Factoring linear differential operators in positive characteristic

JNCF 2023

Raphaël Pagès[1]

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

June 6, 2023

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:

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

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 Unpublished manuscript, 1997.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

Classical (van der Put, Cluzeau)

Tool 1: p-curvature and first reduction

Main tools

Classical (van der Put, Cluzeau)

Tool 1: p-curvature and first reduction

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

Main tools

Classical (van der Put, Cluzeau)

Tool 1: p-curvature and first reduction

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

New! Tool 3: Algebraic geometry tools for solving p-Riccati equation.

- Divisor arithmetic on algebraic curves and Riemann-Roch spaces
- Group structure and p-torsion of the Jacobian.

Main tools

Classical (van der Put, Cluzeau)

Tool 1: p-curvature and first reduction

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

New! Tool 3: Algebraic geometry tools for solving p-Riccati equation.

- Divisor arithmetic on algebraic curves and Riemann-Roch spaces
- Group structure and p-torsion of the Jacobian.

Contribution

An algorithm able to fully factor central differential operators which will extend 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.

Setting

Setting

Trying to factor $N(\partial^p)$

Setting

Setting

Trying to factor $N(\partial^p)$

$N(Y)$ is irreducible over C.

Setting

Setting

Trying to factor $N(\partial^p)$

$N(Y)$ is irreducible over C.

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

Setting

Setting

Trying to factor $N(\partial^p)$

$N(Y)$ is irreducible over C.

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

Notation

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

Setting

Setting

Trying to factor $N(\partial^p)$

$N(Y)$ is irreducible over C.

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

Notation

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

Facts

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

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 is irreducible.

Morita's equivalence

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

Fact

If L is a divisor of $N(\partial^p)$ then L is irreducible if and only if $\text{ord}(L) = \deg(N)$.

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

$$\begin{tikzcd}
\mathbb{F}_p(x)\langle\partial\rangle \arrow[r, hook] \arrow[d] & K_N\langle\partial\rangle \arrow[d, two heads] \\
{}^{\mathbb{F}_p(x)\langle\partial\rangle}/_{N(\partial^p)} \arrow[r, dashed, "\varphi_N"] & {}^{K_N\langle\partial\rangle}/_{\partial^p - y_N}
\end{tikzcd}$$

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

Algorithm

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

- Compute $L = \operatorname{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$.

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

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 $\deg(g)$.

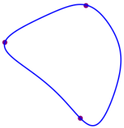
Step 3: Solve an $\mathbb{F}_p$-linear system.

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

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

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

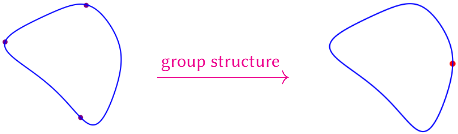
$N(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$



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

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

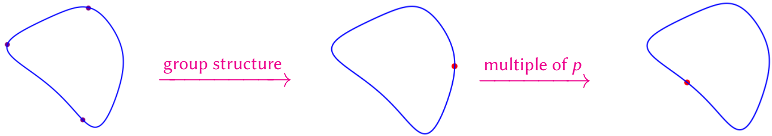
$$N(\partial^3) = (2x^6+2)\partial^6 + (x^6+2)\partial^3 + 2x^6 + 2x^3 + 2.$$



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

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

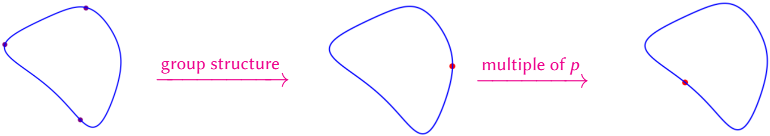
$$N(\partial^3) = (2x^6 + 2)\partial^6 + (x^6 + 2)\partial^3 + 2x^6 + 2x^3 + 2.$$



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

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

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



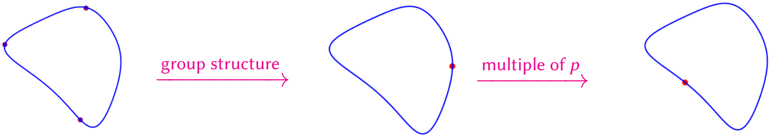
$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

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

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



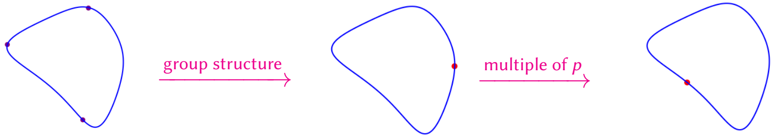
$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

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

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



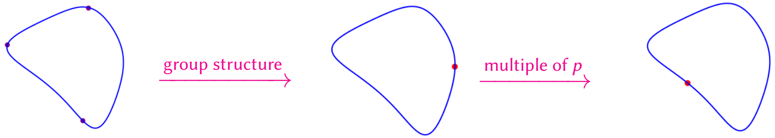
$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

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 of K_N,

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

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



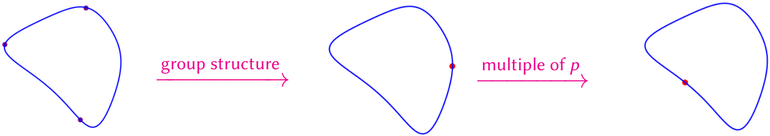
$$(2X^2+2)Y^2 + (X^2+2)Y + 2X^2 + 2X + 2 = 0$$

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 of K_N, a chosen place of degree 1

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

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



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

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

- Compute $L = \operatorname{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$.

Algorithm

- Compute $f \in K_N$ such that $f^{(p-1)} + f^p = y_N$.
  - Construct a divisor A_N such that we know that a solution lives in $\mathcal{L}(A_N)$.
- Compute $L = \mathrm{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$.

Algorithm

- Compute $f \in K_N$ such that $f^{(p-1)} + f^p = y_N$.
  - Construct a divisor A_N such that we know that a solution lives in $\mathcal{L}(A_N)$.
  - Computes the Riemann-Roch space $\mathcal{L}(A_N)$.
- Compute $L = \mathrm{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$.

Algorithm

- Compute $f \in K_N$ such that $f^{(p-1)} + f^p = y_N$.
  - Construct a divisor A_N such that we know that a solution lives in $\mathcal{L}(A_N)$.
  - Computes the Riemann-Roch space $\mathcal{L}(A_N)$.
  - Solve a $\mathbb{F}_p$-linear system over $\mathcal{L}(A_N)$
- Compute $L = \mathrm{gcrd}(\varphi_N^{-1}(\partial - f), N(\partial^p))$.

Running example

$$L_1 = \partial^2 + \left(\frac{2x^5 + x^4 + x^3 + 2x^2 + x + 1}{x^5 + x^4 + x^2 + 2x}\right)\partial + \frac{x^3 + x^2 + 2}{x^3 + x^2 + 2x}$$

Running example

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

Running example

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

$$= \partial^2 + \left(\frac{2x^5 + x^4 + x^3 + 2x^2 + x + 1}{x^5 + x^4 + x^2 + 2x}\right)\partial + \frac{x^3 + x^2 + 2}{x^3 + x^2 + 2x}$$

Running example

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

$$= \partial^2 + \left(\frac{2x^5+x^4+x^3+2x^2+x+1}{x^5+x^4+x^2+2x}\right)\partial + \frac{x^3+x^2+2}{x^3+x^2+2x}$$

$$\times \partial^2 + \left(\frac{2x^3+x^2+1}{x^3+x}\right)\partial + \frac{x^{10}+x^9+x^8+x^5+x^4+2x^2+2}{x^{10}+2x^9+x^8+2x^7+x^5+x^4+x^3+x^2}$$

Running example

$$
\begin{aligned}
&(2x^6+2)\partial^6+(x^6+2)\partial^3+2x^6+2x^3+2\\
=&\partial^2+\left(\frac{2x^5+x^4+x^3+2x^2+x+1}{x^5+x^4+x^2+2x}\right)\partial+\frac{x^3+x^2+2}{x^3+x^2+2x}\\
\times&\partial^2+\left(\frac{2x^3+x^2+1}{x^3+x}\right)\partial+\frac{x^{10}+x^9+x^8+x^5+x^4+2x^2+2}{x^{10}+2x^9+x^8+2x^7+x^5+x^4+x^3+x^2}\\
\times&\left(2x^6+2\right)\partial^2+\left(\frac{x^8+x^7+2x^6+x^5+2x^3+x^2+2x+2}{x^2+x+2}\right)\partial\\
&+\frac{2x^{12}+2x^{10}+2x^9+2x^7+2x^6+x^5+2x+2}{x^6+2x^5+2x^4+x^3+x^2}
\end{aligned}
$$

Size of the p-Riccati solution

We have shown that the solutions of the p-Riccati equation belong in the Riemann-Roch space $\mathcal{L}(A_N)$ with

Size of the p-Riccati solution

We have shown that the solutions of the p-Riccati equation belong in the Riemann-Roch space $\mathcal{L}(A_N)$ with

$$A_N := \max(p^{-1}(y_N)_-, \mathrm{Diff}(K_N)) + \mathcal{R}_N$$

Size of the p-Riccati solution

We have shown that the solutions of the p-Riccati equation belong in the Riemann-Roch space $\mathcal{L}(A_N)$ with

$$A_N := \max(p^{-1}(y_N)_-, \mathrm{Diff}(K_N)) + \mathcal{R}_N$$

where $\mathcal{R}_N$ is a divisor accounting for wildly ramified places, the cokernel of the multiplication by p on the Jacobian and a place of degree 1.

Size of the p-Riccati solution

We have shown that the solutions of the p-Riccati equation belong in the Riemann-Roch space $\mathcal{L}(A_N)$ with

$$A_N := \max(p^{-1}(y_N)_-, \mathrm{Diff}(K_N)) + \mathcal{R}_N$$

where $\mathcal{R}_N$ is a divisor accounting for wildly ramified places, the cokernel of the multiplication by p on the Jacobian and a place of degree 1.
(Usual case is $\mathcal{R}_N = 0$.)

Size of the p-Riccati solution

We have shown that the solutions of the p-Riccati equation belong in the Riemann-Roch space $\mathcal{L}(A_N)$ with

$$A_N := \max(p^{-1}(y_N)_-, \mathrm{Diff}(K_N)) + \mathcal{R}_N$$

where $\mathcal{R}_N$ is a divisor accounting for wildly ramified places, the cokernel of the multiplication by p on the Jacobian and a place of degree 1.
(Usual case is $\mathcal{R}_N = 0$.)

Lemma

Let $E_y = \left(\frac{\mathrm{d}}{\mathrm{d}y}N\right)(y_N)^{1/p}$ and N_k be the quotient of the euclidian division of N by y^k. Then for any $f = \sum_{i=0}^{d-1} f_i y_N^{i/p} \in K_N$ we have

$$f_k = \mathrm{Tr}\left(\frac{N_{k+1}(y_N)^{1/p}}{E_y} \cdot f\right)$$

Size of the p-Riccati solution

Let $\deg_x(N) = r$ and $\deg_y(N) = d$.

Heuristic

With the same notations as the previous slides, supposing $\mathcal{R}_N = 0$ (usual case in experiments), we observe

$$\mathcal{L}(A_N) \subset \frac{\mathbb{F}_p[x, y_N^{1/p}]_{\leqslant r, <d}}{E_y}$$

Complexities

Complexities

Complexities

Complexities

- Dimension of $\mathcal{L}(A_N)$:
  $O(rd) \rightarrow$**size of the basis** $O((rd)^2)$.

Complexities

Complexities

- Dimension of $\mathcal{L}(A_N)$:
  $O(rd)$ $\rightarrow$**size of the basis** $O((rd)^2)$.
- Computing $(p-1)$-th derivatives
  expected possible complexity $\tilde{O}((dr)^{\omega}\sqrt{dp})$.

Complexities

Complexities

- Dimension of $\mathcal{L}(A_N)$:
  $O(rd)$ $\rightarrow$**size of the basis** $O((rd)^2)$.
- Computing $(p-1)$-th derivatives
  expected possible complexity $\tilde{O}((dr)^\omega \sqrt{dp})$.
- Computing φ_N^{-1} $\Leftrightarrow$ changing basis from $(1, y_N^{1/p}, \cdots, y_N^{(d-1)/p})$ to $(1, y_N, \cdots, y_N^{d-1})$.
  inverting $d \times d$ **polynomial matrix with coefficients of degree** $O(pr)$.

Complexities

Complexities

- Dimension of $\mathcal{L}(A_N)$:
  $O(rd) \rightarrow$**size of the basis** $O((rd)^2)$.
- Computing $(p-1)$-th derivatives
  expected possible complexity $\tilde{O}((dr)^{\omega}\sqrt{dp})$.
- Computing $\varphi_N^{-1} \Leftrightarrow$ changing basis from $(1, y_N^{1/p}, \cdots, y_N^{(d-1)/p})$ to $(1, y_N, \cdots, y_N^{d-1})$.
  inverting $d \times d$ **polynomial matrix with coefficients of degree** $O(pr)$.
- Computing gcrd of $N(\partial^p)$ and $\partial - L(\partial^p)$ with $N \in C[Y]$ and $L \in \mathbb{F}_p(x)[Y]$.
  naive approach manipulates objects of size $O(p^2 rd)$

Future works

- Implementation

Future works

- Implementation
- lclm factorisation.

Future works

- Implementation
- lclm factorisation.
- Factorisation of differential systems

Future works

- Implementation
- lclm factorisation.
- Factorisation of differential systems

Thank you for your attention