New York Journal of Mathematics

New York J. Math. **20** (2014) 927–957.

An Arakelov-theoretic approach to naïve heights on hyperelliptic Jacobians

David Holmes

Abstract. 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.

Contents

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 gave a simpler formula for Néron's height. Using this formula, Tate (unpublished), Dem'janenko [Dem68], Zimmer [Zim76], Silverman [Sil90] and more recently Cremona, Prickett and Siksek [CPS06], Uchida [Uch08] and Bruin [Bru13] have given

Received May 20, 2014.

2010 *Mathematics Subject Classification.* Primary: 11G30; secondary: 11G50, 37P30.

Key words and phrases. Néron–Tate height, Arakelov theory, height-difference bounds, hyperelliptic curves.

ISSN 1076-9803/2014

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 either of the Kummer variety, or (in the case of Dem'janenko) of the Jacobian itself. Using equations for the duplication maps, they 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 the Jacobian of a hyperelliptic curve, and a similar (though different) algorithm for the same problem was 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 24.

1.2. Relation to classical naïve heights. Let C be a hyperelliptic curve over a global field, with marked Weierstrass point ∞ and Jacobian J. Let $p = [D - g \cdot \infty]$ be a point on the Jacobian J, where D is a suitably chosen divisor on the curve C. We will define various intermediate heights, but the final naïve height of p (denoted $\mathrm{h}^\dagger(p)$) 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 $\mathrm{H}^0(J, 2\vartheta)$, where ϑ is the theta line bundle, i.e., the line bundle associated to the divisor arising as the image of C^{g-1} under the usual map $C^g \to J$. As such, it is clear that $\mathrm{h}^\dagger \leq \hat{\mathrm{h}} + c$ for some 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 over a number field. 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 4.1), but we can estimate the sizes of the bounds produced by techniques in the literature. Bounds using Merkl's theorem [EC+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 11), 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 Ph.D. 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 45, 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 $86 \log 3$), 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 Propositon 9.3 (page 665) in the paper [DaP02] 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. Acknowledgements. This paper bears some resemblance to the final two chapters of the author's Ph.D. 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. Finally, the author is very grateful to the anonymous referee: firstly for a very rapid and helpful report, which has greatly improved the exposition of the paper, and secondly for some `MAGMA` code which substantially improved the bounds obtained in Section 7.

2. Outline

Let K be a global field, and L/K a finite extension. Write M_L for a proper set of absolute values of L, and $|-|_\nu$ for the valuation at an element $\nu \in M_L$ (see Definition 3 for our conventions regarding these). We define the (absolute) height of an element $x \in L$ by

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

and $\mathrm{H}(x) = \exp \mathrm{h}(x)$. 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. Let C/K be a hyperelliptic curve. For each absolute value ν of K, we will construct a metric or pseudo-metric d_ν on divisors on C 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

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

where D' is a chosen divisor which is linearly equivalent to $-D$ (up to addition of divisors representing 2-torsion points on the Jacobian). Since the curve C is compact and our metrics continuous, the function $\mathrm{d}_\nu(D, D')^{-1}$ 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 5. Theorem 10 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 the integers of 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 18 we define a pseudo-metric on C at each Archimedean absolute value. Theorem 22 bounds the difference between this pseudo-metric and the local Néron pairing.

We apply Theorem 26 (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 45 we give a worked example of how to compute these bounds for several curves including a genus 11 curve over $\mathbb{F}_{101}(t)$.

2.1. Setup and notation.

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 nonzero polynomial $f(X, S) = \sum_{i=0}^{2g+2} f_i X^i S^{2g+2-i} \in K[X, S]$ with exactly $2g+2$ distinct zeroes in $\mathbb{P}^1(K^{\mathrm{alg}})$. 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 nonempty multi-set of nontrivial 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 a 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 $\operatorname{Spec}\mathbb{Z}$. For example, if L is a number field then B_L is the spectrum of the ring of integers of L.

3. Non-Archimedean results

3.1. Defining metrics.

Definition 5. For each absolute value $\nu \in M_K$, we fix $(K_\nu^{\mathrm{alg}}, |-|_\nu)$ to be an algebraic closure of the completion K_ν together with the absolute value which restricts to ν on $K \subset K_\nu^{\mathrm{alg}}$. For non-Archimedean absolute values ν we define

$$\mathrm{d}_\nu : C(K_\nu^{\mathrm{alg}}) \times C(K_\nu^{\mathrm{alg}}) \to \mathbb{R}_{\geq 0}$$

by

$$\mathrm{d}_\nu((X_p : S_p : Y_p), (X_q : S_q : Y_q)) =$$
$$\begin{cases} \max\left(|x_p - x_q|_\nu, \left|y_p^{g+1} - y_q^{g+1}\right|_\nu\right) & \text{if } |X_p|_\nu \leq |S_p|_\nu \text{ and } |X_q|_\nu \leq |S_q|_\nu \\ \max\left(|s_p - s_q|_\nu, \left|{y'_p}^{g+1} - {y'_q}^{g+1}\right|_\nu\right) & \text{if } |X_p|_\nu \geq |S_p|_\nu \text{ and } |X_q|_\nu \geq |S_q|_\nu \\ 1 & \text{otherwise} \end{cases}$$

(here as always $x_p = X_p/S_p$ etc).

Proposition 6. *For each $\nu \in M_K^0$, $\mathrm{d} = \mathrm{d}_\nu$ is a metric on $C(K_\nu^{alg})$. Moreover, for each such ν, we have $\mathrm{d}_\nu(p,q) \leq 1$ for all p and q.*

Proof. We omit the subscripts ν from the absolute values. We begin by observing that if $(X : S : Y) \in C(K_\nu^{\mathrm{alg}})$ 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 $|-|$ is non-Archimedean, we see for all p, $q \in C(K_\nu^{\mathrm{alg}})$ that $\mathrm{d}(p,q) \leq 1$.

For showing that d is a metric, only the triangle inequality is not 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

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

The other cases are similar. □

3.2. A simple formula for the distance function in a special case.

Here we give a simple bound on the logarithm of the distance between two points p and w on C where w is a Weierstrass point. This will be needed in Section 6.

Definition 7. We write W for the set of Weierstrass points of C (over K^{alg}). We assume that C has no Weierstrass point with X-coordinate zero (cf. Assumption 23). Let $\nu \in M_K^0$. We define λ_ν to be the smallest real number ≥ 1 such that the following conditions hold.

- For all Weierstrass points $w \in W$ with $w \neq \infty$, we have
$$1/\lambda_\nu \leq |x_w|_\nu \leq \lambda_\nu.$$
- For all pairs of Weierstrass points w, $w' \in W \setminus \{\infty\}$ with $w \neq w'$ we have $1/\lambda_\nu \leq |x_w - x_{w'}|_\nu \leq \lambda_\nu$.
- 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 ν.

Lemma 8. *Let L/K be a finite extension, and let p, $w \in C(L)$ with $p \neq w$ be such that $s_p \neq 0$ and w is a Weierstrass point with $s_w \neq 0$. Let ν be a non-Archimedean absolute value of L extending an absolute value ν' of K. We have*

$$-\log(\mathrm{d}_\nu(p,w)) \leq \frac{1}{2}\log^+ |x_p - x_w|_\nu^{-1} + (2g + 3/2)\log \lambda_{\nu'}.$$

Proof. The formula we must show is equivalent to (at this point we drop the subscripts ν and ν')

$$\mathrm{d}(p,w)^2 \geq \min(|x_p - x_w|, 1)/\lambda^{4g+3}. \tag{1}$$

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

$$1 < |x_w|, \quad 1 < |x_p| \leq \lambda.$$

In this case, we have

$$\begin{aligned}\mathrm{d}(p,w)^2 &= |x_p - x_w| \max\left(\frac{|x_p - x_w|}{|x_p|^2\,|x_w|^2}, \frac{|f_{2g+1}|\prod_{w'\in W\setminus\{w,\infty\}}|x_p - x_{w'}|}{|x_p|^{2g+2}}\right)\\ &\geq \frac{|x_p - x_w|}{\lambda^{2g+2}}\max\left(|x_p - x_w|, |f_{2g+1}|\prod_{w'\in W\setminus\{w,\infty\}}|x_p - x_{w'}|\right).\end{aligned}$$

Now suppose that $|x_p - x_w| < \lambda$ and

$$|f_{2g+1}|\prod_{w'\in W\setminus\{w,\infty\}}|x_p - x_{w'}| < 1/\lambda^{2g+1}.$$

Then there exists $w_0 \in W \setminus \{w,\infty\}$ such that $|x_{w_0} - x_p| < 1/\lambda$, so by the strong triangle inequality we have

$$|x_w - x_{w_0}| \leq \max(|x_w - x_p|, |x_p - x_{w_0}|) < 1/\lambda,$$

a contradiction. Hence

$$\max\left(|x_p - x_w|, |f_{2g+1}|\prod_{w'\in W\setminus\{w,\infty\}}|x_p - x_{w'}|\right) \geq 1/\lambda^{2g+1},$$

and Equation (1) follows. □

3.3. Local Néron pairings in the non-Archimedean case. We summarise the construction of the local Néron pairing at a non-Archimedean place from [Lan88, IV, §1], where more details can be found. This pairing will play a crucial role in allowing us to compare our 'distance' function d_ν to the local height pairing at ν.

Given an absolute value ν of K, we write $\mathrm{Div}^0(C_{K_\nu})$ 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

$$[-,-]_\nu : \left\{(D,E) \in \mathrm{Div}^0(C_{K_\nu}) \times \mathrm{Div}^0(C_{K_\nu}) | \operatorname{supp}(D) \cap \operatorname{supp}(E) = \emptyset\right\} \to \mathbb{R}.$$

Its definition depends on whether ν is an Archimedean or non-Archimedean absolute value; the definition in the Archimedean case will be given in Section 4.3.

Let ν be a non-Archimedean absolute value. Write $\mathcal{O}_{K_\nu}$ for the ring of integers of the completion K_ν. Let $\mathscr{C} = \mathscr{C}_{\mathcal{O}_{K_\nu}}$ be a proper, flat, regular model of C over $\mathcal{O}_{K_v}$. We write ι_ν for the (rational-valued) intersection pairing between divisors over ν (as defined in [Lan88, IV, §1, page 72]). Let D and E be elements of $\mathrm{Div}^0(C_{K_\nu})$ with disjoint support. We extend D and E to horizontal divisors $\overline{D}$ and $\overline{E}$ on $\mathscr{C}$. Write $\mathbb{Q}\,\mathrm{FDiv}(C_{K_\nu})$ for the group of $\mathbb{Q}$-divisors on $\mathscr{C}$ supported on the special fibre $\mathscr{C}_\nu$. We define a map (cf. [Lan88, III, §3])

$$\Phi : \mathrm{Div}^0(C_{K_\nu}) \to \frac{\mathbb{Q}\,\mathrm{FDiv}(C_{K_\nu})}{\mathbb{Q}(\mathscr{C}_\nu)}$$

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

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

Then define the local Néron pairing by

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

where κ is the residue field at ν.

Proposition 9. *The local Néron pairing at a non-Archimedean absolute value ν is independent of the choice of regular model $\mathscr{C}_{\mathcal{O}_{K_\nu}}$.*

Proof. Combine Theorem 5.1 and Theorem 5.2 of [Lan88, III]. □

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

Theorem 10. *Given a non-Archimedean absolute value $\nu \in M_K^0$, there exists an explicitly computable constant $\mathscr{B}_\nu$ 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 3.3 that $[D, E]_\nu$ denotes the local Néron pairing of D and E at ν. Then

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

Moreover, if C has a smooth proper model over ν, then we may take $\mathscr{B}_\nu = 0$.

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 $\nu \in M_K^0$. Write $\mathscr{C}_1$ for the Zariski closure of $C : Y^2 = F(X, S)$ in $\mathbb{P}_{\mathcal{O}_{K_\nu}}(1, 1, g+1)$. A result of Hironaka, contained in his appendix to [CGO84] (pages 102 and 105) gives us an algorithm to resolve the singularities of $\mathscr{C}_1$ by a sequence of blowups at closed points and along smooth curves (the latter replacing the normalisations used in Lipman's algorithm [Lip78]); we observe that $\mathscr{C}_1$ may locally be embedded in $\mathbb{P}^2_{\mathcal{O}_{K_\nu}}$, and so Hironaka's result can be applied. We fix once and for all a choice of resolution $\mathscr{C}$ of $\mathscr{C}_1$ using this algorithm of Hironaka — thus we fix both the model $\mathscr{C}$ and the sequence of blowups at smooth centres used to obtain it.

We begin by bounding the function Φ. Let F denote the free abelian group generated by prime divisors supported on the special fibre of $\mathscr{C}$ over ν, and let V denote the finite-dimensional $\mathbb{Q}$-vector space obtained by tensoring F over $\mathbb{Z}$ with $\mathbb{Q}$. Let $M : V \times V \to \mathbb{Q}$ be the map induced by tensoring the restriction of the intersection pairing on $\mathscr{C}$ 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 11. *Let M^+ denote the Moore–Penrose pseudo-inverse* [Moo20, Pen55] *of M, let m_- denote the infimum of the entries of M^+ and m_+ their supremum. Let $D = D^+ - D^-$ and $E = E^+ - E^-$ 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*

$$\left|\iota_\nu\left(\Phi(D), \overline{E}\right)\right| \le 2g^2(m_+ - m_-).$$

Proof. For each $1 \le i \le n$, set

$$d_i^+ = \iota_\nu\left(\overline{D}^+, Y_i\right), \qquad d_i^- = \iota_\nu\left(\overline{D}^-, Y_i\right),$$
$$e_i^+ = \iota_\nu\left(\overline{E}^+, Y_i\right), \qquad e_i^- = \iota_\nu\left(\overline{E}^-, Y_i\right),$$

and note that all $d_i^\pm$ and $e_i^\pm$ are nonnegative. Then for each i set

$$d_i = d_i^+ - d_i^-, \qquad e_i = e_i^+ - e_i^-,$$

and define vectors in V by

$$d = (d_i)_i, \qquad d^+ = (d_i^+)_i, \qquad d^- = (d_i^-)_i,$$
$$e = (e_i)_i, \qquad e^+ = (e_i^+)_i, \qquad e^- = (e_i^-)_i.$$

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

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

Expanding out, we find

$$\begin{aligned}\iota_\nu\left(\Phi(D), \overline{E}\right) = &-d^+ \cdot \left(M^+\right)^T \cdot (e^+)^T + d^+ \cdot \left(M^+\right)^T \cdot (e^-)^T \\ &+ d^- \cdot \left(M^+\right)^T \cdot (e^+)^T - d^- \cdot \left(M^+\right)^T \cdot (e^-)^T.\end{aligned}$$

We will bound each of these four terms.

Write π for a uniformiser in $\mathcal{O}_K$ at ν (so $\nu(\pi) = 1$). Write the divisor of π on $\mathscr{C}$ as $\operatorname{div}(\pi) = \sum_i a_i Y_i$, where the a_i are integers greater than 0. Then

$$\sum_i a_i d_i^+ = \iota_\nu\left(\overline{D}^+, \operatorname{div}(\pi)\right) = \deg D^+ \le g,$$

(and similarly for D^- and $E^\pm$), the second equality holding by [Lan88, II, Proposition 2.5]. From this, we see that each $d_i^+ \geq 0$ and $\sum_i d_i^+ \leq g$ (and similarly for d_i^- and $e_i^\pm$). Hence we find that

$$\begin{aligned} -g^2 m^+ &\leq -d^+ (M^+)^T (e^+)^T \leq -g^2 m^-, \\ g^2 m^- &\leq d^+ (M^+)^T (e^-)^T \leq g^2 m^+, \\ g^2 m^- &\leq d^- (M^+)^T (e^+)^T \leq g^2 m^+, \\ -g^2 m^+ &\leq -d^- (M^+)^T (e^-)^T \leq -g^2 m^-, \end{aligned}$$

from which the result follows. □

We have a chosen resolution $\mathscr{C} = \mathscr{C}_{K_\nu}$ (by blowups at smooth centres) of the singularities of the closure $\mathscr{C}_1$ of C in weighted projective space over $\mathcal{O}_{K_\nu}$. Let b_ν denote the longest length of a chain of blowups at smooth centres 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 $\mathscr{C}_1$ is regular.

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 $\overline{D}$ and $\overline{E}$ for the Zariski closures of D and E respectively on the regular model $\mathscr{C}_{K_\nu}$ over $\mathcal{O}_{K_\nu}$ (more precisely, take closures of the prime divisors in the supports of D and E, then define $\overline{D}$ and $\overline{E}$ to be appropriate linear combinations of these new prime divisors). Write ω for the maximal ideal of $\mathcal{O}_{L_\nu}$.

Proposition 12. *We have*

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

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

The proof of Proposition 12 may be found after Lemma 17. 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 13. *Let p, $q \in C(L)$ with $p \neq q$. Write*

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

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

$\overline{q}$ in $\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ of the images of p and q in $C \times_K L$. Then

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

(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 $\overline{p}$ and $\overline{q}$ do not meet on the special fibre so $I_{p,q} = 0$, and by definition we see that $\mathrm{d}(p,q) = 1$.

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 $\overline{p}$ and $\overline{q}$ meet on the special fibre; let Ω be the closed point where $\overline{p}$ and $\overline{q}$ 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 asume F is integral at ν and is irreducible. We have

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

so

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

Now given $a \in L$, we find

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

so

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

and hence

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

Moreover,

$$\log(1/\mathrm{d}(p,q)) = \min\left(-\log|x_p - x_q|, -\log|y_p - y_q|\right),$$

so we are done. □

Lemma 14. *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 $\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ 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 $\mathscr{C}_1$, we have*

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

The analogous statement on $\mathscr{C}$ 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. □

Lemma 15. *Let M be a finite length $\mathcal{O}_K$-module. Then*

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

Proof. Let $M = M_0 \subset M_1 \subset \cdots \subset M_l = 0$ 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

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

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

Lemma 16. *Let $\mathcal{I}_D$ and $\mathcal{I}_E$ denote the ideal sheaves on $\mathscr{C}_1$ corresponding to the closures of the divisors D and E respectively. We have:*

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

The analogous statement on $\mathscr{C}$ also holds.

Proof. Setting $M = \frac{\mathcal{O}_{\mathscr{C}_1}}{\mathcal{I}_D + \mathcal{I}_E}$, we have that M is a finite-length $\mathcal{O}_K$-module, and

$$M \times_{\mathcal{O}_K} \mathcal{O}_L = \frac{\mathcal{O}_{\mathscr{C}_1} \otimes_{\mathcal{O}_K} \mathcal{O}_L}{(\mathcal{I}_D + \mathcal{I}_E) \otimes_{\mathcal{O}_K} \mathcal{O}_L}.$$

We are done by Lemma 15. □

Lemma 17. *Let $\phi : \mathscr{C}_3 \to \mathscr{C}_2$ be one of the blowups involved in obtaining $\mathscr{C}$ from $\mathscr{C}_1$. Let p, $q \in C(L)$ with $p \neq q$. Then*

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

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 $\overline{p}$ does not meet $\overline{q}$ on $\mathscr{C}_2 \times \mathcal{O}_L$ then both the lengths are zero, so we are done. Otherwise, let Ω be the closed point on $\mathscr{C}_2 \times \mathcal{O}_L$ where $\overline{p}$ meets $\overline{q}$, and let α be the closed point of $\mathscr{C}_2$ such that Ω lies over α.

Let u, v be local coordinates on the (three-dimensional) ambient space to $\mathscr{C}_2$ at α, and let R denote the completion at (u, v) of the étale local ring of the ambient space to $\mathscr{C}_2$ 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 the completion 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

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

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

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

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

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

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

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

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

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

Proof of Proposition 12. To prove Proposition 12, we apply Lemmata 13, 17, 14 and 16 in that order to find that there exists

$$0 \leq \beta \leq b_\nu de \log(\#\kappa(\nu))$$

such that

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

Proof of Theorem 10. Let M^+ be the matrix from Lemma 11, let m_- denote the infimum of the entries of M^+ and m_+ their supremum. Let b_ν be the integer appearing in Proposition 12. Set

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

Then the result follows from Lemma 11 and Proposition 12. □

4. Archimedean results

4.1. 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 18. For Archimedean absolute values ν we define

$$\mathrm{d}_\nu : C(K_\nu^{\mathrm{alg}}) \times C(K_\nu^{\mathrm{alg}}) \to \mathbb{R}_{\geq 0}$$

by

$$
\begin{aligned}
&\mathrm{d}_\nu((X_p : S_p : Y_p), (X_q : S_q : Y_q))\\
&\quad = \min\Big(1, \max\left(\left|x_p - x_q\right|_\nu, \left|y_p^{g+1} - y_q^{g+1}\right|_\nu\right),\\
&\qquad\qquad \max\left(\left|s_p - s_q\right|_\nu, \left|{y'}_p^{g+1} - {y'}_q^{g+1}\right|_\nu\right)\Big),
\end{aligned}
$$

where as always $x_p = X_p/S_p$ etc.

4.2. Estimates for the Archimedean distance in a special case. In the special case where points p and q in $C(K)$ are related by the hyperelliptic involution, we can easily relate the distance between p and q to the y-coordinate of p (we will need this estimate in Section 6):

Lemma 19. *There exist computable constants $0 < \delta_1 < \delta_2$ such that for all non-Weierstrass points $p = (X : S : Y) \in C(K^{alg})$, and for all Archimedean absolute values $\nu \in M_K^\infty$ on K with their unique extensions to K^{alg}, we have*

$$\delta_1 \leq \mathrm{d}_\nu(p, p^-)/(2\min(|y|_\nu, |y'|_\nu)) \leq \delta_2,$$

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

Proof. Since M_K^∞ is finite, it is enough to show that such bounds can be found for one $\nu \in M_K^\infty$ at a time. Fix an Archimedean absolute value ν. Recall that d_ν is the metric given in Definition 18. A brief calculation (considering the two cases $|y| \leq |y'|$ and $|y| \geq |y'|$) shows that

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

Recall that C is given by

$$Y^2 = \sum_{i=0}^{2g+2} f_i X^i S^{2g+2-i},$$

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

$$\min\left(1, \frac{1}{2a}\right) \leq \frac{\mathrm{d}_\nu(p, p^-)}{(2\min(|y|_\nu, |y'|_\nu))} \leq 1. \qquad \square$$

4.3. Local Néron pairing in the Archimedean case. As in the non-Archimedean case, we will make use of the local Néron pairing to compare our metric to the local part to the Néron–Tate height. We recall in outline the construction of the pairing from [Lan88], where more details can be found.

Let ν be an Archimedean absolute value of K. Fix an algebraic closure of K_ν, and view $C_\nu = C(K_\nu^{\mathrm{alg}})$ as a compact connected Riemann surface of positive genus and let μ denote the canonical (Arakelov) (1,1)-form μ on C_ν (as in [Lan88, II, §2, page 28]). We write $G(-,-) : C_\nu \times C_\nu \to \mathbb{R}_{\geq 0}$ 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

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

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

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

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

Write $D = \sum_i a_i p_i$ and $E = \sum_j b_j q_j$ with a_i, $b_j \in \mathbb{Z}$ and p_i, $q_j \in C_\nu$ (where D and E are assumed to have degree 0 and disjoint support). Then the local Néron pairing at ν is defined by

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

4.4. Comparing the metric and the local Néron pairing. Fix an embedding of K into $\mathbb{C}$. Let gr be the logarithmic Green's function on the Riemann surface $C(\mathbb{C})$ (defined using this embedding) given in Section 4.3. We have:

Proposition 20. *There exists a constant $c \geq 0$ such that for all pairs of distinct points p, $q \in C(\mathbb{C})$, we have*

$$|\operatorname{gr}(p,q) + \log \mathrm{d}_\nu(p,q)| \leq c.$$

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 [MorB85, 4.10] for details). We need to show that the functions $\operatorname{gr}(-,-)$ and $\log \mathrm{d}_\nu(-,-)$ differ by a bounded amount. This is easy: both functions are continuous outside the diagonal Δ, and exhibit logarithmic poles along the diagonal ([MorB85, 4.11]), so their difference is bounded by a compactness argument. □

The following proposition is the Archimedean analogue of Theorem 10, except we omit the 'explicitly computable'. This makes it much easier to prove.

Proposition 21. *Given an Archimedean absolute value $\nu \in M_K^0$, there exists a constant $\mathscr{B}_\nu$ 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 3.3 that $[D,E]_\nu$ denotes the local Néron pairing of D and E at ν. Then

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

We call such a constant $\mathscr{B}_\nu$ a height-difference bound *at ν.*

Proof. This follows immediately from the definition of the Néron local pairing and Proposition 20. □

The key result is now:

Theorem 22. *There exists an algorithm which, given an Archimedean place ν, will compute a height difference bound $\mathscr{B}_\nu$ 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 were 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 [EC+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 (though note that Silverman [Sil90] essentially gives an explicit value for $\mathscr{B}_\nu$ in the case where $g = 1$). 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.

5. The first naïve height

Assumption 23. In this section we will for the first time require that $\#M_K^\infty \leq 1$ (so $\operatorname{char} K > 0$ 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 24. 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 25. If K has positive characteristic, set $\mu = 1$. Otherwise, let $\mu := \frac{1}{3}\min_{w,w'} \mathrm{d}_\nu(w, w')$ 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 at most 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 $D = \sum_i d_i$, $E = \sum_i q_i$ and $E' = \sum_i q_i'$. Given an absolute value ν of L, define

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

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

$$\mathrm{H}^{\mathrm{n}}(p) = \left(\prod_{\nu \in M_L} \frac{1}{\mathrm{d}_\nu(D-E, D^- - E')} \right)^{\frac{1}{[L:K]}}. \tag{2}$$

We define a logarithmic naïve height by $\mathrm{h}^{\mathrm{n}}(p) = \log(\mathrm{H}^{\mathrm{n}}(p))$.

Note that $\mathrm{d}_\nu(D-E, D^- - E') = 1$ for all but finitely many absolute values ν, and so the product in Equation (2) is finite.

Write $\alpha\colon \mathrm{Div}^0(C) \to \mathrm{Jac}_C(K)$ for the usual map. The crucial result which allows us to relate our naïve height to the Néron–Tate height is:

Theorem 26 (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. Then*

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

where $\hat{\mathrm{h}}$ denotes the Néron–Tate height function with respect to twice the theta-divisor.

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 a number of authors, see, e.g., [Mue13]. □

Theorem 27. *There exists a computable constant $\delta_3 \geq 0$ such that for all $p \in \mathrm{Jac}_C(K)$ we have*

$$\left| \hat{\mathrm{h}}(p) - \mathrm{h}^{n}(p) \right| \leq \delta_3.$$

Proof. For each absolute value ν of K, let $\mathscr{B}_\nu$ be the real number defined in Theorem 10 for ν non-Archimedean, and in Proposition 21 for ν Archimedean. Note that $\mathscr{B}_\nu = 0$ for ν a non-Archimedean absolute value of good reduction for C. Define

$$\delta_3 := \sum_{\nu \in M_K} \mathscr{B}_\nu.$$

Let D, D^-, E, E' be the divisors associated to p as in Definition 25. Recall from Section 3.3 that $[-,-]_\nu$ denotes the local Néron pairing at ν between two divisors of degree zero and with disjoint supports. Then by Theorem 10 and Proposition 21 we have that

$$\left| \sum_{\nu \in M_K} [D - E, D^- - E']_\nu - \mathrm{h}^{\mathrm{n}}(p) \right| \le \delta_3.$$

Now we will use Theorem 26 to compare $\sum_{\nu \in M_K} [D - E, D^- - E']_\nu$ to $\hat{\mathrm{h}}(p)$; in fact, we will show they are equal. First, a little more notation: write

$$[-,-] = \sum_{\nu \in M_K} [-,-]_\nu,$$

(the sum of the local Néron pairings). This pairing is a-priori only defined for degree-zero divisors with disjoint support, but it respects linear equivalence by [Lan88, IV, Theorem 1.1], and hence extends to a bilinear pairing on the whole of $\mathrm{Div}^0(C)$, and moreover factors via $\mathrm{Jac}_C(K)$. Write

$$\langle\langle -,- \rangle\rangle : \mathrm{Jac}_C(K) \times \mathrm{Jac}_C(K) \to \mathbb{R}$$

for the Néron–Tate height pairing (so $\langle\langle x, x \rangle\rangle = -\hat{\mathrm{h}}(x)$ for all $x \in \mathrm{Jac}_C(K)$). Theorem 26 then tells us that

$$[F, F] = -\langle\langle \alpha(F), \alpha(F) \rangle\rangle$$

for every degree-zero divisor F on C, but since a bilinear form is determined by its restriction to the diagonal we find that

$$[F, F'] = -\left\langle\left\langle \alpha(F), \alpha(F') \right\rangle\right\rangle$$

for every pair F, F' of degree-zero divisors on C.

Write $\tilde{p} = \alpha(D - E)$, and $q = \alpha(D^- - E')$. Then there exist 2-torsion points σ, $\tau \in \mathrm{Jac}_C(K)$ such that

$$\tilde{p} = p + \sigma \quad \text{and} \quad -q = p + \tau.$$

By the above discussion, we know that

$$\begin{aligned}\sum_{\nu\in M_K}[D-E,D^- - E']_\nu &= [D-E,D^- - E'] \\ &= \big\langle\big\langle \alpha(D-E),\alpha(D^- - E')\big\rangle\big\rangle \\ &= \langle\langle p+\sigma,-p-\tau\rangle\rangle \\ &= \langle\langle p,-p\rangle\rangle + \langle\langle p,-\tau\rangle\rangle + \langle\langle \sigma,-p\rangle\rangle + \langle\langle \sigma,-\tau\rangle\rangle\,.\end{aligned}$$

Now since $\langle\langle -,-\rangle\rangle$ is bilinear, it vanishes whenever either of the inputs is a torsion point, so we see that

$$\sum_{\nu\in M_K}[D-E,D^- - E']_\nu = \langle\langle p,-p\rangle\rangle = \hat{\mathrm{h}}(p)$$

as desired. □

6. Refined naïve heights

We introduce 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 28. Given $p \in \mathrm{Jac}_C(K)$, let $D = \sum_{i=1}^d p_i$ denote the corresponding divisor over some finite L/K as in Definition 25, and write $p_i = (x_{p_i}, y_{p_i})$. Then set

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

(where h is the absolute usual height on an element of a global field as specified in Section 2) and set

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

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 $\mathrm{h}^{\heartsuit}-\mathrm{h}^{\mathrm{n}}$ and on $\left|\mathrm{h}^{\heartsuit}-\mathrm{h}^{\dagger}\right|$.

Definition 29. Let L/K be a finite extension, and let $p \neq q \in C(L)$ be distinct points. Set

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

Lemma 30. *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

$$\left|\langle p, p^- \rangle_L - (g+1)\,\mathrm{h}(X/S)\right| \le \delta_4$$

Proof. For $|-|_\nu$ non-Archimedean, we have that if $|X|_\nu \le |S_\nu|$ then

$$\mathrm{d}_\nu(p, p^-) = \left|2Y/S^{g+1}\right|_\nu,$$

and if $|S|_\nu \le |X|_\nu$ then $\mathrm{d}_\nu(p,p^-) = \left|2Y/X^{g+1}\right|_\nu$. Hence for non-Archimedean ν we obtain

$$\mathrm{d}_\nu(p,p^-) = |2Y|_\nu \min(1/\,|X|_\nu^{g+1}, 1/\,|S|_\nu^{g+1}).$$

By Lemma 19, for Archimedean ν we have computable $0 < \delta_1 < \delta_2$ such that

$$\delta_1 < \mathrm{d}_\nu(p,p^-)/\min(\left|2Y/X^{g+1}\right|_\nu, \left|2Y/S^{g+1}\right|_\nu) < \delta_2.$$

Hence

$$\prod_{\nu \in M_L^\infty} 1/\delta_2 \le \frac{\prod_{\nu\in M_L} 1/\mathrm{d}_\nu(p,p^-)}{\prod_{\nu\in M_L} |2Y|_\nu^{-1} \prod_{\nu\in M_L} \max(|X|_\nu, |S|_\nu)^{g+1}} \le \prod_{\nu\in M_L^\infty} 1/\delta_1.$$

Now $\prod_{\nu\in M_L^\infty} {\delta_1}^{-1/[L:K]}$ is bounded uniformly in L, and similarly for δ_2. Finally, note

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

Recall that in Definition 7 we defined a constant λ_ν for each non-Archimedean absolute value ν of K, and that these take the value 1 for all but finitely many ν.

Definition 31. We set

$$\delta_5 = (2g + 3/2) \sum_{\nu\in M_K^0} \log \lambda_\nu.$$

Lemma 32. *Let L/K be a finite extension, and let p, $w \in C(L)$ with $p \neq w$ be such that $s_p \neq 0$ and w is a Weierstrass point with $s_w \neq 0$. Then*

$$-\sum_{\nu\in M_L^0} \log \mathrm{d}_\nu(p,w) \le [L:K]\left(\frac{1}{2}\mathrm{h}(x_p - x_w) + \delta_5\right).$$

Proof. The right hand side naturally decomposes as

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

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

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

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

$$-\log(\mathrm{d}_\nu(p,w)) \leq \frac{1}{2} \log^+ |x_p - x_w|_\nu^{-1} + (2g + 3/2) \log \lambda_{\nu'}.$$

This is exactly the statement of Lemma 8. □

Lemma 33. *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 $\mathrm{H}(x_1 + x_2) \leq 2^{\# \mathrm{M}_K^\infty} \mathrm{H}(x_1) \mathrm{H}(x_2)$.*

Proof. Omitted. □

Lemma 34. *There exists a computable constant δ_6 with the following property:*

Let L/K be a finite extension, and let p, $w \in C(L)$ such that $s_p \neq 0$ and w is a Weierstrass point with $s_w \neq 0$. Suppose also that $\mathrm{d}_\nu(p,w) \geq \mu$ for all Archimedean ν (where μ is the constant from Definition 25). Then

$$\langle p, w \rangle_L \leq \frac{1}{2} \mathrm{h}(x_p) + \delta_6.$$

Proof. From Lemma 32 we see that

$$\langle p, w \rangle_L \leq \frac{1}{2} \mathrm{h}(x_p - x_w) + \delta_5 - \log(\mu).$$

Now by Lemma 33, we have

$$\mathrm{h}(x_p - x_w) \leq \mathrm{h}(x_p) + \mathrm{h}(x_w) + \# M_K^\infty \log(2).$$

We define

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

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

$$\langle p, w \rangle_L \leq \frac{1}{2} \mathrm{h}(x_p) + \delta_6(w).$$

Finally, there are only finitely many Weierstrass points, so setting $\delta_6 = \max_w \delta_6(w)$, we are done. □

Lemma 35. *There exists a computable constant δ_7 such that the following holds.*

Given $p \in \mathrm{Jac}_C(K)$, let D, E and E' denote the divisors given in Definition 25. Let L/K be the minimal finite extension such that D, E and E' are all pointwise rational over L. We write

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

Then

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

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

Proof. Recall that

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

We easily bound $\sum_{i,j=1}^{d} \left\langle q_i, q_j' \right\rangle_L$, since the q_i and q_i' are distinct Weierstrass points.

It remains to find a lower bound on the terms $\left\langle p_i, p_j^- \right\rangle_L$ for $i \neq j$. Note that d_ν is bounded above by 1 for all ν, hence $\left\langle p_i, p_j^- \right\rangle_L \geq 0$. □

Lemma 36. *There exists a computable constant δ_8 such that in the setup of Lemma 35 we have*

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

Proof. In Lemma 35 we showed

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

In Lemma 30 we showed (using that the p_i are never Weierstrass points) that for some computable δ_4 we have

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

In Lemma 34 we showed that

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

and similarly for q_j'.

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

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

from which the result follows. □

Theorem 37. *There exists a computable constant δ_9 such that for all $p \in A(K)$ we have*

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

Proof. Set $\delta_9 = \delta_3 + \delta_8$. The result follows from Theorem 27 and Lemma 36. □

Lemma 38. *Fix a finite extension L/K. Given $a_1, \ldots, a_n \in L$, set*

$$\psi_n = \prod_{i=1}^{n}(t - a_i) \in L[t].$$

If $\operatorname{char} K > 0$ then $\mathrm{h}(\psi_n) = \sum_{i=1}^{n} \mathrm{h}(a_i)$, otherwise

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

We summarise this by writing

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

Proof. [Sil09, Theorem VIII.5.9] □

Corollary 39. *For all $p \in A(K)$ we have*

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

Definition 40. Given a real number B, we define

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

and

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

The main result of this paper is the following.

Corollary 41. *Let $B \in \mathbb{R}$. Let $B' = B + \delta_9 + (g \log 2)\delta_{\operatorname{char} K}$. Then for all real numbers B we have*

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

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 (see [Mum84, III, Proposition 1.2]); 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 that $\deg a$, which is widely implemented. □

Remark 42. How hard is it to check whether such a polynomial $f - a^2$ has a factor of degree less that $\deg a$? Note that $\deg f - a^2 = 2g + 1$, and in general $\deg a = g$. Based on this, it seems reasonable that the difficulty of testing for such a factor will be somewhere in between the difficulty of factoring a polynomial of degree $2g + 1$ and that of factoring a polynomial of degree $2g - 1$ (since in the latter case, irreducibility is equivalent to not having a factor of degree at most $g - 1$).

In practice, the integer g will usually be very small (genera 3 and 4 are the obvious cases to treat), but we will have a huge number of polynomials a to run through. Because of this, rather than looking at the time taken to check for factors of degree $< g$ in one polynomial, it is more useful to look at how efficiently we can check this for large families of a. One method to rapidly exclude many possible values of a from the search region is by reduction modulo small primes, followed by the 'Chinese remainder theorem'. The proportion of polynomials of degree $2g + 1$ over a finite field $\mathbb{F}_p$ which are irreducible is approximately

$$\frac{1}{2g+1},$$

and the proportion without a factor of degree less than g is approximately

$$\frac{1}{2g+1} + \frac{1}{g^2} + \frac{1}{g^2+g}.$$

As such, at least from this point of view, we cannot expect very substantial computation savings from the fact that we need only exclude factors of degree less than g (instead of computing the whole factorisation).

7. 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 $|-|_t$ 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 43. 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 with affine equation

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

Proposition 44. *For all points $q \in \operatorname{Jac}_C(K)$, we have*

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

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 $\alpha_0, \cdots, \alpha_{2g}$ 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 $\mathrm{h}(t) = \log p$ and for all n that $\mathrm{h}(\alpha_n) = (\log p)/(2g+1)$. 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 $w_i \neq w_j$, we have

$$\langle w_i, w_j \rangle_L = \frac{2\log p}{2g+1},$$

independent of the field L.

Since K has no Archimedean absolute values we immediately see that we may take $\delta_1 = \delta_2 = \delta_4 = 0$. 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

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

and since

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

(the sum is over distinct points w, w' 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. □

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 45. *Let $p = 3$ and $g = 2$, and let C be as in Definition 43. Then for all points $q \in \mathrm{Jac}_C(K)$, we have*

$$\hat{\mathrm{h}}(q) + 86 \log 3 \geq \mathrm{h}^{\heartsuit}(q) = \mathrm{h}^{\dagger}(q).$$

Let $p = 5$ and $g = 4$, and let C be as in Definition 43. Then for all points $q \in \mathrm{Jac}_C(K)$, we have

$$\hat{\mathrm{h}}(q) + 417 \log 5 \geq \mathrm{h}^{\heartsuit}(q) = \mathrm{h}^{\dagger}(q).$$

Let $p = 101$ and $g = 11$, and let C be as in Definition 43. Then for all points $q \in \mathrm{Jac}_C(K)$, we have

$$\hat{\mathrm{h}}(q) + 5790 \log 101 \geq \mathrm{h}^{\heartsuit}(q) = \mathrm{h}^{\dagger}(q).$$

Proof. We give details for the genus 11 example, the others are similar. `MAGMA` code for the computations for all three curves is available at `http://nyjm.albany.edu/j/2014/20-45-code.zip`.

Let u, t be coordinates on $B_K = \mathbb{P}^1_{\mathbb{F}_{101}}$ with $u = 1/t$. Applying Proposition 44, it is enough to compute the constants $\mathscr{B}_\nu$ from Theorem 10. 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 $\mathscr{B}_\nu = 0$ 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 1 blow up at a closed point and g blowups along smooth curves, for a total of $g + 1 = 12$ consecutive blowups at smooth centres. The fibre over u is now irreducible, and the whole fibre is in the centre of the last blowup.

Now the equation is in a form where we can plug it into `MAGMA`, which yields a regular model after 68 blowups at smooth centres; the longest chain of consecutive blowups used by `MAGMA` has length 7 (I am grateful to the anonymous referee for the code to compute this). Hence $19 = 7 + 12$ is the longest chain of consecutive blowups at smooth centres used (this number becomes 12 in the genus 4 case and 10 in genus 2). 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 $4.102\cdots$ and minimum entry $-8.076\cdots$. As a result, we find that

$$\begin{aligned}\mathscr{B}_{(u)} &= (2g^2(4.102\cdots + 8.076\cdots) + 19g^2) \log 101 \\ &= 5246.07\cdots \log 101.\end{aligned}$$

Proposition 44 yields a bound of

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

from which the result follows. □

Remark 46. The computations for Theorem 45 took under 60 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] Anderson, Greg W. Edited 4Θ-embeddings of Jacobians. *Michigan Math J.* **52** (2004), no. 2, 309–339. MR2069803 (2005d:14044), Zbl 1060.14043, arXiv:math/0209413, doi: 10.1307/mmj/1091112078.

[BoCP97] Bosma, Wieb; Cannon, John; Playoust, Catherine. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265. MR1484478, Zbl 0898.68039, doi: 10.1006/jsco.1996.0125.

[Bru13] Bruin, Peter. Bornes optimales pour la différence entre la hauteur de Weil et la hauteur de Néron–Tate sur les courbes elliptiques sur $\overline{\mathbb{Q}}$. *Acta Arith.* **160** (2013), no. 4, 385–397. MR3119786, Zbl 1287.11083, arXiv:1212.6515, doi: 10.4064/aa160-4-5.

[BMS$^+$08] Bugeaud, Yann; Mignotte, Maurice; Siksek, Samir; Stoll, Michael; Tengely, Szabolcs. Integral points on hyperelliptic curves. *Algebra and Number Theory* **2** (2008), no. 8, 859–885. MR2457355 (2010b:11066), Zbl 1168.11026, arXiv:0801.4459, doi: 10.2140/ant.2008.2.859.

[CGO84] Cossart, Vincent; Giraud, Jean; Orbanz, Ulrich. Resolution of surface singularities. Lecture Notes in Mathematics, 1101. *Springer-Verlag, Berlin*, 1984. vi+132 pp. ISBN: 3-540-13904-4. MR0775681 (87e:14032), Zbl 0553.14003.

[CPS06] Cremona, J. E.; Prickett, M.; Siksek, Samir. Height difference bounds for elliptic curves over number fields. *J. Number Theory* **116** (2006), no. 1, 42–68. MR2197860 (2006k:11121), Zbl 1162.11032, doi: 10.1016/j.jnt.2005.03.001.

[DaP02] David, Sinnou; Philippon, Patrice. Minorations des hauteurs normalisées des sous-variétés de variétés abeliennes. II. *Comment. Math. Helv.* **77** (2002), no. 4, 639–700. MR1949109 (2004a:11055), Zbl 1030.11026, doi: 10.1007/PL00012437.

[Dem68] Dem′janenko, V. A. An estimate of the remainder term in Tate's formula. *Mat. Zametki* **3** (1968), 271–278. MR0227166, (37 #2751) Zbl 0161.40601, doi: 10.1007/BF01387329.

[EC$^+$11] Edixhoven, Bas; Couveignes, Jean–Marc; et. al.; Dirs. Computational aspects of modular forms and Galois representations. How one can compute in polynomial time the value of Ramanujan's tau at a prime. Annals of Mathematics Studies, 176. *Princeton University Press, Princeton, NJ*, 2011. xii+425 pp. ISBN: 978-0-691-14202-9. MR2849700, Zbl 1216.11004, arXiv:math/0605244.

[Fal84] Faltings, Gerd. Calculus on arithmetic surfaces. *Ann. of Math.* (2) **119** (1984), no. 2, 387–424. MR0740897 (86e:14009), Zbl 0559.14005.

[Fly93] Flynn, E.V. The group law on the Jacobian of a curve of genus 2. *J. Reine Angew. Math.* **439** (1993), 45–69. MR1219694 (95b:14022), Zbl 0765.14014, doi: 10.1515/crll.1993.439.45.

[FS97] Flynn, E.V.; Smart, N.P. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.* **79** (1997), no. 4, 333–352. MR1450916 (98f:11066), Zbl 0895.11026.

[Hol12a] Holmes, David. Computing Néron–Tate heights of points on hyperelliptic Jacobians. *J. Number Theory* **132** (2012), no. 6, 1295 – 1305. MR2899805, Zbl 1239.14019, arXiv:1004.4503, doi: 10.1016/j.jnt.2012.01.002.

[Hol12b] Holmes, David. Néron-Tate heights on the Jacobians of high-genus hyperelliptic curves. PhD thesis, University of Warwick, 2012.

[Hol12c] Holmes, David. An Arakelov-theoretic approach to naïve heights on hyperelliptic Jacobians. Preprint, 2012. arXiv:1207.5948.

[Hri83] Hriljac, Paul Marion. The Néron–Tate height and intersection theory on arithmetic surfaces. PhD Thesis, Massachusetts Institute of Technology. 1983. MR2941042.

[Lan88] Lang, Serge. Introduction to Arakelov theory. *Springer-Verlag, New York*, 1988. x+187 pp. ISBN: 0-387-96793-1. MR0969124 (89m:11059), Zbl 0667.14001, doi: 10.1007/978-1-4612-1031-3.

[Lip78] Lipman, Joseph. Desingularization of two-dimensional schemes. *Ann. Math.* (2) **107** (1978), no. 1, 151–207. MR0491722 (58 #10924), Zbl 0349.14004.

[Liu02] Liu, Qing. Algebraic geometry and arithmetic curves. Oxford Graduate Texts in Mathematics, 6. *Oxford University Press, Oxford*, 2002. xvi+576 pp. ISBN: 0-19-850284-2. MR1917232 (2003g:14001), Zbl 0996.14005.

[Man71] Manin, Ju. I. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk* **26** (1971), no. 6(162), 7–71. MR0401653 (53 #5480), Zbl 0266.14012, doi: 10.1070/RM1971v026n06ABEH001272.

[Mat80] Matsumura, Hideyuki. Commutative algebra. Second edition. Mathematics Lecture Note Series, 56. *Benjamin/Cummings Publishing Co., Inc., Reading, Mass.*, 1980. xv+313 pp. ISBN: 0-8053-7026-9. MR0575344 (82i:13003), Zbl 0441.13001.

[Moo20] Moore, E.H. On the reciprocal of the general algebraic matrix. The fourteenth western meeting of the American Mathematical Society. *Bull. Amer. Math. Soc.* **26** (1920), no. 9, 385–396. MR1560324.

[MorB85] Moret–Bailly, Laurent. Métriques permises. *Astérisque* **127** (1985), 29–87. MR0801918, Zbl 1182.11028.

[Mue10] Müller, Jan Steffen. Computing canonical heights on Jacobians. PhD thesis, Universität Bayreuth, 2010. `http://www.mathe2.uni-bayreuth.de/stoll/papers/PhdThesisMueller.pdf`.

[Mue13] Müller, Jan Steffen. Computing canonical heights using arithmetic intersection theory. *Math. Comp.* **83** (2013), no. 285, 311-336. MR3120591, Zbl 06227557, arXiv:1105.1719, doi: 10.1090/S0025-5718-2013-02719-6.

[Mum66] Mumford, D. On the equations defining abelian varieties. I. *Invent. Math.* **1** (1966), 287–354. MR0204427, (34 #4269) Zbl 0219.14024, doi: 10.1007/BF01389737.

[Mum84] Mumford, D. Tata lectures on theta. II. Jacobian theta functions and differential equations. Progress in Mathematics, 43. *Birkhäuser Boston, Inc., Boston, MA*, 1984. xiv+272 pp. ISBN: 0-8176-3110-0. MR0742776 (86b:14017), Zbl 1112.14003, doi: 10.1007/978-0-8176-4578-6.

[Nér65] Néron, A. Quasi-fonctions et hauteurs sur les variétés abéliennes. *Ann. of Math.* **82** (1965), 249–331. MR0179173 (31 #3424), Zbl 0163.15205.

[Pen55] Penrose, R. A generalized inverse for matrices. *Proc. Cambridge Philos. Soc.* **51** (1955), 406–413. MR0069793(16,1082a), Zbl 0065.24603, doi: 10.1017/S0305004100030401.

[Rei72] Reid, M. The complete intersection of two or more quadrics. PhD thesis, University of Cambridge, 1972.

[Sik95] Siksek, Samir. Infinite descent on elliptic curves. *Rocky Mountain J. Math.* **25** (1995), no. 4, 1501–1538. MR1371352(97g:11053), Zbl 0852.11028, doi: 10.1216/rmjm/1181072159.

[Sil90] Silverman, Joseph H. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.* **55** (1990), no. 192, 723–743. MR1035944 (91d:11063), Zbl 0729.14026, doi: 10.1090/S0025-5718-1990-1035944-5.

[Sil09] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094 (2010i:11005), Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6.

[Sto99] Stoll, Michael. On the height constant for curves of genus two. *Acta Arith* **90** (1999), no. 2, 183–201. MR1709054 (2000h:11069), Zbl 0932.11043.

[Sto02] Stoll, Michael. On the height constant for curves of genus two. II. *Acta Arith* **104** (2002), no. 2, 165–182. MR1914251 (2003f:11093), Zbl 1139.11318, doi: 10.4064/aa104-2-6.

[Sto12] Stoll, Michael. Explicit Kummer varieties for hyperelliptic curves of genus 3. Slides from a talk, 2012. http://www.mathe2.uni-bayreuth.de/stoll/talks/Luminy2012.pdf.

[Uch08] Uchida, Yukihiro. The difference between the ordinary height and the canonical height on elliptic curves. *J. Number Theory* **128** (2008), no. 2, 263-279. MR2380321 (2009f:11078), Zbl 1145.11050, doi: 10.1016/j.jnt.2007.10.002.

[VW98] van Wamelen, Paul. Equations for the Jacobian of a hyperelliptic curve. *Trans. Amer. Math. Soc.* **350** (1998), no. 8, 3083–3106. MR1432144 (98k:14038), Zbl 0901.14016, doi: 10.1090/S0002-9947-98-02056-X.

[Zim76] Zimmer, Horst Günter. On the difference of the Weil height and the Néron–Tate height. *Math. Z.* **147** (1976), no. 1, 35–51. MR0419455 (54 #7476), Zbl 0303.14003.

[ZM72] Zarhin, Ju. G.; Manin, Ju. I. Height on families of abelian varieties. *Mat. Sb. (N.S.)* **89(131)** (1972), 171–181, 349. MR0332801 (48 #11127), doi: 10.1070/SM1972v018n02ABEH001749.

Mathematisch Instituut Leiden, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands
holmesdst@math.leidenuniv.nl

This paper is available via http://nyjm.albany.edu/j/2014/20-45.html.