An Explicit Theory of Heights

E. V. Flynn, Mathematical Institute, University of Oxford

Abstract

We consider the problem of explicitly determining the naive height constants for Jacobians of hyperelliptic curves. For genus > 1, it is impractical to apply Hilbert's Nullstellensatz directly to the defining equations of the duplication law; we indicate how this technical difficulty can be overcome by use of isogenies. The height constants are computed in detail for the Jacobian of an arbitrary curve of genus 2, and we apply the technique to compute generators of $\mathcal{J}(\mathbb{Q})$, the Mordell-Weil group for a selection of rank 1 examples.

§0. Introduction

There are an increasing number of methods available [2],[6],[7],[11] for performing a Galois 2-descent on the Jacobian $\mathcal{J}$ of a hyperelliptic curve, giving $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, and hence the rank of $\mathcal{J}(\mathbb{Q})$, the Mordell-Weil group. These methods have collectively found the ranks of 15 Jacobians of curves of genus 2, and one of genus 3; it is likely that minor refinements of [6],[11] will soon lead to rank tables of several hundred Jacobians. What has been lacking, however, is an explicit theory of heights in a form which allows generators of $\mathcal{J}(\mathbb{Q})$ to be deduced from $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. For example, in [7], the curve $Y^2 = X(X-1)(X-2)(X-5)(X-6)$ is shown to have rank 1; the torsion supgroup of $\mathcal{J}(\mathbb{Q})$ is given by the 16 divisors of order 2, and there is the divisor: $(3,6) - \infty \in \mathcal{J}(\mathbb{Q})$ of infinite order. These are shown to generate $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, but the questions is asked by Gordon and Grant in [7], §4, whether they generate $\mathcal{J}(\mathbb{Q})$, and they request: "It would be nice to have the theory of heights on Jacobians of curves of genus two worked out sufficiently explicitly to afford answers to such questions". This gap in the literature is also pointed out by Cassels in [2], p.30. It is the purpose of this paper to fill this gap.

In principle, there is already sufficient theory available to for evaluating the constants involved in height calculations. For example, the duplication map on a suitable embedding [10] of the Jacobian variety is well known to be a morphism of degree 4, from which one

* The author thanks SERC for financial support.

can derive a natural height function and constant C such that $H(2P) \geqslant \big(H(P)\big)^4/C$ for all P on $\mathcal{J}(\mathbb{Q})$. The usual justification for the existence of such a C quotes Hilbert's Nullstellensatz, applied to the non-degenerate quartics which define the duplication map. This can be applied in practice on the projective x-coordinate height on an elliptic curve, but is impractical in dimension > 1. For example, on the Kummer surface height in dimension 2, we would require an impractical resultant calculation on a set of 4 homogeneous quartics in 4 variables; a possible method for such a computation is in [9], however the successive elimination of the variables results in polynomials of enormous degree, and a very poor value for the constant C. We overcome this difficulty by writing the duplication map in dimension 2 as the composition of linear maps and simple quadratic maps relating to an isogeny of Richelot [1].

In Section 1, we present a few preliminary definitions and lemmas relating to general height functions on abelian groups. Section 2 illustrates the technique for the x-coordinate height function on an elliptic curve, and Section 3 extends the properties of the dimension 2 group law in [5],[6] to do the same for the Kummer surface height function on the Jacobian of a general curve of genus 2. In Section 4, we use the explicit constants of Section 3 to find generators of $\mathcal{J}(\mathbb{Q})$ for a selection of rank 1 Jacobians of curves of genus 2.

§1. Preliminary Definitions

In this section, we give a few general definitions of height functions, and a technical lemma required in Sections 2 and 3.

Definition 1.1. Let G be an abelian group. A *height function* H is a map $H : G \mapsto \mathbb{R}^+$ satisfying:

(1). There exists a constant C_1 such that, for all $P, Q \in G$, $H(P+Q)H(P-Q) \leqslant C_1 H(P)^2 H(Q)^2$.

(2). There exists a constant C_2 such that, for all $P \in G$, $H(2P) \geqslant H(P)^4/C_2$.

(3). For any constant C_3, the set $\{P \in G : H(P) \leqslant C_3\}$ is finite.

The constants C_1, C_2 depend only on the group G and the height function H, and we shall refer to them as the *height constants*.

The following property of abelian groups with a height function is proved in [12], p.199.

Lemma 1.2. *Let G be an abelian group with height function H, such that $G/2G$ is a finite set: $\{Q_1, \ldots, Q_n\}$, say. Then G is finitely generated. Explicitly, if $\epsilon = min\{H(P) : P \in G\}$, and $C_1' = max\{H(Q_i)^2 : 1 \leqslant i \leqslant n\} \cdot C_1/\epsilon$, then G is generated by the finite set: $\{P \in G : H(P) \leqslant \sqrt{C_1' C_2}\} \cup \{Q_1, \ldots, Q_n\}$.* □

From now on, K will always represent a finite extension of $\mathbb{Q}$. There is a standard function H which may be defined on $\mathbb{P}^n(K)$,

Definition 1.3. Let $\mathbf{x} = (x_i) \in \mathbb{P}^n(K)$. Define $H(\mathbf{x}) = \big(\prod_v \max_{0 \leqslant i \leqslant n} |x_i|_v\big)^{1/[K:\mathbb{Q}]}$, where $\prod_v$ is over all valuations on K which extend the usual valuations $|\ |_p$ and $|\ |_\infty$ on $\mathbb{Q}$. For any $x \in K$, define $H(x) = H(\binom{1}{x})$.

The following is a standard fact about heights (Theorem 5.11 in [12]).

Lemma 1.4. *For any C, the set $\{\mathbf{x} \in \mathbb{P}^n(K) : H(\mathbf{x}) \leqslant C\}$ is finite.* □

In addition to $\mathbb{P}^n(K)$, it will be useful to refer to the following sets.

Definition 1.5. Given indeterminates $\mathbf{v} = (v_i)$, $\mathbf{w} = (w_i)$, let $K[\mathbf{v}^2, \mathbf{w}^2]$ denote the ring of quartic polynomials which are homogeneous of degree 2 in each of $v_0, \ldots v_n$ and $w_0, \ldots w_n$. Let $K[\mathbf{v}^4]$ denote the ring of polynomials which are homogeneous of degree 4 in $v_0, \ldots v_n$. For any ring $\mathcal{R}$, let $\mathbb{M}^n(\mathcal{R})$ represent all $(n+1) \times (n+1)$ matrices over $\mathcal{R}$ modulo scalar multiplication.

For our purposes, we shall only require members of: $\mathbb{P}^n(K)$, $\mathbb{M}^n(K)$, $\mathbb{M}^n(K[\mathbf{v}^2, \mathbf{w}^2])$ and $\mathbb{P}^n(K[\mathbf{v}^4])$. The height of Definition 1.3 can be extended to these sets.

Definition 1.6. Let $W = (W_{ij}) \in \mathbb{M}^n(K)$, $M = (M_{ij}) \in \mathbb{M}^n(K[\mathbf{v}^2, \mathbf{w}^2])$, $N = (N_i) \in \mathbb{P}^n(K[\mathbf{v}^4])$. Define $H(W) = (n+1)\big(\prod_v \max_{i,j} |W_{ij}|_v\big)^{1/[K:\mathbb{Q}]}$. For each i, j let $|M_{ij}|_v$ denote (number of terms in M_{ij}) $\cdot \max\{|c|_v : c \text{ is a coefficient of } M_{ij}\}$, and for each i let $|N_i|_v$ denote (number of terms in N_i) $\cdot \max\{|c|_v : c \text{ is a coefficient of } N_i\}$. We can now define $H(M) = (n+1)\big(\prod_v \max_{i,j} |M_{ij}|_v\big)^{1/[K:\mathbb{Q}]}$, and $H(N) = (n+1)\big(\prod_v \max_i |N_i|_v\big)^{1/[K:\mathbb{Q}]}$.

We shall always denote matrix multiplication in the style: $M_1 \cdot M_2$. The following technical lemmas are immediate.

Lemma 1.7. *Let Let $W = (W_{ij}) \in \mathbb{M}^n(K)$, $M = (M_{ij}) \in \mathbb{M}^n(K[\mathbf{v}^2, \mathbf{w}^2])$, $N = (N_i) \in \mathbb{P}^n(K[\mathbf{v}^4])$, and $\mathbf{x}, \mathbf{y} \in \mathbb{P}^n(K)$. Then:*

$(i).\ H(\mathbf{x})/H(W^{-1}) \leqslant H(M\cdot\mathbf{x}) \leqslant H(W)H(\mathbf{x}).$
$(ii).\ H\big(M(\mathbf{x},\mathbf{y})\big) \leqslant H(M)H(\mathbf{x})^2H(\mathbf{y})^2.$
$(iii).\ H\big(N(\mathbf{x})\big) \leqslant H(N)H(\mathbf{x})^4.$ □

Lemma 1.8. *Let $\mathbf{x},\mathbf{y}\in\mathbb{P}^n(K)$, and let $M=(x_iy_j+x_jy_i)\in\mathbb{M}^n(K)$. Then $H(\mathbf{x})H(\mathbf{y})\leqslant 2H(M)$.* □

If a group G comes with a finite map to $\mathbb{P}^n(K)$ then the following lemma gives a set of conditions under which the height H on $\mathbb{P}^n(K)$ of Definition 1.3 induces a height function on G.

Lemma 1.9. *Let G be an abelian group and $\kappa : G\longrightarrow\mathbb{P}^n(K)$ be such that, for any $\mathbf{x}\in\mathbb{P}^n(K)$, the set $\kappa^{-1}(\mathbf{x})$ is finite. For any $P\in G$, denote $\kappa(P)=(\kappa_i(P))$. Suppose there exist $M\in\mathbb{M}^n(K[\mathbf{v}^2,\mathbf{w}^2])$, $N\in\mathbb{P}^n(K[\mathbf{v}^4])$ such that:*
$(i).\ \big(\kappa_i(P+Q)\kappa_j(P-Q)+\kappa_j(P+Q)\kappa_i(P-Q)\big)=M(\kappa(P),\kappa(Q))$ *for all $P,Q\in G$,*
$(ii).\ \kappa(2P)=N(\kappa(P))$ *for all $P\in G$,*
and N is non-degenerate over $\overline{K}$ (that is, $N(\mathbf{x})\neq\mathbf{0}$ for all $\mathbf{x}\in\mathbb{P}^n(\overline{K})$, so that N represents a morphism of degree 4). Then there exist $r\in\mathbb{Z}$, $R\in\mathbb{M}^n(K[\mathbf{v}^r])$, such that $R\cdot N=(v_i^{r+4})$, and $H_\kappa(P)=H(\kappa(P))$ defines a height function on G, with height constants $C_1=2H(M)$, $C_2=H(R)$.

Proof. Combining Lemma 18. and Lemma 1.7 (ii), we have $H_\kappa(P+Q)H_\kappa(P-Q)\leqslant 2H\big(M(\kappa(P),\kappa(Q))\big)\leqslant 2H(M)H(P)^2H(Q)^2$, so that property (1) of Definition 1.1 is satisfied with $C_1=2H(M)$. The existence of r,R follows from the non-degeneracy of N and Hilbert's Nullstellensatz. Applying Lemma 1.7 $(i),(ii)$ gives: $H_\kappa(P)^{r+4}=H((R\cdot N)(\kappa(P)))=H(R(\kappa(P))\cdot N(\kappa(P))=H(R(\kappa(P))\cdot\kappa(2P))\leqslant H(R(\kappa(P)))H(\kappa(2P)\leqslant H(R)H_\kappa(P)^rH_\kappa(2P)$. Dividing through by $H(R)H_\kappa(P)^r$ gives property (2) of Definition 1.1 with $C_2=H(R)$. Finally, property (3) of Definition 1.1 follows from Lemma 1.4 and the finiteness of the map κ. □

It is possible, given that M is non-degenerate (that is, $M(\mathbf{x},\mathbf{y})\neq\mathbf{0}$ for all $\mathbf{x},\mathbf{y}\in\mathbb{P}^n(\overline{K})$), to derive the duplication law N from M, in which case the conclusion of the above lemma will follow merely from the existence of M.

Corollary 1.10. *Let G, κ, M be as in Lemma 1.9, with M non-degenerate. Then H_κ is a height function on G.*

Proof. It is sufficient to show the existence of N satisying the conditions of Lemma 1.9. By changing basis, if necessary, so that κ takes the group identity to $(1, 0, \ldots, 0)^T$, we can take $N = (M_{00}(\mathbf{v}, \mathbf{v}), 2M_{01}(\mathbf{v}, \mathbf{v}), \ldots 2M_{0n}(\mathbf{v}, \mathbf{v}))^T$. □

The above lemmas provide a natural process for defining a height function on the Jacobian of a hyperelliptic curve of genus g given by $Y^2 = F(X)$, where F is a polynomial of degree $2g + 1$ or $2g + 2$, defined over a number field, with nonzero discriminant. There is a map $\kappa : \mathcal{J}(K) \longrightarrow \mathbb{P}^{2^g-1}(K)$, taking the quotient under $\pm$, from the K-rational points on the Jacobian to the K-rational points on the Kummer variety $\kappa(J)$. The map κ is injective on the points of order 2 and is 2:1 elsewhere. Classical identities of theta functions (for $\theta_i(z_1+z_2)\theta_j(z_1-z_2)+\theta_j(z_1+z_2)\theta_i(z_1-z_2)$) [8],[10] explicitly describe $M \in \mathbb{M}^{2^g-1}(K[\mathbf{v}^2, \mathbf{w}^2])$, and hence $N \in \mathbf{P}^{2^g-1}(K[\mathbf{v}^4])$, which satisfy precisely the conditions of Lemma 1.9. Strictly speaking, the identities in the classical theory involve maps over $\mathbb{C}$; however, the field of definition of M, N can be taken to be a finite extension of the ground field of the curve. It follows that $H_\kappa(P) = H(\kappa(P))$ defines a height function on $\mathcal{J}(K)$. This gives the most natural generalisation of the projective x-coordinate height on an elliptic curve.

Let us consider what is involved in evaluating explicitly the height constants C_1, C_2 for the Kummer height H_κ on the Jacobian $\mathcal{J}(K)$. Let us suppose that $M \in \mathbb{M}^{2^g-1}(K[\mathbf{v}^2, \mathbf{w}^2])$, $N \in \mathbf{P}^{2^g-1}(K[\mathbf{v}^4])$, have already been determined, as above. The constant $C_1 = 2H(M)$ is straightforward to compute directly from the coefficients of M. However, for C_2, the computation of the resultant matrix $R \in \mathbb{M}^{2^g-1}(K[\mathbf{v}^r])$ in the proof of Lemma 1.9 involves the elimination of $2^g - 1$ variables by iterative resultant calculations; this is only viable for the simplest case $g = 1$. We can overcome this difficulty by factoring the duplication map $N \in \mathbf{P}^{2^g-1}(K[\mathbf{v}^4])$ on the Kummer variety as the composition of isogenies $\phi_\kappa, \hat{\phi}_\kappa \in \mathbb{P}^{2^g-1}(K[\mathbf{v}^2])$. Each of ϕ_κ, $\hat{\phi}_\kappa$ has the identity and $2^g - 1$ points of order 2 as its kernel. Addition by members of the kernel of ϕ_κ induces 2^g linear maps on the kummer variety. If W_3 represents a linear change of basis which simultaneously diagonalises these maps, then the quadratic map τW_3, where $\tau : (v_i) \mapsto (v_i^2)$ is invariant under addition by any member of the kernel of ϕ_κ, and requires only a further linear map

to give ϕ_κ precisely. Note that the eigenvalues of the matrices representing addition by the kernel of ϕ_κ may not lie in K, in which case W_3 will be defined over an extension L of K. Applying the same process to $\hat{\phi}_\kappa$ then finally gives the duplication law N as a composition involving 3 linear maps and 2 applications of τ. The height constant C_2 then becomes straightforward to compute in terms of the linear maps, as follows.

Lemma 1.11. *Let G, n, κ, M, N be as described in Lemma 1.9. Let $\tau : (v_i) \mapsto (v_i^2)$. Suppose that, for some finite extension L of K, there exist matrices $W_1, W_2, W_3 \in \mathbb{M}^n(L)$ such that $N = W_1\tau W_2\tau W_3\mathbf{v}$. Then we can take the height constant $C_2 = H(W_1^{-1})H(W_2^{-1})^2H(W_3^{-1})^4$ for H_κ on G.*

Proof. Immediate from Lemma 1.7 (i), and the fact that $H(\tau(\mathbf{x})) = H(\mathbf{x})^2$. □

We can therefore summarise our strategy for an explicit theory of heights on the Jacobian over a number field as follows.

Step 1. Fix an explicit embedding of the Kummer variety $\kappa : \mathcal{J} \longrightarrow \mathbb{P}^{2^g-1}(K)$, together with $M \in \mathbb{M}^n(K([\mathbf{v}^2, \mathbf{w}^2]))$, $N \in \mathbb{P}^{2^g-1}(K[\mathbf{v}^4])$, as described in Lemma 1.9. Define H_κ on $\mathcal{J}$ by $H_\kappa(P) = H(\kappa(P))$.

Step 2. Axiom (1) of Definition 1.1 is then satisfied with $C_1 = 2H(M)$.

Step 3. Factor the duplication law N on the Kummer variety via isogeny as $N = W_1\tau W_2\tau W_3$, where $W_1, W_2, W_3 \in \mathbb{M}^{2^g-1}(L)$, for some finite extension L of K.

Step 4. Axiom (2) of Definition 1.1 is satisfied with $C_2 = H(W_1^{-1})H(W_2^{-1})^2H(W_3^{-1})^4$.

In Section 2 we shall briefly demonstrate the above process for elliptic curves. The main part of the paper is Section 3, where we give the formulas for the matrices W_1, W_2, W_3 (of step 4 above) for the Kummer surface of the Jacobian of a curve of genus 2.

§2. The x-coordinate Height on an Elliptic Curve

Let $\mathcal{E}$ be an elliptic curve given by:

$$\mathcal{E} : Y^2 = X^3 + AX^2 + BX + C, \quad A, B, C \in K \tag{1}$$

with nonzero discriminant. We choose to retain the X^2 term, so that when we later specialise to $C = 0$ our expressions will apply to a general curve containing the point $(0, 0)$. Let $P = (x, y) \in \mathcal{E}(K)$. Then define

$$\kappa : \mathcal{E}(K) \to \mathbb{P}^1(K) : P \mapsto \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \tag{2}$$

giving the map onto the projective x-coordinate (which for our purposes performs the role of the Kummer variety). The height H_κ is the usual x-coordinate height.

Definition 2.1. For any $P \in \mathcal{E}(K)$ define $H_\kappa(P) = H(\kappa(P))$. Define $M = (M_{ij}) \in \mathbb{M}^1(K[\mathbf{v}^2, \mathbf{w}^2])$, $N = (N_i) \in \mathbb{P}^1(K[\mathbf{v}^4])$ as follows.

$M_{00} = v_0^2 w_0^2 - 2Bv_1v_0w_1w_0 - 4C(v_1^2w_1w_0 + v_1v_0w_1^2) + (B^2 - 4AC)v_1^2w_1^2$.

$M_{10} = M_{01} = v_1v_0w_0^2 + v_0^2w_1w_0 + 2Av_1v_0w_1w_0 + B(v_1^2w_1w_0 + v_1v_0w_1^2) + 2Cv_1^2w_1^2$.

$M_{11} = v_1^2w_0^2 - 2v_1v_0w_1w_0 + v_0^2w_1^2$.

Define $N_0 = M(\mathbf{v}, \mathbf{v})_{00}$, $N_1 = 2M(\mathbf{v}, \mathbf{v})_{01}$, that is:

$N_0 = v_0^4 - 2Bv_1^2v_0^2 - 8Cv_1^3v_0 + (B^2 - 4AC)v_1^4$.

$N_1 = 4(v_1v_0^3 + Av_1^2v_0^2 + Bv_1^3v_0 + Cv_1^4)$.

The above formulas are standard [12] and satisfy the requirements of Lemma 1.9.

Lemma 2.2. *Let M, N be as in Definition 2.1. Then, for any $P, Q \in \mathcal{E}(K)$,*

$\big(\kappa_i(P+Q)\kappa_j(P-Q) + \kappa_j(P+Q)\kappa_i(P-Q)\big) = M(\kappa(P), \kappa(Q))$, *and* $\kappa(2P) = N(\kappa(P))$. *Hence H_κ is a height function on $\mathcal{E}(K)$, with $C_1 = 2H(M)$.* □

In order to determine the more difficult height constant C_2 on H_κ, there are two possible routes. One can either perform resultant calculations on the duplication law N to find the matrix R, as in the proof of Lemma 1.9, or one can use the isogeny approach described at the end of Section 1. The first approach is the one typically employed, either explicitly (as in [12], p.204) or implicitly by way of reference to Hilbert's Nullstellensatz applied to N. The matrix R is straightforward to compute; one first computes the resultant of N_0, N_1 with respect to v_1, giving polynomials $R_{00}, R_{01} \in K[\mathbf{v}^3]$ such that $R_{00}N_0 + R_{01}N_1 = v_0^7$. Similarly, one computes the resultant of N_0, N_1 with respect to v_0 to give polynomials $R_{10}, R_{11} \in K[\mathbf{v}^3]$ such that $R_{10}N_0 + R_{11}N_1 = v_1^7$. Hence $R \cdot N = \binom{v_0^7}{v_1^7}$, so that $R = (R_{ij})$ is as in the proof of Lemma 1.9. It follows that we can take $C_2 = H(R)$. The polynomials R_{ij} are given explicitly in [12], and we do not reproduce them here.

The above provides a perfectly good method for computing the height constants C_1, C_2 of an elliptic curve; however, we shall briefly give the isogeny approach as an alternative since it indicates a simplified version of the methodology which will be required in Section 3. We wish to factor the duplication map via 2-isogeny. We first let L be a finite extension

of K such that $\mathcal{E}(L)$ contains a point of order 2. We can write $\mathcal{E}$ over L as:

$$\mathcal{E} : Y^2 = X^3 + aX^2 + bX, \quad a, b \in L,\ b(a^2 - 4b) \neq 0. \tag{3}$$

The following curve $\widehat{\mathcal{E}}$ is isogenous to $\mathcal{E}$.

$$\widehat{\mathcal{E}} : Y^2 = X^3 + \hat{a}X^2 + \hat{b}X, \text{ where } \hat{a} = -2a,\ \hat{b} = a^2 - 4b. \tag{4}$$

The isogeny $\phi : \mathcal{E} \longrightarrow \widehat{\mathcal{E}} : (x, y) \mapsto \left((x^2 + ax + b)/x, y - by/x^2\right)$ has kernel $\{\infty, (0, 0)\}$ and induces a map ϕ_x on the projective x-coordinate given by:

$$\phi_x : \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \mapsto \begin{pmatrix} v_0^2 + av_0v_1 + bv_1^2 \\ v_0v_1 \end{pmatrix}. \tag{5}$$

We shall also include $\sqrt{b}, \sqrt{\hat{b}}$ in our finite field extension L. We note that translation by $(0, 0)$ induces the map $T : x \mapsto b/x$ on the affine x-coordinate, which can be represented as the matrix $T = \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right) \in \mathbb{M}^1(L)$ on the projective x-coordinate $\left(\begin{smallmatrix} v_0 \\ v_1 \end{smallmatrix}\right)$. Taking eigenvectors of T motivates a change of basis to $\mathbf{v}'$ given by:

$$\mathbf{v}' = \begin{pmatrix} v_0' \\ v_1' \end{pmatrix} = W_3 \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \text{ where } W_3 = \begin{pmatrix} 1 & \sqrt{b} \\ 1 & -\sqrt{b} \end{pmatrix}. \tag{6}$$

The map T is now diagonalised as: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and so the composition τW_3, where $\tau : \left(\begin{smallmatrix} v_0 \\ v_1 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} v_0^2 \\ v_1^2 \end{smallmatrix}\right)$, gives a quadratic map which is invariant under T. It is therefore sufficient to compose τW_3 with a further linear map to obtain ϕ_x. Explicitly, it is easy to verify that:

$$\phi_x = V\tau W_3, \text{ where } V = \begin{pmatrix} 2\sqrt{b} + a & 2\sqrt{b} - a \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1/\sqrt{b} & -1/\sqrt{b} \end{pmatrix}. \tag{7}$$

Further, if we let $\widehat{V}$, $\widehat{W_3}$ represent the corresponding objects on $\widehat{\mathcal{E}}$ (that is to say, with a, b replaced by $\hat{a}$, $\hat{b}$, respectively), then:

$$\hat{\phi}_x = U\widehat{V}\tau\widehat{W_3}, \text{ where } U = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}. \tag{8}$$

Finally, since the duplication map N is $\hat{\phi}_x \circ \phi_x$, we can write N in the required form:

$$N = W_1\tau W_2\tau W_3, \text{ where: } W_1 = U\widehat{V} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 2\sqrt{\hat{b}} + \hat{a} & 2\sqrt{\hat{b}} - \hat{a} \\ 1 & -1 \end{pmatrix},$$

$$W_2 = \widehat{W}_3 V = \begin{pmatrix} 1 & \sqrt{\hat{b}} \\ 1 & -\sqrt{\hat{b}} \end{pmatrix} \begin{pmatrix} 2\sqrt{b}+a & 2\sqrt{b}-a \\ 1 & -1 \end{pmatrix}, \; W_3 = \begin{pmatrix} 1 & \sqrt{b} \\ 1 & -\sqrt{b} \end{pmatrix}. \tag{9}$$

It is straightforward to verify that $N = \binom{N_0}{N_1}$ of Definition 2.1, with $A = a$, $B = b$, $C = 0$, is the same as $W_1 \tau W_2 \tau W_3 \mathbf{v}$ above. It follows that we can compute both height constants as $C_1 = 2H(M)$, $C_2 = H(W_1^{-1})H(W_2^{-1})^2 H(W_3^{-1})^4$, without needing to find the resultant polynomials R on the duplication law. It is not claimed that, for elliptic curves, the above provides a better method; however, in the higher genus situation there is a dramatic difference beween the viability of the analogous approaches.

§3. The Kummer Surface Height on the Jacobian of a Curve of Genus 2

Let $\mathcal{C}$ be a curve of genus 2 over a number field K given by:

$$\mathcal{C} : Y^2 = \mathsf{F}_6 X^6 + \mathsf{F}_5 X^5 + \mathsf{F}_4 X^4 + \mathsf{F}_3 X^3 + \mathsf{F}_2 X^2 + \mathsf{F}_1 X + \mathsf{F}_0, \tag{10}$$

where $\mathsf{F}_0, \ldots, \mathsf{F}_6 \in K$ and $F(X)$ has nonzero discriminant. A $\overline{K}$-rational point on the Jacobian of $\mathcal{C}$, denoted $\mathcal{J} = \mathcal{J}(\mathcal{C}) = \mathrm{Pic}^0(\mathcal{C})$, can be represented by a divisor of the form: $(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-$, where (x_1, y_1), (x_2, y_2) are any points on $\mathcal{C}$ including ∞^+ and ∞^-. We shall follow [4] and use as a shorthand notation the unordered pair $\{(x_1, y_1), (x_2, y_2)\}$. This representation sets up a one-to-one correspondence with members of $\mathcal{J}(\overline{K})$, except that the canonical equivalence class of pairs of the form $\{(x, y), (x, -y)\}$ represents a single menber of $\mathcal{J}(\overline{K})$, denoted $\mathcal{O}$. The members of $\mathcal{J}(\overline{K})$ form a group as follows:

(i). $\mathcal{O}$ serves as the group identity; **(ii).** $-\{(x_1, y_1), (x_2, y_2)\} = \{(x_1, -y_1), (x_2, -y_2)\}$;

(iii). $\{(x_1, y_1), (x_2, y_2)\} + \{(x_3, y_3), (x_4, y_4)\} + \{(x_5, y_5), (x_6, y_6)\} = \mathcal{O}$ if there exists a function of the form $Y =$ cubic in X which meets $\mathcal{C}$ at the points $(x_1, y_1), \ldots (x_6, y_6)$.

The Mordell-Weil group of $\mathcal{J}(\overline{K})$ over K, denoted $\mathcal{J}(K)$, is the subgroup of $\mathcal{J}(\overline{K})$ consisting of K-rational divisors (that is to say, pairs for which (x_1, y_1), (x_2, y_2) are either both defined over K, or are quadratic over K and conjugate). There is a map κ from the group $\mathcal{J}(K)$ into $\mathbb{P}^3(K)$ given by:

$$\kappa : \mathcal{J}(K) \longrightarrow \mathbb{P}^3(K) : \{(x_1, y_1), (x_2, y_2)\} \mapsto \mathbf{v} = \begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix}, \tag{11}$$

where $v_0 = \big(\mathcal{F}(x_1,x_2) - 2y_1y_2\big)/(x_1-x_2)^2,\ \ v_1 = 1,\ \ v_2 = x_1+x_2,\ \ v_3 = x_1x_2,$

$$\begin{aligned}\text{and where } \mathcal{F}(x_1,x_2) =& 2\mathsf{F}_0 + \mathsf{F}_1(x_1+x_2) + 2\mathsf{F}_2x_1x_2 + \mathsf{F}_3x_1x_2(x_1+x_2)\\ &+ 2\mathsf{F}_4(x_1x_2)^2 + \mathsf{F}_5(x_1x_2)^2(x_1+x_2) + 2\mathsf{F}_6(x_1x_2)^3.\end{aligned}$$

The image of this map is the set of K-rational points on a Kummer surface, which will perform the same role as the projective x-coordinate on an elliptic curve. Note that $\kappa(\mathcal{O}) = \left(\begin{smallmatrix}1\\0\\0\\0\end{smallmatrix}\right)$ and that κ identifies $\pm$, being injective on the points of order 2 of $\mathcal{J}(k)$, and a 2-to-1 map elsewhere. Recent work in [5] uses computer symbolic algebra to find objects analogous to M, N of Defintion 2.1 for a general curve of genus 2. These are given explicitly in Appendices B, C of [5], and we do not reproduce them here.

Lemma 3.1. *Let $M \in \mathbb{M}^3(K[\mathbf{v}^3])$, $N \in \mathbb{P}^3(K[\mathbf{v}^4])$ be as given in Appendices B, C of [5]. Then, for any $P,Q \in \mathcal{J}(K)$: $\big(\kappa_i(P+Q)\kappa_j(P-Q)+\kappa_j(P+Q)\kappa_i(P-Q)\big) = M(\kappa(P),\kappa(Q))$ and $\kappa(2P) = N(\kappa(P))$.* □

Lemma 3.1. *For any $P \in \mathcal{J}(K)$, define $H_\kappa(P) = H(\kappa(P))$. Then H_κ is a height function on $\mathcal{J}(K)$.* □

It remains to provide a method for computing the height constants C_1, C_2 of Definition 1.1. As usual, we can take $C_1 = 2H(M)$, where M is the matrix given in Lemma 3.1.; however, the constant C_2 is more difficult. In theory, we can appeal (as with elliptic curves) to Hilbert's Nullstellensatz, which guarrantees the existence of a matrix $R \in \mathbb{M}^3(K[\mathbf{v}^r])$, for some $r \in \mathbb{Z}^+$, such that $R \cdot N = (v_i^{r+4})$. However, as indicated in Section 1, we must instead use isogenies to express the duplication law N on the Kummer surface as: $N = W_1\tau W_2\tau W_3\mathbf{v}$, for matrices $W_1, W_2, W_3 \in \mathbb{M}^3(L)$, where L is a finite extension of K. The remainder of this section is devoted to the derivation of W_1, W_2, W_3.

We first observe ([2], p.41) that points of order 2 on the Jacobian in our notation are of the form: $\{(x_1,0),(x_2,0)\}$, where x_1, x_2 are distinct roots of sextic in equation (10). There are 15 such divisors over the algebraic closure $\overline{K}$, which together with $\mathcal{O}$ give all 16 members of the 2-torsion group. It follows that there is a point of order 2 corresponding to any given quadratic factor of this sextic. We therefore write $\mathcal{C}$ over a finite extension L in the form $Y^2 = q_1(X)q_2(X)q_3(X)$, where each $q_i(X)$ is a quadratic in X (this is analogous to equation (3) in Section 2). The Jacobian of $\mathcal{C}$ has a subgroup of four 2-torsion points,

including $\mathcal{O}$, which will form the kernel of our isogeny. We recall the following isogeny on $\mathcal{J}(\mathcal{C})$ described in [1].

Definition 3.3. Let K be the ground field of $\mathcal{C}$ as expressed in the form $Y^2 =$ sextic in X (as in equation (10)). Write $\mathcal{C}$ over a finite extension of K as:

$$\mathcal{C} : Y^2 = q_1(X)q_2(X)q_3(X) = (f_1X^2+g_1X+h_1)(f_2X^2+g_2X+h_2)(f_3X^2+g_3X+h_3). \quad (12)$$

For any two polynomials $p(X)$, $q(X)$, let $[p, q]$ denote $p'q - pq'$. Define $\widehat{\mathcal{C}}$ by:

$$\widehat{\mathcal{C}} : \Delta Y^2 = \hat{q}_1(X)\hat{q}_2(X)\hat{q}_3(X) = [q_2, q_3][q_3, q_1][q_1, q_2], \text{ where } \Delta = \begin{vmatrix} h_1 & g_1 & f_1 \\ h_2 & g_2 & f_2 \\ h_3 & g_3 & f_3 \end{vmatrix}.$$

For distinct i, j, k, denote $b_{ij} = \text{resultant}(q_i, q_j)$, $b_i = b_{ij}b_{ik}$, $\hat{b}_{ij} = \text{resultant}(\hat{q}_i, \hat{q}_j)$, $\hat{b}_i = \hat{b}_{ij}\hat{b}_{ik}$. Define $L = K(f_i, g_i, h_i, \sqrt{b_i}, \sqrt{\hat{b}_i})$, a finite extension of K. Let $\mathcal{J}$, $\widehat{\mathcal{J}}$ be the Jacobians of $\mathcal{C}$ and $\widehat{\mathcal{C}}$, and let κ, $\hat{\kappa}$ be the corresponding Kummer surfaces embedded into $\mathbb{P}^3$ as in equation (9). Finally, α_i denotes the point of order 2 in $\mathcal{J}(L)$ corresponding to $q_i(X)$; similarly for $\hat{\alpha}_i$.

It has been shown in [1] that $\mathcal{J}$, $\widehat{\mathcal{J}}$ are isogenous. There exists isogenies: $\phi : \mathcal{J} \to \widehat{\mathcal{J}}$ with kernel $\{\mathcal{O}, \alpha_1, \alpha_2, \alpha_3\}$ and $\hat{\phi} : \widehat{\mathcal{J}} \to \mathcal{J}$ with kernel $\{\widehat{\mathcal{O}}, \hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3\}$, such that $\hat{\phi}\circ\phi = [2]$, the duplication map on $\mathcal{J}$. The nice relationship between the underlying curves, $\mathcal{C}$ and $\widehat{\mathcal{C}}$, seems rather special to the genus 2 situation, and so we shall deliberately not make use of the description of the isogeny in [1] (which in any case is in terms of divisors, and not in a form suitable for our purposes); instead, we shall imitate the linear algebra in Section 2 in a form which, we hope, will be amenable to future generalisation to genus > 2. The style of our identities will be motivated by identities of theta functions as in [8] or [10]. We first note that the isogeny ϕ, the duplication map [2], and the maps $P \mapsto P +$ (fixed point of order 2) all remain well defined after taking the quotient by $\pm$; hence all of these give well defined induced maps on the Kummer surface (just as for the projective x-coordinate on an elliptic curve). We wish to expess the induced isogenies on the Kummer surfaces, $\phi_\kappa : \kappa \to \hat{\kappa}$ and $\hat{\phi}_\kappa : \hat{\kappa} \to \kappa$ (and hence the duplication law on the Kummer surface) in the same form as equation (7) of Section 2; that is, as compositions of $\tau : (v_i) \mapsto (v_i^2)$ and linear maps. We let $T_i : \kappa(P) \mapsto \kappa(P + \alpha_i)$, for $i = 1, 2, 3$. These are represented by matrices in $\mathbb{P}^3(L)$ (analogous to the matrix $T = \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right)$ in Section 2) which

are given explicitly in [5], Appendix *A*. The matrices T_1, T_2, T_3 commute and so can be simultaneously diagonalised. We use the standard function ϵ_{ijk}, where $\epsilon_{ijk} = 0$, when any of i, j, k are equal and is otherwise the sign of the permutation $1 \mapsto i, 2 \mapsto j, 3 \mapsto k$. For any function $\psi(i, j, k)$, we use the notation:

$$\langle \psi(i,j,k) \rangle = \sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} \epsilon_{ijk} \psi(i,j,k).$$

For example, in this notation, $\Delta = \langle f_i g_j h_k \rangle$. Let $W_3 \in \mathbb{P}^3(L)$ be given as the following product of matrices.

$$W_3 = \begin{pmatrix} 1 & \sqrt{b_1} & \sqrt{b_2} & \sqrt{b_3} \\ 1 & \sqrt{b_1} & -\sqrt{b_2} & -\sqrt{b_3} \\ 1 & -\sqrt{b_1} & \sqrt{b_2} & -\sqrt{b_3} \\ 1 & -\sqrt{b_1} & -\sqrt{b_2} & \sqrt{b_3} \end{pmatrix} \cdot$$
$$\begin{pmatrix} \Delta & \langle g_i h_i (f_k^2 h_j^2 + f_j g_k^2 h_j) \rangle & \langle f_i h_i (f_k^2 h_j^2 + f_j g_j g_k h_k) \rangle & \langle f_i g_i (f_k g_j^2 h_k + f_k^2 h_j^2) \rangle \\ 0 & g_3 h_2 - g_2 h_3 & f_3 h_2 - f_2 h_3 & f_3 g_2 - f_2 g_3 \\ 0 & g_1 h_3 - g_3 h_1 & f_1 h_3 - f_3 h_1 & f_1 g_3 - f_3 g_1 \\ 0 & g_2 h_1 - g_1 h_2 & f_2 h_1 - f_1 h_2 & f_2 g_1 - f_1 g_2 \end{pmatrix} \tag{13}$$

Then the change of basis W_3 (analogous to that in equation (6)) diagonalises T_1, T_2, T_3 as $\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&-1&0 \\ 0&0&0&-1 \end{pmatrix}$, $\begin{pmatrix} 1&0&0&0 \\ 0&-1&0&0 \\ 0&0&1&0 \\ 0&0&0&-1 \end{pmatrix}$, $\begin{pmatrix} 1&0&0&0 \\ 0&-1&0&0 \\ 0&0&-1&0 \\ 0&0&0&1 \end{pmatrix}$, respectively. Composition with $\tau : (v_i) \mapsto (v_i^2)$ gives a quadratic map on κ which is invariant under T_1, T_2, T_3. Only a further linear map is required to give the isogeny $\phi_\kappa : \kappa \to \hat{\kappa}$. In fact: $\phi_\kappa = V \tau W_3$, where

$$V = \begin{pmatrix} 2\Delta & \langle 4 f_i f_k g_k h_i h_k^2 + 2 f_i^2 g_j h_j h_k^2 \rangle & \langle 2 f_i f_k^2 h_i h_j^2 \rangle & \langle 4 f_i f_k^2 g_j h_i h_j + 2 f_i f_k^2 g_i h_j^2 \rangle \\ 0 & \Delta & 0 & 0 \\ 0 & 0 & \Delta & 0 \\ 0 & 0 & 0 & \Delta \end{pmatrix} \cdot$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -f_1 & -f_2 & -f_3 \\ 0 & g_1 & g_2 & g_3 \\ 0 & -h_1 & -h_2 & -h_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1/\sqrt{b_1} & 1/\sqrt{b_1} & -1/\sqrt{b_1} & -1/\sqrt{b_1} \\ 1/\sqrt{b_2} & -1/\sqrt{b_2} & 1/\sqrt{b_2} & -1/\sqrt{b_2} \\ 1/\sqrt{b_3} & -1/\sqrt{b_3} & -1/\sqrt{b_3} & 1/\sqrt{b_3} \end{pmatrix} \tag{14}$$

Let $\widehat{W_3}$, $\widehat{V}$ be the corresponding objects on $\hat{\kappa}$; that is to say, W_3, V with f_i, g_i, h_i, b_i replaced by $\hat{f}_i$, $\hat{g}_i$, $\hat{h}_i$, $\hat{b}_i$. Then:

$$\hat{\phi}_\kappa = U \widehat{V} \tau \widehat{W_3} \text{ where } U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}. \tag{15}$$

Since $[2] = \hat{\phi}_\kappa \circ \phi_\kappa$ on κ, we now have the duplication law expressed in the desired form.

Theorem 3.4. *Let W_3, $\widehat{W_3}$, V, $\widehat{V}$, U be as above. Let $W_1 = U\widehat{V}$, $W_2 = \widehat{W_3}V$. Then the duplication law $N = W_1\tau W_2\tau W_3\mathbf{v}$.* □

The above identity may be verified by use of a symbolic algebra package.

Corollary 3.5. *Let M be as in Lemma 3.1, and W_1, W_2, W_3 be as in Theorem 3.4. Then H_κ is a height function on $\mathcal{J}(K)$, with height constants given by: $C_1 = 2H(M)$ and $C_2 = H(W_1^{-1})H(W_2^{-1})^2H(W_3^{-1})^4$.* □

Quite aside from the application to the theory of heights, the equation $[2] = W_1\tau W_2\tau W_3$ provides a considerably more concise description of the duplication law than the large quartic forms in [5].

§4. Worked Examples

We first observe the following technical lemma (proved by a straightforward induction on n) which will speed the height computations.

Lemma 4.1. *Let H be a height function on an abelian group G, with height constants C_1, C_2, as in Definition 1.1. Then, for any $Q \in G$ and any positive integer n, we have: $H(Q) \leqslant C_1^{1/6n}H(nQ)^{1/n^2}C_2^{17/50}$. For any $\epsilon > 0$, there exists an N such that, for all $n \geqslant N$, $H(Q) \leqslant H(nQ)^{1/n^2}C_2^{1/3+\epsilon}$.* □

Let us suppose, for example, that we have performed a 2-descent on $\mathcal{J}(\mathbb{Q})$ to find $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, that the rank has been found to be 1, and that we have also determined the torsion group $\mathcal{J}_{\mathrm{tors}}(\mathbb{Q})$. There are several instances of precisely this situation in the literature [6],[7]. In this case, we will already have found a non-torsion $P \in \mathcal{J}(\mathbb{Q})$, and we would like to show that P, together with $\mathcal{J}_{\mathrm{tors}}(\mathbb{Q})$, actually generate $\mathcal{J}(\mathbb{Q})$. Any alternative generator of infinite order, $Q \in \mathcal{J}(\mathbb{Q})$, would have to satisfy $P + P' = nQ$ for some odd $n \geqslant 3$, and some $P' \in \mathcal{J}_{\mathrm{tors}}(\mathbb{Q})$. Specific values of n up to some N can be shown impossible by arguments using finite field reductions, and so Lemma 4.1 can be applied to show $H(Q) \leqslant H(P+P')^{1/N^2}C_2^{1/3+\epsilon}$. Since there are only a finite number of choices for $P+P'$, we can incorporate $H(P+P')$ into the ϵ. In this situation, we therefore need only search through points with height up to $C_2^{1/3+\epsilon}$; if all such points turn out to be generated by P and $\mathcal{J}_{\mathrm{tors}}(\mathbb{Q})$, then we can deduce that these generate all of $\mathcal{J}(\mathbb{Q})$. It is apparent that a crude upper bound for C_1 is sufficient, whereas a sharp value for C_2 is desirable.

Example 4.2. *Let $\mathcal{C} : Y^2 = (X^2+1)(X^2+2)(X^2+X+1)$. Then $\mathcal{J}(\mathbb{Q})$ has rank 1 and is generated by $P = \{\infty^+, \infty^+\}$, of infinite order, together with $\mathcal{J}_{\text{tors}}(\mathbb{Q}) = \{\mathcal{O}, \alpha_1, \alpha_2, \alpha_3\}$, the points of order 2.*

Proof. It was shown in [6] that $\mathcal{J}(\mathbb{Q})$ has rank 1, and that the above points generate $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. In the notation of Definition 3.3, we have: $\Delta = -2$, $b_1 = 1$, $b_2 = 3$, $b_3 = 3$, $\hat{b}_1 = 24$, $\hat{b}_2 = 12$ and $\hat{b}_3 = 32$. On specialising the matrices of Theorem 3.4, we see that the duplication law on κ is given by $\mathbf{v} \mapsto W_1\tau W_2\tau W_3\mathbf{v}$, where:

$$W_1 = \begin{pmatrix} -\sqrt{6} & -\sqrt{6} & -\sqrt{6} & -\sqrt{6} \\ 1-\sqrt{2} & 1+\sqrt{2} & -1-\sqrt{2} & -1+\sqrt{2} \\ 2+\sqrt{3} & 2-\sqrt{3} & -2-\sqrt{3} & -2+\sqrt{3} \\ -2+\sqrt{2} & -2-\sqrt{2} & 2+\sqrt{2} & 2-\sqrt{2} \end{pmatrix}, W_3 = \begin{pmatrix} 1 & 1+\sqrt{3} & -1+\sqrt{3} & 4-\sqrt{3} \\ 1 & 1-\sqrt{3} & -1-\sqrt{3} & 4+\sqrt{3} \\ 1 & 5+\sqrt{3} & 1-\sqrt{3} & 2-\sqrt{3} \\ 1 & 5-\sqrt{3} & 1+\sqrt{3} & 2+\sqrt{3} \end{pmatrix},$$

$$W_2 = \begin{pmatrix} 1-\sqrt{3}-\sqrt{6} & -9-7\sqrt{2}+5\sqrt{3}+4\sqrt{6} & 5+3\sqrt{2}-3\sqrt{3}-2\sqrt{6} & 3+2\sqrt{2}-\sqrt{3}-\sqrt{6} \\ 9-7\sqrt{2}+5\sqrt{3}-4\sqrt{6} & -1-\sqrt{3}+\sqrt{6} & -3+2\sqrt{2}-\sqrt{3}+\sqrt{6} & -5+3\sqrt{2}-3\sqrt{3}+2\sqrt{6} \\ -1-\sqrt{3}+\sqrt{6} & 9-7\sqrt{2}-5\sqrt{3}+4\sqrt{6} & -5+3\sqrt{2}+3\sqrt{3}-2\sqrt{6} & -3+2\sqrt{2}+\sqrt{3}-\sqrt{6} \\ -9-7\sqrt{2}-5\sqrt{3}-4\sqrt{6} & 1+\sqrt{3}+\sqrt{6} & 3+2\sqrt{2}+\sqrt{3}+\sqrt{6} & 5+3\sqrt{2}+3\sqrt{3}+2\sqrt{6} \end{pmatrix}.$$

These matrices could be used directly to obtain a value for C_2 on H_κ; however, a computational improvement can be obtained by a change of basis on κ, in which we take advantage of the fact that the f_i, g_i, h_i are defined over $\mathbb{Q}$. Define $\varsigma : \mathcal{J}(\mathbb{Q}) \longrightarrow \mathbf{P}^3 : P \mapsto \mathbf{s} = (s_i) = S \cdot \kappa(P)$, where $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & -2 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 3 & 1 & -1 & 0 \end{pmatrix}$, and let H_ς be the induced height function on $\mathcal{J}(\mathbb{Q})$, given by: $H_\varsigma(P) = H\big(\varsigma(P)\big)$. The matrix S is the right hand member of the product in equation (13). The duplication law on ς is given by $W_1'\tau W_2'\tau W_3'$, where $W_1' = S^{-1} \cdot W_1$, $W_2' = W_2$ and $W_3' = W_3 \cdot S$. This has the advantage that $H_\varsigma\big((W_3')^{-1}\big) < H_\kappa(W_3^{-1})$, giving a smaller value for C_2. In fact, we obtain $C_2 \leqslant 1.454 \times 10^8$ for H_ς on $\mathcal{J}(\mathbb{Q})$. On specialising the biquadratic forms in [5] (adjusting for the change in basis), we obtain the bound $C_1 \leqslant 3920$ for H_ς on $\mathcal{J}(\mathbb{Q})$.

Now, suppose that P, above, and $\mathcal{J}_{\text{tors}}(\mathbb{Q})$ do not generate $\mathcal{J}(\mathbb{Q})$. Then there would have to exists a point $Q \in \mathcal{J}(\mathbb{Q})$ such that $P = nQ$, for some odd n. By standard arguments using finite field reductions, this can be shown to be impossible for all $n \leqslant 30$. We can apply Lemma 4.1 to bound $H_\varsigma(Q) \leqslant 600$ (close to $C_2^{1/3} \approx 526$). We note that, for any $\mathbf{s} = (s_i) \in \varsigma(\mathcal{J})$, the value of s_3 can easily be computed biuniquely in terms of s_0, s_1, s_2. Therefore, our search is amongst triples: s_0, s_1, s_2 where each is an integer with absolute value $\leqslant 600$. A few simple congruence considerations reduce the number of triples, so that

finally about 10^7 integer triples need to be checked. It was found that all members of $\mathcal{J}(\mathbb{Q})$ which mapped under ς into the search area, were generated by P and $\mathcal{J}_{\rm tors}(\mathbb{Q})$. Hence all of $\mathcal{J}(\mathbb{Q})$ is generated by these points, as required. □

Using the same approach, the following two Jacobians have also been resolved.

Example 4.3. *Let $\mathcal{C} : Y^2 = (X^2+1)(X^2+2)(X^2+2X+2)$. Then $\mathcal{J}(\mathbb{Q})$ is generated by $P = \{\infty^+, \infty^+\}$ of infinite order, together with $\mathcal{J}_{\rm tors}(\mathbb{Q}) = \{\mathcal{O}, \alpha_1, \alpha_2, \alpha_3\}$, the points of order 2 (it was shown in [6] that these generate $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$).* □

Example 4.4. *Let $\mathcal{C} : Y^2 = X(X-1)(X-2)(X-5)(X-6)$. Then $\mathcal{J}(\mathbb{Q})$ is generated by $P = \{(3,6), \infty\}$ of infinite order, together with $\mathcal{J}_{\rm tors}(\mathbb{Q})$, which consists of the full 2-torsion group of size 16 (it was shown in [7] that these generate $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$).* □

It should be conceded that, in its current form, the above method will only cope with curves with small coefficients. However, our approach should be taken merely as a rough first approximation. There are numerous enhancements available for elliptic curves (see [3], 55-61), and work is in progress towards adapting some of these, so that we hope there will eventually be a theory of heights able to complement the increasingly efficient techniques available for computing $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ via Galois descent.

REFERENCES

[1] Bost, J. B. and Mestre, J.-F. *Moyenne arithmético-géometrique et périodes des courbes de genre 1 et 2.* Gaz. Math. Soc. France, **38** (1988), 36-64.

[2] Cassels, J. W. S. *The Mordell-Weil Group of Curves of Genus 2.* Arithmetic and Geometry papers dedicated to I. R. Shafarevich on the occasion of his sixtieth birthday, Vol. **1.** Arithmetic, 29-60, Birkhäuser, Boston (1983).

[3] Cremona, J. E. *Algorithms for modular elliptic curves.* Cambridge University Press (1992).

[4] Flynn, E. V. *The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field.* Math. Proc. Camb. Phil. Soc. **107** (1990), 425-441.

[5] Flynn, E. V. *The group law on the Jacobian of a curve of genus 2.* J. Reine Angew. Math. **438** (1993), 45-69.

[6] Flynn, E. V. *Descent via isogeny on the Jacobian of a curve of genus 2.* Acta Arith. (to appear).

[7] Gordon, D.M. and Grant, D. *Computing the Mordell-Weil rank of Jacobians of curves of genus 2.* Transactions of the American Mathematical Society (to appear).

[8] Hudson, R. W. H. T., *Kummer's Quartic Surface*, Cambridge University Press (1905). Reprint, 1990.

[9] Masser, D. and Wüstholz, G., *Fields of large transcendence degree generated by the values of elliptic functions.* Invent. Math. **72** (1983), 407-464.

[10] Mumford, D. *Tata Lectures on Theta.* Progress in Mathematics, I, **28** and II, **43**, Birkhäuser, Boston (1983).

[11] Schaefer, E.F. *2-descent on the Jacobians of hyperelliptic curves.* J. Number Theory (to appear).

[12] Silverman, J. H. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York (1986).

Prof. E.V. Flynn

Mathematical Institute

University of Oxford

Oxford OX1 3LB

United Kingdom

flynn@maths.ox.ac.uk