EXPLICIT KUMMER VARIETIES OF HYPERELLIPTIC JACOBIAN THREEFOLDS

J. STEFFEN MÜLLER

Abstract. We explicitly construct the Kummer variety associated to the Jacobian of a hyperelliptic curve of genus 3 that is defined over a field of characteristic not equal to 2 and has a rational Weierstraß point defined over the same field. We also construct homogeneous quartic polynomials on the Kummer variety and conjecture that they represent the duplication map.

1. Introduction

Let A be an abelian variety of dimension $g \geq 1$, defined over a field k. The quotient of A by the map taking a point on A to its inverse is a singular projective variety which can also be defined over k and which can be embedded into $\mathbb{P}^{2^g-1}$. It is called the *Kummer variety* K associated to A. The complex case is discussed in [1, §4.8].

If A is an elliptic curve, then K is simply the projective line over k. If A is the Jacobian of a genus 2 curve C, then this construction yields the classical singular Kummer surface, which can be embedded as a projective hypersurface into $\mathbb{P}^3$. In the case where $\mathrm{char}(k) \neq 2$ and C is given by an equation of the form $y^2 = f(x)$, an embedding and defining equation of the Kummer surface has been constructed by Flynn [6], see also the exposition in Chapter 3 of the book [2] by Cassels-Flynn.

A particular useful feature of K is that parts of the group structure remain meaningful on K. For instance, translation by a 2-torsion point and multiplication by an integer n on A commute with negation and hence descend to well-defined maps on K. Moreover, one can define a pseudoaddition on K using certain biquadratic forms B_{ij}. Formulas for duplication, translation by a 2-torsion point and pseudoaddition have also been found by Flynn [6] and can be downloaded from `http://people.maths.ox.ac.uk/flynn/genus2/kummer/`. Analogues of these for the case $\mathrm{char}(k) = 2$ have been found by Duquesne [4] and, independently, a unified treatment for arbitrary k and arbitrary defining equations $y^2 + h(x)y = f(x)$ of C has been presented by the author in [12].

In the present paper we discuss analogues of these objects for Jacobians of hyperelliptic curves of genus 3 with a k-rational Weierstraß point. In this case an embedding of the Kummer variety into $\mathbb{P}^7$ has been constructed by Stubbs [19] and we recall his construction in Section 2. We find a complete set of defining equations for the image of K under this embedding in Section 3; it turns out that K can be defined as the intersection of one quadric and 34 quartics in $\mathbb{P}^7$.

In Section 4 we discuss traces of the group structure on the Jacobian that can be exhibited on the Kummer variety. Duquesne has constructed a matrix W_T representing translation by a 2-torsion point $T \in A$ on K. It turns out that biquadratic forms B_{ij} as in genus 2 cannot exist in our situation, see Proposition 4.1. However, building on work of Duquesne, we construct homogeneous

Date: November 29, 2012.

quartic polynomials $\delta_i \in k[x_1, \ldots, x_8]$ and conjecture, based on numerical evidence, that they represent duplication on K.

The formulas described in this paper are mostly too long to be reproduced here. They can be obtained from `http://www.math.uni-hamburg.de/home/js.mueller/#code`.

Stoll has recently announced the construction of a different embedding of K which is valid for arbitrary hyperelliptic genus 3 curves [18], see also `http://www.mathe2.uni-bayreuth.de/stoll/talks/Luminy2012.pdf`. Using this embedding, he has proved Conjecture 4.2 and Conjecture 4.5.

1.1. **Applications.** In genus 2, the Kummer surface has several arithmetic applications. The first application is an addition algorithm on A that uses pseudoaddition on K, see [7]. Suppose that k is a number field. Letting h denote the naive height on $\mathbb{P}^3_k$, we get an induced naive height on the Jacobian which can be used to search for points in $A(k)$ of bounded height. Stoll's program `j-points` which uses this approach is available from `http://www.mathe2.uni-bayreuth.de/stoll/programs/index.html`. Furthermore, this naive height can be used to define and compute a canonical height $\hat{h}$ on A, which has numerous applications. See Flynn-Smart [7] for the construction and a first algorithm for the computation of $\hat{h}$. Several refinements are presented by Stoll in [16] and [17] and by the author in his thesis [13, Chapter 3].

In our genus 3 situation, we do not have an explicit description of pseudoaddition and hence we do not get an addition algorithm on A. We do get a height function on K by restriction of the standard height function on $\mathbb{P}^7$ and an an induced naive height $h(P) = h(\kappa(P))$ on the Jacobian, where $\kappa : A \to K \hookrightarrow \mathbb{P}^7$ is discussed in Section 2. Using the defining equations of K presented in Section 3, we get an algorithm that lists all k-rational points on K or on A up to a given height bound. We can also define a canonical height function

$$\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h(\kappa(2^n P)).$$

If we assume Conjecture 4.5 which states that we know how to represent duplication on K, then one can prove analogs of several results from [17] and obtains an algorithm for the computation of $\hat{h}$ as in [17]. Further details are given in §4.4 of [13]. Algorithms which computes the canonical height on Jacobians of hyperelliptic curves of any genus have recently been introduced by Holmes [8] and the author [14]. However, these are not easily related to a naive height suitable for point searching, as is required by standard algorithms for saturation of finite index subgroups of the Mordell-Weil group, such as in [17]. A solution to this problem has recently been proposed by Holmes [9].

Acknowledgements. This work forms part of my PhD thesis [13] at the University of Bayreuth. I would like to thank my supervisor Michael Stoll for his constant help and encouragement and I would like to thank Sylvain Duquesne, Victor Flynn, Damiano Testa and Tzanko Matev for helpful conversations. Part of this work was done while I was visiting the Université Rennes I and the University of Oxford and I thank both institutions for their hospitality. Finally, I would like to acknowledge support from DFG through DFG grants STO 299/5-1 and KU 2359/2-1.

2. Embedding the Kummer variety

In his PhD thesis, Stubbs [19] has found an explicit embedding of the Kummer variety associated to the Jacobian of a hyperelliptic curve of genus 3 with a rational Weierstraß point into $\mathbb{P}^7$. In this

section we recall this embedding, also providing formulas for the image on K of non-generic points on the Jacobian.

We first fix some notation that we will use throughout this paper. Let k denote a field of characteristic $\mathrm{char}(k) \neq 2$. We consider a smooth projective hyperelliptic genus 3 curve C over k, given by an equation

$$Y^2 = F(X, Z), \tag{1}$$

in the weighted projective plane over k with respective weights 1, 4 and 1 assigned to the variables X, Y and Z, where

$$F(X,Z) = f_0Z^8 + f_1XZ^7 + f_2X^2Z^6 + f_3X^3Z^5 + f_4X^4Z^4 + f_5X^5Z^3 + f_6X^6Z^2 + f_7X^7Z$$

is a binary octic form in $k[X, Z]$ without multiple factors such that $\deg_X(F(X, 1)) = 7$. Then there is a unique point $\infty \in C$ whose Z-coordinate is 0. Every hyperelliptic genus 3 curve over k with a k-rational Weierstraß point has an equation of the form (1) over k. Let A denote the Jacobian of C and let K denote its Kummer variety.

Every point $P \in A$ has a representative of the form

$$(P_1) + (P_2) + (P_3) - 3(\infty), \tag{2}$$

where $P_1, P_2, P_3 \in C$ and this representation is unique unless two of the P_i are swapped or fixed by the hyperelliptic involution. We call a point $P \in A$ *generic* if P can be represented by an unordered triple of points $(x_1, y_1, 1), (x_2, y_2, 1), (x_3, y_3, 1) \in C$, where all x_i are pairwise distinct.

Let Θ denote the theta-divisor on A with respect to the point ∞. It is well-known that Θ is ample (cf. [**?**]) and that 2Θ is base point free (cf. [15, §II.6]). Hence a basis of $\mathcal{L}(2\Theta)$ gives an embedding of K. Note that $\mathcal{L}(2\Theta)$ is equivalent to a certain space of symmetric functions on C^3 with restrictions on the poles as in [5] or [19]. Using this approach, Stubbs [19, Chapter 3] has found the following basis $\kappa_1, \ldots, \kappa_8$ of the space $\mathcal{L}(2\Theta)$:

$$\begin{aligned}
\kappa_1 &= 1,\\
\kappa_2 &= x_1 + x_2 + x_3,\\
\kappa_3 &= x_1x_2 + x_1x_3 + x_2x_3,\\
\kappa_4 &= x_1x_2x_3,\\
\kappa_5 &= b_0^2 - f_7\kappa_2^3 + f_7\kappa_3\kappa_2 - f_6\kappa_2^2 + 3f_7\kappa_4 + 2f_6\kappa_3,\\
\kappa_6 &= \kappa_2b_0^2 + 2b_0b_1 - f_7\kappa_2^4 + 3f_7\kappa_3\kappa_2^2 - f_6\kappa_2^3 - f_7\kappa_3^2 - f_7\kappa_4\kappa_2 + 2f_6\kappa_3\kappa_2 - f_5\kappa_2^2\\
&\quad + 2f_5\kappa_3,\\
\kappa_7 &= b_1^2 - \kappa_3b_0^2 + f_7\kappa_3\kappa_2^3 - 2f_7\kappa_3^2\kappa_2 + f_6\kappa_3\kappa_2^2 + f_7\kappa_4\kappa_3 - f_6\kappa_3^2 + f_5\kappa_3\kappa_2 - 3f_5\kappa_4,\\
\kappa_8 &= \kappa_2b_1^2 + 2\kappa_3b_0b_1 + \kappa_4b_0^2 + f_7\kappa_3^2\kappa_2^2 - f_7\kappa_2^3\kappa_4 + f_7\kappa_2\kappa_3\kappa_4 - f_7\kappa_3^3 + f_6\kappa_3^2\kappa_2\\
&\quad - f_6\kappa_4\kappa_2^2 + f_5\kappa_3^2 - f_5\kappa_4\kappa_2,
\end{aligned}$$

where

$$\begin{aligned}
b_0 &= (x_1y_2 - x_2y_1 - x_3y_2 + x_3y_1 - x_1y_3 + x_2y_3)/d,\\
b_1 &= (x_3^2y_2 - x_3^2y_1 + x_2^2y_1 + y_3x_1^2 - y_2x_1^2 - y_3x_2^2)/d,\\
d &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3).
\end{aligned}$$

We define a map $\kappa : A \to \mathbb{P}^7$ by

$$\kappa(P) = (\kappa_1(P), \ldots, \kappa_8(P));$$

then κ defines an embedding of the Kummer variety into $\mathbb{P}^7$. We also provide formulas for the values of $\kappa(P)$ when P is not generic. Any $P \in A(k)$ can be represented as a pair of homogeneous forms

$$(A(X,Z), B(X,Z)),$$

where A, $B \in k[X,Z]$ have homogeneous degree 4 and 2, respectively. If P is generic, then b_0 and b_1 as defined above are simply the constant and linear coefficient of $B(X,1) \in k[X]$.

Suppose that P is generic, satisfying $x_1x_2x_3 \neq 0$, and write the $\kappa_i(P)$ in terms of $z_j = 1/x_j$ and $w_j = y_j/x_j$, $j \in \{1,2,3\}$. We then multiply by the common denominator and set $w_3 = 0$. This leads to the following formulas for P having a unique representative of the form $((x_1,y_1,1))+((x_2,y_2,1))-2(\infty)$ and satisfying $x_1 \neq x_2$:

$$\begin{aligned}
\kappa_1(P) &= 0,\\
\kappa_2(P) &= 1,\\
\kappa_3(P) &= x_1 + x_2,\\
\kappa_4(P) &= x_1x_2,\\
\kappa_5(P) &= f_5 + 2f_6\kappa_3(P) + f_7\kappa_3(P)^2 + 2\kappa_4(P)f_7,\\
\kappa_6(P) &= f_4 + f_5\kappa_3(P) - f_7\kappa_4(P)\kappa_3(P),\\
\kappa_7(P) &= -f_4\kappa_3(P) - 3f_5\kappa_4(P) + f_7\kappa_4(P)^2,\\
\kappa_8(P) &= \big(f_3\kappa_3(P)^3 + f_1\kappa_3(P) + f_2\kappa_3(P)^2 + 2f_0 - 2y_1y_2 + f_4\kappa_4(P)\kappa_3(P)^2 - 3f_3\kappa_4(P)\kappa_3(P)\\
&\quad -2f_2\kappa_4(P) + f_5\kappa_4(P)^2\kappa_3(P) - 2f_4\kappa_4(P)^2 + f_7\kappa_4(P)^3\kappa_3(P) + 2f_6\kappa_4(P)^3\big)/(x_1-x_2)^2.
\end{aligned}$$

For the case $x_1 = x_2$ it suffices to use the same $\kappa_1, \ldots, \kappa_7$ and

$$\kappa_8(P) = b_1^2 + (\kappa_4(P) - \kappa_3(P)^2)(-2f_7\kappa_4(P)\kappa_3(P) - f_6\kappa_4(P) + f_7\kappa_3(P)^3 + f_6\kappa_3(P)^2 + f_5\kappa_3(P) + f_4),$$

where b_1 is the linear coefficient of $B(X,1) \in k[X]$ if the Mumford representation of P is (A,B).

Now consider points represented by

$$((x_1,y_1)) - (\infty).$$

We first look at quotients of the form $\kappa_i(P)/\kappa_5(P)$, where P is again assumed generic, and then take the limit $(x_2,y_2,1) \to (x_3,-y_3,1)$.The result is

$$\kappa(P) = (0,0,0,0,1,-x_1,x_1^2,x_1^3).$$

A similar argument shows that we have

$$\kappa(O) = (0,0,0,0,0,0,0,1).$$

where $O \in A$ is the identity element.

If $P \in A$, then we say that $x = (x_1, \ldots, x_8) \in \mathbb{A}^8$ is a *set of Kummer coordinates for* P if $\kappa(P) = (x_1 : \ldots : x_8)$. We set

$$K_{\mathbb{A}} := \{(x_1, \ldots, x_8) \in \mathbb{A}^8 : \ \exists\, Q \in K \text{ such that } Q = (x_1 : \ldots : x_8)\}.$$

Remark 2.1. In the general case where $\deg_X(F(X,1)) = 8$ Stubbs constructs functions analogous to the functions κ_i. However, these do not give an embedding of the Kummer variety, since not all points on A can be represented by unordered triples of points on C. See [19, §3.8] for a discussion.

3. Defining equations for the Kummer variety

In this section we compute defining equations for the Kummer variety K, embedded into $\mathbb{P}^7$ as in the previous section.

The following result is well-known to the experts in algebraic geometry, but no proof seems to exist in the literature. The proof given here was suggested by Tzanko Matev.

Proposition 3.1. *Let A be a Jacobian variety of dimension $g \geq 2$ and let Θ be a theta-divisor on A. If $\kappa_1, \ldots, \kappa_{2^g}$ is a basis for $\mathcal{L}(2\Theta)$ and if $\kappa = (\kappa_1, \ldots, \kappa_{2^g}) : A \to \mathbb{P}^{2^g-1}$, then the image $\kappa(A)$ can be described as an intersection of quartics.*

Proof. Let $\mathcal{Q} = \{q_1, \ldots, q_m\}$ denote the set of monic quadratic monomials in the κ_i, where $m = \binom{2^g+1}{2}$ and we assume, without loss of generality, that $\{q_1, \ldots, q_d\}$ is linearly independent in the space $\mathbb{Q}(f_0, \ldots, f_7)[q_1, \ldots, q_m]$, where $d \leq m$ is the dimension of the space generated by the elements of $\mathcal{Q}$.

Let ι denote the 2-uple embedding of $\mathbb{P}^{2^g-1}$ into $\mathbb{P}^{m-1}$ such that for $P \in A$ we have

$$\iota_i(\kappa(P)) = q_i(P) \quad \text{for all } i \in \{1, \ldots, m\}.$$

Then there are $m - d$ linear relations on the image of $K = \kappa(A)$ under ι. Now consider an embedding $\beta : A \hookrightarrow \mathbb{P}^{4^g-1}$ given by a basis of $\mathcal{L}(4\Theta)$ whose first d elements are equal to $q_1, \ldots, q_d$. Then we have a commutative diagram

$$\begin{array}{ccc} A & \xhookrightarrow{\beta} & \mathbb{P}^{4^g-1} \\ {\scriptstyle\kappa}\downarrow & & \downarrow{\scriptstyle\gamma} \\ \mathbb{P}^{2^g-1} & \xhookrightarrow[\iota]{} & \mathbb{P}^{m-1} \end{array}$$

where γ is a rational map defined as follows: If $z = (z_1, \ldots, z_{4^g})$, then $\gamma(z) = y$, where $y_i = z_i$ for $i = 1, \ldots, d$ and the other y_i are determined by the linear relations on $\mathcal{Q}$. By construction, we have that $\beta(A)$ lies in the domain of γ and in fact

$$\gamma(\beta(A)) \cong \iota(\kappa(A)).$$

But it follows from the corollary on page 349 of [**?**] that the image of A under β is defined by an intersection of quadrics, which then must hold for $\gamma(\beta(A))$ as well, since γ has degree 1. As the pullback under ι of $\gamma(\beta(A))$ is isomorphic to K, the result follows. □

Hence it suffices to find a basis for the space of quartic relations on K to describe K. We first compute a lower bound on the dimension of this space. For $n \geq 1$ let $m(n)$ denote the number of monic monomials of degree n in $\kappa_1, \ldots, \kappa_{2^g}$ and let $d(n)$ denote the dimension of the space spanned by them. Then we have $m(n) = \binom{2^g+n-1}{n}$. Moreover, let $e(n)$ denote the dimension of the space of even functions in $\mathcal{L}(2n\Theta)$. By [1, Corollary 4.7.7] this is equal to $(2n)^g/2 + 2^{g-1}$. Since a monomial of degree n in the κ_i induces an even function in $\mathcal{L}(2n\Theta)$, we always have $d(n) \leq e(n)$.

In genus 2, the dimension count is given in Table 1.

n	$m(n)$	$e(n)$	$d(n)$
1	4	4	4
2	10	10	10
3	20	20	20
4	35	34	34

Table 1. Dimensions in genus 2

n	$m(n)$	$e(n)$	$d(n)$
1	8	8	8
2	36	36	35
3	120	112	112
4	330	260	260

Table 2. Dimensions in genus 3

We know that $d(4)$ can be at most $e(4) = 34$, and indeed the space of quartic relations in the κ_i is one-dimensional, spanned by the Kummer surface equation.

In genus 3, Stubbs has found the following quadratic relation between the κ_i and shown that it is unique up to scalars.

$$R_1 : \kappa_1\kappa_8 - \kappa_2\kappa_7 - \kappa_3\kappa_6 - \kappa_4\kappa_5 - 2f_5\kappa_2\kappa_4 + f_5\kappa_3^2 + 2f_6\kappa_3\kappa_4 + 3f_7\kappa_4^2 = 0 \tag{3}$$

The dimensions for genus 3 are presented in Table 2. The existence and uniqueness of R_1 implies that $d(2) = 35$, but since $e(2) = 36$, this means that there is an even function in $\mathcal{L}(4\Theta)$ not coming from a quadratic monomial in the κ_i, which does not happen in genus 2. Accordingly, we can at this point only bound $d(3)$ and $d(4)$ from above. However, by finding a curve C for which the space of cubic (resp. quartic) homogeneous polynomials has dimension exactly 112 (resp. 260), we can conclude that $d(3) = 112$ and $d(4) = 260$. For this one can use, for instance, the curve given by $Y^2 = Z^8 + X^7Z$.

It follows that in genus 3 there must be $70 = 330 - 260$ quartic relations on the Kummer variety. But 36 of these are multiples of the quadratic relation R_1. Moreover, there are only 8 cubic relations and they are all multiples of R_1. Hence there must be 34 independent irreducible quartic relations. In [19, Chapter 5] Stubbs lists 26 quartic relations and conjectures that together with R_1 these relations are independent and form a basis of the space of all relations on the Kummer variety. His relations are at most quadratic in $\kappa_5, \ldots, \kappa_8$. Using current computing facilities we can verify the former conjecture quite easily, but because of our dimension counting argument, we know that the latter conjecture cannot hold.

To compute a complete set of defining equations for the Kummer variety we employ the technique already used by Stubbs. Because of the enormous size of the algebra involved in these computations, simply searching for relations among all monomials is not feasible. Instead we split the monomials into parts of equal x-weight and y-weight. These are homogeneous weights discussed in [19, §3.5] that were already used by Flynn in [5] in order to derive quadratic relations defining a Jacobian surface in $\mathbb{P}^{15}$. See Table 3.
On monomials of equal x- and y-weight we can use linear algebra to find relations; we continue this process with increasing weights until we have found enough quartic relations to generate a space of

	x	y
x_i	1	0
y_i	0	1
f_i	$-i$	2
$\kappa_i, i \leq 4$	$i-1$	0
$\kappa_i, i > 4$	$i-9$	2

Table 3. x- and y-weight

dimension 70. The difficulty of this process depends essentially on the y-weight. We used `Magma` [11] to find 34 relations $R_2, \ldots, R_{35}$ on K, of y-weight at most 8, such that the space

$$\{R_2, \ldots, R_{35}\} \cup \{\kappa_i \kappa_j R_1 : 1 \leq i \leq j \leq 8\}$$

has dimension equal to 70. These relations can be downloaded from `http://www.math.uni-hamburg.de/home/js.mueller/#code`. Using Proposition 3.1 we have proved the following:

Theorem 3.2. *The relations on the Kummer threefold are generated by the relations $R_1, \ldots, R_{35}$.*

4. Remnants of the group law

Here we investigate which remnants of the group law on A can be exhibited on K. Namely, we recall results of Duquesne, show that analogues of the biquadratic form representing pseudoaddition on the Kummer surface cannot exist in our situation and conjecture formulas for duplication on K.

Let T be a 2-torsion point on A. Duquesne [3, § III.2.1] has found a matrix W_T such that projectively the identity

$$\kappa(P+T) = W_T \cdot \kappa(P)$$

holds for all $P \in A$ if we view $\kappa(P)$ and $\kappa(P+T)$ as column vectors. Duquesne's method of finding W_T is analogous to the method employed by Flynn [6] in the genus 2 case, although there are a few additional technical difficulties. We also have that if $T \in A(k)[2]$, then W_T is defined over k.

Now let $P, Q \in A$. Then in general $\kappa(P+Q)$ and $\kappa(P-Q)$ cannot be found from $\kappa(P)$ and $\kappa(Q)$, but the unordered pair $\{\kappa(P+Q), \kappa(P-Q)\}$ can be. In other words, the map from $\mathrm{Sym}^2(K)$ to itself that maps $\{\kappa(P), \kappa(Q)\}$ to $\{\kappa(P+Q), \kappa(P-Q)\}$ is well-defined. In fact, in the analogous situation in genus 2 there are biquadratic forms $B_{ij} \in k[x_1, \ldots, x_4; y_1, \ldots, y_4]_{2,2}$ such that if x and y are Kummer coordinates for P and Q, respectively, then there are Kummer coordinates w, z for $\kappa(P+Q), \kappa(P-Q)$, respectively, such that

$$w * z = B(x, y) \tag{4}$$

holds. Here (4) is an abbreviation for

$$\begin{aligned} B_{ij}(x,y) &= w_i z_j + w_j z_i \text{ for } i \neq j \\ B_{ii}(x,y) &= w_i z_i. \end{aligned}$$

The following result says that in general such biquadratic forms cannot exist in genus 3.

Proposition 4.1. *Let A be the Jacobian of a smooth projective hyperelliptic curve C of genus 3, given by an equation* (1)*, and let K be the Kummer variety associated to A. There is no set of biquadratic forms $B_{ij}(x,y)$, where $1 \leq i,j \leq 8$, satisfying the following: If x and y are sets of Kummer coordinates for $P, Q \in A$, respectively, then there are Kummer coordinates w, z for $P+Q, P-Q$, respectively, such that* (4) *holds.*

Proof. We can work geometrically, so we assume k is algebraically closed. Let us fix Kummer coordinates $x(T) = (x(T)_1, \ldots, x(T)_8)$ for all $T \in A[2]$.

For each $T \in A[2]$ we get a map

$$\pi_T : k[x_1, \ldots, x_8; y_1, \ldots, y_8] \longrightarrow k[y_1, \ldots, y_8],$$

given by evaluating the tuple $x = (x_1, \ldots, x_8)$ at $x(T)$. This induces a map

$$\pi_T : \frac{k[x_1, \ldots, x_8; y_1, \ldots, y_8]_{2,2}}{(R_1(x), R_1(y))} \longrightarrow \frac{k[y_1, \ldots, y_8]_2}{(R_1(y))}.$$

Suppose a set of forms $B_{ij}(x,y)$, $1 \leq i,j \leq 8$, as in the statement of the proposition does exist and consider

$$R_1(B) := B_{18} - B_{27} - B_{36} - B_{45} - 2f_5B_{24} + 2f_5B_{33} + 2f_6B_{34} + 6f_7B_{44}. \tag{5}$$

Denote by $\overline{R_1(B)}$ the image of $R_1(B)$ in $\frac{k[x_1,\ldots,x_8;y_1,\ldots,y_8]_{2,2}}{(R_1(x),R_1(y))}$. For $T \in A[2]$, an arbitrary $P \in A$ and a set of Kummer coordinates y for P, we have: If $B(x(T), y) = w * z$, then w and z are both Kummer coordinates for $P + T = P - T$, and thus, if $x(T)$ and y are scaled suitably so that $z = w$, we must have $B_{ij}(x(T), y) = 2z_iz_j$ for $1 \leq i \neq j \leq 8$ and $B_{i,i}(x(T), y) = z_i^2$ for $i \in \{1, \ldots, 8\}$. As an element of $K_{\mathbb{A}}$, the tuple z must satisfy (3) and hence this implies

$$\pi_T(\overline{R_1(B)}) = R_1(z) = 0 \quad \text{for all } T \in A[2]. \tag{6}$$

We claim that $\overline{R_1(B)}$ itself vanishes. In order to show this, we fix $T \in A[2]$ and let

$$S(T) = \{s_1(T), \ldots, s_{36}(T)\} = \{x(T)_i x(T)_j : 1 \leq i \leq j \leq 8\}.$$

We also fix a representative

$$\sum_{j=1}^{8} \sum_{l=1}^{8} \lambda_{T,j,l} \cdot y_j \cdot y_l$$

of $\pi_T(\overline{R_1(B)})$, where

$$\lambda_{T,j,l} = \sum_{m=1}^{36} \mu_{T,j,l,m} \cdot s_m(T)$$

is linear in the $s_m(T)$ and we require that $\lambda_{T,1,8} = 0$, which uniquely determines our representative.

From (6) we know that we must have

$$\lambda_{T,j,l} = 0$$

for all j, l and for all $T \in A[2]$ and thus we get 64 linear equations

$$\sum_{m}^{36} \mu_{T,j,l,m} \cdot s_m(T) = 0.$$

For notational purposes, denote the elements of $A[2]$ by $\{T_1, \ldots, T_{64}\}$. It can be shown that the matrix $(s_i(T_j))_{1\leq i\leq 36, 1\leq j\leq 64}$ has generic rank equal to 35, so any linear relation between the $s_i(T)$ satisfied by all $T \in A[2]$ must be a multiple of $R_1(x(T)_1, \ldots, x(T)_8)$. Hence $\overline{R_1(B)}$ must vanish.

The upshot of this is that if we require our $B_{ij}(x, y)$ to contain no multiples of, say, x_1x_8 or y_1y_8 as summands (which we can always arrange by applying (3)), then $R_1(B) = 0$ follows. But this cannot hold in general: For example, take an arbitrary $P \in A \setminus A[2]$ and x a set of Kummer coordinates for P. We must have that $B_{ij}(x, x)$ lies in the ideal generated by the relations $R_1, \ldots, R_{35}$ for all $1 \leq i, j \leq 7$, but $B_{18}(x, x)$ does not. Clearly this cannot happen for all such P; hence $R_1(B)$ cannot vanish in general and so not all of the B_{ij} can be correct. □

This result implies that the situation is much more complicated than in genus 2. Recall Flynn's strategy to compute the biquadratic forms in genus 2 (see [6] or [2]): If $T \in A[2]$ and $P \in A$ is arbitrary, then we can compute

$$\kappa_i(P + T)\kappa_j(P - T) + \kappa_j(P + T)\kappa_i(P - T) = 2\kappa_i(P + T)\kappa_j(P + T)$$

projectively for all i and j by multiplying the matrix W_T by the vector $\kappa(P) \in k^4$. Using some algebraic manipulations, Flynn ensures that the resulting forms B'_{ij} are biquadratic in the $\kappa_i(P)$ and the $\kappa_j(T)$ and satisfy some additional normalization conditions. One can then check that the space of all $\kappa_i(T)\kappa_j(T)$, where $i \leq j$, is linearly independent of dimension 10. Hence for each pair (i, j) at most one biquadratic form that satisfies the same normalization conditions can specialize to B'_{ij}. The crucial point is that from classical theory of theta functions we already know that biquadratic forms B_{ij} satisfying (4) must exist – at least in the complex case (see Hudson's book [10]) and thus, using the Lefshetz principle, for any algebraically closed field of characteristic 0. Therefore Flynn concludes that $B_{ij} = B'_{ij}$ for all i, j.

We can try to use the same strategy in the genus 3 case. Indeed, in [3, § III.2.2], Duquesne computes the correct $B'_{ij}(x, y)$ in the special case that x is a set of Kummer coordinates for $T \in A[2]$. They can be downloaded from `ftp://megrez.math.u-bordeaux.fr/pub/duquesne`. Because of the relation (3), we know that the space of all $\kappa_i(T)\kappa_j(T)$, where $i \leq j$, is not linearly independent. But we also know that it has dimension 35, since R_1 is the only quadratic relation up to a constant factor. Now we can apply $R_1(x)$ and $R_1(y)$ to the $B'_{ij}(x, y)$ to make sure that no terms containing, say x_1x_8 or y_1y_8 appear and this is done by Duquesne. Thus we can draw the same conclusion as in the genus 2 situation, namely that for each pair (i, j) at most one biquadratic form that satisfies the same normalization conditions can specialize to B'_{ij}. By Proposition 4.1, we know that there is no set of biquadratic forms on K satisfying (4) in general. But we can still make use of the B'_{ij}, at least conjecturally, so we analyze them further.

We define two index sets

$$I := \{(i, j) : 1 \leq i \leq j \leq 8\},$$

and

$$E := \{(1, 8), (2, 7), (3, 6), (4, 5), (5, 5), (5, 6), (5, 7), (6, 6)\} \subset I.$$

We say that a pair of points $(P, Q) \in A \times A$ is *good* if there is a pair $(i_0, j_0) \in I \setminus E$ such that if x and y are Kummer coordinates for P and Q, respectively, and w and z denote Kummer coordinates for $P + Q$ and $P - Q$, respectively, then we have

(i) $B'_{i_0j_0}(x, y) \neq 0$;

(ii) $w_{i_0} \neq 0$;
(iii) $z_{j_0} \neq 0$.

If (P, Q) is a good pair and x, y, w, z are as above, then we can normalize w and z such that $w_{i_0} z_{j_0} = B'_{i_0 j_0}(x, y)$. For $1 \leq i, j \leq 8$ we define $\alpha_{i,j}(x, y)$ as follows:

$$\alpha_{ij}(x, y) := w_i z_j + w_j z_i - B'_{ij}(x, y). \tag{7}$$

Building on a large number of numerical experiments we state a list of conjectures regarding the relations between $B'_{ij}(x, y)$ and $w_i z_j + w_j z_i$:

Conjecture 4.2. *Suppose that $(P, Q) \in A \times A$ is a good pair with respective Kummer coordinates x and y. Then the following properties are satisfied:*

(a) *We have $\alpha_{ij}(x, y) = 0$ for $(i, j) \in I \setminus E$.*
(b) *The identities*
$$-\alpha_{1,8}(x, y) = \alpha_{2,7}(x, y) = \alpha_{3,6}(x, y) = \alpha_{4,5}(x, y)$$
and
$$\alpha_{5,7}(x, y) = -2\alpha_{6,6}(x, y)$$
hold.
(c) *If $\alpha_{i_1 j_1}(x, y) = 0$ for some $(i_1, j_1) \in E$, then all $\alpha_{ij}(x, y)$ vanish.*
(d) *If $\alpha_{i_1 j_1}(x, y) \neq 0$ for some $(i_1, j_1) \in E$, then we have $\alpha_{ij}(x, y) \neq 0$ for all $(i, j) \in E$. If this holds and if $(i, j), (i'j') \in E$, then the ratios*
$$\frac{\alpha_{i'j'}(x, y)}{\alpha_{ij}(x, y)},$$
only depend on C and on $(i, j), (i', j')$, but not on x or y.

Remark 4.3. The values $\alpha_{ij}(x, y)$ depend on the choice of the pair $(i_0, j_0) \in I \setminus E$, but note that the assertions of Conjecture 4.2 are independent of this choice.

Remark 4.4. Stoll has recently proved Conjecture 4.2 [18].

The naive height h on the Kummer surface associated to a Jacobian surface A can be used to define and compute a canonical height $\hat{h}$ on A, which has several applications. See Flynn-Smart [7] for the construction and an algorithm for the computation of $\hat{h}$ and [17] for improvements due to Stoll. For this application, one does not have to work with the biquadratic forms B_{ij}, but rather with the quartic duplication polynomials δ which, however, were originally derived from the B_{ij}. If we assume the validity of the first two parts of Conjecture 4.2, then we can find analogs of these polynomials which again turn out to be quartic, although the B_{ij} are not all biquadratic.

More precisely, we define

$$\delta'_i(x) := B'_{i8}(x, x) \in k[x] \quad \text{for } i = 2, \ldots, 8,$$

and

$$\delta'_1(x) := \frac{4B'_{18}(x, x) + R(x)}{3} \in k[x],$$

where $R(x)$ is a certain quartic relation on K which we use to get rid of the denominators in $\frac{4}{3}B_{18}(x,x)$. Let $\delta'(x) := (\delta'_1(x), \ldots, \delta'_8(x))$. We take the δ'_i as our candidates for the duplication polynomials on K.

As in the genus 2 situation, we want that the set $(0, \ldots, 0, 1)$ of Kummer coordinates of the origin is mapped to itself by the duplication map. This is required by the canonical height algorithms in [7] and [17]. In our situation we have

$$\delta'(0,0,0,0,0,0,0,1) = (0,0,0,0,0,0,0,f_7^2).$$

But this can be fixed easily by a simple change of models of K using the map

$$\tau(x_1, \ldots, x_8) = (x_1, \ldots, x_7, f_7 x_8).$$

Setting

$$\delta := \frac{1}{f_7^2}(\tau \circ \delta' \circ \tau^{-1})$$

we find

1) $\delta_i \in \mathbb{Z}[f_0, \ldots, f_7][x_1, \ldots, x_8]$ for all $i = 1, \ldots, 8$;
2) $\delta(0,0,0,0,0,0,0,1) = (0,0,0,0,0,0,0,1)$.

Based on extensive numerical evidence, we make the following conjecture.

Conjecture 4.5. *If $P \in A$, then*

$$\delta'(\kappa(P)) = \kappa(2P)$$

and

$$\delta(\tau(\kappa(P))) = \tau(\kappa(2P)).$$

We can relate this conjecture to our earlier Conjecture 4.2.

Lemma 4.6. *Suppose that* $\mathrm{char}(k) \neq 3$ *and that parts* (a) *and* (b) *of Conjecture 4.2 are satisfied for C. Then Conjecture 4.5 follows for all $P \in A$ such that (P, P) is a good pair.*

Proof. Suppose that $\mathrm{char}(k) \neq 3$ and let $P \in A$ such that (P, P) is a good pair and let x be a set of Kummer coordinates for P. In this situation it obviously suffices to prove $\delta'(\kappa(P)) = \kappa(2P)$. Assuming part (a) of Conjecture 4.2, we can find a set $z \in K_{\mathbb{A}}$ of Kummer coordinates for $2P$ such that $z_i = \delta'_i(x)$ for $i = 2, \ldots, 8$, because we have $\kappa(O) = (0,0,0,0,0,0,0,1)$. Therefore it suffices to show that part (b) of Conjecture 4.2 implies that

$$z_1 = \frac{4}{3}B'_{18}(x,x). \tag{8}$$

Let $Q \in A$ such that (P, Q) is good, let $y \in K_{\mathbb{A}}$ be a set of Kummer coordinates for Q. We normalize Kummer coordinates z and w for $P + Q$ and $P - Q$, respectively and define $\alpha_{ij}(x,y)$ as in (7). For simplicity, let b_{ij} denote $w_i z_j + w_j z_i$ for distinct $1 \leq i, j \leq 8$ and let b_{ii} denote $w_i z_i$ for $1 \leq i \leq 8$.

By construction, the B'_{ij} satisfy $R_1(B') = 0$ (see (5)) and so we have

$$B'_{18} - B'_{27} - B'_{36} - B'_{45} = 2f_5 B'_{24} + 2f_5 B'_{33} + 2f_6 B'_{34} + 6f_7 B'_{44}.$$

But applying the B'_{ij} to the pair (x, y) and using Conjecture 4.2 (b), we get that the left hand side is equal to

$$b_{18} - b_{27} - b_{36} - b_{45} - 4\alpha_{1,8}(x,y),$$

and that the right hand side is equal to

$$2f_5b_{24} + 2f_5b_{33} + 2f_6b_{34} + 6f_7b_{44}.$$

Setting $y = x$, we find that all b_{ij} must vanish unless $i = 8$ or $j = 8$ and so we obtain

$$b_{18} = 4\alpha_{1,8}(x, x), .$$

Hence we conclude

$$z_1 = b_{18} = 4(b_{18} - B'_{18}(x, x)),$$

which proves (8) and thus the Lemma. □

References

[1] C. Birkenhake, H. Lange, *Complex Abelian Varieties*, 2nd edition, Springer-Verlag, Berlin (2004).
[2] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, Cambridge University Press, Cambridge (1996).
[3] S. Duquesne, *Calculs effectifs des points entier et rationnels sur les courbes*, Thèse de doctorat, Université Bordeaux I (2001).
[4] S. Duquesne, *Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2*, Preprint (2007).
[5] E.V. Flynn, *The jacobian and formal group of a curve of genus 2 over an arbitrary ground field*, Math. Proc. Camb. Phil. Soc. **107**, 425–441 (1990).
[6] E.V. Flynn, *The group law on the jacobian of a curve of genus 2*, J. reine angew. Math. **439**, 45–69 (1993).
[7] E.V. Flynn and N.P. Smart, *Canonical heights on the Jacobians of curves of genus* 2 *and the infinite descent*, Acta Arith. **79**, 333–352 (1997).
[8] D. Holmes, *Computing Néron-Tate heights of points on hyperelliptic Jacobians*, J. Number Theory **132**, 2, 1295–1305 (2012).
[9] D. Holmes, *An Arakelov-Theoretic Approach to Naive Heights on Hyperelliptic Jacobians*, Preprint (2012). arXiv:math/1207.5948v2 [math.NT]
[10] R.W.H.T. Hudson, *Kummer's Quartic Surface*, University Press, Cambridge (1905).
[11] 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/`.)
[12] J.S. Müller, *Explicit Kummer surface formulas for arbitrary characteristic*, LMS J. Comput. Math. **13**, 47–64 (2010).
[13] J.S. Müller, *Computing canonical heights on Jacobians*, PhD thesis, Universität Bayreuth (2010).
[14] J.S. Müller, *Computing canonical heights using arithmetic intersection theory*, to appear in Math. Comp. (2012).
D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1**, 287–354 (1966).
[15] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Tata Institute of Fundamental Research, Bombay (1974).
[16] M. Stoll, *On the height constant for curves of genus two*, Acta Arith. **90**, 183–201 (1999).
[17] M. Stoll, *On the height constant for curves of genus two, II*, Acta Arith. **104**, 165–182 (2002).
[18] M. Stoll, *An explicit theory of heights for hyperelliptic Jacobians of genus three*, in preparation.
[19] A.G.J. Stubbs, *Hyperelliptic curves*, PhD thesis, University of Liverpool (2000).

Fachbereich Mathematik, Universität Hamburg, Bundesstrasse 55 (Geomatikum), 20146 Hamburg, Germany

E-mail address: `jan.steffen.mueller@math.uni-hamburg.de`