Fast coefficient computation for algebraic power series in positive characteristic

INRIA Saclay

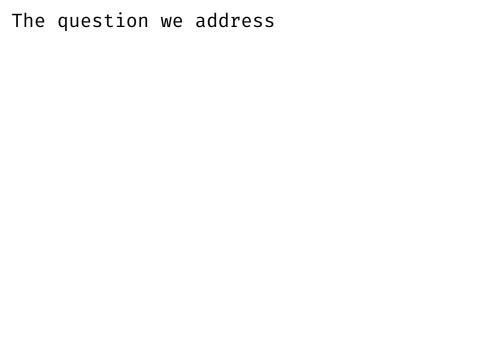
Gilles Christol Université Paris 6

Alin Bostan Xavier Caruso Université Rennes 1

> Philippe Dumas **INRIA Saclay**

Algorithmic Number Theory Symposium

July 19, 2018



We want to design an algorithm with the following specifications

We want to design an algorithm with the following specifications

Input

We want to design an algorithm with the following specifications

Input

1) An algebraic power series

$$f(t) = a_0 + a_1 t + a_2 t^2 + \dots \in \mathbb{F}_p[[t]]$$

We want to design an algorithm with the following specifications

Input

1) An algebraic power series

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots \in \mathbb{F}_{p}[[t]]$$

specified by:

an irreducible polynomial E(t,y) s.t. E(t,f(t))=0 the first a_i 's

We want to design an algorithm with the following specifications

Input

1) An algebraic power series

$$f(t) = a_0 + a_1 t + a_2 t^2 + \dots \in \mathbb{F}_{p}[[t]]$$

specified by:

- an irreducible polynomial E(t,y) s.t. E(t,f(t))=0 the first a_i 's
- ② An integer N

We want to design an algorithm with the following specifications

Input

1) An algebraic power series

$$f(t) = a_0 + a_1 t + a_2 t^2 + \dots \in \mathbb{F}_p[[t]]$$

specified by:

- an irreducible polynomial E(t,y) s.t. E(t,f(t))=0 the first a_i 's
- 2 An integer N

Output

We want to design an algorithm with the following specifications

Input

1) An algebraic power series

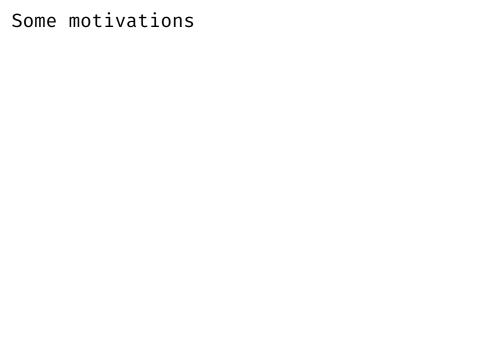
$$f(t) = a_0 + a_1 t + a_2 t^2 + \dots \in \mathbb{F}_p[[t]]$$

specified by:

- an irreducible polynomial E(t,y) s.t. E(t,f(t))=0 the first a_i 's
- ② An integer N

Output

The coefficient a_N



The question is quite natural since efficient methods exist for rational fractions

The question is quite natural since efficient methods exist for rational fractions

binary powering: cost $O(\log N)$

The question is quite natural since efficient methods exist for rational fractions binary powering: cost $O(\log N)$

Compute the N-th coefficient of an algebraic series over $\mathbb Q$ by modular techniques

The question is quite natural since efficient methods exist for rational fractions

binary powering: cost $O(\log N)$

Compute the N-th coefficient of an algebraic series over $\mathbb Q$ by modular techniques

standard methods compute separately the numerator and the denominator of a highly reducible fraction

The question is quite natural since efficient methods exist for rational fractions

binary powering: cost $O(\log N)$

Compute the N-th coefficient of an algebraic series over $\mathbb Q$ by modular techniques

standard methods compute separately the numerator and the denominator of a highly reducible fraction

One of the most difficult questions in modular computations is the complexity of computations mod p for a large prime p of coefficients in the expansion of an algebraic function

Chudnovsky, Chudnovsky

The question is quite natural since efficient methods exist for rational fractions

binary powering: cost $O(\log N)$

Compute the N-th coefficient of an algebraic series over $\mathbb Q$ by modular techniques

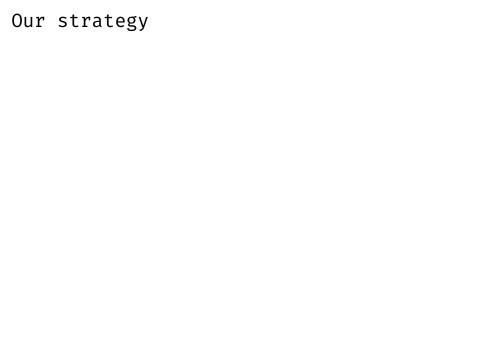
standard methods compute separately the numerator and the denominator of a highly reducible fraction

One of the most difficult questions in modular computations is the complexity of computations mod p for a large prime p of coefficients in the expansion of an algebraic function

Chudnovsky, Chudnovsky

Beyond its relevance to complexity theory, this problem is important in applications to integer factorization and point-counting

Bostan, Gaudry, Schost



Christol's Theorem

Christol's Theorem

Let $f(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n + \cdots$ be an algebraic power series over \mathbb{F}_p .

Christol's Theorem

Let $f(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n + \cdots$ be an algebraic power series over \mathbb{F}_p .

Then there exists a finite dimensional \mathbb{F}_p -vector space containing f(t), and stable under the section operators S_r :

$$S_r(c_0 + c_1t + c_2t^2 + \cdots) = c_r + c_{r+p}t + c_{r+2p}t^2 + \cdots$$

for $0 \le r < p$

Christol's Theorem

Let $f(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n + \cdots$ be an algebraic power series over \mathbb{F}_p .

Then there exists a finite dimensional \mathbb{F}_p -vector space containing f(t), and stable under the section operators S_r :

$$S_r(c_0 + c_1t + c_2t^2 + \cdots) = c_r + c_{r+p}t + c_{r+2p}t^2 + \cdots$$

for $0 \le r < p$

Rough idea behind our algorithms

Christol's Theorem

Let $f(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n + \cdots$ be an algebraic power series over \mathbb{F}_p .

Then there exists a finite dimensional \mathbb{F}_p -vector space containing f(t), and stable under the section operators S_r :

$$S_r(c_0 + c_1t + c_2t^2 + \cdots) = c_r + c_{r+p}t + c_{r+2p}t^2 + \cdots$$

for $0 \le r < p$

Rough idea behind our algorithms

We write $N = \overline{r_\ell \cdots r_1 r_0}^p$

Christol's Theorem

Let $f(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n + \cdots$ be an algebraic power series over \mathbb{F}_p .

Then there exists a finite dimensional \mathbb{F}_p -vector space containing f(t), and stable under the section operators S_r :

$$S_r(c_0 + c_1t + c_2t^2 + \cdots) = c_r + c_{r+p}t + c_{r+2p}t^2 + \cdots$$

for $0 \le r < p$

Rough idea behind our algorithms

We write
$$N = \overline{r_\ell \cdots r_1 r_0}^p$$
; then $a_N = (S_{r_\ell} \cdots S_{r_1} S_{r_0} f)(0)$

Christol's Theorem

Let $f(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n + \cdots$ be an algebraic power series over \mathbb{F}_p .

Then there exists a finite dimensional \mathbb{F}_p -vector space containing f(t), and stable under the section operators S_r :

$$S_r(c_0 + c_1t + c_2t^2 + \cdots) = c_r + c_{r+p}t + c_{r+2p}t^2 + \cdots$$

for $0 \le r < p$

Rough idea behind our algorithms

We write $N = \overline{r_\ell \cdots r_1 r_0}^p$; then $a_N = (S_{r_\ell} \cdots S_{r_1} S_{r_0} f)(0)$

We compute a finite dimension vector space as above and the linear actions of the S_r 's on it

Christol's Theorem

Let $f(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n + \cdots$ be an algebraic power series over \mathbb{F}_p .

Then there exists a finite dimensional \mathbb{F}_p -vector space containing f(t), and stable under the section operators S_r :

$$S_r(c_0 + c_1t + c_2t^2 + \cdots) = c_r + c_{r+p}t + c_{r+2p}t^2 + \cdots$$

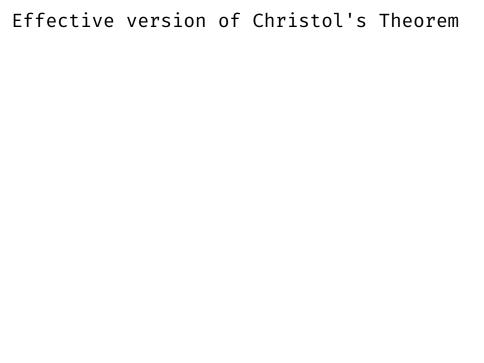
for $0 \le r < p$

Rough idea behind our algorithms

We write $N = \overline{r_\ell \cdots r_1 r_0}^p$; then $a_N = (S_{r_\ell} \cdots S_{r_1} S_{r_0} f)(0)$

We compute a finite dimension vector space as above and the linear actions of the S_r 's on it

Expected complexity: $O(\log_p N)$



Theorem (BC²D, 2018)

Set $d = \deg_v E$ and $h = \deg_t E$. Then, the \mathbb{F}_p -vector space

$$\left\{\begin{array}{ll} \sum_{i=0}^{d-1} a_i(t) \ \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} & \text{with} \quad a_i(t) \in k[t], \ \deg a_i(t) \leq h \end{array}\right\}$$

contains f and is stable by the S_r 's

Theorem (BC²D, 2018)

Set $d = \deg_v E$ and $h = \deg_t E$. Then, the \mathbb{F}_p -vector space

$$\left\{ \begin{array}{l} \displaystyle \sum_{i=0}^{d-1} a_i(t) \, \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} \quad \text{with} \quad a_i(t) \in k[t], \, \deg a_i(t) \leq h \end{array} \right\}$$

contains f and is stable by the S_r 's

Ingredients of the proof

Theorem (BC²D, 2018)

Set $d = \deg_v E$ and $h = \deg_t E$. Then, the \mathbb{F}_p -vector space

$$\left\{\begin{array}{ll} \displaystyle \sum_{i=0}^{d-1} a_i(t) \ \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} & \text{with} \quad a_i(t) \in k[t], \ \deg a_i(t) \leq h \end{array}\right\}$$

contains f and is stable by the S_r 's

Ingredients of the proof

Theorem (BC²D, 2018)

Set $d = \deg_v E$ and $h = \deg_t E$. Then, the \mathbb{F}_p -vector space

$$\left\{ \begin{array}{l} \displaystyle \sum_{i=0}^{d-1} a_i(t) \, \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} \quad \text{with} \quad a_i(t) \in \mathit{k}[t], \, \deg a_i(t) \leq \mathit{h} \end{array} \right\}$$

contains f and is stable by the S_r 's

Ingredients of the proof

① We write:
$$\frac{Q(t,f(t))}{\frac{\partial E}{\partial y}(t,f(t))} = \text{residue}_{y=f(t)} \frac{Q(t,y)}{E(t,y)}$$

We prove a commutation relation between residue and section operators

Theorem (BC²D, 2018)

Set $d = \deg_v E$ and $h = \deg_t E$. Then, the \mathbb{F}_p -vector space

$$\left\{ \begin{array}{l} \displaystyle \sum_{i=0}^{d-1} a_i(t) \, \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} \quad \text{with} \quad a_i(t) \in k[t], \, \deg a_i(t) \leq h \end{array} \right\}$$

contains f and is stable by the S_r 's

Ingredients of the proof

① We write:
$$\frac{Q(t,\mathit{f}(t))}{\frac{\partial E}{\partial y}(t,\mathit{f}(t))} = \mathsf{residue}_{y=\mathit{f}(t)} \frac{Q(t,y)}{E(t,y)}$$

② We prove a commutation relation between residue and section operators

Difficulty: residue are local around f(t) whereas section operators are local around 0

Theorem (BC²D, 2018)

Set $d = \deg_y E$ and $h = \deg_t E$. Then, the \mathbb{F}_p -vector space

$$\left\{ \begin{array}{l} \displaystyle \sum_{i=0}^{d-1} a_i(t) \, \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} \quad \text{with} \quad a_i(t) \in k[t], \, \deg a_i(t) \leq h \end{array} \right\}$$

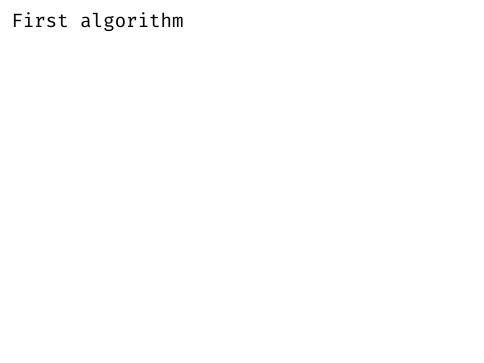
contains f and is stable by the S_r 's

Ingredients of the proof

② We prove a commutation relation between residue and section operators

Difficulty: residue are local around f(t) whereas section operators are local around 0

Solution: We use Cartier operator



First algorithm

$$S_r\left(\sum_{i=0}^{d-1}a_i(t)\,\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}\right) = \sum_{i=0}^{d-1}b_i(t)\,\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}$$

First algorithm

$$S_r\left(\sum_{i=0}^{d-1}a_i(t)\;\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}\right)=\sum_{i=0}^{d-1}b_i(t)\;\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}$$

First algorithm

$$S_r\left(\sum_{i=0}^{d-1}a_i(t)\,\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}\right) = \sum_{i=0}^{d-1}\frac{b_i(t)}{\frac{\partial E}{\partial y}(t,f(t))}$$

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} b_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \quad \deg b_i(t) \le h$$

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} b_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \quad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} b_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \quad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} \frac{b_i(t)}{\frac{\partial E}{\partial y}(t, f(t))} \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \qquad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Compute
$$\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}$$
 mod $t^{O(dhp)}$

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} \frac{b_i(t)}{\frac{\partial E}{\partial y}(t, f(t))} \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \qquad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Compute
$$\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}$$
 mod $t^{O(dhp)}$ $O^{\sim}(d^2hp)$

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} \frac{b_i(t)}{\frac{\partial E}{\partial y}(t, f(t))} \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \qquad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

Inverse the quasi-Toeplitz system

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} \frac{b_i(t)}{\frac{\partial E}{\partial y}(t, f(t))} \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \qquad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

$$\begin{array}{lll} \text{Compute } \frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))} \bmod t^{O(dhp)} & \dots & O^{\sim}\big(d^2hp\big) \\ \text{Inverse the quasi-Toeplitz system } & \dots & O^{\sim}\big(d^\omega h\big) \end{array}$$

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} \frac{b_i(t)}{\frac{\partial E}{\partial y}(t, f(t))} \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \qquad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

Inverse the quasi-Toeplitz system $\dots O^{\sim}(d^{\omega}h)$

Computation

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} \frac{b_i(t)}{\frac{\partial E}{\partial y}(t, f(t))} \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \qquad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

Inverse the quasi-Toeplitz system $\dots O^{\sim}(d^{\omega}h)$

Computation

Evaluate the left hand side

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} b_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \quad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

Inverse the quasi-Toeplitz system $\dots O^{\sim}(d^{\omega}h)$

Computation

Evaluate the left hand side $\dots O(d^2h^2)$

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} b_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \quad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

Compute
$$\frac{\mathit{f}(t)^i}{\frac{\partial \mathit{E}}{\partial \mathit{y}}(t,\mathit{f}(t))}$$
 mod $t^{O(dhp)}$ $O^{\sim}(d^2hp)$

Inverse the quasi-Toeplitz system $\dots O^{\sim}(d^{\omega}h)$

Computation

Evaluate the left hand side $\dots O(d^2h^2)$

Solve the system

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} \frac{b_i(t)}{\frac{\partial E}{\partial y}(t, f(t))} \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \qquad \deg b_i(t) \leq h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

Inverse the quasi-Toeplitz system $\dots O^{\sim}(d^{\omega}h)$

Computation

Evaluate the left hand side
$$O(d^2h^2)$$
 Solve the system $O(d^2h^2)$

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) = \sum_{i=0}^{d-1} b_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))} \quad \deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

Inverse the quasi-Toeplitz system $\dots O^{\sim}(d^{\omega}h)$

Computation

Evaluate the left hand side	(d^2h^2)
Solve the system	(d^2h^2)

Total cost

$$S_r\left(\sum_{i=0}^{d-1}a_i(t)\,\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}\right) = \sum_{i=0}^{d-1}\frac{b_i(t)}{\frac{\partial E}{\partial y}(t,f(t))}\,\frac{f(t)^i}{\frac{\partial E}{\partial y}(t,f(t))}\,\,\deg b_i(t) \le h$$

Quasi-Toeplitz linear system; displacement rank d

Precomputation

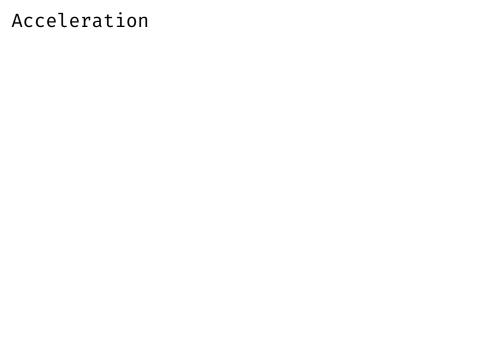
Inverse the quasi-Toeplitz system $\dots O^{\sim}(d^{\omega}h)$

Computation

Evaluate the left hand side
$$O(d^2h^2)$$

Solve the system $\dots O(d^2h^2)$

Total cost
$$O^{\sim}ig(d^2hp+d^{\omega}hig)+Oig(d^2h^2\log Nig)$$



Why?

Why?

The complexity is good w.r.t. d, h, N but is exponential in $\log p$

Why?

The complexity $O^{\sim}(d^2hp + d^{\omega}h) + O(d^2h^2\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Why?

The complexity $O^{\sim}(d^2hp + d^{\omega}h) + O(d^2h^2\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Observation

Why?

The complexity $O^{\sim}(d^2hp + d^{\omega}h) + O(d^2h^2\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Observation

In order to compute

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) \mod t^{2dh}$$

we only need 2dh coefficients of the argument

Why?

The complexity $O^{\sim}(d^2hp + d^{\omega}h) + O(d^2h^2\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Observation

In order to compute

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) \mod t^{2dh}$$

we only need 2dh coefficients of the argument

Strategy

Why?

The complexity $O^{\sim}(d^2hp + d^{\omega}h) + O(d^2h^2\log N)$ is good w.n.t. d, h, N but is exponential in $\log p$

Observation

In order to compute

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) \mod t^{2dh}$$

we only need 2dh coefficients of the argument

Strategy

To compute $S_r(g(t))$:

Why?

The complexity $O^{-}(d^{2}hp + d^{\omega}h) + O(d^{2}h^{2}\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Observation

In order to compute

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) \mod t^{2dh}$$

we only need 2dh coefficients of the argument

Strategy

To compute $S_r(g(t))$:

 \odot we compute a recurrence on the coefficients of g(t)

Why?

The complexity $O^{\sim}(d^2hp + d^{\omega}h) + O(d^2h^2\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Observation

In order to compute

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) \mod t^{2dh}$$

we only need 2dh coefficients of the argument

Strategy

To compute $S_r(g(t))$:

use differential equations

Why?

The complexity $O^{-}(d^{2}hp + d^{\omega}h) + O(d^{2}h^{2}\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Observation

In order to compute

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) \mod t^{2dh}$$

we only need 2dh coefficients of the argument

Strategy

To compute $S_r(g(t))$:

- ① we compute a recurrence on the coefficients of g(t) use differential equations
- 2 we unroll the recurrence

Why?

The complexity $O^{-}(d^{2}hp + d^{\omega}h) + O(d^{2}h^{2}\log N)$ is good w.r.t. d, h, N but is exponential in $\log p$

Observation

In order to compute

$$S_r\left(\sum_{i=0}^{d-1} a_i(t) \frac{f(t)^i}{\frac{\partial E}{\partial y}(t, f(t))}\right) \mod t^{2dh}$$

we only need 2dh coefficients of the argument

Strategy

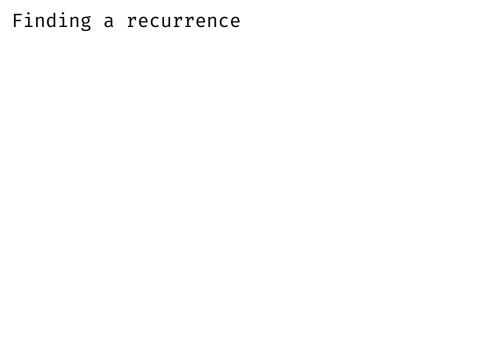
To compute $S_r(g(t))$:

 \odot we compute a recurrence on the coefficients of g(t)

use differential equations

2 we unroll the recurrence

Chudnovsky algorithm



Let g(t)

Let $g(t) \in k(t)[f]$

Let $g(t) \in k(t)[f] = k(t)[y]/E(t,y)$

Let $g(t) \in k(t)[f] = k(t)[y]/E(t,y) = L$

Let $g(t) \in k(t)[f] = k(t)[y]/E(t,y) = L$ L is a finite extension of k(t) of degree d

Let $g(t) \in k(t)[f] = k(t)[y]/E(t,y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Let $g(t) \in k(t)[f] = k(t)[y]/E(t,y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Lemma: L is stable by the derivation $\frac{d}{dt}$

Let $g(t) \in k(t)[f] = k(t)[y]/E(t,y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Lemma: L is stable by the derivation $\frac{d}{dt}$ Proof: Differentiate the relation E(t,f(t))=0

Let $g(t) \in k(t)[f] = k(t)[y]/E(t, y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Lemma: L is stable by the derivation $\frac{d}{dt}$ Proof: Differentiate the relation E(t, f(t)) = 0

Corollary: $g(t), g'(t), \dots, g^{(d)}(t)$ are dependent over k(t):

Let $g(t) \in k(t)[f] = k(t)[y]/E(t, y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Lemma: L is stable by the derivation $\frac{d}{dt}$ Proof: Differentiate the relation E(t, f(t)) = 0

Corollary: $g(t), g'(t), \dots, g^{(d)}(t)$ are dependent over k(t):

$$\lambda_d(t)g^{(d)}(t) + \dots + \lambda_1(t)g'(t) + \lambda_0(t)g(t) = 0$$

Let $g(t) \in k(t)[f] = k(t)[y]/E(t, y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Lemma: L is stable by the derivation $\frac{d}{dt}$ Proof: Differentiate the relation E(t, f(t)) = 0

Corollary: $g(t), g'(t), \dots, g^{(d)}(t)$ are dependent over k(t):

$$\lambda_d(t)g^{(d)}(t) + \dots + \lambda_1(t)g'(t) + \lambda_0(t)g(t) = 0$$

Recurrence

Let $g(t) \in k(t)[f] = k(t)[y]/E(t, y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Lemma: L is stable by the derivation $\frac{d}{dt}$ Proof: Differentiate the relation E(t, f(t)) = 0

Corollary: $g(t), g'(t), \dots, g^{(d)}(t)$ are dependent over k(t):

$$\lambda_d(t)g^{(d)}(t) + \dots + \lambda_1(t)g'(t) + \lambda_0(t)g(t) = 0$$

Recurrence

We write $g(t) = g_0 + g_1 t + g_2 t^2 + \cdots$

Let $g(t) \in k(t)[f] = k(t)[y]/E(t, y) = L$ L is a finite extension of k(t) of degree d

Differential equation

Lemma: L is stable by the derivation $\frac{d}{dt}$

Proof: Differentiate the relation E(t, f(t)) = 0

Corollary: $g(t), g'(t), \dots, g^{(d)}(t)$ are dependent over k(t):

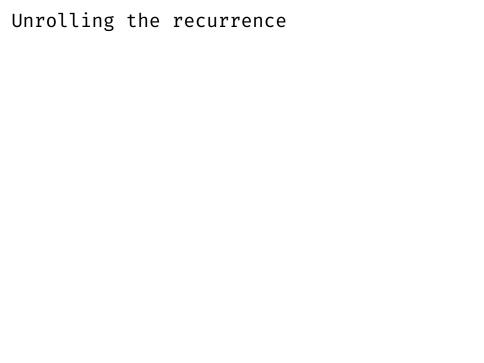
$$\lambda_d(t)g^{(d)}(t) + \dots + \lambda_1(t)g'(t) + \lambda_0(t)g(t) = 0$$

Recurrence

We write $g(t) = g_0 + g_1 t + g_2 t^2 + \cdots$

The differential equation gives:

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$



$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$
$$\begin{pmatrix} g_{n-r+1} & \cdots & g_n \end{pmatrix}^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot \begin{pmatrix} g_0 & \cdots & g_{r-1} \end{pmatrix}^{\mathsf{T}}$$

$$(g_{n-r+1} \cdots g_n)^T = A(n) \cdots A(r+1)A(r) \cdot (g_0 \cdots g_{r-1})^T$$

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$
$$\begin{pmatrix} g_{n-r+1} & \cdots & g_n \end{pmatrix}^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot \begin{pmatrix} g_0 & \cdots & g_{r-1} \end{pmatrix}^{\mathsf{T}}$$

$$(g_{n-r+1} \cdots g_n)^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot (g_0 \cdots g_{r-1})^{\mathsf{T}}$$

Matrix factorial

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$

$$(g_{n-r+1} \quad \cdots \quad g_n)^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot (g_0 \quad \cdots \quad g_{r-1})^{\mathsf{T}}$$

Matrix factorial

To compute $A(n-1)\cdots A(1)A(0)$ (for $n=m^2$)

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$
$$(g_{n-r+1} & \cdots & g_n)^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot (g_0 & \cdots & g_{r-1})^{\mathsf{T}}$$

$$(g_{n-r+1} \quad \cdots \quad g_n)^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot (g_0 \quad \cdots \quad g_{r-1})^{\mathsf{T}}$$

Matrix factorial

To compute $A(n-1)\cdots A(1)A(0)$ [for $n=m^2$]:

① we compute $B(x) = A(mx + m - 1) \cdots A(mx + 1)A(mx)$

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} 1 & & & \\ & & \ddots & \\ & & & 1 \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$

Matrix factorial

To compute $A(n-1)\cdots A(1)A(0)$ [for $n=m^2$]:

① we compute $B(x) = A(mx + m - 1) \cdots A(mx + 1) A(mx)$ divide and conquer: cost $O(m) = O(\sqrt{n})$

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} & & 1 & & & \\ & & \ddots & & \\ & & & 1 \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$

$$(g_{n-r+1} \cdots g_n)^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot (g_0 \cdots g_{r-1})^{\mathsf{T}}$$

Matrix factorial

To compute $A(n-1)\cdots A(1)A(0)$ [for $n=m^2$]:

- ① we compute $B(x) = A(mx+m-1)\cdots A(mx+1)A(mx)$ divide and conquer: cost $O^{\tilde{}}(m) = O^{\tilde{}}(\sqrt{n})$
- ② we compute $B(m-1)\cdots B(1)B(0)$

$$b_0(n)g_n + b_1(n)g_{n-1} + b_2(n)g_{n-2} + \cdots + b_r(n)g_{n-r} = 0$$

Matricial formulation

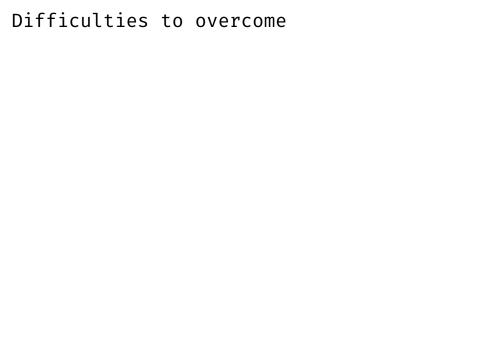
$$A(n) = \frac{-1}{b_0(n)} \begin{pmatrix} & & 1 & & & \\ & & \ddots & & \\ & & & 1 \\ b_r(n) & b_{r-1}(n) & \cdots & b_1(n) \end{pmatrix}$$

$$(g_{n-r+1} \cdots g_n)^{\mathsf{T}} = A(n) \cdots A(r+1)A(r) \cdot (g_0 \cdots g_{r-1})^{\mathsf{T}}$$

Matrix factorial

To compute $A(n-1)\cdots A(1)A(0)$ [for $n=m^2$]:

- ① we compute $B(x) = A(mx+m-1)\cdots A(mx+1)A(mx)$ divide and conquer: cost $O^{\tilde{}}(m) = O^{\tilde{}}(\sqrt{n})$
- ② we compute $B(m-1)\cdots B(1)B(0)$ fast multipoint evaluation: cost $O^{\tilde{}}(m)=O^{\tilde{}}(\sqrt{n})$



lacksquare the denominator $b_0(n)$ vanishes for some n

the denominator $b_0(n)$ vanishes for some n we lift everything in characteristic zero

the denominator $b_0(n)$ vanishes for some n we lift everything in characteristic zero in \mathbb{Z}_p , the ring of p-adic integers

the denominator $b_0(n)$ vanishes for some n we lift everything in characteristic zero in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

 \blacksquare the denominator $b_0(n)$ vanishes for some nwe lift everything in characteristic zero in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

difficult to control the p-adic valuation of $\tilde{b}_0(n)$

the denominator $b_0(n)$ vanishes for some n we lift everything in characteristic zero in \mathbb{Z}_p , the ring of p-adic integers $\tilde{L}_p(n) = \tilde{L}_p(n) = \tilde{L}$

$$\tilde{b}_0(\mathbf{n})\tilde{\mathbf{g}}_{\mathbf{n}} + \tilde{b}_1(\mathbf{n})\tilde{\mathbf{g}}_{\mathbf{n}-1} + \tilde{b}_2(\mathbf{n})\tilde{\mathbf{g}}_{\mathbf{n}-2} + \dots + \tilde{b}_r(\mathbf{n})\tilde{\mathbf{g}}_{\mathbf{n}-r} = 0$$

- difficult to control the p-adic valuation of $b_0(n)$
 - ① we first study the ordinary case

the denominator $b_0(n)$ vanishes for some nwe lift everything in characteristic zero
in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

- difficult to control the p-adic valuation of $ilde{b}_0(n)$
 - ① we first study the ordinary case
 i.e. 0 is an ordinary point of the differential equation

the denominator $b_0(n)$ vanishes for some nwe lift everything in characteristic zero
in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

- difficult to control the p-adic valuation of $\tilde{b}_0(n)$
 - ① we first study the ordinary case
 i.e. 0 is an ordinary point of the differential equation

then:
$$b_0(n) = n(n+1) \cdots (n+r-1)$$

the denominator $b_0(n)$ vanishes for some nwe lift everything in characteristic zero
in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

- difficult to control the p-adic valuation of $\tilde{b}_0(n)$
 - ① we first study the ordinary case
 i.e. 0 is an ordinary point of the differential equation

then:
$$ilde{b}_0(n) = n(n+1)\cdots(n+r-1)$$

② we change the origin

the denominator $b_0(n)$ vanishes for some nwe lift everything in characteristic zero
in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

- lacktriangledown difficult to control the p-adic valuation of $b_0(n)$
 - ① we first study the ordinary case
 i.e. 0 is an ordinary point of the differential equation

then:
$$ilde{b}_0(n) = n(n+1)\cdots(n+r-1)$$

- ② we change the origin
- we need to relate the section operators at 0 and the section operators at another point

the denominator $b_0(n)$ vanishes for some n we lift everything in characteristic zero

in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

- difficult to control the p-adic valuation of $\dot{b}_0(n)$
 - ① we first study the ordinary case
 i.e. 0 is an ordinary point of the differential equation

then:
$$ilde{b}_0(n) = n(n+1)\cdots(n+r-1)$$

- ② we change the origin
- we need to relate the section operators at 0 and the section operators at another point we use (again) the Cartier operator

the denominator $b_0(n)$ vanishes for some n we lift everything in characteristic zero

in \mathbb{Z}_p , the ring of p-adic integers

$$\tilde{b}_0(n)\tilde{g}_n + \tilde{b}_1(n)\tilde{g}_{n-1} + \tilde{b}_2(n)\tilde{g}_{n-2} + \dots + \tilde{b}_r(n)\tilde{g}_{n-r} = 0$$

- difficult to control the p-adic valuation of $ilde{b}_0(n)$
 - ① we first study the ordinary case
 i.e. 0 is an ordinary point of the differential equation

then:
$$\tilde{b}_0(n) = n(n+1)\cdots(n+r-1)$$

- ② we change the origin
- we need to relate the section operators at 0 and the section operators at another point we use (again) the Cartier operator

Conclusion

We get an algorithm with complexity $O^{\tilde{}}(\sqrt{p})$

That's all folks

Thanks for your attention