Computing p-adic heights on hyperelliptic curves and linear quadratic Chabauty

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

Winter Workshop Chabauty-Kim 2024,
Heidelberg University, 15/02/2024

p-adic heights

* Balakrishnan and Besser [BB]: compute p-adic heights on odd-degree hyperelliptic curves.

Goals today:

- Introduce p-adic heights on Jacobians of curves.

p-adic heights

* Balakrishnan and Besser [BB]: compute p-adic heights on odd-degree hyperelliptic curves.

Goals today:

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

p-adic heights

* Balakrishnan and Besser [BB]: compute p-adic heights on odd-degree hyperelliptic curves.

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

* Balakrishnan and Besser [BB]: compute p-adic heights on odd-degree hyperelliptic curves.

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.

p-adic heights

* Balakrishnan and Besser [BB]: compute p-adic heights on odd-degree hyperelliptic curves.

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.

Application discussed today:

Linear quadratic Chabauty for integral points on even degree hyperelliptic curves.

p-adic heights

* Balakrishnan and Besser [BB]: compute p-adic heights on odd-degree hyperelliptic curves.

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.

Application discussed today:

Linear quadratic Chabauty for integral points on even degree hyperelliptic curves.

Other applications:

- Quadratic Chabauty for rational points on hyperelliptic curves.

p-adic heights

* Balakrishnan and Besser [BB]: compute p-adic heights on odd-degree hyperelliptic curves.

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.

Application discussed today:

Linear quadratic Chabauty for integral points on even degree hyperelliptic curves.

Other applications:

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

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 of genus $g > 0$, with good reduction at p, and $J(X) = J$ = its Jacobian.
- Works also for number fields $K/\mathbb{Q}$.
- Coleman-Gross: p-adic heights on J.

Comparison with the real (Néron-Tate) heights

Real heights	p-adic heights
$h := \sum_{v \text{ non-arch}} h_v + \sum_{v\|\infty} h_v$	$h := \sum_{q\neq p \text{ finite prime}} h_q + h_p$
sum of local heights over all places	sum of local heights over all non-archimedean places
distinguish non-archimedean and archimedean places	distinguish primes not diving and diving p

Comparison with the real (Néron-Tate) heights

Real heights	p-adic heights
$h := \sum_{v \text{ non-arch}} h_v + \sum_{v\mid\infty} h_v$	$h := \sum_{q \neq p \text{ finite prime}} h_q + h_p$
sum of local heights over all places	sum of local heights over all non-archimedean places
distinguish non-archimedean and archimedean places	distinguish primes not diving and diving p
v non-archimedean: h_v defined using intersection theory multiplied by a log factor	$q \neq p$: h_q defined using intersection theory multiplied by a log factor

Comparison with the real (Néron-Tate) heights

Real heights	p-adic heights
$h := \sum_{v \text{ non-arch}} h_v + \sum_{v\mid\infty} h_v$	$h := \sum_{q\neq p \text{ finite prime}} h_q + h_p$
sum of local heights over all places	sum of local heights over all non-archimedean places
distinguish non-archimedean and archimedean places	distinguish primes not diving and diving p
v non-archimedean: h_v defined using intersection theory multiplied by a log factor	$q \neq p$: h_q defined using intersection theory multiplied by a log factor
v archimedean: h_v = integral of a certain differential of the third kind	h_p = Coleman integral of a certain differential of the third kind

Comparison with the real (Néron-Tate) heights

Real heights	p-adic heights
$h := \sum_{v \text{ non-arch}} h_v + \sum_{v\mid\infty} h_v$	$h := \sum_{q\neq p \text{ finite prime}} h_q + h_p$
sum of local heights over all places	sum of local heights over all non-archimedean places
distinguish non-archimedean and archimedean places	distinguish primes not diving and diving p
v non-archimedean: h_v defined using intersection theory multiplied by a log factor	$q \neq p$: h_q defined using intersection theory multiplied by a log factor
v archimedean: h_v = integral of a certain differential of the third kind	h_p = Coleman integral of a certain differential of the third kind

- Log factor and a hidden term in h_p come from a continuous idèle class character $\mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* \longrightarrow \mathbb{Q}_p$ with some conditions, which we fix.

Comparison with the real (Néron-Tate) heights

Real heights	p-adic heights
$h := \sum_{v \text{ non-arch}} h_v + \sum_{v\mid\infty} h_v$	$h := \sum_{q\neq p \text{ finite prime}} h_q + h_p$
sum of local heights over all places	sum of local heights over all non-archimedean places
distinguish non-archimedean and archimedean places	distinguish primes not diving and diving p
v non-archimedean: h_v defined using intersection theory multiplied by a log factor	$q \neq p$: h_q defined using intersection theory multiplied by a log factor
v archimedean: $h_v =$ integral of a certain differential of the third kind	$h_p =$ Coleman integral of a certain differential of the third kind

- Log factor and a hidden term in h_p come from a continuous idèle class character $\mathbb{A}_{\mathbb{Q}}^*/\mathbb{Q}^* \longrightarrow \mathbb{Q}_p$ with some conditions, which we fix.
- There is an ambiguity in the choice of the differentials when computing h_p - so we need another input to fix the desired one.

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

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

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

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

- 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 with only simple poles.

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) $\forall f \in \mathbb{Q}_p(X_q)^*$ *(if defined):* $h_q(\mathrm{div}(f), D_2) = -\log_p(q)\,\mathrm{ord}_q(f(D_2))$.

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) $\forall f \in \mathbb{Q}_p(X_q)^*$ *(if defined):* $h_q(\mathrm{div}(f), D_2) = -\log_p(q)\,\mathrm{ord}_q(f(D_2))$.

- $\mathcal{X}_q/\mathbb{Q}_q$ = 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) $\forall f \in \mathbb{Q}_p(X_q)^*$ *(if defined):* $h_q(\mathrm{div}(f), D_2) = -\log_p(q)\,\mathrm{ord}_q(f(D_2))$.

- $\mathcal{X}_q/\mathbb{Q}_q$ = 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 $\int_{D_2} \omega_{D_1}$:
- ω_{D_1} : differential with only simple poles, and for which the residue at every pole is an integer. The points in support of D_1 are exactly the poles of ω_{D_1}, with multiplicities given by their residues.
- Since holomorphic differentials have no singularities, ω_{D_1} apriori is not determined uniquely, so we need another input to define h_p properly.

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 $\int_{D_2} \omega_{D_1}$:
- ω_{D_1} : differential with only simple poles, and for which the residue at every pole is an integer. The points in support of D_1 are exactly the poles of ω_{D_1}, with multiplicities given by their residues.
- Since holomorphic differentials have no singularities, ω_{D_1} apriori is not determined uniquely, so we need another input to define h_p properly.

Third and second 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 $\mathbb{Z}$.

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 $\int_{D_2} \omega_{D_1}$:
- ω_{D_1} : differential with only simple poles, and for which the residue at every pole is an integer. The points in support of D_1 are exactly the poles of ω_{D_1}, with multiplicities given by their residues.
- Since holomorphic differentials have no singularities, ω_{D_1} apriori is not determined uniquely, so we need another input to define h_p properly.

Third and second 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 $\mathbb{Z}$.
- ω is of the second kind if all of its residues are 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 $\int_{D_2} \omega_{D_1}$:
- ω_{D_1} : differential with only simple poles, and for which the residue at every pole is an integer. The points in support of D_1 are exactly the poles of ω_{D_1}, with multiplicities given by their residues.
- Since holomorphic differentials have no singularities, ω_{D_1} apriori is not determined uniquely, so we need another input to define h_p properly.

Third and second 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 $\mathbb{Z}$.
- ω is of the second kind if all of its residues are 0.

- $\{\text{third kind}\} \cap \{\text{second kind}\} = \{\text{holomorphic}\}$.

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 $\int_{D_2} \omega_{D_1}$:
- ω_{D_1} : differential with only simple poles, and for which the residue at every pole is an integer. The points in support of D_1 are exactly the poles of ω_{D_1}, with multiplicities given by their residues.
- Since holomorphic differentials have no singularities, ω_{D_1} apriori is not determined uniquely, so we need another input to define h_p properly.

Third and second 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 $\mathbb{Z}$.
- ω is of the second kind if all of its residues are 0.

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

Introduction to local p-adic heights at p

- The residue divisor homomorphism is

$$\mathrm{Res}\colon \{\text{third kind on } X_p\} \longrightarrow \mathrm{Div}^0(X_p),\ \mathrm{Res}(\omega) = \sum_{P \in X_p} \mathrm{Res}_P(\omega) P.$$

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

Introduction to local p-adic heights at p

- The residue divisor homomorphism is

$$\mathrm{Res}\colon \{\text{third kind on } X_p\} \longrightarrow \mathrm{Div}^0(X_p),\ \mathrm{Res}(\omega) = \sum_{P\in X_p} \mathrm{Res}_P(\omega)P.$$

- Res surjective, but not injective ($\mathrm{Res}(\{\text{holomorphic}\}) = 0$).
- Want ω_{D_1} to be such that $\mathrm{Res}(\omega_{D_1}) = D_1$. This choice is not unique!
- $\exists$ homomorphism "projection" ψ (with many useful properties):

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

Introduction to local p-adic heights at p

- The residue divisor homomorphism is

$$\mathrm{Res}\colon \{\text{third kind on } X_p\} \longrightarrow \mathrm{Div}^0(X_p),\ \mathrm{Res}(\omega) = \sum_{P \in X_p} \mathrm{Res}_P(\omega) P.$$

- Res surjective, but not injective ($\mathrm{Res}(\{\text{holomorphic}\}) = 0$).
- Want ω_{D_1} to be such that $\mathrm{Res}(\omega_{D_1}) = D_1$. This choice is not unique!
- $\exists$ homomorphism "projection" ψ (with many useful properties):

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

- Input for h_p: 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 $\mathrm{H}^{1,0}_{\mathrm{dR}}(X_p/\mathbb{Q}_p)$.

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

- $\implies D \in \mathrm{Div}^0(X_p) \rightsquigarrow$ unique ω_D of the third kind such that

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

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 $h_p(D_1, D_2) := \int_{D_2} \omega_{D_1}$.

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.
* When X_p has good ordinary reduction, we can take $W_p :=$ the unit root subspace (necessary for p-adic BSD).

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.
* When X_p has good ordinary reduction, we can take $W_p :=$ the unit root subspace (necessary for p-adic BSD).
* Independent of a model of X_p under reasonable technical conditions: $\tau\colon X_p \to X'_p \implies h_p(\tau_*(D_1), \tau_*(D_2))_{\text{on } X'_p} = h_p(D_1, D_2)_{\text{on } X_p}$.

Coleman integration in Sage

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

Coleman integration in Sage

- Sage implementation - Balakrishnan: Hyperelliptic curves $C: y^2 = f(x)/\mathbb{Q}_p$ (WARNING: Sage sees only one point at infinity!):
- Monsky-Washnitzer basis differentials $\omega_i := \frac{x^i dx}{y}$ for $0 \leq i \leq \deg(f) - 2 \rightsquigarrow$ can compute $\int_S^R \omega_i$.
- In particular: Coleman integrals of holomorphic differentials.

Coleman integration in Sage

- Sage implementation - Balakrishnan: Hyperelliptic curves $C : y^2 = f(x)/\mathbb{Q}_p$ (WARNING: Sage sees only one point at infinity!):
- Monsky-Washnitzer basis differentials $\omega_i := \frac{x^i dx}{y}$ for $0 \leq i \leq \deg(f) - 2 \rightsquigarrow$ can compute $\int_S^R \omega_i$.
- In particular: Coleman integrals of holomorphic differentials.
- Tiny integrals $\int_S^R \omega$, where $S \equiv R \pmod p$.

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.
- 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.
- 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. Denote by $\iota\colon C \to C$ 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.
- 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. Denote by $\iota\colon C \to C$ the hyperelliptic involution.
- Recall: Balakrishnan and Besser [BB] compute $h_p(P - Q, R - S)$ when $\deg(f)$ odd.
- Gajović-Müller [GM]: Compute $h_p(P - Q, R - S)$ for all hyperelliptic curves over $\mathbb{Q}_p$ with good reduction.

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.
- 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. Denote by $\iota\colon C \to C$ the hyperelliptic involution.
- Recall: Balakrishnan and Besser [BB] compute $h_p(P - Q, R - S)$ when $\deg(f)$ odd.
- Gajović-Müller [GM]: Compute $h_p(P - Q, R - S)$ for all hyperelliptic curves over $\mathbb{Q}_p$ with good reduction.
- For even degree, one more case - when $\{P, Q\} = \{\infty_-, \infty_+\}$. [GM] depends on the points - if they are all affine or $\{P, Q\} = \{\infty_-, \infty_+\}$.

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.
- 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. Denote by $\iota\colon C \to C$ the hyperelliptic involution.
- Recall: Balakrishnan and Besser [BB] compute $h_p(P - Q, R - S)$ when $\deg(f)$ odd.
- Gajović-Müller [GM]: Compute $h_p(P - Q, R - S)$ for all hyperelliptic curves over $\mathbb{Q}_p$ with good reduction.
- For even degree, one more case - when $\{P, Q\} = \{\infty_-, \infty_+\}$. [GM] depends on the points - if they are all affine or $\{P, Q\} = \{\infty_-, \infty_+\}$.
- We now recall [BB] algorithm. [GM] follows the key steps of [BB], but computes some of them differently.

[BB] algorithm - key steps

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

[BB] algorithm - key steps

(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 - key steps

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

[BB] algorithm - key steps

(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 $\psi(\omega')$ 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 - key steps

(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 $\psi(\omega')$ 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 - key steps

(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 $\psi(\omega')$ 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 $\int_S^R \omega'$.

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

Computations depending only on C

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve of genus g.
- We need to compute some quantities related only to C:

Computations depending only on C

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve of genus g.
- We need to compute some quantities related only to C:

(i) Extend the basis $\{\omega_0, \ldots, \omega_{g-1}\}$ of $\mathrm{H}^{1,0}_{\mathrm{dR}}(C/\mathbb{Q}_p)$ to a basis $B_{\mathrm{H}^1_{\mathrm{dR}}}$ of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ using Monsky-Washnitzer basis differentials.

Computations depending only on C

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve of genus g.
- We need to compute some quantities related only to C:

(i) Extend the basis $\{\omega_0, \dots, \omega_{g-1}\}$ of $\mathrm{H}^{1,0}_{\mathrm{dR}}(C/\mathbb{Q}_p)$ to a basis $B_{\mathrm{H}^1_{\mathrm{dR}}}$ of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ using Monsky-Washnitzer basis differentials.

(ii) A basis B_{W_p} of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ corresponding to the decomposition $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) = \mathrm{H}^{1,0}_{\mathrm{dR}}(C/\mathbb{Q}_p) \oplus W_p$ for the fixed complement W_p.

Computations depending only on C

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve of genus g.
- We need to compute some quantities related only to C:

(i) Extend the basis $\{\omega_0, \dots, \omega_{g-1}\}$ of $\mathrm{H}^{1,0}_{\mathrm{dR}}(C/\mathbb{Q}_p)$ to a basis $B_{\mathrm{H}^1_{\mathrm{dR}}}$ of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ using Monsky-Washnitzer basis differentials.

(ii) A basis B_{W_p} of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ corresponding to the decomposition $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) = \mathrm{H}^{1,0}_{\mathrm{dR}}(C/\mathbb{Q}_p) \oplus W_p$ for the fixed complement W_p.

(iii) Cup product matrix CPM.

Computations depending only on C

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve of genus g.
- We need to compute some quantities related only to C:

(i) Extend the basis $\{\omega_0, \ldots, \omega_{g-1}\}$ of $\mathrm{H}^{1,0}_{\mathrm{dR}}(C/\mathbb{Q}_p)$ to a basis $B_{\mathrm{H}^1_{\mathrm{dR}}}$ of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ using Monsky-Washnitzer basis differentials.

(ii) A basis B_{W_p} of $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$ corresponding to the decomposition $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p) = \mathrm{H}^{1,0}_{\mathrm{dR}}(C/\mathbb{Q}_p) \oplus W_p$ for the fixed complement W_p.

(iii) Cup product matrix CPM.

(iv) Action of Frobenius $\phi : C \longrightarrow C$ (given by $x \mapsto x^p$) on $\mathrm{H}^1_{\mathrm{dR}}(C/\mathbb{Q}_p)$.

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 $\mathrm{Res}(\omega') = \infty_- - \infty_+$.

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

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 $\omega' = \omega_g = \frac{x^g\,dx}{y}$.

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

* Only in terms of the Frobenius map and the reduction in cohomology (trick: $\phi^*(\omega') - p\omega'$ is of second kind).

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

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

- Base change from $B_{\mathrm{H}^1_{\mathrm{dR}}}$ to B_{W_p} $\rightsquigarrow$ compute $u_0, \ldots, u_{g-1} \in \mathbb{Q}_p$ such that $\omega_h = \sum_{i=0}^{g-1} u_i \omega_i$.
- Recall $h_p(\infty_- - \infty_+, R - S) = \int_S^R \omega$ for $\omega := \omega' - \sum_{i=0}^{g-1} u_i \omega_i$.

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

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

* Base change from $B_{\mathrm{H}^1_{\mathrm{dR}}}$ to $B_{W_p} \rightsquigarrow$ compute $u_0, \ldots, u_{g-1} \in \mathbb{Q}_p$ such that $\omega_h = \sum_{i=0}^{g-1} u_i \omega_i$.
* Recall $h_p(\infty_- - \infty_+, R - S) = \int_S^R \omega$ for $\omega := \omega' - \sum_{i=0}^{g-1} u_i \omega_i$.

(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 $h_p(P - Q, R - S)$ - 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 $\operatorname{div}\left(\frac{x - x(P)}{x - x(Q)}\right) = P + \iota(P) - Q - \iota(Q)$.
- Rewrite $P - Q = \frac{1}{2}\operatorname{div}\left(\frac{x - x(P)}{x - x(Q)}\right) + \frac{1}{2}(P - \iota(P)) - \frac{1}{2}(Q - \iota(Q)) =$ principal $+$ antisymmetric divisors.

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 $P - Q = \frac{1}{2}\operatorname{div}\left(\frac{x - x(P)}{x - x(Q)}\right) + \frac{1}{2}(P - \iota(P)) - \frac{1}{2}(Q - \iota(Q)) =$ principal $+$ antisymmetric divisors.
- Recall $h_p(\operatorname{div}(f), D_2) = \log_p(f(D_2)) \rightsquigarrow$ enough to compute antisymmetric heights $h_p(P - \iota(P), R - S)$.

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

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

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

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

(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 $\operatorname{Res}(\omega') = P - \iota(P)$.

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

* [BB] express it in terms of CPM, some Coleman integrals and certain residues of differentials.

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

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

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

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

* [BB] express it in terms of *CPM*, some Coleman integrals and certain residues of differentials.
* (NEW) [GM] All these residues are 0 - computational improvement.

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

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

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

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

  * [BB] express it in terms of *CPM*, some Coleman integrals and certain residues of differentials.

  * (NEW) [GM] All these residues are 0 - computational improvement.

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

Computation of $h_p(P - \iota(P), R - S)$ - key step

(viii) (NEW) Compute

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

Computation of $h_p(P - \iota(P), R - S)$ - key step

(viii) (NEW) Compute

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

- * [BB] compute it using a clever but complicated formula that involves computing residues over Weierstrass points which are defined over extensions of $\mathbb{Q}_p$.

- Use a change of variables $\tau \colon C \to C'$ that maps $P, \iota(P) \in C$ to $\infty_-, \infty_+ \in C'$, we have

$$\Longrightarrow \left(\int_S^R \frac{y(P)}{x - x(P)} \frac{dx}{y} \right)_{\text{on } C} = \left(\int_{\tau(S)}^{\tau(R)} \frac{x^g \, dx}{y} \right)_{\text{on } C'}.$$

Computation of $h_p(P - \iota(P), R - S)$ - key step

(viii) (NEW) Compute

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

* [BB] compute it using a clever but complicated formula that involves computing residues over Weierstrass points which are defined over extensions of $\mathbb{Q}_p$.

- Use a change of variables $\tau\colon C \to C'$ that maps $P, \iota(P) \in C$ to $\infty_-, \infty_+ \in C'$, we have

$$\Longrightarrow \left(\int_S^R \frac{y(P)}{x - x(P)} \frac{dx}{y}\right)_{\text{on}\, C} = \left(\int_{\tau(S)}^{\tau(R)} \frac{x^g\, dx}{y}\right)_{\text{on}\, C'}.$$

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

Importance of the infinity case

- Recall: change of variables $\tau\colon C \to C'$ maps $P, \iota(P) \in C$ to $\infty_-, \infty_+ \in C'$
- 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 $h_p(\infty_- - \infty_+, R - S)$!

Importance of the infinity case

- Recall: change of variables $\tau \colon C \to C'$ maps $P, \iota(P) \in C$ to $\infty_-, \infty_+ \in C'$
- 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 $h_p(\infty_- - \infty_+, R - S)$!
- (NEW - work in progress) Our approach generalises to superelliptic curves. Further goal: more general curves using divisors of degree zero supported at infinity.

Quickly recall the algorithm

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve and $P, Q, R, S \in C(\mathbb{Q}_p)$. Want to compute $h_p(P - Q, R - S)$.

Quickly recall the algorithm

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve and $P, Q, R, S \in C(\mathbb{Q}_p)$. Want to compute $h_p(P - Q, R - S)$.
- Precompute all quantities related to C only.

Quickly recall the algorithm

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve and $P, Q, R, S \in C(\mathbb{Q}_p)$. Want to compute $h_p(P - Q, R - S)$.
- Precompute all quantities related to C only.
- $h_p(P - Q, R - S) =$ computed $+ \frac{1}{2}(h_p(P - \iota(P), R - S) - h_p(Q - \iota(Q), R - S))$.

Quickly recall the algorithm

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve and $P, Q, R, S \in C(\mathbb{Q}_p)$. Want to compute $h_p(P-Q, R-S)$.
- Precompute all quantities related to C only.
- $h_p(P-Q, R-S) =$ computed $+\frac{1}{2}(h_p(P-\iota(P), R-S) - h_p(Q-\iota(Q), R-S))$.
- We can compute $h_p(P-\iota(P), R-S)$ as $h_p(\infty_- - \infty_+, R'-S')$ on some other hyperelliptic curve $C'/\mathbb{Q}_p$, but prefer directly.

Quickly recall the algorithm

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve and $P, Q, R, S \in C(\mathbb{Q}_p)$. Want to compute $h_p(P - Q, R - S)$.
- Precompute all quantities related to C only.
- $h_p(P - Q, R - S) =$ computed $+\frac{1}{2}(h_p(P - \iota(P), R - S) - h_p(Q - \iota(Q), R - S))$.
- We can compute $h_p(P - \iota(P), R - S)$ as $h_p(\infty_- - \infty_+, R' - S')$ on some other hyperelliptic curve $C'/\mathbb{Q}_p$, but prefer directly.
- For $\omega' = \dfrac{y(P)}{x - x(P)} \dfrac{dx}{y}$, we have $\mathrm{Res}(\omega') = P - \iota(P)$.
- We compute $\psi(\omega')$ and find the correct one $\omega_P = \omega' -$ holomorphic.

Quickly recall the algorithm

- Let $C/\mathbb{Q}_p$ be a hyperelliptic curve and $P, Q, R, S \in C(\mathbb{Q}_p)$. Want to compute $h_p(P-Q, R-S)$.
- Precompute all quantities related to C only.
- $h_p(P-Q, R-S) =$ computed $+\frac{1}{2}(h_p(P-\iota(P), R-S) - h_p(Q-\iota(Q), R-S))$.
- We can compute $h_p(P-\iota(P), R-S)$ as $h_p(\infty_- - \infty_+, R'-S')$ on some other hyperelliptic curve $C'/\mathbb{Q}_p$, but prefer directly.
- For $\omega' = \frac{y(P)}{x-x(P)}\frac{dx}{y}$, we have $\mathrm{Res}(\omega') = P - \iota(P)$.
- We compute $\psi(\omega')$ and find the correct one $\omega_P = \omega' -$ holomorphic.
- Compute $h_p(P-\iota(P), R-S) = \int_S^R \omega' - \int_S^R \text{holomorphic} =$ $= \int_{S'}^{R'} \frac{x^g\,dx}{y} - \int_S^R \text{holomorphic}$.
- Similarly, compute $h_p(Q-\iota(Q), R-S)$, hence, $h_p(P-Q, R-S)$.

Summary for the local p-adic height above p

- The main difference between [BB] and our algorithm is in computing Coleman integrals of differentials of the third kind and residues.
- Our algorithm is simpler and faster than [BB], and works for both odd and even degree models.

Summary for the local p-adic height above p

- The main difference between [BB] and our algorithm is in computing Coleman integrals of differentials of the third kind and residues.
- Our algorithm is simpler and faster than [BB], and works for both odd and even degree models.
- We compare the timings and success of our and [BB] algorithm in several examples.

Genus	p	Precision	Our time	[BB] time
2	7	10	2s	7s
2	7	300	11m	?>1week
2	503	10	4m	19h
3	11	10	6s	28s
4	23	20	2m	46m
17	11	7	14m	?>1week

Linear Quadratic Chabauty for integral points

- $X/\mathbb{Q}$ = 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 $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee \rightsquigarrow$ we want to use quadratic Chabauty.

Linear Quadratic Chabauty for integral points

- $X/\mathbb{Q}$ = 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 $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee \rightsquigarrow$ we want to use quadratic Chabauty.
- Let $X/\mathbb{Q} \colon y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ monic, $\deg(f) = 2g + 2$.
- Then $\infty_\pm \in X(\mathbb{Q})$. Let $D_\infty := [\infty_- - \infty_+]$.

Linear Quadratic Chabauty for integral points

- $X/\mathbb{Q}$ = 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 $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee$ $\rightsquigarrow$ we want to use quadratic Chabauty.
- Let $X/\mathbb{Q}\colon y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ monic, $\deg(f) = 2g + 2$.
- Then $\infty_\pm \in X(\mathbb{Q})$. Let $D_\infty := [\infty_- - \infty_+]$.
- Denote $X(\mathbb{Z})$:= integral points on X. Goal today: Compute $X(\mathbb{Z})$.

Linear Quadratic Chabauty for integral points

- $X/\mathbb{Q}$ = 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 $(J(\mathbb{Q}) \otimes \mathbb{Q}_p)^\vee \rightsquigarrow$ we want to use quadratic Chabauty.
- Let $X/\mathbb{Q} \colon y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ monic, $\deg(f) = 2g + 2$.
- Then $\infty_\pm \in X(\mathbb{Q})$. Let $D_\infty := [\infty_- - \infty_+]$.
- Denote $X(\mathbb{Z}) :=$ integral points on X. Goal today: Compute $X(\mathbb{Z})$.
- Recall: $h \colon J(\mathbb{Q}) \times J(\mathbb{Q}) \longrightarrow \mathbb{Q}_p$ is a bilinear pairing.
- Then $\lambda(D) := h(D_\infty, D)$ is a linear map $J(\mathbb{Q}) \longrightarrow \mathbb{Q}_p$.
- $\rightsquigarrow$ We can write $h(D_\infty, D) = \sum_{i=0}^{g-1} \alpha_i \int_D \omega_i$, for some $\alpha_i \in \mathbb{Q}_p$.

Linear Quadratic Chabauty for integral points

- Assume $P_0 \in X(\mathbb{Z})$. Consider $\rho_{P_0} \colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) := \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - h_p(D_\infty, P - P_0) = \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - \int_{P_0}^{P} \omega_{D_\infty}.$$

Linear Quadratic Chabauty for integral points

- Assume $P_0 \in X(\mathbb{Z})$. Consider $\rho_{P_0} \colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) := \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - h_p(D_\infty, P - P_0) = \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - \int_{P_0}^{P} \omega_{D_\infty}.$$

- ρ_Q is a locally analytic function.
- If $P \in X(\mathbb{Q})$, $\rho_{P_0}(P) = h - h_p = \sum_{q \neq p} h_q(D_\infty, P - P_0)$.

Linear Quadratic Chabauty for integral points

- Assume $P_0 \in X(\mathbb{Z})$. Consider $\rho_{P_0} \colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) := \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - h_p(D_\infty, P - P_0) = \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - \int_{P_0}^{P} \omega_{D_\infty}.$$

- ρ_Q is a locally analytic function.
- If $P \in X(\mathbb{Q})$, $\rho_{P_0}(P) = h - h_p = \sum_{q \neq p} h_q(D_\infty, P - P_0)$.
- We prove $\forall q \neq p, \forall P, Q \in X(\mathbb{Z}_q)$:
  (1) $h_q(D_\infty, P - Q) \in$ finite and computable T_q;
  (2) $T_q = \{0\}$ for almost all (including good) primes.
- $\implies \rho_{P_0}(X(\mathbb{Z})) \subseteq T$ for a finite and computable set T.

Linear Quadratic Chabauty for integral points

- Assume $P_0 \in X(\mathbb{Z})$. Consider $\rho_{P_0} : X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) := \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - h_p(D_\infty, P - P_0) = \sum_{i=0}^{g-1} \alpha_i \int_{P_0}^{P} \omega_i - \int_{P_0}^{P} \omega_{D_\infty}.$$

- ρ_Q is a locally analytic function.
- If $P \in X(\mathbb{Q})$, $\rho_{P_0}(P) = h - h_p = \sum_{q \neq p} h_q(D_\infty, P - P_0)$.
- We prove $\forall q \neq p, \forall P, Q \in X(\mathbb{Z}_q)$:
  (1) $h_q(D_\infty, P - Q) \in$ finite and computable T_q;
  (2) $T_q = \{0\}$ for almost all (including good) primes.
- $\implies \rho_{P_0}(X(\mathbb{Z})) \subseteq T$ for a finite and computable set T.
- We can compute $S := \rho_{P_0}^{-1}(T) \rightsquigarrow X(\mathbb{Z}) \subseteq S$ for some finite and computable $S \subseteq X(\mathbb{Q}_p)$. If necessary + Mordell-Weil sieve $\rightsquigarrow X(\mathbb{Z})$.

LQC for integral points - algorithm + example $r = g = 2$

- Let $X/\mathbb{Q} : y^2 = f(x) = x^6 + 2x^5 - 7x^4 - 18x^3 + 2x^2 + 20x + 9$.
- $X(\mathbb{Z})_{\text{known}} := \{(0, \pm 3), (1, \pm 3), (-1, \pm 1), (-2, \pm 3), (-4, \pm 37)\}$.
- Goal: Prove $X(\mathbb{Z}) = X(\mathbb{Z})_{\text{known}}$. Use $p = 7$.

LQC for integral points - algorithm + example $r = g = 2$

- Let $X/\mathbb{Q} : y^2 = f(x) = x^6 + 2x^5 - 7x^4 - 18x^3 + 2x^2 + 20x + 9$.
- $X(\mathbb{Z})_{\text{known}} := \{(0, \pm 3), (1, \pm 3), (-1, \pm 1), (-2, \pm 3), (-4, \pm 37)\}$.
- Goal: Prove $X(\mathbb{Z}) = X(\mathbb{Z})_{\text{known}}$. Use $p = 7$.

(1) Compute the finite set $T := \{\sum_{q \neq p} h_q(D_\infty, P - Q) \colon P, Q \in X(\mathbb{Z}_q)\}$.

- For $P, Q \in X(\mathbb{Z}_q)$ and all $q \neq 7$: $h_q(D_\infty, P - Q) = 0 \implies T = \{0\}$.

LQC for integral points - algorithm + example $r = g = 2$

- Let $X/\mathbb{Q} : y^2 = f(x) = x^6 + 2x^5 - 7x^4 - 18x^3 + 2x^2 + 20x + 9$.
- $X(\mathbb{Z})_{\text{known}} := \{(0, \pm 3), (1, \pm 3), (-1, \pm 1), (-2, \pm 3), (-4, \pm 37)\}$.
- Goal: Prove $X(\mathbb{Z}) = X(\mathbb{Z})_{\text{known}}$. Use $p = 7$.

(1) Compute the finite set $T := \{\sum_{q \neq p} h_q(D_\infty, P - Q) \colon P, Q \in X(\mathbb{Z}_q)\}$.

- For $P, Q \in X(\mathbb{Z}_q)$ and all $q \neq 7$: $h_q(D_\infty, P - Q) = 0 \implies T = \{0\}$.

(2) Represent $h(D_\infty, D) = \alpha_0 \int_D \omega_0 + \cdots + \alpha_{g-1} \int_D \omega_{g-1}$.

- Find D_0, D_1 such that $[J(\mathbb{Q}) : \langle D_0, D_1 \rangle] < \infty$. Solve the system of equations for $i = 0, 1$ to compute α_0, α_1

$$h(D_\infty, D_i) = \alpha_0 \int_{D_i} \omega_0 + \alpha_1 \int_{D_i} \omega_1.$$

$$\implies \alpha_0 = 5 + 4 \cdot 7 + 6 \cdot 7^2 + O(7^3),\ \alpha_1 = 6 + 3 \cdot 7 + 5 \cdot 7^2 + O(7^3).$$

LQC for integral points - algorithm + example $r = g = 2$

(3) Assume $P_0 \in X(\mathbb{Z})$. Define $\rho_{P_0}\colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) = \alpha_0 \int_{P_0}^{P} \omega_0 + \cdots + \alpha_{g-1} \int_{P_0}^{P} \omega_{g-1} - h_p(D_\infty, P - P_0).$$

- Set $P_0 = (0, 3)$. Define $\rho_{P_0}(P)\colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) = \alpha_0 \int_{P_0}^{P} \omega_0 + \alpha_1 \int_{P_0}^{P} \omega_1 - h_p(D_\infty, P - P_0).$$

- $\implies \rho_{P_0}(X(\mathbb{Z})) = \{0\}$.

LQC for integral points - algorithm + example $r = g = 2$

(3) Assume $P_0 \in X(\mathbb{Z})$. Define $\rho_{P_0}\colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) = \alpha_0 \int_{P_0}^{P} \omega_0 + \cdots + \alpha_{g-1} \int_{P_0}^{P} \omega_{g-1} - h_p(D_\infty, P - P_0).$$

- Set $P_0 = (0,3)$. Define $\rho_{P_0}(P)\colon X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$

$$\rho_{P_0}(P) = \alpha_0 \int_{P_0}^{P} \omega_0 + \alpha_1 \int_{P_0}^{P} \omega_1 - h_p(D_\infty, P - P_0).$$

- $\implies \rho_{P_0}(X(\mathbb{Z})) = \{0\}$.

(4) In each affine $D(Q)$, for $P \in D(Q)$, compute $\rho(P) \in \mathbb{Q}_p[[z]]$.

- Consider $Q = P_0 = (0,3)$ and $P = (7z, \cdot) \in D(P_0)$ for some $z \in \mathbb{Z}_7$:

$$\rho_{P_0}(z) = (42 + O(7^2))z + (6 \cdot 7^3 + O(7^4))z^2 + (62 \cdot 7^3 + O(7^6))z^3 + O((7z)^4).$$

LQC for integral points - algorithm + example + theorem

(5) For each $u \in T$, p-adically locate the solutions of $\rho_{P_0}(z) = u$ in all affine residue discs. Obtain a finite set S: $X(\mathbb{Z}) \subseteq S \subseteq X(\mathbb{Q}_p)$.

LQC for integral points - algorithm + example + theorem

(5) For each $u \in T$, p-adically locate the solutions of $\rho_{P_0}(z) = u$ in all affine residue discs. Obtain a finite set S: $X(\mathbb{Z}) \subseteq S \subseteq X(\mathbb{Q}_p)$.

- Recall, for $P \in D(Q)$, parameterised by z,

$$\rho_{P_0}(z) = (42+O(7^2))z+(6\cdot7^3+O(7^4))z^2+(62\cdot7^3+O(7^6))z^3+O((7z)^4).$$

- Strassmann's theorem $\implies$ $D(Q) \cap X(\mathbb{Z}) = \{Q\}$.

LQC for integral points - algorithm + example + theorem

(5) For each $u \in T$, p-adically locate the solutions of $\rho_{P_0}(z) = u$ in all affine residue discs. Obtain a finite set S: $X(\mathbb{Z}) \subseteq S \subseteq X(\mathbb{Q}_p)$.

- Recall, for $P \in D(Q)$, parameterised by z,

$$\rho_{P_0}(z) = (42 + O(7^2))z + (6\cdot 7^3 + O(7^4))z^2 + (62\cdot 7^3 + O(7^6))z^3 + O((7z)^4).$$

- Strassmann's theorem $\implies$ $D(Q) \cap X(\mathbb{Z}) = \{Q\}$.
- Similarly in all affine residue discs $\implies$ $X(\mathbb{Z}) = S = X(\mathbb{Z})_{\text{known}}$.

(5) For each $u \in T$, p-adically locate the solutions of $\rho_{P_0}(z) = u$ in all affine residue discs. Obtain a finite set S: $X(\mathbb{Z}) \subseteq S \subseteq X(\mathbb{Q}_p)$.

- Recall, for $P \in D(Q)$, parameterised by z,

$$\rho_{P_0}(z) = (42+O(7^2))z+(6\cdot7^3+O(7^4))z^2+(62\cdot7^3+O(7^6))z^3+O((7z)^4).$$

- Strassmann's theorem $\implies$ $D(Q) \cap X(\mathbb{Z}) = \{Q\}$.
- Similarly in all affine residue discs $\implies$ $X(\mathbb{Z}) = S = X(\mathbb{Z})_{\text{known}}$.

(6) If necessary, use the Mordell-Weil sieve to determine $S \backslash X(\mathbb{Q})$.

LQC for integral points - algorithm + example + theorem

(5) For each $u \in T$, p-adically locate the solutions of $\rho_{P_0}(z) = u$ in all affine residue discs. Obtain a finite set S: $X(\mathbb{Z}) \subseteq S \subseteq X(\mathbb{Q}_p)$.

- Recall, for $P \in D(Q)$, parameterised by z,

$$\rho_{P_0}(z) = (42+O(7^2))z+(6\cdot 7^3+O(7^4))z^2+(62\cdot 7^3+O(7^6))z^3+O((7z)^4).$$

- Strassmann's theorem $\implies$ $D(Q) \cap X(\mathbb{Z}) = \{Q\}$.
- Similarly in all affine residue discs $\implies$ $X(\mathbb{Z}) = S = X(\mathbb{Z})_{\text{known}}$.

(6) If necessary, use the Mordell-Weil sieve to determine $S \backslash X(\mathbb{Q})$.

Theorem (G.-Müller, 2022)

- *$X/\mathbb{Q}$: $y^2 = f(x)$ nice, with $f \in \mathbb{Z}[x]$ monic,* $\deg(f) = 2g+2$ *with $r = g$. There is a locally analytic function $\rho : X(\mathbb{Q}_p) \to \mathbb{Q}_p$, and a finite and computable set T, such that $\rho(X(\mathbb{Z})) \in T$.*

LQC for integral points - algorithm + example + theorem

(5) For each $u \in T$, p-adically locate the solutions of $\rho_{P_0}(z) = u$ in all affine residue discs. Obtain a finite set S: $X(\mathbb{Z}) \subseteq S \subseteq X(\mathbb{Q}_p)$.

- Recall, for $P \in D(Q)$, parameterised by z,

$$\rho_{P_0}(z) = (42+O(7^2))z+(6\cdot 7^3+O(7^4))z^2+(62\cdot 7^3+O(7^6))z^3+O((7z)^4).$$

- Strassmann's theorem $\implies$ $D(Q) \cap X(\mathbb{Z}) = \{Q\}$.
- Similarly in all affine residue discs $\implies$ $X(\mathbb{Z}) = S = X(\mathbb{Z})_{\text{known}}$.

(6) If necessary, use the Mordell-Weil sieve to determine $S \setminus X(\mathbb{Q})$.

Theorem (G.-Müller, 2022)

- *$X/\mathbb{Q}$: $y^2 = f(x)$ nice, with $f \in \mathbb{Z}[x]$ monic,* $\deg(f) = 2g+2$ *with $r = g$. There is a locally analytic function $\rho : X(\mathbb{Q}_p) \to \mathbb{Q}_p$, and a finite and computable set T, such that $\rho(X(\mathbb{Z})) \in T$.*
- *Extended to number fields with an appropriate rank condition.*

The end

Thank you for your attention!

Question

Any questions?