Efficient linear computation of the characteristic polynomials of the p-curvatures of a differential operator with integer coefficients.

Seminar LFANT

Raphaël Pagès[1] [2]

[1]IMB

[2]INRIA - Saclay

November 23, 2020

Motivating the p-curvature

Let $A \in M_n(\mathbb{Q}(z))$.

Motivating the p-curvature

Let $A \in M_n(\mathbb{Q}(z))$.

$$Y' = AY$$

Motivating the p-curvature

Let $A \in M_n(\mathbb{Q}(z))$.

$$Y' = AY$$

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

Motivating the p-curvature

Let $A \in M_n(\mathbb{Q}(z))$.

$$Y' = AY$$

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

Are the solutions of this system algebraic ?

Motivating the p-curvature

Let $A \in M_n(\mathbb{Q}(z))$.

$$Y' = AY$$

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

Are the solutions of this system algebraic ?

Lemma

If this system admits an algebraic basis of solutions then its reduction modulo p has an algebraic basis of solutions for almost all p prime.

Motivating the p-curvature

Let $A \in M_n(\mathbb{Q}(z))$.

$$Y' = AY$$

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

Are the solutions of this system algebraic ?

Lemma

If this system admits an algebraic basis of solutions then its reduction modulo p has an algebraic basis of solutions for almost all p prime.

Grothendieck-Katz conjecture : This implication is in fact an equivalence.

Motivating the p-curvature

Theorem

Let k be a finite field of characteristic and $A \in M_n(k(z))$. Seeking solutions to the problem $Y' = AY$ we have an equality between

Motivating the p-curvature

Theorem

Let k be a finite field of characteristic and $A \in M_n(k(z))$. *Seeking solutions to the problem* $Y' = AY$ *we have an equality between*

- *The dimension of the space of solutions that are algebraic over* $k(z)$.

Motivating the p-curvature

Theorem

Let k be a finite field of characteristic and $A \in M_n(k(z))$. Seeking solutions to the problem $Y' = AY$ we have an equality between

- *The dimension of the space of solutions that are algebraic over $k(z)$.*
- *The dimension of the space of solutions in $k((z))$.*

Motivating the p-curvature

Theorem

Let k be a finite field of characteristic and $A \in M_n(k(z))$. Seeking solutions to the problem $Y' = AY$ we have an equality between

- *The dimension of the space of solutions that are algebraic over $k(z)$.*
- *The dimension of the space of solutions in $k((z))$.*
- *The dimension of the space of solutions in $k(z)$.*

Motivating the p-curvature

Theorem

Let k be a finite field of characteristic and $A \in M_n(k(z))$. Seeking solutions to the problem $Y' = AY$ we have an equality between

- *The dimension of the space of solutions that are algebraic over $k(z)$.*
- *The dimension of the space of solutions in $k((z))$.*
- *The dimension of the space of solutions in $k(z)$.*
- *The dimension of the kernel of the p-curvature of this system.*

Motivating the p-curvature

k is a finite field of characteristic p.

Motivating the p-curvature

k is a finite field of characteristic p.
$M = k(z)^n$ can be equipped with the connexion $\partial_A : Y \mapsto Y' - AY$.

Motivating the p-curvature

k is a finite field of characteristic p.
$M = k(z)^n$ can be equipped with the connexion $\partial_A : Y \mapsto Y' - AY$.

$$\partial(f(z) \cdot m) = f(z)\partial \cdot m + f'(z) \cdot m$$

Lemma

For all differential $k(x)$-module M,

Motivating the p-curvature

k is a finite field of characteristic p.
$M = k(z)^n$ can be equipped with the connexion $\partial_A : Y \mapsto Y' - AY$.

$$\partial(f(z) \cdot m) = f(z)\partial \cdot m + f'(z) \cdot m$$

Lemma

For all differential $k(x)$-module M,
$m \mapsto \partial \cdot m$ is $k(x^p)$-linear.

Motivating the p-curvature

k is a finite field of characteristic p.
$M = k(z)^n$ can be equipped with the connexion $\partial_A : Y \mapsto Y' - AY$.

$$\partial(f(z) \cdot m) = f(z)\partial \cdot m + f'(z) \cdot m$$

Lemma

For all differential $k(x)$-module M,
$m \mapsto \partial \cdot m$ is $k(x^p)$-linear.
$m \mapsto \partial^p \cdot m$ is $k(x)$-linear.

Motivating the p-curvature

k is a finite field of characteristic p.
$M = k(z)^n$ can be equipped with the connexion $\partial_A : Y \mapsto Y' - AY$.

$$\partial(f(z) \cdot m) = f(z)\partial \cdot m + f'(z) \cdot m$$

Lemma

For all differential $k(x)$-module M,
$m \mapsto \partial \cdot m$ is $k(x^p)$-linear.
$m \mapsto \partial^p \cdot m$ is $k(x)$-linear.

When the connexion on M is of the form ∂_A then

$$A_0 = I_n \qquad A_{k+1} = A_k' - AA_k \qquad A_p$$

Motivating the p-curvature

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

Motivating the p-curvature

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

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

Motivating the p-curvature

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

$$A = \begin{pmatrix} 0 & 0 & -\frac{z^3+3}{(z+1)^2} \\ 1 & 0 & -\frac{z}{(z+1)^2} \\ 0 & 1 & 0 \end{pmatrix} \text{ and } A_p = \begin{pmatrix} \frac{2z^3}{(z+1)^2} & \frac{z}{(z+1)^2} & 0 \\ \frac{2z^3}{z^3+1} & \frac{2z^4+2z^3+2z+1}{z^3+1} & \frac{z}{(z+1)^2} \\ \frac{2z^4}{z^4+z^3+z+1} & \frac{z^4+z^3+z^2+2z+2}{z^4+z^3+z+1} & \frac{2z^4+2z^3+z+2}{z^3+1} \end{pmatrix}$$

Motivating the p-curvature

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

$$A = \begin{pmatrix} 0 & 0 & -\frac{z^3+3}{(z+1)^2} \\ 1 & 0 & -\frac{z}{(z+1)^2} \\ 0 & 1 & 0 \end{pmatrix} \text{ and } A_p = \begin{pmatrix} \frac{2z^3}{(z+1)^2} & \frac{z}{(z+1)^2} & 0 \\ \frac{2z^3}{z^3+1} & \frac{2z^4+2z^3+2z+1}{z^3+1} & \frac{z}{(z+1)^2} \\ \frac{2z^4}{z^4+z^3+z+1} & \frac{z^4+z^3+z^2+2z+2}{z^4+z^3+z+1} & \frac{2z^4+2z^3+z+2}{z^3+1} \end{pmatrix}$$

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

Differential operators algebra

Definition

Let $\mathcal{A} = k[x]$ or $k(x)$ with k a field. We define $\mathcal{A}\langle\partial\rangle$.

Differential operators algebra

Definition

Let $\mathcal{A} = k[x]$ or $k(x)$ with k a field. We define $\mathcal{A}\langle\partial\rangle$.

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

Differential operators algebra

Definition

Let $\mathcal{A} = k[x]$ or $k(x)$ with k a field. We define $\mathcal{A}\langle\partial\rangle$.

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

Example

$\mathcal{A} = \mathbb{Q}[x]$

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

Differential operators algebra

Definition

Let $\mathcal{A} = k[x]$ or $k(x)$ with k a field. We define $\mathcal{A}\langle\partial\rangle$.

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

Example

$\mathcal{A} = \mathbb{Q}[x]$

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

$$\partial x = x\partial + 1$$

summary

$$M = {}^{k(x)\langle\partial\rangle}\big/_{k(x)\langle\partial\rangle L}$$

summary

$$M = {}^{k(x)\langle\partial\rangle}\big/_{k(x)\langle\partial\rangle L}$$

L is of size $O(1)$.

summary

$$M = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle L}$$

L is of size $O(1)$.

$A_p(L)$:

- size : $O(p)$.

$\chi(A_p(L))$:

summary

$$M = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle L}$$

L is of size $O(1)$.

$A_p(L)$:

- size : $O(p)$.
- naive computation : $\tilde{O}(p^2)$ arithmetic operations.

$\chi(A_p(L))$:

summary

$$M = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle L}$$

L is of size $O(1)$.

$A_p(L)$:

- size : $O(p)$.
- naive computation : $\tilde{O}(p^2)$ arithmetic operations.
- Best known algorithm : $\tilde{O}(p)$ arithmetic operations [Bostan, Caruso, Schost, 2015].

$\chi(A_p(L))$:

summary

$$M = {}^{k(x)\langle \partial \rangle}/_{k(x)\langle \partial \rangle L}$$

L is of size $O(1)$.

$A_p(L)$:

- size : $O(p)$.
- naive computation : $\tilde{O}(p^2)$ arithmetic operations.
- Best known algorithm : $\tilde{O}(p)$ arithmetic operations [Bostan, Caruso, Schost, 2015].

$\chi(A_p(L))$:

- size : $O(1)$.

summary

$$M = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle L}$$

L is of size $O(1)$.

$A_p(L)$:

- size : $O(p)$.
- naive computation : $\tilde{O}(p^2)$ arithmetic operations.
- Best known algorithm : $\tilde{O}(p)$ arithmetic operations [Bostan, Caruso, Schost, 2015].

$\chi(A_p(L))$:

- size : $O(1)$.
- Best known algorithm : $\tilde{O}(\sqrt{p})$ binary operations [Bostan, Caruso, Schost, 2014].

summary

$$M = {}^{k(x)\langle\partial\rangle}/_{k(x)\langle\partial\rangle L}$$

L is of size $O(1)$.

$A_p(L)$:

- size : $O(p)$.
- naive computation : $\tilde{O}(p^2)$ arithmetic operations.
- Best known algorithm : $\tilde{O}(p)$ arithmetic operations [Bostan, Caruso, Schost, 2015].

$\chi(A_p(L))$:

- size : $O(1)$.
- Best known algorithm : $\tilde{O}(\sqrt{p})$ binary operations [Bostan, Caruso, Schost, 2014].
- Contribution : $L \in \mathbb{Z}(x)\langle\partial\rangle$. Computation of all the characteristic polynomials of its p-curvatures for $p \leqslant N$ in $\tilde{O}(N)$ binary operations.

Summary

$(p-1)!$:

- size : $\tilde{O}(p)$.

$(p-1)! \mod p^s$:

Summary

$(p-1)!$:

- size : $\tilde{O}(p)$.
- naive computation : $\tilde{O}(p^2)$ binary operations.

$(p-1)! \mod p^s$:

Summary

$(p-1)!$:

- size : $\tilde{O}(p)$.
- naive computation : $\tilde{O}(p^2)$ binary operations.
- Best known algorithm : $\tilde{O}(p)$ binary operations [Chudnovsky, Chudnovsky, 1988].

$(p-1)! \mod p^s$:

Summary

$(p-1)!$:

- size : $\tilde{O}(p)$.
- naive computation : $\tilde{O}(p^2)$ binary operations.
- Best known algorithm : $\tilde{O}(p)$ binary operations [Chudnovsky, Chudnovsky, 1988].

$(p-1)! \mod p^s$:

- size : $O(s\log(p))$.

Summary

$(p-1)!$:

- size : $\tilde{O}(p)$.
- naive computation : $\tilde{O}(p^2)$ binary operations.
- Best known algorithm : $\tilde{O}(p)$ binary operations [Chudnovsky, Chudnovsky, 1988].

$(p-1)! \mod p^s$:

- size : $O(s\log(p))$.
- Best known algorithm : $\tilde{O}(s\sqrt{p})$ binary operations [Strassen, 1977] .

Summary

$(p-1)!$:

- size : $\tilde{O}(p)$.
- naive computation : $\tilde{O}(p^2)$ binary operations.
- Best known algorithm : $\tilde{O}(p)$ binary operations [Chudnovsky, Chudnovsky, 1988].

$(p-1)! \mod p^s$:

- size : $O(s\log(p))$.
- Best known algorithm : $\tilde{O}(s\sqrt{p})$ binary operations [Strassen, 1977] .
- Computation of $(p-1)! \mod p^s$ for all $p \leqslant N$: $\tilde{O}(sN)$ binary operations [Costa, Gerbicz, Harvey, 2014].

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad x(x\partial) = (x\partial - 1)x$$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.
Problem : How to rewrite x ?

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.
Problem : How to rewrite x ?
Solution : ∂^{-1}

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.
Problem : How to rewrite x ?
Solution : $\partial^{-1}f(x) = \sum_{i=0}^{p-1}(-1)^i f^{(i)}(x)\partial^{-i-1}$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.
Problem : How to rewrite x ?
Solution : $\partial^{-1}f(x) = \sum_{i=0}^{p-1}(-1)^i f^{(i)}(x)\partial^{-i-1}$
$\partial^i f(\theta) = f(\theta + i)\partial^i$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.
Problem : How to rewrite x ?
Solution : $\partial^{-1}f(x) = \sum_{i=0}^{p-1}(-1)^i f^{(i)}(x)\partial^{-i-1}$
$\partial^i f(\theta) = f(\theta + i)\partial^i$

$$k(x)\langle\partial^{\pm 1}\rangle \qquad k(\theta)\langle\partial^{\pm 1}\rangle$$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad\qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.
Problem : How to rewrite x ?
Solution : $\partial^{-1}f(x) = \sum_{i=0}^{p-1}(-1)^i f^{(i)}(x)\partial^{-i-1}$
$\partial^i f(\theta) = f(\theta + i)\partial^i$

$$k(x)\langle\partial^{\pm 1}\rangle \qquad\qquad k(\theta)\langle\partial^{\pm 1}\rangle$$

$$\begin{array}{ccc} k[x]\langle\partial\rangle & \hookrightarrow & k[x]\langle\partial^{\pm 1}\rangle \\ \downarrow & & \downarrow \\ k(x)\langle\partial\rangle & \hookrightarrow & k(x)\langle\partial^{\pm 1}\rangle \end{array}$$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\theta = x\partial$$

$$\partial(x\partial) = (x\partial + 1)\partial \qquad\qquad x(x\partial) = (x\partial - 1)x$$

Idea : rewrite as elements of $k[\theta]\langle\partial\rangle$.
Problem : How to rewrite x ?
Solution : $\partial^{-1}f(x) = \sum_{i=0}^{p-1}(-1)^i f^{(i)}(x)\partial^{-i-1}$
$\partial^i f(\theta) = f(\theta + i)\partial^i$

$$\begin{array}{ccc} & k(x)\langle\partial^{\pm 1}\rangle & \\ k[x]\langle\partial\rangle & \hookrightarrow & k[x]\langle\partial^{\pm 1}\rangle \\ \downarrow & & \downarrow \\ k(x)\langle\partial\rangle & \hookrightarrow & k(x)\langle\partial^{\pm 1}\rangle \end{array} \qquad \begin{array}{ccc} & k(\theta)\langle\partial^{\pm 1}\rangle & \\ k[\theta]\langle\partial\rangle & \hookrightarrow & k[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow & & \downarrow \\ k(\theta)\langle\partial\rangle & \hookrightarrow & k(\theta)\langle\partial^{\pm 1}\rangle \end{array}$$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\begin{array}{rcl} k[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\sim} & k[\theta]\langle\partial^{\pm 1}\rangle \\ x & \mapsto & \theta\partial^{-1} \\ x\partial & \leftarrow\!\shortmid & \theta \\ \partial & \leftrightarrow & \partial \end{array}$$

$k(\theta)\langle\partial^{\pm 1}\rangle$ et $k(x)\langle\partial^{\pm 1}\rangle$

$$\begin{array}{rcl} k[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\sim} & k[\theta]\langle\partial^{\pm 1}\rangle \\ x & \mapsto & \theta\partial^{-1} \\ x\partial & \leftarrow\!\shortmid & \theta \\ \partial & \leftrightarrow & \partial \end{array}$$

Example

$(x+1)\partial$ invertible in $k(x)\langle\partial^{\pm 1}\rangle$
$\partial + \theta$ non invertible in $k(\theta)\langle\partial^{\pm 1}\rangle$

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

Let $L' = l_m{}'(\theta)\partial^m + \ldots + l_1{}'(\theta)\partial + l_0{}'(\theta)$.

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

Let $L' = l_m{}'(\theta)\partial^m + \ldots + l_1{}'(\theta)\partial + l_0{}'(\theta)$.

$$B(L') = \begin{pmatrix} & & & -\frac{l_0{}'}{l_m{}'} \\ 1 & & & -\frac{l_1{}'}{l_m{}'} \\ & \ddots & & \vdots \\ & & 1 & -\frac{l_{m-1}{}'}{l_m{}'} \end{pmatrix}$$

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

Let $L' = l_m{}'(\theta)\partial^m + \ldots + l_1{}'(\theta)\partial + l_0{}'(\theta)$.

$$B(L') = \begin{pmatrix} & & & -\frac{l_0{}'}{l_m{}'} \\ 1 & & & -\frac{l_1{}'}{l_m{}'} \\ & \ddots & & \vdots \\ & & 1 & -\frac{l_{m-1}{}'}{l_m{}'} \end{pmatrix}$$

$$B_p(L') = \mathrm{Mat}(\partial^p \cdot) = B(L')(\theta) B(L')(\theta+1) \ldots B(L')(\theta+p-1)$$

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

Let $L' = l_m{}'(\theta)\partial^m + \ldots + l_1{}'(\theta)\partial + l_0{}'(\theta)$.

$$B(L') = \begin{pmatrix} & & & -\frac{l_0{}'}{l_m{}'} \\ 1 & & & -\frac{l_1{}'}{l_m{}'} \\ & \ddots & & \vdots \\ & & 1 & -\frac{l_{m-1}{}'}{l_m{}'} \end{pmatrix}$$

$$B_p(L') = \mathrm{Mat}(\partial^p \cdot) = B(L')(\theta)B(L')(\theta+1)\ldots B(L')(\theta+p-1)$$

Let $L = l_m(x)\partial^m + \ldots + l_1(x)\partial + l_0(x)$.

$$\Xi_{x,\partial}(L) = l_m(x)^p \chi(A_p(L))(\partial^p)$$

$$\Xi_{\theta,\partial}(L') = \left(\prod_{i=0}^{p-1} l_m{}'(\theta+i)\right) \chi(B_p(L'))(\partial^p)$$

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

$$\begin{array}{ccc} k[x]\langle\partial\rangle & \xrightarrow{\Xi_{x,\partial}} & k[x^p][\partial^p] \\ \downarrow & & \downarrow \\ k(x)\langle\partial\rangle & \xrightarrow{\Xi_{x,\partial}} & k(x^p)[\partial^p] \end{array} \qquad \begin{array}{ccc} k[\theta]\langle\partial\rangle & \xrightarrow{\Xi_{\theta,\partial}} & k[\theta^p-\theta][\partial^p] \\ \downarrow & & \downarrow \\ k(\theta)\langle\partial\rangle & \xrightarrow{\Xi_{\theta,\partial}} & k(\theta^p-\theta)[\partial^p] \end{array}$$

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

$$\begin{array}{ccc} k[x]\langle\partial\rangle & \xrightarrow{\Xi_{x,\partial}} & k[x^p][\partial^p] \\ \downarrow & & \downarrow \\ k(x)\langle\partial\rangle & \xrightarrow{\Xi_{x,\partial}} & k(x^p)[\partial^p] \end{array} \qquad \begin{array}{ccc} k[\theta]\langle\partial\rangle & \xrightarrow{\Xi_{\theta,\partial}} & k[\theta^p-\theta][\partial^p] \\ \downarrow & & \downarrow \\ k(\theta)\langle\partial\rangle & \xrightarrow{\Xi_{\theta,\partial}} & k(\theta^p-\theta)[\partial^p] \end{array}$$

Lemma

- *Send an irreducible element over a power of an irreductible element of the center*

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

$$\begin{array}{ccc} k[x]\langle\partial\rangle & \xrightarrow{\Xi_{x,\partial}} & k[x^p][\partial^p] \\ \big\downarrow & & \big\downarrow \\ k(x)\langle\partial\rangle & \xrightarrow{\Xi_{x,\partial}} & k(x^p)[\partial^p] \end{array} \qquad \begin{array}{ccc} k[\theta]\langle\partial\rangle & \xrightarrow{\Xi_{\theta,\partial}} & k[\theta^p-\theta][\partial^p] \\ \big\downarrow & & \big\downarrow \\ k(\theta)\langle\partial\rangle & \xrightarrow{\Xi_{\theta,\partial}} & k(\theta^p-\theta)[\partial^p] \end{array}$$

Lemma

- *Send an irreducible element over a power of an irreductible element of the center*
- *Multiplicative.*

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

Theorem

The followin diagram commutes.

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

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

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

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

$$(x^2+2x+1)\partial^3 - x\partial + x^3 + 3 \quad \mapsto \quad \begin{pmatrix} \partial^6+2\theta\partial^5+(\theta^2-\theta)\partial^4 \\ -(\theta+3)\partial^3+(\theta^3-3\theta^2+2\theta) \end{pmatrix} \partial^{-3}$$

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

$$(x^2+2x+1)\partial^3 - x\partial + x^3 + 3 \quad \mapsto \quad \begin{pmatrix} \partial^6+2\theta\partial^5+(\theta^2-\theta)\partial^4 \\ -(\theta+3)\partial^3+(\theta^3-3\theta^2+2\theta) \end{pmatrix} \partial^{-3}$$

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

$\Xi_{x,\partial}$ and $\Xi_{\theta,\partial}$

$$(x^2+2x+1)\partial^3 - x\partial + x^3 + 3 \quad \mapsto \quad \begin{pmatrix} \partial^6+2\theta\partial^5+(\theta^2-\theta)\partial^4 \\ -(\theta+3)\partial^3+(\theta^3-3\theta^2+2\theta) \end{pmatrix} \partial^{-3}$$

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

proof of the commutativity

- Step 1 : Isomorphism with a matrix algebra after scalar extension.

$$\begin{array}{ccc} k[\theta]\langle\partial^{\pm 1}\rangle[T] & \xrightarrow[\sim]{\mathcal{M}_\theta} & M_p(k[\theta^p - \theta][\partial^{\pm p}][T]) \\ \downarrow \wr & & \downarrow \wr \\ k[x]\langle\partial^{\pm 1}\rangle[T] & \xrightarrow[\sim]{\mathcal{M}_x} & M_p(k[x^p][\partial^{\pm p}][T]) \end{array}$$

proof of the commutativity

- Step 1 : Isomorphism with a matrix algebra after scalar extension.

$$\begin{array}{ccc} k[\theta]\langle\partial^{\pm 1}\rangle[T] & \xrightarrow[\sim]{\mathcal{M}_\theta} & M_p(k[\theta^p - \theta][\partial^{\pm p}][T]) \\ \downarrow \wr & & \downarrow \wr \\ k[x]\langle\partial^{\pm 1}\rangle[T] & \xrightarrow[\sim]{\mathcal{M}_x} & M_p(k[x^p][\partial^{\pm p}][T]) \end{array}$$

- Step 2 : The determinant : restriction, corestriction

proof of the commutativity

- Step 1 : Isomorphism with a matrix algebra after scalar extension.

$$\begin{array}{ccc} k[\theta]\langle\partial^{\pm 1}\rangle[T] & \xrightarrow[\sim]{\mathcal{M}_\theta} & M_p(k[\theta^p-\theta][\partial^{\pm p}][T]) \\ \downarrow \wr & & \downarrow \wr \\ k[x]\langle\partial^{\pm 1}\rangle[T] & \xrightarrow[\sim]{\mathcal{M}_x} & M_p(k[x^p][\partial^{\pm p}][T]) \end{array}$$

- Step 2 : The determinant : restriction, corestriction
- Step 3 : Equility of $\Xi_{\theta,\partial}$ (resp. $\Xi_{x,\partial}$) with the determinant.

Step 1 : Isomorphism with a matrix algebra

$$T^p - T = \theta^p - \theta \text{ or } T^p - T = x^p \partial^p$$

Step 1 : Isomorphism with a matrix algebra

$$T^p - T = \theta^p - \theta \text{ or } T^p - T = x^p \partial^p$$

$$k[x]\langle \partial^{\pm 1} \rangle [T] = k[x]\langle \partial^{\pm 1} \rangle \otimes_{k[x^p][\partial^{\pm p}]} k[x^p][\partial^{\pm p}][T]$$

Step 1 : Isomorphism with a matrix algebra

$$T^p - T = \theta^p - \theta \text{ or } T^p - T = x^p \partial^p$$

$$k[x]\langle\partial^{\pm 1}\rangle[T] = k[x]\langle\partial^{\pm 1}\rangle \otimes_{k[x^p][\partial^{\pm p}]} k[x^p][\partial^{\pm p}][T]$$

$$\mathcal{M}_\theta(\theta) = \begin{pmatrix} T & & & \\ & T+1 & & \\ & & \ddots & \\ & & & T+p-1 \end{pmatrix} \text{ and } \mathcal{M}_\theta(\partial) = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \partial^p & & & \end{pmatrix}$$

Step 2 : The determinant, restriction, corestriction

$$\mathcal{D}_{\cdot} = k[\cdot]\langle\partial^{\pm 1}\rangle$$
$$\mathcal{Z}_{\cdot} = \text{le centre associé}$$

Step 2 : The determinant, restriction, corestriction

$$\begin{aligned} \mathcal{D}. &= k[\cdot]\langle \partial^{\pm 1} \rangle \\ \mathcal{Z}. &= \text{le centre associé} \end{aligned}$$

$$\begin{array}{ccccc}
 & & \overset{\mathcal{N}_x}{\frown} & & \\
\mathcal{D}_x[T] & \xrightarrow{\mathcal{M}_x} & M_p(\mathcal{Z}_x[T]) & \xrightarrow{\det} & \mathcal{Z}_x[T] \\
\downarrow \wr & & \downarrow \wr & & \downarrow \wr \\
\mathcal{D}_\theta[T] & \xrightarrow{\mathcal{M}_\theta} & M_p(\mathcal{Z}_\theta[T]) & \xrightarrow{\det} & \mathcal{Z}_\theta[T] \\
 & & \underset{\mathcal{N}_\theta}{\smile} & &
\end{array}$$

Step 2 : The determinant, restriction, corestriction

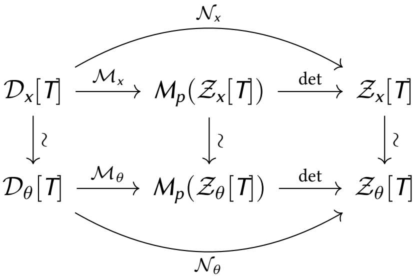
$$\begin{aligned} \mathcal{D}_. &= k[\cdot]\langle\partial^{\pm 1}\rangle \\ \mathcal{Z}_. &= \text{le centre associé} \end{aligned}$$

$$\begin{array}{ccccc} & & \mathcal{N}_x & & \\ \mathcal{D}_x[T] & \xrightarrow{\mathcal{M}_x} & M_p(\mathcal{Z}_x[T]) & \xrightarrow{\det} & \mathcal{Z}_x[T] \\ \downarrow\wr & & \downarrow\wr & & \downarrow\wr \\ \mathcal{D}_\theta[T] & \xrightarrow{\mathcal{M}_\theta} & M_p(\mathcal{Z}_\theta[T]) & \xrightarrow{\det} & \mathcal{Z}_\theta[T] \\ & & \mathcal{N}_\theta & & \end{array}$$

$$\mathcal{N}_.(\mathcal{D}_.) \subset \mathcal{Z}_.$$

Step 2 : The determinant, restriction, corestriction

$$\begin{aligned} \mathcal{D}_\cdot &= k[\cdot]\langle \partial^{\pm 1} \rangle \\ \mathcal{Z}_\cdot &= \text{le centre associé} \end{aligned}$$



$\mathcal{N}_\cdot(\mathcal{D}_\cdot) \subset \mathcal{Z}_\cdot$ Invariance by $T \mapsto T + a$

Step 3 : Equality with the determinant

Lemma

- $\mathcal{N}_{\cdot}(L)$ *and* $\Xi_{\cdot,\partial}(L)$ *have the same leading coefficient.*

Step 3 : Equality with the determinant

Lemma

- *$\mathcal{N}_\cdot(L)$ and $\Xi_{\cdot,\partial}(L)$ have the same leading coefficient.*
- *$\mathcal{N}_\cdot$ is multiplicative.*

Step 3 : Equality with the determinant

Lemma

- $\mathcal{N}_\cdot(L)$ *and* $\Xi_{\cdot,\partial}(L)$ *have the same leading coefficient.*
- $\mathcal{N}_\cdot$ *is multiplicative.*
- $\mathcal{N}_\cdot(L \in \mathcal{Z}_\cdot) = L^p$

Step 3 : Equality with the determinant

Lemma

- $\mathcal{N}_{\cdot}(L)$ *and* $\Xi_{\cdot,\partial}(L)$ *have the same leading coefficient.*
- $\mathcal{N}_{\cdot}$ *is multiplicative.*
- $\mathcal{N}_{\cdot}(L \in \mathcal{Z}_{\cdot}) = L^p$

Step 3 : Equality with the determinant

Lemma

- *$\mathcal{N}_{\cdot}(L)$ and $\Xi_{\cdot,\partial}(L)$ have the same leading coefficient.*
- *$\mathcal{N}_{\cdot}$ is multiplicative.*
- $\mathcal{N}_{\cdot}(L \in \mathcal{Z}_{\cdot}) = L^p$

$$
\begin{array}{ccccc}
 & & \overset{\Xi_{x,\partial}}{\frown} & & \\
k[x]\langle\partial^{\pm1}\rangle & \xrightarrow{\mathcal{M}_x} & M_p(k[x^p][\partial^{\pm p}][T]) & \xrightarrow{\det} & k[x^p][\partial^{\pm p}][T] \\
\downarrow\wr & & \downarrow\wr & & \downarrow\wr \\
k[\theta]\langle\partial^{\pm1}\rangle & \xrightarrow{\mathcal{M}_\theta} & M_p(k[\theta^p][\partial^{\pm p}][T]) & \xrightarrow{\det} & k[\theta^p][\partial^{\pm p}][T] \\
 & & \underset{\Xi_{\theta,\partial}}{\smile} & &
\end{array}
$$

The algorithm's skeleton

$L \in \mathbb{Z}[x]\langle\partial\rangle$

The algorithm's skeleton

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle$$

The algorithm's skeleton

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

The algorithm's skeleton

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L)$ for all $p \leqslant N$.

$$\begin{array}{l} \mathbb{Z}[x]\langle\partial\rangle \\ \downarrow \pi_p \\ \mathbb{F}_p[x]\langle\partial\rangle \xrightarrow{\Phi_p} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \xrightarrow{B_p} \coprod_{n\in\mathbb{N}} M_n(\mathbb{F}_p(\theta)) \end{array}$$

The algorithm's skeleton

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L)$ for all $p \leqslant N$.

$$\begin{array}{ccccc} \mathbb{Z}[x]\langle\partial\rangle & & & & \\ \downarrow \pi_p & & & & \\ \mathbb{F}_p[x]\langle\partial\rangle & \xrightarrow{\Phi_p} & \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle & \xrightarrow{B_p} & \coprod_{n\in\mathbb{N}} M_n(\mathbb{F}_p(\theta)) \end{array}$$

- Step 2 : Compute their characteristic polynomials
  degree : $O(p)$

The algorithm's skeleton

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L)$ for all $p \leqslant N$.

$$\begin{array}{ccccc} \mathbb{Z}[x]\langle\partial\rangle & & & & \\ \big\downarrow{\scriptstyle \pi_p} & & & & \\ \mathbb{F}_p[x]\langle\partial\rangle & \xrightarrow{\Phi_p} & \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle & \xrightarrow{B_p} & \coprod_{n\in\mathbb{N}} M_n(\mathbb{F}_p(\theta)) \end{array}$$

- Step 2 : Compute their characteristic polynomials degree : $O(p)$
- Step 3 : Compute their reciproqual image by Φ_p.

The algorithm's skeleton

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L)$ for all $p \leqslant N$.

$$\begin{array}{l} \mathbb{Z}[x]\langle\partial\rangle \\ \downarrow \pi_p \\ \mathbb{F}_p[x]\langle\partial\rangle \xrightarrow{\Phi_p} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \xrightarrow{B_p} \coprod_{n\in\mathbb{N}} M_n(\mathbb{F}_p(\theta)) \end{array}$$

- Step 2 : Compute their characteristic polynomials
  degree : $O(p)$
- Step 3 : Compute their reciproqual image by Φ_p.

The algorithm's skeleton

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L)$ for all $p \leqslant N$.

$$\begin{array}{l} \mathbb{Z}[x]\langle\partial\rangle \\ \downarrow \pi_p \\ \mathbb{F}_p[x]\langle\partial\rangle \xrightarrow{\Phi_p} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \xrightarrow{B_p} \coprod_{n\in\mathbb{N}} M_n(\mathbb{F}_p(\theta)) \end{array}$$

- Step 2 : Compute their characteristic polynomials
  degree : $O(p)$
- Step 3 : Compute their reciproqual image by Φ_p.

Size of the output at the end of step 2 : $O(N^2)$

Step 3 : computing modulo θ^d

Coefficients of L of degree d in x.

Step 3 : computing modulo θ^d

Coefficients of L of degree d in x.
List of $P \in k[\theta^p - \theta]$.

Step 3 : computing modulo θ^d

Coefficients of L of degree d in x.
List of $P \in k[\theta^p - \theta]$.
$\deg(P_i) \leqslant dp$.

Step 3 : computing modulo θ^d

Coefficients of L of degree d in x.
List of $P \in k[\theta^p - \theta]$.
$\deg(P_i) \leqslant dp$.

$$P = p_d(\theta^p - \theta)^d + \ldots + p_1(\theta^p - \theta) + p_0$$

Step 3 : computing modulo θ^d

Coefficients of L of degree d in x.
List of $P \in k[\theta^p - \theta]$.
$\deg(P_i) \leqslant dp$.

$$P = p_d(\theta^p - \theta)^d + \ldots + p_1(\theta^p - \theta) + p_0$$
$$P = p'_{dp}\theta^{dp} + \ldots + p'_1\theta + p_0$$

Step 3 : computing modulo θ^d

Coefficients of L of degree d in x.
List of $P \in k[\theta^p - \theta]$.
$\deg(P_i) \leqslant dp$.

$$P = p_d(\theta^p - \theta)^d + \ldots + p_1(\theta^p - \theta) + p_0$$
$$P = p'_{dp}\theta^{dp} + \ldots + p'_1\theta + p_0$$

$$\theta^p - \theta \mapsto x^p \partial^p$$

Step 3 : computing modulo θ^d

Coefficients of L of degree d in x.
List of $P \in k[\theta^p - \theta]$.
$\deg(P_i) \leqslant dp$.

$$P = p_d(\theta^p - \theta)^d + \ldots + p_1(\theta^p - \theta) + p_0$$
$$P = p'_{dp}\theta^{dp} + \ldots + p'_1\theta + p_0$$

$$\theta^p - \theta \mapsto x^p \partial^p$$

Lemma

$\forall i \leqslant p - 1$

$$p_i = (-1)^i p'_i$$

Structure of the algorithm

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L) \mod \theta^d$ for all $p \leqslant N$.

Structure of the algorithm

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L) \mod \theta^d$ for all $p \leqslant N$.
- Step 2 : Compute their characteristic polynomials $\mod \theta^d$. $\tilde{O}(N)$.

Structure of the algorithm

$$L \in \mathbb{Z}[x]\langle\partial\rangle \quad \Phi_p : \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle \xrightarrow{\sim} \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \quad \pi_p : \mathbb{Z} \to \mathbb{F}_p$$

- Step 1 : Compute the $B_p \circ \Phi_p \circ \pi_p(L) \mod \theta^d$ for all $p \leqslant N$.
- Step 2 : Compute their characteristic polynomials $\mod \theta^d$.
  $\tilde{O}(N)$.
- Step 3 : Compute their reciproqual image by Φ_p.
  $\tilde{O}(N)$

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]

$N = 7.$

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

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

$N = 7$.

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

$\mod 3^s 5^s 7^s$

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

$N = 7$.

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

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

$N = 7$.

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

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

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

$N = 7$.

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

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

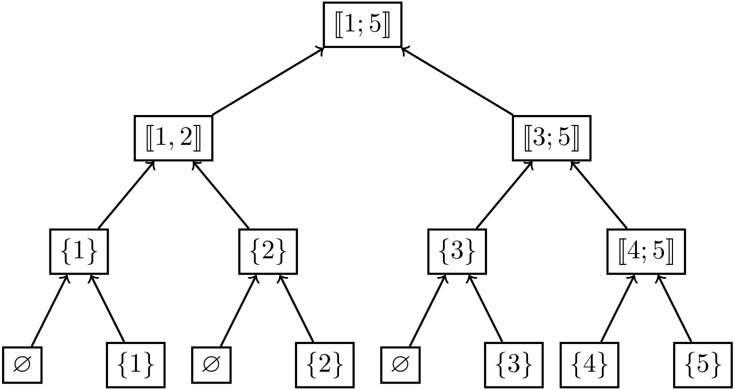
Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]

$N = 7$.

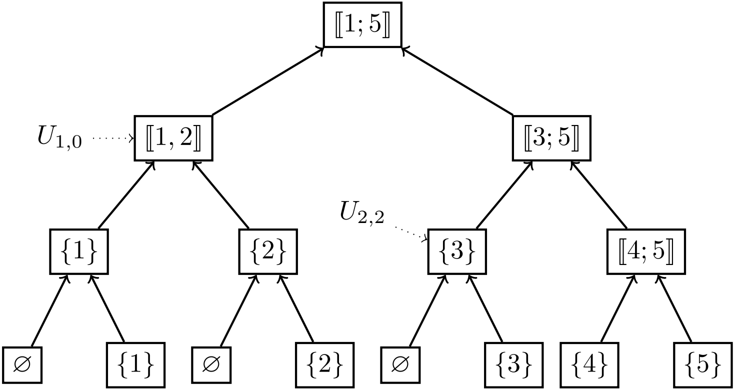
$$(3-1)! \mod 3^s5^s7^s \qquad (5-1)! \mod 5^s7^s \qquad (7-1)! \mod 7^s$$

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

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

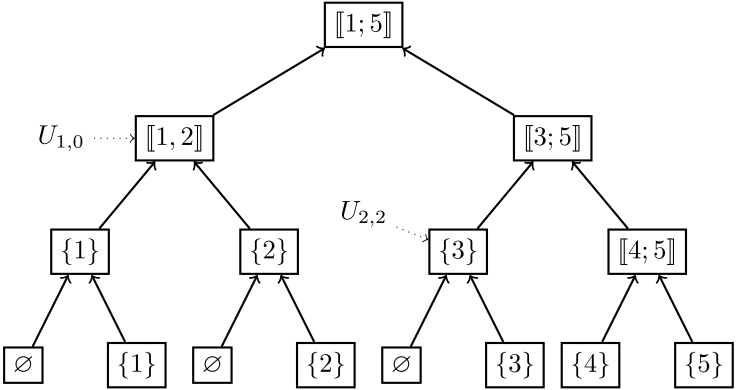


Computation of $(p-1)! \mod p^s$ [Costa, Gerbicz, Harvey, 2014]



$$U_{i,j} = U_{i+1,2j} \amalg U_{i+1,2j+1}$$

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



$U_{i,j} = U_{i+1,2j} \amalg U_{i+1,2j+1} \quad A_{i,j} = \prod_{k \in U_{i,j}} k \quad S_{i,j} = \prod_{\substack{p \in U_{i,j} \\ p \text{ prime}}} p^s$

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

$$(p-1)! \mod p^s = \prod_{j=0}^{l-1} A_{d,j} \mod S_{d,l}$$

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

$(p-1)! \mod p^s = \prod_{j=0}^{l-1} A_{d,j} \mod S_{d,l}$

$W_{i,j} := \prod_{k=0}^{j-1} A_{i,k} \mod S_{i,j}$

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

$(p-1)! \mod p^s = \prod_{j=0}^{l-1} A_{d,j} \mod S_{d,l}$
$W_{i,j} := \prod_{k=0}^{j-1} A_{i,k} \mod S_{i,j}$

$$W_{i+1,2j} = W_{i,j} \mod S_{i+1,2j}$$

$$W_{i+1,2j+1} = A_{i+1,2j} W_{i,j} \mod S_{i+1,2j}$$

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

$(p-1)! \mod p^s = \prod_{j=0}^{l-1} A_{d,j} \mod S_{d,l}$
$W_{i,j} := \prod_{k=0}^{j-1} A_{i,k} \mod S_{i,j}$

$$W_{i+1,2j} = W_{i,j} \mod S_{i+1,2j}$$

$$W_{i+1,2j+1} = A_{i+1,2j} W_{i,j} \mod S_{i+1,2j}$$

$\tilde{O}(sN)$ binary operations.

Final algorithm

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

Final algorithm

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

$$\begin{array}{ccc}
\mathbb{Z}[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi} & \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle \\
\downarrow \pi_{x,p} & & \downarrow \pi_{\theta,p} \\
\mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi_p} & \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle
\end{array}$$

Final algorithm

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

$$\begin{array}{ccc} \mathbb{Z}[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi} & \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow \pi_{x,p} & & \downarrow \pi_{\theta,p} \\ \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi_p} & \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \end{array}$$

$$L \in \mathbb{Z}[x]\langle\partial\rangle \mapsto L_1\partial^{-d} \in \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle$$

$B(\theta) \in M_r(k[\theta])$ the companion matrix of L_1.

Final algorithm

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

$$\begin{array}{ccc} \mathbb{Z}[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi} & \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow{\scriptstyle \pi_{x,p}} & & \downarrow{\scriptstyle \pi_{\theta,p}} \\ \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi_p} & \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \end{array}$$

$$L \in \mathbb{Z}[x]\langle\partial\rangle \mapsto L_1\partial^{-d} \in \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle$$

$B(\theta) \in M_r(k[\theta])$ the companion matrix of L_1.

$$B(\theta)B(\theta+1)\dots B(\theta+p-1) \mod p$$

for $p \leqslant N$.

Final algorithm

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

$$\begin{array}{ccc} \mathbb{Z}[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi} & \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle \\ \downarrow{\scriptstyle \pi_{x,p}} & & \downarrow{\scriptstyle \pi_{\theta,p}} \\ \mathbb{F}_p[x]\langle\partial^{\pm 1}\rangle & \xrightarrow{\Phi_p} & \mathbb{F}_p[\theta]\langle\partial^{\pm 1}\rangle \end{array}$$

$$L \in \mathbb{Z}[x]\langle\partial\rangle \mapsto L_1\partial^{-d} \in \mathbb{Z}[\theta]\langle\partial^{\pm 1}\rangle$$

$B(\theta) \in M_r(k[\theta])$ the companion matrix of L_1.

$$B(\theta)B(\theta+1)\ldots B(\theta+p-1) \mod p$$

for $p \leqslant N$.

$$A_{i,j} = \prod_{k\in U_{i,j}} B(\theta+k) \mod \theta^d \quad S_{i,j} = \prod_{\substack{p\in U_{i,j} \\ p \text{ prime}}} p$$

Final algorithm

- Compute $L_1\partial^{-d_1} = \Phi(L)$.
  $O(1)$

Final algorithm

- Compute $L_1\partial^{-d_1} = \Phi(L)$.
  $O(1)$
- Compute the list of primes p inferior to N
  $\tilde{O}(N)$

Final algorithm

- Compute $L_1\partial^{-d_1} = \Phi(L)$.
  $O(1)$
- Compute the list of primes p inferior to N
  $\tilde{O}(N)$
- Compute the $B(L_1)(\theta + i) \mod \theta^d$ for $i \leqslant N$
  $\tilde{O}(N)$

Final algorithm

- Compute $L_1\partial^{-d_1} = \Phi(L)$.
  $O(1)$
- Compute the list of primes p inferior to N
  $\tilde{O}(N)$
- Compute the $B(L_1)(\theta + i) \mod \theta^d$ for $i \leqslant N$
  $\tilde{O}(N)$
- Compute the $B_p(L_1) \mod \theta^d$ for $p \leqslant N$
  $\tilde{O}(N)$

Final algorithm

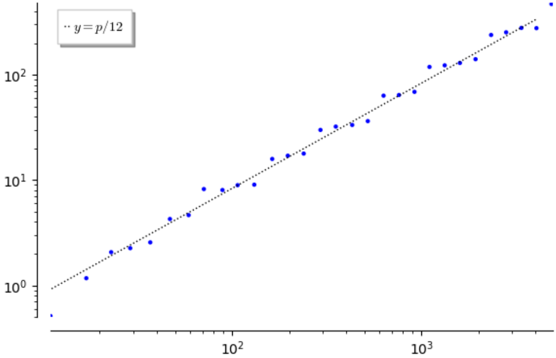
- Compute $L_1\partial^{-d_1} = \Phi(L)$.
  $O(1)$
- Compute the list of primes p inferior to N
  $\tilde{O}(N)$
- Compute the $B(L_1)(\theta + i) \mod \theta^d$ for $i \leqslant N$
  $\tilde{O}(N)$
- Compute the $B_p(L_1) \mod \theta^d$ for $p \leqslant N$
  $\tilde{O}(N)$
- Compute their characteristic polynomials.
  $\tilde{O}(N)$

Final algorithm

- Compute $L_1\partial^{-d_1} = \Phi(L)$.
  $O(1)$
- Compute the list of primes p inferior to N
  $\tilde{O}(N)$
- Compute the $B(L_1)(\theta + i) \mod \theta^d$ for $i \leqslant N$
  $\tilde{O}(N)$
- Compute the $B_p(L_1) \mod \theta^d$ for $p \leqslant N$
  $\tilde{O}(N)$
- Compute their characteristic polynomials.
  $\tilde{O}(N)$
- Deduce the $\chi(A_p(L))$.
  $\tilde{O}(N)$

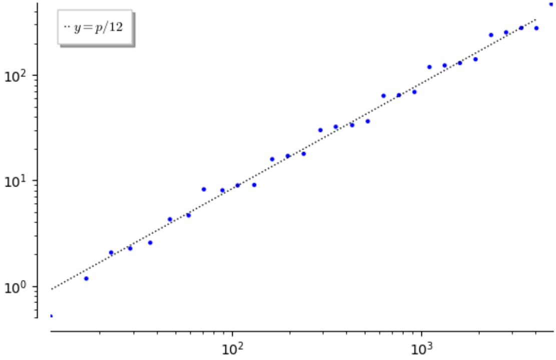
Implementation

Implementation of the algorithm



Implementation

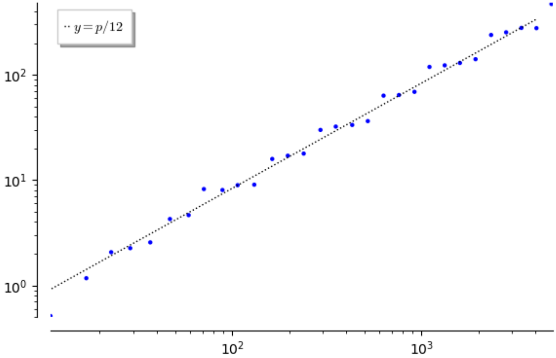
Implementation of the algorithm



Complexity : If $L \in \mathbb{Z}[x]\langle\partial\rangle$ is of degree m, has polynomial coefficients of degree at most d and has integer coefficients of size at most n then :

Implementation

Implementation of the algorithm



Complexity : If $L \in \mathbb{Z}[x]\langle\partial\rangle$ is of degree m, has polynomial coefficients of degree at most d and has integer coefficients of size at most n then :

$$O(Nd((n+d)(m+d)^{w}+(m+d)^{\Omega})).$$

Future works

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

Future works

- [Bostan, Caruso, Schost, 2016] brought the computation of invariant factors of the p-curvature to that of a factorial.
- Extension to operators with coefficients in a number field.