ACTA ARITHMETICA
149.2 (2011)

# Canonical local heights and multiplication formulas for the Jacobians of curves of genus 2

by

Yukihiro Uchida (Kyoto)

**1. Introduction.** In the study of the arithmetic of Abelian varieties, the theory of height functions is very important. For an Abelian variety defined over a global field and a divisor on it, we can choose a good height function which is called the canonical height function. The canonical height function can be decomposed into canonical local height functions, which are functions defined for each absolute value. Néron [12] obtained theoretical results and Tate made these results more explicit for elliptic curves (cf. [9, 20]).

The canonical height function on Jacobians of curves of genus 2 was studied by Flynn and Smart [5], Yoshitomi [19], and Stoll [14, 15]. They studied the canonical height by decomposing it into a sum of canonical local heights. Note that Flynn, Smart, and Stoll treated the case where $Y^2 =$ (sextic) by the method of Cassels and Flynn [2], and that Yoshitomi treated the case where $Y^2 =$ (quintic) by using complex analysis and intersection theory.

In this paper, we study canonical local height functions on Jacobians of curves of genus 2. Although other authors have already treated canonical local height functions, our treatment is more systematic. This systematic treatment enables us to prove some relations for canonical local height functions. We treat the case where $Y^2 =$ (sextic) by the method of Cassels and Flynn [2]; however, almost all the results in this paper hold with a slight modification for the case where $Y^2 =$ (quintic).

To study canonical local height functions on Jacobians of curves of genus 2, we need the multiplication formulas. Kanayama [8] gave the multiplication formulas for the case where $Y^2 =$ (quintic). However, in the case where $Y^2 =$ (sextic), the multiplication formulas are not known. Since the height functions under consideration are defined through the Kummer sur-

2010 *Mathematics Subject Classification*: Primary 11G50; Secondary 11G20, 11G30, 14H40.
*Key words and phrases*: height functions, Jacobian varieties, curves of genus 2.

DOI: 10.4064/aa149-2-2  

face, it is sufficient to construct the multiplication formulas for the Kummer surface. In this paper, we find them, and then we derive some relations between the canonical local height functions.

As applications, we give bounds for the difference between the naive height and the canonical height and an algorithm to compute the canonical height. These height bounds are generalizations of the author's result for elliptic curves [16, 17].

This paper is organized as follows: In Section 2, we review the arithmetic of curves of genus 2 according to [2]. In Section 3, we give the multiplication formulas for the Kummer surfaces associated with curves of genus 2. In Section 4, we recall the concepts and facts needed when we construct the canonical local height functions. In Section 5, we define the canonical local height functions and prove several of their properties. In Section 6, we give bounds for the difference between the naive height function and the canonical height function. Then we discuss algorithms to compute these bounds. In Section 7, we describe a refinement of an algorithm to compute the canonical height.

The proof of Lemma 3.1, which is a proof of irreducibility, requires the use of a computer algebra system. The author used Risa/Asir [13].

**2. Preliminaries for curves of genus 2.** In this section, we review the basis for the arithmetic of curves of genus 2 according to [2].

Let $k$ be a field with $\mathrm{char}(k) \neq 2$. We denote by $\bar{k}$ the algebraic closure of $k$. We consider a non-singular projective curve of genus 2 over $k$,

$$C\colon Y^2 = f(X),$$

where

$$f(X) = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0 \in k[X]$$

is of degree 5 or 6 and has no multiple roots. When $f(X)$ is of degree 6, we denote the two points at infinity of $C$ by $\infty^+$ and $\infty^-$. When $f(X)$ is of degree 5, both $\infty^+$ and $\infty^-$ stand for the unique point at infinity, and then we also denote it by $\infty$. The points $\infty^+$ and $\infty^-$ are defined over $k$ or a quadratic extension of $k$.

Let $J$ be the Jacobian of $C$. A point on $J$ can be written as a divisor class of the form $(P_1)+(P_2)-(\infty^+)-(\infty^-)$, where $P_1, P_2 \in C$. Let $\Theta^+$, $\Theta^-$ be the images of $C$ in $J$ via the embeddings

$$P \mapsto (P) - (\infty^+), \qquad P \mapsto (P) - (\infty^-)$$

respectively. Note that $\Theta^+$ and $\Theta^-$ may not be defined over $k$. However, $\Theta^+ + \Theta^-$ is defined over $k$. Furthermore, $\Theta^+ + \Theta^-$ is linearly equivalent to $2\Theta$, where $\Theta$ is a suitable theta divisor on $J$. By [11, Section 6, Application 1],

$\Theta^+ + \Theta^-$ is base-point free and ample. Since $l(\Theta^+ + \Theta^-) = l(2\Theta) = 4$, there exists a morphism from $J$ to $\mathbb{P}^3$ associated with $\Theta^+ + \Theta^-$.

Following [2], we choose a morphism $\kappa\colon J \to \mathbb{P}^3$ associated with $\Theta^+ + \Theta^-$ as follows: Let $P$ be a point on $J$ corresponding to a divisor $(P_1) + (P_2) - (\infty^+) - (\infty^-)$, where $P_i = (x_i, y_i) \in C$ for $i = 1, 2$. If $P_1, P_2 \neq \infty^+, \infty^-$ and $x_1 \neq x_2$, then we define

$$\kappa(P) = (\xi_1(P), \dots, \xi_4(P)),$$

where

$$\xi_1(P) = 1, \quad \xi_2(P) = x_1 + x_2, \quad \xi_3(P) = x_1 x_2,$$

$$\xi_4(P) = \frac{F_0(x_1, x_2) - 2y_1 y_2}{(x_1 - x_2)^2},$$

$$F_0(x_1, x_2) = 2f_0 + f_1(x_1 + x_2) + 2f_2 x_1 x_2 + f_3 x_1 x_2 (x_1 + x_2) + 2f_4 (x_1 x_2)^2 + f_5 (x_1 x_2)^2 (x_1 + x_2) + 2f_6 (x_1 x_2)^3.$$

If $P$ does not satisfy the above condition, we define $\kappa(P)$ by changing coordinates and taking limits. For example, when we denote by $O$ the identity element of $J$, we have $\kappa(O) = (0, 0, 0, 1)$. We call the image of $\kappa$ the *Kummer surface*, and denote it by $K$.

The defining equation of $K$ is $G(\xi_1, \dots, \xi_4) = 0$, where $G$ is a homogeneous polynomial in $\xi_1, \dots, \xi_4$ of degree 4 with coefficients in $\mathbb{Z}[f_0, \dots, f_6]$. An explicit formula for $G$ is given in [2].

Let $\iota\colon J \to J$ be the involution defined by $\iota(P) = -P$. Then $\kappa \circ \iota = \kappa$, and the quotient variety $J/\langle\iota\rangle$ is isomorphic to $K$ through the morphism induced by $\kappa$. We identify $J/\langle\iota\rangle$ with $K$ by this isomorphism.

We denote the multiplication-by-$m$ map on $J$ by $[m]$. Since $[m](-P) = -([m]P)$, $[m]$ induces a morphism on $K$. We denote by $\delta$ the morphism on $K$ induced by the duplication map, that is, $\kappa([2]P) = \delta(\kappa(P))$. Explicit formulas for $\delta$ are given in [3] and available at [4]. According to these formulas, $\delta = (\delta_1, \dots, \delta_4)$, where $\delta_i$ are homogeneous polynomials in $\xi_1, \dots, \xi_4$ of degree 4 with coefficients in $\mathbb{Z}[f_0, \dots, f_6]$. It is the aim of Section 3 to obtain similar formulas for general multiplication maps.

We cannot recover $\kappa(P+Q)$ from only $\kappa(P)$ and $\kappa(Q)$ because $P$ and $-P$ are identified through $\kappa$. However, we can obtain an unordered pair $(\kappa(P+Q), \kappa(P-Q))$ from $\kappa(P)$ and $\kappa(Q)$.

PROPOSITION 2.1 ([2, Theorem 3.4.1]). *There exist polynomials $B_{ij}$ biquadratic in the two sets of homogeneous variables $(\xi_1(P), \dots, \xi_4(P))$ and $(\xi_1(Q), \dots, \xi_4(Q))$ with coefficients in $\mathbb{Z}[f_0, \dots, f_6]$ such that, for any $P, Q \in J(\bar{k})$, there exists $c \in \bar{k}^\times$ such that*

$$\xi_i(P+Q)\xi_j(P-Q) + \xi_j(P+Q)\xi_i(P-Q) = c \cdot 2B_{ij}(\kappa(P), \kappa(Q)) \tag{2.1}$$

*for all $i, j = 1, 2, 3, 4$.*

Explicit formulas for $B_{ij}$ are also available at [4]. We will use $\delta_i$ and $B_{ij}$ as defined at [4] throughout this paper.

**3. Multiplication formulas.** In this section, we construct the multiplication formulas for the Kummer surfaces associated with curves of genus 2.

For a while, we will assume that $k = \mathbb{Q}(f_0, \dots, f_6)$ and that $f_0, \dots, f_6$ are algebraically independent over $\mathbb{Q}$. We begin with some technical lemmas.

LEMMA 3.1. *Let $G_i$ be the polynomial obtained by substituting 0 for $\xi_i$ in $G$. Then $G_i$ is irreducible in $\mathbb{Z}[f_0, \dots, f_6][\xi_1, \dots, \xi_{i-1}, \xi_{i+1}, \dots, \xi_4]$.*

*Proof.* We can verify the lemma by using a computer algebra system. The author used Risa/Asir [13]. ∎

LEMMA 3.2. *Let $I = \langle G, \xi_i \rangle$ be the ideal in $k[\xi_1, \dots, \xi_4]$ generated by $G$ and $\xi_i$. Then $I$ is a prime ideal. In particular, $I$ is a radical ideal, that is, $\sqrt{I} = I$.*

*Proof.* Let $R = k[\xi_1, \dots, \xi_4]$ and $R' = k[\xi_1, \dots, \xi_{i-1}, \xi_{i+1}, \dots, \xi_4]$. We define a ring homomorphism $\varphi\colon R \to R'$ by

$$\varphi(g(\xi_1, \dots, \xi_4)) = g(\xi_1, \dots, \xi_{i-1}, 0, \xi_{i+1}, \dots, \xi_4).$$

Take $G_i$ as in Lemma 3.1. Note that $G_i = \varphi(G)$.

Let $I'$ be the ideal generated by $G_i$ in $R'$. Then $I = \varphi^{-1}(I')$. By Lemma 3.1, $I'$ is a prime ideal, and so is $I$. ∎

The following theorem gives the multiplication formulas.

THEOREM 3.3. *There exist homogeneous polynomials $\mu_{m,i} \in k[\xi_1, \dots, \xi_4]$ for any $m \geq 0$ and $i = 1, 2, 3, 4$ such that the following conditions are satisfied:*

(i) *We have*

$$\mu_{0,1} = \mu_{0,2} = \mu_{0,3} = 0, \qquad \mu_{0,4} = 1,$$

$$\mu_{1,i} = \xi_i,$$

$$\mu_{2m,i} = \delta_i(\mu_m) \quad (m \geq 1), \tag{3.1}$$

$$\mu_{2m+1,i}\xi_i = B_{ii}(\mu_{m+1}, \mu_m) \quad (m \geq 1) \tag{3.2}$$

*in $k[\xi_1, \dots, \xi_4]/\langle G \rangle$, where $\mu_m = (\mu_{m,1}, \dots, \mu_{m,4})$.*

(ii) *For all $P \in J(\bar{k})$, we have*

$$\kappa([m]P) = (\mu_{m,1}(\kappa(P)), \dots, \mu_{m,4}(\kappa(P))). \tag{3.3}$$

*Proof.* We prove the theorem by induction on $m$. It is clear when $m = 0, 1$.

We assume that we have $\mu_{m,i}$ for $m \leq n$. When $n+1$ is even, we define $\mu_{n+1,i}$ by (3.1). Then we obtain (3.3) for $m = n+1$.

Assume that $n+1$ is odd. We put $n+1 = 2l+1$. By Proposition 2.1, for all $P \in J(\bar{k})$, there exists $c \in \bar{k}^{\times}$ such that

$$\xi_i([2l+1]P)\xi_i(P) = cB_{ii}(\kappa([l+1]P), \kappa([l]P))$$

for all $i = 1, 2, 3, 4$. We define $g \in k[\xi_1, \ldots, \xi_4]$ by

$$g = B_{ii}(\mu_{l+1}, \mu_l).$$

Then $g(Q) = 0$ for all $Q \in K(\bar{k})$ with $\xi_i(Q) = 0$. Hence we have $g \in \sqrt{\langle G, \xi_i \rangle_{\bar{k}}}$ by Hilbert's Nullstellensatz, where $\langle G, \xi_i \rangle_{\bar{k}}$ is the ideal in $\bar{k}[\xi_1, \ldots, \xi_4]$ generated by $G$ and $\xi_i$. Since $g \in k[\xi_1, \ldots, \xi_4]$, we see that

$$g \in \sqrt{\langle G, \xi_i \rangle_{\bar{k}}} \cap k[\xi_1, \ldots, \xi_4] = \sqrt{\langle G, \xi_i \rangle_k},$$

where $\langle G, \xi_i \rangle_k$ is the ideal in $k[\xi_1, \ldots, \xi_4]$ generated by $G$ and $\xi_i$. We have $\sqrt{\langle G, \xi_i \rangle_k} = \langle G, \xi_i \rangle_k$ by Lemma 3.2. Hence we can write

$$g = g_1\xi_i + g_2 G, \tag{3.4}$$

where $g_1, g_2 \in k[\xi_1, \ldots, \xi_4]$. Put $\mu_{n+1,i} = g_1$. Then we obtain (3.3) for $m = n+1$. ∎

REMARK 3.4. The polynomials $\mu_{m,i}$ are uniquely determined modulo $G$.

REMARK 3.5. We can compute $\mu_{2m+1,i}$ by using Gröbner bases (see [1, §5.6]). We can also compute them using the following elementary operations. In (3.4), we can assume that $g_2$ does not contain the variable $\xi_i$. We substitute 0 for $\xi_i$ in (3.4). Let $h$ be the polynomial obtained by substituting 0 for $\xi_i$ in $g$. Then $h = g_2 G_i$, where $G_i$ is taken as in Lemma 3.1. Hence we can calculate $g_2 = h/G_i$ and $g_1 = (g - g_2 G)/\xi_i$.

In Theorem 3.3, the coefficients of $\mu_{m,i}$ are in $k = \mathbb{Q}(f_0, \ldots, f_6)$. In fact, we have the following:

PROPOSITION 3.6. *For all $m \geq 0$ and $i = 1, 2, 3, 4$, we can choose $\mu_{m,i}$ with coefficients in $\mathbb{Z}[f_0, \ldots, f_6]$.*

*Proof.* We prove the conclusion by induction on $m$. It is clear when $m = 0, 1$.

Assume that the conclusion is true if $m < n$. If $n$ is even, the conclusion is clear since $\delta_i$ and $\mu_{n/2,i}$ have coefficients in $\mathbb{Z}[f_0, \ldots, f_6]$.

If $n$ is odd, we have

$$\mu_{2l+1,i}\xi_i = B_{ii}(\mu_{l+1}, \mu_l) + g_2 G \tag{3.5}$$

in $k[\xi_1, \ldots, \xi_4]$, where $n = 2l+1$ and $g_2 \in k[\xi_1, \ldots, \xi_4]$. We can assume that $g_2$ does not contain the variable $\xi_i$ by replacing $\mu_{2l+1,i}$ if necessary. Substitute 0 for $\xi_i$. Then

$$g_2 G_i = H,$$

where $H$ is a polynomial obtained by substituting 0 for $\xi_i$ in $-B_{ii}(\mu_{l+1}, \mu_l)$. Then $H$ has coefficients in $\mathbb{Z}[f_0, \dots, f_6]$ since $B_{ii}$, $\mu_{l+1,j}$, and $\mu_{l,j}$ have the same property. $G_i$ is irreducible in $\mathbb{Z}[f_0, \dots, f_6][\xi_1, \dots, \xi_{i-1}, \xi_{i+1}, \dots, \xi_4]$ by Lemma 3.1. Therefore $g_2$ has coefficients in $\mathbb{Z}[f_0, \dots, f_6]$. Hence the right-hand side of (3.5) has coefficients in $\mathbb{Z}[f_0, \dots, f_6]$, and so does $\mu_{2l+1,i}$. ∎

By Proposition 3.6, we can remove the assumption that $k = \mathbb{Q}(f_0, \dots, f_6)$ and that $f_0, \dots, f_6$ are algebraically independent over $\mathbb{Q}$.

COROLLARY 3.7. *The statement of Theorem* 3.3 *holds for any field* $k$ *with* $\mathrm{char}(k) \neq 2$.

*Proof.* The relations among the polynomials $\mu_{m,i}$ in Theorem 3.3(i) hold for $\mathbb{Z}[f_0, \dots, f_6][\xi_1, \dots, \xi_4]$. Since there is a ring homomorphism $\mathbb{Z}[f_0, \dots, f_6] \to k$, there exist $\mu_{m,i} \in k[\xi_1, \dots, \xi_4]$ such that condition (i) is satisfied. Condition (ii) follows from (i) and Proposition 2.1. ∎

We describe some properties of $\mu_{m,i}$.

LEMMA 3.8. *For all* $m \geq 0$ *and* $i = 1, 2, 3, 4$, $\mu_{m,i}$ *has degree* $m^2$.

*Proof.* Since $\delta_i$ are homogeneous polynomials of degree 4 and $B_{ii}$ are biquadratic forms, the lemma follows by induction on $m$. ∎

LEMMA 3.9. *Let* $O = (0, 0, 0, 1)$. *Then*

$$\mu_{m,1}(O) = \mu_{m,2}(O) = \mu_{m,3}(O) = 0, \qquad \mu_{m,4}(O) = 1 \quad \text{for all } m \geq 0.$$

*Proof.* It is enough to show that $\mu_{m,4}(O) = 1$. First note that we can verify that $\delta_4(O) = 1$ and $B_{44}(O, O) = 1$ by direct computation. We prove the conclusion by induction on $m$. It is clear when $m = 0, 1$. We assume that the conclusion is true for $m < n$. When $n$ is even, put $n = 2l$. Then

$$\mu_{n,4}(O) = \delta_4(\mu_l(O)) = \delta_4(O) = 1.$$

When $n$ is odd, put $n = 2l + 1$. Then

$$\mu_{n,4}(O)\mu_{1,4}(O) = B_{44}(\mu_{l+1}(O), \mu_l(O)) = B_{44}(O, O) = 1.$$

Since $\mu_{1,4}(O) = 1$, we have $\mu_{n,4}(O) = 1$. ∎

PROPOSITION 3.10. *We have*

$$\mu_{m+n,i}\mu_{m-n,j} + \mu_{m+n,j}\mu_{m-n,i} = 2B_{ij}(\mu_m, \mu_n) \tag{3.6}$$

*in* $k[\xi_1, \dots, \xi_4]/\langle G \rangle$ *for all* $m, n \geq 0$ *such that* $m \geq n$ *and for all* $i, j = 1, 2, 3, 4$.

*Proof.* By Proposition 2.1, for all $P \in K(\bar{k})$, there exists $c(P) \in \bar{k}^\times$ such that

$$(\mu_{m+n,i}\mu_{m-n,j} + \mu_{m+n,j}\mu_{m-n,i})(P) = c(P) \cdot 2B_{ij}(\mu_m, \mu_n)(P)$$

for all $i, j = 1, 2, 3, 4$. Since both sides of (3.6) have the same degree by Lemma 3.8, $c$ is a regular function on $K$. However, since $K$ is projective, $c$ must be a constant. Comparing values at $O$, we obtain $c = 1$. ∎

**4. Preliminaries from height theory.** In this section, we state some definitions and propositions needed for the next section. For simplicity, we treat only the case of number fields. However, the results in this and the next sections are valid for more general fields with absolute values. For details on this section, see [7] or [10].

Let $k$ be a number field. We denote by $M_k$ the set of all absolute values on $k$ whose restriction to $\mathbb{Q}$ is one of the standard absolute values on $\mathbb{Q}$.

A function $\gamma\colon M_k \to \mathbb{R}$ is said to be an *$M_k$-constant* if $\gamma(v) = 0$ for all but a finite number of $v$ in $M_k$. We may regard $\gamma$ as a family of constants $\{\gamma_v\}$.

Let $V$ be a variety over $k$. We consider a function on the disjoint union

$$\alpha\colon \coprod_{v\in M_k} V(k_v) \to \mathbb{R}.$$

We denote by $\alpha_v$ the restriction of $\alpha$ to $V(k_v)$. Then we may regard $\alpha$ as a family of functions $\{\alpha_v\}$. We say that $\alpha$ is *$M_k$-bounded* if there exist $M_k$-constants $\gamma$, $\gamma'$ such that

$$\gamma(v) \le \alpha_v(P) \le \gamma'(v)$$

for all $v \in M_k$ and $P \in V(k_v)$.

A subset $Y \subset \coprod_{v\in M_k} V(k_v)$ is said to be *affine $M_k$-bounded* if there exists an affine open subset $V_0$ with affine coordinates $x_1, \dots, x_n$ such that $Y \subset \coprod_{v\in M_k} V_0(k_v)$ and the function

$$\coprod_{v\in M_k} V_0(k_v) \to \mathbb{R}, \quad P \mapsto \max_{1\le i\le n} |x_i(P)|_v$$

is $M_k$-bounded on $Y$. A subset $Y \subset \coprod_{v\in M_k} V(k_v)$ is said to be *$M_k$-bounded* if $Y$ is contained in the finite union of affine $M_k$-bounded subsets.

Let $\alpha\colon \coprod_{v\in M_k} V(k_v) \to \mathbb{R}$ be a function. We say that $\alpha$ is *locally $M_k$-bounded* if $\alpha$ is $M_k$-bounded on any $M_k$-bounded subset. We say that $\alpha$ is *continuous* if $\alpha_v$ is continuous with respect to the $v$-adic topology for all $v \in M_k$.

We use the following proposition later.

PROPOSITION 4.1. *Let $\phi\colon \mathbb{P}^n \to \mathbb{P}^m$ be a rational map given by an $(m+1)$-tuple $\phi = (f_0, \dots, f_m)$ of homogeneous polynomials of degree $d$ over $k$. Let $X$ be a closed subvariety of $\mathbb{P}^n$ such that $\phi$ is defined on $X$. Then there exist $M_k$-constants $C$ and $C'$ such that*

$$C_v \le \log \max_{0\le i\le m} |f_i(P)|_v - d \log \max_{0\le i\le n} |x_i|_v \le C'_v$$

*for all* $v \in M_k$ *and all* $P = (x_0, \dots, x_n) \in X(k_v)$.

Proposition 4.1 is a local version of [7, Theorem B.2.5]. The proof is essentially the same as that in [7].

Let $D$ be a divisor on $V$. We write $V_D = V \setminus \operatorname{supp}(D)$. A function $\lambda_D \colon \coprod_{v\in M_k} V_D(k_v) \to \mathbb{R}$ is called a *local height function* (or *Weil function*) on $V$ associated with $D$ if the following property holds: For any Zariski open subset $U$ of $A$ such that $U \cap \operatorname{supp}(D) \ne \emptyset$ and $D|_U = \operatorname{div}(f)$ for some rational function $f$ on $U$, there exists a locally $M_k$-bounded continuous function $\alpha \colon \coprod_{v\in M_k} U(k_v) \to \mathbb{R}$ such that

$$\lambda_{D,v}(P) = -\log |f(P)|_v + \alpha_v(P)$$

for all $v \in M_k$ and $P \in U_D(k_v)$.

THEOREM 4.2. *Let $A$ be an Abelian variety defined over $k$. For any divisor $D$ on $A$, there exists a local height function $\hat\lambda_D$ on $A$ associated with $D$ such that the following properties hold, where $\gamma_1, \gamma_2, \gamma_3$ denote $M_k$-constants:*

(i) *Let $D$ and $D'$ be divisors on $V$. Then $\hat\lambda_{D+D'} = \hat\lambda_D + \hat\lambda_{D'} + \gamma_1$.*
(ii) *If $D = \operatorname{div}(f)$, then $\hat\lambda_{D,v}(P) = -\log |f(P)|_v + \gamma_2(v)$ for all $v \in M_k$ and $P \in A_D(k_v)$.*
(iii) *For all $v \in M_{\bar k}$ and $P \in A_{[2]^*D}(k_v)$,*

$$\hat\lambda_{[2]^*D,v}(P) = \hat\lambda_{D,v}([2]P) + \gamma_3(v).$$

*Furthermore $\hat\lambda_D$ is determined by $D$ up to an $M_k$-constant.*

*Such functions $\hat\lambda_D$ also have the property that if $\varphi \colon B \to A$ is a homomorphism of Abelian varieties defined over $k$, then*

$$\hat\lambda_{\varphi^*(D),v}(P) = \hat\lambda_{D,v}(\varphi(P)) + \gamma_4(v)$$

*for all $v \in M_k$ and $P \in B_{\varphi^*(D)}(k_v)$, where $\gamma_4$ is an $M_k$-constant.*

*Proof.* See [10, Chapter 11, Theorem 1.1]. ∎

We call $\hat\lambda_D$ in Theorem 4.2 a *canonical local height function* (or *Néron function*) on $A$ associated with $D$.

**5. Canonical local heights.** In this section, we describe the canonical local height functions on the Jacobians of curves of genus 2. For the rest of this paper, we assume that the curve $C$ is defined over a number field $k$.

We define the divisors $\Theta_i$ on $J$ by

$$\Theta_1 = \Theta^+ + \Theta^-, \quad \Theta_i = \Theta_1 + \operatorname{div}\left(\frac{\xi_i}{\xi_1}\right) \quad (i = 2, 3, 4).$$

Note that $P \in \operatorname{supp}(\Theta_i)$ if and only if $\xi_i(P) = 0$.

For $1 \le i \le 4$ and $v \in M_k$, we define the *naive local height function* $\lambda_{i,v}\colon J_{\Theta_i}(k_v) \to \mathbb{R}$ by

$$\lambda_{i,v}(P) = \log \max_{1\le j\le 4} \left|\frac{\xi_j(P)}{\xi_i(P)}\right|_v.$$

It is independent of the choice of homogeneous coordinates for $\kappa(P)$. Furthermore, $\lambda_{i,v}$ is a local height function associated with $\Theta_i$. We have

$$\lambda_{i,v}(P) = \lambda_{j,v}(P) - \log \left|\frac{\xi_i(P)}{\xi_j(P)}\right|_v \quad \text{for any } P \notin \operatorname{supp}(\Theta_i) \cup \operatorname{supp}(\Theta_j).$$

To construct the canonical local height functions, we define the function $\Phi_v\colon J(k_v) \to \mathbb{R}$ by

$$\Phi_v(P) = \frac{\max_i |\delta_i(\kappa(P))|_v}{\max_i |\xi_i(P)|_v^4}.$$

The right-hand side is independent of the choice of homogeneous coordinates for $\kappa(P)$ since $\delta_i$ are homogeneous polynomials of degree 4.

LEMMA 5.1. *$\log \Phi_v$ is an $M_k$-bounded continuous function.*

*Proof.* It is clear that $\log \Phi_v$ is continuous. To prove boundedness, apply Proposition 4.1 to $\delta\colon K \to K$. ∎

By Lemma 5.1, we can define the function $\hat\lambda_{i,v}\colon J_{\Theta_i}(k_v) \to \mathbb{R}$ by

$$\hat\lambda_{i,v}(P) = \lambda_{i,v}(P) + \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P).$$

We call it the *canonical local height function* on $J$ associated with $\Theta_i$. By definition, we have

$$\hat\lambda_{i,v}(P) = \hat\lambda_{j,v}(P) - \log \left|\frac{\xi_i(P)}{\xi_j(P)}\right|_v \tag{5.1}$$

for any $P \notin \operatorname{supp}(\Theta_i) \cup \operatorname{supp}(\Theta_j)$.

REMARK 5.2. Flynn and Smart [5] also defined the canonical local height functions on $J$. They defined only one function for one absolute value. If we denote by $\hat\lambda'_v$ the canonical local height function for $v \in M_k$ as defined by them, then we have

$$\hat\lambda'_v(P) = \hat\lambda_{i,v}(P),$$

where $i$ is the smallest index such that $\xi_i(P) \ne 0$.

We have the following theorem:

THEOREM 5.3. *For each $i$ with $1 \le i \le 4$, $\hat\lambda_{i,v}\colon J_{\Theta_i}(k_v) \to \mathbb{R}$ has the following properties:*

(i) *$\hat\lambda_{i,v} - \lambda_{i,v}$ can be extended to an $M_k$-bounded continuous function on $J(k_v)$.*

(ii) *For any positive integer $m$ and all $P \in J(k_v)$ with $P, [m]P \notin \operatorname{supp}(\Theta_i)$, we have*

$$\hat{\lambda}_{i,v}([m]P) = m^2 \hat{\lambda}_{i,v}(P) - \log \left| \frac{\mu_{m,i}(\kappa(P))}{\xi_i(P)^{m^2}} \right|_v .$$

*Furthermore, $\hat{\lambda}_{i,v}$ is the unique function satisfying* (i) *and* (ii) *for any fixed integer $m \geq 2$. In particular, $\hat{\lambda}_{i,v}$ is a canonical local height function associated with $\Theta_i$ in the sense of Section* 4.

*Proof.* The proof of uniqueness is the same as that in [17, Proposition 9]. By Lemma 5.1, $\hat{\lambda}_{i,v}$ satisfies (i). For $m = 2$, (ii) is satisfied by definition. In particular, $\hat{\lambda}_{i,v}$ is a canonical local height function associated with $\Theta_i$ in the sense of Section 4. We prove (ii) for general $m$.

It is easy to see that

$$\operatorname{div}\left( \frac{\mu_{m,i}(\kappa(P))}{\xi_i(P)^{m^2}} \right) = [m]^* \Theta_i - m^2 \Theta_i .$$

Therefore, by Theorem 4.2, there exists an $M_k$-constant $\gamma$ such that

$$\hat{\lambda}_{i,v}([m]P) = m^2 \hat{\lambda}_{i,v}(P) - \log \left| \frac{\mu_{m,i}(\kappa(P))}{\xi_i(P)^{m^2}} \right|_v + \gamma(v) \tag{5.2}$$

for all $v \in M_k$ and $P \in J(k_v)$ with $P, [m]P \notin \operatorname{supp}(\Theta_i)$. By the definition of $\hat{\lambda}_{i,v}$, we have

$$\begin{aligned} \gamma(v) = {} & \log \max_{1 \leq j \leq 4} |\mu_{m,j}(\kappa(P))|_v - m^2 \log \max_{1 \leq j \leq 4} |\xi_j(P)|_v \\ & + \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n m]P) - m^2 \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P) \end{aligned} \tag{5.3}$$

for all $P \in J(k_v)$ with $P, [m]P \notin \operatorname{supp}(\Theta_i)$. Since both sides are well-defined and continuous on $J(k_v)$, (5.3) holds for all $P \in J(k_v)$. If $P$ is the identity element of $J$, then $\kappa(P) = (0, 0, 0, 1)$. Therefore, by Lemma 3.9, we have $\gamma(v) = 0$. ∎

Corollary 5.4. *Let $P \in J(k_v)$ and $m > 0$ be an integer. If $P \notin \operatorname{supp}(\Theta_i)$ and $[m]P \notin \operatorname{supp}(\Theta_j)$, then*

$$\hat{\lambda}_{j,v}([m]P) = m^2 \hat{\lambda}_{i,v}(P) - \log \left| \frac{\mu_{m,j}(\kappa(P))}{\xi_i(P)^{m^2}} \right|_v . \tag{5.4}$$

*Proof.* This follows from Theorem 5.3 and (5.1). ∎

Corollary 5.5. *Let $m \geq 2$ be an integer. Define the function $\Phi_{m,v} \colon J(k_v) \to \mathbb{R}$ by*

$$\Phi_{m,v}(P) = \frac{\max_{1 \leq i \leq 4} |\mu_{m,i}(\kappa(P))|_v}{\max_{1 \leq i \leq 4} |\xi_i(P)|_v^{m^2}} .$$

*Then*

$$\hat{\lambda}_{i,v}(P) = \lambda_{i,v}(P) + \sum_{n=0}^{\infty} \frac{1}{m^{2(n+1)}} \log \Phi_{m,v}([m^n]P) \tag{5.5}$$

*for all* $P \in J_{\Theta_i}(k_v)$.

*Proof.* We denote the right-hand side of (5.5) by $\hat{\lambda}'_{i,v}$. It is sufficient to show that $\hat{\lambda}'_{i,v}$ satisfies (i) and (ii) for $m$ in Theorem 5.3.

By an argument similar to that in the proof of Lemma 5.1, $\log \Phi_{m,v}$ is an $M_k$-bounded continuous function on $J(k_v)$. Hence $\hat{\lambda}'_{i,v}$ satisfies (i). It is easy to see that $\hat{\lambda}'_{i,v}$ satisfies (ii) for $m$. ∎

As is the case for elliptic curves, we have the *quasi-parallelogram law*.

THEOREM 5.6. *Let* $P, Q \in J(k_v)$. *If* $P, Q, P+Q, P-Q \notin \operatorname{supp}(\Theta_i)$, *then*

$$\hat{\lambda}_{i,v}(P+Q) + \hat{\lambda}_{i,v}(P-Q) = 2\hat{\lambda}_{i,v}(P) + 2\hat{\lambda}_{i,v}(Q) - \log \left| \frac{B_{ii}(\kappa(P), \kappa(Q))}{\xi_i(P)^2 \xi_i(Q)^2} \right|_v.$$

*Proof.* Let $\sigma, \delta, \pi_1, \pi_2 \colon J \times J \to J$ be the homomorphisms defined by

$$\sigma(P,Q) = P+Q, \quad \delta(P,Q) = P-Q, \quad \pi_1(P,Q) = P, \quad \pi_2(P,Q) = Q.$$

Then

$$\operatorname{div}\left( \frac{B_{ii}(\kappa(P), \kappa(Q))}{\xi_i(P)^2 \xi_i(Q)^2} \right) = \sigma^* \Theta_i + \delta^* \Theta_i - 2\pi_1^* \Theta_i - 2\pi_2^* \Theta_i.$$

By Theorem 4.2, there exists an $M_k$-constant $\gamma$ such that

$$\hat{\lambda}_{i,v}(P+Q) + \hat{\lambda}_{i,v}(P-Q) = 2\hat{\lambda}_{i,v}(P) + 2\hat{\lambda}_{i,v}(Q) - \log \left| \frac{B_{ii}(\kappa(P), \kappa(Q))}{\xi_i(P)^2 \xi_i(Q)^2} \right|_v + \gamma(v).$$

By [15, Lemma 3.2], we can prove that $\gamma(v) = 0$ by an argument similar to that in the proof of Theorem 5.3. ∎

We consider the relation between global height functions and local height functions. We define the *naive height function* $h \colon J(\bar{k}) \to \mathbb{R}$ by

$$h(P) = \frac{1}{[L : \mathbb{Q}]} \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \log \max_{1 \le i \le 4} |\xi_i(P)|_v,$$

where $L$ is a finite extension of $k$ with $P \in J(L)$. Then $h(P)$ is independent of the choice of $L$ and of the homogeneous coordinates for $\kappa(P)$.

We define the *canonical height function* $\hat{h} \colon J(\bar{k}) \to \mathbb{R}$ by

$$\hat{h}(P) = \lim_{n \to \infty} \frac{1}{4^n} h([2^n]P).$$

By general theory (see [7] or [10]), the right-hand side converges.

We decompose these height functions into local height functions.

THEOREM 5.7. *Let $P \in J(\bar{k}) \setminus \operatorname{supp}(\Theta_i)$. Let $L$ be any finite extension of $k$ with $P \in J(L)$. Then*

$$h(P) = \frac{1}{[L:\mathbb{Q}]} \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \lambda_{i,v}(P), \tag{5.6}$$

$$\hat{h}(P) = \frac{1}{[L:\mathbb{Q}]} \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \hat{\lambda}_{i,v}(P). \tag{5.7}$$

*Proof.* See [10, Chapter 11, Theorem 1.6] or [7, Chapter B, Theorem 9.3]. ∎

**6. Application 1: height difference bounds.** In this section, we estimate the difference $h - \hat{h}$ (Theorem 6.4), and provide some algorithms to compute the bounds.

Let $k$ be a number field. Let $M_k^0$ be the set of all non-Archimedean absolute values in $M_k$ and $M_k^\infty$ be the set of all Archimedean absolute values in $M_k$. For $v \in M_k$, let $n_v = [k_v : \mathbb{Q}_v]$ be the local degree.

Let $\mathcal{O}_k$ be the ring of integers of $k$. We assume that the coefficients $f_0, \dots, f_6$ belong to $\mathcal{O}_k$.

We define the function $\Psi_v \colon J(k_v) \to \mathbb{R}$ by

$$\Psi_v(P) = -\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P).$$

By definition,

$$\lambda_{i,v}(P) - \hat{\lambda}_{i,v}(P) = \Psi_v(P)$$

for all $P \in J_{\Theta_i}(k_v)$. Note that $\Psi_v$ is bounded and continuous on $J(k_v)$. By Theorem 5.7,

$$\frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \inf_{Q \in J(k_v)} \Psi_v(Q) \le h(P) - \hat{h}(P) \le \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \sup_{Q \in J(k_v)} \Psi_v(Q) \tag{6.1}$$

for all $P \in J(k)$.

When $v$ is non-Archimedean, the following result is known.

THEOREM 6.1. *Under the above assumption, if $v \in M_k^0$, then*

$$\sup_{Q \in J(k_v)} \Phi_v(Q) = 1, \qquad \inf_{Q \in J(k_v)} \Phi_v(Q) \ge |2^4 \operatorname{disc}(f)|_v,$$

*where* $\operatorname{disc}(f)$ *is the discriminant of $f$ as a polynomial of degree* 6.

*Proof.* See [14, Theorem 6.1 and the second remark on p. 189]. ∎

In [14] and [15], further refinements for non-Archimedean absolute values are described.

From now on, we mainly consider Archimedean absolute values although the following results also hold for non-Archimedean absolute values.

By Corollary 5.5, we have

$$\Psi_v(P) = -\sum_{n=0}^{\infty} \frac{1}{m^{2(n+1)}} \log \Phi_{m,v}([m^n]P) \tag{6.2}$$

for all $P \in J(k_v)$. We define

$$\varepsilon_{m,v}^{-1} = \inf_{Q \in J(k_v)} \Phi_{m,v}(Q), \qquad \delta_{m,v}^{-1} = \sup_{Q \in J(k_v)} \Phi_{m,v}(Q),$$

$$S_v(m) = \frac{\log \delta_{m,v}}{m^2 - 1}, \qquad T_v(m) = \frac{\log \varepsilon_{m,v}}{m^2 - 1}.$$

The following proposition easily follows from the definition.

PROPOSITION 6.2. *Let $v \in M_k$ and $m \geq 2$ be an integer. Then for all $P \in J(k_v)$,*

$$S_v(m) \leq \Psi_v(P) \leq T_v(m).$$

REMARK 6.3. Proposition 6.2 also holds for elliptic curves. See [17, Proposition 14].

We can estimate the difference $h - \hat{h}$ as follows:

THEOREM 6.4. *Let $m \geq 2$ be an integer. Then*

$$\frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k^\infty} n_v S_v(m) \leq h(P) - \hat{h}(P)$$
$$\leq \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k^\infty} n_v T_v(m) + \frac{1}{3[k:\mathbb{Q}]} \log N_{k/\mathbb{Q}}(\mathrm{disc}(f)) + \frac{4}{3} \log 2$$

*for all $P \in J(k)$.*

*Proof.* The theorem follows from (6.1), Theorem 6.1, Proposition 6.2, and the product formula. ∎

We obtain the same properties for $S_v(m)$ and $T_v(m)$ as those for elliptic curves described in [17]. We omit the proofs for the following results because they are exactly the same as those in [17].

PROPOSITION 6.5. *Let $m \geq 2$ and $l \geq 1$ be integers. Then*

$$S_v(m) \leq S_v(m^l), \quad T_v(m^l) \leq T_v(m),$$

*that is, the bounds in Proposition 6.2 become sharper when we change $m$ to $m^l$.*

We can estimate the differences between the extrema of $\Phi_v$ and $S_v(m)$, $T_v(m)$ by the following proposition and its corollaries.

PROPOSITION 6.6. *Let $m \geq 2$ be an integer. Then*

$$0 \leq \inf_{P \in J(k_v)} \Psi_v(P) - S_v(m) \leq \frac{1}{m^2-1}\Big( \sup_{P \in J(k_v)} \Psi_v(P) - \inf_{P \in J(k_v)} \Psi_v(P)\Big),$$

$$0 \leq T_v(m) - \sup_{P \in J(k_v)} \Psi_v(P) \leq \frac{1}{m^2-1}\Big( \sup_{P \in J(k_v)} \Psi_v(P) - \inf_{P \in J(k_v)} \Psi_v(P)\Big).$$

COROLLARY 6.7.

$$\lim_{m \to \infty} S_v(m) = \inf_{P \in J(k_v)} \Psi_v(P), \qquad \lim_{m \to \infty} T_v(m) = \sup_{P \in J(k_v)} \Psi_v(P).$$

We estimate the difference between the theoretical bounds and the bounds in Proposition 6.2 in the following corollary.

COROLLARY 6.8.

$$0 \leq \inf_{P \in J(k_v)} \Psi_v(P) - S_v(m) \leq \frac{1}{m^2}(T_v(m) - S_v(m)),$$

$$0 \leq T_v(m) - \sup_{P \in J(k_v)} \Psi_v(P) \leq \frac{1}{m^2}(T_v(m) - S_v(m)).$$

As described above, we can estimate $\Psi_v$ with arbitrary accuracy at least theoretically. However, actual computations are quite difficult because the size of $\mu_{m,i}$ increases rapidly.

In the rest of this section, we describe some algorithms to compute the extrema of $\Phi_{m,v}$. First, we consider the case where $k_v$ is isomorphic to $\mathbb{R}$. We identify $k_v$ with $\mathbb{R}$. We may regard $\Phi_{m,v}$ as a function on $\mathbb{P}^3(\mathbb{R})$. Let $D = \kappa(J(\mathbb{R}))$. Note that $D$ is not equal to $K(\mathbb{R})$ although $D$ is contained in $K(\mathbb{R})$. Thus we need the following lemma.

LEMMA 6.9. *Let $k$ be an arbitrary field with $\mathrm{char}(k) \neq 2$. Let $P = (\xi_1, \ldots, \xi_4) \in K(k)$. Then $P \in \kappa(J(k))$ if and only if all the following numbers are squares in $k$:*

$$\begin{aligned}
S_6(P) &= f_0\xi_3^2\xi_1^2 + (-2f_0\xi_3\xi_2^2 - f_1\xi_3^2\xi_2)\xi_1 + f_0\xi_2^4 \\
&\quad + f_1\xi_3\xi_2^3 + f_2\xi_3^2\xi_2^2 + f_3\xi_3^3\xi_2 + f_4\xi_3^4 + \xi_4\xi_3^3, \\
S_7(P) &= (f_0\xi_2^2 + f_1\xi_3\xi_2 + f_2\xi_3^2)\xi_1^2 + \xi_4\xi_3^2\xi_1 + f_6\xi_3^4, \\
S_8(P) &= f_0\xi_1^4 + (f_4\xi_3^2 + \xi_4\xi_3)\xi_1^2 + f_5\xi_3^2\xi_2\xi_1 + f_6\xi_3^2\xi_2^2, \\
S_9(P) &= f_2\xi_1^4 + (f_3\xi_2 + \xi_4)\xi_1^3 + (f_4\xi_2^2 - f_5\xi_3\xi_2 + f_6\xi_3^2)\xi_1^2 \\
&\quad + (f_5\xi_2^3 - 2f_6\xi_3\xi_2^2)\xi_1 + f_6\xi_2^4.
\end{aligned}$$

*Furthermore, if at least one of the above numbers is a non-zero square in $k$, then $P \in \kappa(J(k))$.*

REMARK 6.10. $S_8$ and $S_9$ have already appeared in [15, p. 172] as $s_2$ and $s_1$ respectively.

To prove Lemma 6.9, we need the following lemmas:

LEMMA 6.11 ([3, Lemma 3.1]). *Let $P \in J$. Regarding $J \subset \mathbb{P}^{15}$ as in* [2], *we write $P = (a_0, a_1, \dots, a_{15})$. Let $E \subset \mathbb{P}^9$ be the image of the projection map*

$$(a_0, a_1, \dots, a_{15}) \mapsto (a_0, a_3, a_4, a_5, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}).$$

*Then $K$ is isomorphic to $E$ under the isomorphism $\rho\colon K \to E$, where*

$$Q = (\xi_1, \dots, \xi_4) \mapsto$$
$$(\rho_0(Q), \rho_3(Q), \rho_4(Q), \rho_5(Q), \rho_{10}(Q), \rho_{11}(Q), \rho_{12}(Q), \rho_{13}(Q), \rho_{14}(Q), \rho_{15}(Q)),$$
$$\rho_0(Q) = \xi_4^2, \quad \rho_3(Q) = \xi_3\xi_4, \quad \rho_4(Q) = \frac{1}{2}(\xi_2\xi_4 - f_1\xi_1^2 - f_3\xi_1\xi_3 - f_5\xi_3^2),$$
$$\rho_5(Q) = \xi_1\xi_4, \quad \rho_{10}(Q) = \xi_3^2, \quad \rho_{11}(Q) = \xi_2\xi_3, \quad \rho_{12}(Q) = \xi_1\xi_3,$$
$$\rho_{13}(Q) = \xi_1\xi_2, \quad \rho_{14}(Q) = \xi_1^2, \quad \rho_{15}(Q) = \xi_2^2 - 4\xi_1\xi_3.$$

REMARK 6.12. The embedding $J \to \mathbb{P}^{15}$ in [2] is different from that in [3]. Hence the above isomorphism $\rho$ is also different from that in [3].

The following lemma is due to the referee.

LEMMA 6.13. *Let $P \in K(\bar{k})$. If*

$$S_6(P) = S_7(P) = S_8(P) = S_9(P) = 0, \tag{6.3}$$

*then there exists a 2-torsion point $Q \in J(\bar{k})$ such that $P = \kappa(Q)$. In particular, if $P \in K(k)$ satisfies* (6.3), *then $P \in \kappa(J(k))$.*

*Proof.* This follows from the fact that $S_i = a_i^2$ in the notation of Lemma 6.11. We omit the details. ∎

*Proof of Lemma 6.9.* We can observe that for any $i, j \in \{1, 2, 6, 7, 8, 9\}$ there exists a defining equation of $J$ (available from `jacobian.variety/defining.equations` in [4]) of the form

$$a_i a_j = E_{ij}(a_0, a_3, a_4, a_5, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}),$$

where $E_{ij}$ is a quadratic form in 10 variables. By Lemma 6.11, for $P = (\xi_1, \dots, \xi_4) \in K$, we have

$$a_i a_j = E_{ij}(\rho_0(P), \rho_3(P), \rho_4(P), \rho_5(P), \rho_{10}(P), \rho_{11}(P), \rho_{12}(P), \rho_{13}(P), \rho_{14}(P), \rho_{15}(P)). \tag{6.4}$$

The right-hand side is a quartic form in $\xi_1, \dots, \xi_4$. In particular,

$$a_i^2 = E_{ii}(\rho_0(P), \rho_3(P), \rho_4(P), \rho_5(P), \rho_{10}(P), \rho_{11}(P), \rho_{12}(P), \rho_{13}(P), \rho_{14}(P), \rho_{15}(P)).$$

Therefore, putting $S_i(P) = E_{ii}(\rho_0(P), \dots, \rho_{15}(P))$, we obtain the last part of the lemma by (6.4).

The first part follows from Lemma 6.13. ∎

Putting $k = \mathbb{R}$ in Lemma 6.9, we obtain the following corollary:

COROLLARY 6.14. *Let* $D = \kappa(J(\mathbb{R}))$. *Then*

$$D = \{P \in \mathbb{P}^3(\mathbb{R}) \mid G(P) = 0, S_i(P) \geq 0 \text{ for } i = 6, 7, 8, 9\}.$$

By the corollary, the computation of the extrema of $\Phi_{m,v}$ reduces to the global optimization of a continuous function with polynomial constraints. Furthermore, we let

$$D_i = D \cap \{(\xi_1, \ldots, \xi_{i-1}, 1, \xi_{i+1}, \ldots, \xi_4) \in \mathbb{P}^3(\mathbb{R}) \mid |\xi_j| \leq 1 \text{ for } j \neq i\}.$$

Then $D = D_1 \cup \cdots \cup D_4$. We may regard $D_i$ as a subset of $\mathbb{R}^3$. The function $\Phi_{m,v}$ can be simplified on $D_i$ as follows:

$$\Phi_{m,v}(P) = \max_{1 \leq j \leq 4} |\mu_{m,j}(P)|$$

for all $P = (\xi_1, \ldots, \xi_{i-1}, 1, \xi_{i+1}, \ldots, \xi_4) \in D_i$. Let

$$e_{m,i} = \inf_{P \in D_i} \Phi_{m,v}(P), \qquad d_{m,i} = \sup_{P \in D_i} \Phi_{m,v}(P).$$

Then

$$\varepsilon_{m,v}^{-1} = \min_{1 \leq i \leq 4} e_{m,i}, \qquad \delta_{m,v}^{-1} = \max_{1 \leq i \leq 4} d_{m,i}.$$

Thus it is sufficient to compute $e_{m,i}$ and $d_{m,i}$. This can be done by a rigorous global optimization. There are several algorithms for rigorous global optimization. The author used interval analysis (cf. [6]) to compute examples.

In practice, the constraints defining $D_i$ may be too complicated for the algorithm used for optimization. In order to make the computations easier, we can omit some of the constraints $S_i(P) \geq 0$. Then we may have weaker bounds; however, they are often sufficient. Note that the closure of the set $\{P \in \mathbb{P}^3(\mathbb{R}) \mid S_i(P) > 0\}$ coincides with $D$ for any fixed index $i = 6, 7, 8, 9$. If we omit all of the constraints $S_i(P) \geq 0$ and let $m = 2$, then our bounds are equal to those in [5].

Next, we consider the case where $k_v$ is isomorphic to $\mathbb{C}$. In this case, we have $\kappa(J(k_v)) = K(k_v)$. Hence we do not need to consider constraints as in Corollary 6.14. The other parts of the algorithm are similar to the case of $\mathbb{R}$.

Finally, we give some examples. In these, we treat only the case where $k_v$ is isomorphic to $\mathbb{R}$ and give bounds only for $T_v(2)$. The author's implementation of the algorithm is available at [18].

EXAMPLE 6.15. We consider the curve

$$Y^2 = X^6 + 8X^5 + 22X^4 + 22X^3 + 5X^2 + 6X + 1,$$

taken from [5, Section 10]. In [5], Flynn and Smart stated that $T_v(2) = (\log \varepsilon_{2,v})/3 \leq 1.474$. Note that $T_v(2)$ is denoted $c_1^{(v)}/3$ in [5] and $\gamma_v/3$ in [14]. However, Stoll [14] pointed out that this bound was incorrect. In fact, he

showed that $T_v(2) \geq 2.241$ by giving a point on $K(\mathbb{R})$. He also stated an upper bound, namely that $T_v(2) \leq 2.6$.

By using interval analysis, we can prove that $T_v(2) \leq 2.24110646$. This agrees with Stoll's computation and is sharper than his bound. Note that interval analysis guarantees the accuracy of the bound. In this example, the constraints $S_i(P) \geq 0$ do not affect the bound.

EXAMPLE 6.16. As an example where the constraints do affect the bound, we consider the curve

$$Y^2 = X(X-1)(X-2)(X-5)(X-6).$$

This curve is taken from [2, (8.1.1)].

When we omit all the constraints $S_i(P) \geq 0$, we have $T_v(2) \leq 3.592$. However, with all the constraints, we obtain $T_v(2) \leq 2.813$.

**7. Application 2: computation of the canonical height.** Algorithms to compute the canonical height on $J(k)$ are described in [5] and [15]. We describe a refinement of those algorithms.

Let $k$ be a number field. We use the same notation as in Section 6. We assume that $f_0, \ldots, f_6 \in \mathcal{O}_k$.

We compute the canonical height by decomposing it into the canonical local heights. The following is important for computing the canonical local heights.

THEOREM 7.1 ([15, Theorem 4.1]). *Let $v \in M_k^0$ and $U = \{P \in J(k_v) \mid \Phi_v(P) = 1\}$. Then $U$ is a subgroup of finite index in $J(k_v)$, and $\Phi_v$ factors through $J(k_v)/U$. Furthermore, $\Phi_v(P) = \Phi_v(-P)$.*

By this theorem, we have the following corollary.

COROLLARY 7.2. *Let $v \in M_k^0$ be a non-Archimedean absolute value. If $P \in U$ and $P \notin \operatorname{supp}(\Theta_i)$, then*

$$\hat{\lambda}_{i,v}(P) = \lambda_{i,v}(P).$$

Combining Corollaries 5.4 and 7.2, we obtain the following proposition.

PROPOSITION 7.3. *Let $v \in M_k^0$ and $P \in J(k_v)$. For a positive integer $m$ with $[m]P \in U$, we have*

$$\Psi_v(P) = -\frac{1}{m^2} \log \Phi_{m,v}(P).$$

Flynn and Smart [5] compute canonical heights as follows:

(i) Find $m$ such that $\Phi_v([m]P) = 1$ for all $v \in M_k^0$.

(ii) Compute

$$\hat{h}([m]P) = h([m]P) + \sum_{v \in M_k^\infty} n_v \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n m]P).$$

(iii) Then $\hat{h}(P) = \hat{h}([m]P)/m^2$.

In this algorithm, the number $m$ may be very large. In fact, we let $m_v$ be the smallest positive integer such that $\Phi_v([m_v]P) = 1$. Then we have to take $m = \operatorname{lcm}\{m_v \mid v \in M_k^0\}$.

Stoll [15] computes the canonical height by using Theorem 7.1, where it is sufficient to compute $[m]P$ for $m = \max\{m_v \mid v \in M_k^0\}$. However, his computation is a little complicated since he uses only the duplication map.

By referring to Proposition 7.3, we obtain a simpler algorithm as follows:

(i) We assume that homogeneous coordinates $\xi_i(P)$ belong to $\mathcal{O}_k$.
(ii) Let $S = \{v \in M_k^0 \mid \Phi_v(P) \neq 1\}$.
(iii) For each $v \in S$, find a positive integer $m_v$ such that $\Phi_v([m_v]P) = 1$.
(iv) For $v \in S$, we have

$$\Psi_v(P) = -\frac{1}{m_v^2} \log \Phi_{m_v,v}(P).$$

(v) For $v \in M_k^0 \setminus S$, we have $\Psi_v(P) = 0$.
(vi) For $v \in M_k^\infty$, compute by definition

$$\Psi_v(P) = -\sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P).$$

We can use a floating-point approximation of the coordinates of $P$ here.

(vii) Then

$$\hat{h}(P) = h(P) - \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \Psi_v(P).$$

In step (ii), we can compute $S$ as follows: Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in $\mathcal{O}_k$ given by

$$\mathfrak{a} = \langle \xi_1(P), \dots, \xi_4(P) \rangle, \qquad \mathfrak{b} = \langle \delta_1(\kappa(P)), \dots, \delta_4(\kappa(P)) \rangle.$$

Then $\mathfrak{b} \cdot \mathfrak{a}^{-4}$ is an integral ideal and $S = \{v \in M_k^0 \mid \mathfrak{b} \cdot \mathfrak{a}^{-4} \subset \mathfrak{p}_v\}$, where $\mathfrak{p}_v$ is the prime ideal in $\mathcal{O}_k$ associated with $v$. If $\mathcal{O}_k$ is a principal ideal domain, then we can compute greatest common divisors to make the above algorithm simpler. See [15, Section 6].

In step (iv), note that it is not necessary to compute the polynomials $\mu_{m_v,i}$. We need only the values $\mu_{m_v,i}(\kappa(P))$, and we can compute them by the relations in Theorem 3.3. See also [5, Section 4]. In fact, it is sufficient to compute the values $\mu_{m_v,i}(\kappa(P))$ instead of $[m_v]P$ in step (iii). In practice, the ideal $\langle \mu_{m,1}(\kappa(P)), \dots, \mu_{m,4}(\kappa(P)) \rangle$ may have a large norm, which may make

the computation slow. To prevent this, we should divide the coordinates $\mu_{m,i}(\kappa(P))$ by an algebraic integer $\alpha_m$ and record $\mathrm{ord}_v(\alpha_m)$ for each $v \in S$. The values $\log \Phi_{m_v,v}(P)$ can be computed by using $\mathrm{ord}_v(\alpha_{m_v})$. If $\mathcal{O}_k$ is a principal ideal domain, we can choose $\alpha_m = \gcd(\mu_{m,1}(\kappa(P)), \ldots, \mu_{m,4}(\kappa(P)))$.

The referee pointed out that the computation in step (iii) and (iv) can be done modulo a sufficiently large power of $\mathfrak{p}_v$. It may reduce the cost of the computation.

Our algorithm computes the canonical height in almost the same time as Stoll's. However, our implementation, available at [18], is a little simpler than Stoll's.

**Acknowledgements.** The author thanks Professor Kazuhiro Fujiwara for useful comments and help. He also thanks the referee for valuable suggestions.

The author was partially supported by the JSPS Research Fellowships for Young Scientists and the JSPS Core-to-Core Program 18005.

## References

[1] T. Becker and V. Weispfenning, *Gröbner Bases*, Grad. Texts in Math. 141, Springer, New York, 1993.

[2] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge Univ. Press, Cambridge, 1996.

[3] E. V. Flynn, *The group law on the Jacobian of a curve of genus 2*, J. Reine Angew. Math. 439 (1993), 45–69.

[4] —, *Genus 2 Site*, ftp://ftp.liv.ac.uk/pub/genus2/.

[5] E. V. Flynn and N. P. Smart, *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith. 79 (1997), 333–352.

[6] E. Hansen and G. W. Walster, *Global Optimization Using Interval Analysis*, 2nd ed., Monogr. Textbooks Pure Appl. Math. 264, Marcel Dekker, New York, 2004.

[7] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Grad. Texts in Math. 201, Springer, New York, 2000.

[8] N. Kanayama, *Division polynomials and multiplication formulae of Jacobian varieties of dimension 2*, Math. Proc. Cambridge Philos. Soc. 139 (2005), 399–409; Corrections, ibid. 149 (2010), 189–192.

[9] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer, Berlin, 1978.

[10] —, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.

[11] D. Mumford, *Abelian Varieties*, 2nd ed., Oxford Univ. Press, Oxford, 1974.

[12] A. Néron, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. (2) 82 (1965), 249–331.

[13] M. Noro et al., *A computer algebra system Risa/Asir*, http://www.math.kobe-u.ac.jp/Asir/.

[14] M. Stoll, *On the height constant for curves of genus two*, Acta Arith. 90 (1999), 183–201.

[15] —, *On the height constant for curves of genus two, II*, ibid. 104 (2002), 165–182.

[16] Y. Uchida, *On the difference between the ordinary height and the canonical height on elliptic curves*, Proc. Japan Acad. Ser. A Math. Sci. 82 (2006), 56–60.

[17] —, *The difference between the ordinary height and the canonical height on elliptic curves*, J. Number Theory 128 (2008), 263–279.

[18] —, *Programs for the Jacobians of curves of genus 2*, http://www.math.kyoto-u.ac.jp/~uchida/programs/.

[19] K. Yoshitomi, *On height functions on Jacobian surfaces*, Manuscripta Math. 96 (1998), 37–66.

[20] H. G. Zimmer, *Quasifunctions on elliptic curves over local fields*, J. Reine Angew. Math. 307/308 (1979), 221–246; Corrections and remarks, ibid. 343 (1983), 203–211.

Yukihiro Uchida
Department of Mathematics
Faculty of Science
Kyoto University
Kyoto 606-8502, Japan
E-mail: uchida@math.kyoto-u.ac.jp

*Received on 26.5.2009*
*and in revised form on 12.10.2010* (6041)