

AN ARAKELOV-THEORETIC APPROACH TO NAÏVE HEIGHTS ON HYPERELLIPTIC JACOBIANS

DAVID HOLMES

ABSTRACT. Published in the New York Journal of Mathematics in 2014, see <http://nyjm.albany.edu/j/2014/20-45.html>.

We use Arakelov theory to define a height on divisors of degree zero on a hyperelliptic curve over a global field, and show that this height has computably bounded difference from the Néron-Tate height of the corresponding point on the Jacobian. We give an algorithm to compute the set of points of bounded height with respect to this new height. This provides an ‘in principle’ solution to the problem of determining the sets of points of bounded Néron-Tate heights on the Jacobian. We give a worked example of how to compute the bound over a global function field for several curves, of genera up to 11.

1. INTRODUCTION

1.1. Previous explicit computational work on Néron-Tate heights.

The Néron-Tate height was defined by Néron [Nér65]. The problems of computing the height of a given point on the Jacobian of a curve and computing the (finite) sets of points of bounded height on the Jacobian have been studied since the work of Tate in the 1960s, who used a different (equivalent) definition to that of Néron. Using this definition, Tate (unpublished), Dem’janenko [Dem68], Zimmer [Zim76], Silverman [Sil90] and more recently Cremona, Prickett and Siksek [CPS06] and Uchida [Uch06] have given increasingly refined algorithms for the case of elliptic curves. Meanwhile, in the direction of increasing genus, Flynn and Smart [FS97] gave an algorithm for the above problems for genus 2 curves building on work of Flynn [Fly93], which was later modified by Stoll ([Sto99] and [Sto02]). Stoll has announced an extension to the hyperelliptic genus 3 case [Sto12].

The technique used by all these authors was to work with a projective embedding of the Jacobian or a quotient (usually the Kummer variety), together with equations for the duplication maps, and thereby obtain results on heights using Tate’s ‘telescoping trick’. However, such projective embeddings become extremely hard to compute as the genus grows - for example, the Kummer variety is \mathbb{P}^1 for an elliptic curve, is a quartic hypersurface in \mathbb{P}^3 for genus 2 and for genus 3 hyperelliptic curves is given by a system of one quadric and 34 quartics in \mathbb{P}^7 [Mue10]. It appears that to extend to much higher genus using these techniques will be impractical.

In [Hol12a], the author used techniques from Arakelov theory to give an algorithm to compute the Néron-Tate height of a point on a hyperelliptic curve, and a similar (though different) algorithm for the same problem was

Date: January 16, 2015.

given by Müller in [Mue13]. Both gave computational examples in much higher genera (9 and 10 respectively) than had been possible with previous techniques. In this paper, we apply Arakelov theory to the problem of computing the sets of points of bounded height. For practical reasons, we will eventually make certain restrictions on the fields considered and on the shape of the curve, namely we insist that the field either has positive characteristic or is \mathbb{Q} , and that there is a rational Weierstrass point at infinity. This is discussed in Remark 20.

1.2. Relation to classical naïve heights. Let $p = [D - g \cdot \infty]$ be a point on the Jacobian J , where D is a suitably chosen divisor on the curve. We will define various intermediate heights, but the final naïve height of p (denoted $h^\dagger(p)$) is given by the height of the polynomial which vanishes at the ‘ x -coordinates’ of points in D (with multiplicity). This is equal to the ‘classical’ naïve height of the image of p under the projective embedding given by a certain linear subspace of $H^0(J, 2\theta)$. As such, it is clear that $h^\dagger \leq \hat{h} + c$ for some positive constant c ; the main result of this paper is to give a practical method to *find* a bound.

1.3. Practicality regarding searching for points of bounded height.

To determine the number of points of bounded Néron-Tate height on a Jacobian, one usually constructs a ‘naïve’ height with bounded difference from the Néron-Tate height, and then searches for points of bounded naïve height. As such, the two main determinants of the speed of such an algorithm will be the size of the bound on the height differences and the dimension of the region in which one must search for points.

1.3.1. Number fields. Let C be a curve of genus g . The algorithm in this paper requires a search region of dimension g . In this paper we do not give a new algorithm for bounding the local Archimedean height difference (see Section 5.1), but we can estimate the sizes of the bounds produced by techniques in the literature. Bounds using Merkl’s theorem [CE⁺11] will be extremely large. Indeed, a Merkl atlas must contain at least $2g + 2$ charts (since every Weierstrass point must lie at the centre of a chart), and the form of Merkl’s theorem then yields a summand like $1200(2g + 2)^2 \approx 4800g^2$ in the difference between the heights. A factor like g^2 seems hard to avoid (for example such a factor appears again in Lemma 33), but the coefficient 4800 is very bad from a practical point of view; since these are differences between logarithmic heights, we obtain a factor like $\exp(4800g^2)$ in the ratio of the exponential heights, making a search for rational points unfeasible in practise. The author’s PhD thesis [Hol12b] contains an alternative algorithm that does not make use of Merkl’s theorem (and so *may* yield better bounds) but is much more cumbersome to write down. There is some hope that techniques from numerical analysis may give much sharper bounds, but unfortunately they will not readily give *rigorous* bounds. This is important as the main intended application of these results is to *proving* statements about sets of points of bounded height. If you only need something that almost certainly works in practice, then simply hunting for points of ‘reasonably large’ naïve height should be sufficient.

1.3.2. *Function fields.* In the case of a positive-characteristic global field, the height-difference bounds in this paper become substantially smaller, but still not yet small enough to be useful. In Theorem 41, we compute bounds for three curves (of genera 2, 4 and 11) over $\mathbb{F}_p(t)$ of the form $y^2 = x^{2g+1} + t$. The bounds we obtain are very roughly of the size $g^4 \log p$. Even in the genus 2 example (where we work over \mathbb{F}_3 , obtaining a bound of $108 \log 3$), to complete a very naïve search for points would require approximately p^{300} factorisations of univariate polynomials over \mathbb{F}_3 , which is entirely impractical (though with sieving techniques one could hope to do much better). The algorithm presented in this paper is not optimised, so with further work we hope it will be possible in future to make this method practical in some higher genera.

1.3.3. *Applications.* If the algorithms in this paper can be made practical, they have applications to the problem of saturation of Mordell-Weil groups (see [Sik95] or [Sto02]), to the computation of integral points on hyperelliptic curves (see [BMS⁺08]), to the use of Manin’s algorithm [Man71], and for numerically testing cases of the Conjecture of Birch and Swinnerton-Dyer.

1.3.4. *Some open problems.*

- improve the bounds produced by this algorithm, to make searching for points practical in some small genera;
- find a practical way to compute bounds at Archimedean places, and even to find good (small) bounds;

1.4. **Other algorithms for heights in arbitrary genus.** It appears that it would be possible to extend the projective-embedding-based approaches mentioned above to give ‘in principle’ algorithms for bounding the difference between the Néron-Tate and naïve heights for curves of arbitrary genus. Mumford [Mum66] and Zarhin and Manin [ZM72] describe the structure of the equations for abelian varieties embedded in projective space and the corresponding heights and height differences, respectively. To apply these results it is necessary to give an algorithm to construct these projective embeddings for Jacobians for curves of arbitrary genus. Work in this direction includes [VW98] and [Rei72] in the hyperelliptic case, and [And02] in the general case. A bound on the difference between the Néron-Tate height and the naïve height arising from such an embedding is given by Proposition 9.3 (page 665) in the paper [DP02] of David and Philippon, using an embedding of the Jacobian using 16ϑ . An algorithm for the construction of this embedding has yet to be written down.

1.5. This paper bears some resemblance to the final two chapters of the author’s PhD thesis [Hol12b]. The author would like to thank Samir Siksek for introducing him to the problem, and also Steffen Müller and Ariyan Javanpeykar for many helpful discussions, as well as very thorough readings of a draft version.

2. SETUP

Definition 1. We work over a fixed global field K with $2 \in K^\times$ and with fixed algebraic closure K^{alg} . We fix an integer $g > 0$ and a separable polynomial $f(x, s) = \sum_{i=1}^{2g+2} f_i x^i s^{2g+2-i} \in K[x, s]$. We denote by C the curve of genus g over K embedded in weighted projective space $\mathbb{P}(1, 1, g+1)$ with coordinates x, s, y , defined by the equation $y^2 = f(x, s)$. We call such a curve a hyperelliptic curve. We write $X = x/s, Y = y/s^{g+1}, S = s/x$ and $Y' = y/x^{g+1}$. We often write X_p for the value of X at p , etc.

Definition 2. We say that a divisor D on C is semi-reduced if it is effective and if there does not exist a prime divisor p of C such that $D \geq p + p^-$ (where p^- denotes the image of p under the hyperelliptic involution). In particular, any Weierstrass point appearing in the support of D has multiplicity 1. If in addition we have $\deg(D) \leq g$, then we say D is reduced.

Definition 3. For a global field L , a proper set of absolute values for L is a non-empty multi-set of non-trivial absolute values on L such that the product formula holds. We fix once and for all such a multi-set M_K of absolute values for K such that every Archimedean absolute value ν comes from an embedding of K into \mathbb{C} with the standard absolute value. Given a finite extension L/K , we fix a proper multi-set of absolute values M_L for L by requiring that for all absolute values $\nu \in M_L$, the restriction of ν to K lies in M_K . We denote by M_L^0 the sub-multi-set of non-Archimedean absolute values and M_L^∞ the sub-multi-set of Archimedean absolute values.

Definition 4. Given a global field L , we define the curve B_L to be the unique normal integral scheme of dimension 1 with field of rational functions L and such that B_L is proper over $\text{Spec } \mathbb{Z}$. For example, if L is a number field then B_L is the spectrum of the ring of integers of L .

Definition 5. Let \mathcal{C}_1 denote the Zariski closure of C in $\mathbb{P}_{B_K}(1, 1, g+1)$. A result of Hironaka, contained in his appendix to [CGO84] (pages 102 and 105) gives us an algorithm to resolve the singularities of \mathcal{C}_1 by a sequence of blowups at closed points and along smooth curves (the latter replacing normalisations); we observe that \mathcal{C}_1 may locally be embedded in $\mathbb{P}_{B_K}^2$, and so Hironaka's result can be applied. We fix once and for all a choice of resolution \mathcal{C} of \mathcal{C}_1 using this algorithm of Hironaka - thus we fix both the model \mathcal{C} and the sequence of blowups at smooth centres used to obtain it.

2.1. Local Néron pairings. Given an absolute value ν of K , we write $\text{Div}^0(C_{K_\nu})$ for the group of degree-zero divisors on the base change of C to the completion of K at ν . The local Néron pairing at ν is a biadditive map $[-, -]_\nu : \{(D, E) \in \text{Div}^0(C_{K_\nu}) \times \text{Div}^0(C_{K_\nu}) \mid \text{supp}(D) \cap \text{supp}(E) = \emptyset\} \rightarrow \mathbb{R}$. Its definition depends on whether ν is an Archimedean or non-Archimedean absolute value.

Suppose first that ν is a non-Archimedean absolute value. Write \mathcal{O}_{K_ν} for the ring of integers of the completion K_ν . We write ι_ν for the (rational-valued) intersection pairing between divisors over ν (as defined in [Lan88, IV, §1]). Let D and E be elements of $\text{Div}^0(C_{K_\nu})$. We extend D and E to horizontal divisors \overline{D} and \overline{E} on $\mathcal{C}_{K_\nu} := \mathcal{C} \times_{B_K} \text{Spec } \mathcal{O}_{K_\nu}$. Write $\mathbb{Q}\text{FDiv}(C_{K_\nu})$

for the group of \mathbb{Q} -divisors on \mathcal{C}_{K_ν} supported on the special fibre $(\mathcal{C}_{K_\nu})_\nu$. We define a map (cf [Lan88, III, §3])

$$\Phi : \text{Div}^0(C_{K_\nu}) \rightarrow \frac{\mathbb{Q} \text{FDiv}(C_{K_\nu})}{\mathbb{Q}(\mathcal{C})_\nu}$$

by requiring that for all fibral divisors $Y \in \text{FDiv}(C_{K_\nu})$, we have

$$\iota_\nu(Y, \bar{D} + \Phi(D)) = 0.$$

Then define the local Néron pairing by

$$[D, E]_\nu = \log(\#\kappa) \iota_\nu(\bar{E}, \bar{D} + \Phi(D)),$$

where κ is the residue field at ν .

Suppose now that ν is an Archimedean absolute value of K . Fix an algebraic closure of K_ν , and view $C_\nu = C(K_\nu^{\text{alg}})$ as a compact connected Riemann surface of positive genus and let μ denote the canonical (Arakelov) (1,1)-form μ on C_ν . We write $G(-, -) : C_\nu \times C_\nu \rightarrow \mathbb{R}_{\geq 0}$ for the exponential Green's function on $C_\nu \times C_\nu$ associated to μ , and gr for its logarithm. We normalise the Green's function to satisfy the following three properties.

1) $G(p, q)$ is a smooth function on $C_\nu \times C_\nu$ and vanishes only at the diagonal. For a fixed $p \in C_\nu$, an open neighbourhood U of p and a local coordinate z on U centred at p , there exists a smooth function α such that for all $q \in U$ with $p \neq q$ we have

$$\text{gr}(p, q) = \log |z(q)| + \alpha(q).$$

2) For all $p \in C_\nu$ we have $\partial_q \bar{\partial}_q \text{gr}(p, q)^2 = 2\pi i \mu(q)$ for $q \neq p$.

3) For all $p \in C_\nu$, we have

$$\int_{C_\nu} \text{gr}(p, q) \mu(q) = 0.$$

Write $D = \sum_i a_i p_i$ and $E = \sum_j b_j p_j$ with $a_i, b_j \in \mathbb{Z}$ and $p_i, p_j \in C_\nu$. Then the local Néron pairing at ν is defined by

$$[D, E]_\nu = \sum_{i,j} a_i b_j \text{gr}(p_i, p_j).$$

3. OUTLINE

Let L/K be a finite extension. We define the height of an element $x \in L$ by

$$h(x) = \frac{1}{[L : K]} \sum_{\nu \in M_L} \log \max(|x|_\nu^{-1}, 1)$$

and $H(x) = \exp h(x)$. This extends to give a well-defined height on the algebraic closure K^{alg} of K .

The definition of our first naïve height is analogous to this. For each absolute value ν of our global field, we will construct a metric or pseudo-metric d_ν on divisors which measures how far apart they are in the ν -adic topology. Given a suitable degree-zero divisor D on C corresponding (up to

2-torsion points) to the point $[D]$ on the Jacobian of C , we define the naïve height of $[D]$ by

$$h^n([D]) = \sum_{\nu \in M_K} \log d_\nu(D, D')^{-1}$$

where D' is a chosen divisor which is linearly equivalent to $-D$ (up to 2-torsion points). Since curve C is compact and our metrics continuous, the function $d_\nu(D, D')^{-1}$ is bounded below uniformly in D , and so we may use $\log(-)$ in place of $\log(\max(-, 1))$.

We define these metrics at non-Archimedean absolute values in Definition 6. Theorem 8 bounds the difference of the distance between two divisors and their local Néron pairing at a non-Archimedean absolute value. The hardest aspect of this is allowing for the fact that the model of C obtained by taking the closure inside projective space over B_K is not in general a regular scheme, so we must compute precisely how the process of resolving its singularities will affect the intersection pairing. In Definition 15 we define a pseudo-metric on C at each Archimedean absolute value. Theorem 18 bounds the difference between this function and the local Néron pairing.

We apply Theorem 22 (due to Faltings and Hriljac) to bound the difference between our height and the Néron-Tate height. We then write down two more naïve heights, with successively simpler definitions, each time bounding in an elementary fashion the difference from the Néron-Tate height. We give a method to compute the number of points of bounded height for the simplest of these naïve heights, completing the algorithm. In Theorem 41 we give a worked example of how to compute these bounds for a certain genus 11 curve over $\mathbb{F}_{101}(t)$.

4. NON-ARCHIMEDEAN ABSOLUTE VALUES

4.1. Defining metrics.

Definition 6. For each absolute value $\nu \in M_K$, we fix $(K_\nu^{alg}, |\cdot|_\nu)$ to be an algebraic closure of the completion K_ν together with the absolute value which restricts to ν on $K \subset K_\nu^{alg}$. For non-Archimedean absolute values ν we define

$$d_\nu : C(K_\nu^{alg}) \times C(K_\nu^{alg}) \rightarrow \mathbb{R}_{\geq 0}$$

by

$$d_\nu((x_p : s_p : y_p), (x_q : s_q : y_q))$$

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

Proposition 7. For each $\nu \in M_K^0$, $d = d_\nu$ is a metric on $C(K_\nu^{alg})$. Moreover, for each such ν , we have $d_\nu(p, q) \leq 1$ for all p and q .

Proof. We omit the subscripts ν from the absolute values. We begin by observing that if $(x : s : y) \in C(K_\nu^{alg})$ then

$$|x| \leq |s| \implies |y| \leq |s|^{g+1} \text{ and } |x| > |s| \implies |y| \leq |x|^{g+1}.$$

Combining this with the fact that $|\cdot|$ is non-Archimedean, we see for all $p, q \in C(K_\nu^{\text{alg}})$ that $d(p, q) \leq 1$.

For showing that d is a metric, only the triangle inequality is non-obvious. Let $p = (x_p, s_p, y_p)$, $q = (x_q, s_q, y_q)$ and $r = (x_r, s_r, y_r)$. Suppose firstly that $|x_p| \leq |s_p|$, $|x_q| \leq |s_q|$ and $|x_r| \leq |s_r|$. Then

$$\begin{aligned} & d(p, q) + d(q, r) \\ &= \max \left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right|, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right| \right) + \max \left(\left| \frac{x_q}{s_q} - \frac{x_r}{s_r} \right|, \left| \frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}} \right| \right) \\ &\geq \max \left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right| + \left| \frac{x_q}{s_q} - \frac{x_r}{s_r} \right|, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right| + \left| \frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}} \right| \right) \\ &\geq d(p, r). \end{aligned}$$

The other cases are similar. \square

4.2. Comparison of the metric and the Néron pairing. The main aim of this section is to prove the following result:

Theorem 8. *Given a non-Archimedean absolute value $\nu \in M_K^0$, there exists an explicitly computable constant \mathcal{B}_ν with the following property:*

Let $D = D_1 - D_2$ and $E = E_1 - E_2$ be differences of reduced divisors on C with no common points in their supports, and assume that D and E both have degree zero. Let L denote the minimal field extension of K_ν such that D and E are pointwise rational over L , and over L write $D = \sum_i d_i p_i$, $E = \sum_j e_j q_j$, with $d_i, e_j \in \mathbb{Z}$ and $p_i, q_j \in C(L)$. Recall from Section 2.1 that $[D, E]_\nu$ denotes the local Néron pairing of D and E at ν . Then

$$\left| [D, E]_\nu - \sum_{i,j} d_i e_j \log \left(\frac{1}{d_\nu(p_i, q_j)} \right) \right| \leq \mathcal{B}_\nu.$$

Moreover, if C is smooth over ν , then we may take $\mathcal{B}_\nu = 0$.

The proof of this result is postponed to the end of this section.

For the remainder of this section we fix a non-Archimedean absolute value $\nu \in M_K^0$. We write K_ν for the completion of K at ν , and \mathcal{O}_{K_ν} for the ring of integers of K_ν .

We begin by bounding the function Φ . Let F denote the free abelian group generated by prime divisors supported on the special fibre of \mathcal{C} over ν , and let V denote the finite-dimensional \mathbb{Q} -vector space obtained by tensoring F over \mathbb{Z} with \mathbb{Q} . Let $M : V \times V \rightarrow \mathbb{Q}$ be the map induced by tensoring the restriction of the intersection pairing on \mathcal{C} to its special fibre with \mathbb{Q} . Then V has a canonical basis of fibral prime divisors, so we may confuse M with its matrix in this basis. Call the basis vectors $Y_1 \dots Y_n$; we use the same labels for the corresponding fibral prime divisors.

Lemma 9. *Let M^+ denote the Moore-Penrose pseudo-inverse (see [Pen55]) of M , let m_- denote the infimum of the entries of M^+ and m_+ their supremum. Let $D = D_1 - D_2$ and $E = E_1 - E_2$ be differences of reduced divisors on C with no common points in their supports, and assume that D and E*

both have degree zero. Then

$$|\iota_\nu(\Phi(D), \bar{E})| \leq g^2(m_+ - m_-).$$

Proof. Let d denote the vector $\sum_{i=1}^n \iota_\nu(\bar{D}, Y_i) Y_i$, and similarly set e to equal $\sum_{i=1}^n \iota_\nu(\bar{E}, Y_i) Y_i$, a pair of vectors in V . Now by definition of Φ we have that for all vectors $v \in V$:

$$v \cdot d^T + v \cdot M \cdot \Phi(D)^T = 0,$$

and hence that

$$d^T = -M \cdot \Phi(D)^T.$$

Recall that if for any matrix A the linear system $Ax = b$ has any solutions, then a solution is given by $x = A^+b$ where A^+ is the Moore-Penrose pseudo-inverse of A . As such, we can take $\Phi(D)$ to be $-d \cdot (M^+)^T$, and so we find

$$\iota_\nu(\Phi(D), \bar{E}) = -d \cdot (M^+)^T \cdot e^T.$$

Now since D and E are differences of reduced divisors, d and e are vectors each formed by assigning at most g copies of ‘+1’ and g copies of ‘-1’ to the basis elements Y_1, \dots, Y_n (allowing multiple ± 1 s to be assigned to a single basis vector), and so the result easily follows. \square

By base change and Definition 5, we have a chosen resolution \mathcal{C}_{K_ν} of the singularities of the closure \mathcal{C}_1 of C in weighted projective space over \mathcal{O}_{K_ν} . Let b_ν denote the longest length of a chain of blowups involved in obtaining this resolution (one blowup is considered to follow another if the centre of one blowup is contained in the exceptional locus of the previous one). Note that $b_\nu = 0$ if \mathcal{C}_1 is smooth over \mathcal{O}_{K_ν} .

For the remainder of this section, let D and E be effective divisors on C with disjoint support, of degrees d and e respectively. Let L_ν/K_ν be the minimal finite extension (of degree m with residue field l) such that D and E are both pointwise rational over L_ν . Write $D = \sum_{i=1}^d p_i$ and $E = \sum_{i=1}^e q_i$, and write \mathcal{D} and \mathcal{E} for the Zariski closures of D and E respectively on the regular model \mathcal{C}_{K_ν} over \mathcal{O}_{K_ν} (more precisely, take closures of the prime divisors in the supports of D and E , then define \mathcal{D} and \mathcal{E} to be appropriate linear combinations of these new prime divisors). Write ω for the maximal ideal of \mathcal{O}_{L_ν} .

Lemma 10. *We have*

$$-\log(\#\kappa(\nu))b_\nu de \leq \log(\#\kappa(\nu)) \iota_\nu(\mathcal{D}, \mathcal{E}) - \log\left(\frac{1}{\prod_{i,j} d(p_i, q_j)}\right) \leq 0,$$

where $\kappa(\nu)$ is the residue field at ν .

The proof of Lemma 10 may be found after Lemma 14. To avoid an excess of notation, we will from now on drop the subscript ν from the fields and models we are considering, since we will exclusively be working locally at ν and places dividing it for the remainder of this section.

Lemma 11. *Let $p, q \in C(L)$ with $p \neq q$. Write*

$$I_{p,q} \stackrel{\text{def}}{=} \sum_{\Omega|\omega} \log(\#\kappa(\Omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right),$$

where the sum is over closed points Ω (with residue field $\kappa(\Omega)$) of $\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ lying over ω , and I_p and I_q are defining ideal sheaves for the closures \bar{p} and \bar{q} in $\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ of the images of p and q in $C \times_K L$. Then

$$I_{p,q} = m \log \left(\frac{1}{d(p,q)} \right)$$

(recall that $m = [L : K]$).

Proof. Write $p = (x_p : s_p : y_p)$, $q = (x_q : s_q : y_q)$ with $x_p, s_p, x_q, s_q \in \mathcal{O}_L$. If $|x_p| < |s_p|$ and $|x_q| > |s_q|$ or vice versa, then \bar{p} and \bar{q} do not meet on the special fibre so $\iota_\omega(\bar{p}, \bar{q}) = 0$, and by definition we see that $d(p,q) = 1$.

Otherwise, possibly after changing coordinates, we may assume that p and q are of the form $(x_p : 1 : y_p)$ and $(x_q : 1 : y_q)$ respectively, for $x_p, y_p, x_q, y_q \in \mathcal{O}_L$. We may moreover assume that \bar{p} and \bar{q} meet on the special fibre; let Ω be the closed point where \bar{p} and \bar{q} meet. After multiplying the defining equation F of C on the coordinate chart containing p and q by a power of a uniformiser at ν , we may assume F is integral at ν and is irreducible. We have

$$\begin{aligned} \frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} &\cong \frac{\mathcal{O}_L[x,y]_{(x,y)}}{(F, x - x_p, y - y_p, x - x_q, y - y_q)} \\ &\cong \frac{\mathcal{O}_L}{(x_p - x_q, y_p - y_q)}, \end{aligned}$$

so

$$\text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right) = \min(\text{ord}_\omega(x_p - x_q), \text{ord}_\omega(y_p - y_q)).$$

Now given $a \in L$, we find

$$\log(\#l) \text{ord}_\omega(a) = -m \log |a|,$$

so

$$\text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right) = m \frac{\min(-\log |x_p - x_q|, -\log |y_p - y_q|)}{\log(\#l)},$$

and hence

$$I_{p,q} = m \min(-\log |x_p - x_q|, -\log |y_p - y_q|).$$

Moreover,

$$\log(1/d(p,q)) = \min(-\log |x_p - x_q|, -\log |y_p - y_q|),$$

so we are done. \square

Lemma 12. *Recalling that over L we can write $D = \sum_{i=1}^d p_i$ and $E = \sum_{i=1}^e q_i$, we define $\mathcal{O}_{\omega_{i,j}}$ to be the local ring at the closed point of $\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ where p_i meets q_j if such exists, and the zero ring otherwise. Letting \mathcal{I}_D and \mathcal{I}_E denote the ideal sheaves of the closures of D and E respectively on \mathcal{C}_1 , we have*

$$\sum_{i,j} \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\omega_{i,j}}}{I_{p_i} + I_{q_j}} \right) = \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1} \otimes_{\mathcal{O}_K} \mathcal{O}_L}{(\mathcal{I}_D + \mathcal{I}_E) \otimes_{\mathcal{O}_K} \mathcal{O}_L} \right).$$

The analogous statement on \mathcal{C} also holds.

Proof. We may decompose \mathcal{I}_D and \mathcal{I}_E into iterated extensions of the sheaves I_{p_i} and I_{q_i} , whereupon the result follows from additivity of lengths in exact sequences. \square

Lemma 13. *Let \mathcal{I}_D and \mathcal{I}_E denote the ideal sheaves on \mathcal{C}_1 corresponding to the closures of the divisors D and E respectively. We have:*

$$\text{length}_{\mathcal{O}_K} \left(\frac{\mathcal{O}_{\mathcal{C}_1}}{\mathcal{I}_D + \mathcal{I}_E} \right) \cdot \text{ram. deg } L/K = \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1} \otimes_{\mathcal{O}_K} \mathcal{O}_L}{(\mathcal{I}_D + \mathcal{I}_E) \otimes_{\mathcal{O}_K} \mathcal{O}_L} \right).$$

The analogous statement on \mathcal{C} also holds.

Proof. Let M be a finite length \mathcal{O}_K -module. We show

$$\text{length}_{\mathcal{O}_K}(M) \cdot \text{ram. deg}(L/K) = \text{length}_{\mathcal{O}_L}(M \otimes_{\mathcal{O}_K} \mathcal{O}_L).$$

Let $M = M_0 \subset M_1 \subset \dots \subset M_l = 0$ be a composition series for M , so each M_i/M_{i+1} is simple. Since \mathcal{O}_K is local, we have by [Mat80, p12] that

$$M_i/M_{i+1} \cong \mathcal{O}_K/\mathfrak{m}_K.$$

By additivity of lengths, it suffices to show

$$\text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_K}{\mathfrak{m}_K} \otimes_{\mathcal{O}_K} \mathcal{O}_L \right) = \text{ram. deg}(L/K),$$

but this is clear since $\mathfrak{m}_K \cdot \mathcal{O}_L = \mathfrak{m}_L^{\text{ram. deg}(L/K)}$. \square

Lemma 14. *Let $\phi : \mathcal{C}_3 \rightarrow \mathcal{C}_2$ be one of the blowups involved in obtaining \mathcal{C} from \mathcal{C}_1 . Let $p, q \in C(L)$ with $p \neq q$. Then*

$$0 \leq \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_2 \times \mathcal{O}_L}}{I_{\bar{p}} + I_{\bar{q}}} \right) - \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_3 \times \mathcal{O}_L}}{I_{\bar{p}} + I_{\bar{q}}} \right) \leq \text{ram. deg}(L/K).$$

Proof. In this proof, we will omit the subscripts ' \mathcal{O}_L ' from the lengths, since all lengths will be taken as \mathcal{O}_L -modules. If \bar{p} does not meet \bar{q} on $\mathcal{C}_2 \times \mathcal{O}_L$ then both the lengths are zero, so we are done. Otherwise, let Ω be the closed point on $\mathcal{C}_2 \times \mathcal{O}_L$ where \bar{p} meets \bar{q} , and let α be the closed point of \mathcal{C}_2 such that Ω lies over α .

Let u, v be local coordinates on the (three-dimensional) ambient space to \mathcal{C}_2 at α , and let R denote the completion at (u, v) of the étale local ring of the ambient space to \mathcal{C}_2 at α . Let $B \subset R$ be the centre of the localisation of ϕ at α . We have

$$R \cong \tilde{\mathcal{O}}_K[[u, v]]_{(u, v, a)}$$

where $\tilde{\mathcal{O}}_K$ is a maximal unramified extension of \mathcal{O}_K and a is a uniformiser in $\tilde{\mathcal{O}}_K$, and that

$$B = (u, v, a) \quad \text{or} \quad B = (u, a),$$

depending on whether we are blowing up a point or a smooth fibral curve.

Blowups commute with flat base change, and the strict transform of a closed subscheme under a blowup is the corresponding blowup of that closed subscheme (see [Liu02, Corollary 8.1.17]), so we can be relaxed with our notation. We may write

$$p = (u - au_p, v - av_p) \quad q = (u - au_q, v - av_q)$$

where u_p, v_p, u_q and v_q are in $\mathcal{O}_L \cdot \tilde{\mathcal{O}}_K$. Setting ω' to be a uniformiser in the maximal ideal of $\tilde{\mathcal{O}}_K \cdot \mathcal{O}_L$, we have

$$\text{length} \left(\frac{\mathcal{O}_{\mathcal{E}_2 \times \mathcal{O}_L}}{I_p + I_q} \right) = \min(\text{ord}_{\omega'}(au_p - au_q), \text{ord}_{\omega'}(av_p - av_q)).$$

In the case $B = (u, v, a)$ we look at the affine patch of the blowup given by setting $a \neq 0$; the equations for p and q transform into

$$p' = (u - u_p, v - v_p) \quad \text{and} \quad q' = (u - u_q, v - v_q),$$

so

$$\begin{aligned} \text{length} \left(\frac{\mathcal{O}_{\mathcal{E}_3 \times \mathcal{O}_L}}{I_p + I_q} \right) &= \min(\text{ord}_{\omega'}(u_p - u_q), \text{ord}_{\omega'}(v_p - v_q)) \\ &= \text{length} \left(\frac{\mathcal{O}_{\mathcal{E}_2 \times \mathcal{O}_L}}{I_p + I_q} \right) - \text{ord}_{\omega'}(a). \end{aligned}$$

In the case $B = (u, a)$ we look again at the affine patch of the blowup given by setting $a \neq 0$; the equations for p and q transform into

$$p' = (u - u_p, v - av_p) \quad \text{and} \quad q' = (u - u_q, v - av_q),$$

so

$$\begin{aligned} \text{length} \left(\frac{\mathcal{O}_{\mathcal{E}_3 \times \mathcal{O}_L}}{I_p + I_q} \right) &= \min(\text{ord}_{\omega'}(u_p - u_q), \text{ord}_{\omega'}(av_p - av_q)) \\ &= \text{length} \left(\frac{\mathcal{O}_{\mathcal{E}_2 \times \mathcal{O}_L}}{I_p + I_q} \right) - (0 \text{ or } 1) \text{ord}_{\omega'}(a), \end{aligned}$$

so the result follows from the fact that, since $\tilde{\mathcal{O}}_K$ is unramified over \mathcal{O}_K , we have

$$\text{ord}_{\omega'}(a) = \text{ram. deg}(L \cdot \tilde{K}/\tilde{K}) = \text{ram. deg}(L/K).$$

□

Proof of Lemma 10. To prove Lemma 10, we apply Lemmata 11, 14, 12 and 13 in that order to find that there exists $0 \leq \beta \leq bde \log(\#\kappa(\nu))$ such that

$$\begin{aligned} \sum_{i,j} \log \left(\frac{1}{d(p_i, q_j)} \right) &= \frac{1}{m} \sum_{i,j} \sum_{\Omega|\nu} \log(\#\kappa(\Omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{E}_1 \times \mathcal{O}_K \mathcal{O}_L, \Omega}}{I_p + I_q} \right) \\ &= \frac{1}{m} \sum_{i,j} \sum_{\Omega|\nu} \log(\#\kappa(\Omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{E} \times \mathcal{O}_K \mathcal{O}_L, \Omega}}{I_p + I_q} \right) + \beta \\ &= \frac{1}{m} \log(\#\kappa(\omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{E} \times \mathcal{O}_L}}{I_D + I_E} \right) + \beta \\ &= \frac{1}{m} \log(\#\kappa(\omega)) \text{length}_{\mathcal{O}_K} \left(\frac{\mathcal{O}_{\mathcal{E}}}{I_D + I_E} \right) \cdot \text{ram. deg}(L/K) + \beta \\ &= \log(\#\kappa(\nu)) \iota_{\nu}(\mathcal{D}, \mathcal{E}) + \beta. \end{aligned}$$

□

Proof of Theorem 8. Let M^+ be the matrix from Lemma 9, let m_- denote the infimum of the entries of M^+ and m_+ their supremum. Let d, e and b_{ν} be the integers appearing in Lemma 10. Set

$$\mathcal{B}_{\nu} = (g^2(m_+ - m_-) + b_{\nu}de) \log(\#\kappa(\nu)).$$

Then the result follows from Lemmas 9 and 10. \square

5. ARCHIMEDEAN ABSOLUTE VALUES

5.1. Defining metrics. As in the non-Archimedean setting, we will define a metric and compare the distance between divisors in this metric to the local Néron pairing between the divisors (more precisely, between the corresponding points on the Jacobian).

Definition 15. For Archimedean absolute values ν we define

$$d_\nu : C(K_\nu^{alg}) \times C(K_\nu^{alg}) \rightarrow \mathbb{R}_{\geq 0}$$

by

$$\begin{aligned} & d_\nu((x_p : s_p : y_p), (x_q : s_q : y_q)) \\ &= \min \left(1, \max \left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right|_\nu, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right|_\nu \right), \max \left(\left| \frac{s_p}{x_p} - \frac{s_q}{x_q} \right|_\nu, \left| \frac{y_p}{x_p^{g+1}} - \frac{y_q}{x_q^{g+1}} \right|_\nu \right) \right). \end{aligned}$$

Recall that the Archimedean local Néron pairing is defined in terms of (logarithmic) Green's functions with respect to the Arakelov metric. Such Green's functions are unique up to addition of scalars - in particular, the pairing between two degree-zero divisors is well-defined. One applies the theory of *admissible metrics* to give a well defined pairing between all divisors (not strictly necessary for our applications, but allows for simpler notation).

Proposition 16. Fix an embedding of K into \mathbb{C} . Let gr be a Green's function with respect to the Arakelov 1-1 form on the Riemann surface $C(\mathbb{C})$ (defined using this embedding). Then there is a constant $c \geq 0$ such that for all pairs of distinct points $p, q \in C(\mathbb{C})$, we have

$$|\text{gr}(p, q) + \log d_\nu(p, q)| \leq c.$$

Proof. Let Δ be the diagonal in the product $C \times_K C$. The Green's function gr can be taken to be the logarithm of the norm of the canonical section of the line bundle $\mathcal{O}_{C \times C}(\Delta)$ (see [MB85, 4.10] for details). We need to show that the functions $\text{gr}(-, -)$ and $\log d_\nu(-, -)$ differ by a bounded amount. This is easy: both functions are continuous outside the diagonal Δ , and exhibit logarithmic poles along the diagonal ([MB85, 4.11]), so their difference is bounded by a compactness argument. \square

The following proposition is the Archimedean analogue of theorem 8, except we omit the 'explicitly computable'. This makes it much easier to prove.

Proposition 17. Given an Archimedean absolute value $\nu \in M_K^0$, there exists a constant \mathcal{B}_ν with the following property:

Let $D = D_1 - D_2$ and $E = E_1 - E_2$ be differences of reduced divisors on C with no common points in their supports, and assume that D and E both have degree zero. Write $D = \sum_i d_i p_i$, $E = \sum_j e_j q_j$, with $d_i, e_j \in \mathbb{Z}$ and

$p_i, q_j \in C(\mathbb{C})$. Recall from Section 2.1 that $[D, E]_\nu$ denotes the local Néron pairing of D and E at ν . Then

$$\left| [D, E]_\nu - \sum_{i,j} d_i e_j \log \left(\frac{1}{d_\nu(p_i, q_j)} \right) \right| \leq \mathcal{B}_\nu.$$

We call such a constant \mathcal{B}_ν a height-difference bound at ν .

Proof. This follows immediately from the definition of the Néron local pairing and proposition 16. \square

The key result is now:

Theorem 18. *There exists an algorithm which, given an Archimedean place ν , will compute a height difference bound \mathcal{B}_ν at ν .*

The author is aware of at least 2 proofs of this result. The first was given in [Hol12b]; it begins by analysing the case where the points in the support of D and E are not too close together using an explicit formula from [Hol12a] for the Green's function in terms of theta functions, together with explicit bounds on the derivatives of theta functions. The case where some points in the support are close together is handled by a 'hands-on' computation of how the Green's function and theta functions behave under linear equivalence of divisors. The proof occupies 33 pages. The second proof was given in a previous version of this paper [Hol12c]; it uses Merkl's theorem [CE⁺11], and requires 13 pages. The problem with these approaches is that they will be hard to implement, and more importantly will give extremely large bounds - with Merkl's theorem terms like $\exp(4800g^2)$ appear in the difference between the exponential heights, making this entirely impractical for calculations. Problems with methods coming from numerical analysis are discussed in the introduction.

What is needed is an algorithm which is practical to implement and gives small, rigorous bounds. It seems that at the time of writing no such algorithm is known. Since the existing algorithms are lengthy to write down and have no practical application (due to the size of the bounds they produce), we will not describe them in detail here.

6. THE FIRST NAÏVE HEIGHT

Assumption 19. *In this section we will for the first time require that $\#M_K^\infty \leq 1$ (so $\text{char } K > 0$ or $K = \mathbb{Q}$). We also assume that the curve C has a rational Weierstrass point, and we move a rational Weierstrass point of C to lie over $s = 0$, so that the affine equation for C has degree $2g + 1$. We denote this point by ∞ . We further assume that there is no Weierstrass point d with $X_d = 0$. None of these assumptions are essential, but they simplify the exposition.*

Remark 20. *The assumption that $\#M_K^\infty \leq 1$ is to ensure the existence of divisors E and E' in the next definition. To treat the general case, one may have to use several pairs of divisors E and E' , one for each Archimedean place of K . The comparisons of the heights will then become more involved.*

Definition 21. If K has positive characteristic, set $\mu = 1$. Otherwise, let $\mu := \frac{1}{3} \min_{w, w'} d_\nu(w, w')$ where the minimum is over pairs of distinct Weierstrass points of C , and ν is the Archimedean absolute value.

Given a rational point p of the Jacobian Jac_C of C , write $p = [D - \deg(D)\infty]$ where D is a reduced divisor on C such that the coefficient of ∞ in D is zero (such a D is unique). If the support of D contains any Weierstrass points, replace D by the divisor obtained by subtracting them off. Let d denote the degree of the resulting divisor D .

Choose once and for all a pair of degree- d effective divisors E and E' with disjoint support, supported on Weierstrass points away from ∞ , such that no point in the support of D is within Archimedean distance μ of any point in the support of E or E' . The existence of such divisors is clear since there are $2g + 1$ Weierstrass points away from ∞ and reduced divisors have degree g .

Let D^- denote the image of D under the hyperelliptic involution. Let L/K denote the minimal field extension over which D , E and E' are pointwise rational. Over L , we write $D = \sum_i d_i$, $E = \sum_i q_i^1$ and $E' = \sum_i q_i^2$. Given an absolute value ν of L , define

$$d_\nu(D - E, D^- - E') := \prod_{i,j} \frac{d_\nu(p_i, p_j^-) d_\nu(q_i^1, q_j^2)}{d_\nu(p_i, q_i^2) d_\nu(p_i^-, q_i^1)}.$$

Define the height $H^n : \text{Jac}_C(K) \rightarrow \mathbb{R}_{\geq 1}$ by

$$H^n(p) = \left(\prod_{\nu \in M_L} \frac{1}{d_\nu(D - E, D^- - E')} \right)^{\frac{1}{[L:K]}}.$$

Note that $d_\nu(D - E, D^- - E') = 1$ for all but finitely many absolute values ν , and so the product is finite. We define a logarithmic naïve height by $h^n(p) = \log(H^n(p))$.

Theorem 22 (Faltings, Hriljac). Let D_1 and D_2 be two divisors of degree zero on C with disjoint support. Suppose D_1 is linearly equivalent to D_2 , and write $[D_1] = [D_2]$ for the point they define in the Jacobian of C . Then

$$\sum_{\nu \in M_K} [D_1, D_2]_\nu = -\hat{h}([D_1])$$

where \hat{h} denotes the Néron-Tate height function.

Proof. See [Fal84] or [Hri83] for the case where K is a number field. The same proof works when K is a global field as has been remarked by number of authors, see e.g. [Mue13]. \square

Theorem 23. There exists a computable constant $\delta_1 \geq 0$ such that for all $p \in \text{Jac}_C(K)$ we have

$$\left| \hat{h}(p) - h^n(p) \right| \leq \delta_1.$$

Proof. For each absolute value ν of K , let \mathcal{B}_ν be the real number defined in Theorem 8 for ν non-Archimedean, and in Proposition 17 for ν Archimedean.

Note that $\mathcal{B}_\nu = 0$ for ν a non-Archimedean absolute value of good reduction for C . Define

$$\delta_1 := \sum_{\nu \in M_K} \mathcal{B}_\nu.$$

Let D, D^-, E, E' be the divisors associated to p as in Definition 21. Then by Theorem 8 and Proposition 17 we have that

$$\left| \sum_{\nu \in M_K} [D - E, D^- - E']_\nu - h^n(p) \right| \leq \delta_1.$$

Write $[D - E] = -[D^- - E'] - \tau$, for some 2-torsion point τ . By Theorem 22 and the biadditivity of the local Néron pairing, we have that

$$\begin{aligned} \hat{h}([D - E]) &= \sum_{\nu \in M_K} -[D - E, D - E]_\nu \\ &= \sum_{\nu \in M_K} [D - E, (D^- - E') + \tau]_\nu \\ &= \sum_{\nu \in M_K} [D - E, D^- - E']_\nu + \sum_{\nu \in M_K} [D - E, \tau]_\nu \\ &= \sum_{\nu \in M_K} [D - E, D^- - E']_\nu, \end{aligned}$$

since τ is torsion. Finally, since (as points in the Jacobian of C) $[D - E]$ and p differ by translation by another 2-torsion point (we subtracted off some Weierstrass points when defining the divisor D), we see that $\hat{h}(p) = \hat{h}([D - E])$, and we are done. \square

7. REFINED NAÏVE HEIGHTS

We define two new naïve heights which are each in turn simpler to compute, and we bound their difference from the Néron-Tate height. We will be able to compute the finite sets of points of bounded height with respect to the last of these heights.

Definition 24. *Given $p \in A(K)$, let $D = \sum_{i=1}^d p_i$ denote the corresponding divisor over some finite L/K as in Definition 21, and write $p_i = (X_{p_i}, Y_{p_i})$. Then set*

$$h^\heartsuit(p) = \sum_{i=1}^d h(X_{p_i}),$$

(where h is the usual height on an element of a global field) and set

$$h^\dagger(p) = h \left(\prod_{i=1}^d (X - X_{p_i}) \right),$$

where the right hand side is the height of a polynomial, which by definition is the height of the point in projective space whose coordinates are given by its coefficients.

We will give computable upper bounds on $h^\heartsuit - h^n$ and on $|h^\heartsuit - h^\dagger|$.

Lemma 25. *There exist computable constants $0 < \delta_2 < \delta_3$ such that for all non-Weierstrass points $p = (x : s : y) \in C(K^{\text{alg}})$, and for all Archimedean absolute values $\nu \in M_K^\infty$ on K with their unique extensions to K^{alg} , we have*

$$\delta_2 \leq d_\nu(p, p^-) / (2 \min(|Y|_\nu, |Y'|_\nu)) \leq \delta_3,$$

where as usual we write $Y = y/s^{g+1}$ and $Y' = y/x^{g+1}$.

Proof. Fix an Archimedean absolute value ν . Recall that d_ν is the metric defined in 15. A brief calculation shows that

$$\frac{d_\nu(p, p^-)}{(2 \min(|Y|_\nu, |Y'|_\nu))} = \min\left(1, \frac{1}{\min(|Y|_\nu, |Y'|_\nu)}\right).$$

Recall that C is given by

$$y^2 = \sum_{i=1}^{2g+2} f_i x^i s^{2g+2-i},$$

and set $a = \sqrt{\sum_i |f_i|_\nu}$. Then $|x/s|_\nu \leq 1$ implies $|Y|_\nu \leq a$ and $|s/x|_\nu \leq 1$ implies $|Y'|_\nu \leq a$, so we find

$$\frac{1}{2a} \leq \frac{d_\nu(p, p^-)}{(2 \min(|Y|_\nu, |Y'|_\nu))} \leq 1.$$

□

Definition 26. *Let L/K be a finite extension, and let $p \neq q \in C(L)$ be distinct points. Set*

$$\langle p, q \rangle_L = \frac{-1}{[L : K]} \log \prod_{\nu \in M_L} d_\nu(p, q).$$

Lemma 27. *There exists a computable constant δ_4 with the following property:*

let L/K be a finite extension, and let $p = (x : s : y) \in C(L)$ be a non-Weierstrass point. Then

$$|\langle p, p^- \rangle_L - (g+1) \text{h}(x/s)| \leq \delta_4$$

Proof. For $|\cdot|_\nu$ non-Archimedean, we have that if $|x|_\nu \leq |s|_\nu$ then $d_\nu(p, p^-) = |2y/s^{g+1}|_\nu$, and if $|s|_\nu \leq |x|_\nu$ then $d_\nu(p, p^-) = |2y/x^{g+1}|_\nu$. Hence for non-Archimedean ν we obtain

$$d_\nu(p, p^-) = |2y|_\nu \min(1/|x|_\nu^{g+1}, 1/|s|_\nu^{g+1}).$$

By Lemma 25, for Archimedean ν we have computable $0 < \delta_2 < \delta_3$ such that

$$\delta_2 < d_\nu(p, p^-) / \min(|2y/x^{g+1}|_\nu, |2y/s^{g+1}|_\nu) < \delta_3.$$

Hence

$$\prod_{\nu \in M_L^\infty} 1/\delta_3 \leq \frac{\prod_{\nu \in M_L} 1/d_\nu(p, p^-)}{\prod_{\nu \in M_L} |2y|_\nu^{-1} \prod_{\nu \in M_L} \max(|x|_\nu, |s|_\nu)^{g+1}} \leq \prod_{\nu \in M_L^\infty} 1/\delta_2.$$

Now $\prod_{\nu \in M_L^\infty} \delta_2^{-1/[L:K]}$ is bounded uniformly in L , and similarly for δ_3 . Finally, note

$$\left(\prod_{\nu \in M_L} |2y|_\nu^{-1} \right) \left(\prod_{\nu \in M_L} \max(|x|_\nu, |s|_\nu) \right)^{g+1} = H(x/s)^{[L:K](g+1)}.$$

□

Definition 28. Let $\nu \in M_K$. We write $|-|_\nu$ for the unique extension of $|-|_\nu$ to the algebraic closure of K_ν . For each non-Archimedean absolute value ν of K , we define λ_ν to be the smallest real number ≥ 1 such that the following conditions hold.

- For all Weierstrass points $d \in W$ with $d \neq \infty$, we have $1/\lambda_\nu \leq |X_d|_\nu \leq \lambda_\nu$ (c.f. Assumption 19).
- For all pairs of Weierstrass points $d, d' \in W \setminus \{\infty\}$ with $d \neq d'$ we have $1/\lambda_\nu \leq |X_d - X_{d'}|_\nu \leq \lambda_\nu$.
- We have $1/\lambda_\nu \leq |f_{2g+1}|_\nu \leq \lambda_\nu$, where f_{2g+1} is the leading coefficient of the defining polynomial f of the curve C .

Note that $\lambda_\nu = 1$ for all but finitely many absolute values ν . We define $\lambda_\nu = 1$ for all Archimedean absolute values ν , and set

$$\delta_5 = (2g + 3/2) \sum_{\nu \in M_K} \log \lambda_\nu.$$

Lemma 29. Let L/K be a finite extension, and let $p, d \in C(L)$ with $p \neq d$ be such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Then

$$- \sum_{\nu \in M_L^0} \log d_\nu(p, d) \leq [L : K] \left(\frac{1}{2} h(X_p - X_d) + \delta_5 \right).$$

Proof. The right hand side naturally decomposes as

$$\sum_{\nu \in M_L} \left(\frac{1}{2} \log^+ |X_p - X_d|_\nu^{-1} + (4g + 3) \log \lambda_\nu \right),$$

where ν' is the absolute value on K which extends to ν . Now it is clear that

$$\sum_{\nu \in M_L^\infty} \frac{1}{2} \log^+ |X_p - X_d|_\nu^{-1} \geq 0,$$

so it suffices to prove that for each non-Archimedean ν we have

$$- \log(d_\nu(p, d)) \leq \frac{1}{2} \log^+ |X_p - X_d|_\nu^{-1} + (4g + 3) \log \lambda_\nu,$$

or equivalently that (at this point we drop the subscript ν from the norm)

$$(1) \quad d_\nu(p, d)^2 \geq \min(|X_p - X_d|, 1) / \lambda^{4g+3}.$$

The proof of this inequality falls into a number of cases depending on the valuations of X_p, X_d etc. We will only give the details of the case

$$1 < |X_d|, \quad 1 < |X_p| \leq \lambda.$$

In this case, we have

$$\begin{aligned} d_\nu(p, d)^2 &= |X_p - X_d| \max \left(\frac{|X_p - X_d|}{|X_p|^2 |X_d|^2}, \frac{|f_{2g+1}| \prod_{d' \in W \setminus \{d, \infty\}} |X_p - X_{d'}|}{|X_p|^{2g+2}} \right) \\ &\geq \frac{|X_p - X_d|}{\lambda^{2g+2}} \max \left(|X_p - X_d|, |f_{2g+1}| \prod_{d' \in W \setminus \{d, \infty\}} |X_p - X_{d'}| \right). \end{aligned}$$

Now suppose that $|X_p - X_d| < \lambda$ and

$$|f_{2g+1}| \prod_{d' \in W \setminus \{d, \infty\}} |X_p - X_{d'}| < 1/\lambda^{2g+1}.$$

Then there exists $d_0 \in W \setminus \{d, \infty\}$ such that $|X_{d_0} - X_p| < 1/\lambda$, so by the strong triangle inequality we have

$$|X_d - X_{d_0}| \leq \max(|X_d - X_p|, |X_p - X_{d_0}|) < 1/\lambda,$$

a contradiction. Hence

$$\max \left(|X_p - X_d|, |f_{2g+1}| \prod_{d' \in W \setminus \{d, \infty\}} |X_p - X_{d'}| \right) \geq 1/\lambda^{2g+1},$$

and Equation (1) follows. \square

Lemma 30. *Let L/K be a finite extension, and let H denote the usual exponential height on L . Let $X_1, X_2 \in L$. Then $H(X_1 + X_2) \leq 2^{\#M_K^\infty} H(X_1) H(X_2)$.*

Proof. Omitted. \square

Lemma 31. *There exists a computable constant δ_6 with the following property.*

Let L/K be a finite extension, and let $p, d \in C(L)$ such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Suppose also that $d_\nu(p, d) \geq \mu$ for all Archimedean ν (where μ is the constant from Definition 21). Then

$$\langle p, d \rangle_L \leq \frac{1}{2} h(X_p) + \delta_6.$$

Proof. From Lemma 29 we see that

$$\langle p, d \rangle_L \leq \frac{1}{2} h(X_p - X_d) + \delta_5 - \log(\mu).$$

Now by Lemma 30, we have

$$h(X_p - X_d) \leq h(X_p) + h(X_d) + \#M_K^\infty \log(2).$$

We define

$$\delta_6(d) = -\log(\mu) + \frac{1}{2} h(X_d) + \frac{\#M_K^\infty}{2} \log(2) + \delta_5.$$

Then we find that for all L and p as in the statement, we have

$$\langle p, d \rangle_L \leq \frac{1}{2} h(X_p) + \delta_6(d).$$

Finally, there are only finitely many Weierstrass points, so setting $\delta_6 = \max_d \delta_6(d)$, we are done. \square

Lemma 32. *There exists a computable constant δ_7 such that the following holds.*

Given $p \in A(K)$, let D , E and E' denote the divisors given in Definition 21. Let L/K be the minimal finite extension such that D , E and E' are all pointwise rational over L . We write

$$D = \sum_{i=1}^d p_i, \quad E = \sum_{i=1}^d q_i, \quad E' = \sum_{i=1}^d q'_i.$$

Then

$$h^n(p) \geq \sum_{i=1}^d \left(\langle p_i, p_i^- \rangle_L - \sum_{j=1}^d \langle p_i, q_j \rangle_L - \sum_{j=1}^d \langle p_i, q'_j \rangle_L \right) + \delta_7,$$

where p_i^- is the image of p_i under the hyperelliptic involution.

Proof. Recall that

$$h^n(p) = \sum_{i,j=1}^d \langle p_i, p_j^- \rangle_L + \sum_{i,j=1}^d \langle q_i, q'_j \rangle_L - \sum_{i,j=1}^d \langle p_i, q_j \rangle_L - \sum_{i,j=1}^d \langle p_i^-, q'_j \rangle_L.$$

Since the q_i and q'_i are distinct Weierstrass points we easily bound $\sum_{i,j=1}^d \langle q_i, q'_j \rangle_L$.

It remains to find a lower bound on the terms $\langle p_i, p_j^- \rangle$. Note that d_ν is bounded above by 1 for all ν , hence $\langle p_i, p_j^- \rangle \geq 0$. \square

Lemma 33. *There exists a computable constant δ_8 such that in the setup of Lemma 32 we have*

$$h^n(p) \geq \sum_{i=1}^d h(X_{p_i}) + \delta_8.$$

Proof. In Lemma 32 we showed

$$h^n(p) \geq \sum_{i=1}^d \left(\langle p_i, p_i^- \rangle_L - \sum_{j=1}^d \langle p_i, q_j \rangle_L - \sum_{j=1}^d \langle p_i, q'_j \rangle_L \right) + \delta_7.$$

In Lemma 27 we showed (using that the p_i are never Weierstrass points) that for some computable δ_4 we have

$$|\langle p_i, p_i^- \rangle_L - (g+1)h(X_{p_i})| \leq \delta_4.$$

In Lemma 31 we showed that

$$\langle p_i, q_j \rangle_L \leq \frac{1}{2}h(X_{p_i}) + \delta_6,$$

and similarly for q'_j .

Combining these, we see using $d \leq g$ that for each i

$$\begin{aligned} \langle p_i, p_i^- \rangle_L - \sum_{j=1}^d \langle p_i, q_j \rangle_L - \sum_{j=1}^d \langle p_i, q'_j \rangle_L &\geq (g+1)h(X_{p_i}) - 2 \sum_{j=1}^d \frac{1}{2}h(X_{p_i}) - \delta_4 + 2d\delta_6 \\ &= ((g+1) - 2d\frac{1}{2})h(X_{p_i}) - \delta_4 + 2d\delta_6 \\ &\geq h(X_{p_i}) - \delta_4 + 2d\delta_6. \end{aligned}$$

from which the result follows. \square

Theorem 34. *There exists a computable constant δ_9 such that for all $p \in A(K)$ we have*

$$\hat{h}(p) + \delta_9 \geq h^\heartsuit(p).$$

Proof. Set $\delta_9 = \delta_1 + \delta_8$. The result follows from Theorem 23 and Lemma 33. \square

Lemma 35. *Fix a finite extension L/K . Given $a_1, \dots, a_n \in L$, set $\psi_n = \prod_{i=1}^n (t - a_i) \in L[t]$. If $\text{char } K > 0$ then $h(\psi_n) = \sum_{i=1}^n h(a_i)$, otherwise*

$$\left| h(\psi_n) - \sum_{i=1}^n h(a_i) \right| \leq n \log 2$$

We summarise this by writing

$$\left| h(\psi_n) - \sum_{i=1}^n h(a_i) \right| \leq (n \log 2) \delta_{\text{char } K}$$

Proof. [Sil09, Theorem VIII.5.9] \square

Corollary 36. *For all $p \in A(K)$ we have*

$$\left| h^\heartsuit(p) - h^\dagger(p) \right| \leq (g \log 2) \delta_{\text{char } K}.$$

Definition 37. *Given a real number B , we define*

$$\hat{M}(B) := \{p \in A(K) \mid \hat{h}(p) \leq B\}$$

and

$$M^\dagger(B) := \{p \in A(K) \mid h^\dagger(p) \leq B\}.$$

The main result of this paper is the following.

Corollary 38. *Let $B \in \mathbb{R}$. Let $B' = B + \delta_9 + (g \log 2) \delta_{\text{char } K}$. Then for all real numbers B we have*

$$\hat{M}(B) \subset M^\dagger(B').$$

Moreover, the finite set $M^\dagger(B')$ is computable, and hence by results in [Hol12a] so is the finite set $\hat{M}(B)$.

Proof. The inclusion follows from the results above. We describe one algorithm to compute $M^\dagger(B)$.

1) Let S be the finite set of all polynomials $\prod_{i=1}^d (X - a_i)$, for $d \leq g$, of height up to B .

2) It suffices to determine for each $a \in S$ whether a is the ‘ x -coordinate polynomial’ of a divisor in Mumford representation; in other words, whether

there exists another univariate polynomial b such that (a, b) satisfy the properties of a Mumford representation. This corresponds to checking whether the polynomial $f - a^2$ has a factor of degree less than $\deg a$, which is widely implemented. \square

8. A WORKED EXAMPLE

Given a prime number p , we fix a proper multi-set of absolute values $M_{\mathbb{F}_p(t)}$ by requiring it to contain exactly once the unique $|\cdot|_t$ such that $|t|_t = p^{-1}$. We begin by bounding the difference between the first and final naïve heights for a certain infinite family of curves. First we define the infinite family:

Definition 39. Fix an integer $g > 0$. Let p be a prime number not dividing $2(2g + 1)$, and let $K = \mathbb{F}_p(t)$. Let C denote the hyperelliptic curve given by affine equation

$$y^2 = x^{2g+1} + t.$$

Proposition 40. For all points $q \in \text{Jac}_C(K)$, we have

$$h^n(q) + \frac{g(8g^2 + 15g + 4) \log p}{2g + 1} \geq h^\heartsuit(q) = h^\dagger(q).$$

Proof. We will need to compute various heights and valuations of elements of K and extensions. Fix a primitive $(2g + 1)$ -th root ζ of 1 in K^{alg} . Write $f = x^{2g+1} + t$, and write $\alpha_0, \dots, \alpha_{2g}$ for the roots in K^{alg} of f , ordered such that $\alpha_n = \alpha_0 \zeta^n$. For all absolute values $\nu \in M_K$, we have $|\zeta|_\nu = 1$ and hence for all n we have

$$|\alpha_n|_\nu = |\alpha_0|_\nu = |t|_\nu^{1/2g+1}.$$

Now $|t|_t = p^{-1}$ and $|t|_{1/t} = p$, and $|t|_\nu = 1$ for all other $\nu \in M_K$. From this we deduce that $h(t) = \log p$ and for all n that $h(\alpha_n) = (\log p)/(2g + 1)$. Noting that $\alpha_n - \alpha_m = \alpha_0(\zeta^n - \zeta^m)$, we have for all $n \neq m$ and $\nu \in M_K$ that $|\alpha_n - \alpha_m|_\nu = |\alpha_0|_\nu$. From this we deduce that for all pairs of distinct Weierstrass points $d_i \neq d_j$, we have

$$\langle d_i, d_j \rangle_L = \frac{2 \log p}{2g + 1},$$

independent of the field L .

Since K has no Archimedean absolute values we immediately see that we may take $\delta_2 = \delta_3 = \delta_4 = 0$. We have $\lambda_\nu = 1$ for all ν apart from $\nu = (t)$ and $\nu = (1/t)$, where we have $\lambda_\nu = p^{1/2g+1}$. From this we see

$$\delta_5 = \frac{(4g + 3) \log p}{2g + 1}.$$

We have

$$\delta_6 = \frac{1}{2} \max_n h(\alpha_n) + \delta_5 = \frac{\log p}{4g + 2} + \frac{(4g + 3) \log p}{2g + 1},$$

and since

$$\sum_{d \neq d'} \langle d, d' \rangle_L = 4g \log p$$

(the sum is over distinct points d, d' in $W \setminus \{\infty\}$) we may take

$$\delta_7 = 4g \log p.$$

Finally we see $\delta_8 = 2g^2\delta_6 + \delta_7$, and the result follows. \square

Finally, for three members of this family of curves, we will bound the difference between the Néron-Tate height and the naïve heights. This requires constructing a regular model of the curve, which we do in **MAGMA** using Steve Donnelly's 'regular models' function. First we give two examples with small genus over small fields, to illustrate the sizes of the bounds, and then we give an example in higher genus, to illustrate that the method to find bounds remains practical.

Theorem 41. *Let $p = 3$ and $g = 2$, and let C be as in (39). Then for all points $q \in \text{Jac}_C(K)$, we have*

$$\hat{h}(q) + 108 \log 3 \geq h^\heartsuit(q) = h^\dagger(q).$$

Let $p = 5$ and $g = 4$, and let C be as in (39). Then for all points $q \in \text{Jac}_C(K)$, we have

$$\hat{h}(q) + 667 \log 5 \geq h^\heartsuit(q) = h^\dagger(q).$$

Let $p = 101$ and $g = 11$, and let C be as in (39). Then for all points $q \in \text{Jac}_C(K)$, we have

$$\hat{h}(q) + 11820 \log 101 \geq h^\heartsuit(q) = h^\dagger(q).$$

Proof. We give details for the genus 11 example, the others are similar. Applying Proposition 40, it is enough to compute the constants \mathcal{B}_ν from Theorem 8. The model given by

$$uy^2 = usx^{2g+1} + ts^{2g+2}$$

in weighted projective space $\mathbb{P}(1, 1, g+1)$ over B_K is regular except over $u = 0$, and moreover all fibres outside $u = 0$ are irreducible. Hence $\mathcal{B}_\nu = 0$ whenever ν does not correspond to the prime (u) .

Next we use **MAGMA** to compute the regular model of C over (u) . We rearrange the equation

$$uy^2 = ux^{23} + 1$$

to $\tilde{y}^2 = u\tilde{x}^{23} + u^{23}$, absorbing u into \tilde{x} and u^{g+1} into \tilde{y} (this process is equivalent to performing $g+2 = 13$ blowups). Now the equation is of a form where we can plug it into **MAGMA**, which yields a regular model after 68 blowups, so $81 = 68 + 13$ blowups were used in total (32 are needed in the genus 4 case, 18 in genus 2). We have made no attempt to count the longest chain of blowups, we just know the total number of blowups used; it would not be hard to improve this. This regular model has 49 irreducible components in its special fibre (21 in the genus 4 case, 13 in genus 2), and the Moore-Penrose pseudo-inverse of its 49×49 intersection matrix has maximum entry $4.102 \dots$ and minimum entry $-8.076 \dots$. As a result, we find that

$$\begin{aligned} \mathcal{B}_{(u)} &= (g^2(4.102 \dots + 8.076 \dots) + 81g^2) \log 101 \\ &= 11274.6 \dots \log 101. \end{aligned}$$

MAGMA code for performing this computation can be obtained by downloading the source files for this paper (arXiv version).

Proposition 40 yields a bound of

$$\frac{11(8(11^2) + 15 \cdot 11 + 4)}{23} = 543.78\dots$$

from which the result follows. \square

Remark 42. *The computations for Theorem 41 took under 10 seconds to perform (and could have been done by hand with reasonable patience for genus 2). It is clear that, with the methods developed in this paper, the bottleneck is now searching for points of bounded naïve height, not finding a bound. As such, it would be very useful to improve the bounds given in these examples, but there seems little point in speeding up the algorithm to compute the bounds.*

REFERENCES

- [And02] G. W. Anderson. Edited 4-theta embeddings of jacobians. *Michigan Math J.*, volume 52, Issue 2 (2004), 303-339.
- [BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [BMS⁺08] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and Sz. Tengely. Integral points on hyperelliptic curves. *Algebra and Number Theory*, 2:859–885, 2008.
- [Bru06] P. Bruin. Green functions on riemann surfaces and an application to arakelov theory. Master’s thesis, Universiteit Leiden, 2006.
- [CE⁺11] J.M. Couveignes, B. Edixhoven, et al. Computational aspects of modular forms and galois representations. 2011.
- [CGO84] V. Cossart, J. Giraud, and U. Orbanz. *Resolution of surface singularities*, volume 1101 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1984. With an appendix by H. Hironaka.
- [CPS06] J. E. Cremona, M. Prickett, and S. Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.
- [Dem68] V. A. Dem’janenko. An estimate of the remainder term in Tate’s formula. *Mat. Zametki*, 3:271–278, 1968.
- [dJ04] R. de Jong. *Explicit Arakelov Geometry*. PhD thesis, Universiteit Leiden, 2004.
- [dJ05] R. de Jong. Arakelov invariants of riemann surfaces. *Documenta Mathematica*, 10:311–329, 2005.
- [DP02] S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés de variétés abeliennes ii. *Commentarii Mathematici Helvetici*, 77(4):639–700, 2002.
- [Fal84] G. Faltings. Calculus on arithmetic surfaces. *The Annals of Mathematics*, 119(2):387–424, 1984.
- [Fly93] E. V. Flynn. The group law on the Jacobian of a curve of genus 2. *J. Reine Angew. Math.*, 439:45–69, 1993.
- [FS97] E. V. Flynn and N. P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, 79(4):333–352, 1997.
- [Hol12a] D. Holmes. Computing Néron-Tate heights of points on hyperelliptic Jacobians. *Journal of Number Theory*, 132(6):1295 – 1305, 2012.
- [Hol12b] D. Holmes. *Néron-Tate heights on the Jacobians of high-genus hyperelliptic curves*. PhD thesis, University of Warwick, 2012.
- [Hol12c] D. Holmes. *An Arakelov-theoretic approach to naïve heights on hyperelliptic Jacobians (version 1)* <http://arxiv.org/abs/1207.5948v1>
- [Hri83] P. Hriljac. The Néron-tate height and intersection theory on arithmetic surfaces. *PhD Thesis, Massachusetts Institute of Technology*, 1983.

- [Jav12] A. Javanpeykar. Polynomial bounds for arakelov invariants of curves with given belyi degree. *To appear in Algebra and Number Theory*, 2012.
- [Lan83] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.
- [Lan88] S. Lang. *Introduction to Arakelov theory*. Springer, 1988.
- [Liu02] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Ern e, Oxford Science Publications.
- [Man71] Ju. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.
- [Mat80] H. Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.
- [MB85] L. Moret-Bailly. M etriques permises. *Ast risque*, 127:29–87, 1985.
- [Mue10] J. S. Mueller. Canonical heights on Jacobians. 2010. Universit t Bayreuth PhD thesis.
- [Mue13] J. S. Mueller. Computing canonical heights using arithmetic intersection theory. *Math. Comp.*, DOI: <http://dx.doi.org/10.1090/S0025-5718-2013-02719-6>, 2013.
- [Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.
- [Mum83] D. Mumford. *Tata lectures on theta I*. Birkh user, 1983.
- [N r65] A. N ron. Quasi-fonctions et hauteurs sur les vari t s ab liennes. *Annals of Mathematics*, 82(2):249–331, 1965.
- [Pen55] R. Penrose. A generalized inverse for matrices. *Proc. Cambridge Philos. Soc.*, 51:406–413, 1955.
- [Rei72] M. Reid. *The complete intersection of two or more quadrics*. PhD thesis, University of Cambridge, 1972.
- [Sik95] S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain Journal of Mathematics*, 25(4), 1995.
- [Sil90] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.
- [Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [Sto99] M. Stoll. On the height constant for curves of genus two. *Acta Arith*, 90(2):183–201, 1999.
- [Sto02] M. Stoll. On the height constant for curves of genus two, ii. *Acta Arith*, 104(2):165–182, 2002.
- [Sto12] M. Stoll. Explicit kummer varieties for hyperelliptic curves of genus 3. 2012.
- [Uch06] Y. Uchida. On the difference between the ordinary height and the canonical height on elliptic curves. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 82(3):56–60, 2006.
- [VW98] P. Van Wamelen. Equations for the jacobian of a hyperelliptic curve. *Trans. Amer. Math. Soc.*, 350:3083–3106, 1998.
- [Zim76] H. G. Zimmer. On the difference of the Weil height and the N ron-Tate height. *Math. Z.*, 147(1):35–51, 1976.
- [ZM72] Ju. G. Zarhin and Ju. I. Manin. Height on families of abelian varieties. *Mat. Sb. (N.S.)*, 89(131):171–181, 349, 1972.

MATHEMATISCH INSTITUUT LEIDEN, NIELS BOHRWEG 1, 2333 CA LEIDEN, THE NETHERLANDS

E-mail address: holmesdst@math.leidenuniv.nl