Computing Characteristic Polynomials of p-Curvatures in Average Polynomial Time

Functional Equation in Limoges 2022

Raphaël Pagès[1 2]

[1]INRIA - LFANT

[2]INRIA - SPECFUN

February 23rd 2022

Differential equations in characteristic p

How "many" algebraic solutions over $\mathbb{F}_p(z)$ does

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

have?

Differential equations in characteristic p

How “many” algebraic solutions over $\mathbb{F}_p(z)$ does

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

have?

Idea: Such an equation has an algebraic basis of solutions iff the ”p-curvature” of this equation is zero.

Differential equations in characteristic p

How "many" algebraic solutions over $\mathbb{F}_p(z)$ does

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

have?

Theorem (Cartier)

For any such linear differential equation we have an equality between

- *the dimension of the space of solutions that are algebraic over* $\mathbb{F}_p(z)$
- *the dimension of the kernel of the p-curvature of this differential equation.*

p-curvature in characteristic 0

Conjecture (Grothendieck-Katz)

A linear differential equation in characteristic 0 admits an algebraic basis of solutions over $\mathbb{Q}(z)$ iff its reduction modulo p has an algebraic basis of solutions over $\mathbb{F}_p(z)$ for all primes p except a finite number.

p-curvature in characteristic 0

Conjecture (Grothendieck-Katz)

A linear differential equation in characteristic 0 admits an algebraic basis of solutions over $\mathbb{Q}(z)$ iff its reduction modulo p has an algebraic basis of solutions over $\mathbb{F}_p(z)$ for all primes p except a finite number.

Theorem (Chudnovsky^2)

If $f \in \mathbb{Z}[[z]]$ (with non zero convergence radius) is a solution of a linear differential equation, then the minimal differential equation for f only has nilpotent p-curvatures, except for a finite number of primes..

Useful for guessing procedures.

Other applications

- Algorithms for factoring differential operators using p-curvatures [Cluzeau, ISSAC 2003]

Other applications

- Algorithms for factoring differential operators using p-curvatures [Cluzeau, ISSAC 2003]
- Algorithms for computing the Lie algebra of differential operators [Barkatou, Cluzeau, Di Vizio, Weil, ISSAC 2016]

Algebra of Differential operators

Definition

Let $\mathcal{A} = \mathbb{F}_p[z]$ or $\mathbb{F}_p(z)$. We define $\mathcal{A}\langle\partial\rangle$.

Algebra of Differential operators

Definition

Let $\mathcal{A} = \mathbb{F}_p[z]$ or $\mathbb{F}_p(z)$. We define $\mathcal{A}\langle\partial\rangle$.

$$\mathcal{A}\langle\partial\rangle \simeq \mathcal{A}[\partial] \text{ as sets}$$

Algebra of Differential operators

Definition

Let $\mathcal{A} = \mathbb{F}_p[z]$ or $\mathbb{F}_p(z)$. We define $\mathcal{A}\langle\partial\rangle$.

$$\mathcal{A}\langle\partial\rangle \simeq \mathcal{A}[\partial] \text{ as sets}$$

Example

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

Algebra of Differential operators

Definition

Let $\mathcal{A} = \mathbb{F}_p[z]$ or $\mathbb{F}_p(z)$. We define $\mathcal{A}\langle\partial\rangle$.

$$\mathcal{A}\langle\partial\rangle \simeq \mathcal{A}[\partial] \text{ as sets}$$

Example

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

$$(z+1)^2\partial^3 - z\partial + (z^3+3)$$

Algebra of Differential operators

Definition

Let $\mathcal{A} = \mathbb{F}_p[z]$ or $\mathbb{F}_p(z)$. We define $\mathcal{A}\langle\partial\rangle$.

$$\mathcal{A}\langle\partial\rangle \simeq \mathcal{A}[\partial] \text{ as sets}$$

Example

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

$$(z+1)^2 \partial^3 - z\partial + (z^3+3)$$

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

The p-curvature

Idea : The p-curvature of an operator is ∂^p modulo this operator

The p-curvature

Definition

The p-curvature of an operator $L \in \mathbb{F}_p(z)\langle\partial\rangle$ is the $\mathbb{F}_p(z)$-linear endomorphism of $\mathbb{F}_p(z)\langle\partial\rangle / \mathbb{F}_p(z)\langle\partial\rangle L$ induced by the left multiplication by ∂^p.

The p-curvature

Definition

The p-curvature of an operator $L \in \mathbb{F}_p(z)\langle\partial\rangle$ is the $\mathbb{F}_p(z)$-linear endomorphism of ${}^{\mathbb{F}_p(z)\langle\partial\rangle}/_{\mathbb{F}_p(z)\langle\partial\rangle L}$ induced by the left multiplication by ∂^p.

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

$$A = \begin{pmatrix} 0 & 0 & -\frac{z^3+3}{(z+1)^2} \\ 1 & 0 & \frac{z}{(z+1)^2} \\ 0 & 1 & 0 \end{pmatrix}$$

The p-curvature

Definition

The p-curvature of an operator $L \in \mathbb{F}_p(z)\langle\partial\rangle$ is the $\mathbb{F}_p(z)$-linear endomorphism of $\mathbb{F}_p(z)\langle\partial\rangle / \mathbb{F}_p(z)\langle\partial\rangle L$ induced by the left multiplication by ∂^p.

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

$$A = \begin{pmatrix} 0 & 0 & -\frac{z^3+3}{(z+1)^2} \\ 1 & 0 & \frac{z}{(z+1)^2} \\ 0 & 1 & 0 \end{pmatrix}$$

$$A_0 = \mathrm{Id} \qquad A_{k+1} = A_k' + AA_k \qquad A_p$$

The p-curvature

Definition

The p-curvature of an operator $L \in \mathbb{F}_p(z)\langle\partial\rangle$ is the $\mathbb{F}_p(z)$-linear endomorphism of ${}^{\mathbb{F}_p(z)\langle\partial\rangle}/_{\mathbb{F}_p(z)\langle\partial\rangle L}$ induced by the left multiplication by ∂^p.

$$(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$$

$$A = \begin{pmatrix} 0 & 0 & -\frac{z^3+3}{(z+1)^2} \\ 1 & 0 & \frac{z}{(z+1)^2} \\ 0 & 1 & 0 \end{pmatrix}$$

$$A_0 = \mathrm{Id} \qquad A_{k+1} = A_k' + AA_k \qquad A_p$$

Size: A_p is of bit size $\tilde{O}(p)$.
Cost: $\tilde{O}(p^2)$ binary operations.

p-curvature of an operator

For $(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$ and $p = 3$.

p-curvature of an operator

For $(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$ and $p = 3$.

$$A_p = \begin{pmatrix} \frac{2z^3}{z^2+2z+1} & \frac{2z^3}{z^3+1} & \frac{2z^4}{z^4+z^3+z+1} \\ \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+2z+1}{z^3+1} & \frac{z^4+z^3+z^2+2z+2}{z^4+z^3+z+1} \\ 0 & \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+z+2}{z^3+1} \end{pmatrix}$$

p-curvature of an operator

For $(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$ and $p = 3$.

$$A_p = \begin{pmatrix} \frac{2z^3}{z^2+2z+1} & \frac{2z^3}{z^3+1} & \frac{2z^4}{z^4+z^3+z+1} \\ \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+2z+1}{z^3+1} & \frac{z^4+z^3+z^2+2z+2}{z^4+z^3+z+1} \\ 0 & \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+z+2}{z^3+1} \end{pmatrix}$$

$$\chi(A_p) = x^3 + \frac{2}{z^3+1}x + \frac{z^6+2z^3}{z^3+1}$$

p-curvature of an operator

For $(z+1)^2 y^{(3)} - zy' + (z^3+3)y = 0$ and $p = 3$.

$$A_p = \begin{pmatrix} \frac{2z^3}{z^2+2z+1} & \frac{2z^3}{z^3+1} & \frac{2z^4}{z^4+z^3+z+1} \\ \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+2z+1}{z^3+1} & \frac{z^4+z^3+z^2+2z+2}{z^4+z^3+z+1} \\ 0 & \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+z+2}{z^3+1} \end{pmatrix}$$

$$\chi(A_p) = x^3 + \frac{2}{z^3+1}x + \frac{z^6+2z^3}{z^3+1}$$

Fact: $\chi(A_p(L)) \in \mathbb{F}_p(z^p)[x]$.

For $(z+1)^2y^{(3)} - zy' + (z^3+3)y = 0$ and $p = 3$.

$$A_p = \begin{pmatrix} \frac{2z^3}{z^2+2z+1} & \frac{2z^3}{z^3+1} & \frac{2z^4}{z^4+z^3+z+1} \\ \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+2z+1}{z^3+1} & \frac{z^4+z^3+z^2+2z+2}{z^4+z^3+z+1} \\ 0 & \frac{z}{z^2+2z+1} & \frac{2z^4+2z^3+z+2}{z^3+1} \end{pmatrix}$$

$$\chi(A_p) = x^3 + \frac{2}{z^3+1}x + \frac{z^6+2z^3}{z^3+1}$$

Fact: $\chi(A_p(L)) \in \mathbb{F}_p(z^p)[x]$.
Size: $\chi(A_p(L))$ is of bit size $O(\log(p))$.

Previous works around the computation of p-curvatures

- First subquadratic time algorithm for computing the p-curvature [Bostan, Schost, ISSAC 2009].

Previous works around the computation of p-curvatures

- First subquadratic time algorithm for computing the p-curvature [Bostan, Schost, ISSAC 2009].
- Computing the p-curvature of an operator in $\tilde{O}(p)$ binary operations [Bostan, Caruso, Schost, ISSAC 2015].

Previous works around the computation of p-curvatures

- First subquadratic time algorithm for computing the p-curvature [Bostan, Schost, ISSAC 2009].
- Computing the p-curvature of an operator in $\tilde{O}(p)$ binary operations [Bostan, Caruso, Schost, ISSAC 2015].
- Computing the characteristic polynomial of the p-curvature of an operator in $\tilde{O}(\sqrt{p})$ binary operations [Bostan, Caruso, Schost, ISSAC 2014].

Previous works around the computation of p-curvatures

- First subquadratic time algorithm for computing the p-curvature [Bostan, Schost, ISSAC 2009].
- Computing the p-curvature of an operator in $\tilde{O}(p)$ binary operations [Bostan, Caruso, Schost, ISSAC 2015].
- Computing the characteristic polynomial of the p-curvature of an operator in $\tilde{O}(\sqrt{p})$ binary operations [Bostan, Caruso, Schost, ISSAC 2014].
- Computing the Invariant factors of the p-curvature of an operator in $\tilde{O}(\sqrt{p})$ binary operations [Bostan, Caruso, Schost, ISSAC 2016].

My Contribution: Theoretical part

Theorem (P., 2021)

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

My Contribution: Theoretical part

Theorem (P., 2021)

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

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

binary operations.

My Contribution: Theoretical part

Theorem (P., 2021)

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

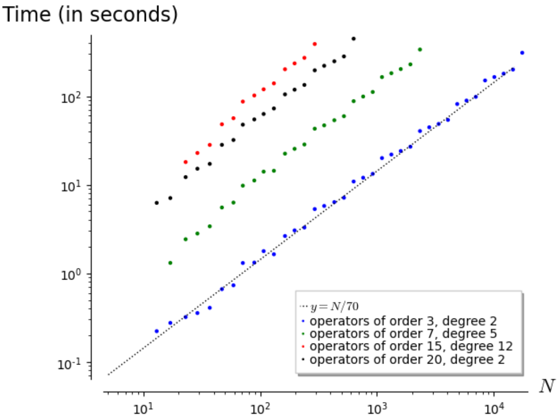
$$\tilde{O}(Nd((B+d)(r+d)^{\omega} + (r+d)^{\Omega}))$$

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.

My Contribution: Practical part

Implementation of the algorithm in Sagemath



Computation of p-curvatures

Goal: Computing all the characteristic polynomials of the p-curvatures of an operator in $\mathbb{Q}(z)\langle\partial\rangle$ for $p \leqslant N$.

Computation of p-curvatures

Goal: Computing all the characteristic polynomials of the p-curvatures of an operator in $\mathbb{Q}(z)\langle\partial\rangle$ for $p \leqslant N$.

Step 1: Reduce the computation of the p-curvature to that of a *matrix factorial* as in [Bostan, Caruso, Schost, ISSAC 2014].

$$M(\theta) \in \mathcal{M}_n(\mathbb{F}_p[\theta])$$

Computation of p-curvatures

Goal: Computing all the characteristic polynomials of the p-curvatures of an operator in $\mathbb{Q}(z)\langle\partial\rangle$ for $p \leqslant N$.

Step 1: Reduce the computation of the p-curvature to that of a *matrix factorial* as in [Bostan, Caruso, Schost, ISSAC 2014].

$$M(\theta) \in \mathcal{M}_n(\mathbb{F}_p[\theta]) \longrightarrow M(\theta)M(\theta+1)\cdots M(\theta+p-1)$$

Computation of p-curvatures

Goal: Computing all the characteristic polynomials of the p-curvatures of an operator in $\mathbb{Q}(z)\langle\partial\rangle$ for $p \leqslant N$.

Step 1: Reduce the computation of the p-curvature to that of a *matrix factorial* as in [Bostan, Caruso, Schost, ISSAC 2014].

$$M(\theta) \in \mathcal{M}_n(\mathbb{F}_p[\theta]) \longrightarrow M(\theta)M(\theta+1)\cdots M(\theta+p-1)$$

Step 2: Use the factorial computation method of [Costa, Gerbicz, Harvey, Math. Comp. 2014]

Step 1: Reduction to the computation of a matrix factorial

Idea: Rewrite operators of $\mathbb{F}_p[z]\langle\partial\rangle$ as operators in the variables ∂ and $\theta = z\partial$.

Step 1: Reduction to the computation of a matrix factorial

Idea: Rewrite operators of $\mathbb{F}_p[z]\langle\partial\rangle$ as operators in the variables ∂ and $\theta = z\partial$.

$$\partial\theta = \partial z\partial = (z\partial + 1)\partial = (\theta + 1)\partial$$

Step 1: Reduction to the computation of a matrix factorial

Idea: Rewrite operators of $\mathbb{F}_p[z]\langle\partial\rangle$ as operators in the variables ∂ and $\theta = z\partial$.

$$\partial\theta = \partial z\partial = (z\partial + 1)\partial = (\theta + 1)\partial$$

$$\partial^{-1}$$

Step 1: Reduction to the computation of a matrix factorial

Idea: Rewrite operators of $\mathbb{F}_p[z]\langle\partial\rangle$ as operators in the variables ∂ and $\theta = z\partial$.

$$\partial\theta = \partial z\partial = (z\partial + 1)\partial = (\theta + 1)\partial$$

$$\partial^{-1}$$

$$\Phi_p : \mathbb{F}_p[z]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle$$

Another p-curvature

Definition

Let $L_\theta \in \mathbb{F}_p(\theta)\langle\partial\rangle$. Its p-curvature $B_p(L_\theta)(\theta)$ is the $\mathbb{F}_p(\theta)$-linear endomorphism of ${}^{\mathbb{F}_p(\theta)\langle\partial\rangle}/_{\mathbb{F}_p(\theta)\langle\partial\rangle L_\theta}$ induced by the left multiplication by ∂^p.

Another p-curvature

Definition

Let $L_\theta \in \mathbb{F}_p(\theta)\langle\partial\rangle$. Its p-curvature $B_p(L_\theta)(\theta)$ is the $\mathbb{F}_p(\theta)$-linear endomorphism of ${}^{\mathbb{F}_p(\theta)\langle\partial\rangle}/_{\mathbb{F}_p(\theta)\langle\partial\rangle L_\theta}$ induced by the left multiplication by ∂^p.

If $B = B(L_\theta)(\theta)$ is its companion matrix then:

$$B_p(L_\theta) = B(\theta)B(\theta+1)\cdots B(\theta+p-1)$$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

Let $L_z \in \mathbb{F}_p(z)\langle\partial\rangle$ (resp. $L_\theta \in \mathbb{F}_p(\theta)\langle\partial\rangle$) with leading coefficient l_z (resp. l_θ).

$$\Xi_{z,\partial}(L_z) := l_z(z)^p \chi(A_p(L_z))(\partial^p)$$

$$\Xi_{\theta,\partial}(L_\theta) := \left(\prod_{i=0}^{p-1} l_\theta(\theta + i)\right) \chi(B_p(L_\theta))(\partial^p)$$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

Properties:

- $\Xi_{\cdot,\partial}$ sends an operator with polynomial coefficients to an operator with polynomial coefficients.

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

Properties:

- $\Xi_{\cdot,\partial}$ sends an operator with polynomial coefficients to an operator with polynomial coefficients.
- $\operatorname{Im}\left(\Xi_{z,\partial}\right) \subset \mathbb{F}_p(z^p)[\partial^p]$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

Properties:

- $\Xi_{\cdot,\partial}$ sends an operator with polynomial coefficients to an operator with polynomial coefficients.
- $\mathrm{Im}\left(\Xi_{z,\partial}\right) \subset \mathbb{F}_p(z^p)[\partial^p]$ and $\mathrm{Im}\left(\Xi_{\theta,\partial}\right) \subset \mathbb{F}_p(\theta^p - \theta)[\partial^p]$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

Properties:

- $\Xi_{\cdot,\partial}$ sends an operator with polynomial coefficients to an operator with polynomial coefficients.
- $\mathrm{Im}\,(\Xi_{z,\partial}) \subset \mathbb{F}_p(z^p)[\partial^p]$ and $\mathrm{Im}\,(\Xi_{\theta,\partial}) \subset \mathbb{F}_p(\theta^p - \theta)[\partial^p]$
- Multiplicativity: $\Xi_{\cdot,\partial} : \mathbb{F}_p(\cdot)\langle\partial^{\pm 1}\rangle \to \mathbb{F}_p(\cdot)\langle\partial^{\pm p}\rangle$.

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

Properties:

- $\Xi_{\cdot,\partial}$ sends an operator with polynomial coefficients to an operator with polynomial coefficients.
- $\mathrm{Im}\,(\Xi_{z,\partial}) \subset \mathbb{F}_p(z^p)[\partial^p]$ and $\mathrm{Im}\,(\Xi_{\theta,\partial}) \subset \mathbb{F}_p(\theta^p - \theta)[\partial^p]$
- Multiplicativity: $\Xi_{\cdot,\partial} : \mathbb{F}_p(\cdot)\langle\partial^{\pm 1}\rangle \to \mathbb{F}_p(\cdot)\langle\partial^{\pm p}\rangle$.

Theorem (Bostan, Caruso, Schost, ISSAC 2014)

The applications $\Xi_{\cdot,\partial}$ commute with the isomorphism Φ_p:

$$\begin{array}{ccc} k[x]\langle\partial^{\pm 1}\rangle & \xrightarrow[\sim]{\Phi_p} & k[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow{\scriptstyle \Xi_{x,\partial}} & & \downarrow{\scriptstyle \Xi_{\theta,\partial}} \\ k[x^p][\partial^{\pm p}] & \xrightarrow[\sim]{\Phi_p} & k[\theta^p - \theta][\partial^{\pm p}] \end{array}$$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

$$(z+1)^2\partial^3 - z\partial + z^3 + 3$$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

$$(z+1)^2\partial^3 - z\partial + z^3 + 3 \quad \mapsto \quad \partial^3 + 2\theta\partial^2 + (\theta^2-\theta)\partial - (\theta+3) + (\theta^3 - 3\theta^2 + 2\theta)\partial^{-3}$$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

$$(z+1)^2\partial^3 - z\partial + z^3 + 3 \quad \mapsto \quad \partial^3+2\theta\partial^2+(\theta^2-\theta)\partial-(\theta+3)+(\theta^3-3\theta^2+2\theta)\partial^{-3}$$

$$\begin{pmatrix} & & -\frac{z^3+3}{z^2+2z+1} \\ 1 & & \frac{z}{z^2+2z+1} \\ & 1 & 0 \end{pmatrix}$$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

$$(z+1)^2\partial^3 - z\partial + z^3 + 3 \quad \mapsto \quad \partial^3+2\theta\partial^2+(\theta^2-\theta)\partial-(\theta+3)+(\theta^3-3\theta^2+2\theta)\partial^{-3}$$

$$\begin{pmatrix} & & -\frac{z^3+3}{z^2+2z+1} \\ 1 & & \frac{z}{z^2+2z+1} \\ & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} & & & & & -(\theta^3-3\theta^2+2\theta) \\ 1 & & & & & 0 \\ & 1 & & & & 0 \\ & & 1 & & & (\theta+3) \\ & & & 1 & & -(\theta^2-\theta) \\ & & & & 1 & -2\theta \end{pmatrix}$$

Two crucial maps: $\Xi_{z,\partial}$ and $\Xi_{\theta,\partial}$

$$(z+1)^2\partial^3 - z\partial + z^3 + 3 \quad \mapsto \quad \partial^3+2\theta\partial^2+(\theta^2-\theta)\partial-(\theta+3)+(\theta^3-3\theta^2+2\theta)\partial^{-3}$$

$$\begin{pmatrix} & & -\frac{z^3+3}{z^2+2z+1} \\ 1 & & \frac{z}{z^2+2z+1} \\ & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} & & & & & -(\theta^3-3\theta^2+2\theta) \\ 1 & & & & & 0 \\ & 1 & & & & 0 \\ & & 1 & & & (\theta+3) \\ & & & 1 & & -(\theta^2-\theta) \\ & & & & 1 & -2\theta \end{pmatrix}$$

$$(z^{10}+2z^5+1)\partial^{15}+ (4z^5+2)\partial^5+z^{15}+2z^5$$

$$\partial^{15}+2(\theta^5-\theta)\partial^{10} +((\theta^5-\theta)^2+2)\partial^5+4(\theta^5-\theta) +2(\theta^5-\theta)\partial^{-5}+(\theta^5-\theta)^3\partial^{-15}$$

Extension to integral coefficients

$$\Phi : \mathbb{Z}[z]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle$$

Extension to integral coefficients

$$\Phi : \mathbb{Z}[z]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle$$

$$\begin{array}{ccc} \mathbb{Z}[z]\langle\partial^{\pm 1}\rangle & \xrightarrow{\text{mod } p} & \mathbb{F}_p[z]\langle\partial^{\pm 1}\rangle \\ \Phi \downarrow \wr & & \Phi_p \downarrow \wr \\ \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle & \xrightarrow{\text{mod } p} & \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \end{array}$$

Extension to integral coefficients

$$\Phi : \mathbb{Z}[z]\langle \partial^{\pm 1} \rangle \xrightarrow{\sim} \mathbb{Z}[\theta]\langle \partial^{\pm 1} \rangle$$

$$\begin{array}{ccc} \mathbb{Z}[z]\langle \partial^{\pm 1} \rangle & \xrightarrow{\text{mod } p} & \mathbb{F}_p[z]\langle \partial^{\pm 1} \rangle \\ \Phi \downarrow \wr & & \Phi_p \downarrow \wr \\ \mathbb{Z}[\theta]\langle \partial^{\pm 1} \rangle & \xrightarrow{\text{mod } p} & \mathbb{F}_p[\theta]\langle \partial^{\pm 1} \rangle \end{array}$$

$B(\theta)$ is the companion matrix of $\Phi(L)$.

$$B(\theta)B(\theta+1)\cdots B(\theta+p-1) \quad \text{mod } p \text{ for all } p < N.$$

A first simplification

If $L \in \mathbb{F}_p[z]\langle\partial\rangle$ has coefficients of degree at most d, then $\Xi_{\theta,\partial}(\Phi_p(L))$ has coefficients of degree at most d in $\theta^p - \theta$.

A first simplification

If $L \in \mathbb{F}_p[z]\langle\partial\rangle$ has coefficients of degree at most d, then $\Xi_{\theta,\partial}(\Phi_p(L))$ has coefficients of degree at most d in $\theta^p - \theta$.

Lemma

It is possible to determine entirely $P \in \mathbb{F}_p[\theta^p - \theta]$ of degree dp in θ from its first d coefficients.

A first simplification

If $L \in \mathbb{F}_p[z]\langle\partial\rangle$ has coefficients of degree at most d, then $\Xi_{\theta,\partial}(\Phi_p(L))$ has coefficients of degree at most d in $\theta^p - \theta$.

Lemma

It is possible to determine entirely $P \in \mathbb{F}_p[\theta^p - \theta]$ of degree dp in θ from its first d coefficients.

Conclusion: All computations can be done modulo θ^{d+1}.

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7$.

$$(3-1)!$$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7.$

$$(3-1)! \qquad (5-1)! \qquad (7-1)!$$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7$.

$(3-1)! \mod 3^s 5^s 7^s$ $\qquad (5-1)!$ $\qquad (7-1)!$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7.$

$$(3-1)! \mod 3^s 5^s 7^s \qquad (5-1)! \mod 5^s 7^s \qquad (7-1)! \mod 7^s$$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7.$

$$(3-1)! \mod 3^s 5^s 7^s \qquad (5-1)! \mod 5^s 7^s \qquad (7-1)! \mod 7^s$$

$$((3-1)! \mod 3^s 5^s 7^s)$$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7.$

$$(3-1)! \mod 3^s5^s7^s \qquad (5-1)! \mod 5^s7^s \qquad (7-1)! \mod 7^s$$

$$((3-1)! \mod 3^s5^s7^s) \times (3 \times 4)$$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7.$

$$(3-1)! \mod 3^s 5^s 7^s \qquad (5-1)! \mod 5^s 7^s \qquad (7-1)! \mod 7^s$$

$$((3-1)! \mod 3^s 5^s 7^s) \times (3 \times 4) \mod 5^s 7^s$$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7.$

$$(3-1)! \mod 3^s5^s7^s \qquad (5-1)! \mod 5^s7^s \qquad (7-1)! \mod 7^s$$

$$((3-1)! \mod 3^s5^s7^s) \times (3 \times 4) \mod 5^s7^s$$

$$((5-1)! \mod 5^s7^s)$$

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7$.

$(3-1)! \mod 3^s5^s7^s$ $\quad$ $(5-1)! \mod 5^s7^s$ $\quad$ $(7-1)! \mod 7^s$

$$((3-1)! \mod 3^s5^s7^s) \times (3 \times 4) \mod 5^s7^s$$

$$((5-1)! \mod 5^s7^s) \times (5 \times 6) \mod 7^s$$

Computation of $B(\theta) \cdots B(\theta + p - 1) \mod p$

$N = 7$.

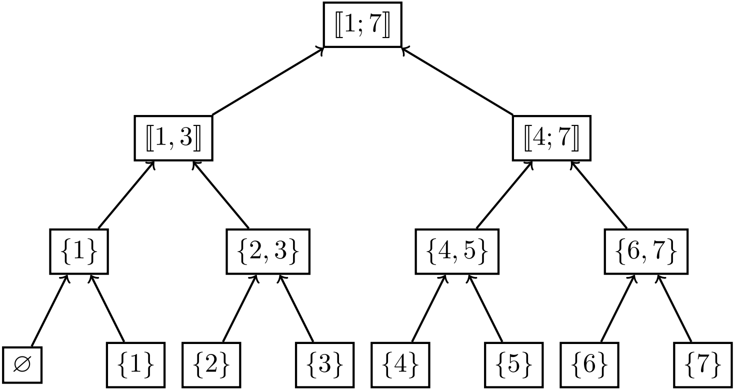
$$B(\theta)B(\theta+1)B(\theta+2) \quad B(\theta)\cdots B(\theta+4) \quad B(\theta)\cdots B(\theta+6)$$
$$\mod 3\times 5\times 7 \qquad\qquad \mod 5\times 7 \qquad\qquad \mod 7$$

$$(B(\theta)B(\theta+1)B(\theta+2) \mod 3\times 5\times 7) \times B(\theta+3)B(\theta+4) \mod 5\times 7$$

$$(B(\theta)\cdots B(\theta+4) \mod 5\times 7) \times B(\theta+5)B(\theta+6) \mod 7$$

Remainder tree.

Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]



Future works

- [Bostan, Caruso, Schost, 2016] brought the computation of invariant factors of the p-curvature to that of a *matrix factorial*

Future works

- [Bostan, Caruso, Schost, 2016] brought the computation of invariant factors of the p-curvature to that of a *matrix factorial* $\Rightarrow$ can a similar method be applied?

Future works

- [Bostan, Caruso, Schost, 2016] brought the computation of invariant factors of the p-curvature to that of a *matrix factorial* $\Rightarrow$ can a similar method be applied?
- Extension to operators with coefficients in a number field.

Future works

- [Bostan, Caruso, Schost, 2016] brought the computation of invariant factors of the p-curvature to that of a *matrix factorial* $\Rightarrow$ can a similar method be applied?
- Extension to operators with coefficients in a number field.

Thank you for your attention