Computing canonical heights on elliptic curves in quasi-linear time

Steffen Müller (Universität Oldenburg)
and
Michael Stoll (Universität Bayreuth)

ANTS–XII
TU Kaiserslautern

Part I

Canonical heights on elliptic curves

Naive height

Let $E/\mathbb{Q}$ be an elliptic curve, given by an equation

$$W : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \,,$$

where $a_1, \ldots, a_6 \in \mathbb{Z}$ and $\Delta(W) \neq 0$.

Let

$$Q = \left(\frac{a_Q}{d_Q^2}, \frac{b_Q}{d_Q^3} \right) \in E(\mathbb{Q}), \quad \text{where}$$

$a_Q,\ b_Q,\ d_Q \in \mathbb{Z}$ and $\gcd(a_Q,\ d_Q) = 1 = \gcd(b_Q,\ d_Q)$.

The naive height of Q is given by

$$h(Q) := \log \max \left\{ |a_Q|,\ d_Q^2 \right\} \in \mathbb{R}_{\geq 0} \,.$$

We also set $h(O) = 0$ for $O = (0 : 1 : 0) \in E(\mathbb{Q})$.

Properties and applications

The canonical height (or Néron-Tate height) of $Q \in E(\mathbb{Q})$ is

$$\hat{h}(Q) := \lim_{n\to\infty} 4^{-n} h(2^n Q) \in \mathbb{R}_{\geq 0}\,.$$

Properties.

- $\hat{h}$ is a quadratic form.
- $\Psi := h - \hat{h}$ is bounded.
- $\{Q \in E(\mathbb{Q}) : \hat{h}(Q) \leq B\}$ is finite for all $B \in \mathbb{R}_{\geq 0}$.
- $\hat{h}(Q) = 0$ if and only if Q has finite order.

Goal. Given $Q \in E(\mathbb{Q})$, compute $\hat{h}(Q)$.

Applications. Required to compute

- generators of $E(\mathbb{Q})$,
- the regulator of $E(\mathbb{Q})$ (appearing in the BSD-conjecture).

Idea. $h(Q)$ is easy to compute. Only need $\Psi(Q)$.

Local height correction functions

Néron '65. Local decomposition

$$\Psi = \sum_{p \text{ prime}} \Psi_p + \Psi_\infty$$

of $\Psi = h - \hat{h}$ such that

- $\Psi_v : E(\mathbb{Q}_v) \to \mathbb{R}$ is v-adically continuous and bounded for every place v of $\mathbb{Q}$;
- $\Psi_p(Q) = 0$ if $Q \in E(\mathbb{Q}_p)$ is smooth modulo p;
- Ψ_∞ is essentially $-\log|\sigma|$, where σ is the Weierstrass sigma-function.

Archimedean correction

Bost-Mestre '93 (unpublished). Can compute $\Psi_\infty(Q)$ for $Q \in E(\mathbb{R})$ to d bits of precision in time quasi-linear in d and in $\log \|W\|$, where $\|W\| = \max\{|a_1|, \ldots, |a_6|\}$.

- Uses degeneration to a singular curve via a sequence of 2-isogenies.
- Isogenies yield quadratically convergent arithmetic-geometric mean formula.
- Extension to complex places work in progress (Caselli).
- Alternative algorithms due to Tate and Silverman.

Non-archimedean corrections

Silverman '88. Fast algorithm to compute $\Psi_p(Q)$ for p prime and $Q \in E(\mathbb{Q}_p)$, provided W is minimal at p.

Uses:

Néron '65. If W is minimal at p, then Ψ_p factors through the finite group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, where $E_0(\mathbb{Q}_p)$ is the set of points having non-singular reduction w.r.t. W.

Problem. To find $\Psi^{\mathrm{f}}(Q) := \sum_p \Psi_p(Q)$ for $Q \in E(\mathbb{Q})$ using this approach, need some integer factorization.

- Factorization of the discriminant $\Delta(W)$ suffices.
- Silverman '97. Computing a globally minimal Weierstrass equation also suffices – but this needs factorization of $\gcd(c_4(W), c_6(W))$.

Part II

An algorithm running in quasi-linear time

A new complexity estimate

Theorem (M.–Stoll '15). Let E be given by a Weierstrass equation W with coefficients in $\mathbb{Z}$ and let $Q \in E(\mathbb{Q})$.

There is an algorithm which computes $\hat{h}(Q)$ to d bits of precision in time quasi-linear in the input size $h(Q) + \log \|W\|$ and in the output size $d + h(Q)$.

- Requires no integer factorization at all.
- Does not need minimality of W.

Series expression for correction functions

There are $f, g \in \mathbb{Z}[x]$ with the following property:
If $Q = (x_Q, y_Q) \in E \setminus E[2]$, then $2Q = (x_{2Q}, y_{2Q})$ with

$$x_{2Q} = g(x_Q)/f(x_Q)\,.$$

Get

$$h(2Q) - 4h(Q) = \sum_v \varphi_v(Q) \text{ for } Q \in E(\mathbb{Q})\,,$$

where, for a place v of $\mathbb{Q}$, we set $\varphi_v(O) := 0$ and

$$\varphi_v(Q) := \log \frac{\max\{|f(x_Q)|_v, |g(x_Q)|_v\}}{\max\{|x_Q|_v^4, 1\}} \text{ for } Q \in E(\mathbb{Q}_v) \setminus \{O\}$$

By Tate's telescoping trick, can take

$$\Psi_v(Q) = -\sum_{n=0}^{\infty} 4^{-n-1} \varphi_v(2^n Q) \text{ for } Q \in E(\mathbb{Q}_v)\,.$$

Computing non-archimedean corrections

Let p be a prime, $Q \in E(\mathbb{Q}_p)$. Set

- $\varepsilon_p(Q) := -\varphi_p(Q)/\log p \in \mathbb{Z}_{\geq 0}$.
- $\mu_p(Q) := \Psi_p(Q)/\log p \in \mathbb{Q}_{\geq 0}$.

From

$$\Psi_p(Q) = -\sum_{n=0}^{\infty} 4^{-n-1}\varphi_p(2^n Q)$$

get

$$\mu_p(Q) = \sum_{n=0}^{\infty} 4^{-n-1}\varepsilon_p(2^n Q)\,.$$

Idea for computing $\mu_p(Q)$ (and hence $\psi_p(Q)$).

- Show that $0 \leq \varepsilon_p(2^n Q) \leq \operatorname{ord}_p(\Delta(W))$.
- Show that $\operatorname{denom}(\mu_p(Q)) \leq \operatorname{ord}_p(\Delta(W))$.
- Compute a sufficiently close approximation of $\mu_p(Q)$ and then find it exactly using continued fractions.

Usually slower than Silverman's algorithm – but more suitable for globalization!

Approximating Ψ^{f}

Goal. Without knowing which primes p contribute, compute

$$\Psi^{\mathrm{f}}(Q) = \sum_p \Psi_p(Q) = \sum_p \mu_p(Q) \log p \,.$$

for $Q \in E(\mathbb{Q})$.

- Have

$$\Psi^{\mathrm{f}}(Q) = \sum_{n=0}^{\infty} 4^{-n-1} \sum_p \varepsilon_p(2^n Q) \log p = \sum_{n=0}^{\infty} 4^{-n-1} \log g_n \,,$$

  where $g_n \in \mathbb{Z}_{\geq 0}$.
- Since $\varepsilon_p(2^n Q) \leq \operatorname{ord}_p(\Delta(W))$, get $g_n \mid \Delta(W)$ for all n.
- Can compute the g_n by repeatedly applying f and g, modulo a suitable power of $\Delta(W)$, and computing gcds.
- Can bound the error of $\sum_{n=0}^{m} 4^{-n-1} \log g_n$ for $m \in \mathbb{N}$ and approximate $\Psi^{\mathrm{f}}(Q)$ to any desired precision.

Computing Ψ^{f} exactly

Can also compute

$$\Psi^{\mathrm{f}}(Q) = \sum_p \mu_p(Q) \log p = \sum_{n=0}^{\infty} 4^{-n-1} \log g_n$$

exactly (as a rational combination of logs) for $Q \in E(\mathbb{Q})$.

Algorithm (M.–Stoll '15).

(1) Compute bounds m and B, using the bounds on $\varepsilon_p(Q)$ and on $\mathrm{denom}(\mu_p(Q))$ for all p.

(2) Compute $g_0, \dots, g_m$, working modulo $\Delta(W)^{m+2}$.

(3) Find pairwise coprime integers $q_1, \dots, q_s$ and $e_{i,n} \in \mathbb{Z}_{\geq 0}$ such that $g_n = \prod_{i=1}^{s} q_i^{e_{i,n}}$ for all n.

(4) For all $i \in \{1, \dots, s\}$:
   (a) compute $a := \sum_{n=0}^{m} 4^{-n-1} e_{i,n}$,
   (b) let μ_i be the simplest fraction between a and $a + 1/B^4$.

(5) Return $\Psi^{\mathrm{f}}(Q) = \sum_{i=1}^{s} \mu_i \log q_i$.

Factorization into coprimes

For step (3) we use:

Bernstein '04. Given $g_0, \ldots, g_m \in \mathbb{N}$ there are unique $q_1, \ldots, q_s \in \mathbb{N}$ such that

- the q_i are pairwise coprime;
- every g_n is a product of powers of the q_i, i.e. $g_n = \prod_{i=1}^{s} q_i^{e_{i,n}}$ for $e_{i,n} \in \mathbb{Z}_{\geq 0}$;
- the q_i can be computed from the g_n using only multiplication, exact quotients and gcds.

Bernstein gives a quasi-linear algorithm to compute the q_i.

Simpler, but quadratic algorithms due to Bach-Driscoll-Shallit '93, see also Buchmann-Lenstra '94.

Precise complexity analysis

Precise statement:

Theorem (M.–Stoll '15). Let E be given by a Weierstrass equation W with coefficients in $\mathbb{Z}$ and let $Q \in E(\mathbb{Q})$.

Let $\mathrm{M}(n)$ denote the time needed to multiply two n bit integers.

Then we can compute $\hat{h}(Q)$ to d bits of precision in time

$$\begin{aligned} &\ll \log(d + h(Q))\,\mathrm{M}(d + h(Q)) \\ &\quad + (\log\log\|W\|)\,\mathrm{M}\big((\log\log\|W\|)(\log\|W\|)\big) \\ &\quad + \log(d + \log\|W\|)^2\,\mathrm{M}(d + \log\|W\|) \\ &\in \tilde{O}(d + h(Q) + \log\|W\|)\,. \end{aligned}$$

Extensions

- Works similarly over number fields
  - totally real fields (with class number 1) immediate;
  - other cases work in progress due to Caselli.
- Can be extended to Jacobians of curves of genus 2 (M.-Stoll '16)
  - work on Kummer surface;
  - compute Ψ^{f} similarly;
  - also works over number fields;
  - no analogue of Bost-Mestre for computing Ψ_∞ known (use Richelot-isogenies?), instead we use series expansion;
  - get an algorithm for $\hat{h}$ which is quasi-linear in the input size and quasi-quadratic in the desired number of bits of precision.
- Idea of our algorithm has been extended to morphisms $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ by Wells ('16).