Factoring linear differential operators in positive characteristic

ACA 2022

Raphaël Pagès[1]

[1]INRIA - France
(Bordeaux, Paris-Saclay)

August 11, 2022

Algebra of differential operators

Object of study

Differential operators in $\mathbb{F}_p(x)\langle\partial\rangle = \{a_n(x)\partial^n + \cdots + a_1(x)\partial + a_0(x)\}$.

Algebra of differential operators

Object of study

Differential operators in $\mathbb{F}_p(x)\langle\partial\rangle = \{a_n(x)\partial^n + \cdots + a_1(x)\partial + a_0(x)\}$.

Commutation rule:

$$\partial f = f\partial + f'$$

Derivation:

$$f' = \frac{\mathrm{d}}{\mathrm{d}x}f$$

Algebra of differential operators

Object of study

Differential operators in $\mathbb{F}_p(x)\langle\partial\rangle = \{a_n(x)\partial^n + \cdots + a_1(x)\partial + a_0(x)\}$.

Commutation rule:

$$\partial f = f\partial + f'$$

Derivation:

$$f' = \frac{\mathrm{d}}{\mathrm{d}x} f$$

Goal: Factor differential operators as a product of irreducible differential operators.

Algebra of differential operators

Object of study

Differential operators in $\mathbb{F}_p(x)\langle\partial\rangle = \{a_n(x)\partial^n + \cdots + a_1(x)\partial + a_0(x)\}$.

Commutation rule:

$$\partial f = f\partial + f'$$

Derivation:

$$f' = \frac{\mathrm{d}}{\mathrm{d}x} f$$

Goal: Factor differential operators as a product of irreducible differential operators.

Running example:

$L = (2x^6 + 2)\partial^6 + (x^6 + 2)\partial^3 + 2x^6 + 2x^3 + 2 \in \mathbb{F}_3(x)\langle\partial\rangle$

State of the art

- M. van der Put. Modular methods for factoring differential operators. Unpublished manuscript, 1997.
- M. Giesbrecht, Y. Zhang, Factoring and decomposing Ore polynomials over $\mathbb{F}_p(t)$, ISSAC 2003.
- T. Cluzeau, factorisation of differential systems in characteristic p, ISSAC 2003.
- X. Caruso, J. Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. JSC 2017.
- J. Gomez-Torrecillas, F. J. Lobillo, G. Navarro, Computing the bound of an Ore polynomial. Applications to factorisation, JSC 2019.

State of the art

Problem: For reducible divisors of $Q(x^p, \partial^p)$ with $Q \in \mathbb{F}_p[u, v]$.

State of the art

Problem: For reducible divisors of $Q(x^p, \partial^p)$ with $Q \in \mathbb{F}_p[u, v]$.

Lacks a way to factor central operators e.g ∂^p

State of the art

Problem: For reducible divisors of $Q(x^p, \partial^p)$ with $Q \in \mathbb{F}_p[u, v]$.

Lacks a way to factor central operators e.g ∂^p

Notation

$C := \mathbb{F}_p(x^p)$ is the field of constants of $\mathbb{F}_p(x)$.
$C[\partial^p]$ is the center of $\mathbb{F}_p(x)\langle\partial\rangle$.

Main tools

Tool 1: p-curvature and first reduction (van der Put, Cluzeau)

Main tools

Tool 1: p-curvature and first reduction (van der Put, Cluzeau)

Tool 2: Understanding the structure of the differential equations. Morita's equivalence.

Main tools

Tool 1: p-curvature and first reduction (van der Put, Cluzeau)

Tool 2: Understanding the structure of the differential equations. Morita's equivalence.

Tool 3: p-Riccati equation.

Main tools

Tool 1: p-curvature and first reduction (van der Put, Cluzeau)

Tool 2: Understanding the structure of the differential equations. Morita's equivalence.

Tool 3: p-Riccati equation.

Tool 4: Divisor arithmetic on algebraic curves.

Main tools

Tool 1: p-curvature and first reduction (van der Put, Cluzeau)

Tool 2: Understanding the structure of the differential equations. Morita's equivalence.

Tool 3: p-Riccati equation.

Tool 4: Divisor arithmetic on algebraic curves.

Contribution

A full factorisation algorithm that extends to operators with coefficients in finite separable extensions of $\mathbb{F}_p(x)$.

A guideline: studying the submodules of $\mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$

Notation

- $\mathcal{D}_L := \mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$.
- $\mathcal{D}_L L'$ is the $\mathbb{F}_p(x)\langle\partial\rangle$-submodule of $\mathcal{D}_L$ generated by L'.

A guideline: studying the submodules of $\mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$

Notation

- $\mathcal{D}_L := \mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$.
- $\mathcal{D}_L L'$ is the $\mathbb{F}_p(x)\langle\partial\rangle$-submodule of $\mathcal{D}_L$ generated by L'.

Let $L \in \mathbb{F}_p(x)\langle\partial\rangle$

A guideline: studying the submodules of $\mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$

Notation

- $\mathcal{D}_L := \mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$.
- $\mathcal{D}_L L'$ is the $\mathbb{F}_p(x)\langle\partial\rangle$-submodule of $\mathcal{D}_L$ generated by L'.

Let $L \in \mathbb{F}_p(x)\langle\partial\rangle$

Lemma

$$L' \mapsto \mathcal{D}_L L'$$

is a one-to-one ***decreasing*** *bijection between*

A guideline: studying the submodules of $\mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$

Notation

- $\mathcal{D}_L := \mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$.
- $\mathcal{D}_L L'$ is the $\mathbb{F}_p(x)\langle\partial\rangle$-submodule of $\mathcal{D}_L$ generated by L'.

Let $L \in \mathbb{F}_p(x)\langle\partial\rangle$

Lemma

$$L' \mapsto \mathcal{D}_L L'$$

is a one-to-one ***decreasing*** *bijection between*

- *The set of right divisors of L (up to a multiplicative element in $\mathbb{F}_p(x)^\times$)*

A guideline: studying the submodules of $\mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$

Notation

- $\mathcal{D}_L := \mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$.
- $\mathcal{D}_L L'$ is the $\mathbb{F}_p(x)\langle\partial\rangle$-submodule of $\mathcal{D}_L$ generated by L'.

Let $L \in \mathbb{F}_p(x)\langle\partial\rangle$

Lemma

$$L' \mapsto \mathcal{D}_L L'$$

is a one-to-one ***decreasing*** *bijection between*

- *The set of right divisors of L (up to a multiplicative element in $\mathbb{F}_p(x)^\times$)*
- *The set of $\mathbb{F}_p(x)\langle\partial\rangle$-submodules of $\mathcal{D}_L$.*

A guideline: studying the submodules of $\mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$

Notation

- $\mathcal{D}_L := \mathbb{F}_p(x)\langle\partial\rangle / \mathbb{F}_p(x)\langle\partial\rangle L$.
- $\mathcal{D}_L L'$ is the $\mathbb{F}_p(x)\langle\partial\rangle$-submodule of $\mathcal{D}_L$ generated by L'.

Let $L \in \mathbb{F}_p(x)\langle\partial\rangle$

Lemma

$$L' \mapsto \mathcal{D}_L L'$$

*is a one-to-one **decreasing** bijection between*

- *The set of right divisors of L (up to a multiplicative element in $\mathbb{F}_p(x)^\times$)*
- *The set of $\mathbb{F}_p(x)\langle\partial\rangle$-submodules of $\mathcal{D}_L$.*

Direct consequence of $\mathbb{F}_p(x)\langle\partial\rangle$ being a left principal ideal domain.

p-curvature

Definition

The p-curvature of L is

$$\begin{array}{rcl} \psi_p^L \quad : \mathcal{D}_L & \rightarrow & \mathcal{D}_L \\ Q & \mapsto & \partial^p Q \end{array}$$

p-curvature

Definition

The p-curvature of L is

$$\begin{array}{rcl} \psi_p^L \quad : \mathcal{D}_L & \rightarrow & \mathcal{D}_L \\ Q & \mapsto & \partial^p Q \end{array}$$

Proposition

Its characteristic polynomial $\chi(\psi_p^L)$ belongs to $\boldsymbol{C}[\boldsymbol{Y}]$.

A first factorisation

Proposition

If $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$ ($N_i \in C[Y]$ irreducible, pairwise distinct), then:

A first factorisation

Proposition

If $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$ ($N_i \in C[Y]$ irreducible, pairwise distinct), then:

- $L = L_1 \cdots L_n$
  with $\chi(\psi_p^{L_i}) = N_i^{\nu_i}(Y)$ and $L_n = \mathrm{gcrd}(L, N_n^{\nu_n}(\partial^p))$.

A first factorisation

Proposition

If $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$ ($N_i \in C[Y]$ irreducible, pairwise distinct), then:

- $L = L_1 \cdots L_n$
  with $\chi(\psi_p^{L_i}) = N_i^{\nu_i}(Y)$ and $L_n = \mathrm{gcrd}(L, N_n^{\nu_n}(\partial^p))$.
- $L = L'_1 \cdots L'_m$ with each L'_j dividing some $N_i(\partial^p)$.

A first factorisation

Proposition

If $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$ ($N_i \in C[Y]$ irreducible, pairwise distinct), then:

- $L = L_1 \cdots L_n$
  with $\chi(\psi_p^{L_i}) = N_i^{\nu_i}(Y)$ and $L_n = \mathrm{gcrd}(L, N_n^{\nu_n}(\partial^p))$.
- $L = L'_1 \cdots L'_m$ with each L'_j dividing some $N_i(\partial^p)$.

Operator version of classical classification results of differential modules in positive characteristic (van der Put).

Running example factorisation

$\chi(\psi_p^L) = N(Y)^3$

Running example factorisation

$$\chi(\psi_p^L) = N(Y)^3$$

$$N(Y) = (2x^6 + 2)Y^2 + (x^6 + 2)Y + 2x^6 + 2x^3 + 2$$

Running example factorisation

$$\chi(\psi_p^L) = N(Y)^{\,3}$$

$$N(Y) = (2x^6 + 2)\,Y^2 + (x^6 + 2)\,Y + 2x^6 + 2x^3 + 2$$

$$L = (2x^6 + 2)\partial^6 + (x^6 + 2)\partial^3 + 2x^6 + 2x^3 + 2$$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^{n} N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.

Refined setting

Setting

L is a divisor of $N(\partial^p)$

Refined setting

Setting

L is a divisor of $N(\partial^p)$

$N(Y)$ is irreducible over C.

Refined setting

Setting

L is a divisor of $N(\partial^p)$

$N(Y)$ is irreducible over C.

Notation

$C_N := {}^{C[Y]}/_{N(Y)}$

Refined setting

Setting

L is a divisor of $N(\partial^p)$

$N(Y)$ is irreducible over C.

Notation

$C_N := {}^{C[Y]}/_{N(Y)}$

Facts

Refined setting

Setting

L is a divisor of $N(\partial^p)$

$N(Y)$ is irreducible over C.

Notation

$C_N := {}^{C[Y]}/_{N(Y)}$

Facts

- $\mathcal{D}_{N(\partial^p)}$ is a C_N-algebra ($Y \mapsto \partial^p$)

Refined setting

Setting

L is a divisor of $N(\partial^p)$

$N(Y)$ is irreducible over C.

Notation

$C_N := {}^{C[Y]}/_{N(Y)}$

Facts

- $\mathcal{D}_{N(\partial^p)}$ is a C_N-algebra ($Y \mapsto \partial^p$)
- $\mathcal{D}_L$ is a left $\mathcal{D}_{N(\partial^p)}$-module

Structure results

Proposition (van der Put)

$\mathcal{D}_{N(\partial^p)}$ is a central simple C_N-algebra of dimension p^2.

Structure results

Proposition (van der Put)

$\mathcal{D}_{N(\partial^p)}$ is a central simple C_N-algebra of dimension p^2.

Theorem (Artin-Wedderburn)

Any central simple C_N- algebra is isomorphic to a matrix algebra over a division algebra.

Structure results

Proposition (van der Put)

$\mathcal{D}_{N(\partial^p)}$ is a central simple C_N-algebra of dimension p^2.

Theorem (Artin-Wedderburn)

Any central simple C_N- algebra is isomorphic to a matrix algebra over a division algebra.

Corollary

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

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.

Morita's equivalence

The categories of C_N-vector spaces and left-$M_p(C_N)$-modules are equivalent.

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.

Morita's equivalence

The categories of C_N-vector spaces and left-$M_p(C_N)$-modules are equivalent.

$$\mathcal{M}\mathrm{or}_N : \mathrm{Mod}^l_{M_p(C_N)} \to \mathrm{Mod}_{C_N}$$

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.

Morita's equivalence

The categories of C_N-vector spaces and left-$M_p(C_N)$-modules are equivalent.

$$\mathcal{M}\mathrm{or}_N : \mathrm{Mod}^l_{M_p(C_N)} \to \mathrm{Mod}_{C_N}$$

Facts

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.

Morita's equivalence

The categories of C_N-vector spaces and left-$M_p(C_N)$-modules are equivalent.

$$\mathcal{M}\mathrm{or}_N : \mathrm{Mod}^l_{M_p(C_N)} \to \mathrm{Mod}_{C_N}$$

Facts

- $\mathcal{M}\mathrm{or}_N(\mathcal{D}_{N(\partial^p)}) = C_N^p$.

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.

Morita's equivalence

The categories of C_N-vector spaces and left-$M_p(C_N)$-modules are equivalent.

$$\mathcal{M}\mathrm{or}_N : \mathrm{Mod}^l_{M_p(C_N)} \to \mathrm{Mod}_{C_N}$$

Facts

- $\mathcal{M}\mathrm{or}_N(\mathcal{D}_{N(\partial^p)}) = C_N^p$.
- L' is an irreducible divisor of L if and only if $\mathcal{M}\mathrm{or}_N(\mathcal{D}_L \cdot L')$ is a hyperplane of $\mathcal{M}\mathrm{or}_N(\mathcal{D}_L)$.

Morita's equivalence

If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor and $L = N(\partial^p)$ is irreducible.

Suppose that $\mathcal{D}_{N(\partial^p)}$ is isomorphic to $M_p(C_N)$.

Morita's equivalence

The categories of C_N-vector spaces and left-$M_p(C_N)$-modules are equivalent.

$$\mathcal{M}\mathrm{or}_N : \mathrm{Mod}^l_{M_p(C_N)} \to \mathrm{Mod}_{C_N}$$

Facts

- $\mathcal{M}\mathrm{or}_N(\mathcal{D}_{N(\partial^p)}) = C_N^p$.
- L' is an irreducible divisor of L if and only if $\mathcal{M}\mathrm{or}_N(\mathcal{D}_L \cdot L')$ is a hyperplane of $\mathcal{M}\mathrm{or}_N(\mathcal{D}_L)$.
- If L' is a divisor of $N(\partial^p)$ then $\dim \mathcal{M}\mathrm{or}_N(\mathcal{D}_{L'}) = \mathrm{ord}(L')/\deg(N)$.

Running example

$$L = N(\partial^p) = (2x^6 + 2)\partial^6 + (x^6 + 2)\partial^3 + 2x^6 + 2x^3 + 2$$

Factoring L by factoring $N(\partial^p)$

Let $LR = N(\partial^p)$.

Factoring L by factoring $N(\partial^p)$

Let $LR = N(\partial^p)$.

$$\begin{array}{ccc} \mathcal{D}_L & \xrightarrow{\sim} & \mathcal{D}_{N(\partial^p)} R \\ Q & \mapsto & Q \cdot R \end{array}$$

Factoring L by factoring $N(\partial^p)$

Let $LR = N(\partial^p)$.

$$\begin{array}{ccc} \mathcal{D}_L & \xrightarrow{\sim} & \mathcal{D}_{N(\partial^p)} R \\ Q & \mapsto & Q \cdot R \end{array}$$

$\mathcal{M}\mathrm{or}(\mathcal{D}_L)$ identifies as a sub-vector space V of C_N^p.

Factoring L by factoring $N(\partial^p)$

Let $LR = N(\partial^p)$.

$$\begin{array}{ccc} \mathcal{D}_L & \xrightarrow{\sim} & \mathcal{D}_{N(\partial^p)}R \\ Q & \mapsto & Q \cdot R \end{array}$$

$\mathcal{M}\mathrm{or}(\mathcal{D}_L)$ identifies as a sub-vector space V of C_N^p.
Let $H_1, \ldots, H_p$ be hyperplanes of C_N^p such that $\bigcap_{i=1}^p H_i = \{0\}$.

Factoring L by factoring $N(\partial^p)$

Let $LR = N(\partial^p)$.

$$\begin{array}{ccc} \mathcal{D}_L & \xrightarrow{\sim} & \mathcal{D}_{N(\partial^p)}R \\ Q & \mapsto & Q \cdot R \end{array}$$

$\mathcal{M}\mathrm{or}(\mathcal{D}_L)$ identifies as a sub-vector space V of C_N^p.
Let $H_1, \ldots, H_p$ be hyperplanes of C_N^p such that $\bigcap_{i=1}^p H_i = \{0\}$.
At least one H_i does not contain V and thus $V \cap H_i$ is a hyperplane of V.

Factoring L by factoring $N(\partial^p)$

Let $LR = N(\partial^p)$.

$$\begin{array}{ccc} \mathcal{D}_L & \xrightarrow{\sim} & \mathcal{D}_{N(\partial^p)}R \\ Q & \mapsto & Q \cdot R \end{array}$$

$\mathcal{M}\mathrm{or}(\mathcal{D}_L)$ identifies as a sub-vector space V of C_N^p.
Let $H_1, \ldots, H_p$ be hyperplanes of C_N^p such that $\bigcap_{i=1}^p H_i = \{0\}$.
At least one H_i does not contain V and thus $V \cap H_i$ is a hyperplane of V.

Theorem (P., 2022)

Let $(H_i)_{1 \leqslant i \leqslant p}$ be irreducible divisors of $N(\partial^p)$ such that $N(\partial^p) = \mathrm{lclm}_{i=1}^p H_i$.

Factoring L by factoring $N(\partial^p)$

Let $LR = N(\partial^p)$.

$$\begin{array}{ccc} \mathcal{D}_L & \xrightarrow{\sim} & \mathcal{D}_{N(\partial^p)} R \\ Q & \mapsto & Q \cdot R \end{array}$$

$\mathcal{M}\mathrm{or}(\mathcal{D}_L)$ identifies as a sub-vector space V of C_N^p.
Let $H_1, \ldots, H_p$ be hyperplanes of C_N^p such that $\bigcap_{i=1}^p H_i = \{0\}$.
At least one H_i does not contain V and thus $V \cap H_i$ is a hyperplane of V.

Theorem (P., 2022)

Let $(H_i)_{1 \leqslant i \leqslant p}$ be irreducible divisors of $N(\partial^p)$ such that $N(\partial^p) = \mathrm{lclm}_{i=1}^p H_i$. For at least one i,

$$\mathrm{lclm}(H_i, R) \cdot R^{-1}$$

is an irreducible divisor of L.

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^{n} N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^{n} N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k \in [\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^{p} H_{i,k} = N_i(\partial^p)$.

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^{n} N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k \in [\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^{p} H_{i,k} = N_i(\partial^p)$.

- Compute $\mathrm{lclm}(R'_j, H_{i,k}) \cdot (R'_j)^{-1}$

Extending the field of constants

Hypothesis: N is separable over C.

Extending the field of constants

Hypothesis: N is separable over C.

Notation

y_N is the image of Y in $C_N = {}^{C[Y]}/_{N(Y)}$.

Extending the field of constants

Hypothesis: N is separable over C.

Notation

y_N is the image of Y in $C_N = {}^{C[Y]}/_{N(Y)}$.
$K_N = \mathbb{F}_p(x) \cdot C_N$

Extending the field of constants

Hypothesis: N is separable over C.

Notation

y_N is the image of Y in $C_N = {}^{C[Y]}/_{N(Y)}$.
$K_N = \mathbb{F}_p(x) \cdot C_N$

Recall: $\mathcal{D}_{N(\partial^p)} = {}^{\mathbb{F}_p(x)\langle\partial\rangle}/_{N(\partial^p)}$

$$\begin{array}{ccc} \mathbb{F}_p(x)\langle\partial\rangle & \hookrightarrow & K_N\langle\partial\rangle \\ \downarrow & & \downarrow\!\!\downarrow \\ {}^{\mathbb{F}_p(x)\langle\partial\rangle}/_{N(\partial^p)} & \overset{\varphi_N}{\dashrightarrow} & {}^{K_N\langle\partial\rangle}/_{\partial^p - y_N} \end{array}$$

"p-Riccati" equation

Lemma (Jacobson, van der Put)

$L' \in K_N\langle\partial\rangle$ is an irreducible divisor of $\partial^p - y_N$ iff $L' = \partial - f$

"p-Riccati" equation

Lemma (Jacobson, van der Put)

$L' \in K_N\langle\partial\rangle$ is an irreducible divisor of $\partial^p - y_N$ iff $L' = \partial - f$ with

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

"p-Riccati" equation

Lemma (Jacobson, van der Put)

$L' \in K_N\langle\partial\rangle$ is an irreducible divisor of $\partial^p - y_N$ iff $L' = \partial - f$ with

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

Lemma (P., 2022)

Let $f \in K_N$ be such that $f^{(p-1)} + f^p = y_N$. Then

$$\partial^p - y_N = \mathrm{lclm}_{i=1}^{p}\left(\partial - f - \frac{i}{x}\right)$$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^{n} N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k \in [\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^{p} H_{i,k} = N_i(\partial^p)$.

- Compute $\mathrm{lclm}(R'_j, H_{i,k}) \cdot (R'_j)^{-1}$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k \in [\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
  - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.

- Compute $\mathrm{lclm}(R'_j, H_{i,k}) \cdot (R'_j)^{-1}$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k\in[\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
  - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
  - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f_i - \frac{k}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(R'_j, H_{i,k}) \cdot (R'_j)^{-1}$

The case when $L \neq N(\partial^p)$ (after van der Put)

$$L_N := \mathrm{gcrd}(\varphi_N(L), \partial^p - y_N)$$

is a non trivial divisor of $\partial^p - y_N$.

The case when $L \neq N(\partial^p)$ (after van der Put)

$$L_N := \mathrm{gcrd}(\varphi_N(L), \partial^p - y_N)$$

is a non trivial divisor of $\partial^p - y_N$.

Fact

If $L_N = \partial^m + a_{m-1}\partial^{m-1} + \cdots + a_0$ then $-\frac{a_{m-1}}{m}$ is a solution of the p-Riccati equation.

The case when $L \neq N(\partial^p)$ (after van der Put)

$$L_N := \mathrm{gcrd}(\varphi_N(L), \partial^p - y_N)$$

is a non trivial divisor of $\partial^p - y_N$.

Fact

If $L_N = \partial^m + a_{m-1}\partial^{m-1} + \cdots + a_0$ then $-\frac{a_{m-1}}{m}$ is a solution of the p-Riccati equation.

proof:

$L_N = (\partial - f_1) \cdots (\partial - f_m)$.

The case when $L \neq N(\partial^p)$ (after van der Put)

$$L_N := \mathrm{gcrd}(\varphi_N(L), \partial^p - y_N)$$

is a non trivial divisor of $\partial^p - y_N$.

Fact

If $L_N = \partial^m + a_{m-1}\partial^{m-1} + \cdots + a_0$ then $-\frac{a_{m-1}}{m}$ is a solution of the p-Riccati equation.

proof:

$L_N = (\partial - f_1) \cdots (\partial - f_m)$.

$-\frac{a_{m-1}}{m} = \frac{1}{m}(f_1 + \cdots + f_m)$

The case when $L \neq N(\partial^p)$ (after van der Put)

$$L_N := \mathrm{gcrd}(\varphi_N(L), \partial^p - y_N)$$

is a non trivial divisor of $\partial^p - y_N$.

Fact

If $L_N = \partial^m + a_{m-1}\partial^{m-1} + \cdots + a_0$ then $-\frac{a_{m-1}}{m}$ is a solution of the p-Riccati equation.

proof:

$L_N = (\partial - f_1)\cdots(\partial - f_m)$.

$-\frac{a_{m-1}}{m} = \frac{1}{m}(f_1 + \cdots + f_m)$

The space of solutions of p-Riccati is an affine space

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k \in [\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
    - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
    - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f - \frac{i}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(L'_{j*}, H_{i,k}) \cdot (L'_{j*})^{-1}$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k\in[\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
    - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
        - Compute $\mathrm{gcrd}(\varphi_{N_i}(L'_j), \partial^p - y_{N_i}) = \partial^{m_j} + a_{m_j-1,j}\partial^{m_j-1} + \cdots + a_{0,j}$.
    - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f - \frac{i}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(L'_{j*}, H_{i,k}) \cdot (L'_{j*})^{-1}$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k\in[\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
  - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
    - Compute $\mathrm{gcrd}(\varphi_{N_i}(L'_j), \partial^p - y_{N_i}) = \partial^{m_j} + a_{m_j-1,j}\partial^{m_j-1} + \cdots + a_{0,j}$.
    - Set $f_i = -\frac{a_{m_j-1,j}}{m_j}$
  - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f - \frac{i}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(L'_{j*}, H_{i,k}) \cdot (L'_{j*})^{-1}$

Factoring $N(\partial^p)$: when $K_N = \mathbb{F}_p(x)$

Suppose that $K_N = \mathbb{F}_p(x)$, $y_N = g^p \in \mathbb{F}_p(x^p)$
and that $f^{(p-1)} + f^p = g^p$ has a solution in $\mathbb{F}_p(x)$.

Factoring $N(\partial^p)$: when $K_N = \mathbb{F}_p(x)$

Suppose that $K_N = \mathbb{F}_p(x)$, $y_N = g^p \in \mathbb{F}_p(x^p)$
and that $f^{(p-1)} + f^p = g^p$ has a solution in $\mathbb{F}_p(x)$.

Step 1: Show that there is a solution whose denominator divides that of g.

Factoring $N(\partial^p)$: when $K_N = \mathbb{F}_p(x)$

Suppose that $K_N = \mathbb{F}_p(x)$, $y_N = g^p \in \mathbb{F}_p(x^p)$
and that $f^{(p-1)} + f^p = g^p$ has a solution in $\mathbb{F}_p(x)$.

Step 1: Show that there is a solution whose denominator divides that of g.

Step 2: Deduce that the degree of the numerator of this solution is at most $\deg(g)$.

Factoring $N(\partial^p)$: when $K_N = \mathbb{F}_p(x)$

Suppose that $K_N = \mathbb{F}_p(x)$, $y_N = g^p \in \mathbb{F}_p(x^p)$
and that $f^{(p-1)} + f^p = g^p$ has a solution in $\mathbb{F}_p(x)$.

Step 1: Show that there is a solution whose denominator divides that of g.

Step 2: Deduce that the degree of the numerator of this solution is at most $\deg(g)$.

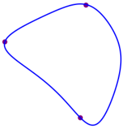
Step 3: Solve an $\mathbb{F}_p$-linear system.

Factoring $N(\partial^p)$: general case

$$N_1(\partial^3) = (2x^6 + 2)\partial^6 + (x^6 + 2)\partial^3 + 2x^6 + 2x^3 + 2.$$

Factoring $N(\partial^p)$: general case

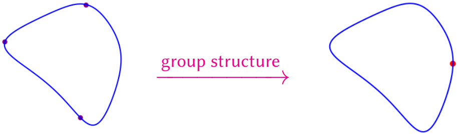
$$N_1(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$$



$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

Factoring $N(\partial^p)$: general case

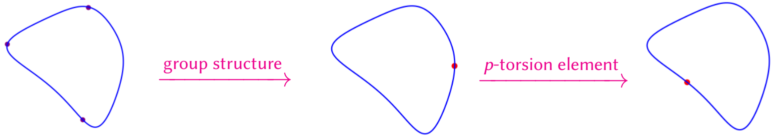
$$N_1(\partial^3) = (2x^6 + 2)\partial^6 + (x^6 + 2)\partial^3 + 2x^6 + 2x^3 + 2.$$



$$(2X^2 + 2)Y^2 + (X^2 + 2)Y + 2X^2 + 2X + 2 = 0$$

Factoring $N(\partial^p)$: general case

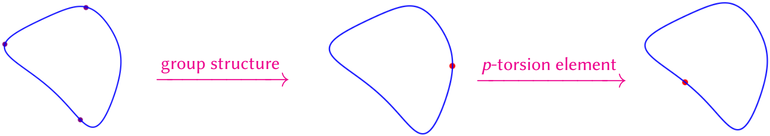
$$N_1(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$$



$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

Factoring $N(\partial^p)$: general case

$$N_1(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$$



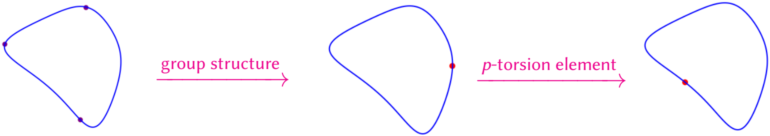
$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

Theorem (P., 2022)

If the p-Riccati has a solution in K_N then one of its solution has its poles located in

Factoring $N(\partial^p)$: general case

$$N_1(\partial^3) = (2x^6 + 2)\partial^6 + (x^6 + 2)\partial^3 + 2x^6 + 2x^3 + 2.$$



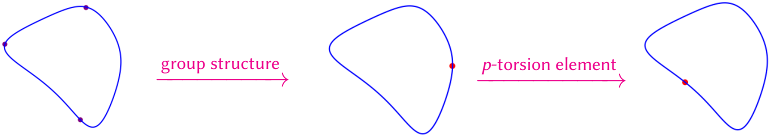
$$(2X^2 + 2)Y^2 + (X^2 + 2)Y + 2X^2 + 2X + 2 = 0$$

Theorem (P., 2022)

If the p-Riccati has a solution in K_N then one of its solution has its poles located in the poles of y_N,

Factoring $N(\partial^p)$: general case

$$N_1(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$$



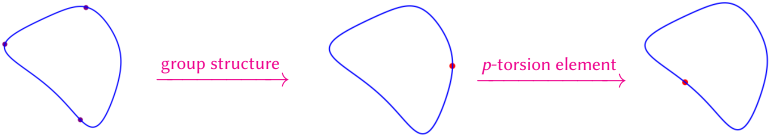
$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

Theorem (P., 2022)

If the p-Riccati has a solution in K_N then one of its solution has its poles located in the poles of y_N, in ramified places and places at infinity of K_N,

Factoring $N(\partial^p)$: general case

$$N_1(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$$



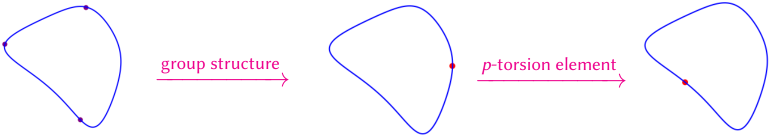
$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

Theorem (P., 2022)

If the p-Riccati has a solution in K_N then one of its solution has its poles located in the poles of y_N, in ramified places and places at infinity of K_N, a chosen place of degree 1

Factoring $N(\partial^p)$: general case

$$N_1(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$$



$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

Theorem (P., 2022)

If the p-Riccati has a solution in K_N then one of its solution has its poles located in the poles of y_N, in ramified places and places at infinity of K_N, a chosen place of degree 1 and in a set of places generating the cokernel of the multiplication by p on the Jacobian.

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k\in[\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
  - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
  - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f - \frac{i}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(L'_{j*}, H_{i,k}) \cdot (L'_{j*})^{-1}$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k \in [\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
    - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
        - Construct a divisor A such that we know that a solution lives in $\mathcal{L}(A)$.
    - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f - \frac{i}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(L'_{j*}, H_{i,k}) \cdot (L'_{j*})^{-1}$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^{n} N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k\in[\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^{p} H_{i,k} = N_i(\partial^p)$.
  - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
    - Construct a divisor A such that we know that a solution lives in $\mathcal{L}(A)$.
    - Computes the Riemann-Roch space $\mathcal{L}(A)$.
  - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f - \frac{i}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(L'_{j*}, H_{i,k}) \cdot (L'_{j*})^{-1}$

Algorithm

- Compute $\chi(\psi_p^L)$ and factor it $\chi(\psi_p^L) = \prod_{i=1}^n N_i^{\nu_i}(Y)$.
- Compute $L = L'_1 \cdots L'_m$ such that each L'_j divides a $N_i(\partial^p)$.
- For each $N_i(\partial^p)$ compute $(H_{i,k})_{k\in[\![1;p]\!]}$ such that $\mathrm{lclm}_{k=1}^p H_{i,k} = N_i(\partial^p)$.
  - Compute $f_i \in K_N$ such that $f_i^{(p-1)} + f_i^p = y_{N_i}$.
    - Construct a divisor A such that we know that a solution lives in $\mathcal{L}(A)$.
    - Computes the Riemann-Roch space $\mathcal{L}(A)$.
    - Solve a $\mathbb{F}_p$-linear system over $\mathcal{L}(A)$
  - Set $H_{i,k} = \mathrm{gcrd}(\varphi_{N_i}^{-1}(\partial - f - \frac{i}{x}), N_i(\partial^p))$.
- Compute $\mathrm{lclm}(L'_{j*}, H_{i,k}) \cdot (L'_{j*})^{-1}$

Future works

- Implementation

Future works

- Implementation
- Good control on the size of the factors

Future works

- Implementation
- Good control on the size of the factors
- Complexity analysis

Future works

- Implementation
- Good control on the size of the factors
- Complexity analysis
- lclm factorisation.

Future works

- Implementation
- Good control on the size of the factors
- Complexity analysis
- lclm factorisation.
- Factorisation of differential systems

Future works

- Implementation
- Good control on the size of the factors
- Complexity analysis
- lclm factorisation.
- Factorisation of differential systems

Thank you for your attention