An algorithm for constructing certain differential operators in prime characteristic

Alberto F. Boix

Ben-Gurion University of the Negev

STNB 2019

Based on joint works with:

- Iván Blanco Chacón (University College Dublin).
- Alessandro De Stefani (University of Nebraska).
- Stiofáin Fordham (University College Dublin).
- Emrah Sercan Yilmaz (University College Dublin).
- Davide Vanzo (Università di Bologna).

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

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

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

Calculation of the level

We have

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

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,

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

INTERLUDE
OTHER WAYS
TO CHARACTERIZE
THE LEVEL

F-jumping numbers review

- R commutative Noetherian regular ring $\supseteq \mathbb{F}_p$
- $\mathfrak{a} \subseteq R$ ideal, $\lambda \in (0, +\infty)$.
- (Blickle, Mustata, Smith'08) The chain

$$\ldots \subseteq I_e(\mathfrak{a}^{\lceil \lambda p^e \rceil}) \subseteq I_{e+1}(\mathfrak{a}^{\lceil \lambda p^{e+1} \rceil}) \subseteq \ldots$$

stabilizes; set

$$\tau(\mathfrak{a}^\lambda) := I_e(\mathfrak{a}^{\lceil \lambda p^e \rceil}) \ e \gg 0.$$

F-jumping numbers review (Blickle, Mustata, Smith'08)

- The chain

$$\ldots \subseteq I_e(\mathfrak{a}^{\lceil \lambda p^e \rceil}) \subseteq I_{e+1}(\mathfrak{a}^{\lceil \lambda p^{e+1} \rceil}) \subseteq \ldots$$

  stabilizes; set

$$\tau(\mathfrak{a}^\lambda) := I_e(\mathfrak{a}^{\lceil \lambda p^e \rceil}) \ e \gg 0.$$

- $\exists \varepsilon > 0$ s.t. $\tau(\mathfrak{a}^\lambda) = \tau(\mathfrak{a}^{\lambda'}) \ \forall \lambda' \in [\lambda, \lambda + \varepsilon)$.
- λ is an F–jumping number if $\tau(\mathfrak{a}^\lambda) \neq \tau(\mathfrak{a}^{\lambda'}) \ \forall \lambda' < \lambda$.
- If $\mathfrak{a} = (f)$, then $\tau(\mathfrak{a}^\lambda) = \tau(\mathfrak{a}^{\lambda+1})$.

Level and F-jumping numbers

- $p \geq 3$, R commutative Noetherian regular F–finite ring $\supseteq \mathbb{F}_p$.
- $f \in R$, and
- λ: greatest F-jumping number of (f) inside $(0, 1]$.

Theorem (Fordham'18)

The level of f is $\lceil 1 - \log_p(1 - \lambda) \rceil$.

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 HYPERELLIPTIC CURVES

Setup

- $g \geq 1$
- $f(x, y, z) := y^2 z^{2g-1} - h(x, z)$, $h \in \mathbb{F}_p[x, z]_{2g+1}$.
- $h(x, 1)$ has no multiple roots.
- $C : f(x, y, z) = 0$.
- Write

$$h(x, 1)^{(p-1)/2} = \sum_{j=0}^{N} c_j x^j, \ N := \left(\frac{p-1}{2}\right)(2g+1).$$

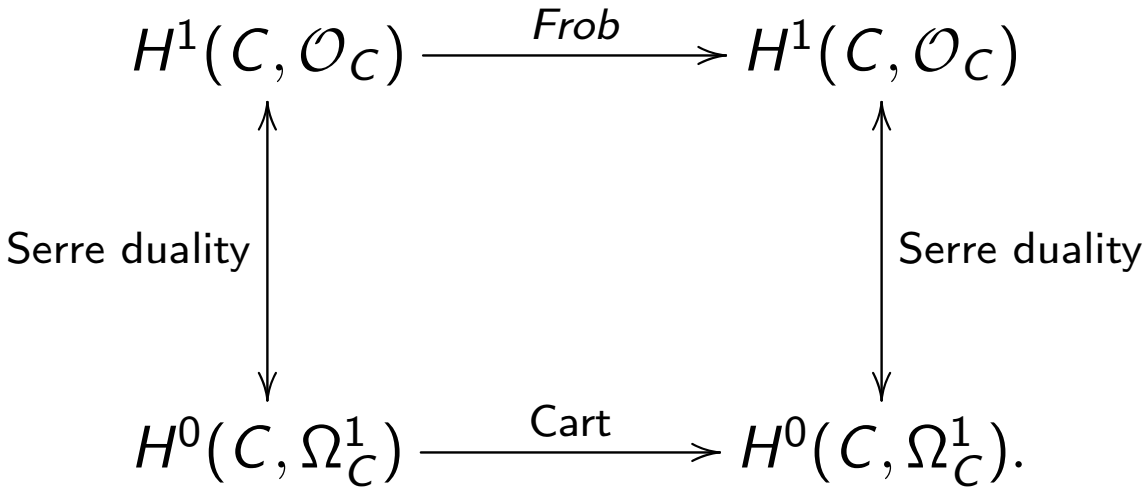
The Cartier–Manin matrix

Definition (Manin'65)

We define the Cartier–Manin matrix of C as

$$A := \begin{pmatrix} c_{p-1} & c_{p-2} & \cdots & c_{p-g} \\ c_{2p-1} & c_{2p-2} & \cdots & c_{2p-g} \\ \vdots & \vdots & \ddots & \vdots \\ c_{gp-1} & c_{gp-2} & \cdots & c_{gp-g} \end{pmatrix}.$$

Why you introduce this matrix?



- Cart is given by A once you fix on $H^0(C, \Omega^1_C)$ the basis

$$\frac{x^{i-1}dx}{y} \ (1 \leq i \leq g).$$

Why you introduce this matrix?

Definition

Let C be as before.

- C is ordinary if A is invertible.
- C is supersingular if $A \neq 0$ and $A^2 = 0$.
- C is superspecial if $A = 0$.
- C is intermediate if neither of the above holds.

THE CASE OF ELLIPTIC CURVES

Ordinary and supersingular elliptic curves

- $C \subseteq \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ elliptic curve defined by f.
- $f^{p-1} = c \cdot (xyz)^{p-1} + \ldots$
- C is ordinary if $c \neq 0$, otherwise supersingular.
- (Takagi, Takahashi'08) C is ordinary iff f has level one.

Ordinary and supersingular elliptic curves

Theorem (B., De Stefani, Vanzo)

C 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 GENUS AT LEAST TWO

Higher genus: the ordinary case

Theorem (Blanco–Chacón, B., Fordham, Yilmaz)

If $p > 2g^2 - 1$ *and* C *is ordinary, then the level of* f *is* 2.

Higher genus: the ordinary case

The converse is, in general, not true.

- $p = 11$, $C : y^2z^3 - x^5 - z^5 = 0$.
- A has rank 1.
- The level of $y^2z^3 - x^5 - z^5$ is two.

Higher genus: the supersingular (not superspecial) case

Theorem (Blanco–Chacón, B., Fordham, Yilmaz)

If $p > 2g^2 - 1$ and C is supersingular (but not superspecial), then the level of f is at least 3.

Higher genus: the supersingular (not superspecial) case

- $C : y^2z^3 - x^5 - z^5 = 0$.
- C is supersingular (not superspecial) for $p = 13$.
- The level of $y^2z^3 - x^5 - z^5$ is 4 for $p = 13$.
- C is superspecial for $p = 17$.
- The level of $y^2z^3 - x^5 - z^5$ is 3 for $p = 17$.

The superspecial case: some examples

Families of superspecial curves with level at least 3. (Kodama, Washio'89, Valentini'95)
Given $0 \neq \mu \in \mathbb{F}_p$:

$$\begin{cases} y^2 z^{2g-1} - x^{2g+1} - \mu z^{2g+1}, \ p \equiv -1 \pmod{2g+1}, \\ y^2 z^{2g-1} - x^{2g+1} - \mu x z^{2g}, \ p \equiv -1 \text{ or } p \equiv 2g+1 \pmod{4g}. \end{cases}$$

WE
STOP
HERE