An algorithm for constructing certain differential operators in prime characteristic

Alberto F. Boix

Universitat Pompeu Fabra

EACA 2016 Communication

Based on joint work with:

- Alessandro De Stefani (University of Virginia).
- Davide Vanzo (Università degli studi di Firenze).

What is the goal of this talk (roughly speaking)?

- Input: A polynomial f with coefficients on $\mathbb{Z}/p\mathbb{Z}$, where p is prime.
- Output: produce a differential equation of the form

$$\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}.$$

BACKGROUND MATERIAL

Preliminaries

- $\mathbb{K}$ any field.
- $S = \mathbb{K}[x_1, \ldots, x_d]$, $f \in S$.

Fact

S_f is not finitely generated as S-module.

Preliminaries

- $S = \mathbb{C}[x_1, \ldots, x_d]$, $f \in S$.
- $\mathcal{D}_S$: ring of $\mathbb{C}$-linear differential operators.
- $\mathcal{D}_S[y] := \mathbb{C}[y] \otimes_{\mathbb{C}} \mathcal{D}_S$.

Theorem (Bernstein (1972))

There are $b(y) \in \mathbb{C}[y]$ and $\Delta(y) \in \mathcal{D}_S[y]$ such that

$$b(n)f^n = \Delta(n) \bullet f^{n+1},$$

for any $n \in \mathbb{Z}$.

Preliminaries

Definition

$b_f(y)$: monic polynomial of smallest degree of the ideal made up by the b's.

Why we introduce b_f?

- m: greatest integer root in absolute value of b_f.
- (Bernstein, 1972) S_f is generated by $1/f^m$ as left $\mathcal{D}_S$-module.
- (Walther, 2005) S_f is not generated by $1/f^i$ for $i < m$.

End of preliminaries

In general, m can be strictly greater than 1.

Example

If $f = x_1^2 + x_2^2 + x_3^2 + x_4^2$, then $b_f(y) = (y+1)(y+2)$.

A SURPRISING FACT

New setup

From now on:

- p prime number.
- $S = \mathbb{Z}/p\mathbb{Z}[x_1, \ldots, x_d]$, $f \in S$.
- $\mathcal{D}_S$: ring of $\mathbb{Z}/p\mathbb{Z}$-linear differential operators.

A surprising fact

Theorem (Àlvarez Montaner, Blickle, Lyubeznik (2005))
S_f is generated by $1/f$ as $\mathcal{D}_S$-module.

THE
LEVEL

What is the level?

We have
$$\mathcal{D}_S = \bigcup_{e\geq 0} \mathcal{D}_S^{(e)},$$
where
$$\mathcal{D}_S^{(e)} := S\langle \partial_i^{[t]} \mid \quad 1 \leq i \leq d, \quad 1 \leq t \leq p^e - 1\rangle$$
and
$$\partial_i^{[t]} := \frac{1}{t!}\frac{\partial^t}{\partial x_i^t}.$$
The exponent e is called the *level*.

Why the surprising fact is true?

Theorem (Àlvarez Montaner, Blickle, Lyubeznik (2005))
There exists $\delta \in \mathcal{D}_S^{(e)}$ such that $\delta(1/f) = 1/f^p$.

Goal
Provide an effective procedure to calculate the level e and δ.

COMPUTING
THE
LEVEL

THE IDEAL OF p^eTH ROOTS

The ideal of p^eth roots

- $g \in S = \mathbb{Z}/p\mathbb{Z}[x_1, \ldots, x_d]$.
- If $\gamma = (c_1, \ldots, c_d) \in \mathbb{N}^d$, then $||\gamma|| := \max\{c_i\}$.

If

$$g = \sum_{0 \le ||\alpha|| \le p^e - 1} g_\alpha^{p^e} \mathbf{x}^\alpha,$$

then $I_e(gS)$ is the ideal of S generated by the g_α's.

Calculation of the level

We have

$$R = I_0\left(f^{p^0-1}\right) \supseteq I_1\left(f^{p-1}\right) \supseteq I_2\left(f^{p^2-1}\right) \supseteq \dots$$

Set

$$e := \inf\left\{s \geq 1 \mid \quad I_{s-1}\left(f^{p^{s-1}-1}\right) = I_s\left(f^{p^s-1}\right)\right\}.$$

Calculation of the level

Theorem (Àlvarez Montaner, Blickle, Lyubeznik (2005))

With the previous choice of e, for any $s \geq 0$

$$I_{e-1}\left(f^{p^{e-1}-1}\right) = I_{e+s}\left(f^{p^{e+s}-1}\right).$$

Moreover,

$$e = \min\left\{ s \geq 1 \mid \quad f^{p^s-p} \in I_s\left(f^{p^s-1}\right)^{[p^s]} \right\}$$

and $e \leq \deg(f)$.

THE ALGORITHM

Input

- p prime number.
- $S = \mathbb{Z}/p\mathbb{Z}[x_1, \ldots, x_d]$, $f \in S$.

The body of the algorithm

Algorithm (B., De Stefani, Vanzo)

Carry out the following steps:

- Compute $\left(e, I_e\left(f^{p^e-1}\right)\right)$, where e is the level of δ.
- Write
$$f^{p^e-1} = \sum_{0 \leq ||\alpha|| \leq p^e-1} f_\alpha^{p^e} \mathbf{x}^\alpha.$$
- For each $0 \leq ||\alpha|| \leq p^e - 1$, there is $\delta_\alpha \in \mathcal{D}_S^{(e)}$ such that
$$\delta_\alpha\left(\mathbf{x}^\beta\right) = \begin{cases} 1, & \text{if } \beta = \alpha, \\ 0, & \text{otherwise.} \end{cases}$$

  Here, $\beta \in \mathbb{N}^d$ with $0 \leq ||\beta|| \leq p^e - 1$

The body of the algorithm

Algorithm (B., De Stefani, Vanzo)

- We have

$$f^{p^e-p} \in I_e\left(f^{p^e-1}\right)^{[p^e]} = \left(f_\alpha^{p^e} \mid \quad 0 \leq ||\alpha|| \leq p^e - 1\right),$$

hence

$$f^{p^e-p} = \sum_{0 \leq ||\alpha|| \leq p^e-1} s_\alpha f_\alpha^{p^e}.$$

- Set

$$\delta := \sum_{0 \leq ||\alpha|| \leq p^e-1} s_\alpha \delta_\alpha.$$

AN
EXAMPLE

An example

- $f = x^2y^3z^5 \in \mathbb{Z}/2\mathbb{Z}[x, y, z]$.
- $f^{15} = x^{30}y^{45}z^{75} = (xy^2z^4)^{16} \cdot (x^{14}y^{13}z^{11})$, so level 4.

Now, needed δ_1 such that

$$\delta_1(x^{14}y^{13}z^{11}) = 1$$

and

$$\delta_1(x^iy^jz^k) = 0 \text{ for any } 0 \leq i, j, k \leq 15 = 2^4 - 1.$$

An example (continued)

- $\delta_1 = (\partial_1^{[15]}\partial_2^{[15]}\partial_3^{[15]}) \cdot (xy^2z^4)$.

Moreover,

$$f^{2^4-2} = (x^{12}y^{10}z^6) \cdot (x^{16}y^{32}z^{64}) \in I_4(f^{15})^{[16]}.$$

Therefore,

$$\delta = (x^{12}y^{10}z^6) \cdot (\partial_1^{[15]}\partial_2^{[15]}\partial_3^{[15]}) \cdot (xy^2z^4).$$

THE
CASE
OF
ELLIPTIC
CURVES

Ordinary and supersingular elliptic curves

- $E \subseteq \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ elliptic curve defined by f.
- $f^{p-1} = h \cdot (xyz)^{p-1} + \dots$
- E is ordinary if $h \neq 0$, otherwise supersingular.
- (Takagi, Takahashi 2008) E is ordinary iff E has level one.

Ordinary and supersingular elliptic curves

Theorem (B., De Stefani, Vanzo)

E is supersingular if and only if f has level two.

The case of elliptic curves: characteristic 2 and 3

- Set $D := \partial_1^{[p^2-1]}\partial_2^{[p^2-1]}\partial_3^{[p^2-1]}$.

p	Elliptic curve	Differential operator
2	$x^3 + y^2z + yz^2$	$y^2Dx^3z + z^2Dx^3y + x^2Dxyz^2$
3	$x^3 - xz^2 - y^2z$	$(x^6z^3 - x^3y^6)Dx^4z^5 +$ $+(x^9 + x^3z^6 + y^6z^3)Dxy^8 + y^3z^6Dx^4y^5$

The case of elliptic curves: sketch of proof

- $p \geq 5$.
- After linear change of coordinates,

$$f = y^2 z - x^3 + axz^2 + bz^3,$$

  where $a, b \in \mathbb{Z}/p\mathbb{Z}$.
- If $a = b = 0$, then $I_1(f^{p-1}) = I_2\left(f^{p^2-1}\right) = (x, y)$.
- Otherwise, $I_1(f^{p-1}) = I_2\left(f^{p^2-1}\right) = (x, y, z)$.

NICE
PLACE
TO
STOP