Factorisation of linear differential operators in positive characteristic

–PhD Defense–

Raphaël Pagès

Thesis prepared at IMB and INRIA

February 21, 2024

Linear differential operator algebra

Definition

K is a differential field if it is equipped with an additive map $f \mapsto f'$ verifying the Leibniz rule

$$(fg)' = f'g + fg'.$$

Linear differential operator algebra

Definition

K is a differential field if it is equipped with an additive map $f \mapsto f'$ verifying the Leibniz rule

$$(fg)' = f'g + fg'.$$

Linear differential operators in $K\langle\partial\rangle = \{a_n\partial^n + \cdots + a_1\partial + a_0\}$.

Linear differential operator algebra

Definition

K is a differential field if it is equipped with an additive map $f \mapsto f'$ verifying the Leibniz rule

$$(fg)' = f'g + fg'.$$

Linear differential operators in $K\langle\partial\rangle = \{a_n\partial^n + \cdots + a_1\partial + a_0\}$.

Commutation rule:

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

Linear differential operator algebra

Definition

K is a differential field if it is equipped with an additive map $f \mapsto f'$ verifying the Leibniz rule

$$(fg)' = f'g + fg'.$$

Linear differential operators in $K\langle\partial\rangle = \{a_n\partial^n + \cdots + a_1\partial + a_0\}$.

Commutation rule:

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

Example of derivation:

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

over $\mathbb{F}_p(x)$

Linear differential operator algebra

Definition

K is a differential field if it is equipped with an additive map $f \mapsto f'$ verifying the Leibniz rule

$$(fg)' = f'g + fg'.$$

Linear differential operators in $K\langle\partial\rangle = \{a_n\partial^n + \cdots + a_1\partial + a_0\}$.

Commutation rule:

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

Example of derivation:

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

over $\mathbb{F}_p(x)$

Exemple :

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

“Resolution” and factorisation

$L \in K\langle\partial\rangle$.

$$L(y) = 0$$

“Resolution” and factorisation

$L \in K\langle\partial\rangle$.

$$L(y) = 0$$

- If L' is a right factor of L then all solutions of L' are solutions of L.

“Resolution” and factorisation

$L \in K\langle\partial\rangle$.

$$L(y) = 0$$

- If L' is a right factor of L then all solutions of L' are solutions of L.
- Factorisation of L gives information on “where” to find solutions.

“Resolution” and factorisation

$L \in K\langle\partial\rangle$.

$$L(y) = 0$$

- If L' is a right factor of L then all solutions of L' are solutions of L.
- Factorisation of L gives information on “where” to find solutions.

Sometimes the only available description of a solution is the smallest LDE it verifies.

“Resolution” and factorisation

$L \in K\langle\partial\rangle$.

$$L(y) = 0$$

- If L' is a right factor of L then all solutions of L' are solutions of L.
- Factorisation of L gives information on “where” to find solutions.

Sometimes the only available description of a solution is the smallest LDE it verifies.

Analogy: Sometimes the only description of a root of a polynomial is its minimal polynomial.

“Resolution” and factorisation

$L \in K\langle\partial\rangle$.

$$L(y) = 0$$

- If L' is a right factor of L then all solutions of L' are solutions of L.
- Factorisation of L gives information on “where” to find solutions.

Sometimes the only available description of a solution is the smallest LDE it verifies.

Analogy: Sometimes the only description of a root of a polynomial is its minimal polynomial.

Objective: How to factor L as a product of irreducible linear differential operators?

Contribution 1

Theorem (P., 2021)

It is possible to compute, for a given linear differential equation with coefficients in $\mathbb{Z}[x]$, the characteristic polynomials of its p-curvatures for all primes $p < N$ using $\tilde{O}(N)$ binary operations.

Contribution 1

Theorem (P., 2021)

It is possible to compute, for a given linear differential equation with coefficients in $\mathbb{Z}[x]$ of order m, with polynomial coefficients of degree at most d and integer coefficients of bit size at most n, all the characteristic polynomials of its p-curvatures for all primes $p < N$ using

$$\tilde{O}(Nd((n+d)(m+d)^{\omega} + (m+d)^{\Omega}))$$

binary operations.

Contribution 1

Theorem (P., 2021)

It is possible to compute, for a given linear differential equation with coefficients in $\mathbb{Z}[x]$ of order m, with polynomial coefficients of degree at most d and integer coefficients of bit size at most n, all the characteristic polynomials of its p-curvatures for all primes $p < N$ using

$$\tilde{O}(Nd((n+d)(m+d)^{\omega} + (m+d)^{\Omega}))$$

binary operations.

- $\omega < 2,373$ is an exponent of matrix multiplication in any ring.
- $\Omega < 2,698$ is an exponent for the computation of the characteristic polynomial in any ring.

Contribution 1

Theorem (P., 2021)

It is possible to compute, for a given linear differential equation with coefficients in $A[x]$ of order m, with polynomial coefficients of degree at most d, all the characteristic polynomials of its p-curvatures for all primes $p < N$ using

$$\tilde{O}(Nd((m+d)^{\omega} + (m+d)^{\Omega}))$$

operations in A.

- $\omega < 2,373$ is an exponent of matrix multiplication in any ring.
- $\Omega < 2,698$ is an exponent for the computation of the characteristic polynomial in any ring.

Contribution 1

Theorem (P., 2021)

It is possible to compute, for a given linear differential equation with coefficients in $A[x]$ of order m, with polynomial coefficients of degree at most d, all the characteristic polynomials of its p-curvatures for all primes $p < N$ using

$$\tilde{O}(Nd((m+d)^{\omega} + (m+d)^{\Omega}))$$

operations in A.

Ingredients:

- Isomorphism with skew polynomials

Contribution 1

Theorem (P., 2021)

It is possible to compute, for a given linear differential equation with coefficients in $A[x]$ of order m, with polynomial coefficients of degree at most d, all the characteristic polynomials of its p-curvatures for all primes $p < N$ using

$$\tilde{O}(Nd((m+d)^{\omega} + (m+d)^{\Omega}))$$

operations in A.

Ingredients:

- Isomorphism with skew polynomials
- Azumaya algebra structure

Contribution 1

Theorem (P., 2021)

It is possible to compute, for a given linear differential equation with coefficients in $A[x]$ of order m, with polynomial coefficients of degree at most d, all the characteristic polynomials of its p-curvatures for all primes $p < N$ using

$$\tilde{O}(Nd((m+d)^{\omega} + (m+d)^{\Omega}))$$

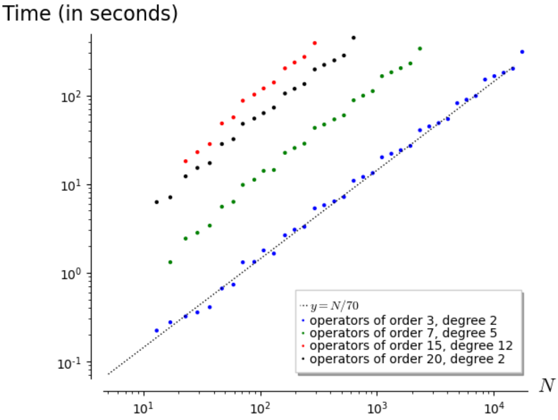
operations in A.

Ingredients:

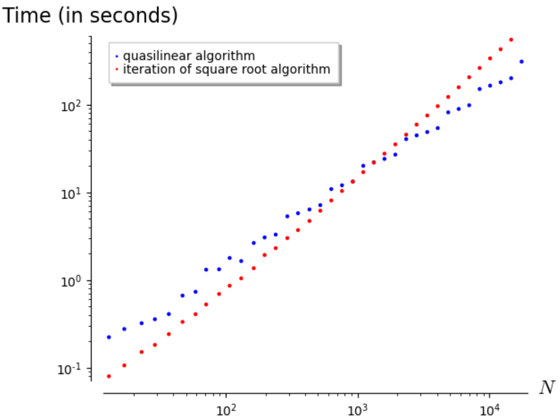
- Isomorphism with skew polynomials
- Azumaya algebra structure
- Fast factorial computation techniques (Harvey 2014)

Implementation

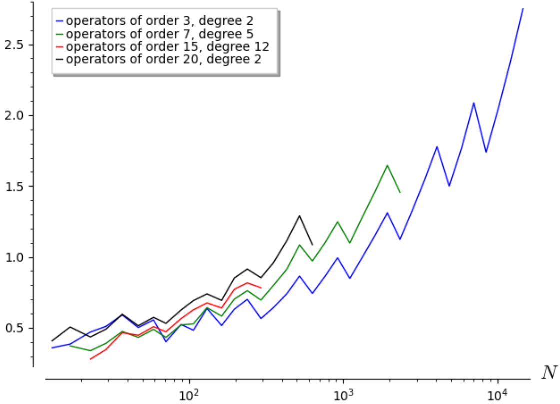
Implementation of the algorithm in SageMath



Comparison with previously best algorithm



Comparison with previously best algorithm



State of the art on factorisation

In characteristic 0:

- D. Yu. Grigoriev, Complexity of factoring and calculating the GCD of linear ordinary differential operators, JSC. 10 (1990).
- M. van Hoeij, Factorization of differential operators with rational functions coefficients, JSC. 24 (1997).
- M. van Hoeij. Rational solutions of the mixed differential equation and its application to factorization of differential operators. ISSAC 1996.
- J. van der Hoeven, Around the numeric-symbolic computation of differential Galois groups. JSC. 42 (2007)
- F. Chyzak, A. Goyer, and M. Mezzarobba, Symbolic-numeric factorization of differential operators. ISSAC 2022.

State of the art on factorisation

In characteristic p:

- M. van der Put, Differential equations in characteristic p. 1995.
- 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 on factorisation

Unsolved case: Central operators

State of the art on factorisation

Unsolved case: Central operators

Facts

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

State of the art on factorisation

Unsolved case: Central operators

Facts

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

Let $N \in C[Y]$ be an irreducible polynomial. **Two questions:**

State of the art on factorisation

Unsolved case: Central operators

Facts

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

Let $N \in C[Y]$ be an irreducible polynomial. **Two questions:**

- Is $N(\partial^p)$ irreducible?

State of the art on factorisation

Unsolved case: Central operators

Facts

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

Let $N \in C[Y]$ be an irreducible polynomial. **Two questions:**

- Is $N(\partial^p)$ irreducible?
- If it isn't, how to determine an irreducible divisor of it?

Contribution 2

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). There exists an algorithm testing the irreducibility of $N_*(x^p, \partial^p)$ in polynomial time in d_x, d_y and $\log(p)$.

Contribution 2

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). There exists an algorithm testing the irreducibility of $N_*(x^p, \partial^p)$ in polynomial time in d_x, d_y and $\log(p)$.

Ingredients:

Contribution 2

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). There exists an algorithm testing the irreducibility of $N_*(x^p, \partial^p)$ in polynomial time in d_x, d_y and $\log(p)$.

Ingredients:

- Central simple algebra

Contribution 2

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). There exists an algorithm testing the irreducibility of $N_*(x^p, \partial^p)$ in polynomial time in d_x, d_y and $\log(p)$.

Ingredients:

- Central simple algebra
- Brauer group, local-global principle

Contribution 2

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). There exists an algorithm testing the irreducibility of $N_*(x^p, \partial^p)$ in polynomial time in d_x, d_y and $\log(p)$.

Ingredients:

- Central simple algebra
- Brauer group, local-global principle
- Hensel lemma

Contribution 3

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). If $N_*(x^p, \partial^p)$ is reducible then there exists an irreducible factor of $N_*(x^p, \partial^p)$ whose coefficients are of degree $O(d_x^2 d_y^4)$ and an algorithm finding such a factor in time polynomial in d_x and d_y and quasi-linear in p.

Contribution 3

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). If $N_*(x^p, \partial^p)$ is reducible then there exists an irreducible factor of $N_*(x^p, \partial^p)$ whose coefficients are of degree $O(d_x^2 d_y^4)$ and an algorithm finding such a factor in time polynomial in d_x and d_y and quasi-linear in p.

Ingredients:

Contribution 3

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). If $N_*(x^p, \partial^p)$ is reducible then there exists an irreducible factor of $N_*(x^p, \partial^p)$ whose coefficients are of degree $O(d_x^2 d_y^4)$ and an algorithm finding such a factor in time polynomial in d_x and d_y and quasi-linear in p.

Ingredients:

- Geometry of curves

Contribution 3

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). If $N_*(x^p, \partial^p)$ is reducible then there exists an irreducible factor of $N_*(x^p, \partial^p)$ whose coefficients are of degree $O(d_x^2 d_y^4)$ and an algorithm finding such a factor in time polynomial in d_x and d_y and quasi-linear in p.

Ingredients:

- Geometry of curves
- Riemann-Roch spaces

Contribution 3

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). If $N_*(x^p, \partial^p)$ is reducible then there exists an irreducible factor of $N_*(x^p, \partial^p)$ whose coefficients are of degree $O(d_x^2 d_y^4)$ and an algorithm finding such a factor in time polynomial in d_x and d_y and quasi-linear in p.

Ingredients:

- Geometry of curves
- Riemann-Roch spaces
- Divisor class group

Contribution 3

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X,Y]$ be an irreducible polynomial of bidegree (d_x, d_y). If $N_*(x^p, \partial^p)$ is reducible then there exists an irreducible factor of $N_*(x^p, \partial^p)$ whose coefficients are of degree $O(d_x^2 d_y^4)$ and an algorithm finding such a factor in time polynomial in d_x and d_y and quasi-linear in p.

Ingredients:

- Geometry of curves
- Riemann-Roch spaces
- Divisor class group

Remark

The algorithm works for operators with coefficients in algebraic function fields.

Setting

We seek to factor $N(\partial^p)$, with $N(Y)$ irreducible separable over C.

Setting

We seek to factor $N(\partial^p)$, with $N(Y)$ irreducible separable 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

We seek to factor $N(\partial^p)$, with $N(Y)$ irreducible separable 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

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

Setting

We seek to factor $N(\partial^p)$, with $N(Y)$ irreducible separable 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

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

Fact

$L \mapsto \mathcal{D}_{N(\partial^p)} L$ is a decreasing bijection between

Setting

We seek to factor $N(\partial^p)$, with $N(Y)$ irreducible separable 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

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

Fact

$L \mapsto \mathcal{D}_{N(\partial^p)} L$ is a decreasing bijection between

- The set of monic divisors of $N(\partial^p)$

Setting

We seek to factor $N(\partial^p)$, with $N(Y)$ irreducible separable 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

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

Fact

$L \mapsto \mathcal{D}_{N(\partial^p)} L$ is a decreasing bijection between

- The set of monic divisors of $N(\partial^p)$
- The set of $\mathbb{F}_p(x)\langle\partial\rangle$-submodules of $\mathcal{D}_{N(\partial^p)}$.

Structural results

Notation

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

Structural results

Notation

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

Proposition (Jacobson)

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

Structural results

Notation

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

Proposition (Jacobson)

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

Theorem (Artin-Wedderburn)

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

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

Structural results

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

Notation

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

Structural results

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

Notation

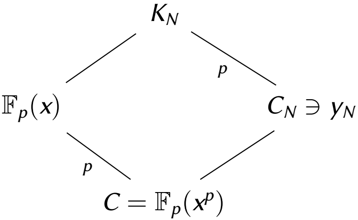
y_N is the image of Y in $C_N = {}^{C[Y]}/_{N(Y)}$
$K_N = \mathbb{F}_p(x) \cdot C_N$

Structural results

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

Notation

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



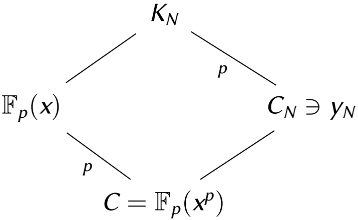
Structural results

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

Notation

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

$$\varphi_N : {}^{\mathbb{F}_p(x)\langle\partial\rangle}/_{N(\partial^p)} \xrightarrow{\sim} {}^{K_N\langle\partial\rangle}/_{\partial^p - y_N}$$

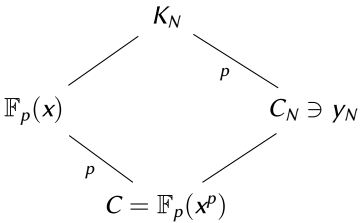


If $\mathcal{D}_{N(\partial^p)}$ is a division algebra then $N(\partial^p)$ has no nontrivial divisor.

Notation

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

$\varphi_N : {}^{\mathbb{F}_p(x)\langle\partial\rangle}/_{N(\partial^p)} \xrightarrow{\sim} {}^{K_N\langle\partial\rangle}/_{\partial^p - y_N}$



Lemma (Jacobson, van der Put)

If $\mathcal{D}_{N(\partial^p)} \simeq M_p(C_N)$ then $L \in K_N\langle\partial\rangle$ is an irreducible divisor of $\partial^p - y_N$ iff $L = \partial - f$ with $f^{(p-1)} + f^p = y_N$.

Local-global principle

$K_N\langle\partial\rangle \big/ \partial^p - y_N$ is a finite dimensional central simple C_N-algebra

Local-global principle

$K_N\langle\partial\rangle\big/\partial^p - y_N$ is a finite dimensional central simple C_N-algebra
$\Rightarrow$ has an isomorphism class in $\mathrm{Br}(C_N)$.

Local-global principle

${}^{K_N\langle\partial\rangle}\big/_{\partial^p - y_N}$ is a finite dimensional central simple C_N-algebra
$\Rightarrow$ has an isomorphism class in $\mathrm{Br}(C_N)$.

$\partial^p - y_N$ is reducible in $K_N\langle\partial\rangle$ iff ${}^{K_N\langle\partial\rangle}\big/_{\partial^p - y_N}$

Local-global principle

${}^{K_N\langle\partial\rangle}\big/_{\partial^p - y_N}$ is a finite dimensional central simple C_N-algebra
$\Rightarrow$ has an isomorphism class in $\mathrm{Br}(C_N)$.

$\partial^p - y_N$ is reducible in $K_N\langle\partial\rangle$ iff ${}^{K_N\langle\partial\rangle}\big/_{\partial^p - y_N} \simeq M_p(C_N)$

Local-global principle

$K_N\langle\partial\rangle \big/ \partial^p - y_N$ is a finite dimensional central simple C_N-algebra
$\Rightarrow$ has an isomorphism class in $\mathrm{Br}(C_N)$.

$\partial^p - y_N$ is reducible in $K_N\langle\partial\rangle$ iff $K_N\langle\partial\rangle \big/ \partial^p - y_N$ is trivial in $\mathrm{Br}(C_N)$

Local-global principle

$K_N\langle\partial\rangle \big/ \partial^p - y_N$ is a finite dimensional central simple C_N-algebra
$\Rightarrow$ has an isomorphism class in $\mathrm{Br}(C_N)$.

$\partial^p - y_N$ is reducible in $K_N\langle\partial\rangle$ iff $K_N\langle\partial\rangle \big/ \partial^p - y_N$ is trivial in $\mathrm{Br}(C_N)$

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

where $\mathbb{P}_{C_N}$ is the set of places of C_N and $C_{N,\mathfrak{P}}$ is the completion of C_N in $\mathfrak{P}$.

Local-global principle

${}^{K_N\langle\partial\rangle}\big/_{\partial^p - y_N}$ is a finite dimensional central simple C_N-algebra
$\Rightarrow$ has an isomorphism class in $\mathrm{Br}(C_N)$.

$\partial^p - y_N$ is reducible in $K_N\langle\partial\rangle$ iff ${}^{K_N\langle\partial\rangle}\big/_{\partial^p - y_N}$ is trivial in $\mathrm{Br}(C_N)$

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

where $\mathbb{P}_{C_N}$ is the set of places of C_N and $C_{N,\mathfrak{P}}$ is the completion of C_N in $\mathfrak{P}$.

Theorem (P. 2023)

$N(\partial^p)$ is reducible iff the equation $f^{(p-1)} + f^p = y_N$ has a local solution in every place of K_N.

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N \qquad \text{in } \mathbb{F}_q((t)),$$

where g is the derivative of a prime element of the place considered.

Hensel lemma

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N \qquad \text{in } \mathbb{F}_q((t)),$$

where g is the derivative of a prime element of the place considered.

Theorem (P. 2023)

If $f \in \mathbb{F}_q((t))$ verifies $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N + O(t^{pn})$ then there exists $f_* \in \mathbb{F}_q((t))$ such that

$$\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f_*) + f_*^p = y_N + O(t^{p(pn+(p-1)(1-\nu(g)))})$$

Irreducibility test

Corollary

- $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N$ has a solution in $\mathbb{F}_q((t))$ iff there exists $f_* \in \mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N + O(t^{p\nu(g)})$.

Irreducibility test

Corollary

- $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N$ has a solution in $\mathbb{F}_q((t))$ iff there exists $f_* \in \mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N + O(t^{p\nu(g)})$.
- The condition is empty unless $\nu(y_N) < p\nu(g)$.

Irreducibility test

Corollary

- $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N$ has a solution in $\mathbb{F}_q((t))$ iff there exists $f_* \in \mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N + O(t^{p\nu(g)})$.
- The condition is empty unless $\nu(y_N) < p\nu(g)$.
- $f^{(p-1)} + f^p = y_N$ has a solution in K_N iff it has a local solution at the poles of y_N and x.

Irreducibility test

Corollary

- $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N$ has a solution in $\mathbb{F}_q((t))$ iff there exists $f_* \in \mathbb{F}_q((t))$ such that $\left(g\frac{\mathrm{d}}{\mathrm{d}t}\right)^{p-1}(f) + f^p = y_N + O(t^{p\nu(g)})$.
- The condition is empty unless $\nu(y_N) < p\nu(g)$.
- $f^{(p-1)} + f^p = y_N$ has a solution in K_N iff it has a local solution at the poles of y_N and x.

Theorem (P. 2023)

Let $N_* \in \mathbb{F}_p[X, Y]$ be an irreducible polynomial of bidegree (d_x, d_y). We can test the irreducibility of $N_*(x^p, \partial^p)$ in $\mathbb{F}_p(x)\langle\partial\rangle$ at the cost of:

- *a factorisation of x and a root of N_* in K_N,*
- *$O(d_x + d_y)$ evals of functions in K_N of size $O(d_y \times (d_x^2 d_y + d_x d_y^2))$,*
- *$O_\varepsilon((d_x + \deg a \log(p)^2 + (d_x^3 d_y^2 + d_x^2 d_y^3)\log(p))$ bit operations.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Any pole of f which is not a pole of a is a simple pole.

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

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

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

Any pole of f which is not a pole of a is a simple pole.

Remove poles by adding multiple of $\frac{h'}{h}$.

p-Riccati equation in the general case

Same ideas:

p-Riccati equation in the general case

Same ideas:

Step 1: Locate and bound the poles of a solution.

p-Riccati equation in the general case

Same ideas:

Step 1: Locate and bound the poles of a solution.

Step 2: Compute a Riemann-Roch space.

p-Riccati equation in the general case

Same ideas:

Step 1: Locate and bound the poles of a solution.

Step 2: Compute a Riemann-Roch space.

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

p-Riccati equation in the general case

Same ideas:

Step 1: Locate and bound the poles of a solution.

Step 2: Compute a Riemann-Roch space.

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

Difference:

p-Riccati equation in the general case

Same ideas:

Step 1: Locate and bound the poles of a solution.

Step 2: Compute a Riemann-Roch space.

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

Difference:

- Poles not necessarily simple. Bounded by ramification index.

p-Riccati equation in the general case

Same ideas:

Step 1: Locate and bound the poles of a solution.

Step 2: Compute a Riemann-Roch space.

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

Difference:

- Poles not necessarily simple. Bounded by ramification index.
- Local improvement $f - \frac{h'}{h}$.

p-Riccati equation in the general case

Same ideas:

Step 1: Locate and bound the poles of a solution.

Step 2: Compute a Riemann-Roch space.

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

Difference:

- Poles not necessarily simple. Bounded by ramification index.
- Local improvement $f - \frac{h'}{h}$.

Problem: By adding $\frac{h'}{h}$ we may add more poles.

p-Riccati equation in the general case

How close is the divisor of poles of f from being a $\frac{h'}{h}$?

p-Riccati equation in the general case

How close is the divisor of poles of f from being a $\frac{h'}{h}$?

Definition

- $D \sim D'$ iff $D - D'$ is principal i.e. equal to $(h) := \sum_{\mathfrak{P} \in \mathbb{P}_{K_N}} \nu_{\mathfrak{P}}(h) \cdot \mathfrak{P}$ for some $h \in K_N$.
- The group of equivalence classes of divisors is the divisor class group of $\mathrm{Cl}(K_N)$

p-Riccati equation in the general case

How close is the divisor of poles of f from being a $\frac{h'}{h}$?

Definition

- $D \sim D'$ iff $D - D'$ is principal i.e. equal to $(h) := \sum_{\mathfrak{P} \in \mathbb{P}_{K_N}} \nu_{\mathfrak{P}}(h) \cdot \mathfrak{P}$ for some $h \in K_N$.
- The group of equivalence classes of divisors is the divisor class group of $\mathrm{Cl}(K_N)$

$\mathrm{Cl}(K_N)$ is a finitely generated commutative group.

p-Riccati equation in the general case

Theorem (P. 2023)

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of ${}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$ then

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing$$

p-Riccati equation in the general case

Theorem (P. 2023)

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of ${}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$ then

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing$$

where

$$A(S) = \max(\mathrm{Diff}(K_N) - 2(x)_\infty + \sum_{\mathfrak{P} \in S} \mathfrak{P}, (a)_\infty).$$

Algorithm

Theorem

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of ${}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$ *then*

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing.$$

Algorithm

Theorem

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of $\mathrm{Cl}(K_N)/_{p\mathrm{Cl}(K_N)}$ then

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing.$$

- Compute S a generating family of $\mathrm{Cl}(K_N)/_{p\mathrm{Cl}(K_N)}$

Algorithm

Theorem

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of ${}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$ then

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing.$$

- Compute S a generating family of ${}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$
- Compute a $\mathbb{F}_p$-basis of $\mathcal{L}(A(S))$.

Algorithm

Theorem

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of $\mathrm{Cl}(K_N)/_{p\mathrm{Cl}(K_N)}$ *then*

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing.$$

- Compute S a generating family of $\mathrm{Cl}(K_N)/_{p\mathrm{Cl}(K_N)}$
- Compute a $\mathbb{F}_p$-basis of $\mathcal{L}(A(S))$.
- Solve a linear system.

Algorithm

Theorem

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of $\mathrm{Cl}(K_N)/p\mathrm{Cl}(K_N)$ *then*

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing.$$

- Compute S a generating family of $\mathrm{Cl}(K_N)/p\mathrm{Cl}(K_N)$
- Compute a $\mathbb{F}_p$-basis of $\mathcal{L}(A(S))$.
- Solve a linear system.

Algorithm

Theorem

Let Σ_N be the set of solutions of the p-Riccati equation. If S is a generating family of ${}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$ then

$$\Sigma_N = \varnothing \Leftrightarrow \Sigma_N \cap \mathcal{L}(A(S)) = \varnothing.$$

- ~~Compute S a generating family of ${}^{\mathrm{Cl}(K_N)}/_{p\mathrm{Cl}(K_N)}$.~~
  Pick sufficiently many random places.
- Compute a $\mathbb{F}_p$-basis of $\mathcal{L}(A(S))$.
- Solve a linear system.

Perspectives

- lclm decomposition. Writing L as the lclm of $L_1, \ldots, L_n$ with $\sum_{i=1}^{n} \operatorname{ord}(L_i) = \operatorname{ord}(L)$.

Perspectives

- lclm decomposition. Writing L as the lclm of $L_1, \ldots, L_n$ with $\sum_{i=1}^{n} \operatorname{ord}(L_i) = \operatorname{ord}(L)$.
- Loewy decomposition: $L = L_1 \ldots L_n$ with L_n being the lclm of all the irreducible right factors of L. Give a lclm decomposition of each L_i.

Perspectives

- lclm decomposition. Writing L as the lclm of $L_1, \ldots, L_n$ with $\sum_{i=1}^{n} \operatorname{ord}(L_i) = \operatorname{ord}(L)$.
- Loewy decomposition: $L = L_1 \ldots L_n$ with L_n being the lclm of all the irreducible right factors of L. Give a lclm decomposition of each L_i.
- Study the fine-grained algorithmic aspects of the algorithm (OM-factorization, Riemann-Roch spaces)

Thank you for your attention

p-Riccati equation in the general case

Denote $K_N = \mathbb{F}_p(x)[a]$ with $a^p = y_N$.
Let $f \in K_N$ verify $f^{(p-1)} + f^p = a^p$. Let $\mathfrak{P}$ be a pole of f, $\nu_{\mathfrak{P}}$ the associated valuation and $e(\mathfrak{P})$ its ramification index.

Lemma

$$\nu_{\mathfrak{P}}(f) \geqslant \min(-e(\mathfrak{P}), \nu_{\mathfrak{P}}(a))$$

Lemma

If $\nu_{\mathfrak{P}}(a) > -e(\mathfrak{P})$, then there exists a unique $k \in \mathbb{F}_p$ such that for all $g \in K_N$ verifying $\nu_{\mathfrak{P}}(g) \equiv k \mod p$,

$$\nu_{\mathfrak{P}}(f - \frac{g'}{g}) \geqslant 1 - e(\mathfrak{P}).$$

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

p-Riccati equation in the general case

Theorem

$$\mathfrak{Re}(f) = \sum_{\mathfrak{P}} \mathfrak{Re}_{\mathfrak{P}}(f) \cdot \mathfrak{P}$$

If $\mathfrak{Re}(f) \sim D'$ *then there exists another solution* f_* *verifying*

$$\nu_{\mathfrak{P}}(f_*) \geqslant \min(\nu_{\mathfrak{P}}(a), 1 - e(\mathfrak{P}))$$

for all $\mathfrak{P} \notin \mathrm{Supp}(D')$.

p-Riccati equation in the general case

Theorem

$$\mathfrak{Re}(f) = \sum_{\mathfrak{P}} \mathfrak{Re}_{\mathfrak{P}}(f) \cdot \mathfrak{P}$$

If $\mathfrak{Re}(f) \sim D'$ *then there exists another solution* f_* *verifying*

$$\nu_{\mathfrak{P}}(f_*) \geqslant \min(\nu_{\mathfrak{P}}(a), 1 - e(\mathfrak{P}))$$

for all $\mathfrak{P} \notin \mathrm{Supp}(D')$.

Corollary

If S is a family of places of K_N generating $\mathrm{Cl}(K_N)$ then there exists another solution f_* of the p-Riccati equation verifying $\nu_{\mathfrak{P}}(f_*) \geqslant \min(\nu_{\mathfrak{P}}(a), 1 - e(\mathfrak{P}))$ for all $\mathfrak{P} \notin S$.

p-Riccati equation in the general case

Theorem

$$\mathfrak{Re}(f) = \sum_{\mathfrak{P}} \mathfrak{Re}_{\mathfrak{P}}(f) \cdot \mathfrak{P}$$

If $\mathfrak{Re}(f) \sim D' + pD_p$ then there exists another solution f_* verifying

$$\nu_{\mathfrak{P}}(f_*) \geqslant \min(\nu_{\mathfrak{P}}(a), 1 - e(\mathfrak{P}))$$

for all $\mathfrak{P} \notin \mathrm{Supp}(D')$.

Corollary

If S is a family of places of K_N generating ${}^{\mathrm{Cl}(K_N)}/{}_{p\mathrm{Cl}(K_N)}$ then there exists another solution f_* of the p-Riccati equation verifying $\nu_{\mathfrak{P}}(f_*) \geqslant \min(\nu_{\mathfrak{P}}(a), 1 - e(\mathfrak{P}))$ for all $\mathfrak{P} \notin S$.