N + O(t_{\mathfrak{P}}^{p(1-e_{\mathfrak{P}})}).$$

In particular if $\nu_{\mathfrak{P}}(y_N) \geqslant p \cdot \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ then the p-Riccati equation relative to N has always a solution in $K_{N,\mathfrak{P}}$.

Proof. Let f be such that $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f + f^p = y_N + O(t_{\mathfrak{P}}^{p(1-e_{\mathfrak{P}})})$ and set $f_0 := 1$. We construct a recursive sequence $(f_k)_{k\in\mathbb{N}} \in K_{N,\mathfrak{P}}^{\mathbb{N}}$ such that the term f_{k+1} is constructed from f_k using Proposition 3.4. We set $n_k := \max\{n \in \mathbb{N} | \frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f_k + f_k^p = y_N + O(t_{\mathfrak{P}}^{pn})\}$ and show that the sequence n_k is strictly increasing. Indeed we have $n_0 > -e_{\mathfrak{P}}$. Thus $n_1 \geqslant pn_0 + (p-1)e_{\mathfrak{P}} > n_0 - (p-1)e_{\mathfrak{P}} + (p-1)e_{\mathfrak{P}} = n_0$. It follows that $n_1 > n_0$ and $n_1 > -e_{\mathfrak{P}}$. By induction we show that $n_k > -e_{\mathfrak{P}}$ for all k and conclude that $n_{k+1} > n_k$ the same way.
From Proposition 3.4 it also follows that $f_k = f_l + O(t_{\mathfrak{P}}^{n_l})$ for all $k \geqslant l$. Thus a solution to the p-Riccati equation in $K_{N,\mathfrak{P}}$ is given by $\lim_{k\to\infty} f_k$.

Let us now suppose that $\nu_{\mathfrak{P}}(y_N) \geqslant p \cdot \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. Then by definition of $e_{\mathfrak{P}}$, the function $f = 0$ verifies

$$\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f + f^p = y_N + O(t_{\mathfrak{P}}^{p(1-e_{\mathfrak{P}})})$$

so the p-Riccati equation relative to N must have a solution in $K_{N,\mathfrak{P}}$ by what precedes. □

Corollary 3.5 is very important because it states that for almost all (all except a finite number) place $\mathfrak{P} \in \mathbb{P}_{K_N}$, the p-Riccati equation has a solution in $K_{N,\mathfrak{P}}$. Indeed, $\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ being the valuation of the divisor $2(x)_\infty - \mathrm{Diff}(K_N)$, the only places where the existence of a solution is not obvious are the places where the valuation of the divisor $p^{-1} \cdot (y_N) + \mathrm{Diff}(K_N) - 2(x)_\infty$ is negative. Since the divisor $\mathrm{Diff}(K_N)$ is effective, those places are either poles of y_N or poles of x.
We now see how to check if the p-Riccati equation has a solution in those places.

Lemma 3.6. *For any $f \in K_{N,\mathfrak{P}}$, $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}} f = \frac{\mathrm{d}^{p-1}}{\mathrm{d}t_{\mathfrak{P}}^{p-1}} (t'^{p-1}_{\mathfrak{P}} f)$.*

Proof. We consider the ring of differential operators $K_{N,\mathfrak{P}}\langle\partial_*\rangle$ where $\partial_* f = f\partial_* + \frac{\mathrm{d}}{\mathrm{d}t_{\mathfrak{P}}}(f)$ for all $f \in K_{N,\mathfrak{P}}$. We know that $\frac{\mathrm{d}}{\mathrm{d}x} = t'_{\mathfrak{P}} \frac{\mathrm{d}}{\mathrm{d}t_{\mathfrak{P}}}$ so we want to show that $(t'_{\mathfrak{P}}\partial_*)^{p-1} = \partial_*^{p-1} t'^{p-1}_{\mathfrak{P}}$. We know that for all $f \in K_{N,\mathfrak{P}}$, $\frac{\mathrm{d}^p}{\mathrm{d}x^p} f = 0$. It follows that $(g\partial_*)^p f = \sum_{i=0}^{p} \binom{p}{i} \frac{\mathrm{d}^i}{\mathrm{d}x^i} f (t'_{\mathfrak{P}}\partial)^{p-i} = f(g\partial_*)^p$. Thus $(g\partial_*)^p$ commutes with all the elements of $K_{N,\mathfrak{P}}$ so it is an element of $K_{N,\mathfrak{P}}[\partial^p]$ and is of the form $a_1\partial_*^p + a_0$. But the leading coefficients a_1 is necessarily $t'^{p-1}_{\mathfrak{P}}$ and $a_0 = \frac{\mathrm{d}1}{\mathrm{d}x} = 0$. Thus we have $(t'_{\mathfrak{P}}\partial_*)^p = t^p_{\mathfrak{P}}\partial_*^p = t'_{\mathfrak{P}}\partial_*^p t'^{p-1}_{\mathfrak{P}}$. We can simplify by $t'_{\mathfrak{P}}\partial_*$ and get the desired equality. □

Theorem 3.7. *Let $\mathfrak{P} \in \mathbb{P}(K_N)$ and $t_{\mathfrak{P}} \in K_N$ be a prime element of $\mathfrak{P}$. We suppose that $\eta := \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - p^{-1} \cdot \nu_{\mathfrak{P}}(y_N) > 0$. Let $(g_0, g_1, \ldots, g_{\eta-1}) \in \mathcal{G}^\eta$ be the first η coefficients of $(t'_{\mathfrak{P}})^{p-1}$ and $(a_0, \ldots, a_{\eta-1}) \in \mathcal{G}^\eta$ be the first η coefficients of a p-th root of y_N. Let $\mathcal{G}_{\mathfrak{P}} = \mathbb{F}_{p^b}$ with $b > 0$. We identify $\mathcal{G}_{\mathfrak{P}}^\eta$ with $\mathbb{F}_p^{b\eta}$. We set*

$$D_{p-1}(\mathfrak{P}) := \begin{pmatrix} & & & & & & & \\ & & & \mathbf{0} & & & & \\ & & & & & & & \\ g_r & \cdots & g_0 & & & & & \\ \vdots & & & \ddots & & & & \\ g_{\eta-1-p} & & \cdots & & g_0 & 0 & \cdots & 0 \\ g_{\eta-1} & & \cdots & & g_p & g_{p-1} & \cdots & g_0 \end{pmatrix}$$

where $D_{p-1}(\mathfrak{P}) \in M_{b\eta}(\mathbb{F}_p)$ is a block matrix and the coefficient g_i is the matrix of the multiplication by g_i in $\mathcal{G}_{\mathfrak{P}}$. Let Φ be the diagonal block matrix in $M_{b\eta}(\mathbb{F}_p)$ whose diagonal block are all the matrix

of the Frobenius endomorphism over $\mathcal{G}_{\mathfrak{P}}$. Then the p-Riccati equation relative to N has a solution in $K_{N,\mathfrak{P}}$ if and only if the system

$$(\Phi - D_{p-1}(\mathfrak{P}))X = \Phi^t(a_0, \dots, a_{\eta-1})$$

has a solution in $\mathcal{G}^{\eta}_{\mathfrak{P}}$.

Proof. Let $f \in K_{N,\mathfrak{P}}$ verifying $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}f + f^p = y_N$. Then $\nu_{\mathfrak{P}}(f) \geqslant p^{-1}\nu_{\mathfrak{P}}(y_N)$. Indeed we know that $\nu_{\mathfrak{P}}(y_N) \geqslant \min(p\nu_{\mathfrak{P}}(f), \nu_{\mathfrak{P}}(\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}f))$. If we had $\nu_{\mathfrak{P}}(f) < p^{-1}\nu_{\mathfrak{P}}(y_N)$ then in particular $\nu_{\mathfrak{P}}(f) < \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$. Since $\nu_{\mathfrak{P}}\left(\frac{\mathrm{d}^{p-1}f}{\mathrm{d}x^{p-1}}\right) \geqslant \nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)$, we find that $\nu_{\mathfrak{P}}\left(\frac{\mathrm{d}^{p-1}f}{\mathrm{d}x^{p-1}}\right) > p\nu_{\mathfrak{P}}(f)$. Thus we would have $\nu_{\mathfrak{P}}(y_N) = \min(p\nu_{\mathfrak{P}}(f), \nu_{\mathfrak{P}}(\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}f)) = p\nu_{\mathfrak{P}}(f)$, which is a contradiction. Thus $\nu_{\mathfrak{P}}(f) \geqslant p^{-1} \cdot \nu_{\mathfrak{P}}(y_N)$.
We set $f := \sum_{k=0}^{\infty} f_k t_{\mathfrak{p}}^{k+p^{-1}\cdot\nu_{\mathfrak{P}}(y_N)}$. We claim that $X = {}^t(f_0, \dots, f_{\eta-1})$ is a solution of the system $(\Phi - D_{p-1}(\mathfrak{P}))X = \Phi \cdot {}^t(a_0, \dots, a_{\eta-1})$. It is in fact enough to check that the vector $-D_{p-1}(\mathfrak{P})^t(f_0, \dots, f_{\eta-1})$ is the vector of the coefficients of $t_{\mathfrak{P}}^{pk}$ in $\frac{\mathrm{d}^{p-1}f}{\mathrm{d}x^{p-1}}$ for $k \in [\![p^{-1}\cdot\nu_{\mathfrak{P}}; \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1]\!]$. We know that $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}(f) = \frac{\mathrm{d}^{p-1}}{\mathrm{d}t_{\mathfrak{P}}^{p-1}}(t'^{p-1}_{\mathfrak{P}}f)$ and the result follows from a straightforward computation.
Conversely, if $(\Phi - D_{p-1}(\mathfrak{P}))X = \Phi \cdot {}^t(a_0, \dots, a_{\eta-1})$ has a solution $(f_0, \dots, f_{\eta-1}) \in \mathcal{G}^{\eta}_{\mathfrak{P}}$ then we set $f = \left(\sum_{k=0}^{\eta-1} f_k t_{\mathfrak{P}}^k\right) t_{\mathfrak{P}}^{p^{-1}\cdot\nu_{\mathfrak{P}}(y_N)}$ and claim that $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}f + f^p = y_N + O(t_{\mathfrak{P}}^{p(1-e_{\mathfrak{P}})})$ which proves the existence of a solution according to Corollary 3.5. From what precedes, we know that the equality is true for the coefficients of t^{pk} for $k \in [\![p^{-1}\cdot\nu_{\mathfrak{P}}(y_N), -e_{\mathfrak{P}}]\!]$. Furthermore, since $\frac{\mathrm{d}^{p-1}}{\mathrm{d}x^{p-1}}f + f^p$ and y_N are constant, all the other coefficients before $t_{\mathfrak{P}}^{p(1-e_{\mathfrak{P}})}$ are equal to zero which gives the desired result. □

We can now write an algorithm for testing the irreducibility of an operator $N(\partial^p)$ where N is an irreducible polynomial over C. From Lemma 3.1, we know that we can take $N_* \in K[Y]$ such that $N_*^p(Y) = N(Y^p)$ and $K_N \simeq {}^{K[Y]}/_{N_*}$. If we denote by a the image of Y in K_N then $y_N = a^p$. This representation is easier to manipulate (because smaller by a factor p in all generality) so we consider that the entry of our algorithm is the polynomial N_*. The correctness of Algorithm 1 is

Input: $N_* \in K[Y]$ a separable irreducible polynomial.
Output: Whether or not $N^p(\partial)$ in irreducible in $K\langle\partial\rangle$

(1) Set $K_N := K[a] = {}^{K[Y]}/_{N}$ where a is a root of N.
(2) Compute $\mathbb{S} := \mathrm{Supp}(a)_- \cup \mathrm{Supp}(x)_-$.
(3) For $\mathfrak{P}$ in $\mathbb{S}$ do:
  (a) Compute $t_{\mathfrak{P}}$ a prime element of $\mathfrak{P}$.
  (b) Compute $t'_{\mathfrak{P}}$ and set $\eta := \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - \nu_{\mathfrak{P}}(a)$.
  (c) If $\eta > 0$ do:
    (i) Compute $g_{\mathfrak{P}}$, the Taylor expansion of $t'_{\mathfrak{P}}$ in $t_{\mathfrak{P}}$ at relative precision η.
    (ii) With fast exponentiation on $g_{\mathfrak{P}}$, compute the first η coefficients $(g_0, \dots, g_{\eta-1})$ of $t'^{p-1}_{\mathfrak{P}}$.
    (iii) Compute $(a_0, \dots, a_{\eta-1})$ the first η coefficients of the Taylor expansion of a in $t_{\mathfrak{P}}$.
    (iv) Check if the system $(\Phi - D_{p-1}(\mathfrak{P})X = \Phi^t(a_0, \dots, a_{\eta-1}$ defined in Theorem 3.7 has a solution in $\mathcal{G}^{\eta}_{\mathfrak{P}}$.
    (v) If it doesn't, return **False** and stop the algorithm.
(4) return **True**

Algorithm 1: irreducibility_test

easily deduced from the discussion that precedes. To evaluate its complexity, we must say a word on the choice of the prime elements $t_{\mathfrak{P}}$. To simplify the exposition, we assume that $K = \mathbb{F}_q(x)$ with $q = p^b$ and that $N_* \in \mathbb{F}_q[x, y]$ with $d_x = \deg_x N_*$ and $d_y = \deg_y N_*$. It follows that K_N is

a field extension of $\mathbb{F}_q(x)$ of degree d_y. As such, any element $f \in K_N$ can be represented by d rational functions in $\mathbb{F}_q(x)$.

Notation 3.8. For any element $f = \frac{1}{D_f}\sum_{i=0}^{d_y-1} f_i a^i \in K_N$ such that $D_f, f_0, \ldots, f_{d_y-1} \in \mathbb{F}_q[x]$ with $\gcd(D_f, f_0, \ldots, f_{d_y-1}) = 1$ we write

$$\deg f := \max(\deg D_f, \deg f_0, \ldots, \deg f_{d_y-1}).$$

In 2011, Jordi Guardia, Jesús Montes and Enric Nart presented in [11] an algorithm designed for number fields called *Montes algorithm*. This algorithm takes in input a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ which defines a number field $K = \mathbb{Q}[\theta]$, where θ is a root of f, and a prime number $p \in \mathbb{Z}$. The algorithm returns a full factorisation $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$ of the ideal $p\mathbb{Z}_K$ as a product of prime ideals of $\mathbb{Z}_K$, where $\mathbb{Z}_K$ is the subring of elements of K which are integral over $\mathbb{Z}$, as well as generators $\alpha_1, \ldots, \alpha_g$ verifying $\mathfrak{p}_i = p\mathbb{Z}_K + \alpha_i\mathbb{Z}_K$. The settings of number fields and algebraic function fields are actually very similar and *Montes algorithm* can be easily adapted to it. The analogous algorithm takes as input a monic irreducible polynomial $f(x, y) \in \mathbb{F}_q[x][y]$ generating an algebraic function field of positive characteristic $F \simeq {}^{\mathbb{F}_q(x)[y]}/_{f(x,y)}$ together with an irreducible polynomial $P \in \mathbb{F}_q[x]$; and it returns the divisor $(P) = e(\mathfrak{P}_1|P)\cdot\mathfrak{P}_1 + \ldots + e(\mathfrak{P}_g|P)\cdot\mathfrak{P}_g$ as well as prime elements $t_{\mathfrak{P}_i}$ for all the places in $\mathrm{Supp}(P)$.

Montes algorithm is the starting point of many algorithms dealing with number fields or algebraic function fields. In [2], a version of *Montes algorithm* where the generators α_i are not computed is used as a key element to compute *OM-representations*, of the ideals dividing p, from which the generators can be obtained as a byproduct. In [14, section 6], Adrien Poteaux and Martin Weimann stated that for a number field $\mathbb{K} = {}^{\mathbb{Q}[x]}/_{(F)}$, where F is a monic integral polynomial, and a prime $p \in \mathbb{Z}$, an *OM-representation* of the prime ideals dividing p can be computed in $\tilde{O}_\varepsilon(\deg_y(f)\delta)$ operations in $\mathbb{F}_p$, where δ is the valuation of $\mathrm{Disc}(F)$ in p, if $p > \deg_y(f)$ or $O_\varepsilon(\deg_y(f)\delta + \delta^2)$ operations in $\mathbb{F}_p$ otherwise. The analogous result for algebraic functions fields is that for an algebraic function field $\mathbb{F} = {}^{\mathbb{F}_q(x)[y]}/_{f(x,y)}$, where f is a monic integral polynomial, and an irreducible polynomial $P \in \mathbb{F}_q[x]$, an *OM-factorisation* of the prime ideals dividing P can be computed in $O_\varepsilon(\deg(P)\deg_y(f)\delta)$ operations in $\mathbb{F}_q$ if $\mathrm{char}(\mathbb{F}_q) > \deg_y(f)$, and $O_\varepsilon(\deg(P)(\deg_y(f)\delta + \delta^2))$ operations in $\mathbb{F}_q$ otherwise, where δ is the valuation of $\mathrm{Disc}(f)$ in P.

In a personal communication, Martin Weimann explained to us that, as a consequence of [11, Proposition 4.28] and of the results of a paper in preparation [15], a prime element $t_{\mathfrak{P}}$ of a place $\mathfrak{P} \in \mathrm{Supp}(P)$ can be computed with $\deg t_{\mathfrak{P}} = O(\deg(P)\frac{\delta}{\deg_y(f)})$ at the cost of an *OM-factorisation* and $O(\deg(P)\delta)$ operations in $\mathbb{F}_q$.

Theorem 3.9. *Let $N_* \in \mathbb{F}_{p^b}[x, y]$ be an irreducible polynomial and let $d_x := \deg_x(N_*)$ and $d_y := \deg_y(N_*)$. Algorithm 1 determines whether N_* is irreducible or not in , solving the local problems can be done at the cost of computing $(a)_-$ and $(x)_-$ as well as $O_\varepsilon(d_x d_y b\log(p))$ bit operations from computing* OM-representations *and prime elements, $O(d_x + d_y)$ evaluation of functions in K_N of degree $O(d_x^2 d_y + d_x d_y^2)$ and $O_\varepsilon(b^\omega(d_x + d_y)^\omega \log^2(p) + (d_x^3 d_y^2 + d_x^2 d_y^3 + d_x d_y^4)b\log(p))$ bit operations.*

Proof. Let l_c be the leading coefficient of N_*. We begin by the cost of computing prime elements for all places $\mathfrak{P} \in S := \mathrm{Supp}(a)_\infty \cup (x)_\infty$. Let us first assume that $\mathrm{Supp}(a)_\infty \cap \mathrm{Supp}(x)_\infty = \varnothing$. Let $\mathfrak{P}$ be a pole of a. We can apply the *OM*-factorisation mentioned earlier to $Q = l_c^{d_y-1}N_*(x, y/l_c)$ which is integral, monic and the minimal polynomial of $l_c a$. We have $\mathrm{Disc}(Q) = l_c^{d_y-1}\mathrm{Disc}(N_*)$ which is of degree $O(d_x d_y)$. There exists $P \in \mathbb{F}_p[x]$ irreducible such that $\mathfrak{P}$ divides P. It follows that the cost of using the *OM-factorisation* algorithm is $O_\varepsilon(\deg(P)(d_y\delta(Q) + \delta(Q)^2) = O((d_y + \deg(\mathrm{Disc}(Q)))\deg(\mathrm{Disc}(Q)) = O((d_x d_y)^2)$ operations in $\mathbb{F}_{p^b}$ and yields a prime element $t_{\mathfrak{P}}$ such that $\deg(t_{\mathfrak{P}}) = O(d_x)$. The sum of these costs over the poles of a results in $O(d_x^3 d_y^2)$ operations in $\mathbb{F}_{p^b}$.

By the symmetry of the roles of x and a, the similar process over the poles of x costs $O_\varepsilon(d_y^3 d_x^2)$ operations in $\mathbb{F}_{p^b}$ and yields prime elements of degree $O(d_y)$ both in x and a.

If now $\mathfrak{P}$ is a pole of both a and x we can replace a by $a \cdot x^\nu$ and $N_*(x, y)$ by $N_*(x, x^{-\nu}y)$ where ν is the valuation of a in $\mathfrak{P}$. Thus we find ourselves in a situation where $\mathfrak{P}$ is not a pole of x and show that the result still holds. Thus this first phase has a cost of $O_\varepsilon((d_x^3 d_y^2 + d_x^2 d_y^3)b\log(p))$ bit operations.

Prime elements of poles of (x) created from this process are written in a basis of $\mathbb{F}_{p^b}(a)[x]$ and need

to be written in the canonical basis of $\mathbb{F}_{p^b}(x)[a]$. This yields prime elements of degree $O(d_x d_y)$ which we now assume to be the size of all our prime elements.

To compute the Taylor expansions we use a naive algorithm which consist in extending the constant base field $\mathbb{F}_{p^b}$ to $\mathcal{G}_{\mathfrak{P}}$ and doing recursive evaluations of $t'_{\mathfrak{P}}$ and a in $\mathcal{G}_{\mathfrak{P}}$. This process over $\mathfrak{P}$ requires to do at most $m_{\mathfrak{P}} := -2\nu_{\mathfrak{P}}(x) - \nu_{\mathfrak{P}}(a)$ evaluations of function of a degree similar to $t_{\mathfrak{P}}^{m_{\mathfrak{P}}}$ that is to say $O(m_{\mathfrak{P}} d_x d_y)$ and $(m_{\mathfrak{P}}^2 d_x d_y)$ operations in $\mathcal{G}_{\mathfrak{P}}$. By definition, the sum of the $m_{\mathfrak{P}} \deg(\mathfrak{P})$ is smaller than $\deg(2(x)_\infty + (a)_\infty) = O(d_x + d_y)$. Thus computing the Taylor expansions requires to do $O(d_x + d_y)$ evaluations of functions in K_N of degree at most $O(d_x^2 d_y + d_x d_y^2)$ and $\tilde{O}((d_x^3 d_y^2 + d_x d_y^4) b \log(p)$ bit operations.
The final part is the resolution of multiple $\mathbb{F}_p$-linear systems of size $m_{\mathfrak{P}} \deg(\mathfrak{P}) b$ each of which can be solved in $\tilde{O}(b^\omega m_{\mathfrak{P}}^\omega \deg(\mathfrak{P})^\omega \log(p)^2)$ bit operations. The factor $\log(p)^2$ comes from the computation of the Frobenius endomorphism over $\mathcal{G}_{\mathfrak{P}}$. The sum of these terms over the poles of a and x gives the final result. □

4. Solving the p-Riccati equation

The goal of this section is to present an algorithm to solve the p-Riccati equation relative to an irreducible polynomial $N \in C[Y]$ over K_N. We discuss its complexity and its applications to the factorisation of differential operators in $K\langle\partial\rangle$. This algorithm makes use of algebraic geometry tools such as Riemann-Roch spaces and the Picard group of K_N.
We recall that van der Put and Singer presented, in [23, §13.2.1], a method to compute solutions of p-Riccati equations over $\mathbb{F}_q(x)$. Their method will serve as a guideline for the techniques we develop in the general case.
We keep the notations of the previous section. In addition, we suppose that $N \in C[Y]$ is a fixed irreducible polynomial and use the notations introduced in Notation 2.5. In particular, we recall that S_N denotes the set of solutions of the p-Riccati equation $f^{(p-1)} + f^p = y_N$.

Proposition 4.1. *Let $\mathfrak{P}$ be a place of K_N, $t_{\mathfrak{P}}$ be a prime element of $\mathfrak{P}$. Then, for all $f \in S_N$, we have $\nu_{\mathfrak{P}}(f) \geqslant \min(p^{-1}\nu_{\mathfrak{P}}(y_N), \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)$.*

Proof. We have

$$\begin{aligned}\nu_{\mathfrak{P}}(y_N) &= \nu_{\mathfrak{P}}(f^{(p-1)} + f^p)\\ &\geqslant \min(\nu_{\mathfrak{P}}(f^{(p-1)}, p\nu_{\mathfrak{P}}(f)).\end{aligned}$$

Furthermore equality holds if $\nu_{\mathfrak{P}}(f^{(p-1)}) \neq p\nu_{\mathfrak{P}}(f)$. Since $\nu_{\mathfrak{P}}(f^{(p-1)}) \geqslant \nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)$ if $\nu_{\mathfrak{P}}(f) < \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$, we find in particular that $p\nu_{\mathfrak{P}}(f) < \nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1) \leqslant \nu_{\mathfrak{P}}(f^{(p-1)})$ so $\nu_{\mathfrak{P}}(y_N) = p\nu_{\mathfrak{P}}(f)$. □

In fact we can show that if solutions exists, some of them verify a slightly better bound.

Definition-Proposition 4.2. *Let $f \in S_N$ and $\mathfrak{P}$ be a place of K_N verifying $\nu_{\mathfrak{P}}(y_N) \geqslant p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. Then there exists $k \in \mathbb{F}_p$ such that for all $g \in K_N$, if $\nu_{\mathfrak{P}}(g) \equiv k \pmod p$ then $f - \frac{g'}{g} \in S_N$ and $\nu_{\mathfrak{P}}\left(f - \frac{g'}{g}\right) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. We call k the ramified residue of f in $\mathfrak{P}$ and write*

$$\mathfrak{Re}_{\mathfrak{P}}(f) := k.$$

Proof. If $\nu_{\mathfrak{P}}(f) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ then we can take $k = 0$. Indeed in this case, if $\nu_{\mathfrak{P}}(g) \equiv 0 \pmod p$ then there exists $l \in \mathbb{N}$ such that $g = t_{\mathfrak{P}}^{pl} u$ with $\nu_{\mathfrak{P}}(u) = 0$. Then $\frac{g'}{g} = \frac{u'}{u} + pl\frac{t'_{\mathfrak{P}}}{t_{\mathfrak{P}}} = \frac{u'}{u}$. Since $\nu_{\mathfrak{P}}(u) = 0$, we can write $u = \sum_{n=0}^{\infty} u_n t_{\mathfrak{P}}^n$ and $u' = t'_{\mathfrak{P}} \sum_{k=0}^{\infty} (n+1) u_{n+1} t_{\mathfrak{P}}^n$. Thus $\nu_{\mathfrak{P}}(u') \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ and $\nu_{\mathfrak{P}}\left(\frac{g'}{g}\right) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$ which yields the result.
Suppose now that $\nu_{\mathfrak{P}}(f) = \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$. We set $e = 1 - \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$, $a := (t_{\mathfrak{P}}^{e-1} t'_{\mathfrak{P}})(\mathfrak{P})$ and $c := (t_{\mathfrak{P}}^e f)(\mathfrak{P})$. Let us show that $c \in \mathbb{F}_p^\times a$. The characteristic p does not divide e, and we know that $\nu_{\mathfrak{P}}(f^{(p-1)}) = -pe$. Furthermore we know (Lemma 3.6) that $f^{(p-1)} := \frac{\mathrm{d}^{p-1}}{\mathrm{d}t_{\mathfrak{P}}^{p-1}}(t_{\mathfrak{P}}^{p-1} f)$. It follows that $(t_{\mathfrak{P}}^{pe} f^{(p-1)})(\mathfrak{P}) = -a^{p-1}c$ and $(t_{\mathfrak{P}}^{pe} f^p)(\mathfrak{P}) = c^p$. But $t_{\mathfrak{P}}^{pe}(f^{(p-1)} + f^p)(\mathfrak{P}) = (t_{\mathfrak{P}}^{pe} y_N)(\mathfrak{P}) = 0$ since $\nu_{\mathfrak{P}}(y_N) > -pe$. It follows that $t_{\mathfrak{P}}^{pe}(f^{(p-1)} + f^p)(\mathfrak{P}) = c^p - a^{p-1}k = 0$. Thus $c^{p-1} = a^{p-1}$ and $c \in \mathbb{F}_p^\times a$. We set $k := c \cdot a^{-1}$.

Let $g \in K_N$ be such that $\nu_{\mathfrak{P}}(g) \equiv k \pmod p$. There exists $l \in \mathbb{Z}$ and $u \in K_N$ such that $\nu_{\mathfrak{P}}(u) = 0$ and $g = t_{\mathfrak{P}}^{pl+k}u$. Then $\frac{g'}{g} = k\frac{t_{\mathfrak{P}}}{t_{\mathfrak{P}}} + \frac{u'}{u}$. Since $\nu_{\mathfrak{P}}(u) = 0$, $\nu_{\mathfrak{P}}(u') > -e$ and $\nu_{\mathfrak{P}}\left(\frac{g'}{g}\right) = -e$. Then $\left(t_{\mathfrak{P}}^e \frac{g'}{g}\right)(\mathfrak{P}) = k(t_{\mathfrak{P}}^{e-1}t_{\mathfrak{P}})(\mathfrak{P}) = ka = c$. Thus $\left(t_{\mathfrak{P}}^e\left(f - \frac{g'}{g}\right)\right)(\mathfrak{P}) = 0$, which is to say that $\nu_{\mathfrak{P}}\left(f - \frac{g'}{g}\right) \geqslant 1 - e = \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. □

In particular if $\mathfrak{P}$ is neither ramified nor a pole of y_N then S_N contains an element with no pole in $\mathfrak{P}$. This local improvement on the bound provided in Proposition 4.1 is accomplished by adding an element of the form $\frac{g'}{g}$. Unfortunately adding such an element makes new poles appear in general so this local approach is not enough. We globalize it in the following theorem.

Theorem 4.3. *Let $f \in S_N$ and $S := \{\mathfrak{P} \in \mathbb{P}_{K_N} | \nu_{\mathfrak{P}}(y_N) < p\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})\}$. Set*

$$\mathfrak{Re}(f) := \sum_{\substack{\mathfrak{P}\in\mathbb{P}_{K_N}\\ \mathfrak{P}\notin S}} \mathfrak{Re}_{\mathfrak{P}}(f)\cdot\mathfrak{P}.$$

If there exist $D', D_p \in \mathrm{Div}(F)$ such that $\mathfrak{Re}(f) \sim D' + pD_P$ then S_N contains an element φ verifying for all places $\mathfrak{P}$ outside $S \cup \mathrm{supp}(D')$ that $\nu_{\mathfrak{P}}(\varphi) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$.

Proof. Since $\mathfrak{Re}(f) \sim D' + pD_p$, there exists $g \in K_N$ such that $\mathfrak{Re}(f) - D' - pD_p = (g)$. From Lemma 2.10, we deduce that $f - \frac{g'}{g} \in S_N$. Let $\mathfrak{P} \in \mathbb{P}_{K_N}\backslash(S \cup \mathrm{supp}(D'))$. Then we find

$$\begin{aligned}\nu_{\mathfrak{P}}(g) &= \nu_{\mathfrak{P}}(\mathfrak{Re}(f)) - \nu_{\mathfrak{P}}(D') - p\nu_{\mathfrak{P}}(D_p)\\ &= \nu_{\mathfrak{P}}(\mathfrak{Re}(f)) - 0 - p\nu_{\mathfrak{P}}(D_p)\\ &\equiv \nu_{\mathfrak{P}}(\mathfrak{Re}(f)) \pmod p\\ &\equiv \mathfrak{Re}_{\mathfrak{P}}(f) \pmod p\end{aligned}$$

By definition of $\mathfrak{Re}_{\mathfrak{P}}(f)$, $f - \frac{g'}{g}$ is an element of S_N verifying for any place $\mathfrak{P}$ outside $S \cup \mathrm{Supp}(D')$ that

$$\nu_{\mathfrak{P}}(f - \frac{g'}{g}) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}).$$

□

Definition 4.4. We consider $\mathfrak{G}_N^p = {}^{\mathrm{Cl}(K_N)}\!/_{p\mathrm{Cl}(K_N)}$. Since K_N is an algebraic function field of characteristic p, $\mathfrak{G}_N^p$ is a finite commutative group of the form $\mathfrak{G}_N^p \simeq \left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^n$ for some $n \in \mathbb{N}^*$.

Corollary 4.5. *For each place $\mathfrak{P} \in \mathbb{P}_{K_N}$ we denote by $t_{\mathfrak{P}}$ a prime element of $\mathfrak{P}$.*
Let $(D_1, \ldots, D_n) \in \mathrm{Div}(K_N)^n$ be a lifting of a generating family of $\mathfrak{G}_N^p$ viewed as a $\mathbb{F}_p$-vector space. Let $S = \bigcup_{i=1}^n \mathrm{Supp}\, D_N$ and set

$$A := \max\left(\sum_{\mathfrak{P}\in S}\mathfrak{P} + \mathrm{Diff}(K_N) - 2(x)_\infty, \frac{(y_N)_-}{p}\right).$$

If S_N is not empty then it contains an element of $\mathcal{L}(A)$.

Proof. Let $f \in S_N$ and let $\mathfrak{Re}(f)$ be defined similarly as in Theorem 4.3. Since $D_1, \ldots, D_n$ is a basis of $\mathfrak{G}_N^p$, there exists a linear combination $D' = a_1D_1 + \ldots + a_nD_n$ such that $\mathfrak{Re}(f) \equiv D' \pmod{\mathfrak{G}_N^p}$. Thus there exists $D_p \in \mathrm{Div}(K_N)$ such that

$$\mathfrak{Re}(f) \sim D' + pD_p.$$

Besides $\mathrm{supp}(D') \subset \bigcup_{i=1}^n \mathrm{supp}(D_i) \subset S$. According to Theorem 4.3, S_N contains an element f^* verifying for all places outside of S that $\nu_{\mathfrak{P}}(f^*) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. The corollary now follows from Proposition 4.1 and the fact that the valuation in $\mathfrak{P}$ of the divisor $\mathrm{Diff}(K_N) - 2(x)_\infty$ is precisely $-\nu_{\mathfrak{P}}(t'_{\mathfrak{P}})$. □

Definition 4.6. For any effective divisor D over K_N, we define

$$A(D) := \max\left(\sum_{\mathfrak{P}\in\mathrm{Supp}\, D}\mathfrak{P} + \mathrm{Diff}(K_N) - 2(x)_-, \frac{(y_N)_-}{p}\right).$$

We say that D is a generating divisor of $\mathfrak{G}_N^p$ if and only if $(\mathfrak{P})_{\mathfrak{P}\in\operatorname{Supp} D}$ is a generating family of $\mathfrak{G}_N^p$. In this case

$$S_N = \varnothing \Leftrightarrow S_N \cap \mathcal{L}(A(D)) = \varnothing.$$

For a family of effective divisors $(D_1, \dots, D_n)$ we define

$$A(D_1, \dots, D_n) = A(D_1 + \dots + D_n).$$

To our knowledge there exists no algorithm able to compute the cokernel of the multiplication by p in the divisor class group of a curve $\mathcal{C}$ of genus g in polynomial time in g and the characteristic p. We instead opt to choose enough uniformly random elements of $\mathfrak{G}_N^p$ to generate the whole group. Since we know that $\mathfrak{G}_N^p$ is of the form $\mathbb{F}_p^n$ with n being an integer smaller than $g+1$, we know that we only need to select $O(g)$ elements on average. We use Algorithm 1 beforehand to ensure the existence of a solution. We refer to [4, Section 3.5] in which the author present an algorithm to select uniformly random elements in $\mathrm{Cl}^0(K_N)$. If K_N is seen as the regular function field of a curve $\mathcal{C}$, [4, Algorithm 3.7] presupposes the choice of a line bundle $\mathcal{L}$ over $\mathcal{C}$ of degree at least $2g+1$. Since we are working over finite fields, line bundles of arbitrary degrees exists and we can choose a line bundle of degree exactly $2g+1$. Then we can use [4, Algorithm 3.7] to pick uniformly random elements in $\mathrm{Cl}^0(K_N)$ represented by uniformly random effective divisors of degree $2g+1$ in polynomial time in g and $\log(q)$. However, [4, Algorithm 3.7] also suppose that the zeta function of $\mathcal{C}$ is known in order to ensure the uniform distribution of the divisors. The computation of the zeta function can be done in time polynomial in g and linear in b and p (precisely $\tilde{O}(pbd_x^6 d_y^4)$ bit operations [19]).

Remark 4.7. In [8, section 13.2] the authors also state that $\mathrm{Cl}^0(K_N)$ is generated by the places of degree less than $1+2\log_q(4g-2)$. This in turns guarantees the existence of D a generating divisor of $\mathfrak{G}_{N_*}^p$ of degree $\tilde{O}(d_x d_y)$. However the probability of generating $\mathfrak{G}_N^p$ with $O(g)$ uniformly chosen effective divisors of degree less than $1+\log_q(4g-2)$ could be very low which is why we do not use it for our algorithm.

From now on we will assume that we are able to pick uniformly random elements in $\mathrm{Cl}^0(K_N)$. If $\mathfrak{G}_N^p$ is of dimension r over $\mathbb{F}_p$ then we only need on average to select $O(r)$ elements to generate $\mathfrak{G}_N^p$.

We now discuss in more details the computation of the linear system representing the p-Riccati equation over some $\mathcal{L}(A(D))$. The main issue lies in the computation of the $(p-1)$-th derivative of the elements of a basis of $\mathcal{L}(A(D))$. Instead of computing their exact value in K_N, we compute their Taylor expansion up to a high enough precision.

Proposition 4.8. *Let $\Phi_N : K_N \to C_N$ denote the Frobenius endomorphism over K_N and $D \in \mathrm{Div}(K_N)$. Let $f \in \mathcal{L}(A(D))$. Then $\Phi_N^{-1}(f^{(p-1)} + f^p) \in \mathcal{L}(A(D))$.*

Proof. Let $\mathfrak{P} \in \mathbb{P}_{K_N}$. If $\mathfrak{P} \notin \operatorname{Supp}(A(D))$ then by definition of $A(D)$, f is not a ramified place and f has no poles in $\mathfrak{P}$. Thus neither $f^{(p-1)}$ nor f^p has a pole in $\mathfrak{P}$. Thus $\Phi_N^{-1}(f^{(p-1)} + f^p)$ has no pole in $\mathfrak{P}$. For $\mathfrak{P} \in \operatorname{Supp}(A(D))$, we let $t_{\mathfrak{P}}$ be a prime element of $\mathfrak{P}$. We know that

$$\nu_{\mathfrak{P}}(\Phi_N^{-1}(f^{(p-1)} + f^p)) \geqslant \min(p^{-1} \cdot (\nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)), \nu_{\mathfrak{P}}(f))$$

Besides we know that if $\nu_{\mathfrak{P}}(f) \leqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$ then $p^{-1} \cdot (\nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)) \geqslant \nu_{\mathfrak{P}}(f)$ so in that case we get that $\nu_{\mathfrak{P}}(\Phi_N^{-1}(f^{(p-1)} + f^p)) \geqslant \nu_{\mathfrak{P}}(f)$ which implies the desired result since $f \in \mathcal{L}(A(D))$. If now we have $\nu_{\mathfrak{P}}(f) > \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$ then $p^{-1} \cdot (\nu_{\mathfrak{P}}(f) + (p-1)(\nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)) > \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1$. Since valuations have to be integers we deduce that $\nu_{\mathfrak{P}}(\Phi_N^{-1}(f^{(p-1)} + f^p)) \geqslant \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) \geqslant -\nu_{\mathfrak{P}}(A(D))$. Thus $\Phi_N^{-1}(f^{(p-1)} + f^p) \in \mathcal{L}(A(D))$. □

Notation 4.9. From this point forward we assume that $K = \mathbb{F}_{p^b}(x)$, for $b \in \mathbb{N}^*$. We suppose that $N \in \mathbb{F}_{p^b}[x^p, y]$ is a fixed separable irreducible polynomial and set $N_*(x,y) \in \mathbb{F}_{p^b}[x,y]$ such that $N_*^p(Y) = N(Y^p)$. Let a be the p-th root of $y_N \in K_N$. Then $N_*(a) = 0$ and $K_N = K[a]$. We set $d_x = \deg_x N_*$ and $d_y = \deg_Y N_*$.

Definition 4.10. Let $f \in K_N$. There exist unique $f_0, \dots, f_{p-1} \in K_N$ such that

$$f = \sum_{i=0}^{p-1} f_i^p x^i.$$

For all $i \in [\![0; p-1]\!]$ We denote by $S_i(f) := f_i$ the i-th section of f.

Although we define sections for all $i \in [\![0; p-1]\!]$, we will really only be interested in S_{p-1} as shown in the following lemma:

Lemma 4.11. *For any $f \in K_N$,*

$$\Phi_N^{-1}(f^{(p-1)}) = -S_{p-1}(f).$$

Proof. Let $f := \sum_{i=0}^{p-1} f_i^p x^i$. It suffices to show that $f^{(p-1)} = -f_{p-1}^p$. But this is obvious since $f^{(p-1)} = (p-1)! f_{p-1}^p$ and $(p-1)! = -1 \mod p$. □

Thus another way of writing p-Riccati equation is

$$b - S_{p-1}(b) = a.$$

We now use the fact that Lemma 4.11 also holds over $K_{N,\mathfrak{P}}$ for any $\mathfrak{P} \in \mathbb{P}_{K_N}$. Let $\mathfrak{P}$ be a place over K_N that does not belong in $\mathrm{Supp}(A(D))$. Then the injective homomorphism from K_N to its $\mathfrak{P}$-completion induces an injective homomorphism of $\mathbb{F}_q$-vector spaces $\mathcal{L}(A(D)) \hookrightarrow \mathcal{G}_{\mathfrak{P}}[[t_{\mathfrak{P}}]]$. It follows that there exists a constant $N \in \mathbb{N}$ such that for all $f \in \mathcal{L}(A(D))$, $f = 0$ if and only if $\nu_{\mathfrak{P}}(f) \geqslant N$.

Lemma 4.12. *Let $\mathfrak{P} \in \mathrm{Div}(K_N)$, let D be an effective divisor of K_N and set $d := \deg(A(D))$. For any $f \in \mathcal{L}(A(D))$,*

$$f = 0 \Leftrightarrow \nu_{\mathfrak{P}}(f) > \frac{d}{\deg(\mathfrak{P})}.$$

Proof. Since $f \in \mathcal{L}(A(D))$, if $f \neq 0$ then we know that $\deg(f)_\infty \leqslant d$. But since $\deg(f)_\infty = \deg(f)_0$ we know that $\nu_{\mathfrak{P}}(f) \leqslant \frac{\deg(f)_\infty}{\deg(\mathfrak{P})} \leqslant \frac{d}{\deg(\mathfrak{P})}$. □

Thus it suffices for a function $f \in \mathcal{B}$ (where $\mathcal{B}$ is a basis of $\mathcal{L}(A(D))$) to compute the image of $f - S_{p-1}(f)$ modulo $t_{\mathfrak{P}}^{\left\lfloor \frac{\deg(A(D))}{\deg \mathfrak{P}} \right\rfloor + 1}$ in $\mathcal{G}_{\mathfrak{P}}[[t_{\mathfrak{P}}]]$. If one writes $f = \sum_{k=0}^{\infty} f_i t_{\mathfrak{P}}^i$ then $S_{p-1}(f)$ mod $t_{\mathfrak{P}}^{\left\lfloor \frac{\deg(A(D))}{\deg \mathfrak{P}} \right\rfloor + 1}$ can be deduced from the knowledge of the coefficients f_{pk+p-1} for $k \leqslant \frac{deg(A(D))}{\deg \mathfrak{P}}$. To that end we can compute the first $p \left\lfloor \frac{\deg(A(D))}{\deg \mathfrak{P}} \right\rfloor + p - 1$ coefficients of the Taylor expansion of f. In practice, we compute the Taylor expansion of a of which we know the minimal polynomial, in $t_{\mathfrak{P}}$ up to the desired precision by Newton iteration (note that by definition of $A(D)$, $a \in \mathcal{L}(A(D))$). This can be done in $\tilde{O}(p \deg(A(D)) d_y)$ operations in $\mathbb{F}_q$. Then, knowing that elements of $\mathcal{L}(A(D))$ are given by polynomials $F(x, a)$ we get their Taylor expansions by composition for an additional cost of $\tilde{O}(p \deg(A(D)) d_y)$ operations in $\mathbb{F}_q$.

Proposition 4.13. *Let Q_i be the quotient of the Euclidean division of $N_*(x, y)$ by y^{i+1} for any $i \in \mathbb{N}$. Then for any $f := \sum_{k=0}^{d_y - 1} f_k a^k \in K_N$ and any $i \in [\![0; d_y - 1]\!]$, $f_i = \mathrm{Tr}_{K_N/\mathbb{F}_q(x)} \left(\frac{Q_i(x,a) f}{\partial_y N_*(x,a)} \right)$.*

Proof. Let us fix $N_*(x, y) = \sum_{k=0}^{d_y} \eta_k(x) y^k$. From [16, Lemma 2 section III. 6] we know that $\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)} \left(\frac{a^i}{\partial_y N_*(x,a)} \right) = \frac{1}{\eta_{d_y}} \delta_{i, d_y - 1}$, for all $i \leqslant d - 1$. Thus the result holds for $i = d_y - 1$, since $Q_{d_y - 1} = \eta_{d_y}$. Then for all i we have $Q_i = Q_{i+1} y + \eta_{i+1}$. We assume the proposition to be true for $i + 1$. Then

$$\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)} \left(\frac{Q_i(x,a) f}{\partial_y N_*(x,a)} \right) = \mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)} \left(\frac{Q_{i+1}(x,a) a f}{\partial_y N_*(x,a)} \right) + \eta_{i+1} \mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)} \left(\frac{f}{\partial_y N_*(x,a)} \right)$$

and by hypothesis $\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)} \left(\frac{Q_{i+1}(x,a) a f}{\partial_y N_*(x,a)} \right)$ is the coefficient of a^{i+1} in af, which is given by $f_i - \frac{f_{d_y - 1} \eta_{i+1}}{\eta_{d_y}}$, while $Tr_{K_N/\mathbb{F}_{p^b}(x)} \left(\frac{f}{\partial_y N_*(x,a)} \right)$ is the coefficient of $a^{d_y - 1}$ of $\frac{f}{\eta_{d_y}}$.

$$\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)} \left(\frac{Q_i(x,a) f}{\partial_y N_*(x,a)} \right) = f_i - \frac{f_{d_y - 1} \eta_{i+1}}{\eta_{d_y}} + \eta_{i+1} \frac{f_{d_y - 1}}{\eta_{d_y}} = f_i.$$

□

Corollary 4.14. *Let D be an effective divisor over K_N and P be an irreducible polynomial in $\mathbb{F}_{p^b}[x]$ coprime with $\mathrm{Disc}(N_*)$ and the leading coefficient of N_*. If none of the places in $\mathrm{Supp}(D)$ divides P then for any $f \in \mathcal{L}(A(D))$, none of the coefficients of f in the basis $(1, a, \dots, a^{d_y-1})$ have a pole in P.*

Proof. Let l_c be the leading coefficient of N_*. The function $l_c a$ is integral and its minimal polynomial is $N_1 = l_c^{d_y-1} N_*(x, Y/l_c)$. We have $\mathrm{Disc}(N_1) = l_c^{d_y-1}\mathrm{Disc}(N_*)$ and $(\partial_Y N_*(x,a))_+ \leqslant (\partial_Y N_1(x, l_c a))_0 \leqslant (d_y-1)(l_c)_0 + (\mathrm{Disc}(N_*))_0$. This shows that for all i (with the notations of the previous proposition), $\frac{Q_i(x,a)}{\partial_y N_*(x,a)}$ has no poles that divides P since the poles of a are among those of l_c.
Let us now show that $\mathrm{Supp}(A(D))$ does not contain any place that divides P. Let $\mathrm{Diff}(K_{N_*})_0$ be the different divisor of K_{N_*} outside of the places at infinity. Since $l_c a$ is integral we know that $\mathrm{Diff}(K_{N_*})_0 \leqslant (\partial_Y N_1(x, l_c a))_0 \leqslant (d_y-1)(l_c)_0 + (\mathrm{Disc}(N_*))_0$. Thus $\mathrm{Supp}(A(D)) \cap \mathrm{Supp}(P) \subset (\mathrm{Supp}(\mathrm{Diff}(K_N)) \cap \mathrm{Supp}(P)) \cup (\mathrm{Supp}(a)_\infty \cap \mathrm{Supp}(P) \subset \mathrm{Supp}(l_c) \cap \mathrm{Supp}(P) = \varnothing$. Thus if we set $\mathcal{O}_P$ the valuation ring associated to P in $\mathbb{F}_{p^b}(x)$ and $\mathcal{O}'_P$ its integral closure in K_N, then for all i and all $f \in \mathcal{L}(A(D))$, $\frac{Q_i(x,a)f}{\partial_y N_*(x,a)} \in \mathcal{O}'_P$. It follows that if f_i denotes the i-th coefficient of f then $f_i = \mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}\left(\frac{Q_i(x,a)f}{\partial_y N_*(x,a)}\right) \in O_P$ and f_i has no pole in P. □

When knowing the Taylor expansion of a up to the desired precision, computing the Taylor expansion of an element f of $\mathcal{L}(A(D))$ by composition requires to compute the Taylor expansion of its coefficients. This can be done in $\tilde{O}(p\max(\eta, \deg A(D))d_y)$ operations in $\mathbb{F}_{p^b}$ where η is the degree of the coefficients of f. As we show now, by construction of $A(D)$, η and $\deg(A(D))$ have the same order of magnitude.

Lemma 4.15. *Let $f \in K_N$ and $\mathfrak{P} \in \mathbb{P}_{\mathbb{F}_{p^b}(x)}$.*

$$\nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}(f)) \geqslant \min_{\mathfrak{P}'|\mathfrak{P}} \left\lfloor \frac{\nu_{\mathfrak{P}'}(f)}{e(\mathfrak{P}'|\mathfrak{P})} \right\rfloor.$$

Proof. Let $\mathcal{O}_{\mathfrak{P}}$ be the valuation ring associated to the place $\mathfrak{P}$ and $\mathcal{O}'_{\mathfrak{P}}$ be its integral closure in K_N. For any $f \in K_N$, if $f \in \mathcal{O}'_{\mathfrak{P}}$ then $\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}(f) \in \mathcal{O}_{\mathfrak{P}}$ [17, Corollary 3.3.2].
It follows that if $\mathfrak{P}$ is a pole of $\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}(f)$, then at least one of the places lying under $\mathfrak{P}$ is a pole of f. Let $\mathfrak{P}^*$ above $\mathfrak{P}$ be such that

$$\left\lfloor \frac{\nu_{\mathfrak{P}^*}(f)}{e(\mathfrak{P}^*|\mathfrak{P})} \right\rfloor = \min_{\mathfrak{P}'|\mathfrak{P}} \left\lfloor \frac{\nu_{\mathfrak{P}'}(f)}{e(\mathfrak{P}'|\mathfrak{P})} \right\rfloor.$$

Set $k = \left\lceil \frac{-\nu_{\mathfrak{P}^*}(f)}{e(\mathfrak{P}^*|\mathfrak{P})} \right\rceil$ and $P \in K_N$ a prime element of $\mathfrak{P}$. Then for any $\mathfrak{P}'$ above $\mathfrak{P}$ we have

$$\nu_{\mathfrak{P}'}(P^k f) = k e(\mathfrak{P}'|\mathfrak{P}) + \nu_{\mathfrak{P}'}(f).$$

By definition $k \geqslant -\frac{\nu_{\mathfrak{P}'}(f)}{e(\mathfrak{P}'|\mathfrak{P})}$ thus $\nu_{\mathfrak{P}'}(P^k f) \geqslant 0$. It follows that

$$\begin{aligned} \nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}(P^k f)) &= \nu_{\mathfrak{P}}(P^k \mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}(f)) \\ &= k + \nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}(f)) \\ &\geqslant 0 \\ \nu_{\mathfrak{P}}(\mathrm{Tr}_{K_N/\mathbb{F}_{p^b}(x)}(f)) &\geqslant -k \end{aligned}$$

which is the desired result. □

Proposition 4.16. *Let D be an effective divisor over K_N and $f = \frac{1}{f_{-1}} \sum_{i=0}^{d_y-1} f_i a^i \in \mathcal{L}(A(D))$ where $f_{-1}, f_0, \dots, f_{d_y-1} \in \mathbb{F}_q[x]$ are globally coprime polynomials.*
Then for any $i \in [\![-1; d_y - 1]\!]$, both $\deg(f_i)$ and $\deg(A(D))$ are in $O(\deg(D) + d_x d_y)$.

Proof. Let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial and let Q_i denote the quotient of the Euclidean division of N_* by Y^{i+1} applied to x and a. If P is a pole of $\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f)$:

$$\begin{aligned}\nu_P(\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f))\deg(P) &\geqslant \min_{\mathfrak{P}|P}\left\lfloor \frac{\nu_{\mathfrak{P}}(Q_i)+\nu_{\mathfrak{P}}(f)}{e(\mathfrak{P}|P)}\right\rfloor \deg(P)\\ &\geqslant \sum_{\mathfrak{P}|P}(\nu_{\mathfrak{P}}(Q_i)+\nu_{\mathfrak{P}}(f))\deg(\mathfrak{P})\\ &\geqslant \sum_{\mathfrak{P}|P}(\nu_{\mathfrak{P}}(Q_i)-\nu_{\mathfrak{P}}(A(D)))\deg(\mathfrak{P})\end{aligned}$$

It follows that

$$\deg(\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f))_\infty \leqslant \deg(Q_i)_\infty + \deg(A(D)).$$

But $A(D) \leqslant D + \mathrm{Diff}(K_N) - 2(x)_\infty + (a)_\infty$. Thus, since $\deg(\mathrm{Diff}(K_N) - 2(x)_\infty) = 2g-2$, where g denotes the genus of K_N, $\deg A(D) \leqslant \deg(D) + d_x + 2g - 2$. Since $g \leqslant (d_x-1)(d_y-1)$ (see [3, Corollary 2.6]), it follows that $\deg(A(D)) = O(\deg(D) + d_x d_y)$ and $\deg(\mathrm{Tr}_{K_{N_*}/\mathbb{F}_q(x)}(Q_i f))_\infty = O(d_x d_y + \deg(D))$. Thus, according to Corollary 4.13, $\partial_y N_*(x,a)f$ has coefficients of degree $O(d_x d_y + \deg(D))$. Since $(\partial_y N_*(x,a)f)^{-1}$ has coefficients of size $O(d_x d_y)$, the result follows. □

Notation 4.17. Let $\mathcal{B}$ be a basis of $\mathcal{L}(A(D))$ with $D \in \mathrm{Div}(K_N)$, and $P \in \mathbb{F}_q[x]$ an irreducible polynomial verifying the hypothesis of Corollary 4.14. Let $\mathfrak{P} \in \mathbb{P}(K_N)$ be lying over P and $t_{\mathfrak{P}}$ be a prime element of $\mathfrak{P}$ and B_0 be an $\mathbb{F}_p$-basis of $\mathcal{G}_{\mathfrak{P}}$. We denote by $\mathcal{T}_{\mathfrak{P}}(\mathcal{B})$ the matrix with coefficient in $\mathbb{F}_p$ whose columns are the Taylor expansion of the image of elements of $\mathcal{B}$ by the map $f \mapsto f - S_{p-1}(f)$, at precision $\left\lfloor \frac{\deg A(D)}{\deg \mathfrak{P}}\right\rfloor + 1$ written in the basis $\mathcal{B}_0 \times (t_{\mathfrak{p}}^i)_{i\deg(P)\leqslant \deg(A(D))}$.

We can now write the final version of our algorithm the solve the p-Riccati equation in Algorithm 2.

Input: $N_* \in \mathbb{F}_{p^b}[x,y]$ an irreducible separable polynomial.
Output: $f \in K[a]$, where a is a root of N_* such that $f^{(p-1)} + f^p = a^p$, if such an f exists.

(1) Test if $N_*^p(\partial)$ is irreducible using Algorithm 1.
(2) **If** $N_*^p(\partial)$ is irreducible **return**.
(3) Set $d_y := \deg_Y N_*$ and $K_{N_*} := K[a] = {}^{\mathbb{F}_{p^b}(x)[y]}\!/_{(N_*)}$.
(4) Compute $(a)_\infty$.
(5) Compute $A := \mathrm{Diff}(K_{N_*}) - 2(x)_\infty$.
(6) Set $D := 0$, $n := 0$ and $l = 0$.
(7) Select $(D_1, \ldots, D_n) \in \mathrm{Div}(K_N)^n$ a family of n randomly chosen divisors of degrees $2g+1$
(8) $D \leftarrow D + D_1 + \ldots D_n$, $l \leftarrow l + n$, $n \leftarrow n + \max(1, l)$ and $A(D) := A$.
(9) **For** $\mathfrak{P}$ Supp D **do:**
  - $A(D) \leftarrow A(D) + \mathfrak{P}$
(10) $A(D) \leftarrow \max((a)_-, A(D_1, \ldots, D_{g+1}))$.
(11) Compute a basis $\mathcal{B}$ of $\mathcal{L}(A(D))$
(12) Select $P \in \mathbb{F}_q[x]$ an irreducible polynomial verifying the hypothesis of Corollary 4.14 with respect to D and $\mathfrak{P}|P$.
(13) Compute the Taylor expansion V of a in $t_{\mathfrak{P}}$ at precision $\left\lfloor \frac{\deg A(D_1,\ldots,D_{g+1})}{\deg \mathfrak{P}}\right\rfloor + 1$
(14) Compute $\mathcal{T}_{\mathfrak{P}}(\mathcal{B})$ (see Notation 4.17).
(15) Solve $\mathcal{T}_{\mathfrak{P}}(\mathcal{B})X = V$.
(16) **If** a solution X exists reconstruct a solution to the p-Riccati equation from it and **return** it.
(17) **Else** redo from step 7

Algorithm 2: p-Riccati_with_irreducibility

Theorem 4.18. *Let r be the dimension of $\mathfrak{G}_N^p$ over $\mathbb{F}_p$, where $N(y^p) = N_*^p(y)$. We have $r \leqslant d_x d_y$ and Algorithm 2 returns if it exists a solution of the p-Riccati equation relative to N whose coefficients are of degree $O(rd_xd_y)$ at the cost of*

- *testing the irreducibility of $N_*^p(\partial)$ using Algorithm 1*
- *factoring the divisors $(a)_\infty$ and $(x)_\infty$*
- *computing the different divisor of K_N*
- *selecting $O(r)$ uniformly random elements of $\mathrm{Div}(K_{N_*})$ of degree $2g+1$*
- *computing $O(\log_2(r))$ basis of Riemann-Roch spaces of dimension $O(rd_xd_y)$.*
- *$\tilde{O}(bpr^2d_x^2d_y^3 + (brd_xd_y)^\omega)$ bit operations.*

The total complexity of the computation is polynomial in b, d_x and d_y and linear in p.

Proof. The cost of steps (1) to (5) in Algorithm 2 is the cost of using Algorithm 1. The cost of step (4) is the cost of computing $(a)_\infty$, $(x)_\infty$ and $\mathrm{Diff}(K_{N_*})$.
The degree of D roughly doubles at each repetition of steps (7) to (15) and are repeated on average $O(\log_2(r))$ times after which we have selected $O(r)$ uniformly random elements of $\mathfrak{G}_N^p$ which form a generating family of it. The cost of steps (7) to (10) is essentially the cost of selecting uniformly random divisors of degree $2g+1$. By definition of $A(D)$, it is of degree $O(d_xd_y + rg)$. Since $g = O(d_xd_y)$ we find that $A(D)$ is of degree $O(rd_xd_y)$.
Since we know that the solution of the p-Riccati equation constructed by Algorithm 2 is an element of $\mathcal{L}(A(D))$, Proposition 4.16 states that this solution has coefficients of degree $O(rd_xd_y)$.
The cost of step (11) is thus the cost of computing a basis of $\mathcal{L}(A(D))$ which is of dimension $O(\deg(A(D)) \subset O(rd_xd_y)$.
Step (11) requires the computation of $\mathrm{Disc}(N_*)$ whose cost is negligible in regard of the final result.
The cost of steps (13) and (14) is the cost of computing the Taylor expansions of $O(rd_xd_y)$ functions in $\mathcal{L}(A(D))$ using Newton iterations. The cost for one such function is $\tilde{O}(bprd_xd_y^2)$ bit operations so the total cost is $\tilde{O}(bpr^2d_x^2d_y^3)$. Using this we can compute the Taylor expansions of $h - S_{p-1}(h)$ for $h \in \mathcal{B}$ at precision $O(\frac{rd_xd_y}{\deg(\mathfrak{P})})$. We recall that $\mathcal{B}$ is an $\mathbb{F}_{p^b}$-basis of $\mathcal{L}(A(D))$. Since we want the result on an $\mathbb{F}_p$-basis, we still need to multiply the result by an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^b}$ which can be done in $\tilde{O}((brd_xd_y)^2\log(p))$ bit operations. Thus steps (13) and (14) can be done in $\tilde{O}(bpr^2d_x^2d_y^3 + (brd_xd_y)^2)$ binary operations.
Finally, step (14) is a matter of solving a $\mathbb{F}_p$-linear system of size $O(brd_xd_y) \times O(brd_xd_y)$ which can be done in $\tilde{O}((brd_xd_y)^\omega)$ operations in $\mathbb{F}_p$.
Reconstructing the solution to the p-Riccati equation is a matter of summing $O(rd_xd_y^2)$ polynomial coefficients in $\mathbb{F}_{p^b}[x]$ of degree $O(rd_xd_y)$ which can be done in $\tilde{O}(br^2d_x^2d_y^3\log(p))$ bit operations.
The sum of those cost yield the final result. □

Remark 4.19. In our experiments we often found that $r = O(1)$ hence the expression of the complexity in terms of this additional parameter and not purely in terms of d_x and d_y.

5. Application to factorisation of differential operators

Now that we have a working algorithm to solve p-Riccati equations and degree bounds for the solutions, we discuss how it fits in the broader context of differential operators factorisation. We begin by discussing how to go from a solution of the p-Riccati equation relative to N, to the corresponding irreducible divisor of $N(\partial^p)$.

Proposition 5.1. *Let $N \in C[Y]$ be a separable irreducible polynomial and $f \in K_N$ be a solution to the p-Riccati equation relative to N. If L is a generator of the ideal of operators in $K\langle\partial\rangle$ which are left multiple of $\partial - f$ then L is an irreducible divisor of $N(\partial^p)$.*

Proof. We consider $K\langle\partial\rangle_{\leqslant\deg(N)} = \{L \in K\langle\partial\rangle | \mathrm{ord}(L) \leqslant \deg(N)\}$ and the K-linear map $\psi_N : K\langle\partial\rangle_{\leqslant\deg(N)} \to {}^{K_N\langle\partial\rangle}/_{K_N\langle\partial\rangle(\partial-f)}$ which maps an operator to its image modulo $\partial - f$.
Since $\dim_K K\langle\partial\rangle_{\leqslant\deg(N)} = \deg(N)+1$ and $\dim_K {}^{K_N\langle\partial\rangle}/_{K_N\langle\partial\rangle(\partial-f)} = \deg(N)$, ψ_N has a nontrivial kernel. In particular $\mathrm{ord}(L) \leqslant \deg(N)$. Let us show that L is a divisor of $N(\partial^p)$. We claim that $\gcd(L, N(\partial^p))$ is a multiple of $\partial - f$. Indeed, $\partial - f$ is a divisor of $\partial^p - y_N$ which is a divisor of $N(\partial^p)$ and is also a divisor of L. By definition of L, $\gcd(L, N(\partial^p)) = L$ and L is a divisor of $N(\partial^p)$. Since $\mathrm{ord}(L) \leqslant \deg(N)$, it has to be irreducible according to Proposition 2.6.(v). □

The proof of this result also points to an algorithmic way of deducing an irreducible divisor of $N(\partial^p)$ from a solution to the p-Riccati equation relative to N.

Corollary 5.2. *Let $N \in C[Y]$ be an irreducible polynomial and $f \in K_N$ be a solution to the p-Riccati equation relative to N. Set $d_y = \deg(N)$.*
Let $a_0 = 1$ and for all $i \in [\![0; d_y - 1]\!]$, $a_{i+1} = a_i f + a_i'$. Consider the matrix $M(f)$ in $M_{d_y, d_y+1}(K)$ whose columns are the coefficients of the a_i (in some fixed K basis of K_N). Then for any nonzero $v = (v_0, \dots, v_{d_y}) \in \ker(M)$, $\sum_{i=0}^{d_y} v_i \partial^i$ is an irreducible divisor of $N(\partial^p)$.

Proof. We consider $K\langle\partial\rangle_{\leqslant \deg(N)} = \{L \in K\langle\partial\rangle | \mathrm{ord}(L) \leqslant \deg(N)\}$ and the K-linear map $\psi_N : K\langle\partial\rangle_{\leqslant \deg(N)} \to {}^{K_N\langle\partial\rangle}/_{K_N\langle\partial\rangle(\partial - f)}$ which maps an operator to its image modulo $\partial - f$. For dimensional reasons, we know that ψ_N has a nontrivial kernel. Besides, any nonzero element of the kernel is a multiple of $\partial - f$ in $K\langle\partial\rangle$ of order less than $\deg(N)$. From Proposition 5.1 and Proposition 2.6.(v) this means that it is a irreducible divisor of $N(\partial^p)$. We claim that the matrix $M(f)$ is the matrix of this restriction from the basis $(1, \partial, \dots, \partial^d)$ to the K-basis of $K_N \simeq {}^{K_N\langle\partial\rangle}/_{K_N\langle\partial\rangle(\partial - f)}$ we have fixed.
Indeed let $L' = \partial^k l_k + \partial^{k-1} l_{k-1} + \cdots + l_0$ be any differential operator in $K_N\langle\partial\rangle$. Then there exists an operator $B = \partial^{k-1} b_{k-1} + \cdots + \partial b_1 + b_0 \in K_N\langle\partial\rangle$ and $b_{-1} \in K_N$ such that

$$L' = B(\partial - f) + b_{-1}.$$

Then

$$\begin{aligned} L' &= \sum_{i=0}^{k-1} \partial^{i+1} b_i - \sum_{i=0}^{k-1} \partial^i (b_i' + f b i) + b_{-1} \\ &= \partial^k b_{k-1} + \sum_{i=0}^{k-1} \partial^i (b_{i-1} - b_i' - f b_i) \end{aligned}$$

and we find that $l_i = b_{i-1} - b_i' - f b_i$, or equivalently $b_{i-1} = l_i + b_i' + f b_i$ and $b_{k-1} = l_k$. We apply this result to $L' = \partial^k$. It immediately follows that the corresponding b_{-1} is the k-th term of the recursive sequence defined by $a_0 = 1$, $a_{i+1} = a_i f + a_i'$, which concludes the proof. □

It is now easy to see that the coefficients of $\mathrm{gcrd}(N(\partial^p), \varphi_N^{-1}(\partial - f))$ are of size independent from p as long as it is also the case for the coefficients of f, which we know to hold true from Theorem 4.18.

Lemma 5.3. *We keep the notation of Corollary 5.2 with the additional hypothesis that $f \in \mathcal{L}(A(D))$ where $D \in \mathrm{Div}(K_N)$ is a generating divisor of $\mathfrak{G}_N^p$. Then for all $i \in [\![1; d_y]\!]$,*

$$a_i \in \mathcal{L}\big(iA(D) + (i-1)\max(\mathrm{Diff}(K_N) - 2(x)_\infty, 0)\big).$$

Proof. We know that $a_1 = f \in \mathcal{L}(A(D))$ so the proposition is verified here. We now suppose that the conclusion of the lemma holds for the index i. Let $\mathfrak{P} \in \mathbb{P}_{K_N}$ be a place and $t_\mathfrak{P}$ be a prime element of it. Then

$$\nu_\mathfrak{P}(a_i') \geqslant \nu_\mathfrak{P}(a_i) + \nu_\mathfrak{P}(t_\mathfrak{P}') - 1.$$

In all generality, $1 - \nu_\mathfrak{P}(t_\mathfrak{P}')$ is precisely one more than the valuation of $\mathrm{Diff}(K_N) - 2(x)_\infty$ in $\mathfrak{P}$. In particular if $\mathfrak{P}$ is ramified then it is smaller than twice the valuation of $\mathrm{Diff}(K_N) - 2(x)_\infty$ which is smaller than the valuation of $A(D) + \mathrm{Diff}(K_N) - 2(x)_\infty$. If it is not ramified then either a_i does not have a pole in $\mathfrak{P}$, in which case neither does a_i' or it has one and we have both $\nu_\mathfrak{P}(a_i') \geqslant \nu_\mathfrak{P}(a_i) - 1$ and $\nu_\mathfrak{P}(A(D)) \geqslant 1$. Thus $\nu_\mathfrak{P}(a_i) - \nu_\mathfrak{P}(a_i')$ is once again smaller than the valuation of $A(D) + \mathrm{Diff}(K_N) - 2(x)_\infty$. Therefore

$$a_i' \in \mathcal{L}\big((i+1)A(D) + i\max(\mathrm{Diff}(K_N) - 2(x)_\infty, 0)$$

Furthermore since $f \in A(D)$, so too does $f a_i$ and the result follows. □

Input: $N_* \in \mathbb{F}_q(x)[Y]$ an irreducible separable polynomial, f a solution of the p-Riccati equation relative to N_*.
Output: $L \in K\langle\partial\rangle$ the smallest monic multiple of $\partial - f$ with coefficients in K.

(1) Set $K_{N_*} = \mathbb{F}_q(x)[a]$ with a a root of N_*.
(2) Set $d_y := \deg N_*$.
(3) Set $a_0 := 1$.
(4) **For** i going from 1 to d_y **do**:
    - Set $a_i := a'_{i-1} + f a_{i-1}$
(5) Set $M \in M_{d,d+1}(\mathbb{F}_q(x))$ the matrix whose columns are the a_i written in the $\mathbb{F}_q(x)$-basis $(1, a, \dots, a^{d_y-1})$ of K_{N_*}.
(6) Solve $MX = 0$.
(7) Reconstruct L from a solution and return it.

Algorithm 3: Irreducible_factors

Theorem 5.4. *Let $N_* \in \mathbb{F}_{p^b}[x, y]$ be a separable irreducible polynomial. Keeping the notations of the previous sections, we suppose that $\dim_{\mathbb{F}_p} \mathfrak{G}^p_{N_*} = r$. Using Algorithm 2 we can compute a solution f of the p-Riccati equation relative to N whose coefficients are of degrees $O(rd_x d_y)$. Then Algorithm 3 computes an irreducible divisor of $N_*^p(\partial)$ whose coefficients are of degree $O(rd_x d_y^3)$ in $\tilde{O}(rd_x d_y^{\omega+2})$ operations in $\mathbb{F}_{p^b}$.*

Proof. The coefficients of the irreducible divisor returned by Algorithm 3 can be expressed using the minors of the matrix M whose columns are the a_i written in the basis $(1, a, \dots, a^{d_y-1})$. Since we know that f has coefficients of degree $O(rd_x d_y)$, by immediate recurrence we get that a_i has coefficients of degree $O(rd_x d_y^2)$. Thus the minors of M are of degree $O(d_y^2 r d_x d_y)$ since M is a matrix of size $d \times (d+1)$. Furthermore, the coefficients a_i can all be computed in $\tilde{O}(rd_x d_y^3)$ operations in $\mathbb{F}_q$. It finally remains to solve a linear system of size $d \times (d+1)$ with coefficients in $\mathbb{F}_q(x)$ of degree $O(rd_x d_y^2)$. This can be done in in $\tilde{O}(rd_x d_y^{\omega+2})$ operations in $\mathbb{F}_{p^b}$ [18]. □

Remark 5.5. In practice we have observed that the growth of the size of the coefficients, from those of the solution to the p-Riccati equation, to those of the corresponding irreducible divisor of $N(\partial^p)$, is only linear in d_y (and not quadratic as shown in Theorem 5.4). We infer that the situation is similar to seeking the minimal polynomial of an algebraic function in some $K[a]$.

References

[1] Alman, J., and Vassilevska Williams, V. A refined laser method and faster matrix multiplication. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)* (2021), [Society for Industrial and Applied Mathematics (SIAM)], Philadelphia, PA, pp. 522–539.

[2] BaNaSt12, J.-D., Nart, E., and Stainsby, H. D. Complexity of OM factorizations of polynomials over local fields. *LMS J. Comput. Math. 16* (2013), 139–171.

[3] Beelen, P. A generalization of Baker's theorem. *Finite Fields Appl. 15*, 5 (2009), 558–568.

[4] Bruin, P. Computing in Picard groups of projective curves over finite fields. *Math. Comp. 82*, 283 (2013), 1711–1756.

[5] Cantor, D. G., and Kaltofen, E. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform. 28*, 7 (1991), 693–701.

[6] Chyzak, F., Goyer, A., and Mezzarobba, M. Symbolic-numeric factorization of differential operators. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2022), ISSAC '22, Association for Computing Machinery, p. 73–82.

[7] Cluzeau, T. Factorization of differential systems in characteristic p. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation* (2003), ACM, New York, pp. 58–65.

[8] Edixhoven, B., and Couveignes, J.-M., Eds. *Computational aspects of modular forms and Galois representations*, vol. 176 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2011. How one can compute in polynomial time the value of Ramanujan's tau at a prime.

[9] Gille, P., and Szamuely, T. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[10] Grigor'ev, D. Complexity of factoring and calculating the gcd of linear ordinary differential operators. *Journal of Symbolic Computation 10*, 1 (1990), 7–37.

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

[12] Harvey, D., and van der Hoeven, J. Integer multiplication in time $O(n \log n)$. *Ann. of Math. (2) 193*, 2 (2021), 563–617.

[13] Kaltofen, E., and Villard, G. On the complexity of computing determinants. *Comput. Complex. 13*, 3–4 (Feb. 2005), 91–130.
[14] Poteaux, A., and Weimann, M. Local polynomial factorisation: Improving the montes algorithm. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2022), ISSAC '22, Association for Computing Machinery, p. 149–157.
[15] Poteaux, A., and Weimann, M. Fast integral basis computation.
[16] Serre, J. *Corps locaux*. Actualités scientifiques et industrielles. Hermann, 2004.
[17] Stichtenoth, H. *Algebraic Function Fields and Codes*, 2nd ed. Springer Publishing Company, Incorporated, 2008.
[18] Storjohann, A. High-order lifting and integrality certification. vol. 36. 2003, pp. 613–648. International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).
[19] Tuitman, J. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl. 45* (2017), 301–322.
[20] van der Put, M. Differential equations in characteristic p. vol. 97. 1995, pp. 227–251. Special issue in honour of Frans Oort.
[21] van der Put, M. Reduction modulo p of differential equations. *Indag. Math. (N.S.) 7*, 3 (1996), 367–387.
[22] van der Put, M. Modular methods for factoring differential operators. Unpublished manuscript (Preliminary Version).
[23] van der Put, M., and Singer, M. F. *Galois theory of linear differential equations*, vol. 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.
[24] Van Hoeij, M. Factorization of differential operators with rational functions coefficients. *Journal of Symbolic Computation 24*, 5 (1997), 537–561.