Computing canonical heights using arithmetic intersection theory

Müller, Steffen

Published in:
Mathematics of Computation

DOI:
10.1090/S0025-5718-2013-02719-6

Publication date:
2014

MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

COMPUTING CANONICAL HEIGHTS USING ARITHMETIC INTERSECTION THEORY

JAN STEFFEN MÜLLER

Abstract. For several applications in the arithmetic of abelian varieties it is important to compute canonical heights. Following Faltings and Hriljac, we show how the canonical height on the Jacobian of a smooth projective curve can be computed using arithmetic intersection theory on a regular model of the curve in practice. In the case of hyperelliptic curves we present a complete algorithm that has been implemented in Magma. Several examples are computed and the behavior of the running time is discussed.

1. Introduction

The canonical height $\hat{h}$ on an abelian variety A defined over a global field k is an object of fundamental importance in the study of the arithmetic of A. For many applications it is required to *compute* $\hat{h}(P)$ for a given point $P \in A(k)$. For instance, given generators of a subgroup of the Mordell-Weil group $A(k)$ of finite index, this is necessary for most known approaches to the computation of generators of the Mordell-Weil group $A(k)$. Furthermore, the regulator of $A(k)$, which appears in the statement of the conjecture of Birch and Swinnerton-Dyer, is defined in terms of the canonical height and thus we need the ability to compute canonical heights in order to gather numerical evidence for the conjecture in the case of positive rank.

Here we are concerned with the case where A is the Jacobian variety of a smooth projective curve C of genus g over k. If $g \leq 3$, it is known how to compute canonical heights using arithmetic on an explicit embedding of the Kummer variety K of A into $\mathbb{P}^{2^g-1}$ (cf. [37, 15, 38, 40] and [29, Chapter 3]). Trying to imitate this approach in the higher genus case quickly causes problems, as the Kummer variety becomes rather complicated (see the discussion in [29, Chapter 4]).

Instead we propose to use a result due to Faltings [13] and Hriljac [22] (see Theorem 3.2), expressing the canonical height in terms of arithmetic intersection theory. Here the non-archimedean intersection multiplicities take place on regular models of C, whereas the archimedean intersection multiplicities are given in terms of Green's functions on the Riemann surface associated to C. In Section 2 we discuss the local theory before putting the local results together in Section 3, culminating in Theorem 3.2 which establishes the connection between $\hat{h}$ and arithmetic intersection theory.

2010 *Mathematics Subject Classification.* Primary 11G50; Secondary 11G10, 11G30, 14G40.
Supported by DFG-grant STO 299/5-1.

In Section 4 we show how the necessary arithmetic intersection multiplicities can be computed in practice. In the non-archimedean case we reduce the problem to the computation of certain Gröbner bases. Then we show that the archimedean intersection multiplicities can be computed using theta functions with respect to the complex torus $\mathbb{C}^g/\Lambda$ associated to A. In order to make these steps practical, we need to be able to decompose divisors into prime divisors and to work on $\mathbb{C}^g/\Lambda$ explicitly.

We present a practical algorithm, implemented in the computer algebra system `Magma` [26], for the computation of $\hat{h}$ for hyperelliptic curves in Section 5 by explaining how these two points can be resolved in that case. Several examples are given in Section 6, where the performance of the algorithm is investigated as well. Finally, we elaborate on what is needed to extend the algorithm to non-hyperelliptic curves. A different, but similar, algorithm for the computation of $\hat{h}$ using arithmetic intersection theory has been developed independently by Holmes [20].

Acknowledgments: The research presented here is also described in Chapters 5 and 6 of my PhD dissertation [29] at the University of Bayreuth. I would like to thank my advisor Michael Stoll for suggesting this topic and for his constant help and encouragement.

Some of the research described in this work was conducted while I was visiting the University of Warwick and the University of Sydney. It is my pleasure to thank both institutions for their hospitality, as well as David Holmes, Samir Siksek and Steve Donnelly for their invitations.

2. Local Néron symbols

In this section we discuss the theory of local Néron symbols whose existence was first proved by Néron in [31]. We shall present an interpretation that is suitable for explicit computations, following essentially Gross [17] and Hriljac [22]. The content of the latter work is also discussed by Lang in [24]. In order to present these results, we need to briefly recall some basic notions of intersection theory on arithmetic surfaces.

In the following 3 sections C denotes a smooth projective geometrically connected curve of positive genus g, defined over a field k which will be specified as we go along. Let $\mathrm{Div}(C)$ denote the group of divisors on $C \times_k k^{\mathrm{sep}}$, where k^{sep} is a separable closure of k. For an extension k' of k contained in k^{sep} we denote the subgroup of k'-rational divisors by $\mathrm{Div}(C)(k')$. For each $n \in \mathbb{Z}$ the set $\mathrm{Div}^n(C)$ is defined to be the set of divisors of degree equal to n and we set

$$\mathrm{Div}^n(C)(k) := \mathrm{Div}^n(C) \cap \mathrm{Div}(C)(k).$$

If $f \in k(C)^*$ and $D = \sum_j m_j(Q_j) \in \mathrm{Div}^0(C)(k)$ is relatively prime to $\mathrm{div}(f)$, then we set $f(D) := \prod_j f(Q_j)^{m_j}$.

Let k be a non-archimedean local field valuation v with discrete valuation ring R, uniformizing element π, residue field $\mathfrak{k}$ and spectrum $S = \mathrm{Spec}(R)$.

Definition 2.1. A *model* $\psi : \mathcal{C} \to S$ of C over S is an integral, flat, Noetherian S-scheme of dimension 2 whose generic fiber is isomorphic to C.

Let $\psi : \mathcal{C} \to S$ denote a model of C over S. By abuse of notation, we often omit ψ and simply call $\mathcal{C}$ a model of C over S. We denote the special fiber of $\mathcal{C}$ by $\mathcal{C}_v$. Then $\mathcal{C}_v$ is connected by [25, Corollary 8.3.6].

Let $\mathrm{Div}(\mathcal{C})$ denote the group of Weil divisors on $\mathcal{C}$. If $D \in \mathrm{Div}(C)(k)$ is prime, then we write $D_{\mathcal{C}}$ for the Zariski closure of D on $\mathcal{C}$. This is a prime divisor on $\mathcal{C}$ and we extend the operation $D \mapsto D_{\mathcal{C}}$ to all of $\mathrm{Div}(C)(k)$ by linearity.

We want to use intersection theory on models of C over S. Although this can be defined more generally, it is convenient to restrict to proper regular models. For a proof that such a model always exists, see [25, §8.3.4]. In our algorithm we shall need a proper regular model of a specific kind; this will be discussed in Section 4.3.

So suppose that $\psi : \mathcal{C} \longrightarrow S$ is a proper regular model of C over S.

Definition 2.2. [24, §III.2] Let D, E be two effective divisors on $\mathcal{C}$ without common component and let $P \in \mathcal{C}_v$ be a closed point. Let $I_{D,P}$ and $I_{E,P}$ be defining ideals of D and E, respectively, in the local ring $\mathcal{O}_{\mathcal{C},P}$. Then the integer

$$i_P(D, E) := \mathrm{length}_{\mathcal{O}_{\mathcal{C},P}} \left(\mathcal{O}_{\mathcal{C},P}/(I_{D,P} + I_{E,P})\right)$$

is called the *intersection multiplicity of D and E at P*. The *total intersection multiplicity of D and E* is

$$i_v(D, E) := \sum_P i_P(D, E)[\mathfrak{k}(P) : \mathfrak{k}],$$

where the sum is over all closed points $P \in \mathcal{C}_v$. Finally, we extend i_P and i_v by linearity to divisors $D, E \in \mathrm{Div}(\mathcal{C})$ without common component.

A *fibral $\mathbb{Q}$-divisor* is an element of the $\mathbb{Q}$-vector space $\mathrm{Div}_v(\mathcal{C})$ generated by the irreducible components of $\mathcal{C}_v$. If $D \in \mathrm{Div}^0(C)(k)$, then we denote by $\Phi_{v,\mathcal{C}}(D)$ a fibral $\mathbb{Q}$-divisor on $\mathcal{C}$ such that $D_{\mathcal{C}} + \Phi_{v,\mathcal{C}}(D)$ has trivial intersection with all elements of $\mathrm{Div}_v(\mathcal{C})$. That such a fibral $\mathbb{Q}$-divisor always exists was first proved by Hriljac, cf. [24, Theorem III.3.6].

Now we have assembled all ingredients necessary to define the central objects of this section in the non-archimedean case.

Definition 2.3. The *local Néron symbol on C over k* is defined on divisors $D, E \in \mathrm{Div}^0(C)(k)$ with disjoint support by

$$\langle D, E\rangle_v := i_v(D_{\mathcal{C}} + \Phi_{v,\mathcal{C}}(D), E_{\mathcal{C}}) \log \#\mathfrak{k}.$$

Remark 2.4. [24, Theorem III.5.2]. The local Néron symbol depends neither on the choice of the regular model $\mathcal{C}$ nor on the choice of $\Phi_{v,\mathcal{C}}(D)$.

Next we let k denote an archimedean local field. We can assume $k = \mathbb{C}$ (see Proposition 2.8(d) below), so that $C(k)$ is actually a compact Riemann surface. In arithmetic intersection theory one uses Green's functions to define archimedean intersection multiplicities, but for us a somewhat weaker notion suffices. The next result follows from [23, Theorem 13.5.2] combined with [24, Proposition II.1.3], see also [17, §3].

Proposition 2.5. Let X be a compact Riemann surface and let $d\mu$ be a positive volume form on X such that $\int_X d\mu = 1$. For each $E \in \mathrm{Div}(X)$ there exists a function

$$g_E : X \setminus \mathrm{supp}(E) \to \mathbb{R},$$

called an *almost-Green's function with respect to E and $d\mu$*, such that the following properties are satisfied:

(i) The function g_E is C^∞ outside of $\mathrm{supp}(E)$ and has a logarithmic singularity along E.

(ii)
$$\deg(E)d\mu = \frac{i}{\pi}\partial\overline{\partial}g_E.$$

Let v be the absolute value on k and fix a volume form $d\mu$ on $C(k)$ such that $\int_X d\mu = 1$.

Definition 2.6. The pairing $\langle\cdot,\cdot\rangle_v$ that associates to all $D, E \in \mathrm{Div}^0(C)(k)$ with disjoint support the *intersection multiplicity*
$$i_v(D,E) := g_E(D)$$
is called the *local Néron symbol on C over k.*

Remark 2.7. It follows from [24, Proposition II.1.3] that the local Néron symbol does not depend on the choice of g_E or $d\mu$. See also [24, Theorem III.5.3].

We list the most important properties of the local Néron symbol, both non-archimedean and archimedean, in the following proposition.

Proposition 2.8. (Néron, Gross, Hriljac) Let k be a local field with valuation v. The local Néron symbol satisfies the following properties, where $D, E \in \mathrm{Div}^0(C)(k)$ have disjoint support.

(a) The symbol is bilinear.
(b) The symbol is symmetric.
(c) If $f \in k(C)^*$, then we have $\langle D, \mathrm{div}(f)\rangle_v = -\log|f(D)|_v$.
(d) If k' is a finite extension of k with valuation v' extending v, then we have $\langle D, E\rangle_{v'} = [k' : k]\langle D, E\rangle_v$.

Proof. See [24, §III.5] and [23, Theorems 11.3.6, 11.3.7].

□

3. Néron symbols and canonical heights

In this section we let k denote a global field with ring of integers $\mathcal{O}_k$. We assume that C is given by $\mathcal{O}_k$-integral equations. Let $M_k = M_k^0 \cup M_k^\infty$ denote the set of places of k, with absolute values $|\cdot|_v$ normalized to satisfy the product formula. Here M_k^0 (respectively M_k^∞) denotes the set of non-archimedean (respectively archimedean) places. For each place $v \in M_k$ we let k_v denote the completion of k at v. If $v \in M_k^0$, we let $\mathcal{O}_v$ be the ring of integers at v.

Let A denote the Jacobian variety of C and let K denote its Kummer variety $A/\{\pm 1\}$. Let $K \hookrightarrow \mathbb{P}^{2^g-1}$ be an embedding of K and let
$$\kappa : A \longrightarrow\!\!\!\!\rightarrow K \hookrightarrow \mathbb{P}^{2^g-1}.$$

Definition 3.1. [31],[17],[15] The *canonical height (or Néron-Tate height) on A* is the function defined by
$$\hat{h}(P) := \lim_{n\to\infty} 4^{-n} h(\kappa(2^n P)),$$

where h is the usual absolute height on $\mathbb{P}^{2^g-1}$. The *canonical height pairing (or Néron-Tate height pairing) on A* is defined by

$$(P,Q)_{\mathrm{NT}} := \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Note that taking the absolute height on $\mathbb{P}^{2^g-1}$ means that $\hat{h}$ does not depend on k.

Next we shall relate the canonical height to Néron symbols. If $D \in \mathrm{Div}(C)(k)$ and $v \in M_k$, then we define $D_v := D \otimes_k k_v$. For $D, E \in \mathrm{Div}^0(C)(k)$ with disjoint support and $v \in M_k$ we define $\langle D, E\rangle_v := \langle D_v, E_v\rangle_v$ and the *global Néron symbol* by

$$\langle D, E\rangle := \sum_{v \in M_k} \langle D, E\rangle_v.$$

This is a finite sum, since over all places of good reduction the Zariski closure $\overline{C}^v$ of the given equations of $C \times_k k_v$ over $\mathrm{Spec}(\mathcal{O}_v)$ is a proper regular model over $\mathrm{Spec}(\mathcal{O}_v)$. Hence we have $\Phi_{v,\overline{C}^v}(D_v) = 0$ for all such v and $i_v(D_{v,\overline{C}^v}, E_{v,\overline{C}^v}) \neq 0$ for only finitely many such v.

By Proposition 2.8(c) and the product formula, $\langle D, E\rangle$ only depends on the classes $[D], [E] \in \mathrm{Pic}^0(C)$ and hence we can drop the assumption that D and E have disjoint support.

Theorem 3.2. *(Faltings* [13]*, Hriljac* [22]*) Suppose C is a smooth projective geometrically connected curve of positive genus g defined over a global field k. If $D, E \in \mathrm{Div}^0(C)(k)$, then we have*

$$\langle D, E\rangle = -([D],[E])_{\mathrm{NT}}.$$

Remark 3.3. Note that Theorem 3.2 was shown in [13] and [22] for curves over number fields. The positive characteristic case can be proved in the same way, since the existence of local Néron symbols whose sum equals minus the canonical height was originally shown by Néron for any global field in [31], see [23, Chapter 11]. Moreover, note that the interpretation of the local Néron symbol at non-archimedean places outlined in the previous section is independent of the characteristic.

The practical importance of this result lies in the fact that we can, at least in principle, compute the canonical height on the Jacobian using data associated to the curve. We do not impose any further conditions on C (yet). Suppose that we are given a point $P \in A(k)$ and we want to compute its canonical height $\hat{h}(P)$. In order to use Theorem 3.2 for this purpose, we proceed as follows:

(1) Find divisors $D, E \in \mathrm{Div}^0(C)(k)$ such that $[D] = [E] = P$ and $\mathrm{supp}(D) \cap \mathrm{supp}(E) = \emptyset$.
(2) Determine a finite set U of places $v \in M_k^0$ such that $\{v \in M_k^0 : \langle D, E\rangle_v \neq 0\} \subset U$.
(3) Find a proper regular model $\mathcal{C}$ of $C \otimes_k k_v$ over $\mathrm{Spec}(\mathcal{O}_v)$ for all $v \in U$.
(4) Compute $i_v(D_{v,\mathcal{C}}, E_{v,\mathcal{C}})$ for all $v \in U$.
(5) Compute $i_v(\Phi_{v,\mathcal{C}}(D_{v,\mathcal{C}}), E_{v,\mathcal{C}})$ for all $v \in U$ of bad reduction. We call this the *correction term.*
(6) Find an almost-Green's function g_{E_v} and compute $g_{E_v}(D_v)$ for all $v \in M_k^\infty$.
(7) Sum up all local Néron symbols.

We deal with these steps in the following sections.

Remark 3.4. We shall tacitly assume from now on that step (1) is always possible in principle, that is every P we encounter can be represented using a k-rational divisor. According to [34, Proposition 3.3] this is guaranteed whenever the curve has a k_v-rational divisor of degree 1 for all $v \in M_k$. If we have $P \in A(k)$ which cannot be represented using a k-rational divisor, then we have two options:

1) Work over a field extension k' of k such that there exists some $D \in \mathrm{Div}^0(C)(k')$ satisfying $[D] = P$.
2) Compute a multiple nP such that there exists $D \in \mathrm{Div}^0(C)(k)$ satisfying $[D] = nP$ and use the quadraticity of the canonical height.

The existence of n as in 2) follows from [34, Proposition 3.2]; we can take for n the period of C over k.

4. Computing Néron symbols

In this section we shall address the steps needed for the computation of global Néron symbols introduced in the previous section. The first two steps are global in nature and can be viewed as preparatory steps for the remaining four sections which are local.

4.1. **Finding suitable divisors of degree zero.**

The basic reference for large parts of the remainder of this section is [19]. If an ideal I is generated by elements $b_1, \ldots, b_n$, then we write $I = (b_1, \ldots, b_n)$. Let k be an arbitrary field. There are essentially two ways to represent a divisor $D \in \mathrm{Div}(C)(k)$.

(a) As a sum
$$D = \sum_i m_i D_i,$$
where $D_i \in \mathrm{Div}(C)(k)$ is irreducible over k and $m_i \in \mathbb{Z}$ for all i. We call this the *free representation of* D.

(b) Assuming D is effective, using a defining ideal
$$I_D \subset k[C^a],$$
where C^a is an affine chart of C containing D. We call this an *ideal representation of* D.

Since in our intended applications we are allowed (and often even required) to vary divisors in their linear equivalence classes, it is a natural question to ask whether it is possible to find divisors linearly equivalent to a given divisor in a way that facilitates explicit computations.

Lemma 4.1. *(Hess) For all $D \in \mathrm{Div}(C)(k)$ and effective $A \in \mathrm{Div}(C)(k)$ there exists an effectively computable triple $(\tilde{D}, r, a)$, where $\tilde{D} \in \mathrm{Div}(C)(k)$ is effective, $r \in \mathbb{Z}$ and $a \in k(C)$ such that $\deg(\tilde{D}) < g + \deg(A)$ and we have*
$$D = \tilde{D} + rA + \mathrm{div}(a).$$
We call $\tilde{D}$ a reduction *of D along A. If $\deg(A) = 1$, then $\tilde{D}$ is the unique effective divisor such that $\dim(\mathcal{L}(\tilde{D} - r'A)) = 0$ for all $r' \geq 1$. In this case we have $D \sim \tilde{D} + rA$, where $r \in \mathbb{Z}$ is the maximal integer such that $\dim(\mathcal{L}(D - rA)) = 1$.*

Proof. See [19, §8]. □

Now assume that k is a global field, that we are given some divisor $D \in \mathrm{Div}^0(C)(k)$ and we want to find $E \sim D$ such that E and D have disjoint support. In other words, we are looking for an effective version of the moving lemma. However, we would like to keep the computations as simple as possible and this means that we would like to work with divisors that are reduced along some effective divisor of small degree whenever possible.

This leads to the following method:

1. Pick two effective divisors $A, A' \in \mathrm{Div}(C)(k)$ with disjoint support.
2. Compute multiples nD, where $n = 1, -1, 2, -2, \ldots$ and reduce them along A and A' until we find some n and n' such that the reduction $\tilde{D}_n$ of nD along A and the reduction $\tilde{D}_{n'}$ of $n'D$ along A' have disjoint support.
3. Let $r_n, r_{n'} \in \mathbb{Z}$ such that $nD \sim \tilde{D}_n + r_n A$ and $n'D \sim \tilde{D'}_{n'} + r_{n'} A'$. Compute

$$\begin{aligned}\langle D, D\rangle &= \frac{1}{nn'}\langle \tilde{D}_n + r_n A, \tilde{D'}_{n'} + r_{n'} A'\rangle \\ &= \frac{1}{nn'}\langle \tilde{D}_n, \tilde{D'}_{n'}\rangle + \frac{r_n}{nn'}\langle A, \tilde{D'}_{n'}\rangle + \frac{r_{n'}}{nn'}\langle \tilde{D}_n, A'\rangle + \frac{r_n r_{n'}}{nn'}\langle A, A'\rangle.\end{aligned}$$

In practice integers n, n' of fairly small absolute value usually suffice.

Remark 4.2. In the method above, it is not obvious how to pick A and A' in a way that facilitates explicit computations. If we have k-rational divisors A, A' of degree 1 on C then they can be used. If C is a plane curve, then we can use the zero or pole divisors of functions of the form $x - \zeta$, where $\zeta \in k$. See Section 5.1 for the case of hyperelliptic curves. In general the choice of A and of A' depends on the specific situation.

4.2. **Determining relevant non-archimedean places.**

We continue to let k denote a global field. Given two divisors D and E with disjoint support, we have to find a finite set of places $v \in M_k^0$ such that any non-archimedean v satisfying $\langle D, E\rangle_v \neq 0$ must lie in U.

We can assume that D and E are effective and use their respective ideal representations. The idea is to cover our curve by affine patches $C^1, \ldots, C^s$ and determine the relevant places for each patch using Gröbner bases. We refer to [1, Chapter 4] for an introduction to the theory and applications of Gröbner bases for polynomial rings over Euclidean rings.

So let

$$C^i = \operatorname{Spec} k[x_1, \ldots, x_n]/(G_{i,1}(x_1, \ldots, x_n), \ldots, G_{i,m_i}(x_1, \ldots, x_n))$$

be such an affine patch, where $G_{i,j}(x_1, \ldots, x_n) \in \mathcal{O}_k[x_1, \ldots, x_n]$ for all j. From now on we will assume that for each $v \in M_k^0$ there is some i, j such that $G_{i,j}$ is a v-adic unit. Note that this implies that the Zariski closure $\overline{C}^v$ of $C \times_k k_v$ over $\operatorname{Spec}(\mathcal{O}_v)$ is a model for C over $\operatorname{Spec}(\mathcal{O}_v)$.

Suppose for now that the ring of integers $\mathcal{O}_k$ is Euclidean and that D and E are represented by ideals $I_{D,i}$ and $I_{E,i}$, respectively, on C^i for each i. In fact we can assume that $I_{D,i}$ and $I_{E,i}$ are given by bases whose elements are in $\mathcal{O}_k[x_1, \ldots, x_n]$. If we compute a Gröbner basis B_i of

$$I_{D,E,i} := (G_{i,1}(x_1, \ldots, x_n), \ldots, G_{i,m_i}(x_1, \ldots, x_n)) + I_{D,i} + I_{E,i}$$

over $\mathcal{O}_k$, then B_i contains a unique element $q_{D,E,i} \in \mathcal{O}_k$.

We define the set U by

$$U := \{v \in M_k^0 : \mathrm{ord}_v(q_{D,E,i}) > 0 \text{ for some } i\}.$$

For the proof of the following Lemma, we need the notion and existence of a desingularization in the strong sense of $\overline{C}^v$ for each v. The necessary details are presented in Section 4.3 below.

Lemma 4.3. *Any non-archimedean place v such that $\langle D, E\rangle_v > 0$ is contained in U.*

Proof. Suppose that $\langle D, E\rangle_v > 0$ and let $\xi : \mathcal{C} \to \overline{C}^v$ denote a desingularization of $\overline{C}^v$ in the strong sense. The existence of ξ is asserted by 4.5, since by assumption $\overline{C}^v$ is a model of $C \times_k k_v$ over $\mathrm{Spec}(\mathcal{O}_v)$. Then we must have

$$i_v(\Phi_{v,\mathcal{C}}(D), E_{v,\mathcal{C}}) > 0 \text{ and } i_v(D_{v,\mathcal{C}}, \Phi_{v,\mathcal{C}}(E)) > 0 \tag{4.1}$$

or

$$i_v(D_{v,\mathcal{C}}, E_{v,\mathcal{C}}) > 0. \tag{4.2}$$

If (4.1) holds, then v must be a place of bad reduction such that both $D_{v,\overline{C}^v}$ and $E_{v,\overline{C}^v}$ intersect the singular locus of $\overline{C}^v$, since otherwise either $\Phi_{v,\mathcal{C}}(D)$ or $\Phi_{v,\mathcal{C}}(E)$ vanish.

If (4.2) holds, the fact that ξ is an isomorphism outside the singular locus of $\overline{C}^v$ implies that the closures $D_{v,\overline{C}^v}$ and $E_{v,\overline{C}^v}$ do not have disjoint supports. But this means that there is a point in the support of D and a point in the support of E having the same reduction modulo v. The claim follows easily from this. □

Hence the problem of determining U comes down to a combination of computing Gröbner bases and factoring.

If $\mathcal{O}_k$ is not a Euclidean ring, then we can still use this Gröbner basis approach by writing k as $k'(\alpha)$ for a primitive element α of k over k', where $k' = \mathbb{Q}$ if k is a number field and $k' = \mathbb{F}_p(T)$ if $\mathrm{char}(k) = p \neq 0$. This trick appears in [1, Exercise 4.3.1]. We add a new variable t to $\mathcal{O}_{k'}[x_1, \ldots, x_n]$, satisfying the relation

$$\phi_\alpha(t) = 0,$$

where ϕ_α is the minimal polynomial of α over k', and replace any occurrence of α in $I_{D,E,i}$ by t. Now we get at most one $q_{D,E,i}(t) \in \mathcal{O}_{k'}[t] \setminus \mathcal{O}_{k'}$ in the Gröbner basis of $I_{D,E,i}$, but we might also have some $q'_{D,E,i} \in \mathcal{O}_{k'}$. We factor the principal ideal $(q_{D,E,i}(\alpha))$ in $\mathcal{O}_k$ and, if necessary, the principal ideal $(q'_{D,E,i})$ in $\mathcal{O}_k$ to find the relevant $v \in M_k^0$.

4.3. **Computing regular models.**

In the following three sections we let k denote a non-archimedean local field with valuation v. Let R be its discrete valuation ring with spectrum $S = \mathrm{Spec}(R)$, uniformizing element π and residue field $\mathfrak{k}$. Suppose that C is given by R-integral equations and that the Zariski closure $\overline{C}$ of C over S is a model of C over S. In practice, it is easy to find such equations for C (for instance by requiring that there is some unit amongst their coefficients).

Definition 4.4. Let $\mathcal{C}'$ be a model of C over S. A *desingularization of $\mathcal{C}'$ in the strong sense* is a proper birational morphism $\xi : \mathcal{C} \to \mathcal{C}'$ such that $\mathcal{C}$ is regular and ξ is an isomorphism above every regular point of $\mathcal{C}'$.

The proof of the following result can be found in [25, Corollary 8.3.51]. It extends a proof due to Lipman, recalled in [2], of the same result in the special case that the given model of C over S is excellent.

Lemma 4.5. *Let $\mathcal{C}'$ be a model of C over S. Then there exists a desingularization of $\mathcal{C}'$ in the strong sense.*

Although the theory works for any proper regular model of C over S, for our algorithm we need a desingularization $\mathcal{C} \to \overline{C}$ in the strong sense, as in the previous section.

Lipman's proof is effective: The idea is to normalize $\overline{C}$ and then blow up the resulting model along its (necessarily isolated) irregular points. Repeating this process yields a desingularization of $\overline{C}$ in the strong sense after finitely many steps. The main problem is that normalizations are more difficult from a computational point of view than blow-ups.

A different effective proof of the existence of a desingularization of $\overline{C}$ in the strong sense is given by Cossart, Jannsen and Saito in [7], although they assume that $\overline{C}$ is excellent. The advantage of their method is that it only involves blow-ups, either along isolated irregular points or along irreducible components if the singular locus of the respective model has positive dimension.

This method has been implemented in `Magma` by Donnelly. The data that can be accessed once $\mathcal{C}$ has been constructed using `Magma` includes the blow-up maps on enough affine patches to cover all intermediate models, the intersection matrix of $\mathcal{C}_v$ and the multiplicities of the irreducible components.

A subtle point is that in the proof in [7] the blow-ups have to be performed in a specific order and this has not yet been included in the implementation, but it should be possible without too much difficulty. In any case, the implementation works well in practice. The only essential restrictions at the moment are that the curve has to be planar and that blow-ups along components are not implemented unless C is defined over $\mathbb{Q}$.

4.4. **Computing non-archimedean intersection multiplicities.**

We keep the notation from the previous section and fix a desingularization $\xi : \mathcal{C} \to \overline{C}$ in the strong sense, covered by affine patches

$$\mathcal{C}^i = \operatorname{Spec} R[x_1, \dots, x_{s_i}]/(H_{i,1}(x_1, \dots, x_{s_i}), \dots, H_{i,t_i}(x_1, \dots, x_{s_i})).$$

For computational purposes we shall assume for the moment that we have two effective divisors D and E with disjoint support whose closures $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ lie entirely in an affine piece $\mathcal{C}^i$.

The following lemma is a well-known result from commutative algebra saying that quotients and localizations commute.

Lemma 4.6. *Let A be a commutative ring with unity and let $T \subset A$ be a multiplicative subset. Let $I \subset A$ be an ideal and let $\bar{T}$ denote the image of T in A/I. Then we have*

$$A_T/IA_T \cong (A/IA)_{\bar{T}},$$

where the subscripts denote localizations.

Proof. See [27, Theorem 4.2]. □

Let $I_{D,i}$ and $I_{E,i}$ denote defining ideals of $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ in the ring $\mathcal{O}_{\mathcal{C}^i}$, respectively. For the computation of the intersection multiplicity we use the following version of the Chinese remainder theorem for modules.

Proposition 4.7. Let A be a commutative ring and let M be an Artinian and Noetherian A-module. Then there is an isomorphism of A-modules

$$M \cong \bigoplus_P M_P,$$

where the sum is over all maximal ideals P of A and M_P denotes the localization of M at P.

Proof. See [12, Theorem 2.13]. □

Proposition 4.8. Suppose that $D_{\mathcal{C}} \cap E_{\mathcal{C}}$ only intersects a single component Γ of $\mathcal{C}_v^i$. Let $\mathcal{O}_\Gamma$ denote the ring of regular functions on Γ. Then we have

$$i_v(D_{\mathcal{C}}, E_{\mathcal{C}}) = \operatorname{length}_{\mathcal{O}_\Gamma} (\mathcal{O}_\Gamma/(I_{D,i} + I_{E,i})\mathcal{O}_\Gamma)$$

Proof. From Proposition 4.7 we get an isomorphism of $\mathcal{O}_\Gamma$-modules

$$\mathcal{O}_\Gamma/(I_{D,i} + I_{E,i}) \cong \bigoplus_P \mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i}), \tag{4.3}$$

where the sum is over all maximal ideals of $\mathcal{O}_\Gamma$, that is, over all closed points $P \in \Gamma$. By our assumptions we have

$$\begin{aligned} i_v(D_{\mathcal{C}}, E_{\mathcal{C}}) &= \sum_P i_P(D_{\mathcal{C}}, E_{\mathcal{C}})[\mathfrak{k}(P) : \mathfrak{k}] \\ &= \sum_P \operatorname{length}_{\mathcal{O}_{\mathcal{C}^i,P}} \left(\mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i})\right)[\mathfrak{k}(P) : \mathfrak{k}] \\ &= \sum_P \operatorname{length}_{\mathcal{O}_\Gamma} \left(\mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i})\right) \\ &= \operatorname{length}_{\mathcal{O}_\Gamma} \bigoplus_P \left(\mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i})\right) \\ &= \operatorname{length}_{\mathcal{O}_\Gamma} (\mathcal{O}_\Gamma/(I_{D,i} + I_{E,i})) \end{aligned}$$

using (4.3), additivity of the length and the fact that if M is an $\mathcal{O}_\Gamma$-module that is also an $\mathcal{O}_{\mathcal{C}^i,P}$-module for some closed point $P \in \Gamma$, then we have

$$\operatorname{length}_{\mathcal{O}_\Gamma}(M) = \operatorname{length}_{\mathcal{O}_{\mathcal{C}^i,P}}(M)[\mathfrak{k}(P) : \mathfrak{k}].$$

□

Instead of computing $\operatorname{length}_{\mathcal{O}_\Gamma} (\mathcal{O}_\Gamma/(I_{D,i} + I_{E,i})\mathcal{O}_\Gamma)$ for each component Γ of $\mathcal{C}_v^i$, we can proceed more directly. Let

$$A_{D,E,i,v} := (R[x_1, \ldots, x_{s_i}]/I_{D,E,i,v})_{(\pi)} \tag{4.4}$$

where

$$I_{D,E,i,v} = (H_1(x_1, \ldots, x_{s_i}) \ldots, H_{t_i}(x_1, \ldots, x_{s_i})) + I_{D,i} + I_{E,i}. \tag{4.5}$$

Corollary 4.9. We have

$$i_v(D_{\mathcal{C}}, E_{\mathcal{C}}) = \operatorname{length}_{\mathcal{O}_{\mathcal{C}_v^i}} A_{D,E,i,v}$$

Proof. Use Proposition 4.8 and additivity of the length. □

Computing $\text{length}_{\mathcal{O}_{\mathcal{C}_v^i}} A_{D,E,i,v}$ is rather easy and can be done, for instance, in `Magma`. The crucial step is the computation of a Gröbner basis B of $I_{D,E,i,v}$ over the Euclidean ring R. Here the property of B that we need is that for every $h \in R[x_1, \ldots, x_{s_i}]$ multivariate division of h by B yields a unique remainder that we call $h \bmod B$.

The idea is to count residue classes as follows, where we start with $d = 0$.

Suppose $d \geq 0$. For each monomial g of total degree $d = \deg(g)$, find the integer n such that $\pi^j g$ is new for $j \in \{0, \ldots, n-1\}$, where we call $\pi^j g$ *new* if the residue classes of $\pi^j g$ has not already been counted. We can test the latter by checking whether the total degree of $\pi^j h \bmod B$ is at most equal to the total degree of h or whether $\pi^j h$ does not divide h.

If we find that no monomial of total degree d contributes a new residue class, then we are done, otherwise we increment d by 1 and repeat this process. See Algorithm 1.

Algorithm 1 Computation of $\text{length}_{\mathcal{O}_{\mathcal{C}_v^i}} A_{D,E,i,v}$

$B = \{g_1(x_1, \ldots, x_{s_i}), \ldots, g_r(x_1, \ldots, x_{s_i}), q\} \leftarrow$ Gröbner basis of $I_{D,E,i,v}$
$m \leftarrow \text{ord}_v(q)$ // q yields m distinct residue classes.
$d \leftarrow 0$ // Total degree
$T \leftarrow \emptyset$ // Monomials all of whose multiples are known not to be new
repeat
  $d \leftarrow d + 1$ // Increment total degree
  $V \leftarrow \{g = \prod_{i=1}^{s_i} x_i^{k_i} : k_i \in \mathbb{N},\ \sum_{i=1}^{s_i} k_i = d \text{ and } h \nmid g \text{ for all } h \in T\}$
  // No monomial of total degree d outside V can be new.
  $m' \leftarrow m$
  for $g \in V$ **do**
    $n \leftarrow 0$
    while $\deg(\pi^n g \bmod B) > d$ or $g \mid \pi^n g \bmod B$ **do**
      $n \leftarrow n + 1$ // $\pi^n g$ is new.
    end while
    $m \leftarrow n + m$ // Get n new residue classes.
    if $n = 0$ **then**
      $T \leftarrow T \cup \{g\}$ // No multiple of g is new.
    end if
  end for
until $m = m'$ // No monomial of total degree d is new.
return m

In order to apply the results of this section we need to be able to find

(a) an affine cover $\mathcal{C}_v^i$ of $\mathcal{C}$ containing $D_{\mathcal{C}} \cap E_{\mathcal{C}}$,
(b) ideal representations $I_{D,i}$ and $I_{E,i}$ of $D_{\mathcal{C}}|_{\mathcal{C}_v^i}$ and $E_{\mathcal{C}}|_{\mathcal{C}_v^i}$.

If the Zariski closure $\overline{C}$ of C over $\text{Spec}(R)$ is regular, then we can solve (a) and (b) by decomposing D and E into prime divisors over k. If the regular model has a more complicated structure, this may not be sufficient and we may have to decompose D and E into prime divisors over the maximal unramified extension k^{nr} since each such prime divisor reduces to a single point on the special fiber of both $\overline{C}$ and $\mathcal{C}$. This might be necessary because our strategy is to start with R-integral

ideal representations of D and E and recursively lift these through the blow-up process.

Note that we do not actually have to work over k^{nr}. In order to decompose D into prime divisors over k^{nr} it suffices to consider the maximal unramified extension l/k contained in the smallest extension $k(D)/k$ such that D becomes pointwise rational. It is possible to compute with such extensions in `Magma`.

Remark 4.10. The strategy employed to decompose D and E depends on the curve at hand; for hyperelliptic curves there is a straightforward method to decompose divisors that only uses factorization of univariate polynomials as explained in Section 5.

All of the above is trivial if D and E are pointwise k-rational:

Corollary 4.11. Suppose $D = \sum_l n_l(P_l)$ and $E = \sum_j m_j(Q_j)$, where $n_l, m_j \in \mathbb{Z}$ and all P_l and Q_j are k-rational such that $D_{\mathcal{C}} \cap \mathcal{C}_v$ and $E_{\mathcal{C}} \cap \mathcal{C}_v$ contain no singular points of $\mathcal{C}_v$. Then we have

$$i_v(D_{\mathcal{C}}, E_{\mathcal{C}}) = \sum_{l,j} n_l m_j \min\{\mathrm{ord}_v(x_1(P_l) - x_1(Q_j)), \ldots, \mathrm{ord}_v(x_{s_i}(P_l) - x_{s_i}(Q_j))\}$$

where $P_l = (x_1(P_l), \ldots, x_{s_i}(P_l))$, $Q_j = (x_1(Q_j), \ldots, x_{s_i}(Q_j)) \in C^i$.

Proof. This follows easily from Proposition 4.8 □

See [20] for a similar version of Lemma 4.11, found independently by Holmes.

Remark 4.12. A different strategy was brought to the attention of the author by Florian Hess and consists in computing the intersection multiplicities of $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ on all affine patches $\mathcal{C}^i$ such that $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ intersect on $\mathcal{C}^i_v$. For simplicity, we assume that these are $\mathcal{C}^1$ and $\mathcal{C}^2$. We then need to subtract from the result all intersections that take place on both $\mathcal{C}^1$ and $\mathcal{C}^2$ which can be expressed as the length of a certain module. This approach is outlined in [42], but it is not clear how it can be made practical if $\overline{C} \neq \mathcal{C}$.

4.5. **Computing the correction term.**

We continue to let $\mathcal{C}$ denote a desingularization in the strong sense of $\overline{C}$ over S. Suppose that the special fiber $\mathcal{C}_v$ is equal to $\sum_{i=0}^r n_i \Gamma_v^i$, where $\Gamma_v^0, \ldots, \Gamma_v^r$ are the irreducible components of $\mathcal{C}_v$. Let M_v denote the intersection matrix $\left(i_v(n_i\Gamma_v^i, n_j\Gamma_v^j)\right)_{0 \leq i,j \leq r}$ of $\mathcal{C}_v$.

Suppose we are given a divisor $D \in \mathrm{Div}^0(C)(k)$ and we want to compute a fibral $\mathbb{Q}$-divisor $\Phi_{v,\mathcal{C}}(D) = \sum_{i=0}^r \alpha_i n_i \Gamma_v^i$ having trivial intersection with $\mathrm{Div}_v(\mathcal{C})$. Also suppose that we have found both M_v and $s(D)$, where

$$s(D) = \left(n_0 i_v(D_{\mathcal{C}}, \Gamma_v^0), \ldots, n_r i_v(D_{\mathcal{C}}, \Gamma_v^r)\right)^T. \tag{4.6}$$

We mention two possible methods here, both easily checked to be correct using [24, §III.3].

(i) Let M_v^+ be the Moore-Penrose pseudoinverse of M_v. Then we can set

$$(\alpha_0, \ldots, \alpha_r)^T := -M_v^+ \cdot s(D).$$

(ii) (Cox-Zucker [8]) Suppose that there exists some i such that $n_i = 1$, say $n_0 = 1$, and let M'_v be the matrix obtained by deleting the first column and row from M_v. We pick $\alpha_0 := 0$ and

$$(\alpha_1, \ldots, \alpha_r)^T := -M_v'^{-1} \cdot s'(D),$$

where $s'(D)$ is the vector obtained by removing the first entry of $s(D)$.

We can now compute $i_v(\Phi_{v,\mathcal{C}}(D), E_{\mathcal{C}})$ easily for $E \in \mathrm{Div}^0(C)(k)$ having support disjoint from D. This is simply equal to

$$s(E)^T \cdot (\alpha_0, \ldots, \alpha_r)^T,$$

where $s(E)$ is defined as in (4.6).

It only remains to discuss how $s(D)$ and $s(E)$ can be computed, because M_v can be computed using `Magma` once $\mathcal{C}$ has been constructed. But this is essentially contained in the previous section: We decompose D and E into prime divisors over k^{nr} and then determine which components the corresponding points map to by lifting ideal representations recursively through the blow-up process. Since for any one of these divisors P all points in its support reduce to the same point in each step, it is easy to pick suitable affine patches covering the intermediate models until we find an affine patch of $\mathcal{C}$ containing $P_{\mathcal{C}}$. The final task is the computation of $i_v(P_{\mathcal{C}}, \Gamma_v^i)$ for all components Γ_v^i intersecting this affine patch which is easy under our assumptions.

4.6. **Computing archimedean intersection multiplicities.**

In order to deal with the computation of archimedean local Néron symbols it suffices to consider $k = \mathbb{C}$. Let $C(\mathbb{C})$ denote the Riemann surface associated to C. According to Section 3 we need to find an almost-Green's function with respect to a divisor $E \in \mathrm{Div}^0(C)(\mathbb{C})$. Notice that we can write any such divisor in the form $E = E_1 - E_2$, where E_1 and E_2 are *non-special*, that is they are effective of degree g and their $\mathcal{L}$-spaces have dimension 1. It suffices to determine almost-Green's functions with respect to non-special divisors and any fixed normalized volume form on $C(\mathbb{C})$.

In order to do this it turns out to be useful to work on the analytic Jacobian, which we view as an abelian variety over the complex numbers. Let τ be an element of the Siegel space $\mathfrak{h}_g$ such that $A(\mathbb{C})$ is isomorphic to the complex torus $\mathbb{C}^g/\Lambda$, where $\Lambda = \mathbb{Z}^g \oplus \tau\mathbb{Z}^g$. Let the map j be defined by

$$j : \mathbb{C}^g \longrightarrow\!\!\!\!\!\rightarrow \mathbb{C}^g/\Lambda \xrightarrow{\cong} A(\mathbb{C}).$$

Moreover, we fix an Abel-Jacobi map, that is an embedding ι of $C(\mathbb{C})$ into $A(\mathbb{C})$, and let $\Theta \in \mathrm{Div}(A)$ denote the theta-divisor with respect to ι. Let $S : \mathrm{Div}(C) \longrightarrow A$ denote the summation map associated to ι.

On $A(\mathbb{C})$ we can find the following canonical 2-form: Let $\eta_1, \ldots, \eta_g$ be an orthonormal basis of the differentials of first kind on the Jacobian. Then the canonical 2-form is given by

$$\frac{1}{2g}(\eta_1 \wedge \bar{\eta}_1 + \ldots + \eta_g \wedge \bar{\eta}_g)$$

and we define the *canonical volume form* $d\mu$ *on* $C(\mathbb{C})$ by pulling this form back using ι, see [23, §13.2]. The details are not important for us as the dependence on $d\mu$ for divisors of degree zero.

For the next theorem, conjectured by Arakelov and proved by Hriljac, we need the concept of Néron functions with respect to divisors on A, for which we refer to [23, Chapter 11]. We will introduce a specific Néron function in the situation we are interested in shortly. We use the notation E_P to denote the translation of a divisor $E \in \mathrm{Div}(A)$ by a point $P \in A$.

Theorem 4.13. *(Hriljac) Let $E \in \mathrm{Div}^g(C)$ be non-special, let $P = S(E)$ and $E' = ([-1]^*(\Theta))_P$. Let $\lambda_{E'}$ be a Néron function with respect to E'. Then $\lambda_{E'} \circ \iota$ is an almost-Green's function with respect to E and $d\mu$, where $d\mu$ is the canonical volume form on $C(\mathbb{C})$.*

Proof. See [23, Theorem 13.5.2]. □

The great news is that it is not difficult to find Néron functions with respect to Θ; we show below that this suffices for our purposes.

Definition 4.14. Let $g \geq 1$ and $a, b \in \mathbb{Q}^g$. Let the function $\theta_{a,b}$ on $\mathbb{C}^g \times \mathfrak{h}_g$ be given by

$$\theta_{a,b}(z,\tau) = \sum_{m \in \mathbb{Z}^g} \exp\left(2\pi i \left(\frac{1}{2}(m+a)^T \tau (m+a) + (m+a)^T (z+b)\right)\right).$$

We call $\theta_{a,b}$ the *theta function with characteristic* $[a;b]$.

Now let $a = (1/2, \ldots, 1/2), b = (g/2, (g-1)/2 \ldots, 1, 1/2) \in \mathbb{Q}^g$ and consider $\theta_{a,b}(z) := \theta_{a,b}(z,\tau)$ as a function on $\mathbb{C}^g$.

Proposition 4.15. (Pazuki) The function $\theta_{a,b}$ has divisor $j^*(\Theta)$. Moreover, the following function is a Néron function associated with Θ:

$$\lambda_\Theta(P) = -\log|\theta_{a,b}(z(P))| + \pi \Im(z(P))^T (\Im(\tau))^{-1} \Im(z(P)),$$

where $j(z(P)) = P$.

Proof. This was stated without proof by Pazuki in [33, Proposition 3.2.11], but it is in fact rather easy to verify: It is a classical theorem (see [23, Theorem 13.4.1]) that the divisor of the Riemann theta function $\theta = \theta_{0,0}$ is a translate by a point w of Θ and that $2w$ is the image on A of the canonical class on C. Using this it is not hard to see that the odd function $\theta_{a,b}$ has divisor $j^*(\Theta)$. Then one uses [23, Theorem 13.1.1] to find an expression of a Néron function in terms of the normalized theta function

$$\theta'_{a,b}(z) := \theta_{a,b}(z) \exp\left(\frac{\pi}{2} z^T (\Im\tau)^{-1} z\right);$$

the right hand side in Proposition 4.15 is equal to this expression after a straightforward manipulation.

Alternatively one can show directly that λ_Θ satisfies the properties of a Néron function. □

Now suppose that $E = E_1 - E_2$, where $E_1, E_2 \in \mathrm{Div}(C)$ are non-special divisors with disjoint support, and let $D_1 = \sum_{i=1}^d (P_i)$ and $D_2 = \sum_{i=1}^d (Q_i)$ be two effective divisors such that $\mathrm{supp}(E_i) \cap \mathrm{supp}(D_j) = \emptyset$ for $i, j \in \{1, 2\}$.

Corollary 4.16. We have

$$\begin{aligned}&\langle D_1 - D_2, E_1 - E_2\rangle_v \\ &= -\log \prod_{i=1}^{d} \frac{|\theta_{a,b}(z(\iota(P_i)) - z(S(E_1)))\theta_{a,b}(z(\iota(Q_i)) - z(S(E_2)))|_v}{|\theta_{a,b}(z(\iota(P_i)) - z(S(E_2)))\theta_{a,b}(z(\iota(Q_i)) - z(S(E_1)))|_v} \\ &\quad - 2\pi \sum_{i=1}^{d} \Im(z(S(E_1) - S(E_2)))^T \Im(\tau)^{-1} \Im(z(\iota(P_i)) - z(\iota(Q_i))),\end{aligned}$$

where for any $Q \in A$ the tuple $z(Q) \in \mathbb{C}^g$ satisfies $j(z(Q)) = Q$.

Proof. Néron functions are invariant under translation of the divisor up to an additive constant, see [23, Theorem 11.2.1]. But according to [23, Theorem 5.5.8], $[-1]^*(\Theta)$ is just Θ translated by $S(\mathfrak{K})$, where $\mathfrak{K}$ is a canonical divisor. Hence the desired result follows from Theorem 4.13 and Proposition 4.15. □

Remark 4.17. In [20] Holmes gives a more direct proof of Lemma 4.16 using [23, §13.6/7], which relies on the theory of differentials of the third kind.

We can use the previous result to compute intersections at archimedean places. In practice we need to be able to do the following:

1) Given $E \in \mathrm{Div}^0(C)$, find non-special E_1, E_2 such that $E = E_1 - E_2$.
2) Compute the period matrix τ.
3) Given $P_1 \in C(\mathbb{C})$ and τ, determine $z \in \mathbb{C}^g$ such that $j(z) = \iota(P_1)$.
4) Given τ and $z \in \mathbb{C}^g$, compute $\theta_{a,b}(z) = \theta_{a,b}(z, \tau)$.

5. The hyperelliptic case

We now discuss how the methods outlined in the previous section can be combined to give a practical algorithm for the computation of canonical heights in the case of hyperelliptic curves.

Suppose that C is a hyperelliptic curve of genus g defined over a field k, given as the smooth projective model of an equation

$$Y^2 + H(X,1)Y = F(X,1), \tag{5.1}$$

where $F(X,Z), H(X,Z) \in k[X,Z]$ are forms of degrees $2g+2$ and $g+1$, respectively, and the discriminant of the equation (5.1) is nonzero. We will vary k as in general discussion of the previous sections.

A different, but related approach to the computation of the local Néron symbols has been developed independently by Holmes [20]. The main difference lies in the computation of the non-archimedean intersection multiplicities. In [20], norm maps of non-archimedean field extensions are used instead of our Gröbner basis approach.

5.1. **Finding suitable divisors of degree zero.**

Suppose that $D \in \mathrm{Div}(C)(k)$ has degree zero. Then the notions introduced in Section 4.1 are all well-known: The reduction process is part of Cantor's algorithm for the addition of divisor classes introduced in [6]; here the divisor A used for reduction is equal to (∞) when we have a k-rational Weierstrass point ∞ at infinity and is equal to $(\infty_1) + (\infty_2)$ when there are two branches ∞_1, ∞_2 over the singular point at infinity in the projective closure of equation (5.1).

In the former case Lemma 4.1 says that the reduction process yields the unique effective divisor $\tilde{D}$ such that

$$D \sim \tilde{D} + r(\infty),$$

where $0 \leq -r = \deg \tilde{D} \leq g$ and $\deg(\tilde{D})$ is minimal. In the latter case it turns out that when g is even we can still find a unique $\tilde{D}$ of minimal nonnegative even degree $-r \leq g$ such that

$$D \sim \tilde{D} + \frac{r}{2}((\infty_1) + (\infty_2))$$

if we impose further conditions on its ideal representation. Conversely, if g is odd we might have to take reductions of degree $g+1$ into account and these are not unique. However, uniqueness of the reduction is not an essential property in our applications and so we shall not discuss it any further.

A possible ideal representation of a reduced effective divisor D is given by the *Mumford representation* which we now recall briefly.

If we view C as embedded in weighted projective space with weights $1, g+1, 1$ assigned to the variables X, Y, Z, then it is given by the equation

$$Y^2 + H(X,Z)Y = F(X,Z).$$

An effective divisor D of degree $d \leq g+1$ corresponds to a pair of homogeneous forms $(A(X,Z), B(X,Z))$, where $A(X,Z)$ and $B(X,Z)$ have degrees d and $g+1$ respectively, such that D is defined by

$$A(X,Z) = 0 = Y - B(X,Z)$$

and we impose the additional condition that

$$A(X,Z) \mid B(X,Z)^2 + H(X,Z)B(X,Z) - F(X,Z).$$

First suppose that there is a unique Weierstrass point ∞ at infinity in $C(k)$. Then any nonzero effective divisor $D = \sum_{j=1}^{d}(P_j)$ that is reduced along (∞) has degree $d \leq g$ and cannot contain ∞ in its support. Hence we can safely dehomogenize in order to represent D and so we may take

$$I_D = (a(x), y - b(x)),$$

where $a(x) = A(x,1)$ and $b(x) = B(x,1)$, for its ideal representation. More concretely, we have

$$a(x) = \prod_{j=1}^{n}(x - x(P_j))$$

and $b(x)$ has minimal degree such that

$$b(x(P_j)) = y(P_j) \text{ for } j = 1, \ldots, d.$$

Conversely, suppose that there are two points ∞_1, ∞_2 at infinity. Suppose that D is reduced along $(\infty_1) + (\infty_2)$. If $\operatorname{supp}(D)$ does not contain a point at infinity, then we can dehomogenize as before to find an affine representation. If this does not hold, say $\infty_1 \in \operatorname{supp}(D)$, then necessarily $\infty_1, \infty_2 \in C(k)$ and $\infty_2 \notin \operatorname{supp}(D)$. This case is more subtle, because we cannot tell the multiplicity of ∞_1 in D from its dehomogenized form. For our applications it suffices to treat the affine and the infinite part of D separately. Hence this complication does not cause any trouble.

Now let k be a global field, and let the divisor D_∞ be defined by $2(\infty)$ if there is a unique k-rational point at infinity and by $(\infty_1)+(\infty_2)$ otherwise. Also suppose d is even and

$$D = \tilde{D} - \frac{d}{2}D_\infty,$$

where $\tilde{D} = \sum_{i=1}^{d}(P_i)$ is reduced along D_∞ such that no P_i is a point at infinity or a Weierstrass point. Then we can always use $n_1 = 1$ and $n_2 = -1$ in the method introduced in Section 4.1; this is due to Holmes, see [20]. Namely, if we apply the hyperelliptic involution

$$Q \mapsto Q^-$$

to the points P_i, then we have

$$D' = \sum_{i=1}^{d}(P_i^-) - \frac{d}{2}D_\infty \sim -D.$$

If we move this by the divisor of a function $x-\zeta$, where $\zeta \in k$ is such that $x(P_i) \neq \zeta$ for all P_i, then we find

$$\operatorname{supp}(D) \cap \operatorname{supp}(E) = \emptyset,$$

where $E = D' + d/2\operatorname{div}(x-\zeta)$. This corresponds to choosing $A = D_\infty$ and $A' = D(\zeta)$ in the method outlined above, where $D(\zeta) = \operatorname{div}(x-\zeta) + D_\infty$.

Instead of computing $\langle D, D\rangle$, we can now compute

$$\hat{h}(P) = -\langle D, D\rangle = \langle D, -D\rangle = \langle D, E\rangle.$$

If we have

$$D = \tilde{D} - \frac{d}{2}D_\infty,$$

where

$$\tilde{D} = \sum_{i=1}^{d'}(P_i) + n_\infty(\infty_1)$$

is reduced along $D_\infty = (\infty_1)+(\infty_2)$, such that $d = d'+n_\infty$ and all P_i are affine non-Weierstrass points (see Section 5.1), then we also have to move D away from ∞_1 using a function $x-\zeta'$, where $x(P_i) \neq \zeta' \neq \zeta$ for all $i = 1, \ldots, d'$. The computation becomes

$$-\langle D, D\rangle = \langle \sum_{i=1}^{d'}(P_i) + n_\infty(\infty_1) - \frac{d}{2}D(\zeta'), \sum_{i=1}^{d'}(P_i^-) + n_\infty(\infty_2) - \frac{d}{2}D(\zeta)\rangle$$

and poses no additional problems due to the bilinearity of the local Néron symbol.

What if there is a unique rational Weierstrass point ∞ at infinity and d is odd? In that case we use

$$D' = 2\sum_{i=1}^{d}(P_i^-) - dD_\infty \sim -2D$$

and compute

$$\hat{h}(P) = -\langle D, D\rangle = \langle D, -D\rangle = \frac{1}{2}\langle D, E\rangle,$$

where $E = D' + d\,\mathrm{div}(x-\zeta)$ and ζ is as above. Note that we can still use the reduced Mumford representation, because we have

$$\langle D, E\rangle = 2\langle D, \sum_{i=1}^{d}(P_i^-)\rangle - d\langle D, D(\zeta)\rangle.$$

Finally, if $\mathrm{supp}(D)$ contains an affine Weierstrass point, then we simply compute $\hat{h}(P) = \frac{1}{n^2}\hat{h}(nP)$ such that nP has a reduced representation not containing an affine Weierstrass point.

5.2. **Determining relevant non-archimedean places.**

Suppose that k is a global field. Our curve C is covered by two affine patches C^1 and C^2, where

$$C^1 : y^2 + H(x,1)y = F(x,1) \tag{5.2}$$

and

$$C^2 : w^2 + H(1,z)w = F(1,z). \tag{5.3}$$

It follows from the discussion at the end of Section 4.2 that we can assume $\mathcal{O}_k$ to be Euclidean. Suppose that D and E are $I_{D,1} = (a(x), cy - b(x))$ and $I_{E,1} = (a'(x), c'y - b'(x))$ on C^1, respectively (where we have multiplied all polynomials by the least common multiple of the denominators of their coefficients, if necessary). Then we need to compute a Gröbner basis of

$$I_{D,E,1} = (y^2 + H(x,1)y - F(x,1), a(x), a'(x), cy - b(x), c'y - b'(x))$$

and factor the unique element $q_{D,E,1}$ of $\mathcal{O}_k$ appearing in this basis.

Now suppose that $v \in M_k^0$ satisfies $i_v(D_{v,\mathcal{C}}, E_{v,\mathcal{C}}) > 0$, where $\mathcal{C} \to \overline{C}^v$ is a desingularization in the strong sense and that the points of intersection do not map to the closure of C^1 in $\mathcal{C}$. Any such v must satisfy $v(a_d) > 0$ and $v(a'_{d'}) > 0$, where a_d and $a'_{d'}$ are the leading coefficients of $a(x)$ and $a'(x)$, respectively. So instead of computing a Gröbner basis of $I_{D,E,2}$, we can factor $\gcd(a_d, a'_d)$ which is usually much easier than factoring $(q_{D,E,2})$. This simplification can make a big difference in practice.

5.3. **Computing non-archimedean intersection multiplicities and the correction term.**

Let k denote a non-archimedean local field and let π be a uniformizing element.

Let $D \in \mathrm{Div}(C)(k)$ be effective such that an ideal representation of D on C^1 is

$$I_{D,1} = (a(x), y - b(x)),$$

where $a(x), b(x) \in k[x]$ and we have $\deg(a) \le g$ and $\deg(b) \le g+1$ as in Section 5.1.

In order to use Proposition 4.8 to compute non-archimedean intersection multiplicities, we need to be able to decompose divisors into prime divisors over unramified extensions. The main point distinguishing the hyperelliptic case from the general situation is that we can decompose divisors by factoring univariate polynomials over non-archimedean local fields; we show how this can be used in this section.

Note that factoring univariate polynomials over p-adic fields and Laurent series over finite fields is implemented in `Magma` (following work of Pauli [32]).

We first deal with the case $\mathcal{C} = \overline{C}$ and use the affine cover $\mathcal{C} = \mathcal{C}^1 \cup \mathcal{C}^2$, where $\mathcal{C}^i$ is defined as follows: Let C^i be the affine curve defined as in Section 5.2 and let $V^i \subset C$ denote the complement of C^i in C. Let $\overline{V^i}$ denote the closure of V^i in $\mathcal{C}$, then $\mathcal{C}^i$ is defined as the complement of $\overline{V^i}$ in $\mathcal{C}$.

We can factor $a(x) = a_1(x)a_2(x)$, where $a_2(x)$ is constant modulo π and $a_1(x) \in R[x]$. This corresponds to a decomposition $D = D_1 + D_2$, where $D_{1,\mathcal{C}}$ lies in $\mathcal{C}^1$ and $D_{2,\mathcal{C}}$ lies in $\mathcal{C}^2$. More precisely, we have

$$I_{D_1,1} = (a_1(x), y - b_1(x)),$$

where $b_1(x) = b(x) \bmod a_1(x)$. In order to use Proposition 4.8, we need $b_1(x) \in R[x]$. Suppose that $a_1(x)$ is irreducible (otherwise factor $a_1(x)$ into irreducibles) and that $b_1(x) \notin R[x]$. If $D_{1,\mathcal{C}}$ does not have a singular point of the special fiber $\overline{C}_v$ in its support (for instance, if a_1 is unramified), then we can safely extend k by a root of a_1 and work over this extension. Repeating this process, if necessary, leads to a finite extension k' of k such that $D_{1,\mathcal{C}}$ splits into prime divisors over k' that have R'-rational ideal representations, where R' is the ring of integers of k'.

Now suppose that $a_1(x)$ reduces to $(x-a)^m \bmod \pi$, where a is the x-coordinate of a singular point of $\overline{C}_v$ and $m \geq 1$. In general we cannot extend the field by a root of a_1, because there may be points in the support of $D_{1,\mathcal{C}}$ that are not regular over this extension. But because of the special shape of a_1, we can simply use the R-rational ideal representation $(a_1(x), \pi^s y - b_1'(x))$, where $b_1(x) = \pi^{-s} b_1'(x)$, and $b_1(x) \in R[x]$ has a unit among its coefficients. Note that this approach does not always work for more general $a_1(x)$.

If we have $\mathcal{C} \neq \overline{C}$, then we simply start by factoring $a(x)$ into irreducibles over k^{nr}. Assuming that $a_1(x)$ is one of the irreducible factors, we lift the ideal representation $I_{D_1,\mathcal{C}} = (a_1(x), \pi^s y - b_1'(x))$ recursively through suitable blow-ups until we arrive at a suitable affine patch where the intersection multiplicities can be computed using Proposition 4.8. As explained in Subsection 4.5, this is also sufficient to compute the correction term.

5.4. **Computing archimedean intersection multiplicities.**

In order to compute archimedean intersection multiplicities, we need algorithms for steps 1)–4) introduced at the end of Section 4.6.

For hyperelliptic curves, steps 2), 3) and 4) have all been implemented in `Magma` by van Wamelen. An earlier version of the implementation using `Mathematica` can be found on van Wamelen's homepage [41]. The routines there only work for genus 2 curves, but the general algorithm in `Magma` work similarly.

It is important to note that step 4), the computation of $\theta_{a,b}$, is done via approximation using the definition, in particular it can be used to compute $\theta_{a,b}$ provably up to desired precision.

We discuss step 1). Here we want to find, given $P, Q \in A$, divisors D_1, D_2, E_1 and E_2 such that

(a) $[D_1 - D_2] = P$ and $[E_1 - E_2] = Q$,
(b) D_1, D_2, E_1, E_2 are effective and have pairwise disjoint support,
(c) E_1 and E_2 are non-special.

We can allow ourselves more freedom, and only require that (a) holds for some multiple nQ, due to the bilinearity of the local Néron symbol. For simplicity we only discuss the case of a unique point at infinity, the other case being similar

with a few minor subtleties if g is odd. We pick $D_1 := \tilde{D}$ and $D_2 := d(\infty)$ if P is represented by $\tilde{D} - d(\infty)$ and $\tilde{D}$ has affine support. Suppose that nQ is represented by $\tilde{E}_n - g(\infty)$, where $\tilde{E}_n$ is non-special and has affine support such that $\tilde{E}_n$ and $\tilde{E}'_n$ have support disjoint from $\tilde{D}$, where $\tilde{E}'_n$ is the result of the hyperelliptic involution applied to the points in the support of $\tilde{E}_n$. Then $2nQ$ is represented by $\tilde{E}_n - \tilde{E}'_n$ and we choose $E_1 := \tilde{E}_n$ and $E_2 := \tilde{E}'_n$. .

With these choices, at most $d + g$ applications of the Abel-Jacobi map and at most $2d$ applications of the theta-function $\theta_{a,b}$ are required in order to compute $\langle D_1 - D_2, E_1 - E_2 \rangle_v$ for an archimedean place v, essentially because we have $\iota(\infty) = 0$.

Now let $\zeta \in k^*$ be as in Section 5.1. We are actually interested in computing

$$\langle \tilde{D} - d(\infty), \tilde{E} - e/2D(\zeta) \rangle_v, \tag{5.4}$$

so we compute a function $\beta \in k(C)^*$ such that

$$\operatorname{div}(\beta) = E_1 - E_2 - 2n\tilde{E} + ndD(\zeta)$$

See [19] for an algorithm that computes β. Using properties (a) and (c) of Proposition 2.8 we can compute (5.4).

Notice that in contrast to the non-archimedean case the running times of steps 3) and 4) do not crucially depend on the heights of the points in the supports of the respective divisors, since we work with the complex uniformization.

6. Examples

In this section we provide a hyperelliptic example of a regulator that was computed using the algorithm outlined in the previous sections. Moreover, we shall discuss, at least in the case of hyperelliptic curves, how the running time changes as we increase

(a) the genus of the curve;
(b) the size of the coefficients of the point.

All times are in seconds, unless noted otherwise. For the computations we have used 50 digits of p-adic and 30 digits of real and complex precision.

We first use the `Magma`-implementation of our algorithm to compute the regulator of the Jacobian of a hyperelliptic genus 3 curve up to an integral square.

Example 6.1. Let C be given by the smooth projective model of the equation

$$Y^2 = X(X-1)(X-2)(X-3)(X-6)(X-8)(X+8).$$

The curve C is a hyperelliptic curve of genus 3, defined over $\mathbb{Q}$. A quick search reveals the following rational non-Weierstrass points on C.

$$(-2, \pm 240), (4, \pm 48), (-6, \pm 1008)$$

Let A denote the Jacobian of C; obviously its entire 2-torsion subgroup is defined over $\mathbb{Q}$. In order to bound the Mordell-Weil rank of A we compute the dimension of the 2-Selmer group of A over $\mathbb{Q}$ using `Magma`. This dimension is equal to 3 and hence we get an upper bound of 3 on the rank. If $P_1, \ldots, P_n \in A$, then we denote the *regulator* of $P_1, \ldots, P_n$ by

$$\operatorname{Reg}(P_1, \ldots, P_n) = \det\left((P_i, P_j)_{\mathrm{NT}}\right)_{i,j}.$$

prime	# of comps.	Ψ_p	time
2	14	$(\mathbb{Z}/2\mathbb{Z})^5$	1.95
3	9	$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z}$	0.35
5	4	$(\mathbb{Z}/2\mathbb{Z})^3$	0.23
7	3	$(\mathbb{Z}/2\mathbb{Z})^2$	0.29
11	2	$\mathbb{Z}/2\mathbb{Z}$	0.10

TABLE 1. Regular model data

$S \in A(\mathbb{Q})$	$\hat{h}(S)$	time
P	1.900087075211040826920480902 66	23.10
Q	1.152617936309056291065144470 88	19.76
R	2.900908316163367270109402142 90	20.96
$P+Q$	2.364815842037153818578368352 38	19.95
$P+R$	5.515840785649853498445720299 52	20.67
$Q+R$	5.749018934841371707555802193 03	21.22

TABLE 2. Canonical height computations

We want to compute the regulator $\mathrm{Reg}(P,Q,R)$ of the subgroup G of $A(\mathbb{Q})$ generated by the points

$$\begin{aligned} P &= (-2,-240)-(\infty) \\ Q &= (4,-48)-(\infty) \\ R &= (-6,1008)-(\infty). \end{aligned}$$

The discriminant of C factors as $2^{50}3^{12}5^6 7^4 11^2$. We first find regular models at the bad primes 2, 3, 5, 7 and 11. All computations in this example were done using `Magma` on a 1.73 GHz Pentium processor. It turns out that all computed regular models are already minimal; we list the number of components of the special fiber of the respective regular model, the (geometric) group of components Ψ_p of the Néron model and the time it took to compute the regular model in Table 1.

After this preparatory step we now compute the entries of the height pairing matrix. The results and timings can be found in Table 2,

Using these results, we find

$$\mathrm{Reg}(P,Q,R) = 4.288809861774632830588619343 66.$$

We can test our findings by computing $\mathrm{Reg}(nP,mQ,lR)$ for several integral values of n,m,l. In all cases we get the relation

$$\mathrm{Reg}(nP,mQ,lR)/\mathrm{Reg}(P,Q,R) = n^2m^2l^2$$

up to an error of less than 10^{-29}. As $\mathrm{Reg}(P,Q,R)$ is clearly non-zero, we know that G is a subgroup of finite index and hence $\mathrm{Reg}(P,Q,R)$ equals $\mathrm{Reg}(A/\mathbb{Q})$ up to a rational square.

Next we want to illustrate the behavior of the running time of our algorithm. We have refrained from a formal complexity analysis, mostly because the algorithm uses several external subroutines, such as the computation of regular models and of theta functions, whose complexities have not yet been analyzed.

In the case of zero-dimensional ideals of polynomial rings over fields, the complexity of a Gröbner basis computation can be shown to be polynomial in D^n, where D is the maximal degree of the elements of the basis we start with and n is the number of variables. See [18] for a summary of results regarding complexity of Gröbner basis computations. In particular this holds for Faugère's $F4$-algorithm [14], used for instance by `Magma` (over fields and Euclidean rings). This result can be extended easily to the case of polynomial rings over Euclidean domains, provided we have fast algorithms available for the linear algebra computations in the $F4$-algorithm, such as those implemented in `Magma`. So the Gröbner basis computations do not cause any trouble in practice, since the way regular models are computed in `Magma` ensures that the number of variables does not grow.

Indeed, the running time of the algorithm is usually dominated by the various analytic computations required for the archimedean local Néron symbols. They depend exponentially on the genus; the curve of largest genus that we have been able to compute with has genus 10, see Example 6.2 below. If the genus is not very large, but the size of the coefficients of the point $P \in A(k)$ that we want to compute the canonical height of is, then it turns out that the main bottlenecks are usually the factorizations alluded to in Section 4.2; recall that these are required in order to find out which places can lead to non-trivial non-archimedean local Néron symbols. See Example 6.3.

d	genus	$\hat{h}(P)$	act	nact
5	2	1.209108948839430454915484865 13	3.51	0.33
7	3	1.319353532098735151587742242 82	6.70	0.34
9	4	1.392372556781794225405948532 90	12.65	0.87
11	5	1.441873081167141031296676041 12	32.30	1.67
13	6	1.476796088419312452293964574 63	120.51	2.99
15	7	1.502657019791286715440057082 36	791.14	5.17
17	8	1.522540763524838385321488272 58	4729.03	8.95
19	9	1.538298826834028248666502818 888	62535.55	14.20
21	10	1.551091270847683786375492927 54	280731.59	21.35

TABLE 3. Canonical heights in a family

All computations for the following two examples were done using a 3.00 GHz Xeon processor.

Example 6.2. Consider the family

$$C_d : y^2 = x^d + 3x^2 + 1$$

for $d \in \{5, 7, 9, 11, 13, 15, 17, 19, 21\}$ and let $P = [(0, 1) - (0, -1)] \in A_d(\mathbb{Q})$, where A_d is the Jacobian of C_d. We compute $\hat{h}(P)$ and record the running time for both the archimedean and the non-archimedean computations. See Table 3, where nact and act denote non-archimedean and archimedean computation time, respectively. This example illustrates the exponential dependency on the genus.

Example 6.3. Next we consider $C : y^2 = x^{10} - x^3 + 1$ and let $P \in A(\mathbb{Q}) = [(0, 1) - \infty_+] \in \mathrm{Jac}(C)(\mathbb{Q})$, where ∞^+ is the point at infinity such that the function y/x^3 has value 1 at ∞_+. The curve C has bad reduction at 2. We use `Magma`

n	$\hat{h}(nP)$	act	nact	factt	digits
1	0.19809838973401855248161508134	2.35	0.02	0.00	1
2	0.79239355893607420992646032538	2.38	0.02	0.00	1
3	1.78288550760616697233453573211	4.06	0.13	0.00	1
4	3.16957423574429683970584130153	3.36	0.11	0.00	1
5	4.95245974335046381204037703364	2.91	0.10	0.00	1
6	7.13154203042466788933814292846	3.39	0.08	0.00	3
7	9.70682109696690907159913898594	3.40	0.06	0.00	6
8	12.67829694297718735882336520 61	3.36	0.34	0.05	9
9	16.04596956845550275101082158 90	3.31	0.29	0.01	11
10	19.80983897340185524816150813 45	3.41	0.95	0.64	16
11	23.96990515781624485027542484 28	3.33	0.37	0.08	19
12	28.52616812169867155735257171 37	3.45	0.47	0.11	21
13	33.47862786504913536939294874 74	3.32	0.34	0.09	21
14	38.82728438786763628639655594 37	3.42	196.87	196.50	30
15	44.57213769015417430836339330 28	3.37	0.53	0.20	38
16	50.71318777190874943529346082 45	3.39	0.90	0.25	42

TABLE 4. Canonical heights for multiples of a point

to compute a regular model at 2; this takes 1.97 seconds and yields 9 irreducible components.

We compute the canonical heights of positive multiples of $P \in A(\mathbb{Q})$ and record running times. The results are in Table 4 and we see that we have $\hat{h}(nP) = n^2\hat{h}(P)$ for all $n \in \{1, \ldots, 16\}$. Here nact and act have the same meaning as in Table 3, factt denotes the time spent on integer factorization and digits denotes the number of digits of the maximal height of the coefficients of the polynomials in the Mumford representation of nP.

For $n \geq 17$, the time spent on factoring increases dramatically. For instance, the factorization needed for $n = 18$ takes about 62 hours. The largest multiple for which we are able to compute $\hat{h}(nP)$ is $n = 21$, where digits $= 79$.

7. Outlook

It is now possible, using the `Magma`-implementation of the algorithm described in this work (see [30]), to compute canonical heights on Jacobians of hyperelliptic curves defined over number fields. There is work in progress on most of the applications outlined in the introduction. Some can now be tackled in a straightforward way, such as the computation of regulators up to integral squares, which can be used to gather numerical evidence for the conjecture of Birch and Swinnerton-Dyer as in [16], some require more work to be done first, such as the computation of generators of the Mordell-Weil group. An algorithm for the latter is presented in [38], but in order to apply it, one also needs a suitable naive height combining the properties that we can list all points of naive height up to some bound and that the difference between the two heights can be bounded effectively. Holmes has recently come up with a good candidate for such a naive height, the details will appear in

his upcoming PhD thesis [21] at the University of Warwick. For the genus three case, there is recent work of Stoll [40] solving this problem.

We now sketch some possible directions for further research regarding the canonical height algorithm itself. First, our algorithm works for any global field and hence it should not be too difficult to implement it for hyperelliptic curves defined over global function fields. In fact, some problems disappear because of the absence of archimedean places. More importantly, it would be interesting to extend our algorithm to the case of non-hyperelliptic curves. Here, there are essentially two problems:

(i) How can we decompose divisors into prime divisors? (see Section 4.2)
(ii) How can we implement the analytic steps 2) – 4) introduced at the end of Section 4.6?

There are 3 approaches to problem (i). If we could factor multivariate polynomials over non-archimedean local fields, then (i) would be solved, but such an algorithm has not been implemented to the author's knowledge. In favorable situations it may be possible to use ideal representations similar to the Mumford representation of hyperelliptic curves and thus decompose divisors using factorization of univariate polynomials. An ideal representation resembling Mumford representation has been proposed in [35] for smooth plane quartics. Finally, it might not be necessary to decompose divisors at all, if we could make the approach mentioned in Remark 4.12 and described in [42] work in our situation.

Of course, problem (i) disappears whenever we deal with divisors having pointwise k_v-rational support for each relevant non-archimedean local field k_v. We have used this to compute all non-archimedean local Néron symbols necessary for the computation of the regulator (up to an integral square) of the Jacobian of a non-hyperelliptic curve of genus 4 without special properties, see [29, Chapter 6]. This curve plays a major part in [39], where it is shown, assuming the first part of the conjecture of Birch and Swinnerton-Dyer, that there are no rational cycles of length 6, an important result in arithmetic dynamics. Our goal was to verify the second part of the conjecture of Birch and Swinnerton-Dyer up to an integral square for this particular curve, a challenge problem posed by Stoll in [39].

Regarding problem (ii), an extension of van Wamelen's algorithm to the non-hyperelliptic case would suffice. This does not appear to be particularly difficult, but we have not attempted it. The main obstacle is the choice of a basis of holomorphic differentials, which will probably depend on the class of curves under consideration (for hyperelliptic curves there is, of course, a canonical choice and this is used by van Wamelen's algorithm).

If we are willing to allow non-rigorous numerical integration methods, then all of the relevant algorithms have been developed (see [10, 5, 11]) by Deconinck et al. for general compact Riemann surfaces. However, these algorithms are not suitable in order to actually *prove* that we have computed the correct canonical height up to given precision.

In any case, Deconinck and his collaborators implemented their algorithms in `Maple` in a package called *algcurves*. Unfortunately, the `Maple` developers have since decided to change some of the functions that algcurves uses, in the process destroying some of the package's crucial functionality. Deconinck's group are currently working on a long-term project to rewrite all necessary routines in `Sage`.

Finally, it would be interesting to formally analyze the complexity of our algorithm. While knowing that the dependence on the genus is exponential due to the necessity of computing theta-functions, we first need to analyze the complexity of `Magma`'s desingularization algorithm and the analytic algorithms that we use before more can be said.

Remark 7.1. Let A be the Jacobian of a smooth projective curve C defined over a number field and let p be a prime such that A has good ordinary reduction at all $v \mid p$. Coleman and Gross [9] have constructed a pairing taking values in $\mathbb{Q}_p$ between divisors D, E on C of degree 0 which can be decomposed into a sum of local height pairings $h_v(D, E)$ over all non-archimedean $v \in M_k$.

They show that this pairing respects linear equivalence and coincides with the p-adic height pairings on A constructed by Schneider [36] and Mazur-Tate [28].

If $v \mid p$, then $h_v(D, E)$ can be expressed in terms of Coleman integration. An algorithm for the computation of $h_v(D, E)$ was introduced by Balakrishnan and Besser in [4], see also [3, Chapter 8]. Computing the local height pairings at $v \nmid p$ is equivalent to computing the local Néron symbol at v (cf. [9, §2]). Hence we can combine the results presented in this work with the method of Balakrishnan and Besser, leading to the first algorithm to compute p-adic heights for $g \geq 2$.

One can define p-adic regulators similar to the classical case (see Section 6). Together with Balakrishnan we have computed the p-adic regulator for all but one of the modular abelian surfaces considered in [16] for all good ordinary $p < 100$. This gives rise to an extension of the p-adic Birch and Swinnerton-Dyer conjecture for elliptic curves due to Mazur, Tate and Teitelbaum to the case of modular abelian surfaces (cf. [3, Conjecture 9.1.4]).

References

1. W.W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, American Mathematical Society, Providence, (1994).
2. M. Artin, *Lipman's proof of resolution of singularities for surfaces*, in G. Cornell and J.H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York–Heidelberg–Berlin (1986).
3. J. Balakrishnan, *Coleman Integration for Hyperelliptic Curves: Algorithms and Applications*, PhD thesis, MIT (2011).
4. J. Balakrishnan and A. Besser, *Local heights on hyperelliptic curves*, Int. Math. Res. Notices. (2011), doi: 10.1093/imrn/rnr111.
5. A. Bobenko, B. Deconinck, M. Heil, M. Schmies and M. van Hoeij, *Computing Riemann Theta Functions*, Math. Comp. **73**, 1417–1442 (2004).
6. D. Cantor, *Computing in the Jacobian of a Hyperelliptic Curve*, Math. Comp. **48** (177), 95–101 (1987).
7. V. Cossart, U. Jannsen and S. Saito, *Canonical embedded and non-embedded resolution of singularities for excellent two-dimensional schemes*, Preprint (2009). arXiv:math/0905.2191v1 [math.AG]
8. D. A. Cox and S. Zucker, *Intersection numbers of sections of elliptic surfaces*, Invent. Math. **53**, 1–44 (1969).
9. R. F. Coleman and B. H. Gross, *p-adic heights on curves*, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathe- matics **17**, 73–81 (1989).
10. B. Deconinck and M. van Hoeij, *Computing Riemann matrices of algebraic curves*, Physica D **152–153**, 28-46 (2001).
11. B. Deconinck and M. Patterson, *Computing the Abel map*, Physica D **237**, 3214–3232 (2008).
12. D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, New York (1995).
13. G. Faltings, *Calculus on arithmetic surfaces*, Ann. of Math. (2) **119**, 387–424 (1984).

14. J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, J. Pure Appl. Algebra **139** (1), 61–88 (1999).
15. E.V. Flynn, N.P. Smart, *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith. **79**, 333–352 (1997).
16. E.V. Flynn, F. Leprévost, E.F. Schaefer, W.A. Stein, M. Stoll and J.L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70**, 1675–1697 (2001).
17. B. Gross, *Local heights on curves*, in G. Cornell and J.H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York–Heidelberg–Berlin, (1986).
18. A. Hashemi and D. Lazard, *Almost polynomial complexity for zero-dimensional Gröbner bases*, in Proceedings of the 7th Asian Symposium on Computer Mathematics (ASCM'2005), Seoul, Korea, 16–21 (2005).
19. F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comp. **33(4)**, 425–445 (2002).
20. D. Holmes, *Computing Néron-Tate heights of points on hyperelliptic Jacobians*, J. Number Theory (2012), doi:10.1016/j.jnt.2012.01.002
21. D. Holmes, *Néron-Tate heights on the Jacobians of high-genus hyperelliptic curves*, PhD thesis, University of Warwick, to appear.
22. P. Hriljac, *Heights and Arakelov's intersection theory*, Amer. J. Math. **107**, 23–38 (1985).
23. S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York (1983).
24. S. Lang, *Introduction to Arakelov theory*, Springer-Verlag, New York (1988).
25. Q. Liu, *Algebraic Geometry and arithmetic curves*, Oxford University Press, Oxford (2002).
26. MAGMA is described in W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp., 24, 235–265 (1997). (See also the Magma home page at `http://magma.maths.usyd.edu.au/magma/`.)
27. H. Matsumura, *Commutative algebra*, W.A. Benjamin, New York (1970).
28. B. Mazur and J. Tate, *Canonical height pairings via biextensions*, in Arithmetic and geometry, Vol. I, Progr. Math., **35**, 195–237, Birkhäuser, Boston (1983).
29. J.S. Müller, *Computing canonical heights on Jacobians*, PhD thesis, Universität Bayreuth (2010).
30. `http://www.math.uni-hamburg.de/home/js.mueller/#code`
31. A. Néron, *Quasi-fonctions et hauteurs sur les variétes abéliennes*, Ann. of Math. **82**, 249–331 (1965).
32. S. Pauli, *Factoring polynomials over local fields*, J. Symbolic Comput. **32**, 533–547 (2001).
33. F. Pazuki, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes: sur la conjecture de Lang et Silverman*, PhD thesis, Université Bordeaux 1 (2008).
34. B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488**, 141–188 (1997).
35. J. Romero-Valencia and A.G. Zamora, *Explicit constructions for genus 3 Jacobians*, Preprint (2009). arXiv:math/0904.4537v1 [math.AG]
36. P. Schneider, *p-adic height pairings I*, Invent. Math. **69**, 401–409 (1982).
37. J.H. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51**, 339–358 (1988).
38. M. Stoll, *On the height constant for curves of genus two, II*, Acta Arith. **104**, 165–182 (2002).
39. M. Stoll, *Rational 6-cycles under iteration of quadratic polynomials*, LMS J. Comput. Math **11**, 367–380 (2008).
40. M. Stoll, *Explicit Kummer varieties for hyperelliptic curves of genus three*, to appear. See also `http://www.mathe2.uni-bayreuth.de/stoll/talks/Luminy2012.pdf`.
41. `http://www.math.lsu.edu/~wamelen/genus2.html`
42. M. Wagner, Über Korrespondenzen zwischen algebraischen Funktionenkörpern, PhD thesis, TU Berlin (2009).

Fachbereich Mathematik, Universität Hamburg
E-mail address: `jan.steffen.mueller@uni-hamburg.de`