Factoring differential operators over algebraic curves in positive characteristic

Raphaël Pagès

▶ **To cite this version:**

Raphaël Pagès. Factoring differential operators over algebraic curves in positive characteristic. ISSAC 2022 - International Symposium on Symbolic and Algebraic Computation, Jul 2022, Lille, France. hal-03759105

HAL Id: hal-03759105
https://hal.science/hal-03759105v1

Submitted on 23 Aug 2022

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

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

Factoring differential operators over algebraic curves in positive characteristic

Raphaël Pagès
Institut de Mathématiques de Bordeaux
University of Bordeaux
Talence, France, 33 405
https://www.math.u-bordeaux.fr/~rpages/

May 20, 2022

Abstract

We present an algorithm for factoring linear differential operators with coefficients in a finite separable extension of $\mathbb{F}_p(x)$. Our methods rely on specific tools arising in positive characteristic: p-curvature, structure of simple central algebras and p-Riccati equations.

1 Introduction

Studying and solving differential equations has been an important subject on mathematicians' mind since the invention of differential calculus and has found many applications. Although those equations are generally studied on real or complex variables, there is an algebraic counterpart to this theory, which makes sense over any base field, including number fields, p-adic fields and fields of positive characteristic. Applications include points counting on elliptic curves [9], isogeny computations [8, 6] and, more generally, the study of (the cohomology of) many arithmetic varieties.

In this work, we focus on linear differential equations of the form $L(y) = 0$ where

$$L = a_r(x)\partial^r + a_{r-1}(x)\partial^{r-1} + \cdots + a_1(x)\partial + a_0(x)$$

and the $a_i(x)$ are regular functions on an algebraic curve. The variable ∂ acts by derivation and L is thus a differential operator. The set of differential operators is provided with a ring structure derived from the Leibniz rule. A natural question arising when studying linear differential operators is that of factorisation.

The case of operators with coefficients in $\mathbb{C}(x)$ is well understood and several algorithms have been proposed throughout the years [7, 14, 3]. They usually rely on transcendental arguments, *e.g.* on properties of the monodromy group. In characteristic p, the monodromy does not exist but other powerful tools are available. One of them is the p-curvature: it was used in the context of factorisation for the first time by van der Put [11, 12]. In his PhD thesis, Cluzeau developed this approach and described a factorisation algorithm for linear differential systems over $\mathbb{F}_q(x)$ (where $\mathbb{F}_q$ is a finite field of characteristic p) [4, 5]. In this work, we present an algorithm that completely factors any differential operator with coefficients in a finite separable extension K of $\mathbb{F}_p(x)$.

2 Main ingredients

Let K be a finite separable extension of $\mathbb{F}_p(x)$. The natural derivation $\frac{\mathrm{d}}{\mathrm{d}x}$ extends uniquely to K and we let $K\langle\partial\rangle$ denote the ring of linear differential operators with coefficients in K. For $L \in K\langle\partial\rangle$, we set $\mathcal{D}_L := {}^{K\langle\partial\rangle}/_{K\langle\partial\rangle L}$. Here are the main ingredients that we will be using in our algorithm:

(I1) the one-to-one decreasing bijection between the set of right divisors of L (up to a multiplicative element of $K^\times$) and the set of $K\langle\partial\rangle$-submodules of $\mathcal{D}_L$ given by

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

this bijection also induces nice relations between the sum and intersection of submodules, and the greatest common right divisor and least common left multiple of operators respectively,

(I2) the p-curvature of L which will allow us to find a first factorisation of L as a product of operators verifying additional properties,

(I3) the arising central simple algebra structure and the Morita equivalence which will allow us to rephrase our problem through the prism of linear algebra and eventually reduce it to solving a "p-Riccati" equation,

(I4) tools of algebraic geometry such as the Jacobian of an algebraic curve to solve this equation.

3 Using the p-curvature

For any $f \in K$, $\frac{\mathrm{d}}{\mathrm{d}x} f^p = 0$. The set of elements of the form f^p forms the subfield of constants of K which we denote by C. Additionally for any $f \in K$, $\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^p f = 0$. Thus the left multiplication by ∂^p induces a K-linear endomorphism of $\mathcal{D}_L$: it is the so-called "p-curvature", which we denote by ψ_p^L. Its characteristic polynomial $\chi(\psi_p^L)$ has coefficients in C. We factor $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$ in the ring $C[Y]$ (commutative factorisation) where the $N_i(Y)$ are pairwise distinct irreducible polynomials over C. The kernel decomposition lemma states:

$$\mathcal{D}_L = \bigoplus_{i=1}^{n} \ker N_i^{\nu_i}(\psi_p^L).$$

Applying (I1), this decomposition translates to a first factorisation of L:

Theorem 1. *There exists a factorisation $L = L_1 \cdots L_n$ such that $\chi(\psi_p^{L_i}) = N_i^{\nu_i}(Y)$ for all $i \in \{1, \ldots, n\}$ and $L_n = \mathrm{gcrd}(L, N_n^{\nu_n}(\partial^p))$.*

Remark 2. Since $\mathcal{D}_L$ decomposes as a direct sum of submodules, we even get a lclm factorisation: $L = \mathrm{lclm}_{i=1}^n(\mathrm{gcrd}(L, N_i^{\nu_i}(\partial^p)))$.

From what precedes, we can safely suppose that $\chi(\psi_p^L)$ is a power of an irreducible polynomial in $C[Y]$ of the form $N^\nu(Y)$. By recursively considering the $\mathrm{gcrd}(L, N(\partial^p)^i)$, we can even further assume that L is a divisor of $N(\partial^p)$ for some irreducible polynomial N in $C[Y]$.

4 Factorisation of central irreducible elements

Let $L \in K\langle\partial\rangle$ be a divisor of some $N(\partial^p)$ with N irreducible in $C[Y]$. The quotient $\mathcal{D}_L$ has a structure of a $\mathcal{D}_{N(\partial^p)}$-module. Write $C_N = {}^{C[Y]}/_{(N)}$; it is a field extension of C. Let y_N be the image of Y in C_N. To avoid technicalities, we shall assume that C_N is separable. We set $K_N = K \cdot C_N$.

Theorem 3 ([10, 11, 2]). *The quotient ring $\mathcal{D}_{N(\partial^p)}$ is a simple central algebra over C_N.*

Using the Artin-Wedderburn theorem [1, Thm. 2.1.3], one shows that $\mathcal{D}_{N(\partial^p)}$ is either a division algebra or isomorphic to $M_p(C_N)$ (the ring of $p \times p$ matrices over C_N). In the former case, $\mathcal{D}_{N(\partial^p)}$ has no nontrivial zero divisor, meaning that $N(\partial^p)$ itself is irreducible.

Let us now suppose that $\mathcal{D}_{N(\partial^p)}$ is a matrix algebra. The Morita equivalence [1, §6] provides us with a (nonexplicit) decreasing bijection between submodules of $\mathcal{D}_{N(\partial^p)}$ and sub-C_N-vector spaces of C_N^p. Furthermore, if $N(\partial^p)$ factors as LL' then $\mathcal{D}_L$ is identified with $\mathcal{D}_{N(\partial^p)}L' \subset \mathcal{D}_{N(\partial^p)}$. We write V for the corresponding subspace of C_N^p. Combining Morita equivalence with (I1), we conclude that irreducible divisors of L are in one-to-one correspondence with hyperplanes of V. Those can be found by computing the intersections of V with generic hyperplanes of C_N^p. Specifically, what we need is a family of p hyperplanes of C_N^p whose intersection is reduced to zero, which in turn corresponds to finding a factorisation of $N(\partial^p)$ as an lclm of irreducible differential operators.

There is now an isomorphism $\varphi_N : {}^{K\langle\partial\rangle}\!/_{(N(\partial^p))} \xrightarrow{\sim} {}^{K_N\langle\partial\rangle}\!/_{(\partial^p - y_N)}$. Thus finding irreducible divisors of N amounts to finding irreducible divisors of $\partial^p - y_N$ with coefficients in K_N. Such divisors are of the form $\partial - f$, with $f \in K_N$ verifying the following "p-Riccati" equation:

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

We let $\mathcal{S}_N$ be the set of solutions of (1). It turns out that $\mathcal{S}_N$ can be fully obtained from a particular solution by adding logarithmic derivatives of functions in K_N.

Theorem 4. *Set $\mathcal{L}_f := \mathrm{lclm}\big(\mathrm{gcrd}\big(N(\partial^p),\, \varphi_N^{-1}(\partial - f)\big),\, L'\big) \cdot L'^{-1}$.*

i) If $L = N(\partial^p)$ then $f \mapsto \mathcal{L}_f$ is a one-to-one correspondence between $\mathcal{S}_N$ and the set of irreducible right divisors of $N(\partial^p)$.

ii) In general, all irreducible right divisors of L are of the form $\mathcal{L}_f$ with $f \in \mathcal{S}_N$.

iii) For all $f \in \mathcal{S}_N$, $L = \mathrm{lclm}\big(\mathcal{L}_f, \mathcal{L}_{f+\frac{1}{x}}, \ldots, \mathcal{L}_{f+\frac{p-1}{x}}\big)$.

5 Resolution of the "p-Riccati" equation

In [13, §13.2.1], Singer and van der Put explain how to solve the p-Riccati equation over $\mathbb{F}_q(x)$. The idea is somehow to show that if Eq.(1) has a solution, then it has another solution with at most the same poles as y_N. We then deduce a bound on the degree of the numerator and conclude using $\mathbb{F}_p$-linearity. The method for the general case follows the same pattern. However, in full generality, all solutions may have more poles than y_N. In order to get around this issue, we use tools from algebraic geometry: Riemann-Roch spaces, Picard group of a curve and Jacobians. For $f \in K_N$, let $\nu_{\mathfrak{P}}(f)$ denote the order of vanishing of f at the place $\mathfrak{P}$.

Proposition 5. *Let $\mathfrak{P}$ be a place of K_N and $t_{\mathfrak{P}} \in K_N$ such that $\nu_{\mathfrak{P}}(t_{\mathfrak{P}}) = 1$. Let f be a solution of Eq. (1). Then $\nu_{\mathfrak{P}}(f) \geq \min(0, p^{-1}\nu_{\mathfrak{P}}(y_N), \nu_{\mathfrak{P}}(t'_{\mathfrak{P}}) - 1)$. Besides, when $\mathfrak{P}$ is not a pole of y_N nor a ramified place, nor a place at infinity, the residue of f at $\mathfrak{P}$ (denoted by $\mathrm{Re}_{\mathfrak{P}}(f)$) is an integer.*

It follows from the previous proposition that, when $\mathfrak{P}$ is not a pole of y_N, nor a ramified place, nor a place at infinity, we always have $\nu_{\mathfrak{P}}(f) \geq -1$. Moreover, when equality holds, one can remove the simple pole at $\mathfrak{P}$ by replacing f by $f - g'/g$ where $g \in K_N$ has a zero of order $\mathrm{Re}_{\mathfrak{P}}(f)$ at $\mathfrak{P}$. Unfortunately, this transformation may lead to other undesirable poles. In order to control this back-and-forth, we use computations in the group of divisors of K_N (which is, by definition, the free commutative group generated by the set of places of K_N).

Proposition 6. *Let S be a set of places containing the poles of y_N, the ramified places of K_N and the places at infinity. Let $\mathfrak{S}$ be a fixed place of K_N of degree 1. Set $D = c \cdot \mathfrak{S} + \sum_{\mathfrak{P} \notin S} \mathrm{Re}_{\mathfrak{P}}(f) \cdot \mathfrak{P}$ where $c \in \mathbb{Z}$ is such that $\deg(D) = 0$. If there exist two divisors D_p and D' such that $D - D' - pD_p$ is a principal divisor, then Eq. (1) has a solution with no pole outside $S \cup D' \cup \{\mathfrak{S}\}$.*

The group of divisors of K_N of degree 0 modulo the subgroup of principal divisors is the so-called *Picard group* of K_N and is denoted by $\mathrm{Pic}^0(K_N)$. Proposition 6 above ensures that we will get an explicit bound on the poles of a solution of Eq. (1) if we can bound the cokernel of the multiplication by p on $\mathrm{Pic}^0(K_N)$. This finally can be achieved using general results on the Jacobian of K_N.

References

[1] F. W. Anderson and K. R. Fuller. *Rings and categories of modules*, volume 13 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1992.

[2] A. Bostan, X. Caruso, and E. Schost. A fast algorithm for computing the characteristic polynomial of the p-curvature. In *ISSAC 2014—Proc. of the 39th International Symposium on Symbolic and Algebraic Computation*, pages 59–66. ACM, 2014.

[3] F. Chyzak, A. Goyer, and M. Mezzarobba. Symbolic-Numeric Factorization of Differential Operators. To appear in *ISSAC 2022*.

[4] T. Cluzeau. Factorization of differential systems in characteristic p. In *Proc. of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 58–65. ACM, 2003.

[5] T. Cluzeau. *Algorithmique modulaire des équations différentielles linéaires*. PhD thesis, Université de Limoges, 2004.

[6] E. Eid. Fast computation of hyperelliptic curve isogenies in odd characteristic. In *ISSAC 2021—Proc. of the 39th International Symposium on Symbolic and Algebraic Computation*. ACM, 2021.

[7] D. Y. Grigoriev. Complexity of factoring and calculating the GCD of linear ordinary differential operators. *J. Symbolic Comput.*, 10(1):7–37, 1990.

[8] P. Lairez and T. Vaccon. On p-adic differential equations with separation of variables. In *ISSAC 2016—Proc. of the 39th International Symposium on Symbolic and Algebraic Computation*, pages 319–323. ACM, 2016.

[9] A. G. B. Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc. (3)*, 88(3):565–602, 2004.

[10] P. Revoy. Algèbres de Weyl en caractéristique p. *C. R. Acad. Sci. Paris Sér. A-B*, 276:A225–A228, 1973.

[11] M. van der Put. Differential equations in characteristic p. volume 97, pages 227–251. 1995. Special issue in honour of Frans Oort.

[12] M. van der Put. Reduction modulo p of differential equations. *Indag. Math. (N.S.)*, 7(3):367–387, 1996.

[13] M. van der Put and M. F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

[14] M. van Hoeij. Factorization of differential operators with rational functions coefficients. *J. Symbolic Comput.*, 24(5):537–561, 1997.