Algorithms for p-adic heights on hyperelliptic curves of arbitrary reduction

Enis Kaya (KU Leuven)
joint work with
Francesca Bianchi and J. Steffen Müller

Sixteenth Algorithmic Number Theory Symposium
Massachusetts Institute of Technology
July 18, 2024

Introduction

Let p be an odd prime number. In the literature, there are several definitions of p-adic height pairings on abelian varieties defined over $\mathbb{Q}$. Some of the definitions were given by Schneider, Mazur–Tate and Nekovář. For Jacobians of curves, there is another definition due to Coleman–Gross.

Algorithms for computing p-adic heights

- allow one to compute p-adic regulators, some of which fit into p-adic versions of BSD conjecture, and
- play a crucial role in carrying out the quadratic Chabauty method to determine integral/rational points on curves of genus at least two.

Goal

Present algorithms to compute

- Coleman–Gross height on hyperelliptic Jacobians, and
- Mazur–Tate height on Jacobian surfaces.

Overview

1. The Coleman–Gross p-adic height pairing
   - Basic definitions
   - The local component at p
   - Computation of Ψ
   - Our algorithm
   - Numerical example: elliptic curve
2. The Mazur–Tate p-adic height function
   - Decomposition into p-adic Néron functions
   - Our algorithm
   - Numerical example: quadratic Chabauty for integral points

§1. The Coleman–Gross p-adic height pairing

Let $C/\mathbb{Q}$ be a nice curve. The Coleman–Gross pairing

$$h^{\mathrm{CG}}\colon \mathrm{Div}^0(C) \times \mathrm{Div}^0(C) \to \mathbb{Q}_p$$

is defined as

$$h^{\mathrm{CG}} = h_p^{\mathrm{CG}} + \sum_{q \neq p} h_q^{\mathrm{CG}}.$$

The local components away from p are described using "arithmetic intersection theory" and their computation is standard these days, but

$$h_p^{\mathrm{CG}}(D_1, D_2) := {}^{\mathrm{Vol}}\!\!\int_{D_2} \omega_{D_1}$$

where

- ω_{D_1} is a "canonical" differential form attached to D_1, and
- ${}^{\mathrm{Vol}}\!\!\int$ is the Vologodsky integration.

From now on, everything is local; so set $X = C \otimes \mathbb{Q}_p$.

§1. Vologodsky integration

Let ω be a meromorphic 1-form on X, let $P, Q \in X(\mathbb{Q}_p)$. To this data, Vologodsky associated an integral

$$\prescript{\mathrm{Vol}}{}{\int_P^Q} \omega \in \mathbb{Q}_p$$

that satisfies the desirable properties. It's called the **Vologodsky integral**.

Remarks:

1. When X has good reduction,
   Vologodsky integral $=$ Coleman integral.
2. When ω is holomorphic,
   Vologodsky integral $=$ abelian integral.
3. There are practical algorithms to compute these:
   - Balakrishnan–Tuitman: Coleman integrals on smooth curves,
   - Katz–K: Vologodsky integrals on hyperelliptic curves,
   - Katz–K (in progress): Vologodsky integrals on "schön" curves.

§1. The logarithm map Ψ

I. A meromorphic 1-form ω on X is of the **third kind** if ω has at most simple poles with integer residues.

II. Let $H^1_{\mathrm{dR}}(X)$ denote the first de Rham cohomology group of X. Let

$$\cup \colon H^1_{\mathrm{dR}}(X) \times H^1_{\mathrm{dR}}(X) \to \mathbb{Q}_p$$

denote the algebraic cup product pairing on $H^1_{\mathrm{dR}}(X)$.

III. Let Ψ be the "logarithm for the universal vectorial extension" of the Jacobian of X. It is a homomorphism

$$\{\text{third kind differentials}\} \to H^1_{\mathrm{dR}}(X)$$

which is the identity on holomorphic differentials.

§1. The local component at p

Let $W = W_p$ be a subspace of $H^1_{\mathrm{dR}}(X)$ that is complementary to the space of holomorphic forms:

$$H^1_{\mathrm{dR}}(X) = H^0(X, \Omega^1_X) \oplus W.$$

There exists a unique form ω_{D_1} of the third kind satisfying

$$\mathrm{Res}(\omega_{D_1}) = D_1, \quad \Psi(\omega_{D_1}) \in W.$$

Then

$$h_p^{\mathrm{CG}}(D_1, D_2) := {}^{\mathrm{Vol}}\!\!\int_{D_2} \omega_{D_1}.$$

Remarks:

- When X has semistable ordinary reduction, there is a canonical choice for W: the unit root subspace for the action of the Frobenius endom.
- An algorithm to compute h_p^{CG} when X is hyperelliptic with good reduction was provided by Balakrishnan–Besser.

§1. Computation of Ψ

A crucial step in computing $h_p^{\mathrm{CG}}(D_1, D_2)$ is the construction of the form ω_{D_1}. This requires the explicit computation of the map Ψ, but its original definition is not suitable for computations.

Proposition (Besser): The logarithm map Ψ can be expressed in terms of the cup product and "global symbol".

Global symbol is defined in terms of Vologodsky integration, so

$$\text{Computing } \Psi \quad \approx \quad \begin{array}{c}\text{computing Vol.}\\ \text{integrals}\end{array} + \begin{array}{c}\text{computing cup}\\ \text{products}\end{array}$$

§1. Computing CG heights on hyperelliptic curves

Let $C/\mathbb{Q}$ be a genus-g hyperelliptic curve with affine model

$$y^2 = f(x), \quad f(x) \in \mathbb{Z}[x] \text{ is monic.}$$

For simplicity, we assume that $\deg(f(x))$ is odd.

The height pairing is bilinear. Therefore we may assume that

$$D_1 = (P) - (Q), \quad D_2 = (R) - (S).$$

We also assume that P, Q, R, S are pairwise distinct.

Set $X = C \otimes \mathbb{Q}_p$. Let $W = W_p$ be a subspace of $H^1_{\mathrm{dR}}(X)$ such that

$$H^1_{\mathrm{dR}}(X) = H^0(X, \Omega^1_X) \oplus W.$$

Step 1. *Pick an* ω *of the third kind with residue divisor* $D_1 = (P) - (Q)$:

$$\omega := \begin{cases} \left(\frac{y + y(P)}{x - x(P)} - \frac{y + y(Q)}{x - x(Q)}\right)\frac{dx}{2y} & \text{if } P \text{ and } Q \text{ are finite;} \\ \frac{y + y(P)}{x - x(P)}\frac{dx}{2y} & \text{if } P \text{ is finite, } Q \text{ is infinite.} \end{cases}$$

Step 2. *Determine the holomorphic form* η *such that* $\Psi(\omega - \eta)$ *lies in* W*; then* $\omega_{D_1} = \omega - \eta$:

I. Compute $\Psi(\omega)$ as an element of $H^1_{\mathrm{dR}}(X)$.

II. Compute $\Psi(\omega)$ as an element of $H^0(X, \Omega^1_X) \oplus W$.

III. Compare them and get η.

§1. Computing CG heights on hyperelliptic curves

Step 3. *Compute the Vologodsky integral* ${}^{\mathrm{Vol}}\!\int_{D_2} \omega_{D_1} = {}^{\mathrm{Vol}}\!\int_S^R (\omega - \eta)$:

I. Cover X by $\{U_i\}_i$ such that each U_i can be embedded into X_i, which is

- either a rational curve,
- or a hyperelliptic curve of good reduction.

II. Express Vologodsky integrals on X as explicit linear combinations of Vologodsky integrals on X_i.

III. In order to compute Vologodsky integrals on X_i,

- parametrize X_i if it is rational,
- make use of the Coleman integration algorithms if X_i is hyperelliptic.

Remark: We can define h_p^{CG} for divisors with common support, but, for instance, $h_p^{\mathrm{CG}}(P - \infty, P - \infty)$ becomes a double Vologodsky integral and we do not know (yet) how to deal with them...

§1. Computing a canonical complementary subspace

All complementary subspaces are equal,
but some are more equal than others.

We now assume that

- X has semistable ordinary reduction, and
- X has genus $g = 2$.

Extending a construction by Blakestad, Bianchi constructed a very "canonical" complementary subspace W^C of $H^1_{\mathrm{dR}}(X)$.

Proposition (Bianchi): If X has good ordinary reduction, then

$$W^C = \text{the unit root subspace.}$$

Algorithm (Bianchi–K–Müller)

We can compute Blakestad's complementary subspace W^C.

§1. Numerical example: elliptic curve

The following curve has split multiplicative reduction at $p = 43$:

$$C\colon y^2 = x^3 - 1351755x + 555015942, \quad P := \left(\tfrac{330483}{361}, \tfrac{63148032}{6859}\right) \in C(\mathbb{Q}).$$

Using `SageMath`, the "canonical" Mazur–Tate height of P is

$$19 \cdot 43 + 7 \cdot 43^2 + 8 \cdot 43^3 + 2 \cdot 43^4 + O(43^5). \tag{1}$$

Canonical MT height = CG height wrt the unit root subspace

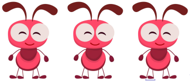
For $Q = (2523, 114912)$, $R = (219, 16416) \in C(\mathbb{Q})$, let

$$D_Q := (Q) - (-Q), \quad D_R := (R) - (-R) \quad \Longrightarrow \quad P = D_Q = D_R.$$

The Coleman–Gross height $h^{\mathrm{CG}}(D_Q, D_R)$ wrt the unit root subspace is

$$\mathbf{9 \cdot \log_{43}(2)} + 29 \cdot 43 + 28 \cdot 43^2 + 10 \cdot 43^3 + 39 \cdot 43^4 + O(43^5). \tag{2}$$

Luckily, (1) and (2) are equal...



§2. The Mazur–Tate p-adic height function

Let $C/\mathbb{Q}$ be a nice curve, and let J be its Jacobian variety. The Mazur–Tate height function

$$h^{\mathrm{MT}} \colon J(\mathbb{Q}) \to \mathbb{Q}_p$$

is defined using "biextensions".

Theorem (Bianchi, Bianchi–K.–Müller)

For each q, there exists a function $\lambda_q \colon J(\mathbb{Q}_q) \to \mathbb{Q}_p$ such that h^{MT} can be decomposed into a sum of λ_q's.

*We call λ_q the p-**adic Néron function** at q. It is*

- *the real-valued Néron function (up to a constant) for $q \neq p$;*
- *defined using Besser's "p-adic log" function for $q = p$.*

This is a p-adic analogue of a classical result in Diophantine geometry: the Néron–Tate height can be decomposed into a sum of Néron functions.

§2. Computing MT heights on Jacobian surfaces

Assume $C/\mathbb{Q}$ is of genus-2 with affine model

$$y^2 = f(x), \quad f(x) \in \mathbb{Z}[x] \text{ is quintic.}$$

Then extending a construction by Blakestad, Bianchi defined a 2-dimensional p-adic sigma function σ_p: it is a certain solution of a differential equation inside the formal group of J.

Algorithm (Bianchi, Bianchi–K.–Müller)

The p-adic Néron function λ_p is essentially the p-adic log of σ_p. Therefore, we can compute the Mazur–Tate height function h^{MT} on J.

This is a genus-2 analogue of a classical result: global p-adic heights on elliptic curves can be expressed in terms of 1-dimensional p-adic sigma functions (this goes back to Bernardi, Mazur–Tate, Mazur–Stein–Tate...).

§2. Num. example: quadratic Chabauty for integral points

Method: It uses properties of local and global heights to produce a locally analytic function

$$\rho\colon C(\mathbb{Z}_p) \to \mathbb{Q}_p$$

such that $\rho(C(\mathbb{Z})) \subset \Gamma$ for an effectively computable finite set Γ. The method requires the computation of local heights of the form $h_q(P - \infty, P - \infty)$. With our p-adic Néron function approach, this is not a problem at all:

Example: The following curve has bad reduction at $p = 5$:

$$C\colon y^2 = x^5 + x^3 - 2x + 1.$$

Applying the quadratic Chabauty method for $p = 5$, we get

$$C(\mathbb{Z}) = \{(0, \pm 1), (1, \pm 1), (-1, \pm 1)\}.$$

Remark: This is, to the best of our knowledge, the first worked quadratic Chabauty example in the literature at a prime of bad reduction...

Thank you! Dank u wel! Teşekkür ederim!

- *p-adic heights on curves* - Coleman–Gross
- *Hodge structure on the fundamental group and its application to p-adic integration* - Vologodsky
- *p-adic heights and Vologodsky integration* - Besser
- *p-adic Arakelov theory* - Besser
- *Computing local p-adic height pairings on hyperelliptic curves* - Balakrishnan–Besser
- *Coleman-Gross height pairings and the p-adic sigma function* - Balakrishnan–Besser
- *Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves* - Balakrishnan–Besser–Müller
- *Explicit Coleman integration for curves* - Balakrishnan–Tuitman
- *On generalizations of p-adic Weierstrass sigma and zeta functions* - Blakestad

- *p-adic integration on bad reduction hyperelliptic curves* - Katz–Kaya
- *Explicit Vologodsky integration for hyperelliptic curves* - Kaya
- *p-adic sigma functions and heights on Jacobians of genus 2 curves* - Bianchi
- *Coleman–Gross heights and p-adic Néron Functions on Jacobians of genus 2 curves* - Bianchi–Kaya–Müller
- *Algorithms for p-adic heights on hyperelliptic curves of arbitrary reduction* - Bianchi–Kaya–Müller