Computing p-adic heights on hyperelliptic curves

Stevan Gajović (Charles University Prague)
Joint work with Steffen Müller (University of Groningen)

Number Theory in Montserrat 2023 ,
Montserrat, 29/06/2023

UNIVERZITA
KARLOVA

p-adic heights

Goals today:

- Introduce p-adic heights on Jacobians of curves.

p-adic heights

Goals today:

- Introduce p-adic heights on Jacobians of curves.
- Briefly mention local p-adic heights away from p.

p-adic heights

Goals today:

- Introduce p-adic heights on Jacobians of curves.
- Briefly mention local p-adic heights away from p.
- Present an algorithm to compute local p-adic heights above p on hyperelliptic curves.

p-adic heights

Goals today:

- Introduce p-adic heights on Jacobians of curves.
- Briefly mention local p-adic heights away from p.
- Present an algorithm to compute local p-adic heights above p on hyperelliptic curves.
- Distinguish two important cases on even degree hyperelliptic curves.
- Key feature: Reduce to computing Coleman integrals of basis differentials.

Applications:

- Quadratic Chabauty for rational points on hyperelliptic curves.

p-adic heights

Goals today:

- Introduce p-adic heights on Jacobians of curves.
- Briefly mention local p-adic heights away from p.
- Present an algorithm to compute local p-adic heights above p on hyperelliptic curves.
- Distinguish two important cases on even degree hyperelliptic curves.
- Key feature: Reduce to computing Coleman integrals of basis differentials.

Applications:

- Quadratic Chabauty for rational points on hyperelliptic curves.
- Quadratic Chabauty for integral points on even degree hyperelliptic curves.

p-adic heights

Goals today:

- Introduce p-adic heights on Jacobians of curves.
- Briefly mention local p-adic heights away from p.
- Present an algorithm to compute local p-adic heights above p on hyperelliptic curves.
- Distinguish two important cases on even degree hyperelliptic curves.
- Key feature: Reduce to computing Coleman integrals of basis differentials.

Applications:

- Quadratic Chabauty for rational points on hyperelliptic curves.
- Quadratic Chabauty for integral points on even degree hyperelliptic curves.
- Numerically test p-adic BSD.

p-adic heights

Goals today:

- Introduce p-adic heights on Jacobians of curves.
- Briefly mention local p-adic heights away from p.
- Present an algorithm to compute local p-adic heights above p on hyperelliptic curves.
- Distinguish two important cases on even degree hyperelliptic curves.
- Key feature: Reduce to computing Coleman integrals of basis differentials.

Applications:

- Quadratic Chabauty for rational points on hyperelliptic curves.
- Quadratic Chabauty for integral points on even degree hyperelliptic curves.
- Numerically test p-adic BSD.
- Other applications or ideas? Feel free to contact Steffen and me! :)

Introduction to p-adic heights

- Bilinear pairing (or quadratic form) defined on abelian varieties.

Introduction to p-adic heights

- Bilinear pairing (or quadratic form) defined on abelian varieties.
- First constructions: Schneider, Mazur-Tate.
- More general: Nekovář.

Introduction to p-adic heights

- Bilinear pairing (or quadratic form) defined on abelian varieties.
- First constructions: Schneider, Mazur-Tate.
- More general: Nekovář.
- $X/\mathbb{Q}$ = nice curve curve of genus $g > 0$, with good reduction at p, and $J/\mathbb{Q}$ = its Jacobian
- Works also for number fields $K/\mathbb{Q}$.
- Coleman-Gross: p-adic heights on J.

Coleman-Gross (CG) p-adic heights

- p-adic height: bilinear map

$$h := \sum_{q \text{ finite prime}} h_q : J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p.$$

Coleman-Gross (CG) p-adic heights

- p-adic height: bilinear map

$$h := \sum_{q \text{ finite prime}} h_q : J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p.$$

- For a prime number q, denote $X_q := X \otimes \mathbb{Q}_q$.
- For each prime $q \in \mathbb{Z}$, define local heights

$$h_q(D_1, D_2), \text{ for } D_1, D_2 \in \mathrm{Div}^0(X_q).$$

Coleman-Gross (CG) p-adic heights

- p-adic height: bilinear map

$$h := \sum_{q \text{ finite prime}} h_q : J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p.$$

- For a prime number q, denote $X_q := X \otimes \mathbb{Q}_q$.
- For each prime $q \in \mathbb{Z}$, define local heights

$$h_q(D_1, D_2), \text{ for } D_1, D_2 \in \mathrm{Div}^0(X_q).$$

- Distinguish h_q for $q \neq p$ and h_p $(*)$.
- h_q for $q \neq p$: intersection multiplicities.
- h_p: Coleman integral of a non-holomorphic differential.

Technicalities

- p-adic height depends on (and we fix it):

Technicalities

- p-adic height depends on (and we fix it):

(a) A continuous idèle class character $\ell\colon \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q} \longrightarrow \mathbb{Q}_p$ with certain technical conditions.

* Technical conditions: For $\mathbb{Q}$, ℓ_p be extended to be the Iwasawa branch $\log_p : \mathbb{Q}_p^* \longrightarrow \mathbb{Q}_p$ of the p-adic logarithm $\log_p(p) = 0$.

Technicalities

- p-adic height depends on (and we fix it):

(a) A continuous idèle class character $\ell\colon \mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q} \longrightarrow \mathbb{Q}_p$ with certain technical conditions.

  * Technical conditions: For $\mathbb{Q}$, ℓ_p be extended to be the Iwasawa branch $\log_p : \mathbb{Q}_p^* \longrightarrow \mathbb{Q}_p$ of the p-adic logarithm $\log_p(p) = 0$.

(b) A choice of a subspace $W_p \subseteq \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$ complementary to the space of holomorphic forms $\mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$.

  * Write $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) = \mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \oplus W_p$.

Heights away from p

Theorem (Local heights for $q \neq p$)

- *There exists a unique function $h_q(D_1, D_2)$ taking values in $\mathbb{Q}_p$:*

Heights away from p

Theorem (Local heights for $q \neq p$)

- *There exists a unique function $h_q(D_1, D_2)$ taking values in $\mathbb{Q}_p$:*

(1) *defined for all $D_1, D_2 \in \mathrm{Div}^0(X_q)$ with disjoint support;*

Heights away from p

Theorem (Local heights for $q \neq p$)

- *There exists a unique function $h_q(D_1, D_2)$ taking values in $\mathbb{Q}_p$:*

(1) *defined for all $D_1, D_2 \in \mathrm{Div}^0(X_q)$ with disjoint support;*

(2) *bi-additive, continuous, and symmetric;*

Heights away from p

Theorem (Local heights for $q \neq p$)

- *There exists a unique function* $h_q(D_1, D_2)$ *taking values in* $\mathbb{Q}_p$*:*

(1) *defined for all* $D_1, D_2 \in \mathrm{Div}^0(X_q)$ *with disjoint support;*

(2) *bi-additive, continuous, and symmetric;*

(3) *for all* $f \in \mathbb{Q}_p(X_q)^*$ *(when defined):* $h_q(\mathrm{div}(f), D_2) = \log_p(f(D_2))$.

Heights away from p

Theorem (Local heights for $q \neq p$)

- *There exists a unique function* $h_q(D_1, D_2)$ *taking values in* $\mathbb{Q}_p$:

(1) *defined for all* $D_1, D_2 \in \mathrm{Div}^0(X_q)$ *with disjoint support;*

(2) *bi-additive, continuous, and symmetric;*

(3) *for all* $f \in \mathbb{Q}_p(X_q)^*$ *(when defined):* $h_q(\mathrm{div}(f), D_2) = \log_p(f(D_2))$.

- $\mathcal{X}_q/\mathbb{Q}_q$ = regular model of X_q with $(- \cdot -)$ = ($\mathbb{Q}$-valued) intersection multiplicity on $\mathcal{X}_q$.
- $\mathcal{D}_1, \mathcal{D}_2$ = extensions of D_1, D_2 to $\mathcal{X}_q$ such that $(\mathcal{D}_i \cdot V) = 0$ for all vertical divisors V on $\mathcal{X}_q$.

Heights away from p

Theorem (Local heights for $q \neq p$)

- *There exists a unique function $h_q(D_1, D_2)$ taking values in $\mathbb{Q}_p$:*

(1) *defined for all $D_1, D_2 \in \mathrm{Div}^0(X_q)$ with disjoint support;*

(2) *bi-additive, continuous, and symmetric;*

(3) *for all $f \in \mathbb{Q}_p(X_q)^*$ (when defined): $h_q(\mathrm{div}(f), D_2) = \log_p(f(D_2))$.*

- $\mathcal{X}_q/\mathbb{Q}_q$ = regular model of X_q with $(- \cdot -)$ = ($\mathbb{Q}$-valued) intersection multiplicity on $\mathcal{X}_q$.
- $\mathcal{D}_1, \mathcal{D}_2$ = extensions of D_1, D_2 to $\mathcal{X}_q$ such that $(\mathcal{D}_i \cdot V) = 0$ for all vertical divisors V on $\mathcal{X}_q$.

Construction of h_q

$$h_q(D_1, D_2) = \log_p(q) \cdot (\mathcal{D}_1 \cdot \mathcal{D}_2).$$

- van Bommel-Holmes-Müller's algorithm: Compute h_q.

Introduction to local p-adic heights at p

Construction of h_p

The local height $h_p(D_1, D_2)$ is a Coleman integral $\int_{D_2} \omega_{D_1}$, for a certain differential of the third kind ω_{D_1} depending on D_1.

Introduction to local p-adic heights at p

Construction of h_p

The local height $h_p(D_1, D_2)$ is a Coleman integral $\int_{D_2} \omega_{D_1}$, for a certain differential of the third kind ω_{D_1} depending on D_1.

Third kind meromorphic differentials

ω is of the third kind if it is holomorphic except possibly at finitely many points and it has at most simple poles with residues in $\mathbb{Z}$.

- Denote $T(\mathbb{Q}_p) := \{\text{the third kind differentials on } X_p\}$.

Introduction to local p-adic heights at p

Construction of h_p

The local height $h_p(D_1, D_2)$ is a Coleman integral $\int_{D_2} \omega_{D_1}$, for a certain differential of the third kind ω_{D_1} depending on D_1.

Third kind meromorphic differentials

ω is of the third kind if it is holomorphic except possibly at finitely many points and it has at most simple poles with residues in $\mathbb{Z}$.

- Denote $T(\mathbb{Q}_p) := \{\text{the third kind differentials on } X_p\}$.
- The residue divisor homomorphism $T(\mathbb{Q}_p) \longrightarrow \mathrm{Div}^0(X_p)$ is given by

$$\mathrm{Res}(\omega) = \sum_{P \in X_p} \mathrm{Res}_P(\omega) P.$$

- Res surjective, but not injective ($\mathrm{Res}(\text{holomorphic differentials}) = 0$).

Introduction to local p-adic heights at p

Construction of h_p

The local height $h_p(D_1, D_2)$ is a Coleman integral $\int_{D_2} \omega_{D_1}$, for a certain differential of the third kind ω_{D_1} depending on D_1.

Third kind meromorphic differentials

ω is of the third kind if it is holomorphic except possibly at finitely many points and it has at most simple poles with residues in $\mathbb{Z}$.

- Denote $T(\mathbb{Q}_p) := \{\text{the third kind differentials on } X_p\}$.
- The residue divisor homomorphism $T(\mathbb{Q}_p) \longrightarrow \mathrm{Div}^0(X_p)$ is given by

$$\mathrm{Res}(\omega) = \sum_{P \in X_p} \mathrm{Res}_P(\omega) P.$$

- Res surjective, but not injective ($\mathrm{Res}(\text{holomorphic differentials}) = 0$).
- Want ω_{D_1} to be such that $\mathrm{Res}(\omega_{D_1}) = D_1$. This choice is not unique!

Second kind meromorphic differentials

ω is of the second kind if all of its residues are 0.

- $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \simeq \{\text{differentials of the second kind}\}/\{df : f \in \mathbb{Q}_p(X)^\times\}$.
- Recall: $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) = \mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \oplus W_p$.

Second kind meromorphic differentials

ω is of the second kind if all of its residues are 0.

- $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \simeq \{\text{differentials of the second kind}\}/\{df : f \in \mathbb{Q}_p(X)^\times\}$.
- Recall: $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) = \mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \oplus W_p$.
- $\exists$ homomorphism "projection" ψ

$$\psi : \{\text{meromorphic differentials on } X_p\} \longrightarrow \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$$

  with many useful properties.
- Projection: if α is of the second kind, then $\psi(\alpha) = [\alpha]$.

Second kind meromorphic differentials

ω is of the second kind if all of its residues are 0.

- $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \simeq \{\text{differentials of the second kind}\}/\{df : f \in \mathbb{Q}_p(X)^\times\}$.
- Recall: $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) = \mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \oplus W_p$.
- $\exists$ homomorphism "projection" ψ

$$\psi : \{\text{meromorphic differentials on } X_p\} \longrightarrow \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$$

  with many useful properties.
- Projection: if α is of the second kind, then $\psi(\alpha) = [\alpha]$.
- $\implies$ $D \in \mathrm{Div}^0(X_p) \rightsquigarrow$ unique $\omega_D \in T(\mathbb{Q}_p)$ such that

$$\mathrm{Res}(\omega_D) = D \text{ and } \psi(\omega_D) \in W_p.$$

- From now on, fix the notation ω_D.

Introduction to local p-adic heights at p

Definition of h_p

Let $D_1, D_2 \in \mathrm{Div}^0(X_p)$ with disjoint support. The local p-adic height pairing at p is given by $h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}$.

Introduction to local p-adic heights at p

Definition of h_p

Let $D_1, D_2 \in \mathrm{Div}^0(X_p)$ with disjoint support. The local p-adic height pairing at p is given by $h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}$.

- Properties of h_p:

Introduction to local p-adic heights at p

Definition of h_p

Let $D_1, D_2 \in \mathrm{Div}^0(X_p)$ with disjoint support. The local p-adic height pairing at p is given by $h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}$.

- Properties of h_p:

* $h_p(D_1, D_2)$ is continuous and bi-additive.

Introduction to local p-adic heights at p

Definition of h_p

Let $D_1, D_2 \in \mathrm{Div}^0(X_p)$ with disjoint support. The local p-adic height pairing at p is given by $h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}$.

- Properties of h_p:

* $h_p(D_1, D_2)$ is continuous and bi-additive.
* $h_p(\mathrm{div}(f), D_2) = \log_p(f(D_2))$.

Introduction to local p-adic heights at p

Definition of h_p

Let $D_1, D_2 \in \mathrm{Div}^0(X_p)$ with disjoint support. The local p-adic height pairing at p is given by $h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}$.

- Properties of h_p:

* $h_p(D_1, D_2)$ is continuous and bi-additive.
* $h_p(\mathrm{div}(f), D_2) = \log_p(f(D_2))$.
* h_p is symmetric if and only if $W_p \subseteq \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$ is isotropic with respect to the cup product pairing.

Definition of h_p

Let $D_1, D_2 \in \mathrm{Div}^0(X_p)$ with disjoint support. The local p-adic height pairing at p is given by $h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}$.

- Properties of h_p:

* $h_p(D_1, D_2)$ is continuous and bi-additive.

* $h_p(\mathrm{div}(f), D_2) = \log_p(f(D_2))$.

* h_p is symmetric if and only if $W_p \subseteq \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$ is isotropic with respect to the cup product pairing.

* Independent of a model of X_p under reasonable technical conditions.

* Independent: $\tau\colon C \to C'$

$$h_p(\tau_*(D_1), \tau_*(D_2))_{\text{on } C'} = h_p(D_1, D_2)_{\text{on } C}.$$

Introduction to local p-adic heights at p

- The cup product pairing $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \times \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$:

$$([\mu_1], [\mu_2]) \mapsto [\mu_1] \cup [\mu_2] := \sum_{P \in X_p} \mathrm{Res}_P \left(\mu_2 \int \mu_1 \right).$$

Introduction to local p-adic heights at p

- The cup product pairing $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \times \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$:

$$([\mu_1], [\mu_2]) \mapsto [\mu_1] \cup [\mu_2] := \sum_{P \in X_p} \mathrm{Res}_P \left(\mu_2 \int \mu_1 \right).$$

- (Besser) $\psi(\omega) \cup \psi(\rho) = -\sum_{P \in X_p} \mathrm{Res}_P \left(\omega \int \rho\right)$.

Introduction to local p-adic heights at p

- The cup product pairing $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \times \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$:

$$([\mu_1],[\mu_2]) \mapsto [\mu_1] \cup [\mu_2] := \sum_{P \in X_p} \mathrm{Res}_P \left(\mu_2 \int \mu_1 \right).$$

- (Besser) $\psi(\omega) \cup \psi(\rho) = -\sum_{P \in X_p} \mathrm{Res}_P \left(\omega \int \rho\right)$.
- Always $\rightsquigarrow$ a symplectic basis $\langle \kappa_0, \ldots, \kappa_{2g-1} \rangle$: $\kappa_i \cup \kappa_j = \pm \delta_{i,2g-1-j}$, where $\langle \kappa_0, \ldots, \kappa_{g-1} \rangle = \mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$.
- We can take $W_p = \langle \kappa_g, \ldots, \kappa_{2g-1} \rangle$.

Introduction to local p-adic heights at p

- The cup product pairing $\mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \times \mathrm{H}^1_{\mathrm{dR}}(X_p/\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$:

$$([\mu_1],[\mu_2]) \mapsto [\mu_1] \cup [\mu_2] := \sum_{P \in X_p} \mathrm{Res}_P \left(\mu_2 \int \mu_1 \right).$$

- (Besser) $\psi(\omega) \cup \psi(\rho) = -\sum_{P \in X_p} \mathrm{Res}_P \left(\omega \int \rho\right)$.
- Always $\rightsquigarrow$ a symplectic basis $\langle \kappa_0, \ldots, \kappa_{2g-1} \rangle$: $\kappa_i \cup \kappa_j = \pm \delta_{i,2g-1-j}$, where $\langle \kappa_0, \ldots, \kappa_{g-1} \rangle = \mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$.
- We can take $W_p = \langle \kappa_g, \ldots, \kappa_{2g-1} \rangle$.
- When $C := X_p$ has good ordinary reduction, we can take $W_p :=$ the unit root subspace, assume from now on.
- Both choices implemented in Sage, we talk about the second one. The difference is just some linear algebra.

- Sage implementation - Balakrishnan: Hyperelliptic curves $y^2 = f(x)/\mathbb{Q}_p$ (WARNING: Sage sees only one point at infinity!):

Coleman integration in Sage and Magma

- Sage implementation - Balakrishnan: Hyperelliptic curves $y^2 = f(x)/\mathbb{Q}_p$ (WARNING: Sage sees only one point at infinity!):
- Monsky-Washnitzer basis differentials $\omega_i := \frac{x^i dx}{2y}$ for $0 \leq i \leq \deg(f) - 2 \rightsquigarrow \int_S^R \omega_i$.
- When we can apply the Monsky-Washnitzer reduction: $\omega = \sum_{i=0}^{\deg(f)-2} \alpha_i \omega_i + du \implies \int_S^R \omega = \sum_{i=0}^{\deg(f)-2} \alpha_i \int_S^R \omega_i + u(R) - u(S)$.
- Tiny integrals $\int_S^R \omega$, where $S \equiv R \pmod{p}$.

Coleman integration in Sage and Magma

- Sage implementation - Balakrishnan: Hyperelliptic curves $y^2 = f(x)/\mathbb{Q}_p$ (WARNING: Sage sees only one point at infinity!):
- Monsky-Washnitzer basis differentials $\omega_i := \frac{x^i dx}{2y}$ for $0 \leq i \leq \deg(f) - 2 \rightsquigarrow \int_S^R \omega_i$.
- When we can apply the Monsky-Washnitzer reduction: $\omega = \sum_{i=0}^{\deg(f)-2} \alpha_i \omega_i + du \implies \int_S^R \omega = \sum_{i=0}^{\deg(f)-2} \alpha_i \int_S^R \omega_i + u(R) - u(S)$.
- Tiny integrals $\int_S^R \omega$, where $S \equiv R \pmod{p}$.
- Endpoints R, S satisfy $\mathrm{ord}_p\, y((R)) \geq 0$, $\mathrm{ord}_p(y(S)) \geq 0$.
- Magma implementation Balakrishnan-Tuitman: On fairly general curves, including plane curves.
- For $\omega \in \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) \rightsquigarrow \int_S^R \omega$.

Coleman integration in Sage and Magma

- Sage implementation - Balakrishnan: Hyperelliptic curves $y^2 = f(x)/\mathbb{Q}_p$ (WARNING: Sage sees only one point at infinity!):
- Monsky-Washnitzer basis differentials $\omega_i := \frac{x^i dx}{2y}$ for $0 \leq i \leq \deg(f) - 2 \rightsquigarrow \int_S^R \omega_i$.
- When we can apply the Monsky-Washnitzer reduction: $\omega = \sum_{i=0}^{\deg(f)-2} \alpha_i \omega_i + du \implies \int_S^R \omega = \sum_{i=0}^{\deg(f)-2} \alpha_i \int_S^R \omega_i + u(R) - u(S)$.
- Tiny integrals $\int_S^R \omega$, where $S \equiv R \pmod{p}$.
- Endpoints R, S satisfy $\operatorname{ord}_p y((R)) \geq 0$, $\operatorname{ord}_p(y(S)) \geq 0$.
- Magma implementation Balakrishnan-Tuitman: On fairly general curves, including plane curves.
- For $\omega \in \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) \rightsquigarrow \int_S^R \omega$.
- When possible, allows $\operatorname{ord}_p(y(R)) < 0$ or $\operatorname{ord}_p(y(S)) < 0$.

Local heights $h_p(D_1, D_2)$ setup

- Assume that $D_1, D_2 \in \mathrm{Div}^0(C)$ are pointwise $\mathbb{Q}_p$-rational. To compute $h_p(D_1, D_2) \rightsquigarrow$ compute $h_p(P - Q, R - S)$ for fixed distinct points $P, Q, R, S \in C(\mathbb{Q}_p)$.

Local heights $h_p(D_1, D_2)$ setup

- Assume that $D_1, D_2 \in \mathrm{Div}^0(C)$ are pointwise $\mathbb{Q}_p$-rational. To compute $h_p(D_1, D_2) \rightsquigarrow$ compute $h_p(P - Q, R - S)$ for fixed distinct points $P, Q, R, S \in C(\mathbb{Q}_p)$.
- Assume from now on that $C\colon y^2 = f(x)$, with $f \in \mathbb{Z}_p[x]$ monic has good reduction.
- Let $\iota\colon C \to C$ denote the hyperelliptic involution.

Local heights $h_p(D_1, D_2)$ setup

- Assume that $D_1, D_2 \in \mathrm{Div}^0(C)$ are pointwise $\mathbb{Q}_p$-rational. To compute $h_p(D_1, D_2) \rightsquigarrow$ compute $h_p(P-Q, R-S)$ for fixed distinct points $P, Q, R, S \in C(\mathbb{Q}_p)$.
- Assume from now on that $C\colon y^2 = f(x)$, with $f \in \mathbb{Z}_p[x]$ monic has good reduction.
- Let $\iota\colon C \to C$ denote the hyperelliptic involution.
- Balakrishnan and Besser [BB]: Compute $h_p(P-Q, R-S)$ when $\deg(f)$ odd.
- We now recall [BB] algorithm.

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

(2) Find one differential ω' such that $\mathrm{Res}(\omega') = P - \iota(P)$.

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

(2) Find one differential ω' such that $\mathrm{Res}(\omega') = P - \iota(P)$.

(3) Compute the map ψ, and especially $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

(2) Find one differential ω' such that $\mathrm{Res}(\omega') = P - \iota(P)$.

(3) Compute the map ψ, and especially $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

(4) Obtain a holomorphic differential ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

(2) Find one differential ω' such that $\mathrm{Res}(\omega') = P - \iota(P)$.

(3) Compute the map ψ, and especially $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

(4) Obtain a holomorphic differential ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

(5) Compute the Coleman integral of the third kind differential $\int_S^R \omega'$.

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

(2) Find one differential ω' such that $\mathrm{Res}(\omega') = P - \iota(P)$.

(3) Compute the map ψ, and especially $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

(4) Obtain a holomorphic differential ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

(5) Compute the Coleman integral of the third kind differential $\int_S^R \omega'$.

* Let $\alpha = \phi^*\omega' - p\omega'$, $\mathcal{P} = \{\text{Weierstrass points}\} \cup \{\text{Poles of } \alpha\}$, $\beta : \mathrm{Res}(\beta) = R - S$, and $I := \int_S^R \omega'$. Then

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

(2) Find one differential ω' such that $\mathrm{Res}(\omega') = P - \iota(P)$.

(3) Compute the map ψ, and especially $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

(4) Obtain a holomorphic differential ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

(5) Compute the Coleman integral of the third kind differential $\int_S^R \omega'$.

* Let $\alpha = \phi^*\omega' - p\omega'$, $\mathcal{P} = \{\text{Weierstrass points}\} \cup \{\text{Poles of } \alpha\}$, $\beta : \mathrm{Res}(\beta) = R - S$, and $I := \int_S^R \omega'$. Then

$$I = \frac{1}{1-p} \cdot \left(\psi(\alpha) \cup \psi(\beta) + \sum_{P \in \mathcal{P}} \mathrm{Res}_P \left(\alpha \int \beta \right) - \int_{\phi(S)}^{S} \omega - \int_R^{\phi(R)} \omega \right)$$

[BB] algorithm

(1) Reduce to computing $h_p(P - \iota(P), R - S)$.

(2) Find one differential ω' such that $\mathrm{Res}(\omega') = P - \iota(P)$.

(3) Compute the map ψ, and especially $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

(4) Obtain a holomorphic differential ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

(5) Compute the Coleman integral of the third kind differential $\int_S^R \omega'$.

* Let $\alpha = \phi^*\omega' - p\omega'$, $\mathcal{P} = \{\text{Weierstrass points}\} \cup \{\text{Poles of } \alpha\}$, $\beta : \mathrm{Res}(\beta) = R - S$, and $I := \int_S^R \omega'$. Then

$$I = \frac{1}{1-p} \cdot \left(\psi(\alpha) \cup \psi(\beta) + \sum_{P \in \mathcal{P}} \mathrm{Res}_P \left(\alpha \int \beta \right) - \int_{\phi(S)}^{S} \omega - \int_{R}^{\phi(R)} \omega \right)$$

(6) Compute $h_p(P - Q, R - S) = \int_S^R \omega' - \int_S^R \omega_h$.

Our algorithm

- Today: all hyperelliptic curves over $\mathbb{Q}_p$ of good reduction.

Our algorithm

- Today: all hyperelliptic curves over $\mathbb{Q}_p$ of good reduction.
- We need to compute some quantities related only to the curve first:

Our algorithm

- Today: all hyperelliptic curves over $\mathbb{Q}_p$ of good reduction.
- We need to compute some quantities related only to the curve first:

* a basis for $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ or W_p;

Our algorithm

- Today: all hyperelliptic curves over $\mathbb{Q}_p$ of good reduction.
- We need to compute some quantities related only to the curve first:

* a basis for $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ or W_p;
* cup product matrix CPM;

Our algorithm

- Today: all hyperelliptic curves over $\mathbb{Q}_p$ of good reduction.
- We need to compute some quantities related only to the curve first:

* a basis for $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ or W_p;
* cup product matrix CPM;
* action of Frobenius (given by $\phi : x \mapsto x^p$) on $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

Our algorithm

- Today: all hyperelliptic curves over $\mathbb{Q}_p$ of good reduction.
- We need to compute some quantities related only to the curve first:
  - a basis for $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ or W_p;
  - cup product matrix CPM;
  - action of Frobenius (given by $\phi : x \mapsto x^p$) on $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.
- We first mention these (pre)computations.
- We then proceed as explained on the previous slide.

Our algorithm

- Today: all hyperelliptic curves over $\mathbb{Q}_p$ of good reduction.
- We need to compute some quantities related only to the curve first:

* a basis for $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ or W_p;
* cup product matrix CPM;
* action of Frobenius (given by $\phi : x \mapsto x^p$) on $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

- We first mention these (pre)computations.
- We then proceed as explained on the previous slide.
- For even degree, we have one more case - when $\{P, Q\} = \{\infty_-, \infty_+\}$.
- The other steps depend on the nature of the points P and Q - if they are affine or $\{P, Q\} = \{\infty_-, \infty_+\}$.
- We distinguish these two cases.

Computations depending only on C

(i) Extend $\eta_0 := \omega_0, \ldots, \eta_{g-1} := \omega_{g-1}$ to a basis of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

* If $\deg(f)$ odd, take $\eta_i := \omega_i$ for $g \leq i \leq 2g-1$.
* If $\deg(f)$ even, for $g \leq i \leq 2g-1$, compute $c_i \in \mathbb{Q}_p$ such that, for $\eta_i := \omega_{i+1} - c_i\omega_g$ has a residue $= 0$ at $\infty_\pm$.

Computations depending only on C

(i) Extend $\eta_0 := \omega_0, \dots, \eta_{g-1} := \omega_{g-1}$ to a basis of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

* If $\deg(f)$ odd, take $\eta_i := \omega_i$ for $g \leq i \leq 2g-1$.
* If $\deg(f)$ even, for $g \leq i \leq 2g-1$, compute $c_i \in \mathbb{Q}_p$ such that, for $\eta_i := \omega_{i+1} - c_i\omega_g$ has a residue $= 0$ at $\infty_\pm$.

(ii)* Compute the cup product matrix on C.

* It is given by $CPM = \left((\deg(f) - 2g)\,\mathrm{Res}_{\infty/\infty_+}\left(\eta_j \int \eta_i\right)\right)_{i,j}$.

Computations depending only on C

(i) Extend $\eta_0 := \omega_0, \dots, \eta_{g-1} := \omega_{g-1}$ to a basis of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

* If $\deg(f)$ odd, take $\eta_i := \omega_i$ for $g \leq i \leq 2g-1$.
* If $\deg(f)$ even, for $g \leq i \leq 2g-1$, compute $c_i \in \mathbb{Q}_p$ such that, for $\eta_i := \omega_{i+1} - c_i\omega_g$ has a residue $= 0$ at $\infty_\pm$.

(ii)* Compute the cup product matrix on C.

* It is given by $CPM = \left((\deg(f) - 2g) \operatorname{Res}_{\infty/\infty_+} \left(\eta_j \int \eta_i\right) \right)_{i,j}$.

(iii) Compute the action of Frobenius $\mathrm{Frob} : \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) \to \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

* Harrison's variant of Kedlaya's algorithm and linear algebra.

Computations depending only on C

(i) Extend $\eta_0 := \omega_0, \ldots, \eta_{g-1} := \omega_{g-1}$ to a basis of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

* If $\deg(f)$ odd, take $\eta_i := \omega_i$ for $g \leq i \leq 2g-1$.

* If $\deg(f)$ even, for $g \leq i \leq 2g-1$, compute $c_i \in \mathbb{Q}_p$ such that, for $\eta_i := \omega_{i+1} - c_i\omega_g$ has a residue $= 0$ at $\infty_\pm$.

(ii)* Compute the cup product matrix on C.

* It is given by $CPM = \Big((\deg(f) - 2g)\,\mathrm{Res}_{\infty/\infty_+}(\eta_j \int \eta_i)\Big)_{i,j}$.

(iii) Compute the action of Frobenius $\mathrm{Frob} : \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) \to \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

* Harrison's variant of Kedlaya's algorithm and linear algebra.

(iv) Compute a basis of the unit root subspace W_p.

* [BB]: $\mathrm{Frob}^n(\eta_g), \ldots, \mathrm{Frob}^n(\eta_{2g-1})$ form a basis of W_p modulo p^n.

** [BB] and our algorithm can work with other subspaces W_p.

Computation of $h_p(\infty_- - \infty_+, R - S)$

- We first consider $\{P, Q\} = \{\infty_-, \infty_+\}$.

Computation of $h_p(\infty_- - \infty_+, R - S)$

- We first consider $\{P, Q\} = \{\infty_-, \infty_+\}$.

(v) (NEW) Find one differential ω' such that $\text{Res}(\omega') = \infty_- - \infty_+$.

* We can take $\omega' = 2\omega_g = \frac{x^g dx}{y}$.

Computation of $h_p(\infty_- - \infty_+, R - S)$

- We first consider $\{P, Q\} = \{\infty_-, \infty_+\}$.

(v) (NEW) Find one differential ω' such that $\mathrm{Res}(\omega') = \infty_- - \infty_+$.

* We can take $\omega' = 2\omega_g = \frac{x^g dx}{y}$.

(vi) (NEW) Compute $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

* Define $\alpha = \phi^*(\omega') - p\omega'$.
* Then α is holomorphic at both $\infty_\pm$ and α is of the second kind.

Computation of $h_p(\infty_- - \infty_+, R - S)$

- We first consider $\{P, Q\} = \{\infty_-, \infty_+\}$.

(v) (NEW) Find one differential ω' such that $\mathrm{Res}(\omega') = \infty_- - \infty_+$.

* We can take $\omega' = 2\omega_g = \frac{x^g\,dx}{y}$.

(vi) (NEW) Compute $\psi(\omega')$ in $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$-basis.

* Define $\alpha = \phi^*(\omega') - p\omega'$.
* Then α is holomorphic at both $\infty_\pm$ and α is of the second kind.
* Let $[\alpha] \in \mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ be the class of α.
* Using Harrison's algorithm, write $\phi^*\omega_g = \sum_{i=0}^{2g} f_{0,i}\omega_i$ modulo exact differentials.
* $\implies [\alpha] = \begin{pmatrix} 2f_{0,g} & \cdots & 2f_{0,g-1} & 2f_{0,g+1} \cdots & 2f_{0,2g} \end{pmatrix}^t$.
* We compute $\psi(\omega') = (\mathrm{Frob} - pI)^{-1}[\alpha]$.

Computation of $h_p(\infty_- - \infty_+, R - S)$

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

Computation of $h_p(\infty_- - \infty_+, R - S)$

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

* Rewrite

$$\psi(\omega') = u_0\eta_0 + \cdots + u_{g-1}\eta_{g-1} + u_g \operatorname{Frob}^n(\eta_g) + \cdots + u_{2g-1} \operatorname{Frob}^n(\eta_{2g-1}).$$

* Then $\omega_h := u_0\eta_0 + \cdots + u_{g-1}\eta_{g-1}$.
* If $\omega := \omega' - \omega_h$, recall that $h_p(\infty_- - \infty_+, R - S) = \int_S^R \omega$.

Computation of $h_p(\infty_- - \infty_+, R - S)$

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

* Rewrite

$$\psi(\omega') = u_0\eta_0 + \cdots + u_{g-1}\eta_{g-1} + u_g \operatorname{Frob}^n(\eta_g) + \cdots + u_{2g-1} \operatorname{Frob}^n(\eta_{2g-1}).$$

* Then $\omega_h := u_0\eta_0 + \cdots + u_{g-1}\eta_{g-1}$.
* If $\omega := \omega' - \omega_h$, recall that $h_p(\infty_- - \infty_+, R - S) = \int_S^R \omega$.

(viii) Compute the third kind integral $\int_S^R \omega'$ and holomorphic integrals.

* Using Balakrishnan's algorithm for Coleman integration, we compute $\int_S^R \omega_g$, $u_0 \int_S^R \omega_0 + \cdots + u_{g-1} \int_S^R \omega_{g-1}$.

Computation of $h_p(\infty_- - \infty_+, R - S)$

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$.

* Rewrite

$$\psi(\omega') = u_0\eta_0 + \cdots + u_{g-1}\eta_{g-1} + u_g \operatorname{Frob}^n(\eta_g) + \cdots + u_{2g-1} \operatorname{Frob}^n(\eta_{2g-1}).$$

* Then $\omega_h := u_0\eta_0 + \cdots + u_{g-1}\eta_{g-1}$.
* If $\omega := \omega' - \omega_h$, recall that $h_p(\infty_- - \infty_+, R - S) = \int_S^R \omega$.

(viii) Compute the third kind integral $\int_S^R \omega'$ and holomorphic integrals.

* Using Balakrishnan's algorithm for Coleman integration, we compute $\int_S^R \omega_g,\ u_0 \int_S^R \omega_0 + \cdots + u_{g-1} \int_S^R \omega_{g-1}$.

- We require that R and S are points in affine residue discs.

Computation of $h_p(P - Q, R - S)$ - affine points

- Now, P and Q are affine points.

Computation of $h_p(P-Q, R-S)$ - affine points

- Now, P and Q are affine points.
- Note $\operatorname{div}\left(\dfrac{x-x(P)}{x-x(Q)}\right) = P + \iota(P) - Q - \iota(Q)$.
- Rewrite $P - Q = \dfrac{1}{2}\operatorname{div}\left(\dfrac{x-x(P)}{x-x(Q)}\right) + \dfrac{1}{2}(P - \iota(P)) - \dfrac{1}{2}(Q - \iota(Q))$.

Computation of $h_p(P - Q, R - S)$ - affine points

- Now, P and Q are affine points.
- Note $\operatorname{div}\left(\frac{x - x(P)}{x - x(Q)}\right) = P + \iota(P) - Q - \iota(Q)$.
- Rewrite $P - Q = \frac{1}{2}\operatorname{div}\left(\frac{x - x(P)}{x - x(Q)}\right) + \frac{1}{2}(P - \iota(P)) - \frac{1}{2}(Q - \iota(Q))$.
- $\implies h_p(P - Q, R - S) = \frac{1}{2}\log_p\left(\frac{x(R) - x(P)}{x(R) - x(Q)}\frac{x(S) - x(Q)}{x(S) - x(R)}\right) +$ $\frac{1}{2}h_p(P - \iota(P), R - S) - \frac{1}{2}h_p(Q - \iota(Q), R - S)$.

Computation of $h_p(P-Q, R-S)$ - affine points

- Now, P and Q are affine points.
- Note $\mathrm{div}\left(\frac{x-x(P)}{x-x(Q)}\right) = P + \iota(P) - Q - \iota(Q)$.
- Rewrite $P - Q = \frac{1}{2}\mathrm{div}\left(\frac{x-x(P)}{x-x(Q)}\right) + \frac{1}{2}(P-\iota(P)) - \frac{1}{2}(Q-\iota(Q))$.
- $\implies h_p(P-Q, R-S) = \frac{1}{2}\log_p\left(\frac{x(R)-x(P)}{x(R)-x(Q)}\frac{x(S)-x(Q)}{x(S)-x(R)}\right) + \frac{1}{2}h_p(P-\iota(P), R-S) - \frac{1}{2}h_p(Q-\iota(Q), R-S)$.
- From now on, we compute $h_p(P-\iota(P), R-S)$.

- Now, P and Q are affine points.
- Note $\operatorname{div}\left(\frac{x-x(P)}{x-x(Q)}\right) = P + \iota(P) - Q - \iota(Q)$.
- Rewrite $P - Q = \frac{1}{2}\operatorname{div}\left(\frac{x-x(P)}{x-x(Q)}\right) + \frac{1}{2}(P-\iota(P)) - \frac{1}{2}(Q-\iota(Q))$.
- $\implies h_p(P-Q, R-S) = \frac{1}{2}\log_p\left(\frac{x(R)-x(P)}{x(R)-x(Q)}\frac{x(S)-x(Q)}{x(S)-x(R)}\right) + \frac{1}{2}h_p(P-\iota(P), R-S) - \frac{1}{2}h_p(Q-\iota(Q), R-S)$.
- From now on, we compute $h_p(P-\iota(P), R-S)$.

(v) Find one differential ω' such that $\operatorname{Res}(\omega') = P - \iota(P)$.

- For $\omega' = \frac{y(P)}{x-x(P)}\frac{dx}{y}$, we have $\operatorname{Res}(\omega') = P - \iota(P)$.

Computation of $h_p(P - \iota(P), R - S)$ - affine points

(vi) Compute $\psi(\omega') = \sum_{i=0}^{2g-1} u_i \eta_i$ - use the cup product and Besser's formula

$$\psi(\omega') \cup [\eta_j] = -\int_{\iota(P)}^{P} \eta_j - (\deg(f) - 2g)\,\mathrm{Res}_{\infty/\infty_+}\left(\omega' \int \eta_j\right).$$

- Here we use, if η is holomorphic at poles of ω

$$\sum_{P \in \mathrm{Res}(\omega)} \mathrm{Res}_P\left(\omega \int \eta\right) = \int_{\mathrm{Res}(\omega)} \eta.$$

- This is a way how [BB] compute integrals of differentials in $T(\mathbb{Q}_p)$.

Computation of $h_p(P - \iota(P), R - S)$ - affine points

(vi) Compute $\psi(\omega') = \sum_{i=0}^{2g-1} u_i\eta_i$ - use the cup product and Besser's formula

$$\psi(\omega') \cup [\eta_j] = -\int_{\iota(P)}^{P} \eta_j - (\deg(f) - 2g)\,\mathrm{Res}_{\infty/\infty_+}\left(\omega' \int \eta_j\right).$$

- Here we use, if η is holomorphic at poles of ω

$$\sum_{P \in \mathrm{Res}(\omega)} \mathrm{Res}_P\left(\omega \int \eta\right) = \int_{\mathrm{Res}(\omega)} \eta.$$

- This is a way how [BB] compute integrals of differentials in $T(\mathbb{Q}_p)$.
- (NEW) In both even and odd case: $\mathrm{Res}_{\infty/\infty_+}(\omega' \int \eta_j) = 0$!
- This is also a computational improvement w.r.t. [BB].

$\implies \begin{pmatrix} u_0 & u_1 & \cdots & u_{2g-1} \end{pmatrix}^t =$

$-CPM^{-1}\begin{pmatrix} -\int_{\iota(P)}^{P} \eta_0 & -\int_{\iota(P)}^{P} \eta_1 & \cdots & -\int_{\iota(P)}^{P} \eta_{2g-1} \end{pmatrix}^t.$

Computation of $h_p(P - \iota(P), R - S)$ - affine points

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$ - as before.

Computation of $h_p(P - \iota(P), R - S)$ - affine points

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$ - as before.

(viii) (NEW) Compute $\int_S^R \omega' = \int_S^R \frac{y(P)}{x - x(P)} \frac{dx}{y}$.

- Use a change of variables

$$\tau \colon C \to C' \colon y'^2 = \frac{1}{y(P)^2} x'^{2g+2} f\left(x(P) + \frac{1}{x'}\right)$$
$$(x, y) \mapsto (x', y') := \left(\frac{1}{x - x(P)}, \frac{-y}{y(P)(x - x(P))^{g+1}}\right).$$

Computation of $h_p(P - \iota(P), R - S)$ - affine points

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$ - as before.

(viii) (NEW) Compute $\int_S^R \omega' = \int_S^R \frac{y(P)}{x - x(P)} \frac{dx}{y}$.

- Use a change of variables

$$\tau \colon C \to C' \colon y'^2 = \frac{1}{y(P)^2} x'^{2g+2} f\left(x(P) + \frac{1}{x'}\right)$$

$$(x, y) \mapsto (x', y') := \left(\frac{1}{x - x(P)}, \frac{-y}{y(P)(x - x(P))^{g+1}}\right).$$

$$\implies \int_S^R \frac{y(P)}{x - x(P)} \frac{dx}{y} = \int_{\tau(S)}^{\tau(R)} \frac{x'^g \, dx'}{y'}.$$

Computation of $h_p(P - \iota(P), R - S)$ - affine points

(vii) Find holomorphic ω_h such that $\psi(\omega' - \omega_h) \in W_p$ - as before.

(viii) (NEW) Compute $\int_S^R \omega' = \int_S^R \frac{y(P)}{x - x(P)} \frac{dx}{y}$.

- Use a change of variables

$$\tau\colon C \to C'\colon y'^2 = \frac{1}{y(P)^2} x'^{2g+2} f\left(x(P) + \frac{1}{x'}\right)$$
$$(x, y) \mapsto (x', y') := \left(\frac{1}{x - x(P)}, \frac{-y}{y(P)(x - x(P))^{g+1}}\right).$$

$$\implies \int_S^R \frac{y(P)}{x - x(P)} \frac{dx}{y} = \int_{\tau(S)}^{\tau(R)} \frac{x'^g dx'}{y'}.$$

- $\frac{x'^g dx'}{y'}$ is a basis MW-differential on C' $\implies \int_{\tau(S)}^{\tau(R)} \frac{x'^g dx'}{y'}$ computed directly (and quickly) by Balakrishnan's algorithm.

Computation of $h_p(P - Q, R - S)$ - comments

- By the independence of a model of local heights, we have $h_p(P - \iota(P), R - S) = h_p(\infty_- - \infty_+, \tau(R) - \tau(S))$.
- $\implies$ It suffices to compute heights of the type $h_p(\infty_- - \infty_+, R - S)$!

Computation of $h_p(P - Q, R - S)$ - comments

- By the independence of a model of local heights, we have $h_p(P - \iota(P), R - S) = h_p(\infty_- - \infty_+, \tau(R) - \tau(S))$.
- $\implies$ It suffices to compute heights of the type $h_p(\infty_- - \infty_+, R - S)$!
- If $\mathrm{ord}_p(y(R)) < 0$ or $\mathrm{ord}_p(y(S)) < 0$, we cannot compute $\int_S^R \frac{x^g dx}{y}$ in Sage, neither any of $\int_S^R \omega_i$.
- General condition for our algorithm in Sage: $p \nmid (x(P) - x(R))(x(P) - x(S))(x(Q) - x(R))(x(Q) - x(S))$.

Computation of $h_p(P - Q, R - S)$ - comments

- By the independence of a model of local heights, we have $h_p(P - \iota(P), R - S) = h_p(\infty_- - \infty_+, \tau(R) - \tau(S))$.
- $\implies$ It suffices to compute heights of the type $h_p(\infty_- - \infty_+, R - S)$!
- If $\mathrm{ord}_p(y(R)) < 0$ or $\mathrm{ord}_p(y(S)) < 0$, we cannot compute $\int_S^R \frac{x^g dx}{y}$ in Sage, neither any of $\int_S^R \omega_i$.
- General condition for our algorithm in Sage: $p \nmid (x(P) - x(R))(x(P) - x(S))(x(Q) - x(R))(x(Q) - x(S))$.
- We can try in Magma: Let $\alpha = \phi^*(\frac{x^g dx}{y}) - p\frac{x^g dx}{y}$.

$$\implies \int_S^R \frac{x^g dx}{y} = \frac{1}{1-p}\left(\int_S^R \alpha - \int_{\phi(S)}^S \frac{x^g dx}{y} - \int_R^{\phi(R)} \frac{x^g dx}{y}\right).$$

Computation of $h_p(P-Q, R-S)$ - comments

- By the independence of a model of local heights, we have $h_p(P-\iota(P), R-S) = h_p(\infty_- - \infty_+, \tau(R)-\tau(S))$.
- $\implies$ It suffices to compute heights of the type $h_p(\infty_- - \infty_+, R-S)$!
- If $\mathrm{ord}_p(y(R)) < 0$ or $\mathrm{ord}_p(y(S)) < 0$, we cannot compute $\int_S^R \frac{x^g dx}{y}$ in Sage, neither any of $\int_S^R \omega_i$.
- General condition for our algorithm in Sage: $p \nmid (x(P)-x(R))(x(P)-x(S))(x(Q)-x(R))(x(Q)-x(S))$.
- We can try in Magma: Let $\alpha = \phi^*(\frac{x^g dx}{y}) - p\frac{x^g dx}{y}$.

$$\implies \int_S^R \frac{x^g dx}{y} = \frac{1}{1-p}\left(\int_S^R \alpha - \int_{\phi(S)}^S \frac{x^g dx}{y} - \int_R^{\phi(R)} \frac{x^g dx}{y}\right).$$

- Maximal condition (still theoretic): $\{P,Q\} \cap \{R, \iota(R), S, \iota(S)\} = \emptyset$.

Summary for the local p-adic height above p

- Our algorithm is significantly simpler and faster than [BB].

Summary for the local p-adic height above p

- Our algorithm is significantly simpler and faster than [BB].
- It is slightly more restrictive, but in practice causes no problems.

Summary for the local p-adic height above p

- Our algorithm is significantly simpler and faster than [BB].
- It is slightly more restrictive, but in practice causes no problems.
- The main difference between [BB] and our algorithm is in computing Coleman integrals of differentials of the third kind and residues.

Summary for the local p-adic height above p

- Our algorithm is significantly simpler and faster than [BB].
- It is slightly more restrictive, but in practice causes no problems.
- The main difference between [BB] and our algorithm is in computing Coleman integrals of differentials of the third kind and residues.
- We compare the timings and success of our and [BB] algorithm in several examples.

Genus of a curve	p	Precision	Our time	[BB] time
2	7	10	2s	9s
2	7	300	14min	infeasible
2	503	10	5min	infeasible
3	11	10	7s	37s
4	23	20	3min	64min
17	11	7	18min	infeasible

Quadratic Chabauty applications

- $X/\mathbb{Q}$ = nice curve of genus $g \geq 2$, with good reduction at p, J = its Jacobian whose rank over $\mathbb{Q}$ is $r = g$.
- Assume that $\int_D \omega_0, \ldots, \int_D \omega_{g-1} \colon J(\mathbb{Q}) \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ form a basis of $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee$.

Quadratic Chabauty applications

- $X/\mathbb{Q}$ = nice curve of genus $g \geq 2$, with good reduction at p, J = its Jacobian whose rank over $\mathbb{Q}$ is $r = g$.
- Assume that $\int_D \omega_0, \ldots, \int_D \omega_{g-1} : J(\mathbb{Q}) \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ form a basis of $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee$.
- Idea: Write $h(E, D) = \sum_{1 \leq i,j \leq g} \alpha_{i,j} \int_D \omega_i \int_E \omega_j$.

Quadratic Chabauty applications

- $X/\mathbb{Q}$ = nice curve of genus $g \geq 2$, with good reduction at p, J = its Jacobian whose rank over $\mathbb{Q}$ is $r = g$.
- Assume that $\int_D \omega_0, \ldots, \int_D \omega_{g-1} : J(\mathbb{Q}) \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ form a basis of $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee$.
- Idea: Write $h(E, D) = \sum_{1 \leq i,j \leq g} \alpha_{i,j} \int_D \omega_i \int_E \omega_j$.
- Idea: Use these relations and "bound" the heights away from p to extract rational or integral points on curves.

Quadratic Chabauty applications

- $X/\mathbb{Q}$ = nice curve of genus $g \geq 2$, with good reduction at p, J = its Jacobian whose rank over $\mathbb{Q}$ is $r = g$.
- Assume that $\int_D \omega_0, \ldots, \int_D \omega_{g-1} \colon J(\mathbb{Q}) \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ form a basis of $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee$.
- Idea: Write $h(E, D) = \sum_{1 \leq i,j \leq g} \alpha_{i,j} \int_D \omega_i \int_E \omega_j$.
- Idea: Use these relations and "bound" the heights away from p to extract rational or integral points on curves.

Quadratic Chabauty for rational points example

- Consider $X_0^+(107)\colon y^2 = x^6 + 2x^5 + 5x^4 + 2x^3 - 2x^2 - 4x - 3$.
- Balakrishnan, Dogra, Müller, Tuitman, Vonk computed $X_0^+(107)(\mathbb{Q})$ using $p = 61 \rightsquigarrow$ 40 minutes.
- They needed an odd model over $\mathbb{Q}_p$ and certain conditions on p.

Quadratic Chabauty applications

- $X/\mathbb{Q}$ = nice curve of genus $g \geq 2$, with good reduction at p, J = its Jacobian whose rank over $\mathbb{Q}$ is $r = g$.
- Assume that $\int_D \omega_0, \ldots, \int_D \omega_{g-1} \colon J(\mathbb{Q}) \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ form a basis of $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee$.
- Idea: Write $h(E, D) = \sum_{1 \leq i,j \leq g} \alpha_{i,j} \int_D \omega_i \int_E \omega_j$.
- Idea: Use these relations and "bound" the heights away from p to extract rational or integral points on curves.

Quadratic Chabauty for rational points example

- Consider $X_0^+(107)\colon y^2 = x^6 + 2x^5 + 5x^4 + 2x^3 - 2x^2 - 4x - 3$.
- Balakrishnan, Dogra, Müller, Tuitman, Vonk computed $X_0^+(107)(\mathbb{Q})$ using $p = 61 \rightsquigarrow$ 40 minutes.
- They needed an odd model over $\mathbb{Q}_p$ and certain conditions on p.
- Now, one can use $p = 7 \rightsquigarrow$ 47 seconds.

Quadratic Chabauty for integral points

- Let $X/\mathbb{Q}$: $y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ monic, $\deg(f) = 2g+2$. Then (important assumption!) $\infty_{\pm} \in X(\mathbb{Q})$. Denote $D_\infty := [\infty_- - \infty_+]$.
- Write $h(D_\infty, D) = \sum_{i=0}^{g-1} \alpha_i \int_D \omega_i$, for some $\alpha_i \in \mathbb{Q}_p$.

Quadratic Chabauty for integral points

- Let $X/\mathbb{Q}\colon y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ monic, $\deg(f) = 2g+2$. Then (important assumption!) $\infty_\pm \in X(\mathbb{Q})$. Denote $D_\infty := [\infty_- - \infty_+]$.
- Write $h(D_\infty, D) = \sum_{i=0}^{g-1} \alpha_i \int_D \omega_i$, for some $\alpha_i \in \mathbb{Q}_p$.
- $X(\mathbb{Z}) :=$ integral points on X.
- Assume $Q \in X(\mathbb{Z})$. Consider $\rho_Q\colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_Q(P) := \sum_{i=0}^{g-1} \alpha_i \int_Q^P \omega_i - h_p(D_\infty, P - Q) = \sum_{i=0}^{g-1} \alpha_i \int_Q^P \omega_i - \int_Q^P \omega_\infty,$$

Quadratic Chabauty for integral points

- Let $X/\mathbb{Q}\colon y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ monic, $\deg(f) = 2g+2$. Then (important assumption!) $\infty_{\pm} \in X(\mathbb{Q})$. Denote $D_\infty := [\infty_- - \infty_+]$.
- Write $h(D_\infty, D) = \sum_{i=0}^{g-1} \alpha_i \int_D \omega_i$, for some $\alpha_i \in \mathbb{Q}_p$.
- $X(\mathbb{Z}) :=$ integral points on X.
- Assume $Q \in X(\mathbb{Z})$. Consider $\rho_Q\colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_Q(P) := \sum_{i=0}^{g-1} \alpha_i \int_Q^P \omega_i - h_p(D_\infty, P - Q) = \sum_{i=0}^{g-1} \alpha_i \int_Q^P \omega_i - \int_Q^P \omega_\infty,$$

- ρ_Q is a locally analytic function.
- If $P \in X(\mathbb{Q})$, $\rho_Q(P) = \sum_{q \neq p} h_q(D_\infty, P - Q)$.

Quadratic Chabauty for integral points

- Let $X/\mathbb{Q}\colon y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ monic, $\deg(f) = 2g+2$. Then (important assumption!) $\infty_\pm \in X(\mathbb{Q})$. Denote $D_\infty := [\infty_- - \infty_+]$.
- Write $h(D_\infty, D) = \sum_{i=0}^{g-1} \alpha_i \int_D \omega_i$, for some $\alpha_i \in \mathbb{Q}_p$.
- $X(\mathbb{Z}) :=$ integral points on X.
- Assume $Q \in X(\mathbb{Z})$. Consider $\rho_Q\colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_Q(P) := \sum_{i=0}^{g-1} \alpha_i \int_Q^P \omega_i - h_p(D_\infty, P-Q) = \sum_{i=0}^{g-1} \alpha_i \int_Q^P \omega_i - \int_Q^P \omega_\infty,$$

- ρ_Q is a locally analytic function.
- If $P \in X(\mathbb{Q})$, $\rho_Q(P) = \sum_{q \neq p} h_q(D_\infty, P-Q)$.
- Intersection theory $\implies \forall P, Q \in X(\mathbb{Z}_q)$, $h_q(\infty_- - \infty_+, P-Q) \in T$, T finite for all $q \neq p$; $T = \{0\}$ for almost all (including good) primes.
- $\implies \rho_Q(X(\mathbb{Z}))$ is a finite and computable set.

Testing the p-adic BSD

- Let $A/\mathbb{Q}$ be modular abelian variety of GL_2-type, with good ordinary reduction at a prime p and the Mordell–Weil rank r.

Testing the p-adic BSD

- Let $A/\mathbb{Q}$ be modular abelian variety of GL_2-type, with good ordinary reduction at a prime p and the Mordell–Weil rank r.
- p-adic BSD: relates rank r, values of p-adic L-functions, p-adic multiplier, Tamagawa numbers, cardinality of the Shafarevich–Tate group, cardinality of the torsion, and regulator.

Testing the p-adic BSD

- Let $A/\mathbb{Q}$ be modular abelian variety of GL_2-type, with good ordinary reduction at a prime p and the Mordell–Weil rank r.
- p-adic BSD: relates rank r, values of p-adic L-functions, p-adic multiplier, Tamagawa numbers, cardinality of the Shafarevich–Tate group, cardinality of the torsion, and regulator.
- Example: $X_0^+(67) = X \colon y^2 = x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1$.
- $A =$ Jacobian of X. Then $A(\mathbb{Q}) = \langle D_1, D_2 \rangle$, where $D_1 = (0,1) - \infty_-$ and $D_2 = (0,1) - (0,-1)$.

Testing the p-adic BSD

- Let $A/\mathbb{Q}$ be modular abelian variety of GL_2-type, with good ordinary reduction at a prime p and the Mordell–Weil rank r.
- p-adic BSD: relates rank r, values of p-adic L-functions, p-adic multiplier, Tamagawa numbers, cardinality of the Shafarevich–Tate group, cardinality of the torsion, and regulator.
- Example: $X_0^+(67) = X\colon y^2 = x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1$.
- $A =$ Jacobian of X. Then $A(\mathbb{Q}) = \langle D_1, D_2 \rangle$, where $D_1 = (0,1) - \infty_-$ and $D_2 = (0,1) - (0,-1)$.
- Regulator at $p = 11$:
  $\mathrm{Reg}_{11}(A/\mathbb{Q}) = h(D_1, D_1)h(D_2, D_2) - h(D_1, D_2)^2$.

Testing the p-adic BSD

- Let $A/\mathbb{Q}$ be modular abelian variety of GL_2-type, with good ordinary reduction at a prime p and the Mordell–Weil rank r.
- p-adic BSD: relates rank r, values of p-adic L-functions, p-adic multiplier, Tamagawa numbers, cardinality of the Shafarevich–Tate group, cardinality of the torsion, and regulator.
- Example: $X_0^+(67) = X\colon y^2 = x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1$.
- $A =$ Jacobian of X. Then $A(\mathbb{Q}) = \langle D_1, D_2 \rangle$, where $D_1 = (0,1) - \infty_-$ and $D_2 = (0,1) - (0,-1)$.
- Regulator at $p = 11$:
  $\mathrm{Reg}_{11}(A/\mathbb{Q}) = h(D_1, D_1)h(D_2, D_2) - h(D_1, D_2)^2$.
- We need suitable multiples of D_1 and D_2 whose representatives are of the shape $P + Q - R - \iota(R)$ and disjoint, and satisfy the condition for our algorithm. Works in practice!

The end

Thank you for your attention!

Question

Any questions?