

Solving p -adic matrix differential equations

Hendrik Hubrechts

Katholieke Universiteit Leuven (Belgium)

Foundations of Computational Mathematics 2008
City University of Hong Kong

June 24, 2008

Outline

Number of rational points

Deformation and differential equation

Two deformation strategies

Strategies for the differential equation

Solving p -adic
matrix differential
equations

**Hendrik
Hubrechts**

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Outline

Number of rational points

Deformation and differential equation

Two deformation strategies

Strategies for the differential equation

Solving p -adic
matrix differential
equations

**Hendrik
Hubrechts**

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Outline

Number of rational points

Deformation and differential equation

Two deformation strategies

Strategies for the differential equation

Solving p -adic
matrix differential
equations

**Hendrik
Hubrechts**

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Outline

Number of rational points

Deformation and differential equation

Two deformation strategies

Strategies for the differential equation

Solving p -adic
matrix differential
equations

**Hendrik
Hubrechts**

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Curves

Solving p -adic
matrix differential
equations

Hendrik
Hubrechts

Definition

Prime number p , field \mathbb{F}_{p^n} . A *hyperelliptic curve* (HEC) \mathcal{C} over \mathbb{F}_{p^n} of genus g has non-singular affine part ($p \geq 3$)

$$\mathcal{C} \longleftrightarrow y^2 = \bar{Q}(x), \quad \bar{Q}(x) = x^{2g+1} + a_{2g}x^{2g} + \dots \in \mathbb{F}_{p^n}[x].$$

For $(a, b) = 1$, a $C_{a,b}$ -curve has equation $y^a + \bar{c}x^b + f(x, y) = 0$, with some conditions.

Associated to \mathcal{C} is its **Jacobian** $\text{Jac}(\mathcal{C})$, a g -dim. abelian variety.

Cryptographers are interested in Jacobians for their (assumed) hard discrete logarithm problem. However, they need to know $\#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n})$ for security reasons.

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Weil zeta function

Strong relationship between $\#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n})$ and $\#\mathcal{C}/\mathbb{F}_{p^n}$.

Definition

The zeta function of $\mathcal{C}/\mathbb{F}_{p^n}$ is given by

$$Z(\mathcal{C}/\mathbb{F}_{p^n}; T) := \exp \left(\sum_{k=1}^{\infty} \frac{\#\mathcal{C}/\mathbb{F}_{(p^n)^k}}{k} T^k \right).$$

Theorem

$$Z(\mathcal{C}/\mathbb{F}_{p^n}; T) = \frac{P_1(T)}{(1-T)(1-pT)}, \quad P_1(T) = p^n T^{2g} + \dots + 1.$$

Theorem

$$\#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n}) = P_1(1).$$

Conclusion: computing zeta function \Rightarrow pointcounting on \mathcal{C} and $\text{Jac}(\mathcal{C})$.

Some point counting algorithms (small primes)

Let \mathcal{C} be a HEC over \mathbb{F}_{p^n} , prime p 'small'.

	Time (bit op)	Space (bits)
Naive	$\geq \tilde{\mathcal{O}}(gp^n)$	$\geq \mathcal{O}(gn)$
Kedlaya ($p \geq 3$)	$\tilde{\mathcal{O}}(g^4 n^3)$	$\mathcal{O}(g^3 n^3)$
Denef-Vercauteren ($p = 2$)	$\tilde{\mathcal{O}}(g^5 n^3)$	$\mathcal{O}(g^4 n^3)$
Lercier-Lubicz ($p = 2$)	$\tilde{\mathcal{O}}(2^g n^2)$	
— ($p \geq 3$)	$\tilde{\mathcal{O}}(g^{4+\omega} n^3)$	$\mathcal{O}(g^4 n^2)$
— ($p = 2$)	$\tilde{\mathcal{O}}(g^{7+\omega} n^3)$	$\mathcal{O}(g^5 n^2)$

Monksy-Washnitzer cohomology

\mathbb{Q}_p = p -adic numbers; \mathbb{Q}_{p^n} = degree n unramified extension.

We define *overconvergent power series*

$$\mathbb{Q}_{p^n}[x]^\dagger := \left\{ \sum_{i \geq 0} a_i x^i \mid \text{converges for } |x|_p < 1 + \epsilon \right\}.$$

Definition

Let $\bar{f}(x, y) = 0$ define an \mathbb{F}_{p^n} -variety \mathcal{C} , with *rigid lift* $f(x, y) \in \mathbb{Z}_{p^n}[x, y]$. With $A^\dagger := \mathbb{Q}_{p^n}[x, y]^\dagger / f(x, y)$, the

Monksy-Washnitzer cohomology of \mathcal{C} is

$H_{MW} := \Omega^1(A^\dagger) / dA^\dagger$, the de Rham cohomology of A^\dagger .

Property H_{MW} is a finite dimensional \mathbb{Q}_{p^n} -vector space.

Property On A^\dagger and H_{MW} we have a Frobenius operator F_{p^n} that carries information on the number of points.

Solving p -adic
matrix differential
equations

Hendrik
Hübrechts

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Monksy-Washnitzer cohomology

\mathbb{Q}_p = p -adic numbers; \mathbb{Q}_{p^n} = degree n unramified extension.

We define *overconvergent power series*

$$\mathbb{Q}_{p^n}[x]^\dagger := \left\{ \sum_{i \geq 0} a_i x^i \mid \text{converges for } |x|_p < 1 + \epsilon \right\}.$$

Definition

Let $\bar{f}(x, y) = 0$ define an \mathbb{F}_{p^n} -variety \mathcal{C} , with *rigid lift* $f(x, y) \in \mathbb{Z}_{p^n}[x, y]$. With $A^\dagger := \mathbb{Q}_{p^n}[x, y]^\dagger / f(x, y)$, the

Monksy-Washnitzer cohomology of \mathcal{C} is

$H_{MW} := \Omega^1(A^\dagger) / dA^\dagger$, the de Rham cohomology of A^\dagger .

Property H_{MW} is a finite dimensional \mathbb{Q}_{p^n} -vector space.

Property On A^\dagger and H_{MW} we have a Frobenius operator F_{p^n} that carries information on the number of points.

Solving p -adic
matrix differential
equations

Hendrik
Hübrechts

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Monksy-Washnitzer cohomology

\mathbb{Q}_p = p -adic numbers; \mathbb{Q}_{p^n} = degree n unramified extension.

We define *overconvergent power series*

$$\mathbb{Q}_{p^n}[x]^\dagger := \left\{ \sum_{i \geq 0} a_i x^i \mid \text{converges for } |x|_p < 1 + \epsilon \right\}.$$

Definition

Let $\bar{f}(x, y) = 0$ define an \mathbb{F}_{p^n} -variety \mathcal{C} , with *rigid lift* $f(x, y) \in \mathbb{Z}_{p^n}[x, y]$. With $A^\dagger := \mathbb{Q}_{p^n}[x, y]^\dagger / f(x, y)$, the

Monksy-Washnitzer cohomology of \mathcal{C} is

$H_{MW} := \Omega^1(A^\dagger) / dA^\dagger$, the de Rham cohomology of A^\dagger .

Property H_{MW} is a finite dimensional \mathbb{Q}_{p^n} -vector space.

Property On A^\dagger and H_{MW} we have a Frobenius operator F_{p^n} that carries information on the number of points.

Solving p -adic
matrix differential
equations

Hendrik
Hübrechts

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Kedlaya's algorithm

Recall $\mathcal{C} \leftrightarrow y^2 = \bar{Q}(x)$. Take rigid lift $y^2 = Q(x)$ over \mathbb{Z}_{p^n} , remove Weierstrass points ($y = 0$), then

$$A^\dagger = \frac{\mathbb{Q}_{p^n}[x, y, y^{-1}]^\dagger}{y^2 - Q(x)}, \quad H_{MW} = \frac{\Omega^1(A^\dagger)}{dA^\dagger};$$

2g-dimensional subspace $H_{MW}^- \subseteq H_{MW}$.

Property

$$\det \left(1 - \text{Matrix}(F_{p^n} |_{H_{MW}^-}) \right) = \#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n}).$$

1. Factor $F_{p^n} = (F_p)^n \Rightarrow$ much better 'convergence'.
2. Make reduction in H_{MW}^- and computation of F_p explicit.

Kedlaya's algorithm

Recall $\mathcal{C} \leftrightarrow y^2 = \bar{Q}(x)$. Take rigid lift $y^2 = Q(x)$ over \mathbb{Z}_{p^n} , remove Weierstrass points ($y = 0$), then

$$A^\dagger = \frac{\mathbb{Q}_{p^n}[x, y, y^{-1}]^\dagger}{y^2 - Q(x)}, \quad H_{MW} = \frac{\Omega^1(A^\dagger)}{dA^\dagger};$$

2g-dimensional subspace $H_{MW}^- \subseteq H_{MW}$.

Property

$$\det \left(1 - \text{Matrix}(F_{p^n} |_{H_{MW}^-}) \right) = \#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n}).$$

1. Factor $F_{p^n} = (F_p)^n \Rightarrow$ much better 'convergence'.
2. Make reduction in H_{MW}^- and computation of F_p explicit.

Kedlaya's algorithm

Recall $\mathcal{C} \leftrightarrow y^2 = \bar{Q}(x)$. Take rigid lift $y^2 = Q(x)$ over \mathbb{Z}_{p^n} , remove Weierstrass points ($y = 0$), then

$$A^\dagger = \frac{\mathbb{Q}_{p^n}[x, y, y^{-1}]^\dagger}{y^2 - Q(x)}, \quad H_{MW} = \frac{\Omega^1(A^\dagger)}{dA^\dagger};$$

2g-dimensional subspace $H_{MW}^- \subseteq H_{MW}$.

Property

$$\det \left(1 - \text{Matrix}(F_{p^n} |_{H_{MW}^-}) \right) = \#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n}).$$

1. Factor $F_{p^n} = (F_p)^n \Rightarrow$ much better 'convergence'.
2. Make reduction in H_{MW}^- and computation of F_p explicit.

Deformation of hyperelliptic curves

Family $\mathcal{C}_\Gamma \leftrightarrow y^2 = \bar{Q}(x, \Gamma)$, with $\bar{Q} \in \mathbb{F}_{p^a}[x, \Gamma]$ monic of degree $2g + 1$ in x . (note: a vs. n : more freedom)

For almost all $\bar{\gamma} \in \mathbb{F}_{(p^a)^n}$: $\mathcal{C}_{\bar{\gamma}}$ is HEC of genus g .

Bad fibers: affine $\mathcal{C}_{\bar{\gamma}}$ is singular $\Leftrightarrow \bar{Q}(x, \bar{\gamma})$ has double root
 $\Leftrightarrow \bar{r}(\Gamma) := \text{Res}_x(\bar{Q}, \frac{\partial}{\partial x} \bar{Q})$ and $\bar{r}(\bar{\gamma}) = 0$.

For $p = 2$ and $C_{a,b}$ -curves: similar.

Main idea of how to proceed: consider MW-cohomology for family as a whole.

First use: Dwork, algorithmic: Lauder.

Solving p -adic
matrix differential
equations

Hendrik
Hubrechts

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Deformation of hyperelliptic curves

Family $\mathcal{C}_\Gamma \leftrightarrow y^2 = \bar{Q}(x, \Gamma)$, with $\bar{Q} \in \mathbb{F}_{p^a}[x, \Gamma]$ monic of degree $2g + 1$ in x . (note: a vs. n : more freedom)

For almost all $\bar{\gamma} \in \mathbb{F}_{(p^a)^n}$: $\mathcal{C}_{\bar{\gamma}}$ is HEC of genus g .

Bad fibers: affine $\mathcal{C}_{\bar{\gamma}}$ is singular $\Leftrightarrow \bar{Q}(x, \bar{\gamma})$ has double root
 $\Leftrightarrow \bar{r}(\Gamma) := \text{Res}_x(\bar{Q}, \frac{\partial}{\partial x} \bar{Q})$ and $\bar{r}(\bar{\gamma}) = 0$.

For $p = 2$ and $C_{a,b}$ -curves: similar.

Main idea of how to proceed: consider MW-cohomology for family as a whole.

First use: Dwork, algorithmic: Lauder.

Solving p -adic
matrix differential
equations

Hendrik
Hubrechts

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Deformation of hyperelliptic curves

Family $\mathcal{C}_\Gamma \leftrightarrow y^2 = \bar{Q}(x, \Gamma)$, with $\bar{Q} \in \mathbb{F}_{p^a}[x, \Gamma]$ monic of degree $2g + 1$ in x . (note: a vs. n : more freedom)

For almost all $\bar{\gamma} \in \mathbb{F}_{(p^a)^n}$: $\mathcal{C}_{\bar{\gamma}}$ is HEC of genus g .

Bad fibers: affine $\mathcal{C}_{\bar{\gamma}}$ is singular $\Leftrightarrow \bar{Q}(x, \bar{\gamma})$ has double root
 $\Leftrightarrow \bar{r}(\Gamma) := \text{Res}_x(\bar{Q}, \frac{\partial}{\partial x} \bar{Q})$ and $\bar{r}(\bar{\gamma}) = 0$.

For $p = 2$ and $C_{a,b}$ -curves: similar.

Main idea of how to proceed: consider MW-cohomology for family as a whole.

First use: Dwork, algorithmic: Lauder.

Deformation in practice (I)

Consider family $y^2 = Q(x, \Gamma)$ over \mathbb{Z}_{p^a} and define $r(\Gamma) := \text{Res}_x(Q, \frac{\partial}{\partial x} Q)$,

$$A_{\Gamma}^{\dagger} := \frac{\mathbb{Q}_{p^a}[x, y, y^{-1}, \Gamma, r(\Gamma)^{-1}]^{\dagger}}{y^2 - Q(x, \Gamma)}.$$

This is a module over $S^{\dagger} := \mathbb{Q}_{p^a}[\Gamma, r(\Gamma)^{-1}]^{\dagger}$.

Let $d : A_{\Gamma}^{\dagger} \rightarrow A_{\Gamma}^{\dagger} dx$ be the differential operator such that $d(\Gamma) = 0$, and define

$$H_{MW}(\Gamma) := \frac{A_{\Gamma}^{\dagger} dx}{dA_{\Gamma}^{\dagger}}, \quad H_{MW}^{-}(\Gamma) \subseteq H_{MW}(\Gamma).$$

Theorem

$H_{MW}^{-}(\Gamma)$ is a free S^{\dagger} -module of rank $2g$.

Deformation in practice (I)

Consider family $y^2 = Q(x, \Gamma)$ over \mathbb{Z}_{p^a} and define $r(\Gamma) := \text{Res}_x(Q, \frac{\partial}{\partial x} Q)$,

$$A_{\Gamma}^{\dagger} := \frac{\mathbb{Q}_{p^a}[x, y, y^{-1}, \Gamma, r(\Gamma)^{-1}]^{\dagger}}{y^2 - Q(x, \Gamma)}.$$

This is a module over $S^{\dagger} := \mathbb{Q}_{p^a}[\Gamma, r(\Gamma)^{-1}]^{\dagger}$.

Let $d : A_{\Gamma}^{\dagger} \rightarrow A_{\Gamma}^{\dagger} dx$ be the differential operator such that $d(\Gamma) = 0$, and define

$$H_{MW}(\Gamma) := \frac{A_{\Gamma}^{\dagger} dx}{dA_{\Gamma}^{\dagger}}, \quad H_{MW}^{-}(\Gamma) \subseteq H_{MW}(\Gamma).$$

Theorem

$H_{MW}^{-}(\Gamma)$ is a free S^{\dagger} -module of rank $2g$.

Deformation in practice (II)

We have a free S^\dagger -module $H_{MW}^-(\Gamma)$ of rank $2g$.

- ▶ p th power Frobenius F_p on H_{MW}^- : $x \mapsto x^p, \Gamma \mapsto \Gamma^p$.
- ▶ Connection ∇ on H_{MW}^- : $t \mapsto \frac{\partial t}{\partial \Gamma} d\Gamma$.
- ▶ **Property** $F_p \circ \nabla = \nabla \circ F_p$.

Fix S^\dagger -basis for $H_{MW}^-(\Gamma)$, matrices $F(\Gamma)$ for F_p , $G(\Gamma)$ for ∇ .

Proposition $\gamma \in \mathbb{Z}_{(p^a)^n}$ s.t. $\gamma^\sigma = \gamma^p \Rightarrow F(\gamma)$ is à la Kedlaya.

$\sigma : \mathbb{Q}_{p^{an}} \rightarrow \mathbb{Q}_{p^{an}}$ is the Frobenius automorphism, γ is a *Teichmüller lift*.

Proposition $F_p \circ \nabla = \nabla \circ F_p \Rightarrow$

$$\frac{\partial}{\partial \Gamma} F(\Gamma) + F(\Gamma) \cdot G(\Gamma) = p\Gamma^{p-1} \cdot G^\sigma(\Gamma^p) \cdot F(\Gamma).$$

Corollary $G(\Gamma)$, $F(0)$ and differential equation $\Rightarrow F(\Gamma)$.

Deformation in practice (II)

We have a free S^\dagger -module $H_{MW}^-(\Gamma)$ of rank $2g$.

- ▶ p th power Frobenius F_p on H_{MW}^- : $x \mapsto x^p, \Gamma \mapsto \Gamma^p$.
- ▶ Connection ∇ on H_{MW}^- : $t \mapsto \frac{\partial t}{\partial \Gamma} d\Gamma$.
- ▶ **Property** $F_p \circ \nabla = \nabla \circ F_p$.

Fix S^\dagger -basis for $H_{MW}^-(\Gamma)$, matrices $F(\Gamma)$ for F_p , $G(\Gamma)$ for ∇ .

Proposition $\gamma \in \mathbb{Z}_{(p^a)^n}$ s.t. $\gamma^\sigma = \gamma^p \Rightarrow F(\gamma)$ is à la Kedlaya.

$\sigma : \mathbb{Q}_{p^{an}} \rightarrow \mathbb{Q}_{p^{an}}$ is the Frobenius automorphism, γ is a *Teichmüller lift*.

Proposition $F_p \circ \nabla = \nabla \circ F_p \Rightarrow$

$$\frac{\partial}{\partial \Gamma} F(\Gamma) + F(\Gamma) \cdot G(\Gamma) = p\Gamma^{p-1} \cdot G^\sigma(\Gamma^p) \cdot F(\Gamma).$$

Corollary $G(\Gamma), F(0)$ and differential equation $\Rightarrow F(\Gamma)$.

Deformation in practice (II)

We have a free S^\dagger -module $H_{MW}^-(\Gamma)$ of rank $2g$.

- ▶ p th power Frobenius F_p on H_{MW}^- : $x \mapsto x^p, \Gamma \mapsto \Gamma^p$.
- ▶ Connection ∇ on H_{MW}^- : $t \mapsto \frac{\partial t}{\partial \Gamma} d\Gamma$.
- ▶ **Property** $F_p \circ \nabla = \nabla \circ F_p$.

Fix S^\dagger -basis for $H_{MW}^-(\Gamma)$, matrices $F(\Gamma)$ for F_p , $G(\Gamma)$ for ∇ .

Proposition $\gamma \in \mathbb{Z}_{(p^a)^n}$ s.t. $\gamma^\sigma = \gamma^p \Rightarrow F(\gamma)$ is à la Kedlaya.

$\sigma : \mathbb{Q}_{p^{an}} \rightarrow \mathbb{Q}_{p^{an}}$ is the Frobenius automorphism, γ is a *Teichmüller lift*.

Proposition $F_p \circ \nabla = \nabla \circ F_p \Rightarrow$

$$\frac{\partial}{\partial \Gamma} F(\Gamma) + F(\Gamma) \cdot G(\Gamma) = p\Gamma^{p-1} \cdot G^\sigma(\Gamma^p) \cdot F(\Gamma).$$

Corollary $G(\Gamma), F(0)$ and differential equation $\Rightarrow F(\Gamma)$.

The 'generic' Frobenius matrix

Structure of $2g \times 2g$ -matrix $F(\Gamma)$? Let $\alpha(\Gamma)$ be an entry.

$$\alpha \in S^\dagger = \mathbb{Q}_p^a[\Gamma, r(\Gamma)^{-1}]^\dagger \Rightarrow$$

$$\alpha = \sum_{i=0}^{\infty} a_i \Gamma^i + \sum_{i=1}^{\infty} \frac{b_i(\Gamma)}{r(\Gamma)^i}, \text{ with } \deg b_i < \deg r \text{ and}$$

1. $\liminf_i \frac{\text{ord}_p(a_i, b_i)}{i} > 0 \Leftrightarrow$
2. $\exists \varepsilon > 0$ s.t. $\forall i \gg 0: \text{ord}_p(a_i, b_i) \geq \varepsilon \cdot i \Leftrightarrow$
3. \exists (computable) $C, \forall M \gg 0:$

$$\alpha \equiv \sum_{i=0}^{C \cdot M} a_i \Gamma^i + \sum_{i=1}^{C \cdot M} \frac{b_i(\Gamma)}{r(\Gamma)^i} \text{ modulo } p^M.$$

The 'generic' Frobenius matrix

Structure of $2g \times 2g$ -matrix $F(\Gamma)$? Let $\alpha(\Gamma)$ be an entry.

$$\alpha \in S^\dagger = \mathbb{Q}_p^a[\Gamma, r(\Gamma)^{-1}]^\dagger \Rightarrow$$

$$\alpha = \sum_{i=0}^{\infty} a_i \Gamma^i + \sum_{i=1}^{\infty} \frac{b_i(\Gamma)}{r(\Gamma)^i}, \text{ with } \deg b_i < \deg r \text{ and}$$

1. $\liminf_i \frac{\text{ord}_p(a_i, b_i)}{i} > 0 \Leftrightarrow$
2. $\exists \varepsilon > 0$ s.t. $\forall i \gg 0: \text{ord}_p(a_i, b_i) \geq \varepsilon \cdot i \Leftrightarrow$
3. \exists (computable) $C, \forall M \gg 0:$

$$\alpha \equiv \sum_{i=0}^{C \cdot M} a_i \Gamma^i + \sum_{i=1}^{C \cdot M} \frac{b_i(\Gamma)}{r(\Gamma)^i} \text{ modulo } p^M.$$

A general differential equation

In all cases ($p = 2$, $p \geq 3$, $C_{a,b}$) the differential equation reads

$$A(\Gamma) \cdot \frac{\partial}{\partial \Gamma} F(\Gamma) \cdot B(\Gamma) = X(\Gamma) \cdot F(\Gamma) \cdot B(\Gamma) + A(\Gamma) \cdot F(\Gamma) \cdot Y(\Gamma).$$

- ▶ $A, B, X, Y \in \mathbb{Q}_{p^a}[\Gamma]$ have 'low' degree and good valuation.
- ▶ $A_0 = A(0)$ and B_0 are invertible.
- ▶ The boundary condition F_0 is assumed to be known.
- ▶ $F(\Gamma)$ converges as explained above.

GOAL. Solution $F(\gamma)$ with $\gamma \in \mathbb{Q}_{p^{an}}$ s.t. $\gamma^{p^{an}} = \gamma$ or $\gamma^p = \gamma^\sigma$ (Teichmüller lift), all with p -adic precision $M \approx n$.

Strategy I - Families defined over small fields

Take **small** a , $\bar{Q}(x, \Gamma) \in \mathbb{F}_{p^a}[x, \Gamma]$, large n and $\bar{\gamma} \in \mathbb{F}_{p^{an}}$.

Goal: curve $\mathcal{C} \leftrightarrow y^2 = \bar{Q}(x, \bar{\gamma})$.

- ▶ Lift \bar{Q} to $Q(x, \Gamma) \in \mathbb{Z}_{p^a}[x, \Gamma]$, compute diff. eq.
- ▶ Compute $F(\Gamma)$ from diff. eq. (see later).
- ▶ Compute $\mathbb{Q}_{p^{an}} = \frac{\mathbb{Q}_{p^a}[x]}{\varphi(x)}$ s.t. $\bar{x} = \bar{\gamma}$ and $x^\sigma = x$.
- ▶ Rewrite $F := F(\gamma) = F(x) \pmod{\varphi(x)}$ (\pm , see later)
- ▶ Compute $F_{p^{an}}(\gamma) = F^{\sigma^{an-1}} \cdot F^{\sigma^{an-2}} \dots F^\sigma \cdot F$.
- ▶ $\#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^{an}}) = \det(1 - F_{p^n}(\gamma))$.

Theorem $\#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^{an}})$ can (here) be computed in time $\tilde{O}(g^{4+\omega} n^{2.667})$ and space $\mathcal{O}(g^5 n^{2.5})$. With recent result of Kedlaya-Umans: time $\tilde{O}(g^{4+\omega} n^2)$ and space $\mathcal{O}(g^5 n^2)$.

Strategy II - General curves

Given is **any HEC** $\bar{C}'_1 \leftrightarrow y^2 = \bar{Q}_1(x)$ over \mathbb{F}_{p^n} .

Define

$$\bar{C}'_0/\mathbb{F}_p \leftrightarrow y^2 = \bar{Q}_0(x) := \begin{cases} x^{2g+1} + 1 & \text{if } p \nmid 2g + 1, \\ x^{2g+1} + x & \text{else.} \end{cases}$$

We 'deform' \bar{C}'_1 to \bar{C}'_0 :

$$\bar{C}_\Gamma \leftrightarrow y^2 = \bar{Q}(x, \Gamma) := (\bar{Q}_1 - \bar{Q}_0)\Gamma + \bar{Q}_0.$$

Then $\bar{C}_0 = \bar{C}'_0$ and $\bar{C}_1 = \bar{C}'_1$, and we can work as before.

Note \bar{C}_0 is defined over \mathbb{F}_p , and hence 'easy'.

Characteristic 2 and $C_{a,b}$ -curves: similar but more complicated results.

Strategy II - General curves

Given is **any HEC** $\bar{C}'_1 \leftrightarrow y^2 = \bar{Q}_1(x)$ over \mathbb{F}_{p^n} .

Define

$$\bar{C}'_0/\mathbb{F}_p \leftrightarrow y^2 = \bar{Q}_0(x) := \begin{cases} x^{2g+1} + 1 & \text{if } p \nmid 2g + 1, \\ x^{2g+1} + x & \text{else.} \end{cases}$$

We 'deform' \bar{C}'_1 to \bar{C}'_0 :

$$\bar{C}_\Gamma \leftrightarrow y^2 = \bar{Q}(x, \Gamma) := (\bar{Q}_1 - \bar{Q}_0)\Gamma + \bar{Q}_0.$$

Then $\bar{C}_0 = \bar{C}'_0$ and $\bar{C}_1 = \bar{C}'_1$, and we can work as before.

Note \bar{C}_0 is defined over \mathbb{F}_p , and hence 'easy'.

Characteristic 2 and $C_{a,b}$ -curves: similar but more complicated results.

Strategy II - General curves

Given is **any HEC** $\bar{C}'_1 \leftrightarrow y^2 = \bar{Q}_1(x)$ over \mathbb{F}_{p^n} .

Define

$$\bar{C}'_0/\mathbb{F}_p \leftrightarrow y^2 = \bar{Q}_0(x) := \begin{cases} x^{2g+1} + 1 & \text{if } p \nmid 2g + 1, \\ x^{2g+1} + x & \text{else.} \end{cases}$$

We 'deform' \bar{C}'_1 to \bar{C}'_0 :

$$\bar{C}_\Gamma \leftrightarrow y^2 = \bar{Q}(x, \Gamma) := (\bar{Q}_1 - \bar{Q}_0)\Gamma + \bar{Q}_0.$$

Then $\bar{C}_0 = \bar{C}'_0$ and $\bar{C}_1 = \bar{C}'_1$, and we can work as before.

Note \bar{C}_0 is defined over \mathbb{F}_p , and hence 'easy'.

Characteristic 2 and $C_{a,b}$ -curves: similar but more complicated results.

What do we want to compute?

Recall: general (matrix) differential equation

$$A(\Gamma) \cdot \frac{\partial}{\partial \Gamma} F(\Gamma) \cdot B(\Gamma) = X(\Gamma) \cdot F(\Gamma) \cdot B(\Gamma) + A(\Gamma) \cdot F(\Gamma) \cdot Y(\Gamma). \quad (1)$$

We know A, B, X, Y, F_0 ; and A_0, B_0 are invertible.

Goal: $F(\gamma)$ for some Teichmüller lift $\gamma \in \mathbb{Q}_p^n$ (often $\gamma = 1$).

Note We can compute enough F_i of $F(\Gamma) = \sum_i F_i \Gamma^i$, but $\sum_i F_i \gamma^i$ does not converge. However,

$$F(\Gamma) \equiv \sum_{i=0}^{C \cdot M} a_i \Gamma^i + \sum_{i=1}^{C \cdot M} \frac{b_i(\Gamma)}{r(\Gamma)^i} \pmod{p^M} \Rightarrow$$

$r(\Gamma)^{C \cdot M} \cdot F(\Gamma) \pmod{p^M}$ is a polynomial (of bounded degree).

Hence $F(\gamma) \equiv r(\gamma)^{-C \cdot M} \cdot [r(\Gamma)^{C \cdot M} \cdot F(\Gamma)]_{|\Gamma=\gamma} \pmod{p^M}$.

What do we want to compute?

Recall: general (matrix) differential equation

$$A(\Gamma) \cdot \frac{\partial}{\partial \Gamma} F(\Gamma) \cdot B(\Gamma) = X(\Gamma) \cdot F(\Gamma) \cdot B(\Gamma) + A(\Gamma) \cdot F(\Gamma) \cdot Y(\Gamma). \quad (1)$$

We know A, B, X, Y, F_0 ; and A_0, B_0 are invertible.

Goal: $F(\gamma)$ for some Teichmüller lift $\gamma \in \mathbb{Q}_p^n$ (often $\gamma = 1$).

Note We can compute enough F_i of $F(\Gamma) = \sum_i F_i \Gamma^i$, but $\sum_i F_i \gamma^i$ does not converge. However,

$$F(\Gamma) \equiv \sum_{i=0}^{C \cdot M} a_i \Gamma^i + \sum_{i=1}^{C \cdot M} \frac{b_i(\Gamma)}{r(\Gamma)^i} \pmod{p^M} \Rightarrow$$

$r(\Gamma)^{C \cdot M} \cdot F(\Gamma) \pmod{p^M}$ is a polynomial (of bounded degree).

Hence $F(\gamma) \equiv r(\gamma)^{-C \cdot M} \cdot [r(\Gamma)^{C \cdot M} \cdot F(\Gamma)]_{|\Gamma=\gamma} \pmod{p^M}$.

1. Local solutions (over \mathbb{Q}_p^a , a small)

Similar to 'homogenous' and 'particular' solutions when solving linear differential equations. Compute $C(\Gamma)$, $D(\Gamma)$:

$$A \cdot \frac{\partial}{\partial \Gamma} C = X \cdot C, \quad C(0) = 1; \quad \frac{\partial}{\partial \Gamma} D \cdot B = D \cdot Y, \quad D(0) = 1.$$

Then $F(\Gamma) := C(\Gamma) \cdot F_0 \cdot D(\Gamma)$ satisfies the diff. eq. (1).

How to solve $A \cdot \frac{\partial}{\partial \Gamma} C = X \cdot C$? Expand $C(\Gamma) = \sum C_i \Gamma^i$, then

$$\text{Coeff. of } \Gamma^0: \quad A_0 C_1 = X_0 C_0 \quad \Rightarrow \quad C_1 = A_0^{-1} X_0 C_0,$$

$$\text{Coeff. of } \Gamma^1: \quad 2A_0 C_2 + A_1 C_1 = X_0 C_1 + X_1 C_0 \quad \Rightarrow \quad C_2 = \frac{1}{2} A_0^{-1} (\dots),$$

$$\text{Coeff. of } \Gamma^{k-1} \quad \Rightarrow \quad C_k = \frac{1}{k} A_0^{-1} (\dots).$$

Note Valuations of C_k are 'reasonable': $\text{ord}_p(C_k) \approx -\log k$.

Finish with $r(\gamma)^{-C \cdot M} [r(\Gamma)^{C \cdot M} \cdot F(\Gamma)]|_{\Gamma=\gamma}$.

1. Local solutions (over \mathbb{Q}_p^a , a small)

Similar to 'homogenous' and 'particular' solutions when solving linear differential equations. Compute $C(\Gamma)$, $D(\Gamma)$:

$$A \cdot \frac{\partial}{\partial \Gamma} C = X \cdot C, \quad C(0) = 1; \quad \frac{\partial}{\partial \Gamma} D \cdot B = D \cdot Y, \quad D(0) = 1.$$

Then $F(\Gamma) := C(\Gamma) \cdot F_0 \cdot D(\Gamma)$ satisfies the diff. eq. (1).

How to solve $A \cdot \frac{\partial}{\partial \Gamma} C = X \cdot C$? Expand $C(\Gamma) = \sum C_i \Gamma^i$, then

$$\begin{aligned} \text{Coeff. of } \Gamma^0: & \quad A_0 C_1 = X_0 C_0 \quad \Rightarrow \quad C_1 = A_0^{-1} X_0 C_0, \\ \text{Coeff. of } \Gamma^1: & \quad 2A_0 C_2 + A_1 C_1 = X_0 C_1 + X_1 C_0 \quad \Rightarrow \quad C_2 = \frac{1}{2} A_0^{-1} (\dots), \\ \text{Coeff. of } \Gamma^{k-1}: & \quad \Rightarrow \quad C_k = \frac{1}{k} A_0^{-1} (\dots). \end{aligned}$$

Note Valuations of C_k are 'reasonable': $\text{ord}_p(C_k) \approx -\log k$.

Finish with $r(\gamma)^{-C \cdot M} [r(\Gamma)^{C \cdot M} \cdot F(\Gamma)]|_{\Gamma=\gamma}$.

2. Unknown coefficients (over \mathbb{Q}_p^a , a small)

Similar to the previous method, but with complete equation:

$$A_0 F_1 B_0 = X_0 F_0 B_0 + A_0 F_0 Y_0 \Rightarrow F_1 = A_0^{-1}(\dots) B_0^{-1},$$

in general this becomes

$$F_k = \frac{1}{k} A_0^{-1}(\dots) B_0^{-1}.$$

Theorem The introduced errors (i.e. the difference between the *computed* $F_k \bmod p^M$ and the *real* $F_k \bmod p^M$) are small (valuation $\approx M - \log k$).

3. Rewriting the equation

We always had to compute $r(\Gamma)^{C \cdot M} \cdot F(\Gamma)$, a product of very large polynomials, which is extremely slow in practice.

Solution: Define $K(\Gamma) := r(\Gamma)^{C \cdot M} F(\Gamma)$, and plug this in the differential equation (1):

$$(rA) \frac{\partial}{\partial \Gamma} KB = \left(rX + M \frac{\partial r}{\partial \Gamma} A \right) KB + (rA) KY.$$

Work as before modulo p^M , but now $K_k \bmod p^M$ will become zero for $k \gg 0$.

Finish with $F(\gamma) = r(\gamma)^{-C \cdot M} K(\gamma)$.

Note Theoretical complexities are not altered by this method. In practice, more than just (a lot of) speed is gained: we can check convergence 'at run-time'.

3. Rewriting the equation

We always had to compute $r(\Gamma)^{C \cdot M} \cdot F(\Gamma)$, a product of very large polynomials, which is extremely slow in practice.

Solution: Define $K(\Gamma) := r(\Gamma)^{C \cdot M} F(\Gamma)$, and plug this in the differential equation (1):

$$(rA) \frac{\partial}{\partial \Gamma} KB = \left(rX + M \frac{\partial r}{\partial \Gamma} A \right) KB + (rA) KY.$$

Work as before modulo p^M , but now $K_k \bmod p^M$ will become zero for $k \gg 0$.

Finish with $F(\gamma) = r(\gamma)^{-C \cdot M} K(\gamma)$.

Note Theoretical complexities are not altered by this method. In practice, more than just (a lot of) speed is gained: we can check convergence 'at run-time'.

4. Avoiding complete storage (over \mathbb{Q}_p^n , n large)

For general HEC's, the differential equation is defined over \mathbb{Q}_p^n for some large n , and we work modulo p^M , $M \approx n$.

The size of $F(\Gamma) \bmod p^M$ is hence $\mathcal{O}(n^3) \Rightarrow$ **storing $F(\Gamma)$ is costly.**

We need only $F(1) = \sum F_i$, therefore: **sliding windows technique.** Recall $F(1) = r(1)^{-C \cdot M} K(1)$.

Method Compute $K_k = (1/k)(\sum)$ as above, where \sum is a sum of $\mathcal{O}_n(1)$ terms. Forget old K_k which are not needed anymore and keep the intermediate sum $\sum_{i=0}^k K_i$ up to date with each new K_k .

Result Time $\tilde{\mathcal{O}}(n^3)$ and space $\mathcal{O}(n^2)$.

4. Avoiding complete storage (over \mathbb{Q}_p^n , n large)

For general HEC's, the differential equation is defined over \mathbb{Q}_p^n for some large n , and we work modulo p^M , $M \approx n$.

The size of $F(\Gamma) \bmod p^M$ is hence $\mathcal{O}(n^3) \Rightarrow$ storing $F(\Gamma)$ is costly.

We need only $F(1) = \sum F_i$, therefore: sliding windows technique. Recall $F(1) = r(1)^{-C \cdot M} K(1)$.

Method Compute $K_k = (1/k)(\sum)$ as above, where \sum is a sum of $\mathcal{O}_n(1)$ terms. Forget old K_k which are not needed anymore and keep the intermediate sum $\sum_{i=0}^k K_i$ up to date with each new K_k .

Result Time $\tilde{\mathcal{O}}(n^3)$ and space $\mathcal{O}(n^2)$.

5. A trick of Chudnovsky and Chudnovsky

Given c_0 and a recurrence relation (with 'small' $\alpha(n)$)

$$c_{n+1} = \alpha(n) \cdot c_n,$$

we want to compute c_N for some large N .

▶ Naive: compute $c_1, c_2, \dots, c_N \Rightarrow \mathcal{O}(N)$ field operations.

▶ C & C used fast polynomial arithmetic

1. $\psi(n) := \prod_{k=0}^{\sqrt{N}-1} \alpha(n+k)$.

Via divide and conquer this takes time $\tilde{\mathcal{O}}(\sqrt{N})$.

2. $c_{\sqrt{N}} = \psi(0)c_0$; $c_{2\sqrt{N}} = \psi(\sqrt{N})\psi(0)c_0$;

$$c_N = \prod_{\ell=0}^{\sqrt{N}-1} \psi(\ell\sqrt{N})c_0.$$

Via fast multipoint evaluation: all factors together in time $\tilde{\mathcal{O}}(\sqrt{N})$, as 'deg(ψ) $\approx \sqrt{N}$ '.

Note Implies 'easy to remember' algorithm for factoring (RSA-) integer n in time $\tilde{\mathcal{O}}(\sqrt[4]{n})$: compute $\sqrt{n}! \pmod n$.

5. A trick of Chudnovsky and Chudnovsky

Given c_0 and a recurrence relation (with 'small' $\alpha(n)$)

$$c_{n+1} = \alpha(n) \cdot c_n,$$

we want to compute c_N for some large N .

► Naive: compute $c_1, c_2, \dots, c_N \Rightarrow \mathcal{O}(N)$ field operations.

► C & C used fast polynomial arithmetic

1. $\psi(n) := \prod_{k=0}^{\sqrt{N}-1} \alpha(n+k)$.

Via divide and conquer this takes time $\tilde{\mathcal{O}}(\sqrt{N})$.

2. $c_{\sqrt{N}} = \psi(0)c_0$; $c_{2\sqrt{N}} = \psi(\sqrt{N})\psi(0)c_0$;

$$c_N = \prod_{\ell=0}^{\sqrt{N}-1} \psi(\ell\sqrt{N})c_0.$$

Via fast multipoint evaluation: all factors together in time $\tilde{\mathcal{O}}(\sqrt{N})$, as 'deg(ψ) $\approx \sqrt{N}$ '.

Note Implies 'easy to remember' algorithm for factoring (RSA-) integer n in time $\tilde{\mathcal{O}}(\sqrt[4]{n})$: compute $\sqrt[4]{n}! \bmod n$.

5. A trick of Chudnovsky and Chudnovsky

Given c_0 and a recurrence relation (with 'small' $\alpha(n)$)

$$c_{n+1} = \alpha(n) \cdot c_n,$$

we want to compute c_N for some large N .

- ▶ Naive: compute $c_1, c_2, \dots, c_N \Rightarrow \mathcal{O}(N)$ field operations.
- ▶ C & C used fast polynomial arithmetic

1. $\psi(n) := \prod_{k=0}^{\sqrt{N}-1} \alpha(n+k)$.

Via divide and conquer this takes time $\tilde{\mathcal{O}}(\sqrt{N})$.

2. $c_{\sqrt{N}} = \psi(0)c_0$; $c_{2\sqrt{N}} = \psi(\sqrt{N})\psi(0)c_0$;

$$c_N = \prod_{\ell=0}^{\sqrt{N}-1} \psi(\ell\sqrt{N})c_0.$$

Via fast multipoint evaluation: all factors together in time $\tilde{\mathcal{O}}(\sqrt{N})$, as 'deg(ψ) $\approx \sqrt{N}$ '.

Note Implies 'easy to remember' algorithm for factoring (RSA-) integer n in time $\tilde{\mathcal{O}}(\sqrt[4]{n})$: compute $\sqrt{n}! \pmod n$.

5. A trick of Chudnovsky and Chudnovsky

Given c_0 and a recurrence relation (with 'small' $\alpha(n)$)

$$c_{n+1} = \alpha(n) \cdot c_n,$$

we want to compute c_N for some large N .

► Naive: compute $c_1, c_2, \dots, c_N \Rightarrow \mathcal{O}(N)$ field operations.

► C & C used fast polynomial arithmetic

1. $\psi(n) := \prod_{k=0}^{\sqrt{N}-1} \alpha(n+k)$.

Via divide and conquer this takes time $\tilde{\mathcal{O}}(\sqrt{N})$.

2. $c_{\sqrt{N}} = \psi(0)c_0$; $c_{2\sqrt{N}} = \psi(\sqrt{N})\psi(0)c_0$;

$$c_N = \prod_{\ell=0}^{\sqrt{N}-1} \psi(\ell\sqrt{N})c_0.$$

Via fast multipoint evaluation: all factors together in time $\tilde{\mathcal{O}}(\sqrt{N})$, as 'deg(ψ) $\approx \sqrt{N}$ '.

Note Implies 'easy to remember' algorithm for factoring (RSA-) integer n in time $\tilde{\mathcal{O}}(\sqrt[4]{n})$: compute $\sqrt{n}! \pmod n$.

5. A trick of Chudnovsky and Chudnovsky

Given c_0 and a recurrence relation (with 'small' $\alpha(n)$)

$$c_{n+1} = \alpha(n) \cdot c_n,$$

we want to compute c_N for some large N .

► Naive: compute $c_1, c_2, \dots, c_N \Rightarrow \mathcal{O}(N)$ field operations.

► C & C used fast polynomial arithmetic

1. $\psi(n) := \prod_{k=0}^{\sqrt{N}-1} \alpha(n+k)$.

Via divide and conquer this takes time $\tilde{\mathcal{O}}(\sqrt{N})$.

2. $c_{\sqrt{N}} = \psi(0)c_0$; $c_{2\sqrt{N}} = \psi(\sqrt{N})\psi(0)c_0$;

$$c_N = \prod_{\ell=0}^{\sqrt{N}-1} \psi(\ell\sqrt{N})c_0.$$

Via fast multipoint evaluation: all factors together in time $\tilde{\mathcal{O}}(\sqrt{N})$, as 'deg(ψ) $\approx \sqrt{N}$ '.

Note Implies 'easy to remember' algorithm for factoring (RSA-) integer n in time $\tilde{\mathcal{O}}(\sqrt[4]{n})$: compute $\sqrt{n}! \pmod n$.

More complicated recurr. seq. and their sum

$$c_{n+1} = \alpha_0(n) \cdot c_n + \alpha_1(n) \cdot c_{n-1} + \cdots + \alpha_\ell(n) \cdot c_{n-\ell}.$$

Assume c_0, \dots, c_ℓ are given, we need c_N . Matrix recurrence:

$$\mathcal{C}_n := \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_{n-\ell} \end{bmatrix} \Rightarrow \mathcal{C}_{n+1} = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{\ell-1} & \alpha_\ell \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \mathcal{C}_n.$$

If we need $\sigma_N := \sum_{k=0}^N c_k$, we set $\sigma^{-1} = 0$ and

$$\mathcal{D}_n := \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_{n-\ell} \\ \sigma_{n-1} \end{bmatrix} \Rightarrow \mathcal{D}_{n+1} = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{\ell-1} & \alpha_\ell & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} \mathcal{D}_n.$$

Now apply C & C's trick to compute \mathcal{D}_{N+1} and hence σ_N in $\tilde{\mathcal{O}}(\ell^\omega \sqrt{N})$ field operations.

More complicated recurr. seq. and their sum

$$c_{n+1} = \alpha_0(n) \cdot c_n + \alpha_1(n) \cdot c_{n-1} + \cdots + \alpha_\ell(n) \cdot c_{n-\ell}.$$

Assume c_0, \dots, c_ℓ are given, we need c_N . Matrix recurrence:

$$C_n := \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_{n-\ell} \end{bmatrix} \Rightarrow C_{n+1} = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{\ell-1} & \alpha_\ell \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} C_n.$$

If we need $\sigma_N := \sum_{k=0}^N c_k$, we set $\sigma^{-1} = 0$ and

$$D_n := \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_{n-\ell} \\ \sigma_{n-1} \end{bmatrix} \Rightarrow D_{n+1} = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{\ell-1} & \alpha_\ell & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} D_n.$$

Now apply C & C's trick to compute D_{N+1} and hence σ_N in $\tilde{O}(\ell^\omega \sqrt{N})$ field operations.

More complicated recurr. seq. and their sum

Solving p -adic
matrix differential
equations

Hendrik
Hübrechts

$$c_{n+1} = \alpha_0(n) \cdot c_n + \alpha_1(n) \cdot c_{n-1} + \cdots + \alpha_\ell(n) \cdot c_{n-\ell}.$$

Assume c_0, \dots, c_ℓ are given, we need c_N . Matrix recurrence:

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

$$\mathcal{C}_n := \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_{n-\ell} \end{bmatrix} \Rightarrow \mathcal{C}_{n+1} = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{\ell-1} & \alpha_\ell \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \mathcal{C}_n.$$

If we need $\sigma_N := \sum_{k=0}^N c_k$, we set $\sigma^{-1} = 0$ and

$$\mathcal{D}_n := \begin{bmatrix} c_n \\ c_{n-1} \\ \vdots \\ c_{n-\ell} \\ \sigma_{n-1} \end{bmatrix} \Rightarrow \mathcal{D}_{n+1} = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{\ell-1} & \alpha_\ell & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \mathbf{1} & 0 & \cdots & 0 & 0 & \mathbf{1} \end{bmatrix} \mathcal{D}_n.$$

Now apply C & C's trick to compute \mathcal{D}_{N+1} and hence σ_N in $\tilde{\mathcal{O}}(\ell^\omega \sqrt{N})$ field operations.

Even more complicated

All the above techniques work also if we let c_n be a $(d \times 1)$ -vector and the $\alpha_i(n)$ are $(d \times d)$ -matrices.

Corollary We can in this case compute $\sum_{n=0}^N c_n$ (with 'deg α_i ' small) in $\tilde{O}((d \cdot \ell)^\omega \sqrt{N})$ field operations.

Solving p -adic
matrix differential
equations

Hendrik
Hubrechts

Number of
rational points

Deformation and
differential
equation

Two deformation
strategies

Strategies for the
differential
equation

Application to our diff. eq. (over \mathbb{Q}_p^n , n large)

$$K_{n+1} = \frac{1}{n+1} \left(\sum_{i=0}^{\ell} Z_i(n) K_{n-i} \tilde{Z}_i(n) \right); Z_i, \tilde{Z}_i \text{ over } \mathbb{Q}_p^n, \ell \approx pg.$$

We cannot put $c_n := K_n$, because of the non-commutativity of matrix multiplication (and \sum'), hence we write all entries of K_n in one large $(4g^2 \times 1)$ column vector: this is c_n . Now we apply the previous proposition, with appropriate 'transformation matrix':

$$\begin{bmatrix} \frac{1}{n+1} Z'_0 & \frac{1}{n+1} Z'_1 & \cdots & \frac{1}{n+1} Z'_\ell & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

(Question: can we exploit the sparseness of the recursion?)

Application to our diff. eq. (over \mathbb{Q}_p^n , n large)

$$K_{n+1} = \frac{1}{n+1} \left(\sum_{i=0}^{\ell} Z_i(n) K_{n-i} \tilde{Z}_i(n) \right); Z_i, \tilde{Z}_i \text{ over } \mathbb{Q}_p^n, \ell \approx pg.$$

We cannot put $c_n := K_n$, because of the non-commutativity of matrix multiplication (and \sum'), hence we write all entries of K_n in one large ($4g^2 \times 1$) column vector: this is c_n . Now we apply the previous proposition, with appropriate 'transformation matrix':

$$\begin{bmatrix} \frac{1}{n+1} Z'_0 & \frac{1}{n+1} Z'_1 & \cdots & \frac{1}{n+1} Z'_\ell & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

(Question: can we exploit the sparseness of the recursion?)

Conclusion

Working modulo p^M we know that $K_k \approx c_k \equiv 0$ for $k \gg 0$, hence for $N \approx n$ large enough we have

$$\sigma_N \equiv \sum_{i=0}^{\infty} K_i \pmod{p^M}.$$

Conclusion We can compute $K(1)$ and $F(1)$ modulo p^M , with $M \approx n$, in $\tilde{O}(\sqrt{n})$ operations in $\mathbb{Q}_p^n \pmod{p^M}$, which gives in total $\tilde{O}(n^{2.5})$ bit operations for finding $F(1)$.

Combined with Kedlaya and Umans' recent results on modular composition of polynomials this enables us to compute the zeta function of a hyperelliptic curve \mathcal{C} (and $\#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n})$) or $C_{a,b}$ -curve over \mathbb{F}_{p^n} in time $\tilde{O}(n^{2.5})$ and polynomial time in the genus.

Conclusion

Working modulo p^M we know that $K_k \approx c_k \equiv 0$ for $k \gg 0$, hence for $N \approx n$ large enough we have

$$\sigma_N \equiv \sum_{i=0}^{\infty} K_i \pmod{p^M}.$$

Conclusion We can compute $K(1)$ and $F(1)$ modulo p^M , with $M \approx n$, in $\tilde{O}(\sqrt{n})$ operations in $\mathbb{Q}_{p^n} \pmod{p^M}$, which gives in total $\tilde{O}(n^{2.5})$ bit operations for finding $F(1)$.

Combined with Kedlaya and Umans' recent results on modular composition of polynomials this enables us to compute the zeta function of a hyperelliptic curve \mathcal{C} (and $\#\text{Jac}(\mathcal{C}/\mathbb{F}_{p^n})$) or $C_{a,b}$ -curve over \mathbb{F}_{p^n} in **time $\tilde{O}(n^{2.5})$** and polynomial time in the genus.