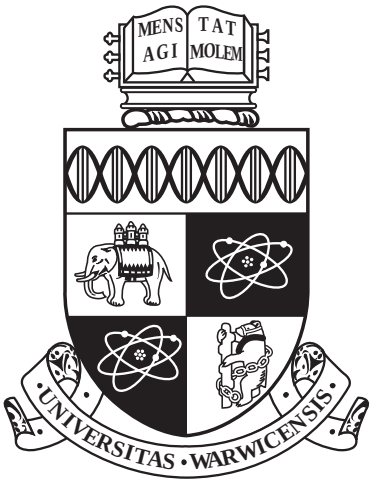


Néron-Tate heights on the Jacobians of high-genus hyperelliptic curves

by

David Holmes

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

April 2012

THE UNIVERSITY OF
WARWICK

Contents

Acknowledgments

I would like to thank my supervisor, Samir Siksek, for a great deal of help and encouragement during my time at Warwick. I am also grateful to numerous other mathematicians for valuable comments and interesting discussions; I would particularly like to thank Johan Bosman, Martin Bright, John Cremona, Steffen Müller, Marco Streng, Damiano Testa and Shengtian Zhou. I am grateful to the EPSRC for funding this research.

Thank you to my parents and to Annie for their care and suppport. Thank you to all those who have made it a great few years, in particular Anna and Dave, Barinder, Damon, Matt R., Sarah and most of all Martha.

Declarations

This thesis is entirely the author's own work, and none of it has been written in collaboration. Chapters 2, 3 and 4 contain background material which is known to the experts, at least in principle. Similar results to those in Chapter 5 were obtained independently and at the same time by S. Müller [Mue11]. A paper based on Chapter 5 has appeared in the Journal of Number Theory [Hol12]

Abstract

We use Arakelov intersection theory to study heights on the Jacobians of high-genus hyperelliptic curves. The main results in this thesis are:

1) new algorithms for computing Néron-Tate heights of points on hyperelliptic Jacobians of arbitrary dimension, together with worked examples in genera up to 9 (pre-existing methods are restricted to genus at most 2 or 3).

2) a new definition of a naïve height of a point on a hyperelliptic Jacobian of arbitrary dimension, which does not make use of a projective embedding of the Jacobian or a quotient thereof.

3) an explicit bound on the difference between the Néron-Tate height and this new naïve height.

4) a new algorithm to compute sets of points of Néron-Tate height up to a given bound on a hyperelliptic Jacobian of arbitrary dimension, again without making use of a projective embedding of the Jacobian or a quotient thereof.

Chapter 1

Introduction

1.1 Statement of the problems

Given a curve C of genus g over a number field k, let A be its Jacobian. The group $A(k)$ of rational points on A is a finitely generated abelian group. A Néron-Tate height pairing is a special non-degenerate quadratic form $\hat{\mathrm{h}}$ on $A(k)/\operatorname{Torsion}$ (see Section 4.5 for a definition), with the property that the set of k-points on A of height less than a given bound is finite. The main computational problems in the theory of these heights are to give effective algorithms for the following problems:

Problem 1. *Given a point p in $A(k)$, compute $\hat{\mathrm{h}}(p)$.*

Problem 2. *Given a bound $B > 0$, compute the finite set*

$$\{p \in A(k) | \hat{\mathrm{h}}(p) \leq B\}. \tag{1.1}$$

1.2 Previous work on these problems

The first definition of the Néron-Tate height was given by Néron in 1965 [Nér65]. The above problems have been studied since the work of Tate in the 1960s (unpublished), who gave a different definition from Néron which is sometimes easier to work with. Using this definition, Tate (unpublished), Dem'janenko [Dem68], Zimmer [Zim76], Silverman [Sil90] and more recently Cremona, Prickett and Siksek [CPS06] have given increasingly refined algorithms in the case of elliptic curves. Meanwhile, in the direction of increasing genus, Flynn and Smart [FS97] gave an algorithm for the above problems in genus 2 building on work of Flynn [Fly93], which was later modified by Stoll ([Sto99] and [Sto02]). Recently, Stoll has announced an extension to genus 3 [Sto12]. All of the work so far cited has been concerned with giving

practical algorithms and obtaining computational results. In contrast, Zarhin and Manin [ZM72] gave an entirely theoretical approach to these problems on arbitrary abelian varieties, using the projective embeddings of Mumford [Mum66].

The technique used by all these authors was to work with an explicit 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 description. However, such projective embeddings become extremely hard to compute with as the genus grows - for example, the Kummer variety is $\mathbb{P}^1$ in genus 1, is a quartic hypersurface in $\mathbb{P}^3$ for genus 2 and in genus 3 is given by a system of one quadric and 34 quartics in $\mathbb{P}^7$ [Mue10]. As such, it appears that to extend to much higher genus using these techniques will be impractical.

This thesis builds on the original results of Néron, combined with work of Arakelov [Ara74], Faltings [Fal84] and Hriljac [Hri77], who interpret $\hat{\mathrm{h}}$ as an arithmetic intersection pairing on the Néron model of the Jacobian, which can be pulled back to an arithmetic intersection pairing on a minimal regular model of C over $\mathcal{O}_k$, the ring of integers of the number field k. This enables us to obtain results which are not dependant on projective embeddings of Jacobians, but which only require equations for the curve. In particular, our new algorithms are far more suited to curves of high genus, as demonstrated by the worked example in genus 9 given in Chapter 5, far beyond what was previously possible.

For the first problem, we show how to effectively compute intersection pairings on arithmetic surfaces by computing norms down to the base scheme $\mathrm{Spec}(\mathcal{O}_k)$, and we compute the Archimedean part of the intersection pairing by expressing the Green's functions of Arakelov in terms of theta functions.

For the second problem we define a naïve height of a point on the Jacobian as an infinite product of distances between a corresponding divisor on the curve and a perturbation of that divisor. A lot of work is needed to give explicit bounds on the difference between this height and the Néron-Tate height. We then give an algorithm to find all divisors on C which correspond to points of bounded naïve height under this new definition. The bounds on the difference between the naïve and Néron-Tate heights then complete the algorithm for Problem 2.

1.3 Applications

Some applications of a solution to the problems above are as follows:

Verifying cases of the conjecture of Birch and Swinnerton-Dyer. Generalisations of the Birch and Swinnerton-Dyer Conjecture predict precisely the

leading Taylor coefficient of the L-series around $s = 1$ of the Jacobian in terms of a number of invariants which include the regulator of the Mordell-Weil group. The conjecture has been numerically verified up to high precision on large families of elliptic curves, and also on a few special examples of Jacobians of genus 2 curves, but not as yet for any curves of higher genus. The results in this thesis remove the last major obstacle to numerically testing the conjecture for modular hyperelliptic curves.

Computing a basis of $A(k)$. The process of descent can be used to determine a basis of a finite index subgroup of $A(k)$ (in practice this usually works, and it always will if we assume the Tate-Shafarevich group to be finite). One is then left with the problem of determining a basis of $A(k)$ from this. To do so, first compute the determinant of the height pairing on the given basis of the finite index subgroup (Problem 1). The geometry of numbers can then be used together with Problem 2 to compute a finite subset of $A(k)$ which contains a basis of $J(k)/\text{Torsion}$.

Computing integral points on hyperelliptic curves. Let $\mathcal{O}_k$ denote the ring of integers of k. Given an affine curve $\mathcal{C}$ over $\mathcal{O}_k$, one can then ask for the set of integral points $\mathcal{C}(\mathcal{O}_k)$. This is of course canonically contained in $\mathcal{C}(k)$, but need not be equal to it. Further, it is often possible to compute $\mathcal{C}(\mathcal{O}_k)$ when it is impossible to compute $\mathcal{C}(k)$. The most effective method to do this in the hyperelliptic case is described in the recent paper [BMS$^+$08]. It combines the latest improvements in the theory of linear forms in logarithms (originally due to Baker [Bak69]) with a variant of the Mordell-Weil sieve, to give a practical method to determine the integral points on a standard affine patch of a hyperelliptic curve. However, in order to apply this, one first needs to know $A(k)$, and then to have effective solutions to Problems 1 and 2 above.

Manin's algorithm.

In [Man71], Manin outlines an algorithm which, assuming the validity of the conjecture of Birch and Swinnerton-Dyer, allows one to effectively determine the rank of $A(k)$. However, to make this algorithm effective, one again needs to resolve Problems 1 and 2 above.

1.4 How we will proceed

Chapters 2, 3 and 4 are background material. Chapter 2 contains discussions in general terms of certain specialised scheme-theoretic notions we will need, as well as the notions of heights and hyperelliptic curves.

Chapter 3 contains basic definitions and statement of foundational results

in Arakelov theory. Most of the chapter is devoted to the analytic theory, as we assume the scheme theory to be well-known. We discuss how to obtain heights from Arakelov theory and compare various heights that arise in this way.

Chapter 4 describes the construction of the Néron-Tate height on a Jacobian via Arakelov theory, together with the relation to the intersection pairing on the curve. We have attempted to present a path through this theory in a reasonably uniform way (rather than the ad-hoc constructions which characterised the subject in its infancy), but we have also remained within the realm of constructions which can reasonably be made explicit; hence we have viewed intersection theory as the action of the first Chern class on cycles, rather than taking a K-theoretic viewpoint. The main references for this material are the original 1965 paper [Nér65] of André Néron and the unpublished PhD thesis of Paul Hriljac [Hri77]. Néron's terminology is somewhat archaic, predating the development of scheme theory and, later, Arakelov theory; as such, a little effort is needed to relate his work to modern approaches. For the connection to the intersection pairing on the curve, the paper [Fal84] of Faltings is also useful.

The first significant new results appear in the fifth chapter, which is essentially devoted to the effective computation of arithmetic intersection pairings on hyperelliptic curves, utilising a formula of Faltings and Hriljac to relate it to the Néron-Tate height. The chapter concludes with worked examples in genera up to 9.

In Chapter 6 we begin by defining an infinite family of metrics on the curve C, one for each place of k. Extending these metrics from points to divisors on the curve, we define a height by taking the reciprocal of the product over these metrics of the distance from a divisor to a perturbation of itself. We then give effective bounds on the difference between this height and the Néron-Tate height.

In the final chapter, we relate this new naïve height to a progression of increasingly simple and more easily computable heights, until we end up with one for which Problem 2 is easily solved. Bounds on the differences between these successive heights then yield a solution to Problem 2 for the Néron-Tate height.

Chapter 2

Preliminaries

In this chapter we will give basic definitions, firstly on heights, then on cycles on relative schemes and hyperelliptic curves. This is included partly to fix notation which we will use throughout the rest of this thesis.

2.1 Heights

What is a height? A wide array of 'styles' of heights can be found in the literature, from the very rigid (such as the Néron-Tate height on an abelian variety [Nér65]) to the freely-deformable heights that arise from Arakelov theory [Lan88]. When one moves the discussion to local heights, this diversity expands - Silverman [Sil94] requires them to transform in a prescribed way under duplication (resulting in a very rigid definition), whereas we view a collection of local heights as a set of functions whose definition is local in the vague sense that they are computed from local data, and which sum to the global height we want. The heights which interest us in this thesis are those which can be combined with descent arguments to give information about rational points. This leads us to the following 'inclusive' definition:

Definition 3. *Given a global field k and an integral finite-type scheme X/k, a height on X/k is an element of $Hom_{sets}(X(k^{sep}), \mathbb{R})$. We say such a height* h *is non-degenerate if for all integers $d > 0$ and bounds $B \in \mathbb{R}$, we have*

$$\#\{p \in X(l) | l/k \text{ finite separable extension such that } [l:k] \leq d \text{ and } \mathrm{h}(p) \leq B\} < \infty. \tag{2.1}$$

Sometimes it is more convenient to consider a height as a function defined only on k-rational points, especially when one is attempting to obtain uniform

bounds on the difference between two heights. This is the approach we will adopt in Section 6.6, since it simplifies the exposition and is adequet for our applications.

How can we go about constructing such a height? We begin with a generalisation of the classical height on projective space.

Definition 4. *Let X/k be as above, and $\mathcal{L}$ a base-point-free line bundle on X, and $s = \{s_0, \ldots, s_n\}$ a basis of $\mathrm{H}^0(X, \mathcal{L})$. We define the height on X associated to $\mathcal{L}$ and s to be*

$$\begin{aligned} \mathrm{h}_{\mathcal{L},s} : X(k^{sep}) &\to \mathbb{R} \\ p &\mapsto \log \left(\prod_{\nu \in M_k} \max_i \left| N_{l/k}\left(s_i(p)\right) \right|_\nu^{\frac{1}{[l:k]}} \right) \end{aligned} \tag{2.2}$$

where M_k is a proper set of absolute values for k, and l/k is a finite separable extension depending on p such that all $s_i(p) \in l$.

For example, if

$$\begin{aligned} X &= \mathbb{P}_k^n = \mathrm{Proj}\left(k\left[x_0, \ldots, x_n\right]\right) \\ \mathcal{L} &= \mathcal{O}_X(1) \\ s &= \{x_0, \ldots, x_n\} \end{aligned} \tag{2.3}$$

then we recover the usual logarithmic height.

A classical fact due to Northcott is:

Theorem 5. *[Lan83, p59] The height defined above on $\mathbb{P}_k^n$ is non-degenerate.*

We also need the following well-known result:

Theorem 6. *Let X be integral, projective and of finite type over a global field k and $\mathcal{L}$ be base-point-free. Consider the canonical map*

$$\varphi : X \to \mathrm{Proj}\left(\mathrm{H}^0\left(X, \mathcal{L}\right)\right)^\vee. \tag{2.4}$$

1) If φ is finite then $\mathcal{L}$ is ample.

2) If moreover we assume X is regular, then the converse holds.

Proof. First, suppose that φ is finite. Then since $\mathcal{L} = \varphi^* \mathcal{O}(1)$ and $\mathcal{O}(1)$ is ample, Serre's criterion for ampleness [Gro61] shows that $\mathcal{L}$ is ample.

Conversely, if $\mathcal{L}$ is ample then (since X is regular) the Nakai-Moishezon criterion ([Nak63] and [Moĭ64]) shows that $\mathcal{L}|_C$ is positive and hence ample for

every curve C on X. As such, no curve can be contracted by φ, so φ is quasi-finite. Since X is projective, φ is in fact finite. $\square$

We thus obtain the useful criterion:

Corollary 7. *Let X be integral and of finite type over a global field k, and $\mathcal{L}$ on X be base-point-free and ample. Then for any (and hence all) choices s of bases of sections of $\mathrm{H}^0(X, \mathcal{L})$, the height $\mathrm{h}_{\mathcal{L},s}$ is non-degenerate.*

For a fixed X/k, how does $\mathrm{h}_{\mathcal{L},s}$ vary as we vary $\mathcal{L}$ and s? To answer this, we first define two equivalence relations on heights.

Definition 8. *Given two heights h_1 and h_2 in $Hom_{sets}(X(k^{sep}), \mathbb{R})$, we say*

1) $\mathrm{h}_1 \sim_1 \mathrm{h}_2$ if there exists a constant $c > 0$ such that for all $p \in X(k^{sep})$, we have $|\mathrm{h}_1(p) - \mathrm{h}_2(p)| \leq c$.

2) $\mathrm{h}_1 \sim_2 \mathrm{h}_2$ if there exist constants $c > 0$ and $\epsilon > 0$ such that for all $p \in X(k^{sep})$, we have $|\mathrm{h}_1(p) - \mathrm{h}_2(p)| \leq \epsilon \cdot \mathrm{h}_1(p) + c$ or $|\mathrm{h}_1(p) - \mathrm{h}_2(p)| \leq \epsilon \cdot \mathrm{h}_2(p) + c$.

We then have the following:

Proposition 9. *[Lan83, Chapter 4] Let X be integral and of finite type over a global field k, and $\mathcal{L}$, $\mathcal{L}_1$, $\mathcal{L}_2$ be ample base-point-free invertible sheaves on X. The following hold:*

1) Let t_1, t_2 be bases of $\mathrm{H}^0(X, \mathcal{L})$. Then $\mathrm{h}_{\mathcal{L},t_1} \sim_1 \mathrm{h}_{\mathcal{L},t_2}$.

2) Say $\mathcal{L}_1 \cong \mathcal{L}_2$, and let s^i be a basis of $\mathrm{H}^0(X, \mathcal{L}_i)$. Then $\mathrm{h}_{\mathcal{L}_1,s^1} \sim_1 \mathrm{h}_{\mathcal{L}_2,s^2}$.

3) Say $\mathcal{L}_1 \sim_{alg} \mathcal{L}_2$, and let s^i be a basis of $\mathrm{H}^0(X, \mathcal{L}_i)$. Then $\mathrm{h}_{\mathcal{L}_1,s^1} \sim_2 \mathrm{h}_{\mathcal{L}_2,s^2}$.

4) Choose any bases of sections of $\mathrm{H}^0(X, \mathcal{L}_i)$ and $\mathrm{H}^0(X, \mathcal{L}_1 \otimes \mathcal{L}_2)$. Then $\mathrm{h}_{\mathcal{L}_1 \otimes \mathcal{L}_2,s} \sim_1 \mathrm{h}_{\mathcal{L}_1,s^1} + \mathrm{h}_{\mathcal{L}_2,s^2}$.

This allows us to construct a map of groups

$$\mathcal{H}_1 : \mathrm{Pic}(X) \to \frac{\mathrm{Hom}_{\mathrm{sets}}(X(k^{\mathrm{sep}}), \mathbb{R})}{\sim_1} \tag{2.5}$$

as follows: given $[\mathcal{L}] \in \mathrm{Pic}(X)$, choose an invertible sheaf $\mathcal{F}$ on X such that both $\mathcal{F}$ and $\mathcal{F} \otimes \mathcal{L}$ are base-point-free and ample. Pick bases s and t of global sections of $\mathcal{F}$ and $\mathcal{F} \otimes \mathcal{L}$ respectively, and set $\mathcal{H}_1([\mathcal{L}]) = \mathrm{h}_{\mathcal{F} \otimes \mathcal{L},t} - \mathrm{h}_{\mathcal{F},s}$.

Denoting the Néron-Severi group of X by $\mathrm{NS}(X)$, we construct in a similar fashion a map of groups

$$\mathcal{H}_2 : \mathrm{NS}(X) \to \frac{\mathrm{Hom}_{\mathrm{sets}}(X(k^{\mathrm{sep}}), \mathbb{R})}{\sim_2}. \tag{2.6}$$

We also have a functoriality result:

Proposition 10. *[Lan83, Chapter 4] Let $f : X \to Y$ be a morphism of regular projective integral varieties over the global field k, and let $\mathcal{L}$ be any ample base-point-free line bundle on Y. Then for any choices of sections, $h_{f^*\mathcal{L}} \sim_1 h_{\mathcal{L}} \circ f$.*

Finally, we reach a definition of the Néron-Tate height:

Theorem 11. *[Nér65, II.14] Let A be an Abelian variety over a number field k, and let $[\mathcal{L}] \in \mathrm{Pic}(A)$. Then there exists a unique quadratic form $q_{\mathcal{L}}$ and linear form $l_{\mathcal{L}}$ on $A(k^{alg})$ such that $q_{\mathcal{L}} + l_{\mathcal{L}} \in \mathcal{H}_1(\mathcal{L})$. Furthermore, if $\mathcal{L}$ is even (that is, $\mathcal{L} \cong \mathrm{inv}^* \mathcal{L}$) then $l_{\mathcal{L}} = 0$.*

The form $q_{\mathcal{L}}$ is called the Néron-Tate height, and is denoted $\hat{h}_{\mathcal{L}}$.

In Section 4.5 we will give a different definition more suited to our applications. The proof of the equivalence of these definitions is due to Néron [Nér65].

2.2 Cycles on relative schemes

We will repeatedly need the notions of cycles and line bundles, and there are subtleties to these notions in the relative context which make it worthwhile to take the time to formulate them precisely. References include [BLR90, 8.2, proof of Theorem 5] and [FGI+05, 9.3]

2.2.1 Algebraic cycles

The notion of algebraic cycles and their intersection theory as found in [Ful84] will be invaluable. We briefly recall the constructions of groups of cycles, and compare them to relative effective divisors. A basic reference is [Ful84, Chapter 20].

Let S be an integral regular scheme of dimension 1, and $X \to S$ be separated and of finite type with X integral and regular; for example, S could be the spectrum of a Dedekind domain, and X a regular model of a curve over the generic point of S. If $V \subset X$ is a closed integral subscheme and T is the closure of the image of V in S, set

$$\dim_S(V) = \mathrm{tr.deg}\left(\frac{F(V)}{F(T)}\right) - \mathrm{codim}(T, S). \tag{2.7}$$

We define $Z_r(X/S)$ to be the free abelian group generated by closed integral subschemes $V \subset X$ such that $\dim_S(V) = r$. If X has dimension n, set $Z^r(X/S) = Z_{n-r}(X/S)$. Set $Z(X/S) = \bigoplus_r Z^r(X/S)$. Note that any integral subscheme V of X is either flat over S or has image contained in a finite union of closed points of S.

A related notion is that of relative effective divisors:

Definition 12 (Relative effective divisors)**.** *Let $X \to S$ be a separated morphism of finite type. A relative effective divisor on X/S is a closed subscheme D of X, flat over S and such that its defining ideal sheaf $\mathcal{I}_D$ is invertible. The associated line bundle $\mathcal{O}_X(D)$ is by definition $\mathcal{I}_D^{-1} = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{I}_D, \mathcal{O}_X)$.*

In other words, a relative effective divisor is an effective Cartier divisor on X which is flat over S. Such divisors can be summed in the usual way; [FGI+05, exercise 9.3.5] shows that the result is again a relative effective divisor. We then define a functor

$$\begin{aligned} \mathrm{REDiv}_{X/S} : \mathrm{Sch}/S &\to \mathrm{Set} \\ T &\mapsto \{\text{relative effective divisors on } X_T/T\}. \end{aligned} \tag{2.8}$$

Suppose in addition that X is flat and projective over S. Then (for example, by [FGI+05, Theorem 9.3.7]) $\mathrm{REDiv}_{X/S}$ is represented by a scheme: call it $\mathbf{REDiv}_{X/S}$. The proof works by observing that $\mathrm{REDiv}_{X/S}$ is an open subfunctor of the Hilbert functor, which is itself representable. From this embedding we also naturally get a decomposition of $\mathrm{REDiv}_{X/S}$ by Hilbert polynomial. A consequence of this in the case of curves we now outline.

In addition to the above, suppose that X/S is a relative curve (that is, all fibres have relative dimension 1). Following [FGI+05, Exercise 9.3.8], we set

$$\begin{aligned} &\mathrm{REDiv}^n_{X/S}(T) = \\ &\qquad \{D \in \mathrm{REDiv}_{X/S}(T) | \deg(D_t) = n \text{ for all geometric points } t \text{ of } T\}. \end{aligned} \tag{2.9}$$

Then the $\mathrm{REDiv}^n_{X/S}$ are represented by $\mathbf{REDiv}^n_{X/S} \subset \mathbf{REDiv}_{X/S}$, which are disjoint and cover $\mathbf{REDiv}_{X/S}$.

We can now see an obvious relation between cycles and relative effective divisors:

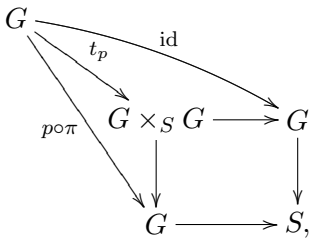
Proposition 13. *With X, S as above, there exists a canonical bijection*

$$\left\{ \begin{array}{l} D \in Z^1(X/S) : D \text{ is effective and all irreducible} \\ \text{components of } |D| \text{ are flat over } s. \end{array} \right\} \cong \mathrm{REDiv}_{X/S}(S). \tag{2.10}$$

Proof. If we drop the condition of flatness on both sides, this follows from [Har77, II, Remark 6.17.1]. Recalling ([Har77, III, Proposition 9.7]) that a scheme over S is flat if and only if all of its associated points map to the generic point of S, we are done. □

2.2.2 Group schemes

Let $\pi : G \to S$ be a group scheme. The identity section we will call 'e_G', the multiplication map 'm_G' and the inverse 'inv_G'; the subscripts may be dropped where no ambiguity will arise. Given a section $p \in G(S)$, we define a translation map τ_p by letting $t_p : G \to G \times_S G$ be the unique map fitting into the commutative diagram



then setting $\tau_p \stackrel{\mathrm{def}}{=} m_G \circ t_p$. This is an automorphism; it has inverse τ_{-p}.

τ_p acts on $\mathbf{REDiv}_{G/S}$ (and indeed, on arbitrary cycles) by $\tau_p(D) = (\tau_p)_* D$, and similarly inv_G acts on $\mathbf{REDiv}_{G/S}$ by pushforward. We often write D_p for $\tau_p(D)$ and D^- for $\mathrm{inv}(D)$.

2.2.3 Picard functors

Since they will be important in what follows, we give a construction of the Néron model of the Jacobian of a curve using the Picard functor.

There are numerous Picard functors, numerous books about them, and numerous different notational conventions. Given a scheme T, we define $\mathrm{Pic}(T)$ to be the set of isomorphism classes of invertible sheaves on T. Given a relative scheme X/S, which we assume to be separated and of finite type, we define the relative Picard functor $\mathrm{Pic}_{X/S}$ to be the functor from schemes over S to sets sending T/S to $\frac{\mathrm{Pic}(X \times_S T)}{\mathrm{Pic}(T)}$.

If the associated sheaf in the Zariski, étale, fppf or fpqc topologies is representable, we call the representing scheme $\mathbf{Pic}_{X/S}$; it is independent of the topology from whence it sprang. There are a great many conditions under which $\mathrm{Pic}_{X/S}$ is known to be representable by a scheme — a survey is provided in [BLR90]. However, it is not precisely the representability of the Picard functor which concerns us, but rather the existence of Néron models of Jacobians. For this, we use:

Theorem 14. *[BLR90, 9.5, Theorem 4 (p267)] Let S be the spectrum of a strictly Henselian discrete valuation ring, and X be a regular proper flat relative curve over S whose generic fibre is geometrically irreducible. Assume that either the residue field of S is perfect or that X admits an étale quasi section. Then:*

1) If P denotes the open subfunctor of $\mathrm{Pic}_{X/S}$ given by invertible sheaves of total degree zero and if E is the schematic closure in P of the identity section on the generic fibres, then $Q = P/E$ is a Néron model of the Jacobian of the generic fibre of X.

2) Let $X_1, \ldots, X_n$ be the irreducible components of the special fibre X_ν of X, and let δ_i be the geometric mutiplicity of X_i in X_ν (see [BLR90, 9.1/3]). Assume that the greatest common divisor of the δ_i is 1. Then $\mathrm{Pic}^0_{X/S}$ is a separated scheme, and so the projection $P \to Q$ gives rise to an isomorphism $\mathrm{Pic}^0_{X/S} \xrightarrow{\sim} Q^0$. Thus, in this case, $\mathrm{Pic}^0_{X/S}$ is the identity component of the Néron model of the Jacobian of the generic fibre of X.

The two conditions (that the residue field of S be perfect or that X admit an étale quasi section) will always both be satisfied in our situations.

2.3 Preliminaries on hyperelliptic curves

In this section we construct in detail a hyperelliptic curve over a field k. The approach we adopt may seem overly technical, but it will be necessary to understand the homogeneous coordinate ring of such a curve as well as the degree of a line bundle, and this is most coherently explained by the terminology we introduce here.

2.3.1 Weighted projective space

Given a field k and a positive integer g, let R denote the graded ring $k[x, s, y]$ where the grading is given by assigning weights 1, 1 and $g+1$ to x, s and y respectively. The weighted projective space $\mathbb{P}(1, 1, g+1)$ is then $\mathrm{Proj}(R)$. We note that as a stack this is given by the quotient $\left[\mathbb{A}^3 \setminus \{0\}/\mathbb{G}_m\right]$ under the action of $\mathbb{G}_m$ on $\mathbb{A}^3 \setminus \{0\}$ by

$$(x_0, x_1, x_2) \mapsto (\lambda \cdot x_0, \lambda \cdot x_1, \lambda^{g+1} \cdot x_2). \tag{2.11}$$

Observe that the stabilisers are trivial away from the point $p_0 = (0, 0, 1)$, which will turn out not to lie on the curve; as such, we can ignore the stack structure of our curve. Observe also that $\mathbb{P}(1, 1, g+1)$ is regular away from p_0; to see an affine neighbourhood of p_0, consider the ring homomorphism

$$\begin{aligned} k[t_1, \cdots, t_{g+1}] \to \{y^n : n \in \mathbb{N}\}^{-1} R^{\mathrm{homog}} &= R\left[\frac{1}{y}\right]^{\mathrm{homog}} \\ t_i \mapsto \frac{x^i s^{g+1-i}}{y} & \end{aligned} \tag{2.12}$$

which is surjective with kernel given by

$$\operatorname{rank}\begin{pmatrix} t_1 & \cdots & t_{g+1} \\ t_2 & \cdots & t_{g+2} \end{pmatrix} = 1. \tag{2.13}$$

2.3.2 The curve

For the purposes of this thesis, a hyperelliptic curve C of genus g is given inside $\mathbb{P}(1,1,g+1)$ by an equation $y^2+yh(x,s) = f(x,s)$ where f has homogeneous degree $2g+2$ in $k[x,s]$ and has no repeated roots over k^{alg}, and h has homogeneous degree $g+1$. Note that p_0 does not lie on C, and so C has trivial stabilisers. Let R_C denote the graded ring $R/(y^2-f)$. If k does not have characteristic 2 we will usually assume $h = 0$. We say C has odd degree if f has a root in k; we move such a root to lie at $s = 0$.

On any hyperelliptic curve C we have an involution map

$$\begin{aligned} \text{inv} : C &\to C \\ x &\mapsto x \\ s &\mapsto s \\ y &\mapsto -y - h(x,s). \end{aligned} \tag{2.14}$$

The map has order 2 and the quotient of C by it is $\mathbb{P}^1$.

2.3.3 Bezout

Bezout's Theorem is a classical fact from algebraic geometry that tells us that the intersection number of two plane curves of degrees d and e respectively in $\mathbb{P}^2$ is $d \cdot e$. To extend this to weighted projective space one must be more careful: given a section ϕ of $R_C(n)$ for some positive integers n, the intersection multiplicity of C with the subvariety of $\mathbb{P}(1,1,g+1)$ cut out by ϕ is

$$\frac{n \cdot \text{degree}(y^2 + hy - f)}{1 \cdot 1 \cdot (g+1)} = 2n. \tag{2.15}$$

2.3.4 Mumford coordinates

Mumford's representation of divisors on hyperelliptic curves is explained in [MM84]. In this thesis we are mainly interested in the case of odd-degree and $h = 0$, and we briefly recall Mumford's coordinate system in this situation. Let $\infty = \infty_C$ denote the unique point at infinity ($s = 0$) of C.

Suppose C is defined by the equation $y^2 + yh(x) = f_{2g+1}(x)$ in $\mathbb{P}(1, 1, g+1)$.

A point on $\mathrm{Jac}(C)$ is given by a pair (α, β) where α, β in $k[x, y]$ such that:

1. α is monic of degree at most g.
2. $\deg(\beta) < \deg(\alpha)$.
3. α divides $\beta^2 + \beta h - f$.

The pair (α, β) corresponds to the divisor $\mathbb{V}(\alpha = 0, y - \beta = 0) - \deg(\alpha).\infty$ on C. The coefficients of such α, β are then coordinates on an affine piece of the Jacobian of C. In particular, k-rational points on the Jacobian correspond exactly to such pairs of α, β with coefficients in k.

2.3.5 Cantor's algorithm

Cantor's algorithm [Can87] allows for the efficient addition of divisors on a hyperelliptic curve in Mumford representation. This is well known, but we will give pseudocode for a trivial extension of Cantor's algorithm which, given as input two divisors $D_1 = (a_1, \beta_1)$, $D_2 = (\alpha_2, \beta_2)$ in Mumford form, gives as output their sum D and also a rational function φ such that $D_1 + D_2 - D = \mathrm{div}(\varphi)$ (to shorten the exposition, we assume that $h(x) = 0$):

0) Set $\varphi = 1$.

1) Using the Euclidean algorithm, compute polynomials $d_1, e_1, e_2 \in k[x]$ such that $d_1 = \gcd(\alpha_1, \alpha_2)$ and $d_1 = e_1\alpha_1 + e_2\alpha_2$.

2) Similarly compute polynomials $d_2, c_1, c_2 \in k[x]$ with $d_2 = \gcd(d_1, \beta_1 + \beta_2)$ and $d_2 = c_1 d_1 + c_2(\beta_1 + \beta_2)$.

3) Put $s_1 = c_1 e_1$, $s_2 = c_1 e_2$ and $s_3 = c_2$, which gives $d_2 = s_1\alpha_1 + s_2\alpha_2 + s_3(\beta_1 + \beta_2)$.

4) Set $\alpha = \alpha_1\alpha_2/(d_2^2)$ and $\beta = s_1\alpha_1\beta_2 + s_2\alpha_2\beta_1 + s_3(\beta_1\beta_2 + f)/d_2 \mod \alpha$.

4') Set $\varphi = \varphi \times d_2$.

5) Set $\alpha' = (f - \beta^2)/\beta$ and $\beta' = -\beta \mod \alpha'$.

5') Set $\varphi = \varphi \times \alpha(y - \beta)/(f - \beta^2)$.

6) If $\deg(\alpha') > g$, then set $\alpha = \alpha'$ and $\beta = \beta'$ and repeat steps 5 and 5' until $\deg(\alpha') \leq g$.

7) Make α' monic by dividing through its leading coefficient.

8) Output $D = (\alpha', \beta')$, φ.

Using Mumford coordinates, it is possible to obtain a detailed description of the structure of divisors on a hyperelliptic curve. In particular, it is possible to choose a unique representative in each degree-zero divisor class (a semi-reduced divisor, see Chapter 6). We do not reproduce the details of these constructions here,

as they are given in great detail in Mumford's book [MM84]. We do however include a slight extension of a result of Mumford as follows:

Lemma 15. *Let C be an odd-degree hyperelliptic curve of genus g over an algebraically closed field k, and let $E = \sum_{i=1}^{g} p_i$ be a divisor such that* $\mathrm{inv}(p_i) \neq p_j$ *if $i \neq j$. Then there does not exist a non-constant rational function on C whose poles are bounded by E (i.e. $H^0(C, \mathcal{O}(E)) = 0$).*

Proof. If none of the p_i are at infinity, then this follows from [MM84, 3.30, Step II]. We may therefore assume that $p_g = \infty$, and we emulate Mumford's proof. Let h be such a function; then $h \cdot \prod_{i=1}^{g-1}(x - x(p_i))$ has poles only at infinity, and hence is a polynomial in the affine coordinates x and y; write it as $\phi(x) + y\psi(x)$. Now $\mathrm{ord}_\infty(y\psi) = -(2g+1)$ which is odd, and $\mathrm{ord}_\infty(\phi)$ and $\mathrm{ord}_\infty(\psi)$ are even, so $\mathrm{ord}_\infty(y\psi) \neq \mathrm{ord}_\infty(\phi)$. Hence if $\psi \neq 0$ we have

$$\begin{aligned} 1 = -\operatorname{ord}_\infty(h) &= -\operatorname{ord}_\infty\left(\frac{\phi + y\psi}{\prod_{i=1}^{g-1}(x - x(p_i))}\right) \geq -\operatorname{ord}_\infty\left(\frac{y\psi}{\prod_{i=1}^{g-1}(x - x(p_i))}\right) \\ &\geq -\operatorname{ord}_\infty(y\psi) - 2(g-1) > 1 - \operatorname{ord}_\infty(\psi) \geq 1, \end{aligned} \tag{2.16}$$

a contradiction. Hence $\psi = 0$, so h is the pullback of a rational function on $\mathbb{P}^1$; this contradicts the assumption that $\mathrm{inv}(p_i) \neq p_j$ if $i \neq j$. □

Chapter 3

Arakelov theory

In this chapter, we give the basic constructions of Arakelov-Chow groups and the action of the first Chern class of a Hermitian line bundle on them. There exist a range of definitions. The first, due to Arakelov [Ara74], was restricted to the case of surfaces and 'admissible' line bundles. Deligne [Del87] showed how the admissibility condition could be dropped, paving the way for the ideas of Gillet and Soule [GS90a], which work in great generality and give a ring structure to the Arakelov-Chow groups after tensoring them with $\mathbb{Q}$.

We pick a middle path. We restrict our definitions to quasi-projective varieties, as without this condition it is unclear how to prove non-degeneracy of heights. We do not restrict to the 'admissible' metrics of Arakelov on surfaces, as we need to work on Néron models of Jacobians, not just on surfaces. However, for our purposes we can assume that the schemes we work with are regular, and further we only need the actions of the first arithmetic Chern class on the Chow groups (in fact only on CH_1), This allows us to avoid the K-theoretic approach of Gillet and Soule in [GS90a], which is advantageous as it is not clear how to make this effective.

It is possible to construct the pairings of Néron and Arakelov in an ad-hoc fashion, and indeed Hriljac in his thesis [Hri77] proves many of the basic results we will need just from such an approach. However, the broader aim of this thesis is to explore effective applications of Arakelov theory to Diophantine geometry, and this is better served by the more general definitions given here.

3.1 Arithmetic varieties

Definition 16. *Given a number field k, let S denote the spectrum of its ring of integers. We define an arithmetic variety to be a scheme $\mathscr{X}/S$ such that :*

1) $\mathscr{X}$ is regular.

2) $\mathscr{X}$ is flat and quasi-projective over S.

3)The generic fibre $\mathscr{X}_k$ is smooth and proper over k.

We do not assume that $\mathscr{X}$ comes with a fixed projective embedding, but we make the projectivity assumption in order to ensure that ample line bundles exist.

Let Σ denote the set of $\mathbb{Z}$-algebra embeddings $\sigma : \mathcal{O}_k \to \mathbb{C}$. For any $\sigma \in \Sigma$, let $\mathscr{X}_\sigma \overset{\text{def}}{=} \mathscr{X} \times_{\mathcal{O}_k,\sigma} \mathbb{C}$. By abuse of notation we denote the corresponding complex manifold by $\mathscr{X}_\sigma$. Let $\mathbb{C}^\Sigma \overset{\text{def}}{=} \mathbb{C} \otimes_{\mathbb{Z}} \mathcal{O}_k = \prod_{\sigma\in\Sigma} \mathbb{C}$. Let $F_\infty : \mathbb{C}^\Sigma \to \mathbb{C}^\Sigma$ be a conjugate linear involution of $\mathbb{C}$-algebras leaving invariant the image of $\mathcal{O}_k$ under the canonical map induced by the tensor product. We then define

$$\mathscr{X}_\Sigma = \bigsqcup_{\sigma\in\Sigma} \mathscr{X}_\sigma = \mathscr{X} \times_{\mathrm{Spec}(\mathcal{O}_k)} \mathrm{Spec}\left(\mathbb{C}^\Sigma\right) = \mathscr{X} \times_{\mathbb{Z}} \mathbb{C}. \tag{3.1}$$

Again, by abuse of notation we denote by $\mathscr{X}_\Sigma$ the corresponding complex manifold. F_∞ then induces a map $\mathscr{X}_\Sigma \to \mathscr{X}_\Sigma$.

Aside 17. *For fixed $\mathscr{X}$, the complex manifolds $\mathscr{X}_\sigma$ can be very different. The first example of this was given by Serre [Ser64], who constructed a smooth projective $\mathscr{X}$ such that two of the $\mathscr{X}_\sigma$ have non-isomorphic fundamental groups.*

3.2 Metrics on line bundles

Definition 18. *Let $\mathscr{X}/S$ be an arithmetic variety, and $\mathcal{L}$ an invertible sheaf on $\mathscr{X}$. Let L denote the corresponding invertible sheaf on $\mathscr{X}_\Sigma$. Following [CL09, §2.4 G], we define a Hermitian metric on L to be a collection of maps $\|s\| : U \to \mathbb{R}_{\geq 0}$ for U running over open subsets of $\mathscr{X}_\Sigma$, and for s running over sections in $L(U)$, satisfying the following properties:*

1) If $V \subset U$ are open sets, and $x \in V$, $s \in L(U)$, then

$$\|s\|(x) = \|s|_V\|(x).$$

2) If $s \in L(U)$ and $f \in \mathcal{O}_{\mathscr{X}_\Sigma}(U)$, then $\|fs\| = |f| \cdot \|s\|$.

We say the metric is smooth, continuous, etc. if for every non-vanishing section s, the map $\|s\|$ is smooth, continuous, etc.

We denote a line bundle L on a complex manifold with a metric $\|-\|$ by $\overline{L} = (L, \|-\|)$, and similarly $\overline{\mathcal{L}} = (\mathcal{L}, \|-\|)$ denotes a line bundle on an arithmetic variety with a metric on the corresponding complex line bundle. Such $\overline{L}$ and $\overline{\mathcal{L}}$ are known variously as metrised or Hermitian line bundles.

3.3 Pull-back of Hermitian line bundles

Let $f : X \to Y$ be a morphism of regular varieties over $\mathbb{C}$, and $\overline{L}$ a Hermitian line bundle on Y. Suppose further that f is the composite of a smooth morphism with a closed immersion (this will prevent the pullback metric from being degenerate). To define the pullback $f^*\overline{L}$, we begin by noting that for any $q \in Y(\mathbb{C})$, open subset U of Y containing q, and section $s \in L(U)$, the metric induces in a canonical way a metric on the fibre L_q. Given $p \in X(\mathbb{C})$ and an open neighbourhood V of p, we let $\varphi_p : (f^*L)_p \to L_{f(p)}$ denote the canonical linear map, and set $\|s\|(p) = \|\varphi_p(s_p)\|$, which makes sense by the observation above. It is clear that this defines a Hermitian line bundle structure on f^*L, but less clear is that if $\overline{L}$ is continuous then $f^*\overline{L}$ is, similarly for smoothness of $\overline{L}$ etc. The easiest way to prove this is to compute the Hermitian <u>form</u> $\langle -, - \rangle$ on L corresponding to $\|-\|$, and then to define $f^* \langle -, - \rangle$ as follows.

Fix an open subset V of X, and sections s_1 and s_2 in

$$(f^*L)(V) = (f^{-1}L)(V) \otimes_{(f^{-1}\mathcal{O}_Y)(V)} (\mathcal{O}_X)(V). \tag{3.2}$$

Then we can find some open set $U \supset f(V)$, integer $n > 0$, and for each $i \in \{1, 2\}$ and $j \in \{0, \ldots, n\}$, sections $t_j^i \in L(U)$ and $r_j^i \in \mathcal{O}_X(V)$ such that

$$s_i = \sum_{j=0}^{n} \left(t_j^i \circ f\right) \otimes r_j^i. \tag{3.3}$$

Then set

$$\langle s_1, s_2 \rangle (-) = \sum_{j=0}^{n} \sum_{l=0}^{n} \langle t_j^1, t_l^2 \rangle (f(-)) \cdot \left|r_j^1(p)\right| \left|r_l^2(p)\right|. \tag{3.4}$$

It is easy to check that this is independent of the representation of s_i in terms of the t_j^i and r_j^1, and also that additional properties such as continuity, smoothness etc. carry through this definition to the induced Hermitian metric $\|-\| = \sqrt{\langle -, - \rangle}$ on f^*L.

3.4 The Fubini-Study metric

Here we give as an example of a metric on a line bundle the Fubini-Study metric on $\mathcal{O}_{\mathbb{P}^n}(1)$; this will play an important rôle when we come to define heights.

Let $\mathbb{P}^n = \mathrm{Proj}\,(\mathbb{C}[x_0, \ldots, x_n])$ where the grading is by unweighted degree, so $\mathrm{H}^0\left(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1)\right) = \mathbb{C}\langle x_0, \ldots, x_n \rangle$ (the $\mathscr{C}$-vector space with basis $x_0, \ldots, x_n$). Fur-

ther, observe that for any open subset U of X and section $s \in \mathcal{O}_{\mathbb{P}^n}(1)(U)$, there exists $l \in \mathbb{C}\langle x_0, \ldots, x_n\rangle$ and $f \in \mathcal{O}_{\mathbb{P}^n}(U)$ such that $f \cdot l = s$. As a result, it suffices to define $\|l\| : \mathbb{P}^n \to \mathbb{R}_{\geq 0}$ for $l \in \mathbb{C}\langle x_0, \ldots, x_n\rangle$. We set

$$\|l\|(t_0, \ldots, t_n) = \frac{|l(t_0, \ldots, t_n)|}{\sqrt{\sum_{j=0}^{n} |t_j|^2}}. \tag{3.5}$$

It is easy to check that this defines a differentiable metric. Pullbacks of this metric will be useful later in constructing heights.

3.5 Morphisms of Hermitian line bundles

Let X be a regular variety over $\mathbb{C}$, and $\overline{L}$, $\overline{M}$ Hermitian line bundles on X. A morphism φ from $\overline{L}$ to $\overline{M}$ is a morphism of the underlying line bundles such that for every open subset U of X, section $s \in L(U)$ and $x \in U(\mathbb{C})$, we have the inequality

$$\|s\|(x) \geq \|\varphi(s)\|(x) \tag{3.6}$$

An isomorphism is a morphism with a two-sided inverse; in particular, it is an isometry on fibres.

If now $\mathscr{X}/S$ is an arithmetic variety, and $\overline{\mathcal{L}}$, $\overline{\mathcal{M}}$ are Hermitian line bundles on $\mathscr{X}$, a morphism from $\overline{\mathcal{L}}$ to $\overline{\mathcal{M}}$ is a morphism of the underlying line bundles $\mathcal{L}$, $\mathcal{M}$ which induces a morphism of the corresponding Hermitian line bundles on $\mathscr{X}_\Sigma$.

Definition 19. *The Arakelov-Picard group $\widehat{\mathrm{Pic}}(\mathscr{X})$ of an arithmetic variety $\mathscr{X}$ is the group of isomorphism classes of Hermitian line bundles on $\mathscr{X}$.*

3.6 Forms and currents

Let X be a regular proper variety over $\mathbb{C}$, which we consider as a complex manifold. Let $\mathscr{A}^{(p,q)}(X)$ denote the space of smooth differential forms of bidegree (p, q) on X, and set $\mathscr{A}^m(X) = \bigoplus_{p+q=m} \mathscr{A}^{(p,q)}(X)$. We give $\mathscr{A}^{(p,q)}(X)$ the structure of a topological vector space as in [GH94, Chapter 3.1], and define the space of currents $\mathscr{D}_{(p,q)}(X)$ to be the topological dual of $\mathscr{A}^{(p,q)}(X)$ (compactness of X allows us to ignore the usual conditions of compact support). If X has dimension n (as a complex manifold or equivalently as an algebraic variety), we define $\mathscr{D}^{(p,q)}(X) = \mathscr{D}_{(n-p,n-q)}(X)$.

In the standard fashion we have an injective map $\mathscr{A}^{(p,q)}(X) \to \mathscr{D}^{(p,q)}(X)$ sending a form ω to the current $\left[\alpha \mapsto \int_X \omega \wedge \alpha\right]$. Push forward and pullback of

currents are defined dually to the corresponding notions for forms in the following manner:

Let $f : X \to Y$ be a morphism of complex manifolds, with X and Y of pure dimensions d and e respectively. The maps $f^* : \mathscr{A}^{(p,q)}(Y) \to \mathscr{A}^{(p,q)}(X)$ induce maps

$$f_* : \mathscr{D}^{(p,q)}(X) \to \mathscr{D}^{(e-d+p,e-d+q)}(Y) \tag{3.7}$$

by $(f_*T)(\alpha) = T(f^*\alpha)$.

If F is a proper submersion, one can integrate along the fibres by a theorem of Ehresmann [Ehr51] (see [GS90a, 1.1.4] for details) to obtain a pushforward

$$f_* : \mathscr{A}^{(p,q)}(X) \to \mathscr{A}^{(e-d+p,e-d+q)}(Y) \tag{3.8}$$

and hence by duality we obtain the pullback $f^* : \mathscr{D}^{(p,q)}(Y) \to \mathscr{D}^{(p,q)}(X)$.

Definition 20 (Real forms and currents)**.** *If our complex manifold is of the form $\mathscr{X}_\Sigma$ for some arithmetic variety $\mathscr{X}$, then it comes with a conjugate linear involution $F_\infty : \mathscr{X}_\Sigma \to \mathscr{X}_\Sigma$ (see Section 3.1). We can thus define subspaces of real forms and currents: given $\omega \in \mathscr{A}^{(p,p)}(\mathscr{X}_\Sigma)$ (respectively $\mathscr{D}^{(p,p)}(\mathscr{X}_\Sigma)$), we say that ω is <u>real</u> if and only if ω is real valued and $F_\infty^*\omega = (-1)^p\omega$ (it makes sense to ask that ω be real-valued since its bidegree is symmetric); see [GS90a, p124]. We write $\mathscr{A}^{(p,p)}(\mathscr{X}_{\Sigma,\mathbb{R}})$ for the space of real forms, and $\mathscr{D}^{(p,p)}(\mathscr{X}_{\Sigma,\mathbb{R}})$ for the space of real currents.*

Note that the operator $\partial\overline{\partial}$ sends the space of real forms $\mathscr{A}^*(\mathscr{X}_{\Sigma,\mathbb{R}})$ to itself, and similarly for currents.

3.7 Integration currents

If X is a smooth complex variety of complex dimension d and $\iota : Y \hookrightarrow X$ an integral subvariety of codimension p, let Y_{ns} denote the regular locus of Y. We then define an integration current δ_Y in $\mathscr{D}^{(p,p)}(X)$ as

$$\delta_Y(\alpha) = \int_{Y_{ns}} \iota^*\alpha, \tag{3.9}$$

for $\alpha \in \mathscr{A}^{(d-p,d-p)}(X)$. That δ_Y is a well defined current is due to Lelong [Lel57]; an alternative proof using Hironaka's resolution of singularities is given in [Sou92, II.1, p40].

3.8 Green currents

Here we give the definition of a Green current for a subvariety — a crucial step in the definition of most arithmetic intersection theories. The motivation for the use of Green currents is twofold; they give a measure of the distance between two subvarieties, thus reflecting the non-Archimedean case, and their precise definition yields appropriate formal properties to give a well-behaved intersection theory.

Definition 21. *Let $\mathscr{X}$ be an arithmetic variety. Given a cycle $z \in Z^p(\mathscr{X}_\Sigma)$, a Green current for z is a current $g_z \in \mathscr{D}^{(p-1,p-1)}(\mathscr{X}_{\Sigma,\mathbb{R}})$ such that there exists a form $\omega_z \in \mathscr{A}^{(p,p)}(\mathscr{X}_{\Sigma,\mathbb{R}})$ for which the equality*

$$\mathrm{dd}^c g_z + \delta_z = [\omega_z] \tag{3.10}$$

holds in $\mathscr{D}^{(p,p)}(\mathscr{X}_{\Sigma,\mathbb{R}})$.

In the work of Arakelov [Ara74], there is an additional restriction put on Green currents by prescribing the differential form ω_z; this leads to the notion of an admissible current, which we will not need here. At a later stage we will show how to make natural choices of ω_z, but to develop the theory in generality it is better to allow arbitrary forms at this point.

3.9 Existence of Green currents

There are many results on the existence of Green currents; we postpone the statement that we need to Theorem 22. Perhaps more difficult is their explicit construction. There are two situations in which this is well understood, one of which is the case of linear subvarieties of projective space; this is by a theorem of Levine, in [Lev60]; see also [Sou92, II.2.3] for a brief overview, or [GS90b, §5] for a detailed exposition. The other easy case is that of a Cartier divisor when a metric is given on an associated line bundle; this is essentially due to the Poincare-Lelong formula as follows.

3.9.1 Green current for a Cartier divisor

Let X be a regular complex variety and $\overline{L}$ a Hermitian line bundle on X. Let M_X denote the sheaf of regular meromorphic functions on X, see [Gro67, IV, §20]. Choose a regular meromorphic section s of L, that is, some $s \in \mathrm{H}^0\left(X, L \otimes_{\mathcal{O}_X} M_X\right)$.

Since L is locally trivial, we can find an open cover $\mathfrak{U} = \{U_i\}$ of X, together with $f_i \in M_X(U_i)$ and $t_i \in L(U_i)$ nowhere-vanishing such that

$$s|_{U_i} = t_i \otimes f_i \tag{3.11}$$

(recall that the tensor product of sheaves is defined to be the sheafification of the presheaf resulting from the naïve definition).

To the pair (L, s) we associate uniquely the Cartier divisor $\{(U_i, f_i)\}$. Now on U_i set $\mathrm{div}_{U_i}(s) = \mathrm{div}_{U_i}(f_i)$, and set $\|s\| = \|t_i\| \cdot |f_i|$. These are both independent of the choice of t_i and f_i, and agree on overlaps of any chosen open sets U_i, and so $\mathrm{div}(s)$ is a globally defined Cartier divisor, and $\|s\|$ makes sense outside the support of $\mathrm{div}(s)$.

We define the first Chern class $c_1(\overline{L})$ of $\overline{L}$ in $\mathscr{A}^{(1,1)}(X)$ as follows: over any open subset $U \subset X$ and $t \in L(U)$ non-vanishing, set $c_1(\overline{L})|_U = \mathrm{dd}^c \log\|t\|^{-1}$. Transition functions are holomorphic, so it is easy to check that this gives a globally defined $(1,1)$-form, whose class then lies in $\mathscr{D}^{(1,1)}(X)$. Now the Poincare-Lelong formula gives

$$\mathrm{dd}^c \log\left(\|s\|^{-1}\right) + \delta_{\mathrm{div}(s)} = \left[c_1(\overline{L})\right], \tag{3.12}$$

and hence $\log\left(\|s\|^{-1}\right)$ is a Green current for $\mathrm{div}(s)$ (see also [CL09, Proposition 2.4.14]). We write $\widehat{c_1}(\overline{L}) = \left(\mathrm{div}(s), c_1(\overline{L})\right)$.

The above example suggests that Green currents for codimension 1 cycles are straightforward, at least in the regular case; certainly they are much more straightforward than for cycles of higher codimension. However, what the above construction has achieved is to move the problem from constructing Green currents to constructing metrics on line bundles. Pulling back the Fubini-Study metric under a projective embedding is one source of metrics, but such metrics are not always sufficient; more involved constructions will be needed for metrics used to obtain Néron-Tate heights.

3.10 Arakelov-Chow groups

Let $\mathscr{X}$ be an arithmetic variety. Let $\widehat{Z}^p(\mathscr{X})$ denote the set of pairs (z, g_z) where z is a cycle in $Z^p(\mathscr{X})$ and g_z is a Green current in $\mathscr{D}^{(p-1,p-1)}(\mathscr{X}_{\Sigma,\mathbb{R}})$ for the cycle in $\mathscr{X}_\Sigma$ corresponding to z. Addition in $\widehat{Z}^p(\mathscr{X})$ is defined pointwise; it is easy to check that the sum of Green currents is a Green current for the sum of cycles. Let $\widehat{R}^p(\mathscr{X}) \subset \widehat{Z}^p(\mathscr{X})$ be the subgroup generated by pairs of one of the following two forms:

1) $\left(\mathrm{div}(f), \left[\log\left(|f|^{-2}\right)\right]\right)$ where $f \in k(y)^*$, a rational function on some prime cycle $y \in Z_{p-1}(\mathscr{X})$.

2) $\left(0, \partial(u) + \overline{\partial}(v)\right)$ for some $u \in \mathscr{D}^{(p-2,p-1)}(\mathscr{X}_{\Sigma,\mathbb{R}})$ and $v \in \mathscr{D}^{(p-1,p-2)}(\mathscr{X}_{\Sigma,\mathbb{R}})$.

Pairs of type (1) obviously reflect the usual notion of rational equivalence of cycles. Those of type (2) arise as a consequence of the Hodge decomposition. We then define the arithmetic Chow group by

$$\widehat{\mathrm{CH}}^p(\mathscr{X}) \stackrel{\mathrm{def}}{=} \widehat{Z}^p(\mathscr{X})/\widehat{R}^p(\mathscr{X}). \tag{3.13}$$

Theorem 22. *[Sou92, III, 1.2] For any arithmetic variety $\mathscr{X}$, the following sequence is exact:*

$$\frac{\mathscr{A}^{(p-1,p-1)}(\mathscr{X}_{\Sigma,\mathbb{R}})}{\left(\mathrm{Image}(\partial) + \mathrm{Image}(\overline{\partial})\right)} \stackrel{a}{\to} \widehat{\mathrm{CH}}^p(\mathscr{X}) \stackrel{b}{\to} \mathrm{CH}^p(\mathscr{X}) \to 0 \tag{3.14}$$

where $a(\omega) = [([\omega], 0)]$, and $b\left([(z, g_z)]\right) = [z]$. In particular, Green currents exist for all cycles.

Aside 23. *For $p \geq 1$ and a cycle $z \in V$, it may happen that $z_{\mathbb{Q}}$ is empty. See [Sou92, III 2.1] for a decomposition of $\widehat{\mathrm{CH}}^p(X)$ along these lines.*

3.11 Intersection pairings

For our applications, we only need the action of the first (arithmetic) Chern class of a Hermitian line bundle on the (arithmetic) Chow groups. This is fortunate, since to go beyond this one must go via K-theory, and can only obtain (at the time of writing) a pairing of the Chow groups with rational coefficients. Since we are primarily interested in heights these coefficients are not a major drawback, but it appears hard to make these K-theoretic results explicit.

We wish to define an action

$$\begin{aligned} \widehat{\mathrm{Pic}}(\mathscr{X}) \times \widehat{CH}^p(\mathscr{X}) &\to \widehat{CH}^{p+1}(\mathscr{X}) \\ \left(\overline{L}, [(z, g_z)]\right) &\mapsto \overline{L} \cdot (z, g_z) \end{aligned} \tag{3.15}$$

for $p > 0$. To do this, fix $\overline{L}$ a Hermitian line bundle and (z, g_z) a cycle whose class lies in $\widehat{CH}^p(\mathscr{X})$; assume further that z is irreducible. Write $j : z \hookrightarrow \mathscr{X}$ for the inclusion map. As in Section 3.9.1, fix a regular meromorphic section s of j^*L, so $s \in \mathrm{H}^0\left(z, j^*L \otimes_{\mathcal{O}_z} M_z\right)$. Then set

$$\overline{L} \cdot (z, g_z) = \left(j_*\left(\mathrm{div}_z(s)\right), j_* \log\|s\|^{-1} + \left[c_1(\overline{L})\right] \wedge g_z\right), \tag{3.16}$$

where the wedge $\big[c_1(\overline{L})\big] \wedge g_z$ is defined by

$$\big\langle \big[c_1(\overline{L})\big] \wedge g_z, \alpha \big\rangle = \big\langle g_z, c_1(\overline{L}) \wedge \alpha \big\rangle \tag{3.17}$$

for all forms α of suitable degree.

Much work remains to show that this defines an element of $\widehat{CH}^{p+1}(\mathscr{X})$; see [Sou92, III.2, Theorem 2 and Remark 2.3.2] or [CL09, §2.5c]. The reader will easily check that the given current lies in $\mathscr{D}^{(p+1,p+1)}(\mathscr{X}_{\Sigma,\mathbb{R}})$.

3.12 Degree of a cycle

The final notion we need to introduce before defining a height is that of the degree of an arithmetic cycle. In classical intersection theory, in the absence of a polarisation, one defines the degree of a zero-cycle to be the degree of its pushforward to a point along the structure map. In the arithmetic context, we still have a pushforward, but it is less clear how to define the degree of a cycle on the base scheme. Recalling that this base scheme will be the spectrum of the ring of integers of some number field, we make the following definitions (which could easily be generalised to an order in a number field).

Definition 24 (Degree of a cycle)**.** *Let $\mathcal{O}_k$ denote the integers of the number field k, and set $S \overset{def}{=} \mathrm{Spec}(\mathcal{O}_k)$. Given a cycle $[(z, g_z)] \in \widehat{CH}^1(S)$, we write $z = \sum_p n_p \cdot p$ where the sum is over prime ideals p of height 1 in $\mathcal{O}_k$, and we observe that $g_z \in \mathscr{D}^{(0,0)}(S_{\Sigma,\mathbb{R}})$ corresponds to an element $\tilde{g}_z = \prod_{\sigma\in\Sigma} g_\sigma \in \mathbb{R}^\Sigma$. Then we define*

$$\widehat{\deg}\left([(z, g_z)]\right) = \sum_p n_p \cdot \log\left(\#\left(\frac{\mathcal{O}_k}{p}\right)\right) + \sum_{\sigma\in\Sigma} g_\sigma, \tag{3.18}$$

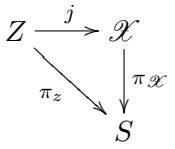
where again the first sum is over prime ideals p of height 1 in $\mathcal{O}_k$. This is independent of the choice of (z, g_z) in $[(z, g_z)]$ (see [CL09, Chapter 1.B]).

3.13 Heights

Suppose we are given an arithmetic variety $\mathscr{X}$, together with a fixed Hermitian line bundle $\overline{\mathcal{L}}$ on $\mathscr{X}$. Recalling that the function field of the base scheme S is a number field k, we obtain a height

$$\mathrm{h}_{\overline{\mathcal{L}}} : Z(\mathscr{X}_k) \to \mathbb{R} \tag{3.19}$$

as follows: fix $z_\eta \in Z(\mathscr{X}_k)$, and let z denote its Zariski closure in $\mathscr{X}$. Write $j : z \hookrightarrow \mathscr{X}$ for the inclusion, and consider the commutative diagram



Define the arithmetic cycle $\hat{z} = (z, g_z)$ associated to z by the equation

$$\mathrm{d}\,\mathrm{d}^c\, g_z + \delta_z = j_* j^* c_1(\overline{\mathcal{L}}); \tag{3.20}$$

the existence of such g_z follows from Theorem 22. Now set

$$\mathrm{h}_{\overline{\mathcal{L}}}(z_\eta) = \widehat{\deg}\left(\pi_{z*}\left(j^*\overline{\mathcal{L}}\right) \cdot (S, 0)\right) \tag{3.21}$$

where $(S, 0) \in \widehat{CH}^0(S)$ is the trivial cycle (this is included since $\pi_{z*}\left(j^*\overline{\mathcal{L}}\right)$ is a line bundle not a cycle and we defined degrees on cycles, but we will on occasion omit it in future for simplicity). If $\mathscr{X}/S$ is projective, then by [Sou92, III, Theorem 3] we have

$$\mathrm{h}_{\overline{\mathcal{L}}}(z_\eta) = \widehat{\deg}\left(\pi_{\mathscr{X}*}\left(\overline{\mathcal{L}} \cdot \hat{z}\right)\right), \tag{3.22}$$

and so the height pairing can be realised directly as an intersection pairing on $\mathscr{X}$.

3.14 Height on $\mathbb{P}^n$

As an example, we consider projective space over $\mathrm{Spec}(\mathbb{Z})$. Write

$$\mathbb{P}^n_{\mathbb{Z}} = \mathrm{Proj}\left(\mathbb{Z}\left[x_0, \ldots, x_n\right]\right), \tag{3.23}$$

and set $\overline{\mathcal{L}} = \mathcal{O}(1)$ with the Fubini-Study metric on the corresponding complex line bundle. Fix $p = (p_0, \ldots, p_n) \in \mathbb{P}^n_{\mathbb{Z}}(\mathbb{Q})$. We may assume the p_i are coprime integers, and so there exist integers u_i such that $\sum_{i=0}^n p_i \cdot u_i = 1$. Let $\overline{p}$ denote the Zariski closure of p in $\mathbb{P}^n_{\mathbb{Z}}$, and $j : \mathrm{Spec}(\mathbb{Z}) \hookrightarrow \mathbb{P}^n_{\mathbb{Z}}$ the corresponding inclusion. Then j corresponds to a ring homomorphism

$$\begin{aligned} \mathbb{Z}[x_0, \ldots, x_n] &\to \mathbb{Z} \\ x_i &\mapsto p_i. \end{aligned} \tag{3.24}$$

Hence $j^*\mathcal{O}(1) \simeq \mathbb{Z}\left[p_0, \ldots, p_n\right] = \mathbb{Z}$.

By Section 3.13, we need to compute $\widehat{\deg}\left(j^*\mathcal{O}(1) \cdot (p, 0)\right)$. To do so, we choose a regular meromorphic section s of $j^*\mathcal{O}(1)$; we take $s = 1$ in $\mathbb{Z}$. Then the finite part of $\widehat{\deg}$ is clearly zero, and it suffices to compute the infinite part, $\log\left(\|s\|^{-1}\right)$.

Now $s \in \mathbb{Z}$ corresponds to the restriction to $p \in \mathbb{P}^n_{\mathbb{Z}}(\mathbb{Q})$ of the section $\tilde{s} = \sum_{i=0}^{b} u_i \cdot x_i \in \mathrm{H}^0\left(\mathbb{P}^n, \mathcal{O}(1)\right)$. As such, it suffices to compute $\|\tilde{s}\|(p)$. From Section 3.4, we see that

$$\|\tilde{s}\|(p_0, \ldots, p_n) = \frac{\left|\sum_{i=0}^{n} u_i \cdot p_i\right|}{\sqrt{\sum_{i=0}^{n} |p_i|^2}} = \frac{1}{\sqrt{\sum_{i=0}^{n} |p_i|^2}}. \tag{3.25}$$

Hence

$$\mathrm{h}_{\overline{\mathcal{O}(1)}}(p) = \log\left(\sqrt{\sum_{i=0}^{n} |p_i|^2}\right). \tag{3.26}$$

If one prefers the height $\mathrm{h}(p) = \log\left(\max_i |p_i|\right)$, this can be arranged by a different choice of metric on $\mathcal{O}(1)$, but this metric will not be differentiable, and so it is sometimes less convenient.

3.15 Relative ampleness of line bundles

In this section, which is something of an aside to the main discourse, we discuss a distinction between two heights that can arise from an ample base point free line bundle on the generic fibre of an arithmetic variety. Suppose that $\mathscr{X}$ is an arithmetic variety, and $\mathcal{L}$ is a base point free ample line bundle on the generic fibre $\mathscr{X}_\eta$ of $\mathscr{X}$, and that we have chosen a basis of the dual space to the space of global sections of $\mathcal{L}$. There are two natural ways to obtain a height on $\mathscr{X}$:

1) Let $\varphi : \mathscr{X}_\eta \to \mathbb{P}^n_k = \mathrm{Proj}\left(\mathrm{H}^0\left(\mathscr{X}_\eta, \mathcal{L}\right)\right)^\vee$ be the canonical map, and set $\mathrm{h}^1(p)$ to be the naïve height of $\varphi(p)$.

2) Extend $\mathcal{L}$ to a bundle $\mathscr{L}$ on $\mathscr{X}$ flat over the base (such an extension exists and is unique, since $\mathscr{L}$ is required to be locally free). Pull back the Fubini-Study metric to get a metric on the complex line bundle associated to $\mathscr{L}$, and apply the constructions of Section 3.13 to obtain a height which we shall call h^2.

How are h^1 and h^2 related? We list some easy results:

If $\mathscr{L}$ is relatively ample and base point free, and yields a map $\mathscr{X} \to \mathbb{P}^n_{\mathcal{O}_k}$ whose generic fibre is φ, then it is easy to see that $\mathrm{h}^1 = \mathrm{h}^2$.

If $\mathscr{L}$ is relatively base point free, then let $\overline{\varphi}$ denote the corresponding morphism from $\mathscr{X}$ to a projective space. Then $\mathscr{L}$ is generically isomorphic to $\overline{\varphi}^*\mathcal{O}(1)$, and so they differ at only finitely many fibres. As such, we see that $\left|\mathrm{h}^1 - \mathrm{h}^2\right|$ is bounded for points rational over extensions of k of bounded degree.

If $\mathscr{X}_\eta$ is an Abelian variety and $\mathscr{X}$ is its Néron model, then [Nér65, II.14]

shows that $\left|\hat{\mathrm{h}} - \mathrm{h}^2\right|$ is bounded, and [Nér65, III] shows that the 'j-pairing' (see 4.4) is bounded and hence $\left|\mathrm{h}^1 - \hat{\mathrm{h}}\right|$ is bounded. Thus we see that $\left|\mathrm{h}^1 - \mathrm{h}^2\right|$ is bounded for points rational over extensions of k of bounded degree.

As a final remark, we consider the case where C/k is a smooth curve, and $\mathscr{C}/\mathcal{O}_k$ is a proper flat model. Suppose we are given $\mathcal{L}$ an ample base point free line bundle on C, and $\mathscr{L}$ is the flat extension to $\mathscr{C}$. Then by [Har77, III Proposition 5.3 p229], we see that $\mathscr{L}$ is ample on $\mathscr{C}$.

3.16 Non-degeneracy of heights

Given a projective arithmetic variety $\mathscr{X}$ and a Hermitian line bundle $\overline{\mathcal{L}}$, it is not clear when the resulting height will be non-degenerate (Definition 3). However, suppose that $\mathcal{L}$ is base point free and that the metric on $\mathcal{L}$ is obtained by pulling back the Fubini-Study metric (or any equivalent metric) along the canonical map $\varphi : \mathscr{X} \to \mathrm{Proj}\left(\mathrm{H}^0\left(\mathscr{X}, \mathcal{L}\right)\right)^\vee$ (after choosing a basis of $\mathrm{H}^0\left(\mathscr{X}, \mathcal{L}\right)$). Then [Sou92, III, Theorem 3] tells us that for all $p \in \mathscr{X}\left(k^{alg}\right)$,

$$\mathrm{h}_{\overline{\mathcal{L}}}(p) = \mathrm{h}_{\overline{\mathcal{O}}(1)}(\varphi(p)). \tag{3.27}$$

As such, finiteness of φ is a necessary and sufficient condition for non-degeneracy of $\mathrm{h}_{\overline{\mathcal{L}}}$. In particular, $\mathrm{h}_{\overline{\mathcal{L}}}$ is non-degenerate if and only if $\mathcal{L}$ is ample; see Theorem 6.

3.17 Several ways to define a height

Suppose $(\mathscr{X}, \mathcal{L})$ is a pair of an arithmetic variety $\mathscr{X}$ and a base point free ample line bundle $\mathcal{L}$ on $\mathscr{X}$. There are four main ways to 'choose' a height on $\mathscr{X}$:

1) Pick a basis s_i of $\mathrm{H}^0\left(\mathscr{X}, \mathcal{L}^\vee\right)$, and use this to pull back the Fubini-Study metric. We then obtain a height as in Section 3.13.

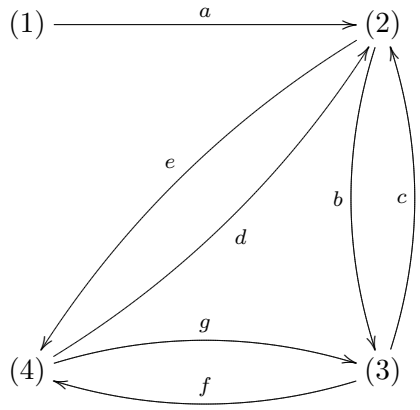
2) Pick a smooth Hermitian metric on $\mathcal{L}$, and apply Section 3.13.

3) Pick a closed differential form $\omega \in \mathscr{A}^{(1,1)}\left(\mathscr{X}_{\Sigma,\mathbb{R}}\right)$ whose cohomology class is that of $\mathcal{L}$. Use this to define a metric on $\mathcal{L}$, and proceed as before.

4) Pick a Green function on a representative of $c_1(\mathcal{L})$. Again, use this to define a metric on $\mathcal{L}$ and proceed as before.

Only method (1) gives us directly a non-degenerate height, but it can be useful to know how to translate between all these approaches. We encode some such information in the following diagram. Numbers refer to the four ways to define a

height given above, and the labeled arrows are ways to get from one description to the other, described below (there is some redundancy in these).



a) Pull back the Fubini-Study metric on $\operatorname{Proj}\left(\mathrm{H}^0\left(X, \mathcal{L}\right)\right)^\vee$.

b) Set $\omega = c_1(\overline{\mathcal{L}})$.

c) This is [CL09, Proposition 2.4.13].

d) This is [CL09, Proposition 2.4.14].

e) Pick a regular meromorphic section s of $\mathcal{L}$, then $\log\left(\|s\|^{-1}\right)$ is a Green current for $\operatorname{div}(s)$.

f) A Green function g_z is determined by the formula $\mathrm{d}\,\mathrm{d}^c\, g_z = \omega + \delta_z$; it exists by arrows (c) and (e).

g) Set $\omega = \mathrm{d}\,\mathrm{d}^c\, g_z - \delta_z$.

3.18 Intersections and local decomposition of heights

In this section, we show how to decompose the height function into a sum of local contributions under some weak assumptions, via an intersection pairing.

Let $\mathscr{X}/S$ be an arithmetic variety, D a Cartier divisor on $\mathscr{X}$, and $j : z \hookrightarrow \mathscr{X}$ a prime cycle on $\mathscr{X}$ of dimension 1 such that $D \times_{\mathscr{X}} z$ has dimension zero (if z and D are horizontal, this is equivalent to requiring that they do not meet on the generic fibre of $\mathscr{X}$). Fix a metric $|-|$ on $\mathcal{O}(D)$, and g_z a Green current for z such that $\mathrm{d}\,\mathrm{d}^c\, g_z + \delta_z = j_* j^* c_1\left(\overline{\mathcal{O}(D)}\right)$. For $\nu \in M_k^0$, define

$$\iota_\nu\left((D, |-|), z\right) = \sum_p \operatorname{length}_{\mathcal{O}_p}\left(\frac{\mathcal{O}_p}{I_D, I_z}\right) \cdot \left[\kappa(p) : \kappa(\nu)\right], \tag{3.28}$$

where p runs over closed points of $\mathscr{X}$ lying over ν, I_D and I_z are defining ideals

for D and z respectively in $\mathcal{O}_p$, and $\kappa(p)$ and $\kappa(\nu)$ are the residue fields at p and ν respectively. Set

$$\langle\langle (D, |-|), z\rangle\rangle_\nu = \iota_\nu\left((D, |-|), z\right) \cdot \log(\#\kappa(\nu)). \tag{3.29}$$

Observe this is independent of the choices of metric $|-|$, so we can just write $\iota_\nu(D, z)$ and $\langle\langle D, z\rangle\rangle_\nu$. For Archimedean $\nu \in M_k^\infty$, define

$$\langle\langle (D, |-|), z\rangle\rangle_\nu = \sum_p \log\left((\|t\|(p))^{-1}\right), \tag{3.30}$$

where p runs over the (finite) set of points in z_ν, and t is a regular meromorphic section of $\mathcal{O}(D)$ whose associated divisor is D.

If S is a local scheme,we may instead write $\iota_{\mathscr{X}}$ rather than ι_ν, and similarly for the pairing $\langle\langle -, -\rangle\rangle_\nu$. We set

$$\langle\langle (D, |-|), z\rangle\rangle = \langle\langle (D, |-|), z\rangle\rangle_{\mathscr{X}} = \sum_{\nu \in M_k} \langle\langle (D, |-|), z\rangle\rangle_\nu. \tag{3.31}$$

Proposition 25.

$$\sum_{\nu \in M_k} \langle\langle (D, |-|), z\rangle\rangle_\nu = \widehat{\deg}\left(\pi_{z*} j^* \overline{\mathcal{O}(D)}\right), \tag{3.32}$$

where $\pi_z : z \to S$ is the structure map, and $(S, 0)$ denotes S as an arithmetic cycle on itself with trivial Green current.

Proof. Let $\pi_{\mathscr{X}} : \mathscr{X} \to S$ denote the structure map, and recall that $\pi_{z*} = \pi_{\mathscr{X}*} \circ j_*$. Throughout this proof, t will denote a regular meromorphic section of $\mathcal{O}(D)$ corresponding to D. We prove the above result locally at ν; firstly, for non-Archimedean ν. We have by definition that the Weil divisor on z supported over ν corresponding to $j^*\mathcal{O}(D)$ is given by

$$\sum_p \mathrm{ord}_p\left(j^* t\right) \cdot p, \tag{3.33}$$

where the sum runs over maximal ideals p on z lying over ν. Now since D is Cartier and j is a closed embedding, one sees that

$$\mathrm{ord}_p\left(j^* t\right) = \mathrm{length}_{\mathcal{O}_q}\left(\frac{\mathcal{O}_q}{I_D, I_z}\right) \tag{3.34}$$

where $j(p) = q$, and I_D and I_z are defining ideals for D and z respectively in $\mathcal{O}_q$. A

formal calculation remains:

$$\begin{aligned}
\langle\langle D, z\rangle\rangle_\nu &= \iota_\nu(D, z) \cdot \log(\#\kappa(\nu)) \\
&= \sum_p \operatorname{length}_{\mathcal{O}_p}\left(\frac{\mathcal{O}_p}{I_D, I_z}\right) \cdot [\kappa(p) : \kappa(\nu)] \cdot \log(\#\kappa(\nu)) \\
(\text{by (3.34)}) &= \sum_p \operatorname{ord}_p(j^* t) \cdot [\kappa(p) : \kappa(\nu)] \cdot \log(\#\kappa(\nu)) \\
&= \operatorname{ord}_\nu(\pi_{z*} j^* t) \cdot \log(\#\kappa(\nu))
\end{aligned} \tag{3.35}$$

which is the ν-part of $\widehat{\deg}\left(\pi_{z*} j^* \overline{\mathcal{O}(D)}\right)$.

For Archimedean $\nu \in M_k^\infty$, we see that the corresponding summand of $\widehat{\deg}\left(\pi_{z*} j^* \overline{\mathcal{O}(D)} \cdot (S, 0)\right)$ is given by (sums are over p in z_ν)

$$\begin{aligned}
&\sum_p \int_{X_\nu} \log\left(\|t\|^{-1}\right) \cdot \delta_p \\
&\quad = \sum_p \log\left(\|t\|(p)^{-1}\right) \\
&\quad = \langle\langle (D, |-|), z\rangle\rangle_\nu .
\end{aligned} \tag{3.36}$$

□

Chapter 4

Néron-Tate heights via Arakelov theory

In the preceding chapter we outlined the general theory of Hermitian line bundles on arithmetic varieties and showed how these techniques lead to height pairings. In this chapter we restrict to the case of curves and their Jacobians, and show that with care and the correct choice of metric we can recover the Néron-Tate height. We also give the results of Faltings and Hriljac relating the Néron-Tate height on the Jacobian of a curve to an intersection pairing on the curve itself; this is the key step to allow the efficient computation of heights for curves of large genus, as detailed in the next chapter. Throughout this chapter, A will denote an Abelian variety over a number field k, with Néron model $\mathscr{A}$ over the spectrum S of the integers $\mathcal{O}_k$ of k.

4.1 Néron's approach to heights on Abelian varieties

Recall from Theorem 11 the definition of the Néron-Tate height $\hat{h}_{\mathcal{L}}$ associated to a line bundle $\mathcal{L}$ on A. It is constructed via approximations by heights arising from projective embeddings of A. However, for computations this is not always practical; for example, the Jacobian of a genus 4 curve embedded by 4Θ lives in $\mathbb{P}^{255}$, and is very far from being a complete intersection — its defining ideal needs an extremely large number of (quadratic) generators. So far it has proven impossible to find these generators, let alone the duplication polynomials which would also be needed to obtain heights by this method. No help can be expected from the Kummer variety either; whilst in genera 1 and 2 the Kummer is geometrically far simpler that the Jacobian, and in genus 3 it is still a little easier to work with, Mumford's work on the equations defining Abelian varieties [Mum66] shows that in general we cannot

expect the Kummer to be simpler than the Jacobian.

In [Nér65, III], Néron offers an alternative construction which sidesteps the problem of finding projective embeddings of abelian varieties. We would now describe his approach as 'Arakelov-theoretic', though it should be remembered that his work long predates that of Arakelov, and indeed the modern concept of scheme theory, due to Grothendieck et al.

A decade later, in his address to the International Congress of Mathematicians [Ara75], Arakelov asserted that his intersection theory on arithmetic surfaces 'coincided' with Néron's construction on their Jacobians. Proofs were later provided by Faltings [Fal84] and Hriljac [Hri77] independently; we will say more about them in Section 4.6.

In what follows, we will restrict ourselves to the case of Jacobians of curves rather than arbitrary Abelian varieties. Néron's work does not use that assumption, but it will somewhat shorten the exposition with no loss of utility for our applications.

4.2 Néron's construction

To use the general method of obtaining heights from Hermitian line bundles as described in Section 2.1 to obtain the Néron-Tate height requires two innovations. One, unsurprisingly, is the construction of a special metric on the line bundle $\mathcal{O}_A(\vartheta)$. The other relates to how one associates to a k-point of A a cycle on $\mathscr{A}$; it turns out that simply taking the Zariski closure is insufficient. This is presented as a 'correction term' to the height pairing one obtains by just taking the Zariski closure, and is usually denoted with the symbol 'j'.

4.3 Choice of metric on $\mathcal{O}(\vartheta)$

From the diagram in Section 3.17 we see that to define a height it suffices to write down a Green current (in fact function) for the ϑ-divisor. That the Green function given below defines the Néron-Tate height is ensured by its Chern form. Fixing a complex embedding σ of the ground field, we view A_σ as a complex torus. We have a quotient map $\pi : \mathbb{C}^g \to A_\sigma$. The theta function $\theta : \mathbb{C}^g \to \mathbb{C}$ descends to a meromorphic function on A_σ. Then there exists a unique Hermitian form $h : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ such that

$$g_\vartheta(z) \stackrel{\text{def}}{=} \log|\theta(z)| - h(z,z) \tag{4.1}$$

on $\mathbb{C}^g$ descends to a smooth function on A_σ outside the support of ϑ (for proofs of the above assertions, see [Nér65, III]).

Proposition 26. *$g_\vartheta(z)$ is a Green function for the divisor ϑ, with chern form $\mathrm{d}\,\mathrm{d}^c\, h(z,z)$.*

Proof. The Poincare-Lelong formula [CL09, Proposition 2.4.7] shows

$$\mathrm{d}\,\mathrm{d}^c \log|\theta(z)| = -\delta_{\mathrm{div}(\theta)} = -\delta_\vartheta. \tag{4.2}$$

It is clear that $\mathrm{d}\,\mathrm{d}^c\, h(z,z)$ is a smooth differential form on $\mathbb{C}^g$. The quotient $\pi : \mathbb{C}^g \to A_\sigma$ is locally an isomorphism, and so $\mathrm{d}\,\mathrm{d}^c\, g_\vartheta(z) = -\delta_\vartheta - \omega$, ω a smooth differential form on A_σ. □

We can translate and sum the g_ϑ to obtain Green functions for any expression in ϑ-translates.

4.4 The correction term 'j'

We recall the definition of j from [Nér65, III]. We also introduce a local version of the term. Let $X \in \mathrm{Div}(A)$ and $p \in \mathscr{A}(S)$. Firstly, we consider the case where X is principal.

Definition 27. *Say $X = \mathrm{div}_A(f)$ for some f in the function field $FF(A) = FF(\mathscr{A})$. Then for $\nu \in M_k^0$ set*

$$j_\nu(X, p-e) \stackrel{def}{=} \langle\!\langle \mathrm{div}_{\mathscr{A}}(f)|_{fib}, p-e \rangle\!\rangle_\nu\,, \tag{4.3}$$

and

$$j(X, p-e) \stackrel{def}{=} \langle\!\langle \mathrm{div}_{\mathscr{A}}(f)|_{fib}, p-e \rangle\!\rangle_{\mathscr{A}} = \sum_{\nu \in M_k} j_\nu(X, p-e). \tag{4.4}$$

where $\langle\!\langle -, - \rangle\!\rangle$ is the pairing defined in Section 3.18, and $\mathrm{div}_{\mathscr{A}}(f)|_{fib}$ is by definition equal to

$$\sum_Y Y\, \mathrm{ord}_Y(f) \tag{4.5}$$

as Y runs over fibral prime divisors of $\mathscr{A}$.

We then generalise to the case of X algebraically equivalent to zero.

Definition 28. *Say $X \sim_{alg} 0$. Then there exists $q \in \mathscr{A}(S)$ and $f \in FF(A)$ such that $X = \vartheta_q - \vartheta + \mathrm{div}_A(f)$. Letting C_T denote the cardinality of the component group*

of $\mathscr{A}_\nu$, the Theorem of the Square [Mum08, p59] tells us that there exists $g \in FF(A)$ such that $c_T \cdot \vartheta_q - \vartheta_{c_T \cdot q} - (c_T - 1) \cdot \vartheta = \mathrm{div}_A(g)$. Then we set

$$j_\nu(X, p - e) \stackrel{def}{=} j_\nu(\mathrm{div}_A(f), p - e) + \frac{1}{c_T} j_\nu(\mathrm{div}_A(g), p - e). \tag{4.6}$$

and similarly

$$j(X, p - e) \stackrel{def}{=} j(\mathrm{div}_A(f), p - e) + \frac{1}{c_T} j(\mathrm{div}_A(g), p - e) = \sum_{\nu \in M_k} j_\nu(X, p - e). \tag{4.7}$$

Finally, we can reduce the case of arbitrary X to that of X algebraically equivalent to zero:

Definition 29. *For any divisor X, we have that $X - (X^-)_p \sim_{alg} 0$. Then set*

$$j_\nu(X, p - e) \stackrel{def}{=} \frac{1}{2} j_\nu(X - (X^-)_p, p - e), \tag{4.8}$$

and

$$j(X, p - e) \stackrel{def}{=} \frac{1}{2} j(X - (X^-)_p, p - e) = \sum_{\nu \in M_k} j_\nu(X, p - e). \tag{4.9}$$

We also recall the useful result:

Proposition 30. *[Nér65, III, 3, Proposition 2, ii] For a fixed divisor X on A, the value of $j_\nu(X, p - e)$ depends only on the connected component of $\mathscr{A}_\nu$ containing p_ν.*

Remark 31. *It is not hard to see that $j_\nu(X, p - e) = 0$ if p reduces to the connected component of the identity modulo ν. In particular, $j_\nu(X, p - e) = 0$ if ν is prime of good reduction.*

4.5 Definition of the Néron-Tate height

We are now in a position to give the definition of the Néron-Tate height on the Jacobian of a curve with respect to the ϑ-divisor.

Definition 32. *As always, let C be a pointed curve over a number field k, and let A denote its Jacobian. For a point $p \in A(k)$ we define the **Neŕon-Tate height** of p by*

$$\hat{h}_\vartheta(p) = h_{\overline{\vartheta}}(p) + j(\vartheta, \overline{p} - e_{\mathscr{A}}) \tag{4.10}$$

where $\overline{p}$ denotes the Zariski closure of p in $\mathscr{A}$ and $h_{\overline{\vartheta}}(p)$ denotes the height of p with respect to the line bundle associated to ϑ with metric as in Section 4.3; see Section 3.13 for the definition of this.

The Néron-Tate height is in fact a special case of a pairing between divisors D on $\mathscr{A}_\eta$ and degree-zero zero cycles. We present the definition in the case where D is a sum of translates of the theta divisor, but it can easily be extended to arbitrary divisors.

Definition 33. *Let $D = \sum_{i=1}^{n} \vartheta_{q_i}$, where q_i are points in $\mathscr{A}(k)$. Let $p_i, \ldots, p_m \in \mathscr{A}(k)$. We fix a metric on $\mathcal{O}_{\mathscr{A}}(D)$ from Section 4.3, and define*

$$\left(D, \sum_i p_i - me_A\right) = \left\langle\left\langle D, \sum_i p_i - me_A \right\rangle\right\rangle + j(D, \sum_i \overline{p_i} - me_{\mathscr{A}}). \tag{4.11}$$

4.6 Connection to the intersection pairing on the curve

In this section we recall the result, due to Faltings [Fal84] and Hriljac [Hri77], relating the Néron-Tate height pairing on the Jacobian of a curve to the self-intersection of a Hermitian line bundle on the curve itself.

We begin by recalling the definition of the canonical Green function associated to a divisor on a curve. Using the diagram in Section 3.17, it is equivalent to define the canonical volume form on the curve, from which the Green functions can be obtained. For this we follow [Lan88, II, Section 2]:

Definition 34. *Let C be a smooth connected curve of genus $g > 0$ over a number field k. Fix a complex embedding σ of k. Viewing C_σ as a Riemann surface, we define a Hilbert space structure on the space of regular differentials on C_σ (differentials of the first kind) by*

$$(\varphi_1, \varphi_2) \mapsto \frac{\sqrt{-1}}{2} \int_{C(\mathbb{C})} \varphi_1 \wedge \overline{\varphi_2}. \tag{4.12}$$

Let $\varphi_0, \ldots, \varphi_{g-1}$ be an orthonormal basis for this space. We then define the canonical volume form on C_σ to be

$$\varphi \stackrel{def}{=} \frac{\sqrt{-1}}{2g}(\varphi_0 \wedge \overline{\varphi_0} + \cdots + \varphi_{g-1} \wedge \overline{\varphi_{g-1}}). \tag{4.13}$$

Lang checks that this is indeed a volume form. We have $\int_{C_\sigma} \varphi = 1$ by definition of an orthonormal basis.

The main result of Faltings and Hriljac can now be stated:

Theorem 35. *[Fal84],[Hri77] Let C be a smooth connected pointed curve of genus $g > 0$ over a number field k with integers $\mathcal{O}_k$, with Jacobian A/k and proper minimal*

regular model $\mathscr{C}/\operatorname{Spec}(\mathcal{O}_k)$. *Let* $p \in A(k)$, *and let* $D \in \operatorname{Div}(C)$ *be a degree-zero divisor such that* $p = [\mathcal{O}(D)]$. *Let* $\widetilde{D}$ *be a divisor on* $\mathscr{C}$ *such that:*

1) $\widetilde{D}_\eta = D$.

2) For each finite place ν *of* $\mathcal{O}_k$ *and each divisor* F *on* $\mathscr{C}$ *supported over* ν, *we have* $\widetilde{D} \cdot F = 0$.

Let $\widehat{\mathcal{O}(\widetilde{D})}$ *denote the Hermitian line bundle whose underlying line bundle is* $\mathcal{O}(\widetilde{D})$ *and whose metric arises from the canonical volume form on* C. *Let* $(\widetilde{D}, g_{\widetilde{D}})$ *be the corresponding arithmetic cycle. Then*

$$-\widehat{\deg}\left(\pi_*\left(\widehat{\mathcal{O}(\widetilde{D})} \cdot (\widetilde{D}, g_{\widetilde{D}})\right)\right) = \hat{h}_\vartheta(p). \tag{4.14}$$

The left hand side is more commonly written as 'minus the self intersection of $\widetilde{D}$'.

Proofs are given in [Fal84] and [Hri77]. Faltings' proof is elegant and conceptual, and obtains the result as a corollary of a deeper arithmetic Riemann-Roch theorem, itself resulting from consideration of volumes on cohomology. However, there are two drawbacks to Faltings' approach:

1) He assumes and makes essential use of semi-stability of the model of C, which is acceptable for some theoretical purposes because of the semistable reduction theorem [BLR90, 9, Theorem 7] due to Deligne-Mumford/Artin-Winters. However, in practice this assumption is not convenient.

2) Since both sides of the equality proven in the theorem are quadratic, it suffices to show that their difference is dominated by a linear form, which Faltings deduces from his Riemann-Roch Theorem. However, this does not make it clear how the various terms in Néron's and Arakelov's pairings match up.

In contrast, Hriljac adopts a slow and arduous approach, explicitly pulling back each term in Néron's pairing to show that it agrees with a corresponding term in Arakelov's. This takes up the first 91 pages of his thesis, in contrast with Faltings 22 pages for the same result. However, for our purposes Hriljac's approach has several advantages:

1) He does not assume semistability.

2) He shows that the model $\mathscr{C}$ does not need to be minimal.

3) He shows clearly how the pairings match up, comparing intersections, correction terms and the analytic part.

4.7 Local decomposition of pairings

We can decompose the 'self-intersection' term of Theorem 35 into a sum of local terms in a similar fashion to Section 3.18, and we benefit again from a lightening of notation.

Fix a maximal ideal ν of $\mathcal{O}_k$. We begin by defining a map Φ_ν from $\mathrm{Div}^0(C)$ to the group of fibral divisors on $\mathscr{C}$ supported over ν, modulo multiples of the whole fibre $\mathscr{C}_\nu$. We set $\Phi_\nu(D)$ to be the unique class of fibral divisors such that for all fibral divisors Y on $\mathscr{C}$ supported over ν, we have $\iota_\nu\left(D + \Phi_\nu(D), Y\right) = 0$. That this is well-defined is proven in [Lan88]. Now given D, $E \in \mathrm{Div}^0(C)$ with disjoint support, set

$$\begin{aligned} \langle D, E\rangle_\nu &= \log|\kappa(\nu)| \cdot \iota_\nu\left(D + \Phi_\nu(D), E\right) \\ &= \log|\kappa(\nu)| \cdot \iota_\nu\left(D + \Phi_\nu(D), E + \Phi_\nu(E)\right). \end{aligned} \tag{4.15}$$

For Archimedean $\nu \in M_k^\infty$, set $\langle D, E\rangle_\nu = \sum g_p(q)$ where the sum is over $p \in D$, $q \in E$ with multiplicity, and g_p is the canonical Green function associated to the divisor p on C.

Combining Section 3.18 and Theorem 35, and choosing $D' \in \mathrm{Div}^0(C)$ linearly equivalent to and disjoint from D, we have

$$\hat{h}_\vartheta([\mathcal{O}(D)]) = -\sum_{\nu \in M_k} \left\langle D, D'\right\rangle_\nu. \tag{4.16}$$

Chapter 5

Computing the canonical height of a point on a hyperelliptic Jacobian

The problem considered in this chapter is that of computing the Néron-Tate (or canonical) height of a point on the Jacobian of a curve of genus greater than 3. As discussed in Chapter 1, for curves of genus 1 and 2 the existing methods (classical in genus 1, and due to Flynn, Smart, Cassels and others in genus 2 [CF96] and [FS97]) make use of explicit equations for projective embeddings of Jacobians, and have proven to be very successful in practice. In adddition, recent work of Stoll [Sto12] has shown that these techniques can be extended to the genus 3 case. It does not seem practical at present to give explicit equations for Jacobians of curves of genus 4 and above, let alone to use these to compute heights. We propose an alternative approach to computing the Néron-Tate height based on Arakelov theory. To demonstrate that our method is practical, we give numerical examples where we compute heights of points on Jacobians of hyperelliptic curves of genus $1 \leq g \leq 9$. We recall from Chapter 1 that such computations have numerous practical applications.

5.1 Choice of curves

Whilst the theoretical sections of this chapter (and indeed, much of the remainder of this thesis) are largely independent of the curve chosen, the very geometric nature of Arakelov theory means that the details of the algorithm, and especially its implementation, will depend greatly on the geometry of the curve considered. Let C be a curve defined over a number field k. Our method makes a number of computational

assumptions:

(a) We have a uniform and convenient way of representing divisor classes on the curve C.

(b) We are able to rigorously compute abelian integrals on C to any required (reasonable) precision.

(c) We are able to write down a regular proper model $\mathscr{C}$ for C over the integers $\mathcal{O}_k$ (though this need not be minimal).

(d) For each non-Archimedean place ν that is a prime of bad reduction for $\mathscr{C}$, we are able to compute the intersection matrix of the special fibre $\mathscr{C}_\nu$.

(e) We have a way of computing Riemann-Roch spaces of divisors on C.

Assumptions (a) and (b) cause us to restrict our attention to hyperelliptic curves. The computer algebra package `MAGMA` [BCP97] has in-built commands to deal with all of these for hyperelliptic curves over number fields. For (a), it uses Mumford's representation (see Section 2.3.4) for divisor classes. A `MAGMA` implementation by P. van Wamelen is used for integral computations in (b); this does not use the usual numerical integration techniques as these are inherently non-rigorous; instead, hyperelliptic functions are locally approximated by truncated power series and formally integrated. The computation of the intersection matrices of the special fibres at the bad places is produced by `MAGMA` as by-product of the computation of the regular proper model, implemented by S. Donnelly using techniques as in [Liu02, Chapter 8]. For computing Riemann-Roch spaces, `MAGMA` makes use of the method of Hess [Hes].

In order to simplify the exposition, we restrict our attention to curves with a rational Weierstrass point. As such, unless otherwise stated, C will denote an odd-degree hyperelliptic curve over a number field k, and $\mathscr{C}$ a proper regular—though not necessarily minimal—model of C over the integers $\mathcal{O}_k$.

5.2 A Formula of Faltings and Hriljac

As before C is an odd degree hyperelliptic curve over a number field k. We fix once and for all the following notation:

- M_k a proper set of places of k;
- M_k^0 the subset of non-Archimedean places of k;

- M_k^∞ the subset of Archimedean places of k;
- $\kappa(\nu)$ the residue field at a $\nu \in M_k^0$;
- ι_ν the usual intersection pairing between divisors over $\nu \in M_k^0$ (see [Lan88, IV,§1]).

We recall from Section 4.7 the following result:

Theorem 36. *(Faltings and Hriljac) Let D be a degree zero divisor on C, and let E be any divisor linearly equivalent to D but with disjoint support. Then the height of the point on $\mathrm{Jac}(C)$ corresponding to D is given by*

$$\hat{h}_\vartheta\left(\mathcal{O}(D)\right) = -\sum_{\nu \in M_k^0} \log|\kappa(\nu)|\, \iota_\nu\left(\overline{D} + \Phi(D), \overline{E}\right) - \frac{1}{2}\sum_{\nu \in M_k^\infty} g_{D,\nu}(E)$$

where Φ and $g_{D,\nu}$ are defined as follows:

- Φ sends a divisor on the curve C to an element of the group of fibral $\mathbb{Q}$-divisors on $\mathscr{C}$ with order zero along the irreducible component containing infinity, such that for any divisor D on C (with Zariski closure $\overline{D}$) and fibral divisor Y on $\mathscr{C}$, we have $\iota_\nu\left(\overline{D} + \Phi(D), Y\right) = 0$ (this is a slight change of normalisation from that given in Section 4.7; we will use it for the remainder of this chapter).

- $g_{D,\nu}$ denotes a Green function for the divisor D, when C is viewed as a complex manifold via the embedding ν.

Our strategy for computing the Néron-Tate height of a degree zero divisor D using the above formula is as follows:

1. Determine a suitable divisor E as above. This is explained in Section 5.3.
2. Determine a finite set $\mathfrak{R} \subset M_k^0$ such that for non-Archimedean places ν **not** in $\mathfrak{R}$, we have $\iota_\nu\left(\overline{D} + \Phi(D), \overline{E}\right) = 0$. This is explained in Section 5.4.
3. Determine $\iota_\nu\left(\Phi(D), \overline{E}\right)$ for $\nu \in \mathfrak{R}$. This is explained in Section 5.5.
4. Determine $\iota_\nu\left(\overline{D}, \overline{E}\right)$ for $\nu \in \mathfrak{R}$. This is explained in Section 5.6.
5. Compute the Green function $g_{D,\nu}(E)$ for Archimedean ν. This is explained in Section 5.7.

In the final section we give a number of worked examples.

By a straightforward Riemann-Roch computation, we can write down a divisor in Mumford form that is linearly equivalent to D. We replace D by this

Mumford divisor. Thus we may suppose that $D = D' - d \cdot \infty$ where $d \leq g$ and $D' = \text{zeros}\,(a(x), y - b(x))$ with $a(x),\ b(x) \in k[x]$ satisfying certain conditions as given in [MM84, 3.19, Proposition 1.2].

5.3 Step 1: Choosing E

If the support of D' does not contain Weierstrass points, choose a $\lambda \in k$ such that $a(\lambda) \neq 0$, and set

$$E = \text{inv}(D') - \frac{d}{2}\,\text{zeros}\,(x - \lambda)\,, \tag{5.1}$$

where inv denotes the hyperelliptic involution. If d is odd, this is not a divisor but a $\mathbb{Q}$-divisor. This is unimportant, but if the reader is troubled he or she should multiply E by 2, and then appeal to the quadraticity of the height.

If the support of D' does contain Weierstrass points, either:

a) replace D by a positive multiple of itself to avoid this, or

b) add a divisor of order 2 to D to remove them.

(a) is simpler to implement, (b) generally faster computationally.

Now $E \sim_{\text{lin}} -D$, and so

$$\hat{h}_\vartheta\left(\mathcal{O}(D)\right) = \sum_{\nu \in M_k^0} \log|\kappa(\nu)|\,\iota_\nu\left(\overline{D} + \Phi(D), \overline{E}\right) + \frac{1}{2}\sum_{\nu \in M_k^\infty} g_{D,\nu}(E).$$

This is seen by viewing the expression on the right hand side as the global Néron pairing on divisor classes, which is a quadratic form; since E is linearly equivalent to $-D$ a minus sign results, which cancels with those in Theorem 36 to yield the above expression.

5.4 Step 2: Determining a Suitable $\mathfrak{R}$

We wish to find a finite set $\mathfrak{R} \subset M_k^0$ such that

$$\iota_\nu\left(\overline{D} + \Phi(D), \overline{E}\right) = 0 \tag{5.2}$$

for all $\nu \notin \mathfrak{R}$. To make this as general as possible, we will for the moment just assume C is a smooth curve over k in the weighted projective space $\mathbb{P}_k(a_0, \ldots, a_n)$. Let C' denote its closure in $\mathbb{P}_{\mathcal{O}_k}(a_0, \ldots, a_n)$. Let Q_1 denote the set of places of bad reduction for C', outside which C' is smooth over $\mathcal{O}_k$.

It suffices to solve our problem for prime divisors, as we can then obtain results for general D and E easily. Let X and Y be prime divisors on C, and let d be

the degree of Y. Let $H_1, \ldots, H_{d+1}$ be a collection of weighted integral homogeneous forms of degrees $e_1, \ldots, e_{d+1} > 0$ on $\mathbb{P}_{\mathcal{O}_k}(a_0, \ldots, a_n)$, geometrically integral on the generic fibre and coprime over k, such that for all pairs $i \neq j$, we have on the generic fibre that $H_i \cap H_j \cap C = \emptyset$ (we will confuse H_i with the hypersurface it defines).

Let Q_2 be the set of $\nu \in M_k^0 \setminus Q_1$ such that

$$(\overline{H}_i)_\nu \cap (\overline{H}_j)_\nu \cap C'_\nu \neq \emptyset$$

for some $1 \leq i,\, j \leq d+1$. Note that $\overline{H}_i \cap \overline{H}_j$ is a zero-dimensional scheme, and so is easy to compute in practice.

Let $FF(Y)$ denote the function field of Y, a finite extension of k, and let $\mathrm{N}_Y : FF(Y) \to k$ denote the norm map. In practice, we can use Gröbner bases to find an isomorphism $FF(Y) \xrightarrow{\sim} k[t]/\alpha(t)$, and so can readily compute N_Y.

Let Q_3 be the set of $\nu \in M_k^0 \setminus (Q_1 \cup Q_2)$ such that

$$\mathrm{ord}_\nu \left(\mathrm{N}_Y \left(H_i^{e_{i+1}} / H_{i+1}^{e_i} \right) \right) \neq 0$$

for some $1 \leq i \leq d$; while Q_2 detects common points of intersection of $\overline{H}_i$, $\overline{H}_j$ and C' over ν, Q_3 detects when the intersection numbers of $\overline{H}_i^{e_i+1}$ and $\overline{H}_{i+1}^{e_i}$ with Y over ν are different.

Let $f_1, \ldots, f_r$ be integral weighted homogeneous equations for X such that no f_i vanishes on Y, and set $\deg(f_j) = d_j$. Finally let Q_4 be the set of $\nu \in M_k^0 \setminus (Q_1 \cup Q_2 \cup Q_3)$ such that

$$\mathrm{ord}_\nu \left(\mathrm{N}_Y \left(f_j^{e_1} / H_1^{d_j} \right) \right) \neq 0$$

for some $1 \leq j \leq r$.

Lemma 37. *Set*

$$\mathfrak{R} = Q_1 \cup Q_2 \cup Q_3 \cup Q_4.$$

If $\nu \notin \mathfrak{R}$ *then* $\iota_\nu \left(\overline{X} + \Phi(X), \overline{Y} \right) = 0$.

Proof. Outside Q_1, C' is smooth over $\mathcal{O}_k$, and hence it is regular and all its fibres are geometrically integral. As a result,

$$\iota_\nu \left(\overline{X} + \Phi(X), \overline{Y} \right) = \iota_\nu \left(\overline{X}, \overline{Y} \right) \text{ for } \nu \notin \mathfrak{R}. \tag{5.3}$$

Suppose $\iota_\nu \left(\overline{X}, \overline{Y} \right) \neq 0$, so $(\overline{X})_\nu \cap (\overline{Y})_\nu \neq \emptyset$. We will show $\nu \in \mathfrak{R}$.

Recall that X and Y are cycles on C' of relative dimension zero over $\mathcal{O}_k$, and so their fibres over closed points are cycles of dimension zero. Observe that,

since the f_j are integral, we must have $\text{zeros}\,(f_j) \supset \overline{X}$ for all j. Hence there is some j_0 such that f_{j_0} vanishes on some irreducible component of (equivalently, closed point in) $(\overline{Y})_\nu$ (in fact, this holds for any j_0). As a result, $\iota_\nu\left(\text{zeros}_{C'}\left(f_{j_0}\right), \overline{Y}\right) > 0$, since we assume $\text{zeros}_{C'}\left(f_{j_0}\right)$ and $\overline{Y}$ have disjoint support on the generic fibre. Now suppose $\nu \notin \mathfrak{R}$. Then for all i, since $\nu \notin Q_4$, we must have

$$\text{ord}_\nu\left(\text{N}_Y\left(f_{j_0}^{e_i}/H_i^{d_{j_0}}\right)\right) = 0.$$

Hence by [Lan88, III, Lemma 2.4, p56], we see that for all i,

$$0 = \iota_\nu\left(\text{div}_{C'}\left(\frac{f_{j_0}^{e_i}}{H_i^{d_{j_0}}}\right), \overline{Y}\right) = e_i \cdot \iota_\nu\left(\text{zeros}_{C'}\left(f_{j_o}\right), \overline{Y}\right) - d_{j_0} \cdot \iota_\nu\left(\text{zeros}_{C'}\left(H_i\right), \overline{Y}\right).$$

Now as $e_i > 0$ and $d_{j_0} > 0$, we see that for all i,

$$\iota_\nu\left(\text{zeros}_{C'}\left(H_i\right), \overline{Y}\right) > 0, \tag{5.4}$$

so every $\text{zeros}_{C'}\left(H_i\right)$ meets $\overline{Y}$. But the zero-dimensional cycles $\text{zeros}_{C'}\left(H_i\right) \cap \overline{Y}$ are pairwise disjoint since $\nu \notin Q_2$, and $\deg(Y) = \deg((\overline{Y})_\nu) = d$. Moreover, $\nu \notin Q_3$ shows that the $(d+1)$ cycles $\text{zeros}\,(H_i) \cap \overline{Y}$ are disjoint, and so cannot all meet the zero-dimensional cycle $(\overline{Y})_\nu$ as it has degree d; this contradicts Equation 5.4, and so we are done. □

5.5 Step 3: Determining $\iota_\nu\left(\Phi(D), \overline{E}\right)$

We next discuss the computation of the term $\iota_\nu\left(\Phi(D), \overline{E}\right)$ for a non-Archimedean place ν. Recall that by our assumptions in Section 5.1 we are able to write down a proper regular model $\mathscr{C}$ and the intersection matrix for $\mathscr{C}_\nu$ for all bad places ν. Clearly $\iota_\nu\left(\Phi(D), \overline{E}\right)$ vanishes if $\mathscr{C}_\nu$ is integral, in particular if ν is a good prime. Suppose ν is a bad prime. Since we have the intersection matrix of $\mathscr{C}_\nu$, we can easily compute both $\Phi(D)$ and $\iota_\nu\left(\Phi(D), \overline{E}\right)$ from the definition of Φ if we can solve the following:

Problem 38. *Given a finite place ν, a horizontal divisor X and a prime fibral divisor Y over ν, compute $\iota_\nu(X, Y)$.*

We may replace the base space $S = \text{Spec}(\mathcal{O}_k)$ by its completion $\hat{S}$ at ν ([Lan88, III, Proposition 4.4, page 65]), and we may further assume that X is a prime horizontal divisor on $\mathscr{C} \times_S \hat{S}$. By Lemma 39 below, this means that the support

of X_ν is a closed point of $\mathscr{C}_\nu$, and so we can find an affine open neighbourhood $U = \mathrm{Spec}(A)$ of X_ν in $\mathscr{C} \times_S \hat{S}$.

Lemma 39. *If X is a prime horizontal divisor on $\mathscr{C} \times_S \hat{S}$, then the support of X_ν is a prime divisor on $\mathscr{X}_\nu$ (in other words, X_ν is irreducible but not necessarily reduced).*

Proof. There exists a number field L and an order R in L such that X is isomorphic to $\mathrm{Spec}(R)$. Write $L = k[t]/\alpha(t)$, where α monic and irreducible with integral coefficients. Let κ denote the residue field of k, and $\overline{\alpha}$ the image of α in $\kappa[t]$. If X_ν is not irreducible, then there exist f, $g \in \kappa[t]$ coprime monic polynomials such that $f \cdot g = \overline{\alpha}$. This factorization of $\overline{\alpha}$ lifts to a factorization of α by Hensel's Lemma. □

Now it is easy to check whether $X_\nu \cap Y = \emptyset$; if so, $\iota_\nu(X, Y) = 0$. Further, if $X_\nu \subset Y$ and X_ν is not contained in any other fibral prime divisor, then $\iota_\nu(X, Y) = \deg(X)$; this is easily seen since locally $Y = \mathrm{zeros}_U(\nu)$, and we can take the norm of ν from the field of fractions $FF(X)$ down to k.

We are left with the case where X_ν lies at the intersection of several fibral prime divisors. Recall that X is assumed to be horizontal. We find equations $\overline{f}_1, \ldots, \overline{f}_r \in A \otimes_{\mathcal{O}_k} \kappa(\nu)$ for Y as a subscheme of U_ν. Then choose any lifts f_i of $\overline{f}_i$ to A. Now we need two easy results in commutative algebra:

Lemma 40. *let R be a ring, $p \in R$ any element, and I an ideal containing p. Suppose we have $t_1, \ldots, t_r \in R$ such that the images $\bar{t}_1, \ldots, \bar{t}_r$ in $R/(p)$ generate the image of I in $R/(p)$. Then $I = (t_1, \ldots, t_r, p)$.*

Proof. Let $x \in I$. Write $\overline{x}$ for the image of x in $R/(p)$, and write $\overline{x} = \sum_{i=1}^r \overline{\alpha}_i \bar{t}_i$ for some $\overline{\alpha} \in R/(p)$. Choose lifts α_i of $\overline{\alpha}_i$ to R. Then $y \stackrel{\text{def}}{=} x - \sum_{i=1}^r \alpha_i t_i$ has the property that $y \in p \cdot R$. Hence x is in $(t_i, \ldots, t_r, p)$ and so $I \subset (t_1, \ldots, t_r, p)$. Now $p \in I$ by assumption, and $\bar{t}_i \in I/(p)$, so there exists g_i in I such that $g_i - t_i \in p \cdot R$, so $t_i \in I$. □

Lemma 41. *Let R be a regular local ring, and $t_1, \ldots, t_r \in R$ be such that $I \stackrel{def}{=} (t_1, \ldots, t_r)$ is a prime ideal of height 1. Now I is principal; write $I = (t)$. Then there exists an index i and a unit $u \in R$ such that $t_i = tu$. In particular, there exists an index i with $I = (t_i)$.*

Proof. R is a unique factorization domain, and so f For each i we can write $t_i = t_i' t$ for some $t_i' \in R$. Hence $I = t \cdot (t_1', \ldots, t_r')$, and $(t_1', \ldots, t_r') = 1$. We want to show some t_i' is a unit. Suppose not; then since A is local, all the t_i' lie in the maximal ideal, so $(t_1', \ldots, t_r')$ is contained in the maximal ideal, a contradiction. □

Now from these we see that one of the f_i or ν must be an equation for Y in a neighbourhood of X_ν (and it cannot be ν as X_ν lies on an intersection of fibral primes). Now if any f_i vanishes on X_ν, it cannot be the f_i we seek. Exclude such f_i, and then for each of the remaining f_i compute its norm from $FF(X)$ to the completion of k. The minimum of the valuations of such norms will be achieved by any f_i which is a local equation for Y at X_ν, and hence $\iota_\nu(Y, X)$ is equal to the minimum of the valuations of the norms.

5.6 Step 4: Determining $\iota_\nu\left(\overline{D}, \overline{E}\right)$

Finally, we come to what appears to be the meat of the problem for non-Archimedean places: given two horizontal divisors D and E and a place $\nu \in \mathfrak{R}$, compute the intersection $\iota_\nu\left(\overline{D}, \overline{E}\right)$. However, the techniques used in previous sections actually make this very simple.

Fix a non-Archimedean place ν. Let $\hat{S}$ denote the ν-adic completion of S, and set $\hat{\mathscr{C}} = \mathscr{C} \times_S \hat{S}$. It is sufficient to compute the intersection $\iota_\nu(X, Y)$ where X and Y are prime horizontal divisors on $\hat{\mathscr{C}}$; in particular (by the lemma above), the supports of X_ν and Y_ν are closed points of $\mathscr{C}_\nu = \hat{\mathscr{C}}_\nu$

Now if $\mathrm{Supp}(X_\nu) \neq \mathrm{Supp}(Y_\nu)$, then $\iota_\nu(X, Y) = 0$. Otherwise, let $U = \mathrm{Spec}(A)$ be an affine open neighbourhood of $\mathrm{Supp}(X_\nu)$. Let $f_1, \ldots, f_r$ generate the ideal of X on U; then by Lemma 41 we know that some f_i generates the ideal of X in a neighbourhood of X_ν. If f_j vanishes on Y, we can throw it away. We obtain

Proposition 42.

$$\iota_\nu(X, Y) = \min_i \left(\mathrm{ord}_\nu\left(f_i[Y]\right)\right)$$

as i runs over $\{1, \ldots, r\}$ such that f_i does not vanish identically on Y_ν. Here $f[Y]$ is defined to be either

1. *the norm from $FF(Y)$ to the completion of k of the image of f_i in $FF(Y)$, or, equivalently,*
2. *$\prod_j f_i(p_j)^{n_j}$ where $Y = \sum_j n_j p_j$ over some finite extension l/k (see [Lan88, II,§2, page 57]).*

Proof. If f_i is not identically zero on Y_ν, then $\mathrm{zeros}_{\hat{\mathscr{C}}}(f_i)$ and Y have no common component and moreover f_i is regular on a neighbourhood of Y so

$$\iota_\nu\left(\mathrm{poles}_{C'}(f_i), Y\right) = 0, \tag{5.5}$$

and so [Lan88, II, Lemma 2.4, p56] shows that

$$\iota_\nu\left(\text{zeros}_{\hat{\mathscr{C}}}\left(f_i\right), Y\right) = \text{ord}_\nu\left(f_i[Y]\right). \tag{5.6}$$

Now $\text{zeros}_{\hat{\mathscr{C}}}\left(f_i\right) \geq X$, so $\text{ord}_\nu\left(f_i[Y]\right) \geq \iota_\nu\left(X, Y\right)$. Moreover, by lemma 40 there is an index i_0 such that f_{i_0} generates X near X_ν, and since $X_\nu = Y_\nu$ is irreducible we have that

$$\begin{aligned}\iota_\nu\left(X, Y\right) = \iota_\nu\left(\text{zeros}_{\hat{\mathscr{C}}}\left(f_{i_0}\right), Y\right) &= \sum_p \text{length}_{\mathcal{O}_p}\left(\frac{\mathcal{O}_p}{f_{i_0}, I_Y}\right) \\ &= \text{length}_{\mathcal{O}_{X_\nu}}\left(\frac{\mathcal{O}_{X_\nu}}{f_{i_0}, I_Y}\right)\end{aligned} \tag{5.7}$$

where the sum is over closed points p of $\hat{\mathscr{C}}$ lying over ν, and I_Y is the defining ideal for Y in the local ring under consideration. Now any other f_i will have

$$\iota_\nu\left(\text{zeros}_{\hat{\mathscr{C}}}\left(f_i\right), Y\right) \geq \iota_\nu\left(\text{zeros}_{\hat{\mathscr{C}}}\left(f_{i_0}\right), Y\right), \tag{5.8}$$

so the result follows. □

As regards the computation of the $f_i[Y]$, definitions (1) and (2) given in Proposition 42 lead to slightly different approaches, but both make use of Pauli's algorithms [PR01]. In our implementation, discussed in Section 5.8, we use (2) as it seems easier; however (1) may lead to an implementation that is faster in practice.

5.7 Step 5: Computing $g_{D,\nu}(E)$

Finally, we must compute the Archimedean contribution. Fix for the remainder of this section an embedding σ of k in $\mathbb{C}$ corresponding to a place $\nu \in M_k^\infty$. Let C_σ denote the Riemann surface corresponding to $C \times_{k,\sigma} \mathbb{C}$.

5.7.1 The PDE to be Solved

As a starting point, we take [Lan83, Chapter 13, Theorem 7.2], which we summarise here.

Given a divisor a on C_σ of degree zero, let ω be a differential form on C_σ such that the residue divisor $\text{res}(\omega)$ equals a (such an ω can always be found using the Riemann-Roch Theorem). Normalise ω by adding on holomorphic forms until

the periods of ω are purely imaginary. Let

$$dg_a \stackrel{\text{def}}{=} \omega + \bar{\omega}. \tag{5.9}$$

Then g_a is a Green function for a. Thus it remains to find, normalise and integrate such a form ω.

5.7.2 Application of theta functions to the function theory of hyperelliptic curves

We can use ϑ-functions to solve the partial differential equation (5.9) of Section 5.7.1, in a very simple way. For background on ϑ-functions we refer to the first two books of the 'Tata lectures on theta' trilogy, [Mum83], [MM84]. ϑ-functions are complex analytic functions on $\mathbb{C}^g$ which satisfy some quasi-periodicity conditions, thus they are an excellent source of differential forms on the (analytic) Jacobian of C_σ. To get from this a differential form on C_σ we simply use that C_σ is canonically embedded in $\mathrm{Jac}(C_\sigma)$ by the Abel-Jacobi map, so we can pull back forms from $\mathrm{Jac}(C_\sigma)$ to C_σ.

Fix a symplectic homology basis A_i, B_i on C_σ as in [MM84]; by this we mean that if $i(-,-)$ denotes the intersection of paths, then we require that the A_i, B_i form a basis of $H_1(C_\sigma, \mathbb{Z})$ such that

$$i(A_i, A_j) = i(B_i, B_j) = 0 \text{ for } i \neq j$$

and

$$i(A_i, B_j) = \delta_{ij}.$$

We also choose a basis $\omega_1, \ldots \omega_g$ of holomorphic 1-forms on C_σ, normalised such that

$$\int_{A_i} \omega_j = \delta_{ij}.$$

We recall the definition and some basic properties of the multivariate ϑ-function:

$$\vartheta(z;\Omega) \stackrel{\text{def}}{=} \sum_{\underline{n} \text{ in } \mathbb{Z}^g} \exp(\pi i \underline{n} \Omega \underline{n}^{\mathrm{T}} + 2\pi i \underline{n} \cdot z) \tag{5.10}$$

which converges for z in $\mathbb{C}^g$ and Ω a $g \times g$ symmetric complex matrix with positive definite imaginary part. The ϑ-function satisfies the following periodicity conditions for $\underline{m}, \underline{n}$ in $\mathbb{Z}^g$:

$$\vartheta(z + \underline{m}; \Omega) = \vartheta(z; \Omega), \tag{5.11}$$

$$\vartheta(z + \underline{n}\Omega; \Omega) = \exp(-\pi i \underline{n}\Omega \underline{n}^{\mathrm{T}} - 2\pi i \underline{n} z)\, \vartheta(z; \Omega). \tag{5.12}$$

We will set Ω to be the period matrix of the analytic Jacobian of C_σ with respect to the fixed symplectic homology basis (as in [MM84]), and z will be a coordinate on the analytic Jacobian. This means that

$$\Omega_{ij} = \int_{B_i} \omega_j.$$

Let

$$\delta' \stackrel{\text{def}}{=} \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}, \frac{1}{2}\right) \in \frac{1}{2}\mathbb{Z}^g$$

$$\delta'' \stackrel{\text{def}}{=} \left(\frac{g}{2}, \frac{g-1}{2}, \ldots, 1, \frac{1}{2}\right) \in \frac{1}{2}\mathbb{Z}^g$$

$$\Delta \stackrel{\text{def}}{=} \Omega \cdot \delta' + \delta''.$$

Then [MM84, Theorem 5.3, part 1] tells us that $\vartheta(\Delta - z) = 0$ if and only if there are $P_1, \ldots P_{g-1}$ in C_σ such that

$$z \equiv \sum_{i=1}^{g-1} \int_\infty^{P_i} \underline{\omega} \pmod{\mathbb{Z}^g + \Omega\mathbb{Z}^g}.$$

This is a crucial result which allows us to construct a quasifunction on $\mathrm{Jac}(C_\sigma)$ with prescribed zeros, and from this obtain the Green function we seek.

5.7.3 Solution of the Partial Differential Equation

Let D, D_0 be two effective reduced divisors of degree g on C_σ with disjoint support, containing no Weierstrass points or points at infinity, nor any pairs $p + q$ of points such that $p = \mathrm{inv}(q)$. Then the classes $[\mathcal{O}(D - g \cdot \infty)]$ and $[\mathcal{O}(D_0 - g \cdot \infty)]$ lie outside the ϑ-divisor on the Jacobian; indeed, the association $D \mapsto [\mathcal{O}(D - g \cdot \infty)]$ is an isomorphism from divisors with the above properties to $\mathrm{Jac}(C_\sigma) \setminus \vartheta$, see [MM84, 3.31]. Write $\alpha : \mathrm{Div}(C_\sigma) \to \mathrm{Jac}(C_\sigma)$ for the map sending a divisor E to the class $[\mathcal{O}(E - \deg(E) \cdot \infty)]$.

For z in $\mathrm{Jac}(C_\sigma)$ we set

$$G(z) = \frac{\vartheta(z + \Delta - \alpha(D))}{\vartheta(z + \Delta - \alpha(D_0))}.$$

Then for p in C_σ we set $F(p) = G(\alpha(p))$ so

$$F(p) = \frac{\vartheta(\alpha(p) + \Delta - \alpha(D))}{\vartheta(\alpha(p) + \Delta - \alpha(D_0))}. \tag{5.13}$$

If we let $\omega = d \log F(p)$ then it is clear that $\mathrm{res}(\omega) = D - D_0$. It then remains to normalise ω to make its periods purely imaginary, and then integrate it. We have a homology basis A_i, B_i, and we find:

$$\int_{A_k} \omega = \int_{A_k} d \log F(p) = \log G(\alpha(p) + e_k) - \log G(\alpha(p)) = 0$$

(where $e_k = (0, 0, \ldots 0, 1, 0 \ldots, 0)$ with the 1 being in the k-th position), and

$$\begin{aligned} \int_{B_k} \omega = \int_{B_k} d \log F(p) &= \log G(\alpha(p) + \Omega.e_k) - \log G(\alpha(p)) \\ &= 2\pi i \, e_k^T \cdot (\alpha(D) - \alpha(D_0)). \end{aligned}$$

From this we can deduce that the normalisation is

$$\begin{aligned} \omega = d \log &\left[\frac{\vartheta(\alpha(p) + \Delta - \alpha(D))}{\vartheta(\alpha(p) + \Delta - \alpha(D_0))} \right] \\ &- 2\pi i \left[(\mathrm{Im}(\Omega))^{-1} \, \mathrm{Im}(\alpha(D) - \alpha(D_0)) \right] . \begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_g \end{bmatrix} \end{aligned}$$

where p is a point on C_σ.

Now we integrate to get the Green function $g_{D-D_0}(p) = \int_{\infty_{C_\sigma}}^{p} \omega + \overline{\omega}$, where ∞_{C_σ} denotes the point at infinity on C_σ:

$$g_{D-D_0}(p) = 2\log\left|\frac{\vartheta(\alpha(p)+\Delta-\alpha(D))}{\vartheta(\alpha(p)+\Delta-\alpha(D_0))}\right|$$

$$+ 4\pi\left[(\mathrm{Im}(\Omega))^{-1}\,\mathrm{Im}(\alpha(D)-\alpha(D_0))\right].\mathrm{Im}\left(\int_{\infty_{C_\sigma}}^{p}\begin{bmatrix}\omega_1\\ \omega_2\\ \vdots\\ \omega_g\end{bmatrix}\right)$$

$$= 2\log\left|\frac{\vartheta(\alpha(p)+\Delta-\alpha(D))}{\vartheta(\alpha(p)+\Delta-\alpha(D_0))}\right| + 4\pi(\mathrm{Im}(\Omega))^{-1}\cdot\mathrm{Im}(\alpha(D)-\alpha(D_0))\cdot\mathrm{Im}\left(\alpha(p)\right).$$

Given divisors D, D_0 and E, E_0 containing no Weierstrass points or infinite points or pairs of points which are involutions of each other, and having disjoint support we can this formula to compute $\frac{1}{2}g_{D-D_0}[E-E_0]$ which is simply the sum over points $p \in \mathrm{Supp}(E-E_0)$ of $g(p)$. We are done.

5.8 Examples

We have created a test implementation of the above algorithm in `MAGMA`. The following results were obtained using a 2.50 GHz Intel Core2 Quad CPU Q9300:

First, we let $C/\mathbb{Q}$ be the genus 3 hyperelliptic curve given by

$$C : y^2 = x^7 - 15x^3 + 11x^2 - 13x + 25.$$

Let D, E be the points on the Jacobian corresponding to the degree 0 divisors $(1,3)-\infty$, $E = (0,-5)-\infty$ respectively. We obtain the following:

$$\hat{h}(D) = 1.77668\ldots$$

$$\hat{h}(E) = 1.94307\ldots$$

$$\hat{h}(D+E) = 4.35844\ldots$$

$$\hat{h}(D-E) = 3.08107\ldots$$

$$2\hat{h}(D) + 2\hat{h}(E) - \hat{h}(D+E) - \hat{h}(D-E) = 1.26217 \times 10^{-28}$$

with a total running time of 31.75 seconds. We note that our result is consistent with the parallelogram law for the Néron-Tate height, which provides a useful check that our implementation is running correctly.

Next we give two families of curves of increasing genus. Firstly the family $y^2 = x^{2g+1}+2x^2-10x+11$ with D denoting the point on the Jacobian corresponding to the degree 0 divisor $(1,2)-\infty$ (all times are in seconds unless otherwise stated):

g	$\hat{h}(D)$	time
1	$1.11466\ldots$	1.94
2	$1.35816\ldots$	6.44
3	$1.50616\ldots$	15.10
4	$1.61569\ldots$	32.71
5	$63.4292\ldots$	72.23
6	$1.77778\ldots$	212.37
7	$51.0115\ldots$	20 minutes
8	$1.89845\ldots$	3 hours
9	$78.8561\ldots$	16 hours

Now we consider the family $y^2 = x^{2g+1} + 6x^2 - 4x + 1$ with D denoting the point $(1,2) + (0,1) - 2 \cdot \infty$ on the Jacobian:

g	$\hat{h}(D)$	time/seconds
1	$1.41617\ldots$	2.06
2	$1.37403\ldots$	6.73
3	$1.50396\ldots$	15.62
4	$1.40959\ldots$	32.60
5	$1.70191\ldots$	76.48
6	$1.81093\ldots$	291.17
7	$1.71980\ldots$	1621.50

A fully-functioning and more efficient implementation of Néron-Tate height computations is currently being carried out in `MAGMA` by J. S. Müller, combining ideas from this chapter with those from his own PhD thesis, [Mue10]. Müller's approach to computing $\iota_\nu(D,E)$ is quite different from that used here; he uses Gröbner bases to compute directly the $\mathcal{O}_p$-length of the modules $\frac{\mathcal{O}_p}{I_D+I_E}$ as p runs over closed points of the special fibre, in contrast to the method in this chapter where we compute norms down to the ground field and then compute valuations.

Chapter 6

The difference between the naïve and Néron-Tate heights

In this chapter we give a definition of a naïve height on divisors on a hyperelliptic curve over a number field, and show that this naïve height has computably bounded difference from the Néron-Tate height of the corresponding point on the Jacobian.

Our definition of the height is analogous to the definition of the height of an element of a number field K as

$$\mathrm{h}(x) = \sum_{\nu \in M_K} \log^+ |x|_\nu^{-1} . \tag{6.1}$$

For each place ν of our number field, we will construct a metric d_ν on divisors which measures how far apart they are in the ν-adic topology. We define

$$\mathscr{H}([D]) = \sum_{\nu \in M_K} \log \mathrm{d}_\nu(D, D')^{-1} \tag{6.2}$$

where D' is a specified divisor which is linearly equivalent to $-D$. Since our curve is compact (and our metrics reflect this) there is no need to take $\log^+$; taking log will do.

After setting up these metrics, we will first show how to bound the difference between the distance between two divisors and their local arithmetic intersection pairing at a non-Archimedean place. This will involve bounding the term Φ of Section 4.7, and then comparing distances between divisors and lengths of modules, in Section 6.3. The hardest aspect of this will be allowing for the fact that the model of C obtained by taking the integral closure inside relative projective space is not in general a regular scheme, so we must compute precisely how the process of

resolving its singularities will affect the intersection pairing.

We must then obtain similar bounds at Archimedean places. If the divisors we consider have supports which are not too close together, then we may obtain bounds by using the expressions for Green's functions in terms of theta functions given in Section 5.7.3. We bound the derivatives of these expressions in theta functions which allows us to numerically compute explicit bounds. The case where the divisors in question have supports which are close to one another is somewhat harder, and we cover it in Section 6.5 by finding systematic ways to move the divisors further appart by linear equivalence, and then computing the effect that this moving has on the Green's functions.

6.1 Metrics on $\mathbb{P}^1$ and C

We begin by setting up a collection of metrics.

Definition 43. *Let K be a field of characteristic zero with a norm $|-|$. Let $\mathrm{d}_A : K \times K \to \mathbb{R}$ be given by*

$$\mathrm{d}_A(p,q) = \frac{|p-q|}{(1+|p|)(1+|q|)}. \tag{6.3}$$

Proposition 44. *d_A is a metric on K.*

Proof. Only the triangle inequality is non-obvious. Let p, q and $r \in K$.

$$\begin{aligned} \mathrm{d}_A(p,q) + \mathrm{d}_A(q,r) &= \frac{|p-q|}{(1+|p|)(1+|q|)} + \frac{|q-r|}{(1+|q|)(1+|r|)} \\ &= \frac{|p-q|\,(1+|r|) + |q-r|\,(1+|p|)}{(1+|p|)(1+|q|)(1+|r|)} \\ &\geq \frac{|p-r| + |q|\,|p-r|}{(1+|p|)(1+|q|)(1+|r|)} = \mathrm{d}_A(p,r). \end{aligned} \tag{6.4}$$

□

We note that for all p and $q \in K$, we have $\mathrm{d}_A(p,q) < 1$.

Definition 45. *Let K be a field equipped with an Archimedean norm. Let $\mathrm{d}_P : \mathbb{P}^1(K) \times \mathbb{P}^1(K) \to \mathbb{R}$ be given by:*

$$\mathrm{d}_P((p_1:p_2),(q_1:q_2)) = \begin{cases} \mathrm{d}_A(p_1/p_2, q_1/q_2) & \text{if } p_2q_2 \neq 0 \\ \mathrm{d}_A(p_2/p_1, q_2/q_1) & \text{if } p_1q_1 \neq 0 \\ 1 & \text{if } p_1 = q_2 = 0 \text{ or } p_2 = q_1 = 0. \end{cases} \tag{6.5}$$

Proposition 46. d_P *is a metric.*

Proof. Firstly, d_P is well defined; one easily checks that if $x, y \in K^*$ then $\mathrm{d}_A(x, y) = \mathrm{d}_A(1/x, 1/y)$. Again we check only the triangle inequality, since the others are obvious. Choose three points $p = (p_1 : p_2)$, $q = (q_1 : q_2)$ and $r = (r_1 : r_2)$. If all three are contained in one of the two coordinate charts of $\mathbb{P}^1$ then the result follows from the affine case. If any two of p, q and r coincide then the inequality is obvious. We are thus left with two cases:

Case 1: $p_1 = q_2 = 0$ and $r_1 r_2 \neq 0$. Then

$$\mathrm{d}_P(p, q) + \mathrm{d}_P(q, r) = 1 + \mathrm{d}_P(q, r) \geq 1 \geq \mathrm{d}_P(p, r). \tag{6.6}$$

Case 2: $p_1 = r_2 = 0$ and $q_1 q_2 \neq 0$. Then

$$\mathrm{d}_P(p, q) + \mathrm{d}_P(q, r) = \frac{|q_1/q_2|}{1 + |q_1/q_2|} + \frac{|q_2/q_1|}{1 + |q_2/q_1|} = 1 = \mathrm{d}_P(p, r). \tag{6.7}$$

□

Remark 47. *Even if the norm on K is non-Archimedean, the metrics d_A and d_P need not be.*

Definition 48. *Let K denote a finite extension of $\mathbb{Q}_p$ with a norm $|-|$ extending the p-adic one. Let $\mathrm{d}_P : \mathbb{P}^1(K) \times \mathbb{P}^1(K) \to \mathbb{R}$ be given by:*

$$\mathrm{d}_P((p_1 : p_2), (q_1 : q_2)) = \begin{cases} |p_1/p_2 - q_1/q_2| & \text{if } |p_1| \leq |p_2| \text{ and } |q_1| \leq |q_2| \\ |p_2/p_1 - q_2/q_1| & \text{if } |p_1| \geq |p_2| \text{ and } |q_1| \geq |q_2| \\ 1 & \text{otherwise.} \end{cases} \tag{6.8}$$

Proposition 49. d_P *is a metric.*

Proof. Firstly, d_P is well defined; if $|p_1| = |p_2|$ and $|q_1| = |q_2|$ then

$$|p_1/p_2 - q_1/q_2|\,|p_2|\,|q_2| = |p_2/p_1 - q_2/q_1|\,|p_1|\,|q_1|\,. \tag{6.9}$$

We also observe that for all p, $q \in K$ we have $\mathrm{d}_P(p, q) \leq 1$; this is because $(K, |-|)$ is non-Archimedean.

Only the triangle inequality is non-obvious, and we prove it by cases. Choose three points $p = (p_1 : p_2)$, $q = (q_1 : q_2)$ and $r = (r_1 : r_2)$. Without loss of generality we may assume $|p_1| \leq |p_2|$.

Case 1: $|q_1| \leq |q_2|$ and $|r_1| \leq |r_2|$. This follows from the triangle inequality for the norm on K.

Case 2: $|q_1| \leq |q_2|$ and $|r_1| > |r_2|$.
If $|q_1| < |q_2|$ then

$$\mathrm{d}_P(p,q) + \mathrm{d}_P(q,r) = \mathrm{d}_P(p,q) + 1 \geq 1 \geq \mathrm{d}_P(p,r), \tag{6.10}$$

so we may assume that $|q_1| = |q_2|$.

If $|p_1| < |p_2|$ then $\mathrm{d}_P(p,q) = |p_1/p_2 - q_1/q_2| = \max(|p_1/p_1|, |q_1/q_2|) = 1$ since $|-|$ is a p-adic norm. Hence

$$\mathrm{d}_P(p,q) + \mathrm{d}_P(q,r) = 1 + \mathrm{d}_P(q,r) \geq 1 \geq \mathrm{d}_P(p,r). \tag{6.11}$$

Otherwise, $|p_1| = |p_2|$ and we are back to Case 1.
Case 3: $|q_1| > |q_2|$ and $|r_1| \leq |r_2|$.
If $|p_1| < |p_2|$ then

$$\mathrm{d}_P(p,q) + \mathrm{d}_P(q,r) = 1 + \mathrm{d}_P(q,r) \geq 1 \geq \mathrm{d}_P(p,r). \tag{6.12}$$

If $|r_1| < |r_2|$ then

$$\mathrm{d}_P(p,q) + \mathrm{d}_P(q,r) = \mathrm{d}_P(p,q) + 1 \geq 1 \geq \mathrm{d}_P(p,r). \tag{6.13}$$

Otherwise, $|p_1| = |p_2|$ and $|r_1| = |r_2|$, so we are back to Case 1.

Case 4: $|q_1| \geq |q_2|$ and $|r_1| \geq |r_2|$. Interchanging p and r returns us to Case 2.

□

Definition 50. *C is as always a hyperelliptic curve of genus g over a number field K living inside weighted projective space $\mathbb{P}(1,1,g+1)$ with coordinates x, s, y. We assume C is defined by $y^2 = f(x,s)$ where $f = \sum_{i-1}^{2g+2} f_i x^i s^{2g+2-i}$ has integral coefficients.*

For each place $\nu \in M_K$, we define $(K_\nu^{alg}, |-|)$ to be an algebraic closure of the completion K_ν together with the norm which restricts to ν on $K \subset K_\nu^{alg}$. For non-Archimedean places ν we define $\mathrm{d}_\nu : C(K_\nu^{alg}) \times C(K_\nu^{alg})$ by

$$\begin{aligned}
&\mathrm{d}_\nu((x_p,s_p,y_p),(x_q,s_q,y_q)) \\
&= \begin{cases}
\max\left(|x_p/s_p - x_q/s_q|, \left|y_p/s_p^{g+1} - y_q/s_q^{g+1}\right|\right) & \text{if } |x_p| \leq |s_p| \text{ and } |x_q| \leq |s_q| \\
\max\left(|s_p/x_p - s_q/x_q|, \left|y_p/x_p^{g+1} - y_q/x_q^{g+1}\right|\right) & \text{if } |x_p| \geq |s_p| \text{ and } |x_q| \geq |s_q| \\
1 & \text{otherwise.}
\end{cases}
\end{aligned} \tag{6.14}$$

Proposition 51. *For each $\nu \in M_K^0$, $\mathrm{d} = \mathrm{d}_\nu$ is a metric on $C(K_\nu^{alg})$.*

Proof. Checking that the function is well defined proceeds as for Proposition 49. Again, only the triangle inequality is non-obvious. We begin by observing that if $(x : s : y) \in C(K_\nu^{\mathrm{alg}})$ then

$$|x| \leq |s| \implies |y| \leq |s|^{g+1} \tag{6.15}$$

and

$$|x| > |s| \implies |y| \leq |x|^{g+1}. \tag{6.16}$$

The first implication holds as

$$|y|^2 = \left| \sum_i f_i x^i s^{2g+2-i} \right| \leq \left(\max_i |f_i| \right) |s|^{2g+2} \leq |s|^{2g+2}, \tag{6.17}$$

and the other case is similar. Combining this with the fact that $|-|$ is p-adic, we see for all p, $q \in C(K_\nu^{\mathrm{alg}})$ that $\mathrm{d}(p,q) \leq 1$.

From now on we proceed case-by-case. Let $p = (x_p, s_p, y_p)$, $q = (x_q, s_q, y_q)$ and $r = (x_r, s_r, y_r)$. Note that the change of coordinates $x \mapsto s$, $s \mapsto x$, $y/s^{g+1} \mapsto y/x^{g+1}$ preserves the metric (replacing f by its reciprocal polynomial). As such, we may assume without loss of generality that $|x_p| \leq |s_p|$.

Case 1: $|x_q| \leq |s_q|$ and $|x_r| \leq |s_r|$. Then

$$\begin{aligned}
&\mathrm{d}(p,q) + \mathrm{d}(q,r) \\
&= \max\left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right|, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right| \right) + \max\left(\left| \frac{x_q}{s_q} - \frac{x_r}{s_r} \right|, \left| \frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}} \right| \right) \\
&\geq \max\left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right| + \left| \frac{x_q}{s_q} - \frac{x_r}{s_r} \right|, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right| + \left| \frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}} \right| \right) \\
&\geq \mathrm{d}(p,r).
\end{aligned} \tag{6.18}$$

Case 2: $|x_q| \leq |s_q|$ and $|x_r| > |s_r|$. If $|x_q| < |s_q|$ then

$$\mathrm{d}(p,q) + \mathrm{d}(q,r) = \mathrm{d}(p,q) + 1 \geq 1 \geq \mathrm{d}(p,r), \tag{6.19}$$

so we may assume $|x_q| = |s_q|$. Now if $|x_p| = |s_p|$ then we are back to Case 1, so assume $|x_p| < |s_p|$. Then since $|-|$ is p-adic, we have $|x_p/s_p - x_q/s_q| =$

$\max(|x_p/s_p|, |x_q/s_q|) = 1$, so

$$\begin{aligned}\mathrm{d}(p,q) + \mathrm{d}(q,r) &\geq \max\left(\left|\frac{x_p}{s_p} - \frac{x_q}{s_q}\right| + \left|\frac{x_q}{s_q} - \frac{x_r}{s_r}\right|, \left|\frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}}\right| + \left|\frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}}\right|\right) \\ &\geq 1 \geq \mathrm{d}(p,r).\end{aligned} \tag{6.20}$$

Case 3: $|x_q| > |s_q|$ and $|x_r| \leq |s_r|$. If $|x_p| < |s_p|$ then

$$\mathrm{d}(p,q) + \mathrm{d}(q,r) = 1 + \mathrm{d}(q,r) \geq 1 \geq \mathrm{d}(p,r), \tag{6.21}$$

and if $|x_r| < |s_r|$ then

$$\mathrm{d}(p,q) + \mathrm{d}(q,r) = \mathrm{d}(p,q) + 1 \geq 1 \geq \mathrm{d}(p,r). \tag{6.22}$$

Otherwise we are back to Case 1.

Case 4: $|x_q| \geq |s_q|$ and $|x_r| \geq |s_r|$. Interchanging p and r reduces us to the second case.

□

Definition 52. *Let ν be an Archimedean place of K. As before, $(K_\nu^{alg}, |-|)$ is an algebraic closure of the completion K_ν together with the norm which restricts to ν on $K \subset K_\nu^{alg}$. We will define three symmetric functions on $C(K_\nu^{alg}) \times C(K_\nu^{alg})$, each of which satisfies the triangle inequality, and then define d_ν to be their sum, which will inherit the triangle inequality and will be easily seen to be a metric.*

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

$$\mathrm{d}_1(p,q) = \frac{|x_p s_q - x_q s_p|}{(|x_p| + |s_p|)(|x_q| + |s_q|)}, \tag{6.23}$$

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

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

$$\mathrm{d}_2(p,q) = \frac{\left|y_p x_q^{g+1} - y_q x_p^{g+1}\right|}{(|x_p|^{g+1} + |y_p|)(|x_q|^{g+1} + |y_q|)}. \tag{6.24}$$

Define $\mathrm{d}_3 : C(K_\nu^{alg}) \times C(K_\nu^{alg})$ by setting $\mathrm{d}_3(p,(1:0:0)) = 1/(1+\left|y_p/s_p^{g+1}\right|)$,

and otherwise

$$\mathrm{d}_3(p,q) = \frac{\left|y_p s_q^{g+1} - y_q s_p^{g+1}\right|}{(|s_p|^{g+1} + |y_p|)(|s_q|^{g+1} + |y_q|)}. \tag{6.25}$$

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

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

Proposition 53. d *is a metric.*

Proof. Only the triangle inequality is non-trivial to check, and it suffices to show this for each of d_1, d_2 and d_3 separately. Since each is continuous, it suffices to check this on a dense open set. The result then follows from Proposition 44 (the weighting makes no difference). □

Proposition 54. *For each* $\nu \in M_K^0$ *a non-Archimedean place, and for each* p, $q \in C(K_\nu^{alg})$, *we have*

$$\mathrm{d}_\nu(p,q) \leq 1. \tag{6.26}$$

For each $\nu \in M_K^\infty$ *an Archimedean place, and for each* p, $q \in C(K_\nu^{alg})$, *we have*

$$\mathrm{d}_\nu(p,q) \leq 3. \tag{6.27}$$

Proof. The non-Archimedean case is proven at the start of the proof of Proposition 51. For the Archimedean version, it suffices to recall that for all a, $b \in K$, we have $\mathrm{d}_A(a,b) \leq 1$. □

As a matter of notation, we often write $X = x/s$, $Y = y/s^{g+1}$, $S = s/x$ and $Y' = y/x^{g+1}$.

6.2 Non-Archimedean I: the Φ term

In this section we work locally over a non-Archimedean place, so for the remainder of this section let $\mathscr{C}$ denote a regular model of the curve C over a discrete valuation ring R finite over $\mathbb{Z}_p$. We replace R by an unramified extension such that all irreducible components of the special fibre of $\mathscr{C}$ over R are geometrically irreducible. If $\mathscr{C}$ is smooth over R, then the constructions in this section are trivial.

Let F denote the free abelian group generated by prime divisors supported on the special fibre, and let V denote the $\mathbb{Q}$-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 intersection

pairing on the special fibre of $\mathscr{C}$ 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.

We will make use of the Moore-Penrose pseudo-inverse (first defined in [Pen55]) of the matrix M:

Definition 55. *Let A be a real matrix. Then its Moore-Penrose pseudo-inverse A^+ is uniquely defined by the following four properties:*
1) $AA^+A = A$
2) $A^+AA^+ = A^+$
3) $(AA^+)^T = AA^+$
4) $(A^+A)^T = A^+A$.

We will only need the property that if the linear system $Ax = b$ has any solutions, then a solution is given by $x = A^+b$.

Proposition 56. *Let M^+ denote the Moore-Penrose pseudo-inverse of M, let m_- denote the infimum of its entries and m_+ their supremum.*

Let $D = D_1 - D_2$ and $E = E_1 - E_2$ be differences of semi-reduced divisors on C. Then

$$\left|\iota_\nu\left(\Phi(D), \overline{E}\right)\right| \leq g^2(m_+ - m_-), \tag{6.28}$$

where Φ is the function defined in Section 5.2.

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

$$v \cdot d^T + v \cdot M \cdot \Phi(D)^T = 0, \tag{6.29}$$

and hence that

$$d^T = -M \cdot \Phi(D)^T. \tag{6.30}$$

According to the property in Definition 55, we can take $\Phi(D)$ to be $-d \cdot (M^+)^T$, and so we find

$$\iota_\nu\left(\Phi(D), \overline{E}\right) = -d \cdot \left(M^+\right)^T \cdot e^T. \tag{6.31}$$

Now d and e are vectors each formed by assigning g copies of '+1' and g copies of '-1' to the basis elements $Y_1, \dots, Y_n$ (allowing multiple ± 1s to be assigned to a single basis vector), and so the result easily follows.

□

Definition 57. *Using the above proposition, we can define a computable constant $\mathscr{B}_1$ depending only on C such that for all semi-reduced divisors D and E, we have*

$$\left| \sum_{\nu \in M_K^0} \iota_\nu \left(\Phi_\nu(D), \overline{E} \right) \right| \leq \mathscr{B}_1. \tag{6.32}$$

6.3 Non-Archimedean II: local comparison of metrics and intersection pairings

Throughout this section, K will be a finite degree-n extension of $\mathbb{Q}_p$ for some prime p, with integers $\mathcal{O}_K$, residue field k and maximal ideal ν. We normalise the norm on K to extend the usual norm on $\mathbb{Q}$ - that which sends p to p^{-1}.

We begin by comparing the metric and intersection pairing on $\mathbb{P}^1$. This is not logically necessary, but gives a clear view of how the theory will proceed.

Lemma 58. *Let $p \neq q \in \mathbb{P}^1(K)$ be distinct points, and let $\overline{p}$ and $\overline{q}$ denote their closures inside $\mathbb{P}^1_{\mathcal{O}_K}$. Then*

$$\log(\#k) \cdot \iota_\nu \left(\overline{p}, \overline{q} \right) / n = \log \left(\frac{1}{\mathrm{d}_P(p,q)} \right). \tag{6.33}$$

Proof. Write $p = (p_1 : p_2)$, $q = (q_1 : q_2)$ with p_i, $q_i \in \mathcal{O}_K$. If $|p_1| < |p_2|$ and $|q_1| > |q_2|$ or vice versa, then $\overline{p}$ and $\overline{q}$ do not meet on the special fibre of $\mathbb{P}^1_{\mathcal{O}_K}$ so $\iota_\nu \left(\overline{p}, \overline{q} \right) = 0$, and by definition we see that $\mathrm{d}_P(p,q) = 1$.

Otherwise, possibly after changing coordinates, we may assume that p and q are of the form $(p_1 : 1)$ and $(q_1 : 1)$ respectively, for p_1, $q_1 \in \mathcal{O}_K$.

Now an easy calculation using (3.28) shows

$$\log(\#k) \cdot \iota_\nu \left(\overline{p}, \overline{q} \right) = -n \log \left| p_1 - q_1 \right|, \tag{6.34}$$

and

$$\log \left(\frac{1}{\mathrm{d}_P(p,q)} \right) = - \log \left| p_1 - q_1 \right|, \tag{6.35}$$

from which the result follows. □

Next we obtain similar results for points on C. The main additional difficulty is that of working with regular models for C; the naïve projective closure of the generic fibre is not in general regular, but rather must be modified by a sequence of blowups and normalisations to obtain a regular model. We must determine how these modifications will affect the intersection numbers, and also keep careful track

of the base field since regular models are not in general stable under ramified base change. In essence, viewing intersection theory from the point of Serre's formula, our aim in this section is to bound the dimensions of the higher Tor groups.

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/K be a finite extension of degree m with residue field l such that D and E are both pointwise rational over L. Write $D = \sum_{i=1}^{d} p_i$ and $E = \sum_{i=1}^{e} q_i$. Write ω for the maximal ideal of $\mathcal{O}_L$.

Let $\mathscr{C}_1$ denote the Zariski closure of C in $\mathbb{P}_{\mathcal{O}_K}(1, 1, g+1)$. Let $\mathscr{C}/\mathcal{O}_K$ denote a regular model of $\mathscr{C}_1$, obtained by a fixed sequence of blowups at closed points and along smooth fibral curves (the latter replace normalisations, and are often computationally easier to work with). That such a resolution is possible is a result of Hironaka, contained in his appendix to [CGO84]: see pages 102 and 105. We observe that $\mathscr{C}_1$ may locally be embedded in $\mathbb{P}^2_S$, and so the proof given in that appendix suffices.

Let b denote the longest length of a chain of blowups involved in obtaining $\mathscr{C}$ from $\mathscr{C}_1$ (one blowup is considered to follow another if the centre of one blowup is contained in the exceptional locus of the previous one).

Proposition 59. *Let $\mathscr{D}$ and $\mathscr{E}$ denote the Zariski closures of D and E respectively on the minimal regular model $\mathscr{C}$ over $\mathcal{O}_K$. Then*

$$-bde \leq \iota_\nu(\mathscr{D}, \mathscr{E}) - \frac{1}{[L:K]} \log^+ \left(\frac{1}{\prod_{i,j} \mathrm{d}(p_i, q_j)} \right) \leq 0. \tag{6.36}$$

To prove this, we will need a sequence of lemmas, but we begin by noting a corollary:

Corollary 60. *There exists a computable constant $\mathscr{B}_2$ such that for all semi-reduced divisors D and E on C with closures $\mathscr{D}$ and $\mathscr{E}$ on $\mathscr{C}$, we have*

$$\left| \sum_{\nu \in M_K^0} \iota_\nu(\mathscr{D}, \mathscr{E}) - \frac{1}{[L:K]} \sum_{\nu \in M_L^0} \log^+ \left(\frac{1}{\prod_{i,j} \mathrm{d}(p_i, q_j)} \right) \right| \leq \mathscr{B}_2. \tag{6.37}$$

Proof. We begin by noting that there exists a finite extension of K such that every effective degree-g divisor becomes pointwise rational over that field, and also that there are only finitely many places of bad reduction of K. At each such place, set $\mathscr{B}_{\nu,2} = b_\nu g^2$ where b_ν is the number of blowups needed over ν, and then $\mathscr{B} = \sum_\nu \mathscr{B}_\nu$. □

Lemma 61. *Let $p \neq q \in C(L) = \mathrm{Hom}_L(L, C_L)$. Write*

$$I_{p,q} \stackrel{def}{=} \sum_{\Omega|\omega} \log(\#\kappa(\Omega)) \operatorname{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right), \tag{6.38}$$

where the sum is over closed points Ω 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 in $\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ of the images of p and q in $C \times_K L$. Then

$$I_{p,q} = mn \log \left(\frac{1}{\mathrm{d}(p,q)} \right). \tag{6.39}$$

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 $\iota_\nu(\overline{p}, \overline{q}) = 0$, and by definition we see that $\mathrm{d}_P(p,q) = 1$.

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, $y_q \in \mathcal{O}_L$. Writing F for the (integral) defining equation of C on the coordinate chart containing p and q, and taking Ω to be the closed point where $\overline{p}$ and $\overline{q}$ meet, we have

$$\begin{aligned} \frac{\mathcal{O}_{\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} &\cong \frac{\mathcal{O}_L[x,y]_{(x,y)}}{(F, x - x_p, y - y_p, x - x_q, y - y_q)} \\ &\cong \frac{\mathcal{O}_L}{(x_p - x_q, y_p - y_q)}, \end{aligned} \tag{6.40}$$

so

$$\operatorname{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right) = \min\left(\mathrm{ord}_\omega(x_p - x_q), \mathrm{ord}_\omega(y_p - y_q) \right). \tag{6.41}$$

Now given $a \in L$, we find

$$\log(\#l)\, \mathrm{ord}_\omega(a) = -mn \log|a|, \tag{6.42}$$

so

$$\operatorname{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right) = mn \min\left(-\log|x_p - x_q|, -\log|y_p - y_q| \right) / \log(\#l), \tag{6.43}$$

and hence

$$I_{p,q} = mn \min\left(-\log|x_p - x_q|, -\log|y_p - y_q| \right). \tag{6.44}$$

However,

$$\log(1/\mathrm{d}(p,q)) = \min\left(-\log|x_p - x_q|, -\log|y_p - y_q| \right), \tag{6.45}$$

so we are done. □

Lemma 62. *Recalling that over L we can write $D = \sum_{i=1}^{d} p_i$ and $E = \sum_{i=1}^{e} q_i$, we define $\omega_{i,j}$ to be 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 unit ideal 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*

$$\sum_{i,j} \text{length}_{\mathcal{O}_L}\left(\frac{\mathcal{O}_{\omega_{i,j}}}{I_{p_i} + I_{q_i}}\right) = \text{length}_{\mathcal{O}_L}\left(\frac{\mathcal{O}_{\mathscr{C}_1} \otimes_{\mathcal{O}_K} \mathcal{O}_L}{(\mathcal{I}_D + \mathcal{I}_E) \otimes_{\mathcal{O}_K} \mathcal{O}_L}\right). \tag{6.46}$$

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 63. *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.*

$$\text{length}_{\mathcal{O}_K}\left(\frac{\mathcal{O}_{\mathscr{C}_1}}{\mathcal{I}_D + \mathcal{I}_E}\right) \cdot \text{ram. deg}\, L/K = \text{length}_{\mathcal{O}_L}\left(\frac{\mathcal{O}_{\mathscr{C}_1} \otimes_{\mathcal{O}_K} \mathcal{O}_L}{(\mathcal{I}_D + \mathcal{I}_E) \otimes_{\mathcal{O}_K} \mathcal{O}_L}\right). \tag{6.47}$$

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

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

$$\text{length}_{\mathcal{O}_K}(M) \cdot \text{ram. deg}(L/K) = \text{length}_{\mathcal{O}_L}(M \otimes_{\mathcal{O}_K} \mathcal{O}_L). \tag{6.48}$$

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

$$M_i/M_{i+1} \cong \mathcal{O}_K/\mathfrak{m}_K. \tag{6.49}$$

By additivity of lengths, it suffices to show

$$\text{length}_{\mathcal{O}_L}\left(\frac{\mathcal{O}_K}{\mathfrak{m}_K} \otimes_{\mathcal{O}_K} \mathcal{O}_L\right) = \text{ram. deg}(L/K), \tag{6.50}$$

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

Lemma 64. *Let $\phi : \mathscr{C}_3 \to \mathscr{C}_2$ be one of the blowups involved in obtaining $\mathscr{C}$ from $\mathscr{C}_1$. Let $p \neq q \in C_L(L)$. Then*

$$0 \leq \text{length}\left(\frac{\mathcal{O}_{\mathscr{C}_2 \times \mathcal{O}_L}}{I_{\overline{p}} + I_{\overline{q}}}\right) - \text{length}\left(\frac{\mathcal{O}_{\mathscr{C}_3 \times \mathcal{O}_L}}{I_{\overline{p}} + I_{\overline{q}}}\right) \leq \text{ram. deg}(L/K). \tag{6.51}$$

Proof. 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 $\Omega|\alpha$.

Let R denote the local ring of the (three-dimensional) ambient space to $\mathscr{C}_2$ at α, and similarly let A be the local ring of $\mathscr{C}_2$ at α. Let $B \subset R$ be the centre of the localisation of ϕ at α. After étale base-change, we may assume that we have

$$R = \overline{\mathcal{O}_K}[[x, y]]_{(x,y,a)} \tag{6.52}$$

where $\overline{\mathcal{O}_K}$ is finite étale over $\mathcal{O}_K$ and a is a maximal ideal in $\overline{\mathcal{O}_K}$, and that

$$B = (x, y, a) \quad \text{or} \quad B = (x, a), \tag{6.53}$$

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 canonical map from the blowup of that closed subscheme, so we can be relaxed with our notation. Setting ω' to be a uniformiser in the maximal ideal of $\overline{\mathcal{O}_K} \cdot \mathcal{O}_L$, we may write

$$p = (x - \omega' x_p, y - \omega' y_p) \qquad q = (x - \omega' x_q, y - \omega' y_q) \tag{6.54}$$

where x_p, y_p, x_q and y_q are in $\mathcal{O}_L \cdot \overline{\mathcal{O}_K}$. As usual, we have

$$\operatorname{length}\left(\frac{\mathcal{O}_{\mathscr{C}_2 \times \mathcal{O}_L}}{I_p + I_q}\right) = \min\left(\operatorname{ord}_{\omega'}(\omega' x_p - \omega' x_q), \operatorname{ord}_{\omega'}(\omega' y_p - \omega' y_q)\right). \tag{6.55}$$

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

$$P' = (x - x_p, y - y_p) \quad \text{and} \quad q' = (x - x_q, y - y_q), \tag{6.56}$$

so

$$\begin{aligned} \operatorname{length}\left(\frac{\mathcal{O}_{\mathscr{C}_3 \times \mathcal{O}_L}}{I_p + I_q}\right) &= \min\left(\operatorname{ord}_{\omega'}(x_p - x_q), \operatorname{ord}_{\omega'}(y_p - y_q)\right) \\ &= \operatorname{length}\left(\frac{\mathcal{O}_{\mathscr{C}_2 \times \mathcal{O}_L}}{I_p + I_q}\right) - \operatorname{ord}_{\omega'}(a). \end{aligned} \tag{6.57}$$

In the case $B = (x, a)$ we look again at the affine patch of the blowup given by

setting $\omega' \neq 0$; the equations for p and q transform into

$$p' = (x - x_p, y - \omega' y_p) \quad \text{and} \quad q' = (x - x_q, y - \omega' y_q), \tag{6.58}$$

so

$$\begin{aligned} \operatorname{length}\left(\frac{\mathcal{O}_{\mathscr{C}_3 \times \mathcal{O}_L}}{I_p + I_q}\right) &= \min\left(\operatorname{ord}_{\omega'}(x_p - x_q), \operatorname{ord}_{\omega'}(\omega' y_p - \omega' y_q)\right) \\ &= \operatorname{length}\left(\frac{\mathcal{O}_{\mathscr{C}_2 \times \mathcal{O}_L}}{I_p + I_q}\right) - (0 \text{ or } 1) \operatorname{ord}_{\omega'}(a), \end{aligned} \tag{6.59}$$

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

$$\operatorname{ord}_{\omega'}(a) = \text{ram. deg}(L \cdot \overline{K}/\overline{K}) = \text{ram. deg}(L/K). \tag{6.60}$$

□

Proof of Proposition 59. To prove Proposition 59, we apply Lemmata 61, 64, 62 and 63 in that order to find that there exists $0 \leq \beta \leq bde$ such that

$$\begin{aligned} n \sum_{i,j} \log\left(\frac{1}{\mathrm{d}(p_i, q_j)}\right) &= \frac{1}{m} \sum_{\Omega|\nu} \log(\#\kappa(\Omega)) \operatorname{length}_{\mathcal{O}_L}\left(\frac{\mathcal{O}_{\mathscr{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q}\right) \\ &= \frac{1}{m} \sum_{\Omega|\nu} \log(\#\kappa(\Omega)) \operatorname{length}_{\mathcal{O}_L}\left(\frac{\mathcal{O}_{\mathscr{C} \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q}\right) + \beta \\ &= \frac{1}{m} \log(\#\kappa(\omega)) \operatorname{length}_{\mathcal{O}_L}\left(\frac{\mathcal{O}_{\mathscr{C} \times \mathcal{O}_L}}{I_D + I_E}\right) + \beta \\ &= \frac{1}{m} \log(\#\kappa(\omega)) \operatorname{length}_{\mathcal{O}_K}\left(\frac{\mathcal{O}_{\mathscr{C}}}{I_D + I_E}\right) . \text{ram. deg}(L/K) + \beta \\ &= \iota_\nu(\mathscr{D}, \mathscr{E}) + \beta. \end{aligned} \tag{6.61}$$

□

Remark 65. *Note that $\beta = 0$ for all but finitely many places ν.*

6.4 Archimedean I: bounds on Green's functions away from the diagonal

We fix for the remainder of this section a complex place ν of K, and we view the resulting set $C(\mathbb{C})$ as a (connected) complex manifold in the usual fashion. The aim

of this section is to prove the following proposition:

Proposition 66. *Given any sufficiently small $\mu > 0$, there is a computable constant $M(\mu)$ such that the following property holds:*
for all p, $q \in C(\mathbb{C})$ and distinct Weierstrass points ∞_p and ∞_q such that $\mathrm{d}(p,q) \geq \mu$, $\mathrm{d}(p,\infty_q) \geq \mu$ and $\mathrm{d}(q,\infty_p) \geq \mu$, we have

$$\left|g_{p-\infty_p}(q-\infty_q)\right| \leq M(\mu). \tag{6.62}$$

The reader will notice that we did not overtly assume that ∞_p and ∞_q were far apart, but this is hidden in the assumption that μ be sufficiently small; we simply impose the condition that μ be at most equal to the shortest distance between two Weierstrass points.

As so often happens, the existence of such constants $M(\mu)$ is clear, this time from elementary properties of Green's functions:

Proposition 67. *Proposition 66 holds if we do not the existence of an algorithm to compute the constant $M(\mu)$.*

Proof. For fixed p and ∞_p, cover $C(\mathbb{C})$ with finitely many closed sets U_i (in the Euclidean topology) on which $p-\infty_p$ is represented by a rational function ϕ_i. Then on each U_i we have by [Lan88, p21] that

$$g_{p-\infty_p}(q) = -\log|\phi_i(q)|^2 + \alpha(q) \tag{6.63}$$

for some smooth function α; in particular, $g_{p-\infty_p}(q)$ is bounded. To make the resulting bound uniform in p and ∞_p, it suffices to see that $C(\mathbb{C})$ is compact and that the sets U_i and functions α_i can be chosen in a way which is continuous with varying p and ∞_p; this follows from the fact that our Green's functions are defined relative to a continuous metric on $C(\mathbb{C})$. □

Thus, the remainder of this section will be devoted to making the constant explicit.

Remark 68. *It is clear that if $M(\mu)$ is such a constant and $\mu \leq \mu'$, then we can take $M(\mu') = M(\mu)$.*

We begin the construction of $M(\mu)$. Recall that d_P is the metric on $\mathbb{P}^1(\mathbb{C})$ defined in Section 6.1

Definition 69. *Let $W \subset \mathbb{P}^1(\mathbb{C})$ denote the set of Weierstrass points of C.*

We define a permissible box *of radius $r > 0$ and centered at $t = (x_t : s_t) \in \mathbb{P}^1(\mathbb{C})$ to be a subset $B_r(t) \subset \mathbb{P}^1(\mathbb{C})$ of one of the following forms:*

$$1) \quad B_r(t) = \{(x : s) : |\Re(x/s) - \Re(x_t/s_t)| \leq r \text{ and } |\Im(x/s) - \Im(x_t/s_t)| \leq r\} \tag{6.64}$$

with $|x_t| \leq \frac{2}{3}|s_t|$.

$$2) \quad B_r(t) = \{(x : s) : |\Re(s/x) - \Re(s_t/x_t)| \leq r \text{ and } |\Im(s/x) - \Im(s_t/x_t)| \leq r\} \tag{6.65}$$

with $|s_t| \leq \frac{3}{2}|x_t|$.

In addition, we require that for all $w \in W$, if $w \in B_r(t)$ then $w = t$.

We will call these boxes of type (1) and type (2) respectively.

Definition 70. *Given a finite cover $\tilde{\mathbb{T}}$ of $\mathbb{P}^1(\mathbb{C})$ by permissible boxes, let $\tilde{\mathbb{T}}_0$ denote the set of centres of boxes in $\tilde{\mathbb{T}}$. Let $\mathbb{T}$ denote the cover of $C(\mathbb{C})$ obtained by lifting $\tilde{\mathbb{T}}$ and then decomposing each of the resulting sets into its connected components, and similarly let $\mathbb{T}_0$ denote the lift of $\tilde{\mathbb{T}}_0$.*

Proposition 71. *Each disk in $\mathbb{T}$ contains a unique point of $\mathbb{T}_0$.*

Proof. Write π for the projection from C to $\mathbb{P}^1$. Fix $D \in \mathbb{T}$. The existance of a point of $\mathbb{T}_0$ in D is clear, and so we must prove uniqueness. If D contains a Weierstrass points this is clear, so suppose that D contains no Weierstrass point. Let $p \in \tilde{\mathbb{T}}_0$ be the unique point in $\tilde{\mathbb{T}}_0$ which is the centre of $\pi(D)$, and let $\pi^{-1}(p) = \{q_1, q_2\}$. We must show that only one of the q_i lies in D.

Suppose for the purposes of contradiction that $q_1 \in D$ and $q_2 \in D$. D is path connected, and so we may let γ denote a path from q_1 to q_2 inside D. Now since $\pi(\gamma) \subset \pi(D)$ is a path, and $\pi(D) \setminus W$ is simply connected (as D contains no Weierstrass point), a contradiction follows if we can show that $\pi(\gamma)$ represents a non-trivial homotopy class in the fundamental group of $\mathbb{P}^1(\mathbb{C}) \setminus W$.

To prove that $\pi(\gamma)$ represents a non-trivial element of the fundamental group $\mathbb{P}^1(\mathbb{C}) \setminus W$, we again work by contradiction: if $\pi(\gamma)$ represents a trivial homology class, then we may deform it inside $\mathbb{P}^1(\mathbb{C}) \setminus W$ to a constant path at p. Since $C(\mathbb{C}) \setminus W \to \mathbb{P}^1(\mathbb{C}) \setminus W$ is a covering space, we may lift this deformation to a deformation of γ inside $C(\mathbb{C}) \setminus W$ to a path (still from q_1 to q_2) which is contained in the fibre of π over p. Since this fibre is a discrete set of two elements, this is nonsense and we have a contradiction. □

Lemma 72. *Given $\epsilon > 0$, we can find a constant $\tau > 0$ and a finite cover $\tilde{\mathbb{T}}$ of $\mathbb{P}^1(\mathbb{C})$ by permissible boxes of radius τ with the following property:*

for any two points p, $q \in \mathbb{P}^1(\mathbb{C})$ such that $\mathrm{d}_P(p,q) \geq \epsilon$, there exist boxes D_p and D_q in $\tilde{\mathbb{T}}$ such that $p \in D_p$, $q \in D_q$ and $D_p \cap D_q = \emptyset$.

Proof. It is clear that if τ is small enough then any such cover will suffice, so it suffices to prove the existence of permissible covers for sufficiently small τ. We may consider the hemispheres $|x| \leq |s|$ and $|x| \geq |s|$ separately, and we will treat only the former. For this, assume that

$$\tau < \min\left(\frac{1}{4}, \frac{1}{3}\min_{w \neq w' \in W}\left(\min\left(\left|\Re\left(\frac{x_w}{s_w} - \frac{x_{w'}}{s_{w'}}\right)\right|, \left|\Im\left(\frac{x_w}{s_w} - \frac{x_{w'}}{s_{w'}}\right)\right|\right)\right)\right). \quad (6.66)$$

Write T for a cover of $\{z \in \mathbb{C} : |z| \leq 1\}$ by boxes of side length 2τ in a rectangular grid (we do not care about its orientation or centering; this is unlikely to be a cover by permissible boxes). Then remove from T all boxes which contain Weierstrass points. Finally, for each Weierstrass point w, add in to T nine boxes of side length 2τ forming a square of side length 6τ centered at w. Our assumptions on τ ensure this will form a cover by permissible boxes. □

Definition 73. *Given a cover $\tilde{\mathbb{T}}$ of $\mathbb{P}^1(\mathbb{C})$ by permissible boxes of radius τ, with lift $\mathbb{T}$ to $C(\mathbb{C})$, we set*

$$\rho(\tilde{\mathbb{T}}) = \max_{B_1, B_2}\left(\sup_{p,q \in B_1 \cup B_2}(\mathrm{d}_2(p,q) + \mathrm{d}_3(p,q))\right), \quad (6.67)$$

where the maximum is taken over pairs of boxes B_1, B_2 in the lift $\mathbb{T}$ such that $B_1 \cap B_2$ is non-empty. $\rho(\tilde{\mathbb{T}})$ is always finite; indeed, it is bounded above by 2.

Given $\tilde{\mathbb{T}}$ as above, suppose also that the boxes in $\tilde{\mathbb{T}}$ have centres t with $|X_t| \leq 1$ for boxes of type (1) and centres with $|S_t| \leq 1$ for boxes of type (2); we say that such a cover has <u>small centres</u>. The proof given above of the existance of permissible covers extends trivially to show the existance of covers with small centres.

Given any cover $\tilde{\mathbb{T}}$ by permissible boxes, set $\zeta(\tilde{\mathbb{T}})$ to be the cover of $\mathbb{P}^1(\mathbb{C})$ by (not necessarily permissible) boxes of radius $\tau/3$ obtained by covering each box in $\tilde{\mathbb{T}}$ by 9 boxes of radius $\tau/3$ in the unique way.

Given $\tilde{\mathbb{T}}$ a permissible cover with small centres, we define a sequence $(\tilde{\mathbb{T}}_n)_{n=0}^{\infty}$ of covers by setting $\tilde{\mathbb{T}}_0 = \tilde{\mathbb{T}}$ and $\tilde{\mathbb{T}}_{n+1} = \zeta(\tilde{\mathbb{T}}_n)$. If in addition we have that $\tau < 1/2$, then the additional conditions on the centres of boxes in $\tilde{\mathbb{T}}$ ensure that each $\tilde{\mathbb{T}}_n$ is again a cover by permissible boxes.

Proposition 74. *Given any cover by permissible boxes $\tilde{\mathbb{T}}$ with small centres, of radius $\tau < 1/2$, the sequence of real numbers $\left(\rho(\tilde{\mathbb{T}}_n)\right)_{n=0}^{\infty}$ is decreasing and null.*

Proof. Since every box in $\tilde{\mathbb{T}}_{n+1}$ is contained in some box of $\tilde{\mathbb{T}}_n$, the sequence is decreasing. To show that it is null, we will construct an upper bound on $\rho(\tilde{\mathbb{T}}_\tau)$ for $\tilde{\mathbb{T}}_\tau$ a cover by permissible boxes of radius τ arising as part of such a sequence, and show that the bound tends to 0 as $\tau \to 0$.

Write B_p and B_q for the permissible boxes containg p and q respectively. We may assume $|X_p| \leq 1$. Since we are interested only in the limit as $n \to \infty$, we may assume that $8\sqrt{2}\tau < 1$. The condition that p and q lie in a pair of overlapping boxes can be used to show that $|X_q| \leq 1/(1 - 4\sqrt{2}\tau)$; one can check (for example by considering all possible cases) that the greatest absolute value of X_q is achieved when p and q lie at the corners of a pair of boxes (call them Bp and B_q) each of type (2), which meet at a single corner opposite the corners at which p and q lie, and which are arranged so that one of their diagonals is radial to $X = 0$. We then see that the S-coordinate of B_p must be at least $1 - 2\sqrt{2}\tau$, and similarly that the S-coordinate of B_q must in turn be at least $1 - 4\sqrt{2}\tau$, so the claimed bound follows.

We may use these bounds on $|X_p|$ and $|X_q|$ to obtain upper bounds on $|Y_p|$ and $|Y_q|$ using Lemma 84.

A similar calculation to that above shows that the condition that p and q lie in overlapping boxes implies that $|X_p - X_q| \leq 8\sqrt{2}\tau$ (if B_p and B_q both have centres whose X-coordinate has absolute value at most 1, then the bound would be $4\sqrt{2}\tau$, but as before we must consider also the other cases, from which this bound may be derived). A very slight modification of the proof of Case Q_1 of Lemma 102 yields a computable upper bound c so that

$$\frac{\mathrm{d}_2(p,q) + \mathrm{d}_3(p,q)}{|Y_p - Y_q|} \leq c. \tag{6.68}$$

As such, it suffices to find upper bounds on $|Y_p - Y_q|$ which tend to 0 as τ tends to 0.

Let $R = \frac{1}{2}\min_{w \neq w' \in W} |X_w - X_{w'}|$. We may assume $24\sqrt{2}\tau \leq R$. We consider three cases:

Case 1) For every Weierstrass point $w \in W$, we have $|X_p - X_w| \geq R$.
This implies that for all $w \in W$ we have $|X_w - X_q| \geq R - 8\sqrt{2}\tau \geq R/2$. Let c_1 denote an upper bound on $\left|\frac{\mathrm{d}Y}{\mathrm{d}X}\right|$ as X runs over

$$\{X \in \mathbb{C} : |X| \leq 1 \text{ and } \forall w \in W : |X - X_w| \geq R/2\}. \tag{6.69}$$

Let γ be a path from p to q contained in $B_p \cup B_q$. γ may be chosen such that the length of its projection to $\mathbb{C}$ is less that or equal to $8\sqrt{2}\tau$, and so we see by

integrating along γ that

$$|Y_p - Y_q| \leq c_1 \cdot 8\sqrt{2}\tau, \tag{6.70}$$

which tends to 0 as $\tau \to 0$.

Case 2) There exists a Weierstrass point $w \in W$ such that $|X_w - X_p| \leq 16\sqrt{2}\tau$ and $|X_w - X_q| \leq 16\sqrt{2}\tau$. Then set

$$c_2 = \sup_t |f(t)/(X_w - t)| \tag{6.71}$$

where the supremum runs over $t \in \mathbb{C}$ with $|t - X_w| \leq 16\sqrt{2}\tau$. Hence

$$|Y_p - Y_q| \leq |Y_p| + |Y_q| \leq \sqrt{c_2 |X_w - X_p|} + \sqrt{c_2 |X_w - X_q|} \leq 2\sqrt{c_2 8\sqrt{2}\tau}, \tag{6.72}$$

which tends to 0 as $\tau \to 0$.

Case 3) There is a weierstrass point $w \in W$ such that $|X_p - X_w| \leq R$, and $|X_w - X_p| \geq 8\sqrt{2}\tau$ and $|X_w - X_q| \geq 8\sqrt{2}\tau$.
For this case we will have to make more precise use of the form of the covers $\tilde{\mathbb{T}}_n$, namely we observe that because successive covers are obtained by subdividing the previous cover in a specified manner, for n sufficiently large we have

$$\inf_{t \in B_p \cup B_q} |X_t - X_w| \geq \tau. \tag{6.73}$$

Set $c_3 = \sup_{t \in \mathbb{C}:|t| \leq 1} f'(t)$ and

$$c_4 = \sup_t |f(t)/(X_w - t)| \tag{6.74}$$

where the supremum runs over $t \in \mathbb{C}$ with $|t - X_w| \leq R + 4\sqrt{2}\tau$. We calculate that

$$\left|\frac{\mathrm{d}\, Y}{\mathrm{d}\, X}\right| = \left|\frac{f'(X)}{2Y}\right| = \left|\frac{f'(X)}{2\sqrt{f(X)}}\right| \leq \left|\frac{c_3}{2\sqrt{f(X)}}\right| \leq \frac{c_3}{2\sqrt{c_4}} \frac{1}{\left|\sqrt{X - X_w}\right|}, \tag{6.75}$$

and so combining with Equation (6.73) and integrating along a path from p to q inside $B_p \cup B_q$ we see

$$|Y_p - Y_q| \leq \frac{8\sqrt{2}\tau c_3}{2\sqrt{c_4}\sqrt{\tau}} = \frac{8\sqrt{2}\sqrt{\tau} c_3}{2\sqrt{c_4}}, \tag{6.76}$$

which tends to 0 as $\tau \to 0$.

□

Lemma 75. *Given $\mu > 0$ there exist a constant $\tau > 0$ and a finite cover $\tilde{\mathbb{T}}$ of $\mathbb{P}^1$ by permissible boxes of radius τ with the following property:*
for any two points p, $q \in C(\mathbb{C})$ such that $\mathrm{d}(p,q) \geq \mu$, there exist disjoint boxes D_p and D_q in $\mathbb{T}$ such that $p \in D_p$ and $q \in D_q$.

Proof. Fix $\mu > 0$. We give an algorithm to construct τ:

1) Set $\tau = \mu$.

2) Choose a cover $\tilde{\mathbb{T}}_\tau$ of $\mathbb{P}^1(\mathbb{C})$ by permissible boxes of small centres and of radius τ.

3) If $\mu - 8\sqrt{2}\tau > \rho(\tilde{\mathbb{T}}_\tau)$, stop. Otherwise, replace τ by $\tau/3$ and $\tilde{\mathbb{T}}_\tau$ by $\zeta(\tilde{\mathbb{T}}_\tau)$, and go to (3).

Termination of the algorithm follows from the fact that the sequence of $\rho(\tilde{\mathbb{T}}_\tau)$ is null and the sequence of $\mu - 8\sqrt{2}\tau$ tends to $\mu > 0$.

It remains to show that the resulting τ and cover $\tilde{\mathbb{T}}_\tau$ will suffice. Fix p, $q \in C(\mathbb{C})$ such that $\mathrm{d}(p,q) \geq \mu$. If $\pi(p)$ and $\pi(q)$ lie in disjoint boxes in $\tilde{\mathbb{T}}_\tau$ then we are done, and if not then this forces $\pi(p)$ and $\pi(q)$ to be close together; explicitly, assuming without loss of generality that $|X_p| \leq 1$ and arguing as in the proof of the previous lemma, we see

$$|X_p - X_q| \leq 8\sqrt{2}\tau. \tag{6.77}$$

Hence

$$\mathrm{d}_1(p,q) = \frac{|X_p - X_q|}{(1+|X_p|)(1+|X_q|)} \leq |X_p - X_q| \leq 8\sqrt{2}\tau, \tag{6.78}$$

so

$$\mathrm{d}_2(p,q) + \mathrm{d}_3(p,q) \geq \mu - \mathrm{d}_1(p,q) \geq \mu - 8\sqrt{2}\tau. \tag{6.79}$$

Hence if $\mu - 8\sqrt{2}\tau > \rho(\tilde{\mathbb{T}}_\tau)$ then $\mathrm{d}_2(p,q) + \mathrm{d}_3(p,q) > \rho(\tilde{\mathbb{T}}_\tau)$, which by definition of $\rho(\tilde{\mathbb{T}}_\tau)$ means that p and q live in disjoint boxes in the lift $\mathbb{T}_\tau$ on $C(\mathbb{C})$.

□

Definition 76. *For each $p \in \mathbb{T}_0$, let $D_p \in \mathbb{T}$ be the disk at whose centre p lies. For each $p \in \mathbb{T}_0$ and for each $q \in D_p$, we define a path $\gamma_{p,q}$ as follows:*
1) if $|x_p| \leq |s_p|$, then $\gamma_{p,q}$ is the unique continuous path in C from p to q which is a lift of a straight line in the affine space contained in $\mathbb{P}^1$ by setting $s = 1$.
2) if $|x_p| > |s_p|$, then $\gamma_{p,q}$ is the unique continuous path in C from p to q which is a lift of a straight line in the affine space contained in $\mathbb{P}^1$ by setting $x = 1$.
The parametrisations of the paths will be given later.

We recall the setup of hyperelliptic integration from Section 5.7.2. Let $\tilde{\omega}_0 = \frac{\mathrm{d}\,x}{y}, \ldots, \tilde{\omega}_{g-1} = \frac{x^{g-1}\,\mathrm{d}\,x}{y}$ be a basis of differential 1-forms on C, let $\{A_i, B_i : i =$

$1, \dots g\}$ be a symplectic homology basis, and let $\{\omega_i = \sum_j c_{i,j}\tilde{\omega}_j : i = 1, \dots, g\}$ be a normalised basis of differential forms such that

$$\int_{A_i} \omega_j = \delta_{i,j}. \tag{6.80}$$

Let $\Lambda \subset \mathbb{C}^{g\times g}$ be the resulting period matrix. Let $\mathfrak{D} \subset \mathbb{C}^g$ be the fundamental domain, and let $\alpha : C(\mathbb{C}) \to \mathfrak{D}$ be the map obtained by integrating (α_i will denote its ith component, obtained by integrating ω_i). It is possible to compute $c_{i,j}$, Λ and $\mathfrak{D}$ and to evaluate α at given points to high precision due to work of Paul Van-Wamalen implemented in `MAGMA` [BCP97].

Proposition 77. *For each disk $D \in \mathbb{T}$, we can find an explicit compact box $\alpha[D]$ in $\mathfrak{D}$ which contains the image $\alpha(D)$ of D under α, such that the diameters of such boxes tend to zero as $\tau \to 0$ uniformly in D.*

Write $\tilde{\tau}$ for such a uniform bound on the diameters.

Proof. Let p be the centre of D, and τ the radius of its projection to $\mathbb{P}^1(\mathbb{C})$. Without loss of generality, we assume $|x_p| \le |s_p|$. Throughout this proof, given $X \in \mathbb{C}$, $Y(X)$ will denote a square-root of $f(X)$, chosen to be continuous along radial paths if $p \in W$ and otherwise chosen to have no branch cuts in D (the cover $\mathbb{T}$ was carefully constructed so that this is possible).

Case 1: p not in W

Fix $q \in D$. We parametrise the path $\gamma = \gamma_{p,q}$ by $X(\gamma(t)) = X_p + (X_q - X_p)t$. Thus for all $i \in \{0, \dots, g-1\}$ we have

$$\begin{aligned} |\alpha_i(p) - \alpha_i(q)| &\le \left| \int_{\gamma_{p,q}} \frac{X^i}{Y(X)} \,\mathrm{d}\, X \right| \\ &\le \int_{\gamma_{p,q}} \left| \frac{X^i}{Y(X)} \right| \mathrm{d}\, X \\ &\le \int_0^1 \left| \frac{X(\gamma(t))^i}{Y(X(\gamma(t)))} \right| \left|\gamma'(t)\right| \mathrm{d}\, t \\ &\le \tau \sup_{r \in B_\tau(X_p)} \frac{|r|^i}{\left|\sqrt{f(r)}\right|} \end{aligned} \tag{6.81}$$

Case 2: $p \in W$

Fix $q \in D$. We parametrise the path $\gamma = \gamma_{p,q}$ by $X(\gamma(t)) = X_p + (X_q - X_p)t^{3/2}$.

Thus for all $i \in \{0, \dots, g-1\}$ we have

$$\begin{aligned} |\alpha(p)_i - \alpha(q)_i| &\leq \left| \int_{\gamma_{p,q}} \frac{X^i}{Y(X)} \, \mathrm{d}\, X \right| \\ &< \frac{3}{2} |X_p - X_q| \left| \int_0^1 \frac{X(\gamma(t))^i}{Y(X(\gamma(t)))} t^{1/2} \, \mathrm{d}\, t \right| \\ &\leq \frac{3}{2} \tau \sup_{r \in B_\tau(X_p)} \frac{|r|^i}{\left| \sqrt{f(r)/(r-p)} \right|} \end{aligned} \tag{6.82}$$

It is easy to check that the given bounds tend to zero uniformly with τ, so we are done. □

Lemma 78. *Fix $\epsilon > 0$. Let z, $w \in \mathbb{C}^g$ such that z lies within distance ϵ of the fundamental domain $\mathfrak{D}$, and w lies within distance ϵ of z (both distances in the L^1 metric). Let c_1 and c_2 be positive constants such that*

$$\max_i |\Im(z_i)| < \frac{c_1}{2\pi}, \qquad \text{and} \qquad \Im(\Lambda) \geq c_2 I_{g \times g}. \tag{6.83}$$

Set $t(n) = \sqrt{\pi c_2}(n - \frac{c_1}{2\pi c_2})$, and write

$$A = \exp(\frac{c_1^2}{4\pi c_2}) \left(\sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} e^{-t(n)^2} + \frac{1}{2\sqrt{c_2}} \right),$$

and

$$B = 2\pi e^{\frac{c_1^2}{4\pi c_2}} \left(\frac{1}{\sqrt{\pi c_2}} \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil + 1} t(n) e^{-t(n)^2} + \frac{1}{2\sqrt{c_2 \pi}} + \frac{c_1}{2\pi c_2} \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} e^{-t(n)^2} + \frac{c_1}{4\pi c_2^{3/2}} \right),$$

two constants independent of ϵ. Then we have the following bounds:

$$\begin{aligned} &1) \quad \left| \frac{\partial \vartheta}{\partial z_i}(z) \right| \leq 2^g A^{g-1} B \\ &2) \quad |\vartheta(z) - \vartheta(w)| \leq \epsilon 2^g A^{g-1} B. \end{aligned}$$

Suppose also that $|\vartheta(z)| \geq c > 2^g A^{g-1} B$. Then

$$\begin{aligned} &3) \quad \left| \frac{\partial (1/\vartheta)}{\partial z_i}(z) \right| \leq (c - \epsilon 2^g A^{g-1} B)^{-2} 2^g A^{g-1} B \\ &4) \quad \left| \frac{1}{\vartheta(z)} - \frac{1}{\vartheta(w)} \right| \leq \epsilon (c - \epsilon 2^g A^{g-1} B)^{-2} 2^g A^{g-1} B. \end{aligned}$$

Proof. Detailed background material for this proof may be found in [Mum83, II §1]. From the power series expansion

$$\vartheta(z) = \sum_{n\in\mathbb{Z}^g} \exp\left(\pi\imath n^t \Lambda n + 2\pi\imath n\cdot z\right), \tag{6.84}$$

(here $\imath$ denotes the a square-root of -1, to distinguish it from the index i) we see

$$\begin{aligned}
\left|\frac{\partial^r\vartheta}{\partial z_i^r}(z)\right| &= \left|\sum_{n\in\mathbb{Z}^g}\left(\exp\left(\pi\imath n^t\Lambda n + 2\pi\imath n\cdot z\right)(2\pi\imath n_i)^r\right)\right| \\
&\le \sum_{n\in\mathbb{Z}^g}\left(\exp\left(-\pi c_2\sum_i n_i^2 + c_1\sum_i |n_i|\right)(2\pi\imath n_i)^r\right) \\
&\le 2^g\sum_{n\in\mathbb{N}^g}\left(\exp\left(-\pi c_2\sum_i n_i^2 + c_1\sum_i n_i\right)(2\pi\imath n_i)^r\right) \\
&\le 2^g\left(\sum_{n\in\mathbb{N}}\exp\left(-\pi c_2 n^2 + c_1 n\right)\right)^{g-1}\left(\sum_{n\in\mathbb{N}}(2\pi n)^r\exp\left(-\pi c_2 n^2 + c_1 n\right)\right).
\end{aligned}$$

Now

$$\int_0^\infty x^r e^{-x^2}\,\mathrm{d}\,x = \frac{1}{2}\Gamma\left(\frac{1+r}{2}\right), \tag{6.85}$$

so recalling $t(n) = \sqrt{\pi c_2}(n - \frac{c_1}{2\pi c_2})$, we obtain

$$\begin{aligned}
&\sum_{n\in\mathbb{N}}\exp(-\pi c_2 n^2 + c_1 n) \\
&= \exp\left(\frac{c_1^2}{4\pi c_2}\right)\sum_{n\in\mathbb{N}}\exp(-t(n)^2) \\
&\le \exp\left(\frac{c_1^2}{4\pi c_2}\right)\left(\sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil}\exp(-t(n)^2) + \int_{n=\lceil\frac{c_1}{2\pi c_2}\rceil}^\infty \exp(-t(n)^2)\,\mathrm{d}\,n\right) \\
&\le \exp\left(\frac{c_1^2}{4\pi c_2}\right)\left(\sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil}\exp(-t(n)^2) + \frac{1}{\sqrt{\pi c_2}}\int_{t=0}^\infty \exp(-t^2)\,\mathrm{d}\,t\right) \\
&= \exp\left(\frac{c_1^2}{4\pi c_2}\right)\left(\sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil}\exp(-t(n)^2) + \frac{1}{2\sqrt{c_2}}\right).
\end{aligned}$$

Now we must do the same for $\sum_{n\in\mathbb{N}}(2\pi n)\exp(-\pi c_2 n^2 + c_1 n)$ (exactly the same

argument would work for the rth derivative, but we need only the first derivative):

$$\sum_{n\in\mathbb{N}}(2\pi n)\exp(-\pi c_2 n^2+c_1 n) = 2\pi\exp(\frac{c_1^2}{4\pi c_2})\sum_{n\in\mathbb{N}} n\exp(-t(n)^2)$$
$$= 2\pi\exp\left(\frac{c_1^2}{4\pi c_2}\right)\left(\frac{1}{\sqrt{\pi c_2}}\sum_{n\in\mathbb{N}} t(n)\exp(-t(n)^2)+\frac{c_1}{2\pi c_2}\sum_{n\in\mathbb{N}}\exp(-t(n)^2)\right).$$

Now

$$\begin{aligned}\sum_{n\in\mathbb{N}} t(n)\exp(-t(n)^2) &\leq \sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil+1} t(n)\exp(-t(n)^2)+\int_{n=\lceil\frac{c_1}{2\pi c_2}\rceil}^{\infty}|t(n)|\exp(-t(n)^2)\,\mathrm{d}\,n\\ &\leq \sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil+1} t(n)\exp(-t(n)^2)+\frac{1}{\sqrt{\pi c_2}}\int_{t=0}^{\infty} t\exp(-t^2)\,\mathrm{d}\,t\\ &= \sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil+1} t(n)\exp(-t(n)^2)+\frac{1}{2\sqrt{\pi c_2}},\end{aligned} \tag{6.86}$$

so combining the above results we find

$$\sum_{n\in\mathbb{N}}(2\pi n)\exp(-\pi c_2 n^2+c_1 n) \leq$$
$$2\pi\exp\left(\frac{c_1^2}{4\pi c_2}\right)\left(\frac{1}{\sqrt{\pi c_2}}\sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil+1} t(n)e^{-t(n)^2}+\frac{1}{2\sqrt{c_2\pi}}+\frac{c_1}{2\pi c_2}\sum_{n=0}^{\lceil\frac{c_1}{2\pi c_2}\rceil} e^{-t(n)^2}+\frac{c_1}{4\pi c_2^{3/2}}\right).$$

This concludes the computation of the bounds for (1). The bound for (2) is simple; it is simply ϵ times the bound for (1). For (3), we use

$$\frac{\partial(1/\vartheta)}{\partial z_i}(z) = \frac{-1}{\vartheta(z)^2}\frac{\partial\vartheta}{\partial z_i}(z) \tag{6.87}$$

to conclude that the bound for (3) is $(c-\epsilon 2^g A^{g-1}B)^{-2}$ times the bound for (1), and similarly that the bound for (4) is ϵ times the bound for (3).

□

Proposition 79. *Let $\mathscr{D}_1$ and $\mathscr{D}_2$ be a pair of disjoint disks in $\mathbb{T}$, with centres p_1 and p_2 respectively. Then (possibly after shrinking μ), there exists a computable bound*

$\beta = \beta(\mathscr{D}_1, \mathscr{D}_2) > 0$ *such that for all* $q_1 \in \mathscr{D}_1$ *and* $q_2 \in \mathscr{D}_2$*, we have*

$$|g_{p_1-\infty}(p_2) - g_{q_1-\infty}(q_2)| \leq \beta. \tag{6.88}$$

Proof. We will use notation from Section 5.7.3. Let F be a degree-g divisor such that neither $\alpha(F)$ nor the coset $\alpha(F) + \mathscr{D}_1$ meet the theta divisor on the analytic Jacobian; this is possible for sufficiently small μ. Let F_{p_1} denote the amenable divisor in the class of $F + p_1 - \infty$, and similarly let F_{q_1} denote the amenable divisor in the class of $F + q_1 - \infty$. Now recall from Section 5.7.3 that

$$\begin{aligned} g_{F_{p_1}-F}(p_2) = 2\log\left|\frac{\vartheta(\alpha(p_2)+\Delta-\alpha(F_{p_1}))}{\vartheta(\alpha(p_2)+\Delta-\alpha(F))}\right| \\ + 4\pi(\Im(\Omega))^{-1}\cdot\Im(\alpha(F_{p_1})-\alpha(F))\cdot\Im\left(\alpha(p_2)\right). \end{aligned}$$

and similarly for q_1, Subtracting, we obtain

$$\begin{aligned} &g_{F_{p_1}-F}(p_2) - g_{q_1-\infty}(q_2) = \\ &2\log\left|\frac{\vartheta(\alpha(p_2)+\Delta-\alpha(F_{p_1}))}{\vartheta(\alpha(p_2)+\Delta-\alpha(F))}\right| - 2\log\left|\frac{\vartheta(\alpha(q_2)+\Delta-\alpha(F_{q_1}))}{\vartheta(\alpha(q_2)+\Delta-\alpha(F))}\right| \\ &+ 4\pi(\Im(\Omega))^{-1}\cdot\left(\Im(\alpha(F_{p_1})-\alpha(F))\cdot\Im\left(\alpha(p_2)\right) - \Im(\alpha(F_{q_1})-\alpha(F))\cdot\Im\left(\alpha(q_2)\right)\right). \end{aligned}$$

Now

$$\left|2\log\left|\frac{\vartheta(\alpha(p_2)+\Delta-\alpha(F_{p_1}))}{\vartheta(\alpha(p_2)+\Delta-\alpha(F))}\right| - 2\log\left|\frac{\vartheta(\alpha(q_2)+\Delta-\alpha(F_{q_1}))}{\vartheta(\alpha(q_2)+\Delta-\alpha(F))}\right|\right|$$

may be effectively bounded using Lemma 78, and

$$|(\Im(\alpha(F_{p_1})-\alpha(F))\cdot\Im\left(\alpha(p_2)\right) - \Im(\alpha(F_{q_1})-\alpha(F))\cdot\Im\left(\alpha(q_2)\right))|$$

is trivially bounded since $\alpha(p_1)$ is close to $\alpha(q_1)$ and $\alpha(p_2)$ is close to $\alpha(q_2)$. □

The proof of Proposition 66 is now complete. We have shown that any two points of $C(\mathbb{C})$ which are at least distance μ apart can be put into disjoint disks in a cover consisting of lifts of permissible boxes (Lemma 75), and have then shown how to compute bounds on the difference between the Green's function computed at the centre of the disks to the Green's function evaluated at any points in the disks (Proposition 79). Using results from Chapter 5 we can evaluate the Green's function at the centres of the disks, since there are only finitely many disks in the cover.

6.5 Archimedean II: the case of divisors approaching the diagonal

In this section, we work over the complex numbers; in particular, all points are complex points, and all norms are Euclidean.

In Section 6.4 we gave an algorithm which, given a constant $\mu > 0$ and a pair of distinct Weierstrass points ∞ and $\tilde{\infty}$, will give an explicit constant $M(\mu) > 0$ such that given any two points p, $q \in C(\mathbb{C})$ we have

$$\mathrm{d}(p, \tilde{\infty}) \geq \mu \text{ and } \mathrm{d}(q, \infty) \geq \mu \text{ and } \mathrm{d}(p, q) \geq \mu \implies |g_{p-\infty}(q - \tilde{\infty})| \leq M(\mu). \tag{6.89}$$

In this section, we will show that as p approaches q the Green's function above exhibits a logarithmic pole, in an explicitly described manner. This result should be seen as analogous to the appearance of the symbol $\log^+ |x(p)|_\nu$ in the classical definition of the local height on an elliptic curve.

The idea we will use to achieve this is a simple one; when two points p and q are close together we will move one of the away by linear equivalence in a prescribed fashion, and then apply (6.89) to the new pair of points. In order to turn this into an effective algorithm, two ingredients are needed:

1) we need to find a systematic way of moving points by linear equivalence, so that uniform bounds will result.

2) we need to determine how moving by linear equivalence affects the Green's function.

Definition 80. *Given two divisors with disjoint support, $D = \sum_i a_i p_i$ and $E = \sum_j b_j q_j$, we set*

$$\mathrm{d}(D, E) = \prod_{i,j} \mathrm{d}(p_i, q_j)^{a_i b_j}. \tag{6.90}$$

Given also a rational function ϕ whose divisor has support disjoint from D, we define $\phi[D]$ to be the norm of ϕ from the residue field of D to K if D is a prime divisor, and then extend multiplicatively to all divisors.

Lemma 81. *Suppose $\mu > 0$. Let D and E be a pair of divisors of degree 0, and let ϕ be a rational function on C such that for all p appearing in the support of $D - \mathrm{div}(\phi)$ and for all q appearing in the support of E, we have $\mathrm{d}(p, q) \geq \mu$.*

Write $D - \mathrm{div}(\phi) = D' = D'^+ - D'^-$ where D'^+ and D'^- are both effective, and write $E = E^+ - E^-$ where again E^+ and E^- are both assumed effective. Suppose also that D'^- and E^- are supported on Weierstrass points (this is just to improve

the constants). Then

$$|g_D(E) + \log(\mathrm{d}(D,E))| \leq M(\mu)\deg(D'^{+})\deg(E^{+}) + \left|\log\left|\frac{\mathrm{d}(D,E)}{\phi[E]}\right|\right|. \tag{6.91}$$

Proof. A basic property of Green's functions is that

$$g_{\mathrm{div}(\phi)}(E) = -\log|\phi[E]|, \tag{6.92}$$

and so

$$g_D(E) = g_{D'}(E) - \log|\phi[E]|. \tag{6.93}$$

Now from Equation (6.89) we have

$$|g_{D'}(E)| \leq M(\mu)\deg(D'^{+})\deg(E^{+}), \tag{6.94}$$

so

$$\begin{aligned} |g_D(E) + \log(\mathrm{d}(D,E))| &= |g_{D'}(E) - \log|\phi[E]| + \log(\mathrm{d}(D,E))| \\ &\leq M(\mu)\deg(D'^{+})\deg(E^{+}) + \left|\log\left|\frac{\mathrm{d}(D,E)}{\phi[E]}\right|\right| \end{aligned} \tag{6.95}$$

as required. □

6.5.1 Some constants

In this section we will define various constants we will need later. Their existence is in general obvious from compactness arguments, but the important point is that we can find the constants explicitly; we give algorithms to do so.

The function Δf

Given a polynomial $f \in \mathbb{C}[X]$, define $\Delta f \in \mathbb{C}(X_1, X_2)$ by

$$\Delta f(X_1, X_2) = \frac{f(X_1) - f(X_2)}{X_1 - X_2}. \tag{6.96}$$

It is clear that in fact $\Delta f \in \mathbb{C}[X_1, X_2]$ since $X_1^n - X_2^n = (X_1 - X_2)(X_1^{n-1} + \cdots + X_2^{n-1})$.

Lemma 82. *Let $w \in \mathbb{C}$ be a root of f, and suppose $\epsilon > 0$ is such that for all $t \in \overline{B_\epsilon t}$ (the closed ball of radius ϵ around t in the Euclidean metric on $\mathbb{C}$) we have $\frac{\mathrm{d}f}{\mathrm{d}X}(t) \neq 0$ (in particular, w is not a repeated root). Then Δf has no zeros on $\overline{B_\epsilon t} \times \overline{B_\epsilon t}$.*

Proof. Say $\Delta f(t_1, t_2) = 0$. Then $f(t_1) = f(t_2)$, but we can apply the inverse function theorem to f on $\overline{B_\epsilon t}$ since the derivative does not vanish, and so if t_1 and $t_2 \in \overline{B_\epsilon t}$ then $t_1 = t_2$. It thus suffices to consider this case. Fix $t_1 \in \overline{B_\epsilon t}$, and consider $g(t) \stackrel{\text{def}}{=} \Delta f(t_1, t)$. Clearly g is continuous, and as $t \to t_1$ we see $g(t) \to \frac{\mathrm{d}\, f}{\mathrm{d}\, X}(t_1)$. By continuity, $\Delta f(t_1, t_1) = \frac{\mathrm{d}\, f}{\mathrm{d}\, X}(t_1) \neq 0$ by assumption. □

Now computing such an ϵ is easy, and since Δf is an easily computed polynomial, it is also easy to bound $|\Delta f|$ on $\overline{B_\epsilon t}$.

Lemma 83. *Fix $\epsilon > 0$. Then there exists a computable constant $\delta_1(\epsilon)$ such that for all $p \in C(\mathbb{C})$ and all Weierstrass points d:*

$$\left(s_d \neq 0 \text{ and } |x_p| \leq |s_p| \text{ and } \left|y_p / s_p^{g+1}\right| \geq \epsilon\right) \implies |x_p/s_p - x_d/s_d| \geq \delta_1(\epsilon), \quad (6.97)$$

and

$$\left(x_d \neq 0 \text{ and } |x_p| \geq |s_p| \text{ and } \left|y_p / x_p^{g+1}\right| \geq \epsilon\right) \implies |s_p/x_p - s_d/x_d| \geq \delta_1(\epsilon) \quad (6.98)$$

Proof. Fixing $p \in C(\mathbb{C})$, we may without loss of generality assume that $|x_p| \leq |s_p|$. Let D denote the set of Weierstrass points d such that $s_d \neq 0$. Write d_0 for a Weierstrass point minimising $\delta \stackrel{\text{def}}{=} |x_p/s_p - x_{d_0}/s_{d_0}|$. Let

$$m = \max_{d_1, d_2 \in D} \left|x_{d_1}/s_{d_1} - x_{d_2}/s_{d_2}\right|. \quad (6.99)$$

Then

$$|Y_p| \geq \epsilon \Leftrightarrow |f(X_p)| \geq \epsilon^2 \Leftrightarrow \prod_{d \in D} |x_p/s_p - x_d/s_d| \geq \epsilon^2 \implies \delta(\delta + m)^{\#D-1} \geq \epsilon^2, \quad (6.100)$$

from which the result is clear. □

Lemma 84. *Fix $\epsilon > 0$. There exists a computable constant $\delta_2(\epsilon)$ such that*

$$|x_p| \leq \epsilon\, |s_p| \implies \left|y_p / s_p^{g+1}\right| \leq \delta_2(\epsilon), \quad (6.101)$$

and

$$|s_p| \geq \epsilon\, |x_p| \implies \left|y_p / x_p^{g+1}\right| \leq \delta_2(\epsilon). \quad (6.102)$$

Proof. Assume $|x_p| \leq \epsilon\, |s_p|$, and write $X = x_p/s_p$, $Y = y_p/s_p^{g+1}$. Now $Y^2 = f(X)$,

so writing $f(t) = \sum_i f_i t^i$, set

$$\delta_2(\epsilon) = \sum_i |f_i| \, \epsilon^i, \tag{6.103}$$

and we are done by repeatedly applying the triangle inequality. For the second equation, use the reciprocal polynomial of f, and then take the larger of the two resulting bounds. □

Lemma 85. *Fix $\delta > 0$ and $0 < \epsilon < \min(1/2, 2\delta_2(\delta)/(1+\delta_2(\delta))^2)$. Then there exists a computable constant $\delta_3(\delta, \epsilon)$ tending to zero with ϵ such that for all $p \in C(\mathbb{C})$ with $\mathrm{d}(p, p^-) \leq \epsilon$ we have:*

$$|x_p| \leq \delta \, |s_p| \implies \left|y_p / s_p^{g+1}\right| \leq \delta_3(\delta, \epsilon), \tag{6.104}$$

and

$$|s_p| \leq \delta \, |x_p| \implies \left|y_p / x_p^{g+1}\right| \leq \delta_3(\delta, \epsilon). \tag{6.105}$$

Proof. Say $|x_p| \leq \delta \, |s_p|$, and write $a = \left|y_p / s_p^{g+1}\right|$ and $d = \delta_2(\delta)$, so $a \leq d$. Now

$$\epsilon \geq \mathrm{d}(p, p^-) \geq 2a/(1+a)^2, \tag{6.106}$$

or equivalently

$$a^2 + (2 - 2/\epsilon)a + 1 \geq 0. \tag{6.107}$$

Now since $a \geq 0$, this implies that either

$$1) \quad a \leq (1 - \epsilon - \sqrt{1-2\epsilon})/\epsilon \tag{6.108}$$

or

$$2) \quad a \geq (1 - \epsilon + \sqrt{1-2\epsilon})/\epsilon, \tag{6.109}$$

both of which are real since $\epsilon \leq 1/2$. However, in case (2) we have

$$d \geq a \geq (1 - \epsilon + \sqrt{1-2\epsilon})/\epsilon, \tag{6.110}$$

which contradicts $\epsilon < 2\delta_2(\delta)/(1+\delta_2(\delta))^2$, so (1) must hold. Setting

$$\delta_3(\delta, \epsilon) = (1 - \epsilon + \sqrt{1-2\epsilon})/\epsilon, \tag{6.111}$$

one easily checks that $|\delta_3(\delta, \epsilon)| \leq \epsilon/3$, so we are done. □

Lemma 86. *Fix $\epsilon > 0$. There exists a constant $\delta_4(\epsilon) > 0$ such that for all $p \in C(\mathbb{C})$*

such that $|x_p| \leq |s_p|$ *and* $\left|y_p/s_p^{g+1}\right| \leq \epsilon$*, there exists a Weierstrass point* d *with* $s_d \neq 0$ *such that*

$$|x_p/s_p - x_d/s_d| \leq \delta_4(\epsilon). \tag{6.112}$$

The same holds with x *and* s *interchanged.*

Proof. Let D denote the set of Weierstrass points d such that $s_d \neq 0$. Now

$$\left|y_p/s_p^{g+1}\right| \leq \epsilon \Leftrightarrow |f(x_p/s_p)| \leq \epsilon^2 \Leftrightarrow \prod_{d\in D} |x_p/s_p - x_d/s_d| \leq \epsilon^2, \tag{6.113}$$

and this implies that there exists a Weierstrass point $d \in D$ such that

$$|x_p/s_p - x_d/s_d| \leq \epsilon^{2/\#D}. \tag{6.114}$$

Setting $\delta_4(\epsilon) = \epsilon^{2/\#D}$, we are done. □

Lemma 87. *Fix* $\epsilon > 0$*. there exists a computable constant* $\delta_5(\epsilon) > 0$ *with the property that for all* $p \in C(\mathbb{C})$ *with* $\mathrm{d}(p, p^-) \geq \epsilon$*, we have either*

$$\left|y_p/s_p^{g+1}\right| \geq \delta_5(\epsilon) \tag{6.115}$$

or

$$\left|y_p/x_p^{g+1}\right| \geq \delta_5(\epsilon). \tag{6.116}$$

Proof. Write $a = \left|y_p/s_p^{g+1}\right|$ and $b = \left|y_p/x_p^{g+1}\right|$. Now

$$\epsilon \leq \mathrm{d}(p, p^-) = \frac{2a}{(1+a)^2} + \frac{2b}{(1+b)^2}, \tag{6.117}$$

so without loss of generality say $a/(1+a)^2 \geq \epsilon/4$, which rearranges to

$$0 \geq 1 + (2 - 4/\epsilon)a + a^2. \tag{6.118}$$

Solving, and setting $\delta_5(\epsilon) = (2 - \epsilon - 2\sqrt{1-\epsilon})/\epsilon > 0$, we are done. □

Lemma 88. *Fix* $\delta \geq 0$ *and* $\epsilon < 1/(1+\delta)$*. Then there exists a constant* $\delta_6(\delta, \epsilon) \geq 0$ *such that for all* p*,* $q \in C(\mathbb{C})$ *with*
1) $\mathrm{d}(p, q) \leq \epsilon$*, and*
2) $|x_p| \leq \delta\,|s_p|$*,*
we have $|x_q| \leq |s_q|\,\delta_6(\delta, \epsilon)$*.*

Proof. Set

$$\delta_6(\delta,\epsilon) = \frac{\delta + \epsilon(1+\delta)}{1-\epsilon(1+\delta)} > \delta. \tag{6.119}$$

We may assume $|X_q| \leq \delta$, otherwise the result is obvious. Then

$$\epsilon \geq \frac{|X_p - X_q|}{(1+|X_p|)(1+|X_q|)} \geq \frac{|X_q| - \delta}{(1+|X_q|)(1+\delta)}, \tag{6.120}$$

which using $\epsilon < 1/(1+\delta)$ rearranges to

$$|X_q| \leq \frac{\delta + \epsilon(1+\delta)}{1-\epsilon(1+\delta)} \tag{6.121}$$

as required. □

Lemma 89. *Given $\epsilon > 0$, there exists a computable constant $\delta > 0$ such that for all $p \in C(\mathbb{C})$ and Weierstrass points $w \in W$, if $|X_p| \leq 1$ and $\mathrm{d}(p, p^-) \geq \epsilon$ then $|X_p - X_w| \geq \epsilon$.*

Proof. Write $\mathrm{d}_2 = \mathrm{d}_2(p,p^-)$ and $\mathrm{d}_3 = \mathrm{d}_3(p,p^-)$, and $X = X_p$, $Y = Y_p$. . We begin by finding a sufficiently small constant $R > 0$ such that:
1) if $(0:1:0) \in W$ then $\overline{B_{2R}(0)} \cap W = \{(0:1:0)\}$.
2) if $(0:1:0) \notin W$ then $\overline{B_{2R}(0)} \cap W = \emptyset$
Case 1: $|X_p| \geq R$.
Let $\epsilon_1 = \max(1/R^{g+1}, R^{g+1})$.

Claim 90. $\mathrm{d}_2 \leq \epsilon_1 \, \mathrm{d}_3$.

Proof of claim.

$$\begin{aligned} &\mathrm{d}_2 \leq \epsilon_1 \, \mathrm{d}_3 \iff \mathrm{d}_2 \,/\, \mathrm{d}_3 \leq \epsilon_1 \\ &\iff |X|^{g+1} (1+|Y|)^2 \leq \epsilon_1 (|X|^{g+1} + |Y|)^2 \\ &\iff 0 \leq |X|^{g+1} (\epsilon_1 |X|^{g+1} - 1) + 2(\epsilon_1 - 1)|Y| \, |X|^{g+1} + (\epsilon_1 - |X|^{g+1}) |Y|^2 . \end{aligned} \tag{6.122}$$

□

Thus $\epsilon \leq \mathrm{d}_2 + \mathrm{d}_3 \leq (1+\epsilon_1)\,\mathrm{d}_3$. Writing $\epsilon_2 = (\epsilon - \epsilon_1 - 1)/\epsilon$ and using that $\mathrm{d}(p,p^-) \geq \epsilon$, we find

$$0 \geq 1 + 2\epsilon_2 |Y| + |Y|^2 , \tag{6.123}$$

which shows for ϵ sufficiently small that

$$0 < -\epsilon_2 - \sqrt{\epsilon_2^2 - 1} \leq |Y| \leq -\epsilon_2 + \sqrt{\epsilon_2^2 - 1}. \tag{6.124}$$

Writing $\epsilon_3 = -\epsilon_2 - \sqrt{\epsilon_2^2 - 1} > 0$, we find by Lemma 83 that for all Weierstrass points $w \in W$ we have $|X - X_w| \geq \delta_1(\epsilon_3)$, so take $\delta_7 = \delta_1(\epsilon_3)$.

Case 2: $|X| \leq R$.

Case 2.1: $(0:1:0) \notin W$.

Then since $\overline{B_{2R}(0)} \cap W = \emptyset$, we can take $\delta_7 = R$.

Case 2.1: $(0:1:0) \in W$.

We easily compute constants $0 < c_1 \leq c_2$ such that $c_1 |X| \leq |Y|^2 \leq c_2 |X|$. Set

$$\epsilon_1 = \frac{R^g}{\sqrt{c_1}} \left(1 + 2\sqrt{c_2} R^{1/2} + \sqrt{c_1} R\right), \tag{6.125}$$

then shrink R until $\epsilon_1 \leq 1$.

Claim 91. $\mathrm{d}_2 \leq \epsilon_1 \, \mathrm{d}_3$.

Proof of claim.

$$\begin{aligned}
&\mathrm{d}_2 \leq \epsilon_1 \, \mathrm{d}_3 \\
&\Leftrightarrow 0 \leq |X|^{g+1} \left(\epsilon_1 |X|^{g+1} - 1\right) + 2(\epsilon_1 - 1) |Y| \, |X|^{g+1} + (\epsilon_1 - |X|^{g+1}) |Y|^2 \\
&\Leftarrow 0 \leq |X|^{g+1} \left(\epsilon_1 |X|^{g+1} - 1\right) + 2(\epsilon_1 - 1)\sqrt{c_2} \, |X|^{g+3/2} + (\epsilon_1 - |X|^{g+1})\sqrt{c_1} \, |X| \\
&\Leftrightarrow |X|^{g+1} + 2\sqrt{c_2} \, |X|^{g+3/2} + |X|^{g+2} \sqrt{c_1} \leq \epsilon_1 \left(|X|^{2g+2} + 2\sqrt{c_2} \, |X|^{g+3/2} + |X| \sqrt{c_1}\right) \\
&\Leftarrow |X|^g \left(1 + 2\sqrt{c_2} \, |X|^{1/2} + \sqrt{c_1} \, |X|\right) \leq \sqrt{c_1} \epsilon_1 \\
&\Leftarrow R^g \left(1 + 2\sqrt{c_2} R^{1/2} + \sqrt{c_1} R\right) \leq \sqrt{c_1} \epsilon_1.
\end{aligned} \tag{6.126}$$

□

We now proceed as in Case 1, writing $\epsilon_2 = (\epsilon - \epsilon_1 - 1)/\epsilon$, to find that for all Weierstrass points $w \in W$ we have

$$|X - X_w| \geq \delta_1(-\epsilon_2 - \sqrt{\epsilon_2^2 - 1}). \tag{6.127}$$

□

Lemma 92. *Given $\epsilon > 0$, there exists a computable constant $\delta_8(\epsilon) > 0$ such that for all points $p \in C(\mathbb{C})$ and all Weierstrass points $w \in W$, if $|X_p| \leq 1$ and $\mathrm{d}(p, w) \geq \epsilon$*

then $|X_p - X_w| \geq \delta_8(\epsilon)$.

Proof. This lemma may be proven in a way almost identical to that of Lemma 89 □

Lemma 93. *Fix* $\epsilon > 0$. *There exists a computable constant* $\delta_9(\epsilon) > 0$ *such that for all* $p \in C(\mathbb{C})$ *such that* $\mathrm{d}(p, p^-) \geq \epsilon$, *and for all Weierstrass points* d, *we have*

$$\mathrm{d}_2(p, d) \geq \delta_9(\epsilon) \tag{6.128}$$

or

$$\mathrm{d}_3(p, d) \geq \delta_9(\epsilon). \tag{6.129}$$

Proof. Without loss of generality, suppose $|X_p| \leq 1$. Using Lemma 89, we may construct a compact subset D of $\mathbb{C}$ such that

$$\mathrm{d}(p, p^-) \geq \epsilon \Rightarrow X_p \in D. \tag{6.130}$$

Now $\mathrm{d}_3(p, d) = |Y_p| / (1 + |Y_p|)$ is a ratio of two non-vanishing polynomials on D considered as a subset of $\mathbb{R}^2$, and so we can bound the derivative of $\mathrm{d}_3(p, d)$ and thus bound its values numerically.

□

Lemma 94. *Fix* $\epsilon > 0$. *There exists a computable constant* $\delta_{10}(\epsilon) > 0$ *such that for all* $p \in C(\mathbb{C})$ *such that* $\mathrm{d}(p, p^-) \geq \epsilon$ *and for all Weierstrass points* d, *we have*

$$\mathrm{d}_1(d, p) \geq \delta_{10}(\epsilon). \tag{6.131}$$

Proof. We consider the case $|X_p| \leq 1$. Using Lemma 89 we may construct a compact subset D of $\mathbb{C}$ containing no Weierstrass points and such that $X_p \in D$. The result then follows easily.

□

Lemma 95. *Fix a sufficiently small* $\epsilon > 0$. *There exists a constant* $\delta_{11}(\epsilon) > 0$ *such that for all points* $p \neq q \in C(\mathbb{C})$ *with* $\mathrm{d}(p, p^-) \geq \epsilon$, $\mathrm{d}(q, q^-) \geq \epsilon$ *and* $\mathrm{d}(p, q) \leq \epsilon$, *we have*

$$(1) \quad \frac{\mathrm{d}_2(p, q)}{\mathrm{d}_1(p, q)} \leq \delta_{11}(\epsilon) \tag{6.132}$$

and

$$(2) \quad \frac{\mathrm{d}_3(p, q)}{\mathrm{d}_1(p, q)} \leq \delta_{11}(\epsilon) \tag{6.133}$$

Proof. Appealing to symmetry, we only prove assertion (2). Write $X_p = x_p/s_p$, $Y_p = y_p/s_p^{g+1}$ and similarly for q. Fix a constant $R > 0$ such that $|X| \geq 1/\delta_6(1/R) \implies |X^g/f(X)| < 2$.

Case 1: $|X_p| \leq R$.

Then $|X_q| \leq \delta_6(R, \epsilon)$, so $|Y_p| \leq \delta_2(R)$ and $|Y_q| \leq \delta_2(\delta_6(R, \epsilon))$.

Now $Y^2 = f(X)$, so there exists a bivariate polynomial $\Delta(f)$ such that

$$Y_p^2 - Y_q^2 = (X_p - X_q)\Delta(f)(X_p, X_q), \tag{6.134}$$

so

$$\frac{\mathrm{d}_3(p,q)}{\mathrm{d}_1(p,q)} = \frac{\Delta(f)(X_p, X_q)(1+|X_p|)(1+|X_q|)}{|Y_p + Y_q|\,(1+|Y_p|)(1+|Y_q|)}. \tag{6.135}$$

Moreover, the conditions $\mathrm{d}(p, p^-) \geq \epsilon$ and $\mathrm{d}(q, q^-) \geq \epsilon$ keep p and q away from Weierstrass points, and the condition $\mathrm{d}(p, q) \leq \epsilon$ keeps them close together, so we find that for small enough ϵ the function $|Y_p + Y_q|$ has no zeros. As such, the right hand side of (6.135) is a rational function on a compact set with no poles, and so we can bound its derivatives and then bound it numerically.

Case 2: $|X_p| > R$.

Write $S_p = s_p/x_p$, and similarly for q, so $|S_p| \leq 1/R$ and $|S_q| \leq 1/\delta_6(R, \epsilon)$, and similarly we obtain positive lower bounds on $|Y_p|$ and $|Y_q|$. Now

$$\frac{\mathrm{d}_3(p,q)}{\mathrm{d}_1(p,q)} = \frac{(1+|S_p|)(1+|S_q|)}{(1+|1/Y_p|)(1+|1/Y_q|)} \frac{|1/Y_p - 1/Y_q|}{|1/X_p - 1/X_q|}, \tag{6.136}$$

and it is clear that $\frac{(1+|S_p|)(1+|S_q|)}{(1+|1/Y_p|)(1+|1/Y_q|)}$ is bounded above, so it remains to bound above the expression

$$\frac{|1/Y_p - 1/Y_q|}{|1/X_p - 1/X_q|} = \frac{|Y_p - Y_q|\,|X_p X_q|}{|X_p - X_q|\,|Y_p Y_q|} = \frac{\left|Y_p^2 - Y_q^2\right|\,|X_p X_q|}{|Y_p + Y_q|\,|X_p - X_q|\,|Y_p Y_q|}. \tag{6.137}$$

Writing $\tilde{f}$ for the reciprocal polynomial of f and d for its degree (both taken as homogeneous polynomials), we find

$$\begin{aligned} \frac{|f(X_p) - f(X_q)|\,|X_p X_q|}{|Y_p + Y_q|\,|X_p - X_q|\,|Y_p Y_q|} &= \frac{\left|S_q^d \tilde{f}(S_p) - S_p^d \tilde{f}(S_q)\right|}{|Y_p + Y_q|\,|S_p - S_q|\left|\tilde{f}(S_p)\tilde{f}(S_q)\right|} \\ &\leq \frac{\left|S_q^d \tilde{f}(S_p) - S_p^d \tilde{f}(S_q)\right|}{|S_p - S_q|\left|\tilde{f}(S_p)\tilde{f}(S_q)\right|} \times \text{const.} \end{aligned} \tag{6.138}$$

Now there exists a computable bivariate polynomial G such that

$$S_q^d \tilde{f}(S_p) - S_p^d \tilde{f}(S_q) = (S_p - S_q)G(S_p, S_q), \tag{6.139}$$

and moreover that if $\tilde{f}(0) = 0$ (so there is a Weierstrass point at $S = 0$) then $G(S_p, S_q)$ is divisible by $S_p S_q$. As such, in the even-degree case we bound numerically the function

$$\frac{|G(S_p, S_q|}{\left|\tilde{f}(S_p)\tilde{f}(S_q)\right|} \tag{6.140}$$

on the compact set $|S_p| \leq R$, $|S_q| \leq 1/\delta_6(R, \epsilon)$, and in the odd-degree case we similarly bound

$$\frac{|G(S_p, S_q)/(S_p S_q)|}{\left|\tilde{f}(S_p)/S_p\right|\left|\tilde{f}(S_q)/S_q\right|}. \tag{6.141}$$

□

Lemma 96. *Fix $\epsilon > 0$. There exists a computable constant $\delta_{12}(\epsilon) > 0$ such that for all $p \in C(\mathbb{C})$ and all Weierstrass points d such that $\mathrm{d}(p, d) \geq \epsilon$, we have*

$$\frac{\mathrm{d}_2(p, d)}{\mathrm{d}_1(p, d)} \leq \delta_{12}(\epsilon) \tag{6.142}$$

and

$$\frac{\mathrm{d}_3(p, d)}{\mathrm{d}_1(p, d)} \leq \delta_{12}(\epsilon). \tag{6.143}$$

Proof. By symmetry, it suffices to do the case of d_3. Since $\mathrm{d}_3(d, p) \leq 1$, it suffices to bound $\mathrm{d}_1(d, p)$ below. Now $\mathrm{d}(p, d) \geq \epsilon$, so Lemma 92 supplies the required lower bound on $\mathrm{d}_1(d, p)$. □

Before going further, we need to find a value of the constant μ which is small enough that we can always move divisors to be at least distance μ apart (for example, $\mu > 3$ won't do, since no two points on C are of distance greater than 3 apart). We begin with an easy lemma.

Lemma 97. *Let a be a complex polynomial in z with a root α, and let $r > 0$ be such that for all $t \in \mathrm{B}_r(\alpha)$, $|a'(t)| > 0$. Then $\mathrm{roots}(a) \cap \mathrm{B}_r(\alpha) = \{\alpha\}$.*

Proof. Let $\beta \in \mathrm{roots}(a)$ and let γ be a straight path from α to β. Then $a(\beta) = 0 = a(\alpha) + \int_\gamma a' = \int_\gamma a'$. Suppose $\beta \in \mathrm{B}_r(\alpha)$, so γ is contained in $\mathrm{B}_r(\alpha)$. Then $|a(\beta)| \geq \int_\gamma |a'| > 0$, a contradiction. □

Proposition 98. *There exist positive real constants μ, ϵ and λ such that the following conditions hold:*

Given $p \in C(\mathbb{C})$ such that $\mathrm{d}(p, p^-) \leq \epsilon$, let

$$\phi = (y - y(p)) - \lambda(x - x(p))^{g+1} \tag{6.144}$$

and let $P = \mathrm{zeros}_C(\phi) \setminus \{p\}$. Then for all $p' \in P$ and for all Weierstrass points d, we have

$$\mathrm{d}(p, p') > \mu \quad \textit{and} \quad \mathrm{d}(p', d) > \mu. \tag{6.145}$$

Proof. Without loss of generality, we may assume $|x_p| \leq |s_p|$. Since $\mathrm{d}(p, p^-) \leq \epsilon$, we have $|Y_p| \leq \delta_3(1, \epsilon)$, which tends to 0 as $\epsilon \to 0$. Thus there exists a Weierstrass point d_0 such that $|X_p - X_{d_0}| \leq \delta_4(\delta_3(1, \epsilon))$. Since there are only finitely many Weierstrass points, there exists a constant $\mu_1 > 0$ such that for all other Weierstrass points $d' \neq d_0$, we have $|X_{d_0} - X_{d'}| \geq \mu_1$.

Next, we must look at the function ϕ. Say $p' \in P$ is another zero of ϕ on C. We start by showing that we can adjust λ or ϵ so as to make p' avoid all Weierstrass points $d \neq d_0$. Let D denote the set of Weierstrass points $d \neq d_0$ such that $s_d \neq 0$. Write $\mu_2 = \frac{1}{2} \min_{d \in D} |X_d - X_{d_0}|$. We first assume $\left|X_p - X_{p'}\right| \geq \mu_2$. Now

$$|Y_p| + \left|Y_{p'}\right| \geq \left|Y_p - Y_{p'}\right| = \lambda \left|X_p - X_p'\right|^{g+1} \geq \lambda \mu_2^{g+1}, \tag{6.146}$$

so it suffices to bound $\lambda \mu_2^{g+1} - |Y_p|$ below, using $|Y_p| \leq \delta_3(\epsilon)$ which tends to 0 as $\epsilon \to 0$. Clearly, this can be achieved either by shrinking ϵ or growing λ. We thus obtain an effective positive lower bound on $\left|Y_{p'}\right|$, call it c. Thus for all Weierstrass points d we have

$$\mathrm{d}_3(p', d) = \frac{\left|Y_{p'}\right|}{(1 + \left|Y_{p'}\right|)} \geq \frac{c}{c+1} > 0. \tag{6.147}$$

We now need to adjust the constants so that p' avoids the Weierstrass point d_0. Writing $\zeta = \left|X_p - X_{p'}\right|$, we will bound ζ below by a constant which does not tend to zero with ϵ, and so by shrinking ϵ this forces p' away from d_0.

Possibly after shrinking ϵ, there exists a constant $c_1 > 0$ such that for all X with $|X - X_{d_0}| \leq \zeta + \delta_4(\delta_3(1, \epsilon))$, we have $|f'(X)| \geq c_1$. Thus, applying the inverse function theorem, f^{-1} exists locally near X_{d_0}, and setting $c_2 = 1/c_1 > 0$ we find that for all t such that $\left|f^{-1}(t) - X_{d_0}\right| \leq \zeta + \delta_4(\delta_3(1, \epsilon))$ we have $\left|f^{-1\prime}(t)\right| \leq c_2$. From this it follows that

$$\left|f(X_p) - f(X_{p'})\right| \geq \left|X_p - X_{p'}\right| / c_2 = \zeta / c_2. \tag{6.148}$$

Observe that

$$\left|f(X_p) - f(X_{p'})\right| = \left|Y_p^2 - Y_{p'}^2\right| = \left|Y_p + Y_{p'}\right| \left|Y_p - Y_{p'}\right| \leq \lambda\zeta^{g+1}(\delta_3(1,\epsilon) + \lambda\zeta^{g+1}), \tag{6.149}$$

and so by substituting we see

$$\lambda\zeta^{g+1}(1 + \lambda\zeta^{g+1}) \geq \lambda\zeta^{g+1}(\delta_3(1,\epsilon) + \lambda\zeta^{g+1}) \geq \left|f(X_p) - f(X_{p'})\right| \geq \zeta/c_2, \tag{6.150}$$

which gives a positive lower bound on ζ depending only on λ and c_2, call it c_4.

We have shown that $\left|X_p - X_{p'}\right| \geq c_4 > 0$. Now $|X_p - X_{d_0}| \leq \delta_4(\delta_3(1,\epsilon))$ which tends to 0 with ϵ, so combining this with (6.147) and shrinking ϵ we find a positive constant $c_3 > 0$ such that $\left|X_{p'} - X_{d_0}\right| \geq c_3$. Further, we may assume $\left|X_p - X_{p'}\right| \leq \mu_2$, since otherwise p' cannot be close to d_0. This implies by the triangle inequality that

$$\left|X_{p'}\right| \leq |X_p| + \mu_2 \leq 1 + \mu_2. \tag{6.151}$$

Thus

$$\mathrm{d}(p', d) \geq \mathrm{d}_1(p', d) \geq \frac{c_3}{(2+\mu_2)(1+|X_{d_0}|)} > 0. \tag{6.152}$$

Finally, we show that p' cannot be too close to a Weierstrass point at $s = 0$, if such should exist. This is easy; we combine the equations ϕ and $Y^2 = f(X)$ to see that

$$f(X_{p'}) = (Y_p + \lambda(X_{p'} - X_p)^{g+1})^2, \tag{6.153}$$

and since p is close to a Weierstrass point away from $s = 0$, we have uniform upper bounds on $|X_p|$ and $|Y_p|$, and so (6.153) yields an upper bound on $\left|X_{p'}\right|$.

□

6.5.2 Cases

Definition 99. *Given two degree-zero divisors D, E on C, let*

$$\Delta(D, E) = \left|g_D(E) - \log(1/\,\mathrm{d}(D, E))\right|. \tag{6.154}$$

We bound $\Delta(D, E)$ uniformly in D and E (given bounds on the degrees of their effective parts) by working through the different possible configurations of these divisors on C. We use additivity of Green's functions to see that it suffices to consider divisors of the form $D = d - \infty_d$ and $E = e - \infty_e$ where d and e are complex points of C, and ∞_d, ∞_e are distinct Weierstrass points. Without loss of generality, we may always assume that $\mathrm{d}(\infty_d, \infty_e) \geq 3\mu$. We begin with the easiest

case.

Lemma 100. *Suppose the following hold:*
$\mathrm{d}(d,e) \geq \mu$
$\mathrm{d}(d,\infty_e) \geq \mu$
$\mathrm{d}(e,\infty_d) \geq \mu$.
Then

$$\Delta(D,E) \leq M(\mu) - 2\log(\mu). \tag{6.155}$$

Proof. From equation (6.89) we see that $|g_D(E)| \leq M(\mu)$. We also have $\mu^2 \leq \mathrm{d}(D,E) \leq \mu^{-2}$, and so the result follows by the triangle inequality. □

Lemma 101. *Suppose the following hold:*
$\mathrm{d}(d,e) < \mu$
$\mathrm{d}(d,\infty_e) \geq \mu$
$\mathrm{d}(e,\infty_d) \geq \mu$
$\mathrm{d}(d,d^-) \geq 2\mu$. *Then*

$$\Delta(D,E) \leq M(\mu) + \log\left((1+2\delta_{11}(\mu))(1+2\delta_{12}(\mu))^{-2}\right). \tag{6.156}$$

Proof. We apply Lemma 81 with the rational function $\phi = (x - x(d))/(x - x(\infty_d))$; since ∞_e is a Weierstrass point we see $\mathrm{d}(d^-,\infty_e) = \mathrm{d}(d,\infty_e) \geq \mu$ and from the triangle inequality we have $\mathrm{d}(d^-,e) \geq \mu$, so we can apply the lemma to see

$$|g_D(E) + \log(\mathrm{d}(D,E))| \leq M(\mu) + \left|\log\left|\frac{\mathrm{d}(D,E)}{\phi[E]}\right|\right|. \tag{6.157}$$

Now

$$\left|\log\left|\frac{\mathrm{d}(D,E)}{\phi[E]}\right|\right| = \left|\log\left|\frac{\mathrm{d}(d,e)}{|x_d - x_e|} \cdot \frac{\mathrm{d}(\infty_d,\infty_e)}{|x_{\infty_d} - x_{\infty_e}|} \cdot \frac{|x_d - x_{\infty_e})|}{\mathrm{d}(d,\infty_e)} \cdot \frac{|x_e - x_{\infty_d}|}{\mathrm{d}(e,\infty_d)}\right|\right|, \tag{6.158}$$

and by multiplying through we find that this equals

$$\left|\log\left|\frac{\mathrm{d}(d,e)}{\mathrm{d}_1(d,e)} \cdot \frac{\mathrm{d}(\infty_d,\infty_e)}{\mathrm{d}_1(\infty_d,\infty_e)} \cdot \frac{\mathrm{d}_1(d,\infty_e)}{\mathrm{d}(d,\infty_e)} \cdot \frac{\mathrm{d}_1(e,\infty_d)}{\mathrm{d}(e,\infty_d)}\right|\right| \tag{6.159}$$

where d_1 is the function defined in 6.1. We study the quotients inside the logarithm one at a time. Firstly, it is clear that

$$\frac{\mathrm{d}(\infty_d,\infty_e)}{\mathrm{d}_1(\infty_d,\infty_e)} = 1. \tag{6.160}$$

From Lemma 95 we find

$$1 \leq \frac{\mathrm{d}(d,e)}{\mathrm{d}_1(d,e)} = 1 + \frac{\mathrm{d}_2(d,e)}{\mathrm{d}_1(d,e)} + \frac{\mathrm{d}_3(d,e)}{\mathrm{d}_1(d,e)} \leq 1 + 2\delta_{11}(\mu), \tag{6.161}$$

Lemma 96 yields

$$1 \leq \frac{\mathrm{d}(d,\infty_e)}{\mathrm{d}_1(d,\infty_e)} =\leq 1 + 2\delta_{12}(\mu), \tag{6.162}$$

and similarly

$$1 \leq \frac{\mathrm{d}(e,\infty_d)}{\mathrm{d}_1(e,\infty_d)} \leq 1 + 2\delta_{12}(\mu). \tag{6.163}$$

□

We introduce some notation: given A and B, we say $A \sim B$ if there exist computable constants $c_1 > 0$ and $c_2 > 0$ depending only on C such that

$$c_1 \leq |A/B| \leq c_2. \tag{6.164}$$

Lemma 102. *Suppose the following hold:*
$\mathrm{d}(d,e) < \mu$
$\mathrm{d}(d,\infty_e) \geq \mu$
$\mathrm{d}(e,\infty_d) \geq \mu$
$\mathrm{d}(d,d^-) < 2\mu$.
We should also assume that $s_{\infty_e} \neq 0$, otherwise we would have to refine the definition of ϕ. Then there exists a computable upper bound on $\Delta(D,E)$ uniform in d, e, ∞_d and ∞_e (the bound is similar to that in the previous proposition, but is untidy to write a formula for).

Proof. We apply Lemma 81 with the rational function

$$\phi = \left((y - y(d)) - \lambda(x - x(d))^{g+1}\right)/(x - x(\infty_d))^{g+1}, \tag{6.165}$$

and let $P = \mathrm{zeros}_C(\phi) \setminus \{p\}$. By Proposition 98 we know for all $p' \in P$ and for all Weierstrass points d we have

$$\mathrm{d}(p,p') > \mu \quad \text{and} \quad \mathrm{d}(p',d) > \mu, \tag{6.166}$$

so we can apply the lemma to see

$$|g_D(E) + \log(\mathrm{d}(D,E))| \leq (2g+1)M(\mu) + \left|\log\left|\frac{\mathrm{d}(D,E)}{\phi[E]}\right|\right|. \tag{6.167}$$

We define some quotients:

$$\begin{aligned} Q_1 &= \frac{\mathrm{d}(d,e)(1+|X(d)|)^{g+1}(1+|X(e)|)^{g+1}}{|(Y(e)-Y(d))-\lambda(X(d)-X(e))^{g+1}|} \\ Q_2 &= \frac{\mathrm{d}(\infty_d,\infty_e)}{\mathrm{d}_1(\infty_d,\infty_e)^{g+1}} \\ Q_3 &= \frac{\left|(Y(\infty_e)-Y(d))-\lambda(X(\infty_e)-X(d))^{g+1}\right|}{\mathrm{d}(d,\infty_e)(1+|X(d)|)^{g+1}(1+|X(\infty_e)|)^{g+1}} \\ Q_4 &= \frac{\mathrm{d}_1(e,\infty_d)^{g+1}}{\mathrm{d}(e,\infty_d)} \end{aligned} \tag{6.168}$$

So after multiplying through, we obtain

$$\left|\log\left|\frac{\mathrm{d}(D,E)}{\phi[E]}\right|\right| = \log|Q_1Q_2Q_3Q_4| \tag{6.169}$$

We bound each of the Q_i in turn. Firstly, it is easy to compute

$$Q_2 = \frac{\mathrm{d}(\infty_d,\infty_e)}{\mathrm{d}_1(\infty_d,\infty_e)^{g+1}}, \tag{6.170}$$

and since there are only finitely any Weierstrass points, we do not even need to know which ones were chosen as ∞_d and ∞_e to get a bound. Now for

$$Q_4 = \frac{\mathrm{d}_1(e,\infty_d)^{g+1}}{\mathrm{d}(e,\infty_d)}, \tag{6.171}$$

we know $1 \geq \mathrm{d}(e,\infty_d) \geq \mu$ and $1 \geq \mathrm{d}_1(e\infty_d)^{g+1}$, so it suffices to find a positive lower bound on $\mathrm{d}_1(e,\infty_d)$, which is provided in the proof of Lemma 96.

Because $\mathrm{d}(d,d^-) \leq 2\mu$ and $\mathrm{d}(d,e) \leq \mu$ they are both close to the same Weierstrass point. We divide the bounding of Q_1 into three cases.

Case 1: The Weierstrass point does not lie at $x=0$ or $s=0$.

We obtain computable upper and positive lower bounds on $|X_d|$ and $|X_e|$, and computable upper bounds on $|Y_d|$ and $|Y_e|$. Thus

$$Q_1 \sim \frac{\mathrm{d}_1(d,e)+\mathrm{d}_2(d,e)+\mathrm{d}_3(d,e)}{|(Y_d-Y_e)-\lambda(X_d-X_e)^{g+1}|}. \tag{6.172}$$

Now

$$\frac{\mathrm{d}_1(d,e)}{|(Y_d-Y_e)-\lambda(X_d-X_e)^{g+1}|} \sim \frac{|X_d-X_e|}{|(Y_d-Y_e)-\lambda(X_d-X_e)^{g+1}|}, \tag{6.173}$$

and using Lemma 82 to find constants $0 < c_1 \leq c_2$ such that

$$c_1 \left|Y_d^2 - Y_e^2\right| \leq |X_d - X_e| \leq c_2 \left|Y_d^2 - Y_e^2\right|, \tag{6.174}$$

we see

$$\begin{aligned}
&\frac{|X_d - X_e|}{|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|} \\
&\leq \frac{|X_d - X_e|}{\left||Y_d - Y_e| - |\lambda| \, |X_d - X_e|^{g+1}\right|} \\
&\leq \frac{\left|Y_d^2 - Y_e^2\right| c_2}{\max\left(|Y_d - Y_e| - c_2^{g+1} \, |\lambda| \left|Y_d^2 - Y_e^2\right|^{g+1}, c_1^{g+1} \, |\lambda| \left|Y_d^2 - Y_e^2\right|^{g+1} - |Y_d - Y_e|\right)} \\
&= \frac{|Y_d + Y_e| \, c_2}{\max\left(1 - c_2^{g+1} \, |\lambda| \left|Y_d^2 - Y_e^2\right|^g |Y_d + Y_e|, -1 + c_1^{g+1} \, |\lambda| \left|Y_d^2 - Y_e^2\right|^g |Y_d + Y_e|\right)},
\end{aligned} \tag{6.175}$$

which is bounded above for μ sufficiently small. Next,

$$\frac{\mathrm{d}_3(d,e)}{|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|} \sim \frac{|Y_d - Y_e|}{|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|}, \tag{6.176}$$

and the same argument as above yields upper bounds. To obtain a lower bound, we observe

$$\begin{aligned}
\frac{|Y_d - Y_e|}{|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|} &\geq \frac{|Y_d - Y_e|}{|(Y_d - Y_e)| + |\lambda(X_d - X_e)^{g+1}|} \\
&\geq \frac{|Y_d - Y_e|}{|(Y_d - Y_e)| + c_2^{g+1} \, |\lambda| \left|Y_d^2 - Y_e^2\right|^{g+1}} \\
&= \frac{1}{1 + c_2^{g+1} \, |\lambda| \left|Y_d^2 - Y_e^2\right|^g |Y_d + Y_e|}.
\end{aligned} \tag{6.177}$$

Finally,

$$\begin{aligned}
&\frac{\mathrm{d}_2(d,e)}{|(Y_d - Y_e) - \lambda(Y_d - Y_e)^{g+1}|} \\
&= \frac{\left|Y_d/X_d^{g+1} - Y_e/X_e^{g+1}\right|}{(1 + \left|Y_d/X_d^{g+1}\right|)(1 + \left|Y_e/X_e^{g+1}\right|)\,|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|} \\
&\leq \frac{\left|Y_d/X_d^{g+1} - Y_e/X_e^{g+1}\right|}{\max\left(|Y_d - Y_e| - c_2^{g+1}\,|\lambda|\left|Y_d^2 - Y_e^2\right|^{g+1}, c_1^{g+1}\,|\lambda|\left|Y_d^2 - Y_e^2\right|^{g+1} - |Y_d - Y_e|\right)},
\end{aligned} \tag{6.178}$$

and for μ sufficiently small the denominator of the above expression is greater than or equal to $|Y_d - Y_e|/2$, so it suffices to bound above the expression

$$(*) \stackrel{\text{def}}{=} \frac{\left|Y_d/X_d^{g+1} - Y_e/X_e^{g+1}\right|}{|Y_d - Y_e|}. \tag{6.179}$$

Setting $t = X_d/X_e$ and $s = t^{g+1}$, we find

$$\begin{aligned}
(*) &= \frac{|sY_d - Y_e|}{|X_e|^{g+1}\,|Y_d - Y_e|} \\
&= \frac{|sY_d - sY_e + sY_e - Y_e|}{|X_e|^{g+1}\,|Y_d - Y_e|} \\
&\leq \frac{|s|}{|X_e|^{g+1}} + \frac{|Y_e|}{|X_e|^{g+1}} \cdot \frac{|s-1|}{|Y_d - Y_e|},
\end{aligned} \tag{6.180}$$

so it remains to bound above the expresion

$$\frac{|s-1|}{|Y_d - Y_e|}. \tag{6.181}$$

Well $|s-1| = |t-1| \cdot \left|t^g + t^{g-1} + \cdots + 1\right|$, and $\left|t^g + t^{g-1} + \cdots + 1\right|$ we can bound above, so since $|Y_d + Y_e| \leq 1$ for μ sufficiently small, it remains to bound above

$$\frac{|X_d - X_e|}{|Y_d - Y_e|} \leq \frac{|X_d - X_e|}{\left|Y_d^2 - Y_e^2\right|}. \tag{6.182}$$

Now recall from Lemma 82 that we have

$$\left|Y_d^2 - Y_e^2\right| = |X_d - X_e|\,|\Delta f(X_d, X_e)| \tag{6.183}$$

where Δf is a polynomial with no zeros for d and e close to a Weierstrass point, and that we can find a positive lower bound on $|\Delta f|$ on a small disk around a Weierstrass point. Hence writing

$$\frac{|X_d - X_e|}{\left|Y_d^2 - Y_e^2\right|} = \frac{1}{|\Delta f(X_d, X_e)|}, \tag{6.184}$$

we are done.

Case 2: The Weierstrass point lies at $x = 0$.

We obtain computable upper bounds on $|X_d|$ and $|X_e|$, and computable upper bounds on $|Y_d|$ and $|Y_e|$. Thus

$$Q_1 \sim \frac{\mathrm{d}_1(d,e) + \mathrm{d}_2(d,e) + \mathrm{d}_3(d,e)}{|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|}, \tag{6.185}$$

and we obtain upper bounds on

$$\mathrm{d}_1(d,e)/(\left|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}\right|) \tag{6.186}$$

and upper and positive lower bounds on

$$\mathrm{d}_3(d,e)/(\left|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}\right|) \tag{6.187}$$

exactly as in the previous case. To obtain an upper bound on

$$\mathrm{d}_2(d,e)/(\left|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}\right|), \tag{6.188}$$

we begin by writing

$$\begin{aligned}
&\frac{\mathrm{d}_2(d,e)}{|(Y_d - Y_e) - \lambda(Y_d - Y_e)^{g+1}|} \\
&= \frac{\left|Y_d/X_d^{g+1} - Y_e/X_e^{g+1}\right|}{(1 + \left|Y_d/X_d^{g+1}\right|)(1 + \left|Y_e/X_e^{g+1}\right|)\,|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|} \\
&= \frac{\left|X_d^{g+1}/Y_d - X_e^{g+1}/Y_e\right|}{(1 + \left|X_d^{g+1}/Y_d\right|)(1 + \left|X_e^{g+1}/Y_e\right|)\,|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|} \\
&\leq \frac{\left|X_d^{g+1}/Y_d - X_e^{g+1}/Y_e\right|}{|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}|},
\end{aligned} \tag{6.189}$$

and as we have seen before, for μ sufficiently small we can find a constant $c > 0$ such that

$$\left|(Y_d - Y_e) - \lambda(X_d - X_e)^{g+1}\right| \geq c\,|Y_d - Y_e|\,, \tag{6.190}$$

so it suffices to bound above the expression

$$\frac{\left|X_d^{g+1}/Y_d - X_e^{g+1}/Y_e\right|}{|Y_d - Y_e|}. \tag{6.191}$$

Define a polynomial f_0 by $t \cdot f_0(t) = f(t)$, which has no zeros for t within distance μ of 0. Fixing $\sigma \in \mathbb{C}$ such that

$$\sigma^{2g+1} = \left(\frac{f_0(X_e)}{f_0(X_d)}\right)^{g+1}, \tag{6.192}$$

and using $Y^2 = X f_0(X)$, we can show

$$\begin{aligned}\frac{\left|X_d^{g+1}/Y_d - X_e^{g+1}/Y_e\right|}{|Y_d - Y_e|} &= \frac{1}{|f_0(X_e)|^{g+1}} \frac{\left|(\sigma Y_d)^{2g+1} - Y_e^{2g+1}\right|}{|Y_d - Y_e|} \\ &\leq \frac{\left|(\sigma Y_d)^{2g} + \cdots + Y_e^{2g}\right|}{|f_0(X_e)|^{g+1}} \frac{|\sigma Y_d - Y_e|}{|Y_d - Y_e|}.\end{aligned} \tag{6.193}$$

We easily bound above $\left|(\sigma Y_d)^{2g} + \cdots + Y_e^{2g}\right|$, and so it suffices to find an upper bound on

$$\frac{|\sigma Y_d - Y_e|}{|Y_d - Y_e|}, \tag{6.194}$$

which amounts to showing that σ tends to 1 fast enough as d and e get close together. Observe that

$$|\sigma - 1| \leq \left|\frac{f_0(X_e)}{f_0(X_d)} - 1\right| \tag{6.195}$$

since $(g+1)/(2g+1) \leq 1$, and hence

$$|\sigma - 1| \leq \frac{|X_d - X_e|}{|f_0(X_d)|} \left|\sup_{t_0 \in \overline{B_\mu(0)}} \frac{\mathrm{d}\, f_0}{\mathrm{d}_X}(t_0)\right|. \tag{6.196}$$

Recalling from Lemma 82 that

$$\frac{|X_d - X_e|}{|f(X_d) - f(X_e)|} \leq \frac{1}{|\Delta f(X_d, X_e|} \tag{6.197}$$

which we may bound above, we obtain

$$\begin{aligned}\frac{|\sigma Y_d - Y_e|}{|Y_d - Y_e|} &\leq 1 + |Y_d| \frac{|\sigma - 1|}{|Y_d - Y_e|} \\ &\leq 1 + \frac{|Y_d|\,|Y_d + Y_e|}{|f_0(X_d)|\,|\Delta f(X_d, X_e)|} \left| \sup_{t_0 \in \overline{B_\mu(0)}} \frac{\mathrm{d}\, f_0}{\mathrm{d}_X}(t_0) \right|,\end{aligned} \tag{6.198}$$

so we are done.

Case 3: The Weierstrass point lies at $s = 0$.
Swap x and s, then appeal to Case (2).

For Q_3, we note that $\mathrm{d}(d, \infty_e)$ is bounded above and below by a positive constant, and since $\mathrm{d}(d, d^-) \leq 2\mu$ this keeps d near a Weierstrass point. If that Weierstrass point does not lie at $s = 0$ then $|X_d|$ is bounded. This yields upper and lower bounds on $(1 + |X_d|^{g+1})(1 + |X_{\infty_e}|^{g+1})$, so it remains to bound $\left|(y(\infty_e) - y(d)) - \lambda(x(\infty_e) - x(d))^{g+1}\right|$. An upper bound follows easily from the bounds on $|X_d|$. For a lower bound, recall that in Lemma 98 we proved constructively that any roots of $y - y(d) - \lambda(x - x(d))^{g+1}$ must either be equal to d or have large Y-coordinate; this clearly excludes ∞_e, and can be used to give a lower bound as desired.

We are thus left with the cases where d is close to a Weierstrass point at $s = 0$ (since we assumed $S_{\infty_e} \neq 0$). Thus $Y_d^2 = X_d^{2g+1} + \mathrm{l.\,o.\,t.}$ (lower order terms), so

$$\begin{aligned}Q_3 &\sim \frac{\left|Y_{\infty_e} - Y_d - \lambda(X_{\infty_e} - X_d)^{g+1}\right|}{(1 + |X_d|)^{g+1}} \\ &= \frac{\left|Y_{\infty_e} - (X_d^{2g+1} + \mathrm{l.\,o.\,t.})^{1/2} - \lambda(-X_d)^{g+1} + \mathrm{l.\,o.\,t.}\right|}{|X_d|^{g+1} + \mathrm{l.\,o.\,t.}} \\ &\sim \frac{\left|(X_d)^{g+1/2} + \lambda(-X_d)^{g+1}\right|}{|X_d|^{g+1}} \\ &\sim \left|\lambda(-1)^{g+1} + X_d^{-1/2}\right| \\ &\sim |\lambda|\end{aligned} \tag{6.199}$$

which is bounded above and below by positive constants as required. □

It may seem at this point that we are near the start of a long sequence of messy calculations such as that above, to cover all possible cases of arrangements of points in D and E. However, there is a trick which means that the messy calculations are in fact complete. The key is that given any configuration of divisors D and E,

we can move into one of the three cases handled above if we allow ourselves to move the base-points ∞_d and ∞_e. This in itself is not hard to check, but there are two more things needed to make it useful. The first is the observation that moving the base points in this way (replacing one Weierstrass point with a different Weierstrass point) has no effect on the height of the divisor being considered; this is because degree-zero divisors formed from differences of Weierstrass points are torsion in the Jacobian.

The second important point is that such rearranging is still possible when our divisors are of a more complicated form than simply 'a point minus a Weierstrass point'; namely, we must consider D and E to be of the form 'a semi-reduced divisor minus g Weierstrass points'. The following easy lemma proves what we need:

Lemma 103. *Let $D = \sum_i p_i$ be a semi-reduced divisor on C containing no Weierstrass points in its support, and let $D^- = \sum_i p_i^-$ denote its image under the hyperelliptic involution. Then there exist a pair of degree-g divisors $\infty_1 = \sum_i q_i$ and $\infty_2 = \sum_i q_i'$ on $C \times_K \mathbb{C}$, supported on Weierstrass points away from $s = 0$, such that for all pairs of integers i, $j \in \{1, \ldots, g\}$, the divisors $p_i - q_i$ and $p_j^- - q_j'$ satisfy the hypotheses of at least one of Lemmas 100, 101 or 102.*

Proof. p_i is close to a Weierstrass point d if and only if p_i^- is also close to d, hence there are at most g Weierstrass points which have points in $\mathrm{Supp}(D) \cup \mathrm{Supp}(D^-)$ close to them. Since there are $2g + 1$ distinct Weierstrass points away from $s = 0$, we are left with $g + 1$ to select the q_i and q_i' from. Since the q_i are permitted to repeat themselves, and similarly the q_i', the requirements are easy to achieve. □

Corollary 104. *There exists a computable constant $\mathscr{B}_3$ depending only on C such that for all semi-reduced divisors D on C, and all choices of base-divisors ∞_1 and ∞_2 as in Lemma 103, we have*

$$\left| g_{D-\infty_1}(D^- - \infty_2) - \log(1/\,\mathrm{d}(D - \infty_1, D^- - \infty_2) \right| \leq \mathscr{B}_3. \tag{6.200}$$

Proof. Given any $p \in \mathrm{Supp}(D - \infty_1)$ and $q \in \mathrm{Supp}(D^- - \infty_2)$, if $\mathrm{d}(p, q) \geq \mu$ then $-\log(\mu) \geq -\log \mathrm{d}(p, q) \geq -\log(3)$ and $|g_p(q)| \leq M(\mu)$, so $|g_p(q) - \log(1/\,\mathrm{d}(p, q))| \leq M(\mu) - \log(\mu)$. Otherwise $\mathrm{d}(p, q) < \mu$, whereupon we appeal to Lemma 103 to see that we are in the situation of one of Lemmas 100, 101 or 102, which will supply a bound. □

6.6 Reconstruction of global heights

In this section, we will combine the local computations of the previous sections to obtain a global naïve height and to compare it to the Néron-Tate height. We define a naïve height for points on the Jacobian using the metrics from Section 6.1. That this height has bounded difference from the Néron-Tate height will follow immediately from results in previous sections.

We restrict from now on to curves over number fields K with only one Archimedean place (for example, $K = \mathbb{Q}$). This is so that in Definition 105 for each semi-reduced divisor D supported away from Weierstrass points, we can choose as base point Weierstrass points which are 'not too close' to D in any Archimedean place.

If K had many Archimedean places this might not be possible, since it could happen that there exists such a divisor D such that for every Weierstrass point q there exists an Archimedean place $|-|$ and a point p in the support of D such that $|p - q|$ is very small. In fact, this problem is easily worked around by allowing ourselves to choose for each D different Weierstrass points at each Archimedean place of K. We can then use the behaviour of Green's functions and Néron symbols under linear equivalence to show that this will affect the height by at most a function linear in the square root of the height. This would allow all our results to continue to work without significant change, but it would make the notation and later comparison results (see Chapter 7) considerably more messy. Given that in high genus it seems likely that in the near future these results will only be applied over $\mathbb{Q}$ in any case, we restrict in this thesis to the case of K having a single Archimedean place.

Definition 105. *We define a naïve height* $\tilde{\mathrm{H}} : A(K) \to \mathbb{R}_{>1}$ *as follows. Given* $p \in A(K)$*, write* $p = [D - g\infty]$ *where* D *is a semi-reduced divisor on* C*. If the support of* D *contains any Weierstrass points, replace* D *by the divisor obtained by subtracting them off; this equates to translating* p *by a 2-torsion point, and so will not affect the Néron-Tate height. Let* d *denote the degree of the resulting divisor* D*.*

Choose once and for all a pair of degree-d *effective divisors* ∞_p^1 *and* ∞_p^2 *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* ∞_p^1 *or* ∞_p^2*. Here* μ *is the 'sufficiently small' constant from Section 6.4 (which may have been further shrunk in Section 6.5) and the existence of such divisors is clear since there are* $2g + 1$ *Weierstrass points away from* ∞ *and semi-reduced divisors have degree* g*.*

Now define

$$\tilde{\mathrm{H}}(p) = \left(\prod_{\nu \in M_L} \frac{1}{\mathrm{d}_\nu(D - \infty_p^1, D^- - \infty_p^2)} \right)^{\frac{1}{[L:K]}}, \tag{6.201}$$

for any finite extension L/K over which D, ∞_p^1 and ∞_p^2 are pointwise rational, recalling that if $D = \sum_i d_i$, $\infty_p^1 = \sum_i q_i^1$ and $\infty_p^2 = \sum_i q_i^2$ then

$$\mathrm{d}_\nu(D - \infty_p^1, D^- - \infty_p^2) = \prod_{i,j} \frac{\mathrm{d}_\nu(p_i, p_j^-)\, \mathrm{d}_\nu(q_i^1, q_j^2)}{\mathrm{d}_\nu(p_i, q_i^2)\, \mathrm{d}_\nu(p_i^-, q_i^1)}. \tag{6.202}$$

We define a logarithmic naïve height by $\mathscr{H}(p) = \log(\tilde{\mathrm{H}}(p))$.

Proposition 106. *The products in the definition above are finite; in particular, the heights are well defined.*

Proof. From the definitions of the metrics over non-Archimedean places, it is clear that $\mathrm{d}_\nu(D - \infty_p^1, D^- - \infty_p^2) = 1$ for all but finitely many such places. □

Combining previous results, we obtain the following theorem, which is the main result of this chapter.

Theorem 107. *Fix a finite extension L/K (such that $\#_L^\infty = 1$). Then for all $p \in A(L)$ we have*

$$\left| \hat{\mathrm{h}}(p) - \mathscr{H}(p) \right| \leq \mathscr{B}_1 + \mathscr{B}_2 + \mathscr{B}_3, \tag{6.203}$$

where $\mathscr{B}_1$ is from Definition 57, $\mathscr{B}_2$ is from Corollary 60 and $\mathscr{B}_3$ is from Corollary 104.

Write $c = c(L)$ for the constant $\mathscr{B}_1 + \mathscr{B}_2 + \mathscr{B}_3$.

The naïve height $\mathscr{H}$ has the great advantage that it is far easier to compute that the Néron-Tate height; the former is completely elementary, whereas the latter required considerable machinery and took up the whole of Chapter 5. Given a real number $B > 0$, define $\hat{M}(L, B) = \{p \in A(L) : \hat{\mathrm{h}}(p) \leq B\}$ and $\mathscr{M}(L, B) = \{p \in A(L) : \mathscr{H}(p) \leq B\}$. Then by construction we have $\hat{M}(L, B) \subset \mathscr{M}(L, B + c(L))$, so it suffices to compute the latter (finite) set. This problem will be the subject of the next chapter.

Chapter 7

An algorithm to compute the number of points up to bounded height

For the remainder of this chapter $\overline{K}$ will denote an algebraic closure of our number field K. Given a divisor D, we write L_D for a finite extension of K over which D becomes pointwise rational. L will usually denote a finite extension on K, and we then let M_L denote a proper set of valuations satisfying the product formula - in particular, each valuation in M_L extends a valuation in M_K. As usual, C is a hyperelliptic curve over K. As we proceed, various conditions will be imposed on C; these conditions will be sufficiently mild that every hyperelliptic curve over K has a model of the required form after possible passing to a finite extension of K (though recall the remark in Section 105).

In this chapter, we will construct two new naïve heights, each simpler than the last, and bound the differences between these heights and the naïve height of Chapter 6. The last of these heights will be simple enough that it will enable us to solve Problem 2 of Section 1.1, using the algorithm given in the final section of this chapter.

Lemma 108. *There exist computable constants $0 < c_1 < c_2$ with the following property:*

for all $p = (x : s : y) \in C(\overline{K})$, and for all Archimedean norms $|-|_\nu$ on $\overline{K}$, we have

$$c_1 \leq \mathrm{d}_\nu(p, p^-)/(2\min(|Y|_\nu, |Y'|_\nu)) \leq c_2, \tag{7.1}$$

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

Proof. Write $|-|$ for $|-|_\nu$. We may assume without loss of generality that $|x| \leq |s|$, so write $X = x/s$. We wish to show that $\mathrm{d}_\nu(p, p^-) \sim 2\,|Y|$. Now by Lemma 84 we see $|Y| \leq \delta_2(1)$, so in particular $(1 + |Y|)^2 \sim 1$.

If C has no Weierstrass point d with $x_d = 0$, then let $R > 0$ be such that there is no Weierstrass point d with $|x_d/s_d| \leq R$. If C has a Weierstrass point d with $x_d = 0$, then let $R > 0$ be such that d is the only Weierstrass point with $|x_d/s_d| \leq R$.

We treat first the case of $|X| > R$. This yields a computable upper bound on $|Y'|$, again using Lemma 84, and so in turn we see $(1 + |Y'|)^2 \sim 1$. In addition we have non-zero upper and lower bounds on $|X|$, in other words $|X| \sim 1$. Thus $|Y'| \sim |Y|$, so

$$\begin{aligned} \mathrm{d}_\nu(p, p^-) &= \mathrm{d}_2(p, p^-) + \mathrm{d}_3(p, p^-) \\ &= \frac{|2Y'|}{(1 + |Y'|)^2} + \frac{|2Y|}{(1 + |Y|)^2} \\ &\sim \left|2Y'\right| + |2Y| \\ &\sim 2\,|Y|\,. \end{aligned} \tag{7.2}$$

We next consider the case $|X| < R$. This splits in to two sub-cases, depending on whether or not there is a Weierstrass point at $X = 0$.

Case 1: no Weierstrass point at $X = 0$.
Thus we obtain positive lower bounds on $|Y|$, say $|Y| \geq \delta > 0$. Then $|Y| \sim 1$, and hence $\mathrm{d}_3(p, p^-) \sim |2Y| \sim 1$. Now $Y' = Y/X^{g+1}$, so we see $|Y'| > \delta/R^{g+1}$. Now

$$\begin{aligned} \mathrm{d}_2(p, p^-) &= \frac{|2Y'|}{(1 + |Y'|)^2} \\ &= \frac{|2/Y'|}{(1 + |1/Y'|)^2}, \end{aligned} \tag{7.3}$$

so this lower bound on $|Y'|$ yields a computable upper bound on $\mathrm{d}_2(p, p^-)$. Then

$$\mathrm{d}(p, p^-) = \mathrm{d}_2(p, p^-) + \mathrm{d}_3(p, p^-) \sim 1 \sim 2\,|Y|\,, \tag{7.4}$$

so we are done.

Case 2: there is a Weierstrass point d with $X_d = 0$.
Our assumptions on R show that $\left|Y^2\right| \sim |X|$, yielding an upper bound on $|Y|$ (say $|Y| \leq c$), so $\mathrm{d}_3(p, p^-) \sim |2Y|$. Now let $0 < c_1 \leq c_2$ be such that

$$\frac{c_1}{|Y|^{2g+1}} \leq \left|Y'\right| \leq \frac{c_2}{|Y|^{2g+1}}. \tag{7.5}$$

Hence

$$\mathrm{d}_2(p,p^-)=\frac{2\left|Y'\right|}{(1+\left|Y'\right|)^2}\leq\frac{2\left|Y'\right|}{(1+c_1/\left|Y\right|^{2g+1})^2}=\frac{2\left|Y\right|^{2g+1}}{(c_1+\left|Y\right|^{2g+1})^2}\leq\frac{2\left|Y\right|^{2g+1}}{c_1^2},\quad(7.6)$$

and

$$\mathrm{d}_2(p,p^-)=\frac{2\left|Y'\right|}{(1+\left|Y'\right|)^2}\geq\frac{2\left|Y'\right|}{(1+c_2/\left|Y\right|^{2g+1})^2}=\frac{2\left|Y\right|^{2g+1}}{(c_2+\left|Y\right|^{2g+1})^2}\geq\frac{2\left|Y\right|^{2g+1}}{(c_2+c^{2g+1})^2},\quad(7.7)$$

so

$$\mathrm{d}_2(p,p^-)\sim 2\left|Y\right|^{2g+1}.\quad(7.8)$$

Hence

$$\mathrm{d}(p,p^-)\sim 2\left|Y\right|,\quad(7.9)$$

since $|Y|$ is bounded above. □

Definition 109. *Let $p\neq q\in C(L)$ be distinct points. Set*

$$\langle p,q\rangle=\frac{-1}{[L:K]}\log\prod_{\nu\in M_L}\mathrm{d}_\nu(p,q).\quad(7.10)$$

It is clear that this is independent of the choice of the extension L.

Lemma 110. *Let $p=(x:s:y)\in C(L)$ be a non-Weierstrass point. Then there exists a computable constant c such that*

$$\left|\left\langle p,p^-\right\rangle-(g+1)\,\mathrm{h}(x/s)\right|\leq c\quad(7.11)$$

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

$$\mathrm{d}_\nu(p,p^-)=|2y|_\nu\min(1/\left|x\right|_\nu^{g+1},1/\left|s\right|_\nu^{g+1}).\quad(7.12)$$

We have shown above that for Archimedean ν we have computable $0<c_1<c_2$ such that

$$c_1<\mathrm{d}_\nu(p,p^-)/\min(\left|2y/x^{g+1}\right|,\left|2y/s^{g+1}\right|)<c_2.\quad(7.13)$$

Hence

$$\prod_{\nu\in M_L^\infty}1/c_2\leq\frac{\prod_{\nu\in M_L}1/\,\mathrm{d}_\nu(p,p^-)}{\prod_{\nu\in M_L}|2y|_\nu^{-1}\prod_{\nu\in M_L}\max(|x|_\nu,|s|_\nu)^{g+1}}\leq\prod_{\nu\in M_L^\infty}1/c_1.\quad(7.14)$$

Now $\prod_{\nu \in M_L^\infty} c_1^{-1/[L:K]}$ is bounded uniformly in L, and similarly for c_2. Finally, note

$$\left(\prod_{\nu \in M_L} |2y|_\nu^{-1} \right) \left(\prod_{\nu \in M_L} \max(|x|_\nu, |s|_\nu) \right)^{g+1} = H(x/s)^{[L:K](g+1)}. \tag{7.15}$$

□

Definition 111. *Assume that the hyperelliptic polynomial f is monic. Given a Weierstrass point d with $s_d \neq 0$, set $\tilde{f}_d$ to be the univariate polynomial such that for all $p \neq d \in C(\overline{K})$, we have*

$$\tilde{f}_d(X_p)(X_p - X_d) = f(X_p). \tag{7.16}$$

It is clear that $\tilde{f}_d$ will have integral coefficients, since f does and X_d is a root of f.

Lemma 112. *Let p, $d \in C(L)$ such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Assume further that the hyperelliptic polynomial f is monic, so that X_d is integral. Let ν be a non-Archimedean place of L, and suppose $|X_p - X_d|_\nu < \left|\tilde{f}_d(X_d)\right|_\nu$. Then*

$$|Y_p|_\nu^2 = |X_p - X_d|_\nu \left|\tilde{f}_d(X_d)\right|_\nu. \tag{7.17}$$

Proof. By definition, we have

$$|Y_p|_\nu^2 = |X_p - X_d|_\nu \left|\tilde{f}_d(X_p)\right|_\nu, \tag{7.18}$$

so it suffices to show that $\left|\tilde{f}_d(X_p)\right|_\nu = \left|\tilde{f}_d(X_d)\right|_\nu$. Writing

$$\tilde{f}_d(X_p) = (X_p - X_d)^n + \star(X_p - X_d)^{n-1} + \cdots + \star(X_p - X_d) + \tilde{f}_d(X_d) \tag{7.19}$$

where the coefficients $\star$ are integral, we see that the greatest norm of any term on the right hand side is achieved by $\tilde{f}_d(X_d)$ and no other term, so the result follows. □

Lemma 113. *Let $p \neq d \in C(L)$ be such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Assume further that the hyperelliptic equation f is monic, so that X_d is integral. Then*

$$-\sum_{\nu \in M_L^0} \log \mathrm{d}_\nu(p, d) \leq [L:K] \left(\frac{1}{2} \mathrm{h}(X_p - X_d) + \mathrm{h}(\tilde{f}(X_d)) \right). \tag{7.20}$$

Note that the sum is over the non-Archimedean places.

Proof. The right hand side naturally decomposes as

$$[L:K](\frac{1}{2}\,\mathrm{h}(X_p - X_d) + \mathrm{h}(\tilde{f}_d(X_d))) = \sum_{\nu \in M_L} \frac{1}{2}\log^+ |X_p - X_d|_\nu^{-1} + \log^+ \left|\tilde{f}_d(X_d)\right|_\nu^{-1}. \tag{7.21}$$

Now it is clear that

$$\sum_{\nu \in M_L^\infty} \frac{1}{2}\log^+ |X_p - X_d|_\nu^{-1} + \log^+ \left|\tilde{f}_d(X_d)\right|_\nu^{-1} \geq 0, \tag{7.22}$$

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

$$-\log(\mathrm{d}_\nu(p,d)) \leq \frac{1}{2}\log^+ |X_p - X_d|_\nu^{-1} + \log^+ \left|\tilde{f}_d(X_d)\right|_\nu^{-1}, \tag{7.23}$$

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

$$\mathrm{d}_\nu(p,d)^{-2} \leq \max(|X_p - X_d|^{-1}, 1)\max(\left|\tilde{f}_d(X_d)\right|^{-1}, 1)^2. \tag{7.24}$$

Recalling that $\left|\tilde{f}_d(X_d)\right| \leq 1$ and writing $F = \left|\tilde{f}_d(X_d)\right|$ for simplicity, we see this is equivalent to showing

$$\mathrm{d}_\nu(p,d)^2 \geq F^2 \min(|X_p - X_d|, 1). \tag{7.25}$$

We divide proving this in to two cases. The first is when $|X_p - X_d| \geq F$. Then

$$\mathrm{d}_\nu(p,d) \geq \begin{cases} F & \text{if } |X_p| \leq 1 \\ 1 & \text{if } |X_p| > 1, \end{cases} \tag{7.26}$$

so Equation (7.25) follows.

The harder case is when $|X_p - X_d| < F$. We apply Lemma 112 to see that

$|Y_p|^2 = |X_p - X_d|\, F$, and so

$$\begin{aligned}
\mathrm{d}_\nu(p,d)^2 &= \begin{cases} \max(|X_p - X_d|^2, |Y_p|^2) & \text{if } |X_p| \le 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\
&= \begin{cases} \max(|X_p - X_d|^2, |X_p - X_d|\, F) & \text{if } |X_p| \le 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\
&\ge \begin{cases} F \max(|X_p - X_d|^2, |X_p - X_d|) & \text{if } |X_p| \le 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\
&= \begin{cases} F\,|X_p - X_d| & \text{if } |X_p| \le 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\
&= F \min(|X_p - X_d|, 1) \\
&\ge F^2 \min(|X_p - X_d|, 1)
\end{aligned} \tag{7.27}$$

□

Lemma 114. *Fix $\mu > 0$. Let $d \in C(L)$ be a Weierstrass point, and let $p \in C(L)$ be such that for all Archimedean places $\nu \in M_L^\infty$, we have $\mathrm{d}_\nu(p,d) \ge \mu$. Then*

$$\mu^{\#M_L^\infty} \le \prod_{\nu \in M_L^\infty} \mathrm{d}_\nu(p,d) \le 3^{\#M_L^\infty}. \tag{7.28}$$

Proof. The lower bound is clear, and the upper bound follows from Proposition 54. □

Lemma 115. *Let X_1, $X_2 \in L$. Then*

$$\mathrm{H}(X_1 + X_2) \le 2^{\#M_L^\infty/[L:K]}\, \mathrm{H}(X_1)\, \mathrm{H}(X_2). \tag{7.29}$$

Proof.

$$\begin{aligned}
&\mathrm{H}(X_1 + X_2)^{[L:K]} = \prod_{\nu \in M_L} \max(1, |X_1 + X_2|_\nu) \\
&\le \left(\prod_{\nu \in M_L^0} \max(1, |X_1|_\nu, |X_2|_\nu) \right) \left(\prod_{\nu \in M_L^\infty} \max(1, |X_1|_\nu + |X_2|_\nu) \right) \\
&\le \left(\prod_{\nu \in M_L^0} \max(1, |X_1|_\nu) \max(1, |X_2|_\nu) \right) \left(\prod_{\nu \in M_L^\infty} 2 \max(1, |X_1|_\nu) \max(1, |X_2|_\nu) \right) \\
&= 2^{\#M_L^\infty}\, \mathrm{H}(X_1)^{[L:K]}\, \mathrm{H}(X_2)^{[L:K]}
\end{aligned} \tag{7.30}$$

as required. □

Lemma 116. *Fix $\mu > 0$. There exists a computable constant ϕ_μ with the following property:*

Let p, $d \in C(L)$ such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Assume further that the hyperelliptic equation f is monic, and also that for all Archimedean places $\nu \in M_L^\infty$, we have $\mathrm{d}_\nu(p, d) \geq \mu$. Then

$$\langle p, d \rangle \leq \frac{1}{2}\,\mathrm{h}(X_p) + \phi_\mu. \tag{7.31}$$

Proof. Combining Lemmata 113 and 114, we see that

$$\langle p, d \rangle \leq \frac{1}{2}\,\mathrm{h}(X_p - X_d) + \mathrm{h}(\tilde{f}_d(X_d))) - \log(\mu)\#M_L^\infty/[L:K]. \tag{7.32}$$

Now by Lemma 115, we have

$$\mathrm{h}(X_p - X_d) \leq \mathrm{h}(X_p) + \mathrm{h}(X_d) + \frac{\#M_L^\infty}{[L:K]}\log(2), \tag{7.33}$$

so for fixed L and d we may take

$$\phi_\mu^{L,d} = \frac{1}{2}\,\mathrm{h}(\tilde{f}_d(X_d))) - \log(\mu)\frac{\#M_L^\infty}{[L:K]} + \mathrm{h}(X_d) + \frac{\#M_L^\infty}{2[L:K]}\log(2). \tag{7.34}$$

Thus the existence of a bound uniform in L and d is clear (since there are only finitely many Weierstrass points). □

Lemma 117. *There exists a computable constant c such that the following holds:*

given $p \in A(K)$, let D, ∞_p^1 and ∞_p^2 denote the divisors given in Definition 105. Over some finite extension L/K, we may write

$$\begin{aligned} D &= \sum_{i=1}^{d} p_i \\ \infty_p^1 &= \sum_{i=1}^{d} q_i \\ \infty_p^2 &= \sum_{i=1}^{d} q_i'. \end{aligned} \tag{7.35}$$

Then

$$\mathscr{H}(p) \geq \sum_{i=1}^{d}\left(\langle p_i, p_i^- \rangle - \sum_{j=1}^{d}\langle p_i, q_j\rangle - \sum_{j=1}^{d}\langle p_i, q_j'\rangle\right) + c. \tag{7.36}$$

Proof. Recall that

$$\mathscr{H}(p) = \sum_{i,j=1}^{d} \left\langle p_i, p_j^- \right\rangle + \sum_{i,j=1}^{d} \langle q_i, q_j' \rangle - \sum_{i,j=1}^{d} \langle p_i, q_j \rangle - \sum_{i,j=1}^{d} \langle p_i^-, q_j' \rangle . \tag{7.37}$$

Since the q_i and q_i' are distinct Weierstrass points we easily bound $\sum_{i,j=1}^{d} \left\langle q_i, q_j' \right\rangle$. For $i \neq j$, we see

$$\left\langle p_i, p_j^- \right\rangle \geq -\log(3).\#M_L^\infty/[L:K], \tag{7.38}$$

so the result follows. □

Lemma 118. *There exists a computable constant c' such that in the setup of Lemma 117 we have*

$$\mathscr{H}(p) \geq \sum_{i=1}^{d} h(X_{p_i}) + c' \tag{7.39}$$

Proof. In Lemma 117 we showed

$$\mathscr{H}(p) \geq \sum_{i=1}^{d} \left(\langle p_i, p_i^- \rangle - \sum_{j=1}^{d} \langle p_i, q_j \rangle - \sum_{j=1}^{d} \langle p_i, q_j' \rangle \right) + c. \tag{7.40}$$

In Lemma 110 we showed (using that the p_i are never Weierstrass points) that for some computable c_1 we have

$$\left| \langle p_i, p_i^- \rangle - (g+1)\, \mathrm{h}(X_{p_i}) \right| \leq c_1. \tag{7.41}$$

In Lemma 116 we showed (using that $\mathrm{d}_\nu(p_i, q_j) \geq \mu$ where μ is as in Definition 105) that

$$\langle p_i, q_j \rangle \leq \frac{1}{2}\, \mathrm{h}(X_p) + \phi_\mu. \tag{7.42}$$

and similarly for q_j'.

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

$$\begin{aligned} \langle p_i, p_i^- \rangle - \sum_{j=1}^{d} \langle p_i, q_j \rangle - \sum_{j=1}^{d} \langle p_i, q_j' \rangle &\geq (g+1)\, \mathrm{h}(X_{p_i}) - 2 \sum_{j=1}^{d} \frac{1}{2}\, \mathrm{h}(X_{p_i}) + c_1 + 2d\phi_\mu \\ &= ((g+1) - 2d\frac{1}{2})\, \mathrm{h}(X_{p_i}) + c_1 + 2d\phi_\mu \\ &\geq \mathrm{h}(X_{p_i}) + c_1 + 2d\phi_\mu. \end{aligned} \tag{7.43}$$

from which the result follows. □

Definition 119. *Given $p \in A(K)$, we take the divisor $D = \sum_{i=1}^{d} p_i$ over some finite L/K as in Definition 105. Then set*

$$\mathrm{h}^{\heartsuit}(p) = \sum_{i=1}^{d} \mathrm{h}(X_{p_i}), \tag{7.44}$$

and set

$$\mathrm{h}^{\dagger}(p) = \mathrm{h}\left(\prod_{i=1}^{d}(X - X_{p_i})\right), \tag{7.45}$$

where the right hand side is the height of a polynomial, which equals the height of the point in projective space whose coordinates are given by its coefficients. Given $B > 0$, define

$$M^{\heartsuit}(B) = \{p \in A(K) : \mathrm{h}^{\heartsuit}(p) \leq B\} \tag{7.46}$$

and

$$M^{\dagger}(B) = \{p \in A(K) : \mathrm{h}^{\dagger}(p) \leq B\} \tag{7.47}$$

Theorem 120. *There exists a computable constant c such that for all $p \in A(K)$ we have*

$$\hat{\mathrm{h}}(p) + c \geq \mathrm{h}^{\heartsuit}(p). \tag{7.48}$$

Proof. From Theorem 107 we know that there exists a computable constant c' such that

$$\hat{\mathrm{h}}(p) + c' \geq \mathscr{H}(p). \tag{7.49}$$

The result follows from combining this with Lemma 118. □

Corollary 121. *For any constant B:*

$$\hat{M}(B) \subset M^{\heartsuit}(B + c) \tag{7.50}$$

where c is the computable constant from Theorem 120.

Lemma 122. *Fix a finite extension L/K. Given $a_1, \ldots, a_n \in L$, set $\psi_n = \prod_{i=1}^{n}(t - a_i)$. Then*

$$\left|\mathrm{h}(\psi_n) - \sum_{i=1}^{n} \mathrm{h}(a_i)\right| \leq \#M_K^{\infty} \log(4)(n^2 + n - 2)/2. \tag{7.51}$$

Proof. From [Lan83, Chapter 3, Proposition 2.4] we have for all $m \geq 2$ that

$$|\mathrm{h}(t - a_m) + \mathrm{h}(\psi_{m-1}) - \mathrm{h}(\psi_m)| \leq m\#M_K^{\infty} \log(4) \tag{7.52}$$

(note the difference in normalisations between our heights and Lang's). The formula follows by induction and using that $\mathrm{h}(t - a_i) = \mathrm{h}(a_i)$. □

Corollary 123. *For all $p \in A(K)$ we have*

$$\left|\mathrm{h}^{\heartsuit}(p) - \mathrm{h}^{\dagger}(p)\right| \leq \#M_K^{\infty} \log(4)(g^2 + g - 2)/2. \tag{7.53}$$

The main result of this chapter is then

Theorem 124. *Let c be the computable constant from Theorem 120. Then for all constants B we have*

$$\hat{M}(B) \subset M^{\dagger}\left(B + c + \#M_K^{\infty} \log(4)(g^2 + g - 2)/2\right). \tag{7.54}$$

The point is that these finite sets $M^{\dagger}(B)$ are effectively computable, so we can in turn use the results from Chapter 5 to compute the finite sets $\hat{M}(B)$. We describe one algorithm to compute $M^{\dagger}(B)$, setting $K = \mathbb{Q}$ for simplicity:

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) for each polynomial $a \in S$, if a is not irreducible remove it from S and insert into S each of the irreducible factors of a.

3) 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 listed in Section 2.3.4. Now the polynomial a also determines a set of $2\deg(a)$ distinct complex points on C - the preimages of zeros of a under the hyperelliptic projection. These can be computed to any finite precision. Such points will satisfy $y = b(x)$, thus if we can bound the denominators of the coefficients of b then we can find a finite precision to which we need to compute the complex points to see if they correspond to a polynomial b with rational coefficients. Such a bound on the denominators is supplied by the folowing proposition.

Proposition 125. *Let $K/\mathbb{Q}$ be a finite extension, with integers $\mathcal{O}_K$ and p a prime ideal in $\mathcal{O}_K$. Let $g > 0$ be an integer. Let f, $h \in K[x]$ be polynomials which are integral with respect to p and such that*

- *f is separable*
- *f has degree $2g + 1$*
- *h has degree at most $g + 1$.*

Fix an integer $1 \leq d \leq g$. Suppose we are given a pair of polynomials $a = \sum_{i=0}^{d} a_i x^i$ of degree d and $b = \sum_{i=0}^{d-1} b_i x^i$ of degree at most $d-1$ in $K[x]$ and a constant $c \in K$ with the following properties:

- a, b and c are integral at p

- a is primitive

- $\mathrm{ord}_p\, c > \min_i(\mathrm{ord}_p\, b_i)$

- $\Delta = \mathrm{disc}(a)$ is non-zero.

Suppose also that

$$a \mid \left(\frac{b}{c}\right)^2 + \left(\frac{b}{c}\right) \cdot h - f. \tag{7.55}$$

Then

$$\mathrm{ord}_p\, c \leq \frac{1}{2}\,\mathrm{ord}_p\, \Delta + \left(d^2 - d + \max\left(\frac{2g+1}{2}, \deg(h)\right)\right) \mathrm{ord}_p\, a_d. \tag{7.56}$$

Proof. Let L be a 'sufficiently large' extension of the completion K_p; by this we mean that L is a finite extension of the completion which we will require to be closed under taking roots of a certain finite collection of polynomials, which will be described as we go along. Let π denote a uniformiser of L, and $\mathcal{O}_L$ its integers.

We assume a splits in L; write $x_1, \ldots x_d$ for the roots. Each x_i may be uniquely written as $x_i = \tilde{x_i}/\pi^{r_i}$ where $r_i \geq 0$ and $\tilde{x_i} \in \mathcal{O}_L$ has minimal valuation. Let

$$\tilde{a} = \prod_{i=1}^{d} (\pi^{r_i} x - \tilde{x_i}) \in \mathcal{O}_L[x]. \tag{7.57}$$

Now a and $\tilde{a}$ have the same degree and (distinct) roots, are integral, and both have at least one coefficient which is a unit in $\mathcal{O}_L$, hence a and $\tilde{a}$ differ by a unit in $\mathcal{O}_L$.

Let

$$\widetilde{M} = \begin{pmatrix} \pi^{(d-1)r_1} & \pi^{(d-2)r_1}\tilde{x}_1 & \ldots & \tilde{x}_1^{d-1} \\ \pi^{(d-1)r_2} & \pi^{(d-2)r_2}\tilde{x}_2 & \ldots & \tilde{x}_2^{d-1} \\ \vdots & & & \\ \pi^{(d-1)r_d} & \pi^{(d-2)r_d}\tilde{x}_d & \ldots & \tilde{x}_d^{d-1} \end{pmatrix}, \tag{7.58}$$

so $\det(\widetilde{M})^2 = \mathrm{disc}(\tilde{a}) = \text{unit} \times \Delta$. Let

$$M = \begin{pmatrix} 1 & x_1 & \ldots & {x_1}^{d-1} \\ 1 & x_2 & \ldots & {x_2}^{d-1} \\ \vdots & & & \\ 1 & x_d & \ldots & {x_d}^{d-1} \end{pmatrix}. \tag{7.59}$$

By (7.55) we know that for all $1 \leq i \leq d$ we have

$$\sum_{j=0}^{d-1} \left(\frac{b_j}{c} \right) x_i^j = y_i \tag{7.60}$$

for some y_i in L (obtained by assuming L sufficiently large) satisfying $y_i^2 + h(x_i)y_i = f(x_i)$, and hence that

$$\frac{1}{c} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{d-1} \end{pmatrix} = M^{-1} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_d \end{pmatrix}. \tag{7.61}$$

In order to bound above the order of c at π, it therefore suffices to bound below the order of the right hand side of (7.61) at π. We do this in two steps. Firstly, we easily obtain from properties of valuations that

$$\operatorname{ord}_\pi y_i \geq -r_i \max\left(\frac{2g+1}{2}, \deg(h) \right). \tag{7.62}$$

Secondly, we must do the same for M^{-1}. Now $M \cdot \pi^{(d-1)\max_i r_i}$ is a matrix over $\mathcal{O}_L$, and hence so is its transposed matrix of cofactors, which we shall denote M_c. We then find that

$$M^{-1} = \frac{1}{\pi^{d(d-1)\max_i r_i}} \times \frac{1}{\det(M)} \times M_c. \tag{7.63}$$

We also compute that

$$\begin{aligned} \det(M) &= \pi^{-(d-1)\sum_i r_i} \det(\widetilde{M}) \\ &= \pi^{-(d-1)\sum_i r_i} \sqrt{\Delta \cdot \text{unit}}, \end{aligned} \tag{7.64}$$

and hence

$$M^{-1} = \frac{M_c}{\sqrt{\Delta \cdot \text{unit}}\, \pi^{d(d-1)\max_i(r_i) - (d-1)\sum_i r_i}}. \tag{7.65}$$

We also note that $\sum_i r_i = \operatorname{ord}_\pi a_d$, and $\max_i(r_i) \leq \sum_i r_i$, so combining the above results we see that

$$\operatorname{ord}_\pi c \leq \frac{1}{2} \operatorname{ord}_\pi \Delta + \left((d-1)^2 + \max\left(\frac{2g+1}{2}, \deg(h) \right) \right) \operatorname{ord}_\pi a_d, \tag{7.66}$$

from which the result immediately follows. □

We note that in the elliptic case, we recover the classical result that $c^3 \mid a_1^2$.

Bibliography

[Ara74] S. Y. Arakelov. An intersection theory for divisors on an arithmetic surface, Math. *USSR izvestija*, 8:1167–1180, 1974.

[Ara75] S. Y. Arakelov. Theory of intersections on the arithmetic surface. In *Proceedings of the International Congress of Mathematicians (Vancouver, B.C., 1974), Vol. 1*, pages 405–408. Canad. Math. Congress, Montreal, Que., 1975.

[Bak69] A. Baker. Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.*, 65:439–444, 1969.

[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).

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*. Springer, 1990.

[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.

[Can87] D.G. Cantor. Computing in the jacobian of a hyperelliptic curve. *Math. Comp*, 48(177):95–101, 1987.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[CGO84] Vincent Cossart, Jean Giraud, and Ulrich Orbanz. *Resolution of surface singularities*, volume 1101 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1984. With an appendix by H. Hironaka.

[CL09] Antoine Chambert-Loir. *Arakelov geometry: heights and the Bogomolov Conjecture*. 2009.

[CPS06] J. E. Cremona, M. Prickett, and Samir Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.

[Del87] P. Deligne. Le déterminant de la cohomologie. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 93–177. Amer. Math. Soc., Providence, RI, 1987.

[Dem68] V. A. Dem′janenko. An estimate of the remainder term in Tate's formula. *Mat. Zametki*, 3:271–278, 1968.

[Ehr51] Charles Ehresmann. Les connexions infinitésimales dans un espace fibré différentiable. In *Colloque de topologie (espaces fibrés), Bruxelles, 1950*, pages 29–55. Georges Thone, Liège, 1951.

[Fal84] G. Faltings. Calculus on arithmetic surfaces. *The Annals of Mathematics*, 119(2):387–424, 1984.

[FGI+05] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure, and A. Vistoli. *Fundamental algebraic geometry*, volume 123 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005. Grothendieck's FGA explained.

[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.

[Ful84] W. Fulton. *Intersection theory*. Springer, 1984.

[GH94] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1994. Reprint of the 1978 original.

[Gro61] A. Grothendieck. Éléments de géométrie algébrique. III. étude cohomologique des faisceaux cohérents. I. *Inst. Hautes Études Sci. Publ. Math.*, (11):167, 1961.

[Gro67] Alexander Grothendieck. Éléments de géométrie algébrique. *Inst. Hautes Études Sci. Publ. Math.*, 1960–1967.

[GS90a] Henri Gillet and Christophe Soulé. Arithmetic intersection theory. *Inst. Hautes Études Sci. Publ. Math.*, (72):93–174 (1991), 1990.

[GS90b] Henri Gillet and Christophe Soulé. Characteristic classes for algebraic vector bundles with Hermitian metric. II. *Ann. of Math. (2)*, 131(2):205–238, 1990.

[Har77] R. Hartshorne. *Algebraic Geometry*. Springer, Berlin, 1977.

[Hes] F. Hess. Computing riemann-roch spaces in algebraic function fields and related topics. *Journal of Symbolic Computation*, 33:425–445.

[Hol12] D. Holmes. Computing Néron-Tate heights of points on hyperelliptic Jacobians. *Journal of Number Theory*, 132(6):1295 – 1305, 2012.

[Hri77] P. Hriljac. The Néron-tate height and intersection theory on arithmetic surfaces. *PhD Thesis, Massachusetts Institute of Technology*, 1977.

[Lan83] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[Lan88] S. Lang. *Introduction to Arakelov theory*. Springer, 1988.

[Lel57] Pierre Lelong. Intégration sur un ensemble analytique complexe. *Bull. Soc. Math. France*, 85:239–262, 1957.

[Lev60] Harold I. Levine. A theorem on holomorphic mappings into complex projective space. *Ann. of Math. (2)*, 71:529–535, 1960.

[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 Erné, Oxford Science Publications.

[Man71] Ju. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[MM84] D. Mumford and C. Musili. *Tata Lectures on Theta: Jacobian theta functions and differential equations*. Springer, 1984.

[Moĭ64] B. G. Moĭšezon. A projectivity criterion of complete algebraic abstract varieties. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:179–224, 1964.

[Mue10] J. S. Mueller. Canonical heights on Jacobians. 2010. Universität Bayreuth PhD thesis.

[Mue11] J. S. Mueller. Computing canonical heights using arithmetic intersection theory. *ArXiv e-prints*, May 2011.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[Mum83] D. Mumford. *Tata lectures on theta I*. Birkhäuser, 1983.

[Mum08] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[Nak63] Yoshikazu Nakai. A criterion of an ample sheaf on a projective scheme. *Amer. J. Math.*, 85:14–26, 1963.

[Nér65] A. Néron. Quasi-fonctions et hauteurs sur les variétés abéliennes. *Annals of Mathematics*, 82(2):249–331, 1965.

[Pen55] R. Penrose. A generalized inverse for matrices. *Proc. Cambridge Philos. Soc.*, 51:406–413, 1955.

[PR01] S. Pauli and X.F. Roblot. On the computation of all extensions of a p-adic field of a given degree. *Mathematics of Computation*, 70(236):1659, 2001.

[Ser64] Jean-Pierre Serre. Exemples de variétés projectives conjuguées non homéomorphes. *C. R. Acad. Sci. Paris*, 258:4194–4196, 1964.

[Sil90] Joseph H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sou92] C. Soulé. *Lectures on Arakelov geometry*, volume 33 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1992. With the collaboration of D. Abramovich, J.-F. Burnol and J. Kramer.

[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.

[Zim76] Horst Günter Zimmer. On the difference of the Weil height and the Néron-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.