Algorithms for p-Curvatures of Difference Operators

Yi Zhou

Department of Mathematics
Florida State University

Outline

- Definitions

Outline

- Definitions
- Algorithms:

Outline

- Definitions
- Algorithms:
  - a plain algorithm
  - an algorithm computing $P(L)\mid_{x=\alpha}$
  - α-generator
  - desingularizer

Outline

- Definitions
- Algorithms:
    - a plain algorithm
    - an algorithm computing $P(L)\mid_{x=\alpha}$
    - α-generator
    - desingularizer
- More on p-curvature

Difference Equations and Difference Operators

Definition

Let $k = \mathbb{C}(x)$. The shift operator τ is the $\mathbb{C}$-automorphism of k defined by

$$(\tau(f))(x) = f(x+1).$$

Difference Equations and Difference Operators

Definition

Let $k = \mathbb{C}(x)$. The shift operator τ is the $\mathbb{C}$-automorphism of k defined by

$$(\tau(f))(x) = f(x+1).$$

A difference operator is an operator

$$L = a_n(x)\tau^n + \cdots + a_0(x)\tau^0$$

that acts in the following way on a rational function f

$$(L(f))(x) = a_n(x)f(x+n) + \cdots + a_0(x)f(x).$$

Difference Operators

The set of all difference operators is

$$k[\tau] = \{a_n\tau^n + \cdots + a_0\tau^0 | n \in \mathbb{N}, a_0, \ldots, a_n \in k\}.$$

It is a ring, with multiplication defined by

$$\tau \cdot a = \tau(a)\tau,$$

where $a \in k \subset k[\tau]$.

Difference Operators: Order and Degrees

Definition

Let $L = \sum_{i=0}^{n} a_i(x)\tau^i$ be a non-zero difference operator. Define the *order* of L to be

$$\mathrm{ord}(L) := \max\{i | a_i \neq 0\}.$$

Difference Operators: Right Division

Theorem (Right Division with Remainder)

Suppose $L_1, L_2 \in k[\tau]$ *and* $\mathrm{ord}(L_2) > 0$. *There exist unique difference operators* q, r *such that*

$$L_1 = qL_2 + r,$$

and $\mathrm{ord}(r) < \mathrm{ord}(L_2)$.

Final Goal

An algorithm that for any $L \in D$ finds all the pairs L_1, L_2 with lower orders than L such that $L = L_1 L_2$.

Difference Operators Over Finite Fields

Definition

Define multiplication on the set $\mathbb{F}_p(x)[\tau]$ by

$$\tau x = (x+1)\tau.$$

Denote $D_p = \mathbb{F}_p(x)[\tau]$.

Difference Operators Over Finite Fields

Definition

Define multiplication on the set $\mathbb{F}_p(x)[\tau]$ by

$$\tau x = (x + 1)\tau.$$

Denote $D_p = \mathbb{F}_p(x)[\tau]$.

Note: D_p has a non-trivial center $\mathbb{F}_p(x^p - x)[\tau^p]$.

p-Curvature

The D_p-module D_p/D_pL is a $\mathbb{F}_p(x)$-vector space.

p-Curvature

The D_p-module D_p/D_pL is a $\mathbb{F}_p(x)$-vector space.
$\tau : D_p/D_pL \to D_p/D_pL$ induces a $\mathbb{F}_p$-linear map which is not $\mathbb{F}_p(x)$-linear, since

$$\tau(x) = (x+1)\tau.$$

p-Curvature

The D_p-module D_p/D_pL is a $\mathbb{F}_p(x)$-vector space.
$\tau : D_p/D_pL \to D_p/D_pL$ induces a $\mathbb{F}_p$-linear map which is not $\mathbb{F}_p(x)$-linear, since

$$\tau(x) = (x+1)\tau.$$

τ^p induces a $\mathbb{F}_p(x)$-linear map, since

$$\tau^p(x) = (x+p)\tau^p = x\tau^p.$$

p-Curvature

Definition

For $L \in D_p$, the characteristic polynomial of the $\mathbb{F}_p(x)$-linear map $\tau^p : D_p/D_pL \to D_p/D_pL$ is called the *p-curvature* of L, denoted by $P(L)$.

p-Curvature

Definition

For $L \in D_p$, the characteristic polynomial of the $\mathbb{F}_p(x)$-linear map $\tau^p : D_p/D_pL \to D_p/D_pL$ is called the *p-curvature* of L, denoted by $P(L)$.

Proposition (The Product Rule)

$$P(L_1L_2) = P(L_1)P(L_2).$$

p-Curvature

How does p-curvature help factor operators in $\mathbb{Q}(x)[\tau]$?

p-Curvature

How does p-curvature help factor operators in $\mathbb{Q}(x)[\tau]$?
We can define p-curvature for operators in $\mathbb{Z}[x][\tau]$.

p-Curvature

How does p-curvature help factor operators in $\mathbb{Q}(x)[\tau]$?
We can define p-curvature for operators in $\mathbb{Z}[x][\tau]$.

- Prove the irreducibility.

p-Curvature

How does p-curvature help factor operators in $\mathbb{Q}(x)[\tau]$?
We can define p-curvature for operators in $\mathbb{Z}[x][\tau]$.

- Prove the irreducibility.
- Restrict search for right-hand factors to some particular orders.

Computing p-curvature: a Plain Algorithm

Goal: finding the matrix A such that

$$(\tau^p, \tau^{p+1}, \ldots, \tau^{p+n-1}) = (1, \tau, \ldots, \tau^{n-1})A,$$

and calculate its char poly.

Computing p-curvature: a Plain Algorithm

Goal: finding the matrix A such that

$$(\tau^p, \tau^{p+1}, \ldots, \tau^{p+n-1}) = (1, \tau, \ldots, \tau^{n-1})A,$$

and calculate its char poly.

- $L = \sum_{i=0}^{n} a_i \tau^i = 0 \implies \tau^n$

Computing p-curvature: a Plain Algorithm

Goal: finding the matrix A such that

$$(\tau^p, \tau^{p+1}, \ldots, \tau^{p+n-1}) = (1, \tau, \ldots, \tau^{n-1})A,$$

and calculate its char poly.

- $L = \sum_{i=0}^{n} a_i \tau^i = 0 \implies \tau^n$
- $\tau L = \sum_{i=0}^{n} a_i (x+1) \tau^{i+1} = 0 \implies \tau^{n+1}$

Computing p-curvature: a Plain Algorithm

Goal: finding the matrix A such that

$$(\tau^p, \tau^{p+1}, \ldots, \tau^{p+n-1}) = (1, \tau, \ldots, \tau^{n-1})A,$$

and calculate its char poly.

- $L = \sum_{i=0}^{n} a_i \tau^i = 0 \implies \tau^n$
- $\tau L = \sum_{i=0}^{n} a_i (x+1)\tau^{i+1} = 0 \implies \tau^{n+1}$
- $\ldots$
- $\tau^k L = 0 \implies \tau^{n+k}$
- $\ldots$
- A and $\mathrm{char}(A) = P(L)$

Computing p-Curvature: $P(L)\mid_{x=\alpha}$

Note: if each x is replaced by some $\alpha \in \overline{F_p}$ in ALG I, then the output is $P(L)\mid_{x=\alpha}$.

Computing p-Curvature: $P(L)\mid_{x=\alpha}$

Note: if each x is replaced by some $\alpha \in \overline{F_p}$ in ALG I, then the output is $P(L)\mid_{x=\alpha}$.

To build $P(L)$ from a number of $P(L)\mid_{x=\alpha}$s, we need the following information:

Computing p-Curvature: $P(L)\mid_{x=\alpha}$

Note: if each x is replaced by some $\alpha \in \overline{F_p}$ in ALG I, then the output is $P(L)\mid_{x=\alpha}$.

To build $P(L)$ from a number of $P(L)\mid_{x=\alpha}$s, we need the following information:

- a denominator bound, i.e. some $B \in \mathbb{F}_p[x]$ such that $BP(L) \in \mathbb{F}_p[x][\lambda]$;

Computing p-Curvature: $P(L)\mid_{x=\alpha}$

Note: if each x is replaced by some $\alpha \in \overline{F_p}$ in ALG I, then the output is $P(L)\mid_{x=\alpha}$.

To build $P(L)$ from a number of $P(L)\mid_{x=\alpha}$s, we need the following information:

- a denominator bound, i.e. some $B \in \mathbb{F}_p[x]$ such that $BP(L) \in \mathbb{F}_p[x][\lambda]$;
- a degree bound for $BP(L)$.

Computing p-Curvature: $P(L) \mid_{x=\alpha}$

Notation:

$$\sigma(a(x)) = a(x)a(x+1)\ldots a(x+p-1)$$

and

$$\tilde{P}(L) = \sigma(a_n)P(L).$$

Computing p-Curvature: $P(L)\mid_{x=\alpha}$

Notation:

$$\sigma(a(x)) = a(x)a(x+1)\dots a(x+p-1)$$

and

$$\tilde{P}(L) = \sigma(a_n)P(L).$$

Proposition

When $L = \sum_{i=0}^{n} a_i \tau^i$ has polynomial coefficients, then

Computing p-Curvature: $P(L)\mid_{x=\alpha}$

Notation:

$$\sigma(a(x)) = a(x)a(x+1)\dots a(x+p-1)$$

and

$$\tilde{P}(L) = \sigma(a_n)P(L).$$

Proposition

When $L = \sum_{i=0}^{n} a_i \tau^i$ has polynomial coefficients, then

- $\tilde{P}(L) \in \mathbb{F}_p[\theta][\lambda]$, *where* $\theta = x^p - x$;

Computing p-Curvature: $P(L) \mid_{x=\alpha}$

Notation:

$$\sigma(a(x)) = a(x)a(x+1)\ldots a(x+p-1)$$

and

$$\tilde{P}(L) = \sigma(a_n)P(L).$$

Proposition

When $L = \sum_{i=0}^{n} a_i \tau^i$ has polynomial coefficients, then

- $\tilde{P}(L) \in \mathbb{F}_p[\theta][\lambda]$, *where* $\theta = x^p - x$;
- $\deg_\theta(\tilde{P}(L)) = \deg_x(L)$;

Computing p-Curvature: $P(L)\mid_{x=\alpha}$

Notation:

$$\sigma(a(x)) = a(x)a(x+1)\dots a(x+p-1)$$

and

$$\tilde{P}(L) = \sigma(a_n)P(L).$$

Proposition

When $L = \sum_{i=0}^{n} a_i \tau^i$ has polynomial coefficients, then

- $\tilde{P}(L) \in \mathbb{F}_p[\theta][\lambda]$, *where* $\theta = x^p - x$;
- $\deg_\theta(\tilde{P}(L)) = \deg_x(L)$;

Computing p-Curvature: α-Generator

Need:

- each distinct $x = \alpha$ yields a distinct value of $x^p - x$.

Computing p-Curvature: α-Generator

Need:

- each distinct $x = \alpha$ yields a distinct value of $x^p - x$.

Require minimal polynomials of α to be

Computing p-Curvature: α-Generator

Need:

- each distinct $x = \alpha$ yields a distinct value of $x^p - x$.

Require minimal polynomials of α to be

- not of degree divisible by p;

Computing p-Curvature: α-Generator

Need:

- each distinct $x = \alpha$ yields a distinct value of $x^p - x$.

Require minimal polynomials of α to be

- not of degree divisible by p;
- in the form of

$$x^n + 0x^{n-1} + \cdots .$$

Computing p-Curvature: α-Generator

Algorithm:

- Generate some irreducible polynomials randomly.

Computing p-Curvature: α-Generator

Algorithm:

- Generate some irreducible polynomials randomly.
- Discard polys of degree divisible by p and transform the others into the form

$$x^n + 0x^{n-1} + \cdots .$$

Computing p-Curvature: α-Generator

Algorithm:

- Generate some irreducible polynomials randomly.
- Discard polys of degree divisible by p and transform the others into the form
$$x^n + 0x^{n-1} + \cdots .$$
- Repeat this process until $\sum \deg(irrpoly) \geq d$.

Note: a polynomial of degree n selected this way contributes to n different values of $x^p - x$.

Computing p-Curvature: Desingularizer

Definition

$L, A \in \mathbb{F}_p[x][\tau]$. Suppose $\operatorname{ord}(A) = n$ and $L_1 = AL$.
$f := \frac{lc(L)}{\tau^{-n}(lc(L_1))}$ is called a *removable factor* of L at order n.

- Proposition: $\sigma(a_n)$ is a denominator bound for $P(L)$.

Computing p-Curvature: Desingularizer

Definition

$L, A \in \mathbb{F}_p[x][\tau]$. Suppose $\mathrm{ord}(A) = n$ and $L_1 = AL$.
$f := \frac{lc(L)}{\tau^{-n}(lc(L_1))}$ is called a *removable factor* of L at order n.

- Proposition: $\sigma(a_n)$ is a denominator bound for $P(L)$.
- Conjecture: $\sigma(\frac{a_n}{\text{removable factors}})$ is a denominator bound.

Computing p-Curvature: Desingularizer

Definition

$L, A \in \mathbb{F}_p[x][\tau]$. Suppose $\mathrm{ord}(A) = n$ and $L_1 = AL$.
$f := \frac{lc(L)}{\tau^{-n}(lc(L_1))}$ is called a *removable factor* of L at order n.

- Proposition: $\sigma(a_n)$ is a denominator bound for $P(L)$.
- Conjecture: $\sigma(\frac{a_n}{\text{removable factors}})$ is a denominator bound.
- Can prove: $\sigma(\frac{a_n}{\text{some removable factor of order 1}})$ is a denominator bound.

Computing p-Curvature: the Main Algorithm

Algorithm:

Computing p-Curvature: the Main Algorithm

Algorithm:
Input: $L \in \mathbb{F}_p[x][\tau]$.

Computing p-Curvature: the Main Algorithm

Algorithm:
Input: $L \in \mathbb{F}_p[x][\tau]$.

- Use the desingularizer to find a denominator bound B and compute the degree bound d for $BP(L)$.

Computing p-Curvature: the Main Algorithm

Algorithm:
Input: $L \in \mathbb{F}_p[x][\tau]$.

- Use the desingularizer to find a denominator bound B and compute the degree bound d for $BP(L)$.
- Use the α-generator to generate d αs (their minimal polynomials, in fact).

Computing p-Curvature: the Main Algorithm

Algorithm:
Input: $L \in \mathbb{F}_p[x][\tau]$.

- Use the desingularizer to find a denominator bound B and compute the degree bound d for $BP(L)$.
- Use the α-generator to generate d αs (their minimal polynomials, in fact).
- Evaluate $BP(L)$ at each $x = \alpha$.

Computing p-Curvature: the Main Algorithm

Algorithm:
Input: $L \in \mathbb{F}_p[x][\tau]$.

- Use the desingularizer to find a denominator bound B and compute the degree bound d for $BP(L)$.
- Use the α-generator to generate d αs (their minimal polynomials, in fact).
- Evaluate $BP(L)$ at each $x = \alpha$.
- Interpolation.

Comparison

$$L := -4x\tau^3 - 83\tau^2 * x^2 - 10x^4 + 97\tau^2 - 73x^2 - 62\tau$$

p	Plain Alg	New Alg
31	4.750s	0.656s
73	1082.704s	2.453
127	∞	5.281

Comparison

$$L = 43\tau^7 - 47x^3\tau^5 + 58x^5\tau^3 + 48x^3\tau^3 + 66x^2\tau^2 + 69x$$

Comparison

$$L = 43\tau^7 - 47x^3\tau^5 + 58x^5\tau^3 + 48x^3\tau^3 + 66x^2\tau^2 + 69x$$

p	Plain Alg II	New Alg
3	1s	1s
53	81.837s	3.141

More on p-Curvature

Proposition

$P(L)(\tau^p)$ is a multiple of L.

More on p-Curvature

Proposition

$P(L)(\tau^p)$ is a multiple of L.

Example

Let $L = \tau - x$. $P(L) = \lambda - (x^p - x)$. $\tau^p - (x^p - x)$ is a multiple of L.

More on p-Curvature

Conjecture:

- $$P(L)(\tau^p) = Z^p \mathrm{LCLM}(N, N\mid_{x=x+1}, \ldots, N\mid_{x=x+p-1}),$$

  $Z \in \mathbb{F}_p(x^p - x)[\tau^p]$: *maximal center factor*
  N: *minimal non-center factor*

More on p-Curvature: Newton Polygon

Conjecture:

More on p-Curvature: Newton Polygon

Conjecture:

- $\tilde{P}(L)$ has the same "Newton Polygon" as L.

More on p-Curvature: Newton Polygon

Conjecture:

- $\tilde{P}(L)$ has the same "Newton Polygon" as L.

Example

Let $L = \tau^3 + (x^2+1)\tau + 3x^3$ and $p = 5$.

$$\tilde{P}(L) = \lambda^3 + 2\lambda^2 + (\theta^2 + 3\theta + 2)\lambda + 3\theta^3.$$

$NP(L)$: lower convex hull of $(0,3),(1,2),(2,-\infty),(3,0)$
$NP(\tilde{P}(L))$: lower convex hull of $(0,3),(1,2),(2,0),(3,0)$

More on p-Curvature: Relation with Generalized Exponents

Let $K = \mathbb{C}((t))$ and $K_r = \mathbb{C}((t^{\frac{1}{r}}))$, where $t = \frac{1}{x}$. Any operator in $K[\tau]$ can be factored completely in some $K_r[\tau]$:

$$L = (\tau - e_1)(\tau - e_2) \cdots (\tau - e_n).$$

More on p-Curvature: Relation with Generalized Exponents

Let $K = \mathbb{C}((t))$ and $K_r = \mathbb{C}((t^{\frac{1}{r}}))$, where $t = \frac{1}{x}$. Any operator in $K[\tau]$ can be factored completely in some $K_r[\tau]$:

$$L = (\tau - e_1)(\tau - e_2)\cdots(\tau - e_n).$$

Can we factor any operator in D_p into linear factors in some algebraic extension of $\mathbb{F}_p(x)$ or $\mathbb{F}_p((t))$?

More on p-Curvature: Relation with Generalized Exponents

Let $K = \mathbb{C}((t))$ and $K_r = \mathbb{C}((t^{\frac{1}{r}}))$, where $t = \frac{1}{x}$. Any operator in $K[\tau]$ can be factored completely in some $K_r[\tau]$:

$$L = (\tau - e_1)(\tau - e_2)\cdots(\tau - e_n).$$

Can we factor any operator in D_p into linear factors in some algebraic extension of $\mathbb{F}_p(x)$ or $\mathbb{F}_p((t))$?
No. Counter example: $\tau^2 - x$ over $\mathbb{F}_2$.

More on p-Curvature: Relation with Generalized Exponents

Let $K = \mathbb{C}((t))$ and $K_r = \mathbb{C}((t^{\frac{1}{r}}))$, where $t = \frac{1}{x}$. Any operator in $K[\tau]$ can be factored completely in some $K_r[\tau]$:

$$L = (\tau - e_1)(\tau - e_2) \cdots (\tau - e_n).$$

Can we factor any operator in D_p into linear factors in some algebraic extension of $\mathbb{F}_p(x)$ or $\mathbb{F}_p((t))$?
No. Counter example: $\tau^2 - x$ over $\mathbb{F}_2$.
But we believe Yes, "wild ramification" (ramification index is divisible by p) is avoided.

More on p-curvature: Global Curvature

Definition

Given $L \in \mathbb{Z}[x][\tau]$. If there is $f \in \mathbb{Q}(\theta)[\lambda]$ such that for almost all primes, the p-curvature of L is $f \bmod p$, then f is called the *global curvature* of L.

More on p-curvature: Global Curvature

Definition

Given $L \in \mathbb{Z}[x][\tau]$. If there is $f \in \mathbb{Q}(\theta)[\lambda]$ such that for almost all primes, the p-curvature of L is $f \bmod p$, then f is called the *global curvature* of L.

Example

$L = \tau - x$ has a global curvature $\lambda - \theta$.

More on p-curvature: Global Curvature

Definition

Given $L \in \mathbb{Z}[x][\tau]$. If there is $f \in \mathbb{Q}(\theta)[\lambda]$ such that for almost all primes, the p-curvature of L is $f \bmod p$, then f is called the *global curvature* of L.

Example

$L = \tau - x$ has a global curvature $\lambda - \theta$.

Example

Based on experiments, we guess $L_i = \tau^2 + (x+1)\tau + x + i (i \in \mathbb{Z})$ has global p-curvature $(\lambda + 1)(\lambda + \theta)$.

Work To Be Done

- Newton polygon;
- factoring operators into linear factors in char p;
- desingularization and denominator bound;
- global curvature;
- relation with p-curvature of differential operators;
- $\cdots$