NAÏVE HEIGHTS ON JACOBIANS OF CURVES USING ARAKELOV THEORY

DAVID HOLMES

Abstract. These are notes for a talk given to the number theory seminar at the University of Hamburg on 2nd of May 2012. The talk was the second of a pair, in the first of which I described Néron-Tate heights, and the computational difficulties surrounding them as the dimension of the Abelian variety increases. I talked about an algorithm to compute the height of a point to arbitrary precision using Arakelov theory, as described in my JNT paper. In this talk, I will describe more recent work showing how to construct a naïve height using Arakelov theory, and apply it to the problem of saturation. This was work carried out at the University of Warwick, and forms part of my PhD thesis.

1. Introduction

2. Last time

Last time we gave the definition of the Néron-Tate height of a point on an abelian variety, and we noted two key problems which we want to solve:

1) given a point p on an abelian variety A, compute the canonical height $\hat{\mathrm{h}}p$ to any required precision.

2) given a bound $B > 0$, compute the finite set

$$M_A(B) = \{p \in A(\mathbb{Q}) : \hat{\mathrm{h}}(p) \leq B\}. \tag{1}$$

Recall that solutions to these problems have a variety of interesting applications:

- computing generators for the Mordell-Weil group $A(\mathbb{Q})$
- testing cases of the BSD conjectures up to rational squares with (1), or more precisely with (2) as well.
- computing integral points on hyperelliptic curves
- computing analytic ranks using Manin's algorithm.

Last week we described the classical techniques which are effective for solving both these problems in dimensions 1 and 2, and we also showed how Arakelov theory can be used to provide effective solutions in much higher dimensions, at least if we restrict to the Jacobians of hyperelliptic curves. this used the following theorem:

Date: May 1, 2012.

Theorem 1 (Faltings, Hriljac, 1984)**.** *Let $\mathscr{C}/\operatorname{Spec}(\mathbb{Z})$ denote a proper regular model of the curve C, and let $p \in J(C)(\mathbb{Q})$ be a rational point represented by a divisor D of degree 0 on C. Let $\overline{D}$ denote the Zariski closure of D on $\mathscr{C}$, and let $\Phi(D)$ be a vertical divisor on $\mathscr{C}$ such that for all vertical Y, we have $\iota(\overline{D} + \Phi(D), Y) = 0$. Then*

$$\hat{\mathrm{h}}(p) = -\left\langle \overline{D} + \Phi(D), \overline{D} + \Phi(D) \right\rangle. \tag{2}$$

The key point is that this turns computing the canonical height from a problem on the Jacobian (which is computationally inaccessible in high dimension) to a problem on a regular model of the curve, which is (comparatively) easy to compute.

Last week we saw how this can be used to give an algorithm for the first problem (computing $\hat{\mathrm{h}}$) which is effective for curves of high genus. The aim of this talk is to describe how we can use this Arakelov-theoretic approach to solve the harder problem (2), that of finding sets of points of bounded height.

3. Strategy

The basic idea is to define another height $\mathscr{H}$ on points of J, with the following properties:

1) there exists a constant c such that for all $p \in A(\mathbb{Q})$, we have $|\hat{\mathrm{h}}(p) - \mathscr{H}(p)| \leq c$

2) can compute the finite sets

$$\mathscr{M}_A(B) = \{p \in A(\mathbb{Q}) : \mathscr{H}(p) \leq B\}. \tag{3}$$

It is easy to see how these can be combined to solve problem (2).

In this talk I will define $\mathscr{H}$, and will outline how the constant c can be computed, and how we can go about computing the finite sets $\mathscr{M}_A(B)$.

4. Hyperelliptic curves

Tis week I will again restrict attention to Abelian varieties which are the Jacobians of hyperelliptic curves, indeed curves of odd degree. This is to make the problem easier; a lot of what we will do will depend greatly on the exact geometry of the curve we study, and so it makes sense to fix one class of curves. Recall that an odd- degree hyperelliptic curve is given on an affine patch by an equation $y^2 = f(x)$, where f is a polynomial of degree $2g+1$ with no repeated roots over the algebraic closure.

However, we really want to look at the global geometry of the curve, so we should choose a projective embedding. For this, we will embed our curve in a weighted projective space $\mathbb{P}(1, 1, g+1)$ with variables

x, s, y. As such, our curve is given by a (weighted) homogeneous equation looking something like

$$y^2 = sx^7 + 4s^3x^5 - 6s^6x^2 + 14s^8 \tag{4}$$

(a curve of genus 3).

How much of a restriction is it to only look at the Jacobians of hyperelliptic curves? As we noted last week, in genera 1 and 2 it is no restriction. In dimension g, the space of Abelian varieties has dimension $g(g+1)/2$, whereas the moduli space of curves of genus g has dimension $3g-3$, and the moduli space of hyperelliptic curves has dimension $2g-1$.

5. Heights and valuations

Do we want this section?

Recall that the arithmetic self-intersection pairing is a sum of a 'finite' (non-Archimedean) and an 'infinite' (Archimedean) part. We start by noting that the same holds for the 'usual' height of a point $p = (p_0, \ldots, p_n)$in $\mathbb{P}^n$:

$$\hat{\mathrm{h}}(p) = \log \max_i |p_i| = \log \prod_{\nu \in M_{\mathbb{Q}}} \max_i |p_i|_\nu. \tag{5}$$

Here $M_{\mathbb{Q}}$ is a proper set of absolute values for $\mathbb{Q}$, and the norms $|-|_\nu$ are the ν-adic norms.

Note that for the first expression, it is necessary that the p_i be coprime integers, but for the second expression this is no longer needed; this can be checked (along with the equivalence of the two formulae) by using the product formula for valuations.

6. Naive heights

The height $\mathscr{H}$ will be again a sum of local contributions. We will define an infinite family of metrics d_ν on divisors, indexed by places ν of $\mathbb{Q}$. We will then make the following definition:

Definition 2. *Let $p \in A(\mathbb{Q})$, and let D_1 and D_2 be specified divisors of degree zero on C such that $p = [\mathcal{O}(D_i)]$, and such that the supports of the D_i do not meet. We then define*

$$\mathscr{H}(p) = \sum_{\nu \in M_{\mathbb{Q}}} \log \mathrm{d}_\nu(D_1, D_2)^{-1}. \tag{6}$$

Thus to define $\mathscr{H}$ it remains to define the metrics d_ν and to say how the divisors D_i are chosen. In fact, we will not say much about the latter, since it does not greatly matter which divisors we choose; it is just important that our choices are consistent and that we choose the D_i to be differences of effective divisors of degree g. For the remainder of this talk, we will pretend that we can choose the D_i to have pointwise rational support- that is, they are just formal sums of rational points

on C. This is of course not true in general, but it will simplify the exposition, and the general case is not much more complicated.

Since the D_i are assumed to have disjoint support, we can simply define our metrics d_ν on points of C and then extend them to. divisors in the following manner: say $D_1 = \sum_j p_j n_j$ and $D_2 = \sum_l q_l m_l$, then set

$$\mathrm{d}_\nu(D_1, D_2) = \prod_{j,l} \mathrm{d}_\nu(p_j, q_l)^{n_j m_l}. \tag{7}$$

7. Definitions of metrics

The definitions of metrics we will give appear rather complicated, and so to justify their complexity we point out a few important properties they must possess:

1) they should be invariant under interchanging the coordinates s and x.

2) they should induce the 'correct' topology on C

3) everywhere locally they should be a continuous non-zero scalar multiple pf the restriction of the standard metric on affine space.

For non-Archimedean places ν we define $\mathrm{d}_\nu : C(\mathbb{Q}) \times C(\mathbb{Q}) \to \mathbb{R}$ by

(8)
$$\mathrm{d}_\nu((x_p, s_p, y_p), (x_q, s_q, y_q)) = \begin{cases} \max\left(|x_p/s_p - x_q/s_q|, |y_p/s_p^{g+1} - y_q/s_q^{g+1}|\right) & \text{if } |x_p| \leq |s_p| \text{ and } |x_q| \leq |s_q| \\ \max\left(|s_p/x_p - s_q/x_q|, |y_p/x_p^{g+1} - y_q/x_q^{g+1}|\right) & \text{if } |x_p| \geq |s_p| \text{ and } |x_q| \geq |s_q| \\ 1 & \text{otherwise.} \end{cases}$$

It is not immediately clear why this defines a metric, but we will omit the proof here.

Let ν be an Archimedean place of $\mathbb{Q}$. We will define three symmetric functions on $C(\mathbb{Q}) \times C(\mathbb{Q})$, each of which satisfies the triangle inequality, and then define d_ν to be their sum, which will inherit the triangle inequality and will be easily seen to be a metric.

Let $p = (x_p : s_p : y_p)$ and $q = (x_q : s_q : y_q) \in C(K_\nu^{\mathrm{alg}})$. Define $\mathrm{d}_1 : C(\mathbb{Q}) \times C(\mathbb{Q})$ by

$$\mathrm{d}_1(p, q) = \frac{|x_p s_q - x_q s_p|}{(|x_p| + |s_p|)(|x_q| + |s_q|)}, \tag{9}$$

note that this is continuous, and is well defined since $(0 : 0 : 1) \notin C(K_\nu^{\mathrm{alg}})$.

Define $\mathrm{d}_2 : C(\mathbb{Q}) \times C(\mathbb{Q})$ by setting $\mathrm{d}_2(p, (0 : 1 : 0)) = 1/(1 + |y_p/x_p^{g+1}|)$, and otherwise

$$\mathrm{d}_2(p, q) = \frac{|y_p x_q^{g+1} - y_q x_p^{g+1}|}{(|x_p|^{g+1} + |y_p|)(|x_q|^{g+1} + |y_q|)}. \tag{10}$$

Define $\mathrm{d}_3 : C(\mathbb{Q}) \times C(\mathbb{Q})$ by setting $\mathrm{d}_3(p,(1:0:0)) = 1/(1+|y_p/s_p^{g+1}|)$, and otherwise

$$\mathrm{d}_3(p,q) = \frac{|y_p s_q^{g+1} - y_q s_p^{g+1}|}{(|s_p|^{g+1}+|y_p|)(|s_q|^{g+1}+|y_q|)}. \tag{11}$$

Both d_2 and d_3 may be checked to be continuous using the smoothness of C and by studying the behaviour of the functions near Weierstrass points at $(0:1:0)$ and $(1:0:0)$ if such exist.

Set $\mathrm{d}_\nu = \mathrm{d}_1 + \mathrm{d}_2 + \mathrm{d}_3$.

8. Comparing the naive and canonical heights

We have now given a definition of the naive height $\mathscr{H}$, and we wish to compare it to the canonical height. Using the Arakelov-theoretic description of the canonical height, we see that both these heights can be defined locally, and so we will attempt to bound the difference between them in a local fashion.

In addition, both heights behave well with respect to addition of divisors, and so it suffices to do the following:

for all places ν of $\mathbb{Q}$, find a bound c_ν such that for all point $p_1, p_2, q_1, q_2 \in C(\mathbb{Q})$, we have

$$|\log\left(\frac{\mathrm{d}_\nu(p_1,q_2)\,\mathrm{d}_\nu(p_2,q_1)}{\mathrm{d}_\nu(p_1,q_1)\,\mathrm{d}_\nu(p_2,q_2)}\right) - \langle p_1 - p_2, q_1 - q_2\rangle| \leq c_\nu, \tag{12}$$

and such that

$$\sum_{\nu \in M_\mathbb{Q}} c_\nu < \infty. \tag{13}$$

9. Comparing metrics and intersections at non-Archimedean places

At places ν where the Zariski closure of C in $\mathbb{P}_\mathbb{Z}(1,1,g+1)$ is smooth, it is not hard to check that we can take $c_\nu = 0$. In particular, this shows that the sum of the c_ν will necessarily be finite.

At places of bad reduction for C, we have to allow for 'blowing up', since the pairing $\langle -,-\rangle$ is computed on a regular model of C. The trick to doing this is to use a result of Hironaka that shows that we can obtain a resolution of singularities of an arithmetic surface by blowups at smooth centres only; no normalisations are required. Now since the smooth locus of such a blowup is etale-localy just a line or a point, we can compute exactly the effect that blowing up will have on the intersection pairing, and thus obtain a value for c_ν.

10. Comparing metrics and Green's functions 'away from the diagonal'

To compare the naive and canonical heights, it remains for us to bound the difference between them locally at Archimedean places. Recall that we defined the Archimedean part of the intersection pairing to be

$$\langle p, q \rangle_\infty = g_p(q), \tag{14}$$

where g_p is the Green's function in a certain special metric. As such, we wish to construct a bound c_ν such that for all $p, q \in C(\mathbb{C})$, we have

$$|g_p(q) - \log \mathrm{d}_\nu(p,q)^{-1}| \leq c_\nu. \tag{15}$$

Lemma 3. *Fix $\epsilon > 0$. Then there exists a computable constant c such that for all $p, q \in C(\mathbb{C})$ with $\mathrm{d}_\nu(p,q) \geq \epsilon$, we have*

$$|g_p(q) - \log \mathrm{d}_\nu(p,q)^{-1}| \leq c. \tag{16}$$

The fact that the constant c is computable is essential for our applications, but makes the result significantly harder to prove. Indeed, without this requirement the result follows almost immediately from basic properties of green's functions, in the following manner:

Recall the follwing important properties of Green's functions:

Let D be a divisor on C. Then g_D is defined as a function on $C(\mathbb{C}) - \mathrm{Supp}(D)$. Suppose D is represented by a rational function f on an open set U. The there exists a smooth function α on U such that for all $p \notin \mathrm{Supp}(D)$, we have

$$g_D(p) = -\log|f(p)|^2 + \alpha(p). \tag{17}$$

This shows that the values of the Green's function $g_p(q)$ are bounded on compact sets away from p. It is easy to check that the same holds for the function $\log \mathrm{d}_\nu(p,q)^{-1}$, so we are done.

How do we make the constant effective? We can express the Green's function using hyperelliptic integrals and theta functions. The hyperelliptic integrals can be bounded using bounds on the coeffisipcients of our equations for the curve C, and theta functions are given as absolutely convergent power series, so it is possible to bound the values these will talk.

11. Comparing metrics and intersection pairings along the diagonal

Recall that or bounding the difference between the naive and canonical heights, we must bound the difference between $\log \mathrm{d}_\nu(p,q)^{-1}$ and $g_p(q)$ for points p and q which are close together (in the metric d_ν). Note that both terms have logarithmic poles as p and q approach each other, so this is unlikely to be as easy as the case when they are far apart.

We begin with an easy lemma:

Lemma 4. *Suppose $\epsilon > 0$. Let D and E be a pair of divisors of degree 0, and let ϕ be a rational function on C such that for all p appearing in the support of $D - \mathrm{div}(\phi)$ and for all q appearing in the support of E, we have $\mathrm{d}(p,q) \geq \epsilon$.*

Write $D - \mathrm{div}(\phi) = D' = D'^{+} - D'^{-}$ where D'^{+} and D'^{-} are both effective, and write $E = E^{+} - E^{-}$ where again E^{+} and E^{-} are both assumed effective. Suppose also that D'^{-} and E^{-} are supported on Weierstrass points (this is just to improve the constants). Then writing $c(\epsilon)$ for the constant from the previous section, we have

$$|g_D(E) + \log(\mathrm{d}(D,E))| \leq c(\epsilon)\deg(D'^{+})\deg(E^{+}) + |\log|\frac{\mathrm{d}(D,E)}{\phi[E]}||. \tag{18}$$

How do we use this lemma? We describe an easy case; suppose the points p and q that interest us are close together, but not close to any Weieratrass point. Let ϕ be the rational function

$$\frac{x - x_1}{x - x(p)} \tag{19}$$

where x_1 is chosen to be far from the x-coordinates of p and q. Then we can apply the lemma to see that it suffices to bound

$$\frac{\mathrm{d}_\nu(p,q)}{\phi(q)}, \tag{20}$$

which can be done by carefully studying the structure of the metric d_ν.

Much harder is the case when p and q are both close to the same Weierstrass point. We use the same basic approach, but now the rational function ϕ we construct is rather more complicated, and bounding the corresponding term

$$\frac{\mathrm{d}_\nu(p,q)}{\phi(q)}, \tag{21}$$

takes about 20 pages of my thesis.

12. Conclusion of bounding the difference

A while ago we set out to bound the difference between the naive and canonical heights for a point on a hyperelliptic Jacobian. We have shown how to do this by considering local pairings, so we now have an algorithm to give an explicit bound c such that for all $p \in A(\mathbb{Q})$, we have

$$|\hat{\mathrm{h}}(p) - \mathscr{H}(p)| \leq c. \tag{22}$$

Recall that the reason we wanted this was to help us in computing the finite sets

$$M_A(B) = \{p \in A(\mathbb{Q}) : \hat{\mathrm{h}}(p) \leq B\}, \tag{23}$$

be computing the finite set

$$\mathscr{M}_A(B+c) = \{p \in A(\mathbb{Q}) : \hat{\mathrm{h}}(p) \leq B + c\}. \tag{24}$$

However, it still remains to compute $\mathscr{M}_A(B+c)$, and it is not a-priori obvious that this will be any easier than computing $M_A(B)$ directly! The trick is to introduce a third height:

Definition 5. *Given $p \in A(\mathbb{Q})$, let D be an effective divisor of degree g such that $p = [\mathcal{O}(D - g\infty)]$. Letting $\pi : C \to \mathbb{P}^1$ denote the projection map, we see that $\pi_* D$ is an effective divisor of degree g on $\mathbb{P}^1$, which is the same as a rational point in $\mathbb{P}^g$. We set $\hat{\mathrm{h}}^{\heartsuit}(p)$ to be the usual naive height of this point in projective space.*

Of course, the key is that there exists a computable constant c' such that for all $p \in A(\mathbb{Q})$, we have

$$|\mathscr{H}(p) - \hat{\mathrm{h}}^{\heartsuit}(p)| \leq c'. \tag{25}$$

The proof of this result is delicate; it is very dependant on the exact form of the metrics on divisors that we gave at the beginning of this talk; indeed, the fact that it works is really the justification for those somewhat weird metrics.

Finally, we note that it is easy to give an algorithm compute the finite sets

$$M_A^{\heartsuit}(B) = \{p \in A(\mathbb{Q}) : \hat{\mathrm{h}}^{\heartsuit}(p) \leq B\}, \tag{26}$$

since we just have to list the finite set of points in $\mathbb{P}^g$ of height less that B, then check which of these come from points on A. So we are done.

13. Final remarks

To be able to apply these results to the applications I listed at the beginning of the talk, it is or course necessary to implement this algorithm. In its current state this will be a lot of work, and more importantly it looks unlikely that the resulting bounds will be sufficiently small to make the resulting search region practicable especially since the dimension of the search region increases linearly with the genus.

The places where improvements could most likely be made is in the bounding of the local Archimedean terms, where we compare metrics and Greens functions. If a better way could be found to carry out this bit of the algorithm, it would be great!

References