Fast coefficient computation for algebraic power series in positive characteristic

Alin Bostan
INRIA Saclay

Xavier Caruso
Université Rennes 1

Gilles Christol
Université Paris 6

Philippe Dumas
INRIA Saclay

Algorithmic **N**umber **T**heory **S**ymposium

July 19, 2018

The question we address

The question we address

We want to design an algorithm
with the following specifications

The question we address

We want to design an algorithm
with the following specifications

Input

The question we address

We want to design an algorithm
with the following specifications

Input

① An algebraic power series

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

The question we address

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

The question we address

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

② An integer N

The question we address

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

② An integer N

Output

The question we address

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

② An integer N

Output

The coefficient a_N

Some motivations

Some motivations

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

Some motivations

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

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

Some motivations

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

Some motivations

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

Some motivations

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

Some motivations

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

Our strategy

Our strategy

Christol's Theorem

Our strategy

Christol's Theorem

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$
be an algebraic power series over $\mathbb{F}_p$.

Our strategy

Christol's Theorem

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$
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:

$$S_r\big(c_0 + c_1 t + c_2 t^2 + \cdots\big) = c_r + c_{r+p} t + c_{r+2p} t^2 + \cdots$$

for $0 \leq r < p$

Our strategy

Christol's Theorem

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$
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:

$$S_r\left(c_0 + c_1 t + c_2 t^2 + \cdots\right) = c_r + c_{r+p} t + c_{r+2p} t^2 + \cdots$$

for $0 \leq r < p$

Rough idea behind our algorithms

Our strategy

Christol's Theorem

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$
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:

$$S_r\big(c_0 + c_1 t + c_2 t^2 + \cdots\big) = c_r + c_{r+p} t + c_{r+2p} t^2 + \cdots$$

for $0 \leq r < p$

Rough idea behind our algorithms

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

Our strategy

Christol's Theorem

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$
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:

$$S_r\big(c_0 + c_1 t + c_2 t^2 + \cdots\big) = c_r + c_{r+p} t + c_{r+2p} t^2 + \cdots$$

for $0 \leq r < p$

Rough idea behind our algorithms

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

Our strategy

Christol's Theorem

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$
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:

$$S_r\big(c_0 + c_1 t + c_2 t^2 + \cdots\big) = c_r + c_{r+p} t + c_{r+2p} t^2 + \cdots$$

for $0 \leq r < p$

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

Our strategy

Christol's Theorem

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$
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:

$$S_r\big(c_0 + c_1 t + c_2 t^2 + \cdots\big) = c_r + c_{r+p} t + c_{r+2p} t^2 + \cdots$$

for $0 \leq r < p$

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: $O(\log_p N)$

Effective version of Christol's Theorem

Effective version of Christol's Theorem

Theorem (BC^{2}D, 2018)

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

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

contains f and is stable by the S_r's

Effective version of Christol's Theorem

Theorem (BC^{2}D, 2018)

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

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

contains f and is stable by the S_r's

Ingredients of the proof

Effective version of Christol's Theorem

Theorem (BC^{2}D, 2018)

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

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

contains f and is stable by the S_r's

Ingredients of the proof

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

Effective version of Christol's Theorem

Theorem (BC^{2}D, 2018)

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

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

contains f and is stable by the S_r's

Ingredients of the proof

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

② We prove a commutation relation between residue and section operators

Effective version of Christol's Theorem

Theorem (BC^{2}D, 2018)

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

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

contains f and is stable by the S_r's

Ingredients of the proof

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

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

Effective version of Christol's Theorem

Theorem (BC^{2}D, 2018)

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

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

contains f and is stable by the S_r's

Ingredients of the proof

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

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

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

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

First algorithm

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

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

Inverse the quasi-Toeplitz system

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

Inverse the quasi-Toeplitz system .... $\tilde{O}\left(d^\omega h\right)$

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

Inverse the quasi-Toeplitz system .... $\tilde{O}\left(d^\omega h\right)$

Computation

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

Inverse the quasi-Toeplitz system .... $\tilde{O}\left(d^\omega h\right)$

Computation

Evaluate the left hand side

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

Inverse the quasi-Toeplitz system .... $\tilde{O}\left(d^\omega h\right)$

Computation

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

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

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

Computation

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

Solve the system

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

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

Computation

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

Solve the system .... $O(d^2 h^2)$

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

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

Computation

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

Solve the system .... $O(d^2h^2)$

Total cost

First algorithm

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

Quasi-Toeplitz linear system; displacement rank d

Precomputation

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

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

Computation

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

Solve the system .... $O(d^2h^2)$

Total cost $\tilde{O}(d^2hp + d^{\omega}h) + O(d^2h^2 \log N)$

Acceleration

Acceleration

Why?

Acceleration

Why?

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

Acceleration

Why?

The complexity $\tilde{O}\left(d^2hp + d^\omega h\right) + O\left(d^2h^2 \log N\right)$

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

Acceleration

Why?

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

Observation

Acceleration

Why?

The complexity $\tilde{O}\left(d^2 hp + d^\omega h\right) + O\left(d^2 h^2 \log N\right)$
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

Acceleration

Why?

The complexity $\tilde{O}\left(d^2 hp + d^\omega h\right) + O\left(d^2 h^2 \log N\right)$
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

Acceleration

Why?

The complexity $\tilde{O}\left(d^2 h p + d^\omega h\right) + O\left(d^2 h^2 \log N\right)$
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 $S_r(g(t))$:

Acceleration

Why?

The complexity $\tilde{O}\left(d^2 hp + d^\omega h\right) + O\left(d^2 h^2 \log N\right)$
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 $S_r\big(g(t)\big)$:

① we compute a recurrence on the coefficients of $g(t)$

Acceleration

Why?

The complexity $\tilde{O}\left(d^2 h p + d^\omega h\right) + O\left(d^2 h^2 \log N\right)$

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 $S_r\big(g(t)\big)$:

① we compute a recurrence on the coefficients of $g(t)$

use differential equations

Acceleration

Why?

The complexity $\tilde{O}\left(d^2 hp + d^\omega h\right) + O\left(d^2 h^2 \log N\right)$

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

Acceleration

Why?

The complexity $\tilde{O}\left(d^2 h p + d^\omega h\right) + O\left(d^2 h^2 \log N\right)$

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

Chudnovsky algorithm

Finding a recurrence

Finding a recurrence

Let $g(t)$

Finding a recurrence

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

Finding a recurrence

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

Finding a recurrence

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

Finding a 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

Finding a 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

Finding a 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 $\frac{d}{dt}$

Finding a 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 $E(t, f(t)) = 0$

Finding a 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: $g(t), g'(t), \ldots, g^{(d)}(t)$ are dependent over $k(t)$:

Finding a 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 $k(t)$:

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

Finding a 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: $g(t), g'(t), \ldots, g^{(d)}(t)$ are dependent over $k(t)$:

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

Recurrence

Finding a 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: $g(t), g'(t), \ldots, g^{(d)}(t)$ are dependent over $k(t)$:

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

Recurrence

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

Finding a 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 $k(t)$:

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

Recurrence

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

The differential equation gives:

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

Unrolling the recurrence

Unrolling the recurrence

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

Unrolling the recurrence

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

Matricial formulation

Unrolling the recurrence

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

Matricial formulation

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

Unrolling the recurrence

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

Matricial formulation

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

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

Unrolling the recurrence

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

Matricial formulation

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

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

Matrix factorial

Unrolling the recurrence

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

Matricial formulation

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

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

Matrix factorial

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

Unrolling the recurrence

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

Matricial formulation

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

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

Matrix factorial

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

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

Unrolling the recurrence

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

Matricial formulation

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

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

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 $\tilde{O}(m) = \tilde{O}(\sqrt{n})$

Unrolling the recurrence

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

Matricial formulation

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

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

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 $\tilde{O}(m) = \tilde{O}(\sqrt{n})$

② we compute $B(m-1)\cdots B(1)B(0)$

Unrolling the recurrence

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

Matricial formulation

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

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

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 $\tilde{O}(m) = \tilde{O}(\sqrt{n})$

② we compute $B(m-1) \cdots B(1)B(0)$

fast multipoint evaluation: cost $\tilde{O}(m) = \tilde{O}(\sqrt{n})$

Difficulties to overcome

Difficulties to overcome

- ☞ the denominator $b_0(n)$ vanishes for some n

Difficulties to overcome

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

Difficulties to overcome

☞ 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

Difficulties to overcome

☞ 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

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

Difficulties to overcome

- ☞ 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

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

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

Difficulties to overcome

☞ 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

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

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

① we first study the ordinary case

Difficulties to overcome

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

Difficulties to overcome

- ☞ 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

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

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

Difficulties to overcome

☞ 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

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

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

② we change the origin

Difficulties to overcome

☞ 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

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

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

② we change the origin

☞ we need to relate the section operators at 0 and the section operators at another point

Difficulties to overcome

☞ 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

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

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

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

Difficulties to overcome

☞ 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

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

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

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 $\tilde{O}(\sqrt{p})$

That's all folks

Thanks for your attention