

AN EXPLICIT THEORY OF HEIGHTS FOR HYPERELLIPTIC JACOBIANS OF GENUS THREE

MICHAEL STOLL

ABSTRACT. We develop an explicit theory of Kummer varieties associated to Jacobians of hyperelliptic curves of genus 3, over any field k of characteristic $\neq 2$. In particular, we provide explicit equations defining the Kummer variety \mathcal{K} as a subvariety of \mathbb{P}^7 , together with explicit polynomials giving the duplication map on \mathcal{K} . A careful study of the degenerations of this map then forms the basis for the development of an explicit theory of heights on such Jacobians when k is a number field. We use this input to obtain a good bound on the difference between naive and canonical height, which is a necessary ingredient for the explicit determination of the Mordell-Weil group. We illustrate our results with two examples.

1. INTRODUCTION

The goal of this paper is to take up the approaches used to deal with Jacobians and Kummer surfaces of curves of genus 2 by Cassels and Flynn [CF] and by the author [Sto1, Sto3] and extend them to hyperelliptic curves of genus 3. We always assume that the base field k has characteristic $\neq 2$. A hyperelliptic curve \mathcal{C} over k of genus 3 is then given by an equation of the form $y^2 = f(x)$, where f is a squarefree polynomial of degree 7 or 8 with coefficients in k ; we take \mathcal{C} to be the smooth projective curve determined by this affine equation. We denote the Jacobian variety of \mathcal{C} by \mathcal{J} . Identifying points with their negatives on \mathcal{J} , we obtain the Kummer variety of \mathcal{J} . It is known that the morphism $\mathcal{J} \rightarrow \mathbb{P}^7$ given by the linear system $|2\Theta|$ on \mathcal{J} (where Θ denotes the theta divisor) induces an isomorphism of the Kummer variety with the image of \mathcal{J} in \mathbb{P}^7 ; we denote the image by $\mathcal{K} \subset \mathbb{P}^7$. Our first task is to find a suitable basis of the Riemann-Roch space $L(2\Theta)$ and to give explicit equations defining \mathcal{K} , thereby completing earlier work by Stubbs [Stu], Duquesne [Duq] and Müller [Mü1, Mü3]. To this end, we make use of the canonical identification of \mathcal{J} with $\mathcal{X} = \text{Pic}^4(\mathcal{C})$ and realize the complement of Θ in \mathcal{X} as the quotient of an explicit 6-dimensional variety \mathcal{V} in \mathbb{A}^{15} by the action of a certain group Γ . This allows us to identify the ring of

Date: January 3, 2017.

2010 Mathematics Subject Classification. 14H40, 14H45, 11G10, 11G50, 14Q05, 14Q15.

Key words and phrases. Kummer variety, hyperelliptic curve, genus 3, canonical height.

regular functions on $\mathcal{X} \setminus \Theta$ with the ring of Γ -invariants in the coordinate ring of \mathcal{V} . In this way, we obtain a natural basis of $L(2\Theta)$, and we find the quadric and the 34 quartics that define \mathcal{K} ; see Section 2. We give the relation between the coordinates chosen here and those used in previous work and discuss how transformations of the curve equation induced by the action of $\mathrm{GL}(2)$ on (x, z) act on our coordinates; see Section 3. We then give a recipe that allows to decide whether a k -rational point on \mathcal{K} comes from a k -rational point on \mathcal{J} (Section 4).

The next task is to describe the maps $\mathcal{K} \rightarrow \mathcal{K}$ and $\mathrm{Sym}^2 \mathcal{K} \rightarrow \mathrm{Sym}^2 \mathcal{K}$ induced by multiplication by 2 and by $\{P, Q\} \mapsto \{P + Q, P - Q\}$ on \mathcal{J} . We use the approach followed in [Sto1]: we consider the action of a double cover of the 2-torsion subgroup $\mathcal{J}[2]$ on the coordinate ring of \mathbb{P}^7 . This induces an action of $\mathcal{J}[2]$ itself on forms of even degree. We use the information obtained on the various eigenspaces and the invariant subspaces in particular to obtain an explicit description of the duplication map $\underline{\delta}$ and of the add-and-subtract map on \mathcal{K} . The study of the action of $\mathcal{J}[2]$ is done in Sections 5 and 6; the results on the duplication map and on the sum-and-difference map are obtained in Sections 7 and 8, respectively. In Section 9, we then study the degeneration of these maps that occur when we allow the curve to acquire singularities. This is relevant in the context of bad reduction and is needed as input for the results on the height difference bound.

We then turn to the topic motivating our study, which is the canonical height \hat{h} on the Jacobian, and, in particular, a bound on the difference $h - \hat{h}$ between naive and canonical height. Such a bound is a necessary ingredient for the determination of generators of the Mordell-Weil group $\mathcal{J}(k)$ (where k now is a number field; in practice, usually $k = \mathbb{Q}$), given generators of a finite-index subgroup. The difference $h - \hat{h}$ can be expressed in terms of the local ‘loss of precision’ under $\underline{\delta}$ at the various primes of bad reduction and the archimedean places of k . In analogy with [Sto1], we obtain an estimate for this local ‘loss of precision’ in terms of the valuation of the discriminant of f . This is one of the main results of Section 10, together with a statement on the structure of the local ‘height correction function’, which is analogous to that obtained in [Sto3, Theorem 4.1]. These results allow us to obtain reasonable bounds for the height difference. We illustrate this by determining generators of the Mordell-Weil group of the Jacobian of the curve $y^2 = 4x^7 - 4x + 1$. We then use this result to determine the set of integral solutions of the equation $y^2 - y = x^7 - x$, using the method of [BM+]; see Section 11.

In addition, we show in Section 12 how one can obtain better bounds (for a modified naive height) when the polynomial defining the curve is not primitive. As an example, we determine explicit generators of the Mordell-Weil group of the Jacobian of the curve given by the binomial coefficient equation

$$\binom{y}{2} = \binom{x}{7}.$$

We have made available at [Data] files that can be read into Magma [BCP] and provide explicit representations of the quartics defining the Kummer variety, the matrices giving the action of 2-torsion points, the polynomials defining the duplication map and the matrix of bi-quadratic forms related to the ‘sum-and-difference map’.

Acknowledgments. I would like to thank Steffen Müller for helpful comments on a draft version of this paper and for pointers to the literature. The necessary computations were performed using the Magma computer algebra system [BCP]. At [Data] we have made available the file `Kum3-verification.magma`, which, when loaded into Magma, will perform the computations necessary to verify a number of claims made throughout the paper. These claims are marked by a star, like this★.

2. THE KUMMER VARIETY

We consider a hyperelliptic curve of genus 3 over a field k of characteristic different from 2, given by the affine equation

$$\mathcal{C}: y^2 = f_8x^8 + f_7x^7 + \cdots + f_1x + f_0 = f(x),$$

where f is a squarefree polynomial of degree 7 or 8. (We do not assume that \mathcal{C} has a Weierstrass point at infinity, which would correspond to f having degree 7.) Let $F(x, z)$ denote the octic binary form that is the homogenization of f ; F is squarefree. Then \mathcal{C} has a smooth model in the weighted projective plane $\mathbb{P}_{1,4,1}^2$ given by $y^2 = F(x, z)$. Here x and z have weight 1 and y has weight 4. We denote the hyperelliptic involution on \mathcal{C} by ι , so that $\iota(x : y : z) = (x : -y : z)$.

As in the introduction, we denote the Jacobian variety of \mathcal{C} by \mathcal{J} . We would like to find an explicit version of the map

$$\mathcal{J} \longrightarrow \mathbb{P}^7$$

given by the linear system of twice the theta divisor; it embeds the Kummer variety $\mathcal{J}/\{\pm 1\}$ into \mathbb{P}^7 . We denote the image by \mathcal{K} .

We note that the canonical class \mathfrak{W} on \mathcal{C} has degree 4. Therefore $\mathcal{J} = \text{Pic}_{\mathcal{C}}^0$ is canonically isomorphic to $\mathcal{X} = \text{Pic}_{\mathcal{C}}^4$, with the isomorphism sending \mathfrak{D} to $\mathfrak{D} + \mathfrak{W}$. Then the map induced by ι on \mathcal{X} corresponds to multiplication by -1 on \mathcal{J} . There is a canonical theta divisor on $\text{Pic}_{\mathcal{C}}^0$ whose support consists of the divisor classes of the form $[(P_1) + (P_2)] - \mathfrak{m}$, where \mathfrak{m} is the class of the polar divisor $(x)_{\infty}$; we have $\mathfrak{W} = 2\mathfrak{m}$. The support of the theta divisor is the locus of points on \mathcal{X} that are not represented by divisors in general position, where an effective divisor \mathfrak{D} on \mathcal{C} is *in general position* unless there is a point $P \in \mathcal{C}$ such that $\mathfrak{D} \geq (P) + (\iota P)$. This can be seen as follows. The image on \mathcal{X} of a point $[(P_1) + (P_2)] - \mathfrak{m}$ on the theta divisor is represented by all effective divisors of the form $(P_1) + (P_2) + (P) + (\iota P)$

for an arbitrary point $P \in \mathcal{C}$. If $P_2 \neq \iota P_1$, then the Riemann-Roch Theorem implies that the linear system containing these divisors is one-dimensional, and so *all* divisors representing our point on \mathcal{X} have this form; in particular, there is no representative divisor in general position. If $P_2 = \iota P_1$, then the linear system has dimension 2 and consists of all divisors of the form $(P) + (\iota P) + (P') + (\iota P')$, none of which is in general position.

We identify \mathcal{J} and \mathcal{X} , and we denote the theta divisor on \mathcal{J} and its image on \mathcal{X} by Θ . We write $L(n\Theta)$ for the Riemann-Roch space $L(\mathcal{X}, n\Theta) \cong L(\mathcal{J}, n\Theta)$, where n is an integer. It is known that $\dim L(n\Theta) = n^3$. Since Θ is symmetric, the negation map acts on $L(n\Theta)$ (via $\phi \mapsto (P \mapsto \phi(-P))$), and it makes sense to speak of even and odd functions in $L(n\Theta)$ (with respect to this action). We write $L(n\Theta)^+$ for the subspace of even functions. It is known that $\dim L(n\Theta)^+ = n^3/2 + 4$ for n even and $\dim L(n\Theta)^+ = (n^3 + 1)/2$ for n odd.

We can parameterize effective degree 4 divisors in general position as follows. Any such divisor \mathfrak{D} is given by a binary quartic form $A(x, z)$ specifying the image of \mathfrak{D} on \mathbb{P}^1 under the hyperelliptic quotient map $\pi: \mathcal{C} \rightarrow \mathbb{P}^1$, $(x, y) \mapsto x$, together with another quartic binary form $B(x, z)$ such that $y = B(x, z)$ on the points in \mathfrak{D} , with the correct multiplicity. (Note that by the ‘general position’ condition, y is uniquely determined by x and z for each point in the support of \mathfrak{D} .) More precisely, we must have that

$$(2.1) \quad B(x, z)^2 - A(x, z)C(x, z) = F(x, z)$$

for a suitable quartic binary form $C(x, z)$. We then have a statement analogous to that given in [CF, Chapter 4] for Pic^3 of a curve of genus 2, which we formulate as a lemma.

We let Q be the ternary quadratic form $x_2^2 - x_1x_3$. We write

$$(2.2) \quad D = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix},$$

for the associated symmetric matrix (times 2) and

$$\Gamma = \text{SO}(Q) = \{\gamma \in \text{SL}(3) : \gamma D \gamma^\top = D\};$$

then $-\Gamma = \text{O}(Q) \setminus \text{SO}(Q)$, and $\pm\Gamma = \text{O}(Q)$. We have the following elements in Γ (for arbitrary λ and μ in the base field):

$$t_\lambda = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda^{-1} \end{pmatrix}, \quad n_\mu = \begin{pmatrix} 1 & \mu & \mu^2 \\ 0 & 1 & 2\mu \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad w = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix};$$

these elements generate Γ .

Lemma 2.1. *Two triples (A, B, C) and (A', B', C') satisfying (2.1) specify the same point on \mathcal{X} if and only if $(A', B', C') = (A, B, C)\gamma$ for some $\gamma \in \Gamma$. They represent opposite points (with respect to the involution on \mathcal{X} induced by ι) if and only if the relation above holds for some $\gamma \in -\Gamma$.*

Proof. We first show that two triples specifying the same point are in the same Γ -orbit. Let \mathfrak{D} and \mathfrak{D}' be the effective divisors of degree 4 given by $A(x, x) = 0$, $y = B(x, z)$ and by $A'(x, z) = 0$, $y = B'(x, z)$, respectively. By assumption, \mathfrak{D} and \mathfrak{D}' are linearly equivalent, and they are both in general position. If \mathfrak{D} and \mathfrak{D}' share a point P in their supports, then subtracting P from both \mathfrak{D} and \mathfrak{D}' , we obtain two effective divisors of degree 3 in general position that are linearly equivalent. Since such divisors are non-special, they must be equal, hence $\mathfrak{D} = \mathfrak{D}'$. So A and A' agree up to scaling, and $B' - B$ is a multiple of A :

$$A' = \lambda A, \quad B' = B + \mu A, \quad C' = \lambda^{-1}(C + 2\mu B + \mu^2 A);$$

then $(A', B', C') = (A, B, C)n_\mu t_\lambda$. So we can now suppose that the supports of \mathfrak{D} and \mathfrak{D}' are disjoint. Then, denoting by $\iota\mathfrak{D}'$ the image of \mathfrak{D}' under the hyperelliptic involution, $\mathfrak{D} + \iota\mathfrak{D}'$ is a divisor of degree 8 in general position, which is in twice the canonical class, so it is linearly equivalent to $4\mathfrak{m}$. Since the Riemann-Roch space of that divisor on \mathcal{C} is generated by (in terms of the affine coordinates obtained by setting $z = 1$) $1, x, x^2, x^3, x^4, y$, there is a function of the form $y - \tilde{B}(x, 1)$ with \tilde{B} homogeneous of degree 4 that has divisor $\mathfrak{D} + \iota\mathfrak{D}' - 4\mathfrak{m}$. Equivalently, $\mathfrak{D} + \iota\mathfrak{D}'$ is the intersection of \mathcal{C} with the curve given by $y = \tilde{B}(x, z)$. This implies that $\tilde{B}^2 - F$ is a constant times AA' . Up to scaling A' and C' by λ and λ^{-1} for a suitable λ (this corresponds to acting on (A', B', C') by $t_\lambda \in \Gamma$), we have

$$\tilde{B}^2 - AA' = F,$$

so that (A, \tilde{B}, A') corresponds to \mathfrak{D} and $(A', -\tilde{B}, A)$ corresponds to \mathfrak{D}' . The argument above (for the case $\mathfrak{D} = \mathfrak{D}'$) shows that (A, B, C) and (A, \tilde{B}, A') are in the same Γ -orbit, and the same is true of (A', B', C') and $(A', -\tilde{B}, A)$. Finally,

$$(A', -\tilde{B}, A) = (A, \tilde{B}, A')w.$$

Conversely, it is easy to see that the generators of Γ given above do not change the linear equivalence class of the associated divisor — the first two do not even change the divisor, and the third replaces \mathfrak{D} by the linearly equivalent $\iota\mathfrak{D}'$ where $\mathfrak{D} + \mathfrak{D}' \sim 2\mathfrak{W}$ is the divisor of $y - B(x, z)$ on \mathcal{C} .

For the last statement, it suffices to observe that $(A, -B, C)$ gives the point opposite to that given by (A, B, C) ; the associated matrix is $-t_{-1} \in -\Gamma$. \square

We write A, B, C as follows.

$$\begin{aligned} A(x, z) &= a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \\ B(x, z) &= b_4x^4 + b_3x^3z + b_2x^2z^2 + b_1xz^3 + b_0z^4 \\ C(x, z) &= c_4x^4 + c_3x^3z + c_2x^2z^2 + c_1xz^3 + c_0z^4 \end{aligned}$$

and use $a_0, \dots, a_4, b_0, \dots, b_4, c_0, \dots, c_4$ as affine coordinates on \mathbb{A}^{15} . We arrange these coefficients into a matrix

$$(2.3) \quad L = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ b_0 & b_1 & b_2 & b_3 & b_4 \\ c_0 & c_1 & c_2 & c_3 & c_4 \end{pmatrix}.$$

Then $\gamma \in \pm\Gamma$ acts on \mathbb{A}^{15} via multiplication by γ^\top on the left on L . Since there is a multiplicative group sitting inside Γ acting by $(A, B, C) \cdot \lambda = (\lambda A, B, \lambda^{-1}C)$, any Γ -invariant polynomial must be a linear combination of monomials having the same number of a_i and c_j . Hence in any term of a homogeneous Γ -invariant polynomial of degree d , the number of factors b_i has the same parity as d . This shows that such a Γ -invariant polynomial is even with respect to ι if d is even, and odd if d is odd.

It is not hard to see that there are no Γ -invariant polynomials of degree 1: by the above, they would have to be a linear combination of the b_i , but the involution $(A, B, C) \mapsto (C, -B, A) = (A, B, C)w$ negates all the b_i . It is also not hard to check that the space of invariants of degree 2 is spanned by the coefficients of the quadratic form

$$B_l^2 - A_l C_l \in \text{Sym}^2\langle x_0, x_1, x_2, x_3, x_4 \rangle,$$

where

$$\begin{aligned} A_l &= a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ B_l &= b_0x_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \\ C_l &= c_0x_0 + c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 \end{aligned}$$

are linear forms in five variables. We write

$$B_l^2 - A_l C_l = \sum_{0 \leq i < j \leq 4} \eta_{ij} x_i x_j,$$

so that $\eta_{ii} = b_i^2 - a_i c_i$ and for $i < j$, $\eta_{ij} = 2b_i b_j - a_i c_j - a_j c_i$. Up to scaling, the quadratic form corresponds to the symmetric matrix

$$(2.4) \quad L^\top D L = \begin{pmatrix} 2\eta_{00} & \eta_{01} & \eta_{02} & \eta_{03} & \eta_{04} \\ \eta_{01} & 2\eta_{11} & \eta_{12} & \eta_{13} & \eta_{14} \\ \eta_{02} & \eta_{12} & 2\eta_{22} & \eta_{23} & \eta_{24} \\ \eta_{03} & \eta_{13} & \eta_{23} & 2\eta_{33} & \eta_{34} \\ \eta_{04} & \eta_{14} & \eta_{24} & \eta_{34} & 2\eta_{44} \end{pmatrix},$$

and the image \mathcal{Q} of the map $q: \mathbb{A}^{15} \rightarrow \text{Sym}^2 \mathbb{A}^5$ given by this matrix consists of the matrices of rank at most 3; it is therefore defined by the 15 different quartics obtained as 4×4 -minors of this matrix.

Scaling x by λ corresponds to scaling a_j, b_j, c_j by λ^j . This introduces another grading on the coordinate ring of our \mathbb{A}^{15} ; we call the corresponding degree the *weight*. We then have $\text{wt}(a_j) = \text{wt}(b_j) = \text{wt}(c_j) = j$ and therefore $\text{wt}(\eta_{ij}) = i + j$. The 15 quartics defining \mathcal{Q} have weights

$$12, 13, 14, 14, 15, 15, 16, 16, 17, 17, 18, 18, 19, 20.$$

We will reserve the word *degree* for the degree in terms of the η_{ij} ; then it makes sense to set $\deg(a_j) = \deg(b_j) = \deg(c_j) = \frac{1}{2}$.

We let $\mathcal{V} \subset \mathbb{A}^{15}$ be the affine variety given by (2.1). The defining equations of \mathcal{V} then read

$$\begin{aligned} b_0^2 - a_0c_0 &= \eta_{00} &= f_0 \\ 2b_0b_1 - (a_0c_1 + a_1c_0) &= \eta_{01} &= f_1 \\ 2b_0b_2 + b_1^2 - (a_0c_2 + a_1c_1 + a_2c_0) &= \eta_{02} + \eta_{11} &= f_2 \\ 2b_0b_3 + 2b_1b_2 - (a_0c_3 + a_1c_2 + a_2c_1 + a_3c_0) &= \eta_{03} + \eta_{12} &= f_3 \\ 2b_0b_4 + 2b_1b_3 + b_2^2 - (a_0c_4 + a_1c_3 + a_2c_2 + a_3c_1 + a_4c_0) &= \eta_{04} + \eta_{13} + \eta_{22} &= f_4 \\ 2b_1b_4 + 2b_2b_3 - (a_1c_4 + a_2c_3 + a_3c_2 + a_4c_1) &= \eta_{14} + \eta_{23} &= f_5 \\ 2b_2b_4 + b_3^2 - (a_2c_4 + a_3c_3 + a_4c_2) &= \eta_{24} + \eta_{33} &= f_6 \\ 2b_3b_4 - (a_3c_4 + a_4c_3) &= \eta_{34} &= f_7 \\ b_4^2 - a_4c_4 &= \eta_{44} &= f_8; \end{aligned}$$

in particular, the image of \mathcal{V} under q is a linear ‘slice’ \mathcal{W} of \mathcal{Q} , cut out by the nine linear equations above. It is then natural to define $\deg(f_j) = 1$ and $\text{wt}(f_j) = j$.

By Lemma 2.1, the quotient \mathcal{V}/Γ of \mathcal{V} by the action of Γ can be identified with $\mathcal{U} := \mathcal{X} \setminus \Theta$, the complement of the theta divisor in \mathcal{X} . Since the map q is given by $\pm\Gamma$ -invariants, we obtain a surjective morphism $\mathcal{K} \setminus \kappa(\Theta) \rightarrow \mathcal{W}$. We will see that it is actually an isomorphism.

Functions in the Riemann-Roch space $L(n\Theta)$ will be represented by Γ -invariant polynomials in the a_i, b_i, c_i . Similarly, functions in the even part $L(n\Theta)^+$ of this space are represented by $\pm\Gamma$ -invariant polynomials. A Γ -invariant polynomial that is homogeneous of degree n in the a_i, b_i, c_i will conversely give rise to a function in $L(n\Theta)$. Modulo the relations defining \mathcal{V} , there are six independent such invariants of degree 2. We choose

$$\eta_{02}, \eta_{03}, \eta_{04}, \eta_{13}, \eta_{14}, \eta_{24}$$

as representatives. As mentioned above, invariants of even degree are $\pm\Gamma$ -invariant and so give rise to even functions on \mathcal{X} with respect to ι , whereas invariants of odd degree give rise to odd functions on \mathcal{X} . Together with the constant function

1, we have found seven functions in $L(2\Theta) = L(2\Theta)^+$. Since $\dim L(2\Theta) = 2^3 = 8$, we are missing one function. We will see that is given by some quadratic form in the η_{ij} above, with the property that it does not grow faster than them when we approach Θ .

To find this quadratic form, we have to find out what $(\eta_{02} : \eta_{03} : \cdots : \eta_{24})$ tends to as we approach the point represented by $(x_1, y_1) + (x_2, y_2) + \mathfrak{m}$ on \mathcal{X} . A suitable approximation, taking $y = \ell(x)$ to be the line interpolating between the two points,

$$B(x, 1) = \lambda(x - x_0)(x - x_1)(x - x_2) + \ell(x),$$

$A_0(x) = (x - x_1)(x - x_2)$, $\varphi_{\pm}(x) = (f(x) \pm \ell(x)^2)/A_0(x)^2$, $\psi(x) = \ell(x)/A_0(x)$, and $A(x, 1) = A_0(x)(\lambda^2(x - x_0)^2 + (2\lambda\psi(x_0) - \varphi'_+(x_0))(x - x_0) - \varphi_-(x_0) + O(\lambda^{-1}))$, shows that[★]

$$\begin{aligned} \eta_{02} &= -\lambda^2(x_1x_2)^2 + O(\lambda) \\ \eta_{03} &= \lambda^2(x_1 + x_2)x_1x_2 + O(\lambda) \\ \eta_{04} &= -\lambda^2x_1x_2 + O(\lambda) \\ \eta_{13} &= -\lambda^2(x_1^2 + x_2^2) + O(\lambda) \\ \eta_{14} &= \lambda^2(x_1 + x_2) + O(\lambda) \\ \eta_{24} &= -\lambda^2 + O(1) \end{aligned}$$

as $\lambda \rightarrow \infty$. There are various quadratic expressions in these that grow at most like λ^3 , namely

$$\begin{aligned} 2\eta_{04}\eta_{24} + \eta_{13}\eta_{24} - \eta_{14}^2, \quad \eta_{03}\eta_{24} - \eta_{04}\eta_{14}, \quad \eta_{02}\eta_{24} - \eta_{04}^2, \\ \eta_{02}\eta_{14} - \eta_{03}\eta_{04}, \quad 2\eta_{02}\eta_{04} + \eta_{02}\eta_{13} - \eta_{03}^2 \end{aligned}$$

(they provide five independent even functions in $L(3\Theta)$ modulo $L(2\Theta)$) and

$$(2.5) \quad \eta = \eta_{02}\eta_{24} - \eta_{03}\eta_{14} + \eta_{04}^2 + \eta_{04}\eta_{13},$$

which in fact only grows like λ^2 and therefore gives us the missing basis element of $L(2\Theta)$. We find that[★]

$$\eta = \lambda^2 \frac{G(x_1, x_2) - 2y_1y_2}{(x_1 - x_2)^2} + O(\lambda),$$

where

$$G(x_1, x_2) = 2 \sum_{j=0}^4 f_{2j}(x_1x_2)^j + (x_1 + x_2) \sum_{j=0}^3 f_{2j+1}(x_1x_2)^j.$$

(Note the similarity with the fourth Kummer surface coordinate in the genus 2 case; see [CF].)

The map $\mathcal{X} \rightarrow \mathbb{P}^7$ we are looking for is then given by

$$(1 : \eta_{24} : \eta_{14} : \eta_{04} : \eta_{04} + \eta_{13} : \eta_{03} : \eta_{02} : \eta).$$

We use (ξ_1, \dots, ξ_8) to denote these coordinates (in the given order). The reason for setting $\xi_5 = \eta_{04} + \eta_{13}$ rather than η_{13} is that this leads to nicer formulas later on. For example, we then have the simple quadratic relation

$$(2.6) \quad \xi_1 \xi_8 - \xi_2 \xi_7 + \xi_3 \xi_6 - \xi_4 \xi_5 = 0.$$

Regarding degree and weight, we have, writing $\underline{\xi} = (\xi_1, \xi_2, \dots, \xi_8)$, that

$$\deg(\underline{\xi}) = (0, 1, 1, 1, 1, 1, 1, 2) \quad \text{and} \quad \text{wt}(\underline{\xi}) = (0, 6, 5, 4, 4, 3, 2, 8).$$

It is known that the image \mathcal{K} of the Kummer variety in \mathbb{P}^7 of a generic hyperelliptic Jacobian of genus 3 is given by a quadric and 34 independent quartic relations that are not multiples of the quadric; see [Mü3, Thm. 3.3]. (For this, we can work over an algebraically closed field, so that we can change coordinates to move one of the Weierstrass points to infinity so that we are in the setting of [Mü3].) The quadric is just (2.6). It is also known [Mü3, Prop. 3.1] that \mathcal{K} is defined by quartic equations. Since there are 36 quartic multiples of the quadric (2.6), the space of quartics in eight variables has dimension 330 and the space $L(8\Theta)^+$ has dimension 260, there must be at least 34 further independent quartics vanishing on \mathcal{K} : the space of quartics vanishing on \mathcal{K} is the kernel of $\text{Sym}^4 L(2\Theta) \rightarrow L(8\Theta)^+$, which has dimension ≥ 70 . We can find these quartics as follows.

There are 15 quartic relations in $(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6, \xi_7)$ coming from the quartics defining \mathcal{Q} . They are given by the 4×4 minors of the matrix (2.4), which restricted to \mathcal{V} is

$$(2.7) \quad M = \begin{pmatrix} 2f_0\xi_1 & f_1\xi_1 & \xi_7 & \xi_6 & \xi_4 \\ f_1\xi_1 & 2(f_2\xi_1 - \xi_7) & f_3\xi_1 - \xi_6 & \xi_5 - \xi_4 & \xi_3 \\ \xi_7 & f_3\xi_1 - \xi_6 & 2(f_4\xi_1 - \xi_5) & f_5\xi_1 - \xi_3 & \xi_2 \\ \xi_6 & \xi_5 - \xi_4 & f_5\xi_1 - \xi_3 & 2(f_6\xi_1 - \xi_2) & f_7\xi_1 \\ \xi_4 & \xi_3 & \xi_2 & f_7\xi_1 & 2f_8\xi_1 \end{pmatrix}.$$

Since these relations do not involve ξ_8 , they cannot be multiples of the quadratic relation. We find 55 further independent quartics vanishing on \mathcal{K} (and thence a basis of the ‘new’ space of quartics that are not multiples of the quadratic relation) by searching for polynomials of given degree and weight that vanish on \mathcal{V} when pulled back to \mathbb{A}^{15} . Removing those that are multiples of the invariant quadric, we obtain quartics with the following 34 pairs of degree and weight:

$$\text{deg} = 4: \quad \text{wt} = 12, 13, 14, 14, 15, 15, 16, 16, 16, 17, 17, 18, 18, 19, 20;$$

$$\text{deg} = 5: \quad \text{wt} = 17, 18, 18, 19, 19, 20, 20, 20, 21, 21, 22, 22, 23;$$

$$\text{deg} = 6: \quad \text{wt} = 22, 23, 24, 24, 25, 26.$$

(Recall that ‘degree’ refers to the degree in terms of the original η_{ij} .) These quartics are given in the file `Kum3-quartics.magma` at [Data]. The quartics are scaled so that their coefficients are in $\mathbb{Z}[f_0, \dots, f_8]$. The 15 quartics of degree 4 are exactly those obtained as 4×4 -minors of the matrix M above.

Lemma 2.2. *Let $f_0, \dots, f_8 \in k$ be arbitrary. Then the 70 quartics constructed as described above are linearly independent over k .*

Proof. We can find[★] 70 monomials such that the 70×70 -matrix formed by the coefficients of the quartics with respect to these monomials has determinant ± 1 . \square

Note that regarding k , this is a slight improvement over [Mü3, Lemma 3.2], where k was assumed to have characteristic $\neq 2, 3, 5$.

We now show that these quartics indeed give all the relations.

Lemma 2.3. *The natural map $\text{Sym}^2 L(4\Theta)^+ \rightarrow L(8\Theta)^+$ is surjective.*

Proof. Mumford shows [Mum, §4, Thm. 1] that $\text{Sym}^2 L(4\Theta) \rightarrow L(8\Theta)$ is surjective. The proof can be modified to give the corresponding result for the even subspaces, as follows (we use the notations of [Mum]). We work with the even functions $\delta_{a+b} + \delta_{-a-b}$ and $\delta_{a-b} + \delta_{-a+b}$. This gives

$$\begin{aligned} & \sum_{\eta \in Z_2} l(\eta)(\delta_{a+b+\eta} + \delta_{-a-b-\eta}) * (\delta_{a-b+\eta} + \delta_{-a+b-\eta}) \\ &= \left(\sum_{\eta \in Z_2} l(\eta)q_1(b+\eta) \right) \left(\sum_{\eta \in Z_2} l(\eta)(\delta_{a+\eta} + \delta_{-a-\eta}) \right) \\ & \quad + \left(\sum_{\eta \in Z_2} l(\eta)q_1(a+\eta) \right) \left(\sum_{\eta \in Z_2} l(\eta)(\delta_{b+\eta} + \delta_{-b-\eta}) \right). \end{aligned}$$

We fix the homomorphism $l: Z_2 \rightarrow \{\pm 1\}$ and the class of $a \bmod K(\delta)$. By (*) in [Mum, p. 339] there is some b in this class such that $\sum_{\eta} l(\eta)q(b+\eta) \neq 0$. Taking $a = b$, we see that

$$\Delta(b) := \sum_{\eta} l(\eta)(\delta_{b+\eta} + \delta_{-b-\eta})$$

is in the image. Using this, we see that for all other a in the class, $\Delta(a)$ is also in the image. Inverting the Fourier transform, we find that all $\delta_a + \delta_{-a}$ are in the image, which therefore consists of all even functions. \square

Corollary 2.4. *The natural map $\text{Sym}^4 L(2\Theta) \rightarrow L(8\Theta)^+$ is surjective.*

Proof. Note that $L(2\Theta) = L(2\Theta)^+$, so the image of $\text{Sym}^4 L(2\Theta) \rightarrow L(8\Theta)$ is contained in the even subspace. Since there is exactly one quadratic relation, the map $\text{Sym}^2 L(2\Theta) \rightarrow L(4\Theta)^+$ is not surjective, but has a one-dimensional cokernel.

We will see below in Section 7 that this cokernel is generated by the image of a function Ξ such that $\xi_i \xi_j \Xi$ (for all i, j) and Ξ^2 can be expressed as quartics in the ξ_i . This implies that the image of the map in the statement contains the image of $\text{Sym}^2 L(4\Theta)^+$, and surjectivity follows from Lemma 2.3. Note that once we have found Ξ explicitly, the assertions relating to it made above can be checked directly and without relying on the considerations leading to the determination of Ξ . \square

Theorem 2.5. *Let k be a field of characteristic different from 2 and let $F \in k[x, z]$ be homogeneous of degree 8 and squarefree. Then the image \mathcal{K} in \mathbb{P}^7 of the Kummer variety associated to the Jacobian variety of the hyperelliptic curve $y^2 = F(x, 1)$ is defined by the quadric (2.6) and the 34 quartics constructed above.*

Proof. By Corollary 2.4 the dimension of the space of quartics vanishing on \mathcal{K} is 70. By Lemma 2.2 the quadric and the 34 quartics give rise to 70 independent quartics vanishing on \mathcal{K} . By [Mü3, Prop. 3.1] \mathcal{K} can be defined by quartics, so the claim follows. \square

This improves on [Mü3, Thm. 3.3] by removing the genericity assumption (and allowing characteristic 3 or 5).

To conclude this section, we determine the images of some special points on \mathcal{J} under the map to \mathcal{K} .

The discussion on page 8 shows that on a point $[(x_1, y_1) + (x_2, y_2) + \mathfrak{m}] \in \Theta$, the map restricts to

$$\begin{aligned} & \left(0 : 1 : -(x_1 + x_2) : x_1 x_2 : x_1^2 + x_1 x_2 + x_2^2 \right. \\ & \quad \left. : -(x_1 + x_2)x_1 x_2 : (x_1 x_2)^2 : \frac{2y_1 y_2 - G(x_1, x_2)}{(x_1 - x_2)^2} \right). \end{aligned}$$

If we write $(X - x_1)(X - x_2) = \sigma_0 X^2 + \sigma_1 X + \sigma_2$, then this can be written as

$$(0 : \sigma_0^2 : \sigma_0 \sigma_1 : \sigma_0 \sigma_2 : \sigma_1^2 - \sigma_0 \sigma_2 : \sigma_1 \sigma_2 : \sigma_2^2 : \xi_8),$$

where, rewriting $((x_1 - x_2)^2 \xi_8 - G(x_1, x_2))^2 = 4F(x_1, 1)F(x_2, 1)$, we have that

$$\begin{aligned}
& (\sigma_1^2 - 4\sigma_0\sigma_2)\xi_8^2 \\
& + (4f_0\sigma_0^4 - 2f_1\sigma_0^3\sigma_1 + 4f_2\sigma_0^3\sigma_2 - 2f_3\sigma_0^2\sigma_1\sigma_2 + 4f_4\sigma_0^2\sigma_2^2 \\
& \quad - 2f_5\sigma_0\sigma_1\sigma_2^2 + 4f_6\sigma_0\sigma_2^3 - 2f_7\sigma_1\sigma_2^3 + 4f_8\sigma_2^4)\xi_8 \\
& + (-4f_0f_2 + f_1^2)\sigma_0^6 + 4f_0f_3\sigma_0^5\sigma_1 - 2f_1f_3\sigma_0^5\sigma_2 - 4f_0f_4\sigma_0^4\sigma_1^2 \\
& \quad + (-4f_0f_5 + 4f_1f_4)\sigma_0^4\sigma_1\sigma_2 + (-4f_0f_6 + 2f_1f_5 - 4f_2f_4 + f_3^2)\sigma_0^4\sigma_2^2 \\
& \quad + 4f_0f_5\sigma_0^3\sigma_1^3 + (8f_0f_6 - 4f_1f_5)\sigma_0^3\sigma_1^2\sigma_2 + (8f_0f_7 - 4f_1f_6 + 4f_2f_5)\sigma_0^3\sigma_1\sigma_2^2 \\
& \quad + (-2f_1f_7 - 2f_3f_5)\sigma_0^3\sigma_2^3 - 4f_0f_6\sigma_0^2\sigma_1^4 + (-12f_0f_7 + 4f_1f_6)\sigma_0^2\sigma_1^3\sigma_2 \\
& \quad + (-16f_0f_8 + 8f_1f_7 - 4f_2f_6)\sigma_0^2\sigma_1^2\sigma_2^2 + (8f_1f_8 - 4f_2f_7 + 4f_3f_6)\sigma_0^2\sigma_1\sigma_2^3 \\
& \quad + (-4f_2f_8 + 2f_3f_7 - 4f_4f_6 + f_5^2)\sigma_0^2\sigma_2^4 + 4f_0f_7\sigma_0\sigma_1^5 \\
& \quad + (16f_0f_8 - 4f_1f_7)\sigma_0\sigma_1^4\sigma_2 + (-12f_1f_8 + 4f_2f_7)\sigma_0\sigma_1^3\sigma_2^2 \\
& \quad + (8f_2f_8 - 4f_3f_7)\sigma_0\sigma_1^2\sigma_2^3 + (-4f_3f_8 + 4f_4f_7)\sigma_0\sigma_1\sigma_2^4 - 2f_5f_7\sigma_0\sigma_2^5 \\
& \quad - 4f_0f_8\sigma_1^6 + 4f_1f_8\sigma_1^5\sigma_2 - 4f_2f_8\sigma_1^4\sigma_2^2 + 4f_3f_8\sigma_1^3\sigma_2^3 - 4f_4f_8\sigma_1^2\sigma_2^4 \\
& \quad + 4f_5f_8\sigma_1\sigma_2^5 + (-4f_6f_8 + f_7^2)\sigma_2^6 \\
& = 0.
\end{aligned}$$

(This is similar to the quartic defining the Kummer surface in the genus 2 case.) The image on \mathcal{K} of the theta divisor is a surface of degree 12 in $\mathbb{P}^6 = \mathbb{P}^7 \cap \{\xi_1 = 0\}$; the intersection of \mathcal{K} with the hyperplane $\xi_1 = 0$ is twice the image of Θ . (The equation above is cubic in the middle six coordinates and ξ_8 , so we get three times the degree of the Veronese surface. It is known that \mathcal{K} has degree 24.)

When (x_2, y_2) approaches $(x_1, -y_1)$, then the last coordinate tends to infinity, whereas the remaining ones stay bounded, so the origin on \mathcal{J} is mapped to

$$o := (0 : 0 : 0 : 0 : 0 : 0 : 0 : 1).$$

Points in $\mathcal{J}[2]$ are represented by factorizations $F = GH$ with $d = \deg G$ even, compare Section 5 below. Writing

$$G = g_d x^d + g_{d-1} x^{d-1} z + \dots + g_0 z^d \quad \text{and} \quad H = h_{8-d} x^{8-d} + h_{7-d} x^{7-d} z + \dots + h_0 z^{8-d},$$

we see that a 2-torsion point represented by (G, H) with $\deg G = 2$ maps to

$$(2.8) \quad (0 : g_2^2 : g_1 g_2 : g_0 g_2 : g_1^2 - g_0 g_2 : g_0 g_1 : g_0^2 : g_0^3 h_6 + g_0^2 g_2 h_4 + g_0 g_2^2 h_2 + g_2^3 h_0).$$

A 2-torsion point represented by (G, H) with $\deg G = 4$ maps to

$$(2.9) \quad \begin{aligned} & (1 : g_2h_4 + g_4h_2 : g_1h_4 + g_4h_1 : g_0h_4 + g_4h_0 \\ & \quad : g_0h_4 + g_4h_0 + g_1h_3 + g_3h_1 : g_0h_3 + g_3h_0 : g_0h_2 + g_2h_0 \\ & \quad : (g_0h_4 + g_4h_0)^2 + (g_0h_2 + g_2h_0)(g_2h_4 + g_4h_2) + (g_1h_0 - g_0h_1)(g_4h_3 - g_3h_4)); \end{aligned}$$

this is obtained by taking $(A, B, C) = (G, 0, H)$ in our original parameterization.

3. TRANSFORMATIONS

We compare our coordinates for the Kummer variety with those of Stubbs [Stu], Duquesne [Duq] and Müller [Mü1] in the special case $f_8 = 0$. In this case there is a rational Weierstrass point at infinity, and we can fix the representation of a point outside of Θ by requiring that A vanishes at infinity and that $\deg B(x, 1) < \deg A(x, 1)$. For a generic point P on \mathcal{J} , $\deg A(x, 1) = 3$; let (x_j, y_j) for $j = 1, 2, 3$ be the three points in the effective divisor D such that $P = [D - 3 \cdot \infty]$. Generically, the three points are distinct. Then

$$A(x, 1) = (x - x_1)(x - x_2)(x - x_3)$$

and $B(x, 1)$ is the interpolation polynomial such that $B(x_j, 1) = y_j$ for $j = 1, 2, 3$. We obtain the c_j from $C = (B^2 - F)/A$ by polynomial division. This leads to[★]

$$\begin{aligned} \xi_1 &= \kappa_1 \\ \xi_2 &= -f_7\kappa_2 \\ \xi_3 &= f_7\kappa_3 \\ \xi_4 &= -f_7\kappa_4 \\ \xi_5 &= f_4\kappa_1 + f_5\kappa_2 + 2f_6\kappa_3 + 3f_7\kappa_4 - \kappa_5 \\ \xi_6 &= f_3\kappa_1 + f_4\kappa_2 + f_5\kappa_3 - \kappa_6 \\ \xi_7 &= f_2\kappa_1 - f_4\kappa_3 - 3f_5\kappa_4 - \kappa_7 \\ \xi_8 &= -f_2f_7\kappa_2 - f_3f_7\kappa_3 - f_4f_7\kappa_4 + f_7\kappa_8 \end{aligned}$$

where $\kappa_1, \kappa_2, \dots, \kappa_8$ are the coordinates used by the other authors.

We consider the effect of a transformation of the curve equation. First suppose that $\tilde{F}(x, z) = F(x + \lambda z, z)$ (corresponding to a shift of the x -coordinate in the affine equation). A point represented by a triple $(A(x, z), B(x, z), C(x, z))$ of polynomials will correspond to the point $(\tilde{A}(x, z), \tilde{B}(x, z), \tilde{C}(x, z))$ with $\tilde{A}(x, z) = A(x + \lambda z, z)$

and analogously for \tilde{B} and \tilde{C} . We obtain[★]

$$\begin{aligned}
\tilde{\xi}_1 &= \xi_1 \\
\tilde{\xi}_2 &= \xi_2 + 3\lambda f_7 \xi_1 + 12\lambda^2 f_8 \xi_1 \\
\tilde{\xi}_3 &= \xi_3 + 2\lambda \xi_2 + 3\lambda^2 f_7 \xi_1 + 8\lambda^3 f_8 \xi_1 \\
\tilde{\xi}_4 &= \xi_4 + \lambda \xi_3 + \lambda^2 \xi_2 + \lambda^3 f_7 \xi_1 + 2\lambda^4 f_8 \xi_1 \\
\tilde{\xi}_5 &= \xi_5 + \lambda(2f_5 \xi_1 + 3\xi_3) + \lambda^2(6f_6 \xi_1 + 3\xi_2) + 17\lambda^3 f_7 \xi_1 + 34\lambda^4 f_8 \xi_1 \\
\tilde{\xi}_6 &= \xi_6 + \lambda(3\xi_4 + \xi_5) + \lambda^2(f_5 \xi_1 + 3\xi_3) + \lambda^3(2f_6 \xi_1 + 2\xi_2) + 5\lambda^4 f_7 \xi_1 + 8\lambda^5 f_8 \xi_1 \\
\tilde{\xi}_7 &= \xi_7 + \lambda(f_3 \xi_1 + 2\xi_6) + \lambda^2(2f_4 \xi_1 + 3\xi_4 + \xi_5) + \lambda^3(4f_5 \xi_1 + 2\xi_3) \\
&\quad + \lambda^4(6f_6 \xi_1 + \xi_2) + 9\lambda^5 f_7 \xi_1 + 12\lambda^6 f_8 \xi_1 \\
\tilde{\xi}_8 &= \xi_8 + \lambda(f_3 \xi_2 + 2f_5 \xi_4 + 3f_7 \xi_7) \\
&\quad + \lambda^2(3f_3 f_7 \xi_1 + 2f_4 \xi_2 + f_5 \xi_3 + 6f_6 \xi_4 + 3f_7 \xi_6 + 12f_8 \xi_7) \\
&\quad + \lambda^3((12f_3 f_8 + 6f_4 f_7) \xi_1 + 4f_5 \xi_2 + 4f_6 \xi_3 + 17f_7 \xi_4 + f_7 \xi_5 + 16f_8 \xi_6) \\
&\quad + \lambda^4((24f_4 f_8 + 11f_5 f_7) \xi_1 + 8f_6 \xi_2 + 12f_7 \xi_3 + 46f_8 \xi_4 + 6f_8 \xi_5) \\
&\quad + \lambda^5((44f_5 f_8 + 18f_6 f_7) \xi_1 + 16f_7 \xi_2 + 32f_8 \xi_3) \\
&\quad + \lambda^6((68f_6 f_8 + 29f_7^2) \xi_1 + 32f_8 \xi_2) + 148\lambda^7 f_7 f_8 \xi_1 + 148\lambda^8 f_8^2 \xi_1
\end{aligned}$$

For the transformation given by $\tilde{F}(x, z) = F(z, x)$, we have

$$\tilde{a}_j = a_{4-j}, \quad \tilde{b}_j = b_{4-j}, \quad \tilde{c}_j = c_{4-j}$$

and therefore

$$(\tilde{\xi}_1, \tilde{\xi}_2, \tilde{\xi}_3, \tilde{\xi}_4, \tilde{\xi}_5, \tilde{\xi}_6, \tilde{\xi}_7, \tilde{\xi}_8) = (\xi_1, \xi_7, \xi_6, \xi_4, \xi_5, \xi_3, \xi_2, \xi_8).$$

More generally, consider an element

$$\sigma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}(2)$$

acting by $(x, z) \mapsto (rx + sz, tx + uz)$. Let $\Sigma \in \mathrm{GL}(5)$ be the matrix whose columns are the coefficients of $(rx + sz)^j (tx + uz)^{4-j}$, for $j = 0, 1, 2, 3, 4$ (this is the matrix giving the action of σ on the fourth symmetric power of the standard representation of $\mathrm{GL}(2)$). Recall the matrix L from (2.3) whose rows contain the coefficients of A , B and C . Then the effect on our variables a_i, b_i, c_i is given by $L \mapsto L\Sigma^\top$. With D as in (2.2), we have $L^\top DL = M$ with M as in (2.7). So the effect of σ on M is given by $M \mapsto \Sigma M \Sigma^\top$. Note that $\tilde{\xi}_1 = \xi_1$ and that we can extract $\tilde{\xi}_2, \dots, \tilde{\xi}_7$ from M ; to get $\tilde{\xi}_8$ when ξ_1 is not invertible, we can perform a generic computation and then specialize.

This allows us to reduce our more general setting to the situation when there is a Weierstrass point at infinity: we adjoin a root of $F(x, 1)$, then we shift this root to zero and invert. This leads to an equation with $f_8 = 0$. This was used to obtain the matrix representing the action of an even 2-torsion point, see below in Section 5.

4. LIFTING POINTS TO THE JACOBIAN

Let $P \in \mathcal{K}(k)$ be a k -rational point on the Kummer variety. We want to decide if $P = \kappa(P')$ for a k -rational point P' on the Jacobian \mathcal{J} . Consider an odd function h on \mathcal{J} (i.e., such that $h(-Q) = -h(Q)$ for $Q \in \mathcal{J}$) such that h is defined over k ; then $h(P') \in k$ (or h as a pole at P'). Since h^2 is an even function, it descends to a function on \mathcal{K} , and we must have that $h^2(P) = h^2(P') = h(P')^2$ is a square in k . Conversely, any non-zero odd function h on \mathcal{J} will generically separate the two points in the fiber of the double cover $\mathcal{J} \rightarrow \mathcal{K}$, so if $h^2(P)$ is a non-zero square in k , then this implies that P lifts to a k -rational point on \mathcal{J} .

So we will now exhibit some odd functions that we can use to decide if a point lifts. Since $L(2\Theta)$ consists of even functions only, we look at $L(3\Theta)$, which has dimension $3^3 = 27$. Its subspace of even functions has dimension 14 and is spanned by ξ_1, \dots, ξ_8 , the five quadratics $\xi_2(\xi_4 + \xi_5) - \xi_3^2$, $\xi_2\xi_6 - \xi_3\xi_4$, $\xi_2\xi_6 - \xi_4^2$, $\xi_3\xi_6 - \xi_4\xi_7$, $(\xi_4 + \xi_5)\xi_7 - \xi_6^2$ and a further function, which can be taken to be[★]

$$2(2f_0\xi_2^2 - f_1\xi_2\xi_3 + 2f_2\xi_2\xi_4 - f_3\xi_2\xi_6 + 2f_4\xi_2\xi_7 - f_5\xi_3\xi_7 + 2f_6\xi_4\xi_7 - f_7\xi_6\xi_7 + 2f_8\xi_7^2) - 7\xi_2\xi_4\xi_7 + \xi_2\xi_5\xi_7 + \xi_2\xi_6^2 + \xi_3^2\xi_7 + 4\xi_3\xi_4\xi_6 - 2\xi_3\xi_5\xi_6 + \xi_4^3 - 5\xi_4^2\xi_5 + 2\xi_4\xi_5^2.$$

The subspace of odd functions has dimension 13. We obtain a ten-dimensional subspace of this space by considering the coefficients of $A_l \wedge B_l \wedge C_l$, which is an expression of degree 3, of odd degree in B and invariant even under $\text{SL}(3)$ acting on (A, B, C) . (One can check that there are no further Γ -invariants of degree 3.) These coefficients are given by the 3×3 -minors of the matrix L of (2.3). If we denote the minor corresponding to $0 \leq i < j < k \leq 4$ by μ_{ijk} , then we find

$$(4.1) \quad \mu_{ijk}^2 = \eta_{ii}\eta_{jk}^2 + \eta_{jj}\eta_{ik}^2 + \eta_{kk}\eta_{ij}^2 - 4\eta_{ii}\eta_{jj}\eta_{kk} - \eta_{ij}\eta_{ik}\eta_{jk}.$$

If L_{ijk} is the corresponding 3×3 submatrix of L , then we have that

$$\mu_{ijk}^2 = \det(L_{ijk})^2 = -\frac{1}{2} \det(L_{ijk}^\top D L_{ijk})$$

with D as in (2.2). We also have that $L^\top D L = M$, where M is the matrix corresponding to the quadratic form $B_l^2 - A_l C_l$ given in (2.7). We can express this by saying that μ_{ijk}^2 is $-\frac{1}{2}$ times the corresponding principal minor of M . In the same way, one sees that $\mu_{ijk}\mu_{i'j'k'}$ is $-\frac{1}{2}$ times the minor of M given by selecting rows i, j, k and columns i', j', k' . This shows that if one $\mu_{ijk}^2(P)$ is a non-zero square in k , then all $\mu_{i'j'k'}^2(P)$ are squares in k . All ten of them vanish simultaneously if

and only if A , B and C are linearly dependent (this is equivalent to the rank of $B_l^2 - A_l C_l$ being at most 2). The dimension of the space spanned by A , B and C cannot be strictly less than 2, since this would imply that F is a constant times a square, which contradicts the assumption that F is squarefree. So we can write A , B and C as linear combinations of two polynomials A' and C' , and after a suitable change of basis, we find that $F = B^2 - AC = A'C'$. This means that the point is the image of a 2-torsion point on \mathcal{J} , and it will always lift.

So for a point P in $\mathcal{K}(k)$ with $\xi_1 = 1$ (hence outside the theta divisor) to lift to a point in $\mathcal{J}(k)$, it is necessary that all these expressions, when evaluated at P , are squares in k , and sufficient that one of them gives a non-zero square. For points with $\xi_1 = 0$, we can use the explicit description of the image of Θ given in Section 2.

Geometrically, the map $\mathcal{V} \rightarrow \mathcal{X} \setminus \Theta$ is a conic bundle: for a point on \mathcal{X} outside the theta divisor, all effective divisors representing it are in general position, and the corresponding linear system has dimension 1 by the Riemann-Roch Theorem, so the fibers are Severi-Brauer varieties of dimension 1. If \mathcal{C} has a k -rational point P , then the bundle has a section (and so is in fact a \mathbb{P}^1 -bundle), since we can select the unique representative containing P in its support. If k is a number field and \mathcal{C} has points over every completion of k , then all the conics in fibers above k -rational points on $\mathcal{X} \setminus \Theta$ have points over all completions of k and therefore are isomorphic to \mathbb{P}^1 over k . We can check whether a k -defined divisor representing a lift of P to a k -rational point on \mathcal{J} exists and find one in this case in the following way. We assume that P is not in the image of Θ and is not the image of a 2-torsion point. We are looking for a matrix $\tilde{L} \in \mathbb{A}^{15}(k)$ representing a lift $P' \in \mathcal{J}(k)$ of P . Since we exclude 2-torsion, the matrix \tilde{L} must have rank 3, and there is a minor μ_{ijk} such that $\mu_{ijk}^2(P) = \mu_{ijk}(P')^2$ is a non-zero square in k . The rank of $M(P) = \tilde{L}^\top D \tilde{L}$ is also 3, so both $L(\tilde{P})$ and $M(P)$ have the same 2-dimensional kernel. We can compute the kernel from $M(P)$ and then we find the space generated by the rows of \tilde{L} as its annihilator, which is simply given by rows i, j, k of $M(P)$. If we find an invertible 3×3 matrix U with entries in k such that $M_{ijk}(P) = U^\top D U$ (where M_{ijk} is the principal 3×3 submatrix of M given by rows and columns i, j, k), then we can find a suitable matrix \tilde{L} whose rows are in the space generated by rows i, j, k of $M(P)$ and such that $\tilde{L}_{ijk} = U$. Then $\tilde{L}^\top D \tilde{L} = M(P)$, so \tilde{L} gives us the desired representative. Finding U is equivalent to finding an isomorphism between the quadratic forms given by

$$(x_1, x_2, x_3)M_{ijk}(P)(x_1, x_2, x_3)^\top \quad \text{and} \quad 2x_1x_3 - 2x_2^2,$$

for whose existence a necessary condition is that $\det M_{ijk}(P) = -2\mu_{ijk}^2(P)$ is a square times $\det D = -2$. Given this, the problem comes down to finding a point on the conic given by the first form (which is the conic making up the fiber above P' or $-P'$) and then parameterizing the conic using lines through the point.

Remark 4.1. One can check[★] that the following three expressions are a possible choice for the missing three basis elements of the odd subspace of $L(3\Theta)$:

$$\begin{aligned} & \xi_2\mu_{012} - \xi_3\mu_{013} + \xi_5\mu_{014} \\ & \xi_3\mu_{014} - (\xi_4 + \xi_5)\mu_{024} + \xi_4\mu_{123} + \xi_6\mu_{034} \\ & \xi_5\mu_{034} - \xi_6\mu_{134} + \xi_7\mu_{234} \end{aligned}$$

5. THE ACTION OF THE 2-TORSION SUBGROUP ON \mathcal{K}

We follow the approach taken in [Sto1] and consider the action of the 2-torsion subgroup of \mathcal{J} on \mathcal{K} and the ambient projective space. Note that translation by a 2-torsion point commutes with negation on \mathcal{J} , so the translation descends to an automorphism of \mathcal{K} , and since 2Θ is linearly equivalent to its translate, this automorphism actually is induced by an automorphism of the ambient \mathbb{P}^7 .

We will see that this projective representation of $\mathcal{J}[2] \simeq (\mathbb{Z}/2\mathbb{Z})^6$ can be lifted to a representation of a central extension of $\mathcal{J}[2]$ by μ_2 on the space of linear forms in the coordinates ξ_1, \dots, ξ_8 . This representation is irreducible. In the next section, we consider this representation and the induced representations on the spaces of quadratic and quartic forms in ξ_1, \dots, ξ_8 , whereas in this section, we obtain an explicit description of the action of $\mathcal{J}[2]$ on \mathbb{P}^7 .

There is a natural bijection between the 2-torsion subgroup $\mathcal{J}[2]$ of the Jacobian and the set of unordered partitions of the set $\Omega \subset \mathbb{P}^1$ of zeros of F into two subsets of even cardinality. The torsion point T corresponding to a partition $\{\Omega_1, \Omega_2\}$ is

$$\left[\sum_{\omega \in \Omega_1} (\omega, 0) \right] - \frac{\#\Omega_1}{2} \mathbf{m} = \left[\sum_{\omega \in \Omega_2} (\omega, 0) \right] - \frac{\#\Omega_2}{2} \mathbf{m}.$$

Since $\#\Omega = 8$ is divisible by 4, the quantity $\varepsilon(T) = (-1)^{\#\Omega_1/2} = (-1)^{\#\Omega_2/2}$ is well-defined. We say that T is *even* if $\varepsilon(T) = 1$ and *odd* if $\varepsilon(T) = -1$. By definition, the even 2-torsion points are the 35 points corresponding to a partition into two sets of four roots, together with the origin, and the odd 2-torsion points are the 28 points corresponding to a partition into subsets of sizes 2 and 6. The Weil pairing of two torsion points T and T' represented by $\{\Omega_1, \Omega_2\}$ and $\{\Omega'_1, \Omega'_2\}$, respectively, is given by

$$e_2(T, T') = (-1)^{\#(\Omega_1 \cap \Omega'_1)}.$$

It is then easy to check that

$$(5.1) \quad e_2(T, T') = \varepsilon(T)\varepsilon(T')\varepsilon(T + T').$$

Note that Pic_C^0 is canonically isomorphic to Pic_C^2 (by adding the class of \mathbf{m}), which contains the theta characteristics. ($\mathfrak{D} \in \text{Pic}_C^2$ is a *theta characteristic* when $2\mathfrak{D} = \mathfrak{W}$.) In this way, the theta characteristics are identified with the 2-torsion points,

and the odd (resp., even) theta characteristics correspond to the odd (resp., even) 2-torsion points.

Using the transformations described in Section 3 and the matrices obtained by Duquesne [Duq] representing the translation by a 2-torsion point, we find the corresponding matrices in our setting for an even nontrivial 2-torsion point. The matrices corresponding to odd 2-torsion points can then also be derived. For each factorization $F = GH$ into two forms of even degree, there is a matrix $M_{(G,H)}$ whose entries are polynomials with integral coefficients in the coefficients of G and H and whose image in $\mathrm{PGL}(8)$ gives the action of the corresponding 2-torsion point. These entries are too large to be reproduced here, but are given in the file `Kum3-torsionmats.magma` at [Data].

The matrices satisfy the relations[★]

$$(5.2) \quad M_{(G,H)}^2 = \mathrm{Res}(G, H)I_8 \quad \text{and} \quad \det M_{(G,H)} = \mathrm{Res}(G, H)^4,$$

where Res denotes the resultant of two binary forms. Let

$$S = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

be the matrix corresponding to the quadratic relation (2.6) satisfied by points on the Kummer variety.

Definition 5.1. We will write $\langle \cdot, \cdot \rangle_S$ for the pairing given by S . Concretely, for vectors $\underline{\xi} = (\xi_1, \dots, \xi_8)$ and $\underline{\zeta} = (\zeta_1, \dots, \zeta_8)$, we have

$$\langle \underline{\xi}, \underline{\zeta} \rangle_S = \xi_1\zeta_8 - \xi_2\zeta_7 + \xi_3\zeta_6 - \xi_4\zeta_5 - \xi_5\zeta_4 + \xi_6\zeta_3 - \xi_7\zeta_2 + \xi_8\zeta_1.$$

One checks[★] that for all G, H as above,

$$(SM_{(G,H)})^\top = (-1)^{(\deg G)/2} SM_{(G,H)}.$$

If $T \neq 0$ is even, then all corresponding matrices $M_{(G,H)}$ are equal; we denote this matrix by M_T . In this case, also the resultant $\mathrm{Res}(G, H)$ depends only on T ; we write it $r(T)$, so that we have $M_T^2 = r(T)I_8$. For T odd and represented by (G, H) with $\deg G = 2$, we have $M_{(\lambda G, \lambda^{-1}H)} = \lambda^2 M_{(G,H)}$. As a special case, we have $M_{(1,F)} = I_8$. For $T \neq 0$ even, the entry in the upper right corner of M_T is 1, for all other 2-torsion points, this entry is zero.

For a 2-torsion point $T \in \mathcal{J}[2]$, if we denote by M_T the matrix corresponding to one of the factorizations defining T , we therefore have (using that $S = S^\top = S^{-1}$)

$$(SM_T)^\top = \varepsilon(T)SM_T, \quad \text{or equivalently,} \quad M_T = \varepsilon(T)SM_T^\top S.$$

This implies (using that $M_{T'}M_T$ is, up to scaling, a matrix corresponding to $T+T'$)

$$\begin{aligned} M_TM_{T'} &= \varepsilon(T)SM_T^\top S \cdot \varepsilon(T')SM_{T'}^\top S \\ &= \varepsilon(T)\varepsilon(T')S(M_{T'}M_T)^\top S = \varepsilon(T)\varepsilon(T')\varepsilon(T+T')M_{T'}M_T \end{aligned}$$

Using (5.1), we recover the well-known fact that

$$(5.3) \quad M_TM_{T'} = e_2(T, T')M_{T'}M_T.$$

Since M_T^2 is a scalar matrix, the relation given above implies that the quadratic relation is invariant (up to scaling) under the action of $\mathcal{J}[2]$ on \mathbb{P}^7 :

$$M_T^\top SM_T = \text{Res}(G, H)S.$$

6. THE ACTION ON LINEAR, QUADRATIC AND QUARTIC FORMS

We work over an algebraically closed field k of characteristic different from 2. The first result describes a representation of a central extension G of $\mathcal{J}[2]$ on the space of linear forms that lifts the action on \mathbb{P}^7 .

Lemma 6.1. *There is a subgroup G of $\text{SL}(8)$ and an exact sequence*

$$0 \longrightarrow \mu_2 \longrightarrow G \longrightarrow \mathcal{J}[2] \longrightarrow 0$$

induced by the standard sequence

$$0 \longrightarrow \mu_8 \longrightarrow \text{SL}(8) \longrightarrow \text{PSL}(8) \longrightarrow 0$$

and the embedding $\mathcal{J}[2] \rightarrow \text{PSL}(8)$ given by associating to T the class of any matrix M_T .

Proof. Let $T \in \mathcal{J}[2]$ and let $M_T \in \text{GL}(8)$ be any matrix associated to T . Then $M_T^2 = cI_8$ with some c (compare (5.2)), and we let \tilde{M}_T denote one of the two matrices γM_T where $\gamma^2 c = \varepsilon(T)$. Then $\tilde{M}_T \in \text{SL}(8)$, since (again by (5.2))

$$\det \tilde{M}_T = \gamma^8 \det M_T = (\varepsilon(T)c^{-1})^4 c^4 = 1.$$

Since any two choices of M_T differ only by scaling, \tilde{M}_T is well-defined up to sign. Among the lifts of the class of M_T in $\text{PSL}(8)$ to $\text{SL}(8)$, $\pm \tilde{M}_T$ are characterized by the relation $\tilde{M}_T^2 = \varepsilon(T)I_8$. We now set

$$G = \{\pm \tilde{M}_T : T \in \mathcal{J}[2]\}.$$

It is clear that G surjects onto the image of $\mathcal{J}[2]$ in $\mathrm{PSL}(8)$ and that the map is two-to-one. It remains to show that G is a group. So let $T, T' \in \mathcal{J}[2]$. Then $\tilde{M}_T \tilde{M}_{T'}$ is a matrix corresponding to $T + T'$. Since (using (5.3) and (5.1))

$$\begin{aligned} (\tilde{M}_T \tilde{M}_{T'})^2 &= \tilde{M}_T \tilde{M}_{T'} \tilde{M}_T \tilde{M}_{T'} = e_2(T, T') \tilde{M}_T^2 \tilde{M}_{T'}^2 \\ &= e_2(T, T') \varepsilon(T) \varepsilon(T') I_8 = \varepsilon(T + T') I_8, \end{aligned}$$

we find that $\tilde{M}_T \tilde{M}_{T'} \in G$. \square

Remark 6.2. Note that the situation here is somewhat different from the situation in genus 2, as discussed in [Sto1]. In the even genus hyperelliptic case, the theta characteristics live in $\mathrm{Pic}^{\mathrm{odd}}$ rather than in $\mathrm{Pic}^{\mathrm{even}}$ and can therefore not be identified with the 2-torsion points. The effect is that there is no map $\varepsilon: \mathcal{J}[2] \rightarrow \mu_2$ that induces the Weil pairing as in (5.1), so that we have to use a fourfold covering of $\mathcal{J}[2]$ in $\mathrm{SL}(4)$ rather than a double cover.

We now proceed to a study of the representations of G on linear, quadratic and quartic forms on \mathbb{P}^7 that are induced by $G \subset \mathrm{SL}(8)$. The representation ρ_1 on the space V_1 of linear forms is the standard representation. For its character χ_1 , we find

$$\chi_1(\pm I_8) = \pm 8 \quad \text{and} \quad \chi_1(\pm \tilde{M}_T) = 0 \quad \text{for all } T \neq 0.$$

This follows from the observation that T can be written as $T = T' + T''$ with $e_2(T', T'') = -1$. Since $\pm \tilde{M}_T = \tilde{M}_{T'} \tilde{M}_{T''} = -\tilde{M}_{T''} \tilde{M}_{T'}$, the trace of \tilde{M}_T must be zero. We deduce that ρ_1 is irreducible. (ρ_1 is essentially the representation $V(\delta)$ in [Mum], where $\delta = (2, 2, 2)$ in our case.)

The representation ρ_2 on the space V_2 of quadratic forms is the symmetric square of ρ_1 . Since $\pm I_8$ act trivially on even degree forms, ρ_2 descends to a representation of $\mathcal{J}[2]$. Its character χ_2 is given by

$$\begin{aligned} \chi_2(0) &= 36 \quad \text{and} \\ \chi_2(T) &= \frac{1}{2} (\chi_1(\tilde{M}_T)^2 + \chi_1(\tilde{M}_T^2)) = \frac{1}{2} (0 + 8\varepsilon(T)) = 4\varepsilon(T) \quad \text{for } T \neq 0. \end{aligned}$$

Since $\mathcal{J}[2]$ is abelian, this representation has to split into a direct sum of one-dimensional representations. Let χ_T denote the character of $\mathcal{J}[2]$ given by $\chi_T(T') = e_2(T, T')$. Then the above implies that

$$(6.1) \quad \rho_2 = \bigoplus_{T: \varepsilon(T)=1} \chi_T.$$

So for each even $T \in \mathcal{J}[2]$, there is a one-dimensional eigenspace of quadratic forms such that the action of T' is given by multiplication with $e_2(T, T')$. For $T = 0$, this eigenspace is spanned by the invariant quadratic (2.6).

Definition 6.3. We set

$$y_0 = 2(\xi_1 \xi_8 - \xi_2 \xi_7 + \xi_3 \xi_6 - \xi_4 \xi_5);$$

this is the quadratic form corresponding to the matrix S in the sense that $y_0(\underline{\xi}) = \underline{\xi} S \underline{\xi}^\top = \langle \underline{\xi}, \underline{\xi} \rangle_S$. For nontrivial even T , we denote by y_T the form in the eigenspace corresponding to T that has coefficient 1 on ξ_8^2 . We will see that this makes sense, i.e., that this coefficient is always nonzero.

Lemma 6.4. *For every nontrivial even 2-torsion point T , the matrix corresponding to the quadratic form y_T is the symmetric matrix SM_T . In particular, if T corresponds to a factorization $F = GH$ into two polynomials of degree 4, then the coefficients of y_T are polynomials in the coefficients of G and H with integral coefficients, and the coefficients of the monomials $\xi_i \xi_j$ with $i \neq j$ are divisible by 2.*

Proof. We show that $\tilde{M}_{T'}^\top (SM_T) \tilde{M}_{T'} = e_2(T, T') SM_T$. We use that $\tilde{M}_{T'}^2 = \varepsilon(T') I_8$, $S \tilde{M}_{T'} = \varepsilon(T') \tilde{M}_{T'}^\top S$ and the fact that the Weil pairing is given by commutators. This gives

$$\tilde{M}_{T'}^\top SM_T \tilde{M}_{T'} = \varepsilon(T') S \tilde{M}_{T'} M_T \tilde{M}_{T'} = \varepsilon(T') e_2(T, T') SM_T \tilde{M}_{T'}^2 = e_2(T, T') SM_T$$

as desired, so SM_T gives a quadratic form in the correct eigenspace. Since the upper right entry of M_T is 1, the lower right entry, which corresponds to the coefficient of ξ_8^2 , of SM_T is 1, so that we indeed obtain y_T . \square

We can express y_T as $y_T(\underline{\xi}) = \langle \underline{\xi}, \underline{\xi} M_T^\top \rangle_S$.

Remark 6.5. Note that if T is an odd 2-torsion point, represented by the factorization (G, H) , then the same argument shows that the alternating bilinear form corresponding to the matrix $SM_{(G,H)}$ is multiplied by $e_2(T, T')$ under the action of $T' \in \mathcal{J}[2]$.

We set

$$(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7, \varepsilon_8) = (1, -1, 1, -1, -1, 1, -1, 1);$$

these are the entries occurring in S along the diagonal from upper right to lower left.

Corollary 6.6. *Let T be a nontrivial even 2-torsion point with image on \mathcal{K} given by*

$$(1 : \tau_2 : \tau_3 : \tau_4 : \tau_5 : \tau_6 : \tau_7 : \tau_8).$$

Then

$$y_T = \xi_8^2 + 2 \sum_{j=2}^8 \varepsilon_j \tau_j \xi_{9-j} \xi_8 + (\text{terms not involving } \xi_8).$$

A similar statement is true for $T = 0$ if we take coordinates $(0 : \dots : 0 : 1)$: $y_0 = 2\xi_1 \xi_8 + (\text{terms not involving } \xi_8)$.

Proof. The last column of M_T has entries $1, \tau_2, \dots, \tau_8$ (since M_T maps the origin to the image of T and has upper right entry 1). Multiplication by S from the left reverses the order and introduces the signs ε_j . Since the coefficients of y_T of monomials involving ξ_8 are given by the entries of the last column of SM_T by Lemma 6.4, the claim follows. \square

We define a pairing on the space of bilinear forms $V_1 \otimes V_1$ as follows. If the bilinear forms ϕ and ϕ' are represented by matrices A and A' with respect to our standard basis ξ_1, \dots, ξ_8 of V_1 , then $\langle \phi, \phi' \rangle = \frac{1}{8} \text{Tr}(A^\top A')$ (the scaling has the effect of giving the standard quadratic form norm 1).

For an even 2-torsion point T , we write \tilde{y}_T for the symmetric bilinear form corresponding to the matrix $S\tilde{M}_T$ (this is well-defined up to sign) and \tilde{z}_T for the symmetric bilinear form corresponding to $S\tilde{M}_T^\top = \tilde{M}_T S$. Also, z_T will denote the form corresponding to $SM_T^\top = M_T S$. Then, since $S(M_T S)S = SM_T$, we have the relation $z_T(\underline{\xi}) = y_T(\underline{\xi}S)$; explicitly,

$$z_T(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6, \xi_7, \xi_8) = y_T(\xi_8, -\xi_7, \xi_6, -\xi_5, -\xi_4, \xi_3, -\xi_2, \xi_1).$$

Lemma 6.7. *For all even 2-torsion points T and T' , we have*

$$\langle \tilde{z}_T, \tilde{y}_{T'} \rangle = \begin{cases} 1 & \text{if } T = T', \\ 0 & \text{if } T \neq T'. \end{cases}$$

Equivalently,

$$\langle z_T, y_{T'} \rangle = \begin{cases} r(T) & \text{if } T = T', \\ 0 & \text{if } T \neq T'. \end{cases}$$

Here we restrict the scalar product defined above to $V_2 \subset V_1 \otimes V_1$.

Proof. The claim is that $\text{Tr}((S\tilde{M}_T^\top)^\top(S\tilde{M}_{T'}))$ is zero if $T \neq T'$ and equals 8 if $T = T'$. We have

$$\text{Tr}((S\tilde{M}_T^\top)^\top(S\tilde{M}_{T'})) = \text{Tr}(\tilde{M}_T S^2 \tilde{M}_{T'}) = \text{Tr}(\tilde{M}_T \tilde{M}_{T'}) = \pm \text{Tr}(\tilde{M}_{T+T'}).$$

If $T \neq T'$, then this trace is zero, as we had already seen. If $T = T'$, then $\pm \tilde{M}_{T+T'} = I_8$, so the result is 8 as desired. \square

This allows us to express the ξ_j^2 in terms of the y_T . We set $r(0) = 1$ and $M_0 = I_8$. We denote the coefficient of $\xi_i \xi_j$ in a quadratic form $q \in V_2$ by $[\xi_i \xi_j]q$

Lemma 6.8. *For every $j \in \{1, 2, \dots, 8\}$, we have*

$$\xi_j^2 = \sum_{T: \varepsilon(T)=1} \frac{[\xi_{9-j}^2]y_T}{8r(T)} y_T.$$

Similarly, for $1 \leq i < j \leq 8$, we have

$$2\xi_i\xi_j = \varepsilon_i\varepsilon_j \sum_{T: \varepsilon(T)=1} \frac{[\xi_{9-i}\xi_{9-j}]y_T}{8r(T)}y_T.$$

Proof. We have by Lemma 6.7

$$\begin{aligned} \xi_j^2 &= \sum_{T: \varepsilon(T)=1} \langle \tilde{z}_T, \xi_j^2 \rangle \tilde{y}_T = \sum_{T: \varepsilon(T)=1} \frac{\langle z_T, \xi_j^2 \rangle}{r(T)} y_T \\ &= \sum_{T: \varepsilon(T)=1} \frac{[\xi_j^2]z_T}{8r(T)} y_T = \sum_{T: \varepsilon(T)=1} \frac{[\xi_{9-j}^2]y_T}{8r(T)} y_T. \end{aligned}$$

In the same way, we have for $i \neq j$ that

$$\begin{aligned} 2\xi_i\xi_j &= \sum_{T: \varepsilon(T)=1} 2\langle \tilde{z}_T, \xi_i\xi_j \rangle \tilde{y}_T = \sum_{T: \varepsilon(T)=1} 2\frac{\langle z_T, \xi_i\xi_j \rangle}{r(T)} y_T \\ &= \sum_{T: \varepsilon(T)=1} \frac{[\xi_i\xi_j]z_T}{8r(T)} y_T = \varepsilon_i\varepsilon_j \sum_{T: \varepsilon(T)=1} \frac{[\xi_{9-i}\xi_{9-j}]y_T}{8r(T)} y_T. \end{aligned}$$

(Note that $8\langle z_T, \xi_i\xi_j \rangle$ is half the coefficient of $\xi_i\xi_j$ in z_T .) □

Corollary 6.9. *We have*

$$\sum_{T: \varepsilon(T)=1} \frac{1}{8r(T)} y_T(\underline{\xi}) y_T(\underline{\zeta}) = \left(\sum_{j=1}^8 \varepsilon_j \xi_j \zeta_{9-j} \right)^2 = \langle \underline{\xi}, \underline{\zeta} \rangle_S^2.$$

In particular, setting $\underline{\zeta} = \underline{\xi}$, we obtain

$$\sum_{T: \varepsilon(T)=1} \frac{1}{8r(T)} y_T^2 = y_0^2 = 4(\xi_1\xi_8 - \xi_2\xi_7 + \xi_3\xi_6 - \xi_4\xi_5)^2.$$

Proof. We compute using Lemma 6.8:

$$\begin{aligned} &\sum_{T: \varepsilon(T)=1} \frac{1}{8r(T)} y_T(\underline{\xi}) y_T(\underline{\zeta}) \\ &= \sum_{i=1}^8 \xi_i^2 \sum_{T: \varepsilon(T)=1} \frac{[\xi_i^2]y_T(\underline{\xi})}{8r(T)} y_T(\underline{\zeta}) + \sum_{1 \leq i < j \leq 8} \xi_i \xi_j \sum_{T: \varepsilon(T)=1} \frac{[\xi_i \xi_j]y_T(\underline{\xi})}{8r(T)} y_T(\underline{\zeta}) \\ &= \sum_{i=1}^8 \xi_i^2 \zeta_{9-i}^2 + 2 \sum_{1 \leq i < j \leq 8} \varepsilon_i \varepsilon_j \xi_i \xi_j \zeta_{9-i} \zeta_{9-j} \\ &= \left(\sum_{j=1}^8 \varepsilon_j \xi_j \zeta_{9-j} \right)^2. \end{aligned} \quad \square$$

Now we consider the representation ρ_4 of $\mathcal{J}[2]$ on the space V_4 of quartic forms. For its character χ_4 , we have the general formula

$$\chi_4(T) = \frac{1}{24}(\chi_1(\tilde{M}_T)^4 + 8\chi_1(\tilde{M}_T)\chi_1(\tilde{M}_T^3) + 3\chi_1(\tilde{M}_T^2)^2 + 6\chi_1(\tilde{M}_T)^2\chi_1(\tilde{M}_T^2) + 6\chi_1(\tilde{M}_T^4)).$$

This gives us that

$$\chi_4(0) = 330 \quad \text{and} \quad \chi_4(T) = 10 \quad \text{for } T \neq 0.$$

We deduce that

$$(6.2) \quad \rho_4 = \chi_0^{\oplus 15} \oplus \bigoplus_{T \neq 0} \chi_T^{\oplus 5}.$$

7. THE DUPLICATION MAP AND THE MISSING GENERATOR OF $L(4\Theta)^+$

We continue to work over a field k of characteristic $\neq 2$. We also continue to assume that $F \in k[x, z]$ is squarefree, so that \mathcal{C} is a smooth hyperelliptic curve of genus 3 over k .

Consider the commutative diagram

$$\begin{array}{ccc} \mathcal{J} & \xrightarrow{\cdot 2} & \mathcal{J} \\ \downarrow \kappa & & \downarrow \kappa \\ \mathcal{K} & \xrightarrow{\delta} & \mathcal{K} \hookrightarrow \mathbb{P}^7, \end{array}$$

where the map in the top row is multiplication by 2 and δ is the endomorphism of \mathcal{K} induced by it. Pulling back a hyperplane section to the copy of \mathcal{J} on the right, we obtain a divisor in the class of 2Θ . Pulling it further back to the copy on the left, we obtain a divisor in the class of the pull-back of 2Θ under duplication, which is the class of 8Θ (Θ is symmetric, so pulling back under multiplication by n multiplies its class by n^2). The combined map from the left \mathcal{J} to \mathbb{P}^7 then is given by an 8-dimensional subspace of $L(8\Theta)^+$; by Corollary 2.4 this means that δ is given by eight quartics in $\underline{\xi}$. Since δ maps o , the image of the origin on \mathcal{K} , to itself, we can normalize these quartics so that they evaluate to $(0, \dots, 0, 1)$ on $(0, \dots, 0, 1)$. We use $\underline{\delta} = (\delta_1, \dots, \delta_8)$ to denote these quartic forms; they are determined up to adding a quartic form vanishing on \mathcal{K} . We write $E_4 \subset V_4$ for the subspace of quartics vanishing on \mathcal{K} . Note that we can test whether a given homogeneous polynomial in $\underline{\xi}$ vanishes on \mathcal{K} by pulling it back to \mathcal{W} or to \mathbb{A}^{15} and checking whether it vanishes on \mathcal{V} .

We now determine the structure of E_4 as a representation of $\mathcal{J}[2]$ and we identify the space generated by $\underline{\delta}$ in V_4/E_4 .

Lemma 7.1.

- (1) *The restriction of ρ_4 to E_4 splits as $\rho_4|_{E_4} = \chi_0^{\oplus 7} \oplus \bigoplus_{T \neq 0} \chi_T$.*

- (2) *The images of $\delta_1, \dots, \delta_8$ form a basis of the quotient $V_4^{\mathcal{J}[2]}/E_4^{\mathcal{J}[2]}$ of invariant subspaces.*

Proof.

- (1) The dimension of E_4 is 70 by Theorem 2.5, and a subspace of dimension 36 is given by y_0V_2 . The latter splits in the same way as ρ_2 does. Since for the generic curve, the Galois action is transitive on the odd 2-torsion points and on the nontrivial even 2-torsion points, the multiplicities of all odd characters and those of all nontrivial even characters in $\rho_4|_{E_4}$ have to agree. The only way to make the numbers come out correctly is as indicated.
- (2) Since the result of duplicating a point is unchanged when a 2-torsion point is added to it, the images of all δ_j in V_4/E_4 must lie in the same eigenspace of the $\mathcal{J}[2]$ -action. Since K spans \mathbb{P}^7 and the duplication map $\delta: K \rightarrow K$ is surjective, the images of the δ_j in V_4/E_4 must be linearly independent. So they must live in an eigenspace of dimension at least eight. The only such eigenspace is that of the trivial character, which has dimension exactly $8 = 15 - 7$ by the first part. \square

We see that the 36 quartic forms y_T^2 for T an even 2-torsion point are in the invariant subspace of V_4 of dimension 15. Let $\mathcal{T}_{\text{even}}$ denote the finite k -scheme whose geometric points are the 36 even 2-torsion points (we can consider $\mathcal{T}_{\text{even}}$ as a subscheme of \mathcal{J} or of \mathcal{K}), and denote by k_{even} its coordinate ring; this is an étale k -algebra of dimension 36. Then $y: T \mapsto y_T$ can be considered as a quadratic form with coefficients in k_{even} and $r: T \mapsto r(T)$ is an element of k_{even}^\times .

Lemma 7.2. *The 36 coefficients $c_{ii} = [\xi_i^2]y$, for $1 \leq i \leq 8$, and $c_{ij} = \frac{1}{2}[\xi_i\xi_j]y$, for $1 \leq i < j \leq 8$, constitute a k -basis of k_{even} .*

Proof. We define further elements of k_{even} by

$$\tilde{c}_{ii} = \frac{1}{8r}[\xi_{9-i}^2]y \quad \text{and} \quad \tilde{c}_{ij} = \frac{\varepsilon_i\varepsilon_j}{8r}[\xi_{9-i}\xi_{9-j}]y.$$

Lemma 6.8 can be interpreted as saying that

$$\text{Tr}_{k_{\text{even}}/k}(\tilde{c}_{ij}c_{i'j'}) = \begin{cases} 1 & \text{if } (i, j) = (i', j'), \\ 0 & \text{otherwise.} \end{cases}$$

This shows that the given elements are linearly independent over k . \square

We can compute the structure constants of k_{even} with respect to this basis and use this to express y^2 in terms of the basis again. Extracting coefficients, we obtain 36 quartic forms with coefficients in k that all lie in the 15-dimensional space of invariants under $\mathcal{J}[2]$. We check \star that they indeed span a space of this dimension

$$\begin{aligned}
q_1 &= \xi_1 \xi_8^3 + 2(-f_2 \xi_2 + f_3 \xi_3 - f_4 \xi_4 - f_4 \xi_5 + f_5 \xi_6 - f_6 \xi_7) \xi_1 \xi_8^2 + \dots \\
q_2 &= \xi_2 \xi_8^3 + (4f_8(-f_0 \xi_2 + f_2 \xi_4 + f_4 \xi_7) - 2f_3 f_8 \xi_6 - f_5 f_7 \xi_7) \xi_1 \xi_8^2 + \dots \\
q_3 &= \xi_3 \xi_8^3 + (f_7(-2f_0 \xi_2 + 2f_2 \xi_4 + f_3 \xi_6) \\
&\quad + 2f_8(-2f_0 \xi_3 + 4f_1 \xi_4 - 2f_2 \xi_6 - f_3 \xi_7)) \xi_1 \xi_8^2 + \dots \\
q_4 &= \xi_4 \xi_8^3 + (-2f_0 f_7 \xi_3 + (12f_0 f_8 + f_1 f_7) \xi_4 - 2f_1 f_8 \xi_6) \xi_1 \xi_8^2 + \dots \\
q_5 &= \xi_5 \xi_8^3 + ((4f_0 f_6 - 2f_1 f_5) \xi_2 + (-2f_0 f_7 - 2f_1 f_6 + 2f_2 f_5) \xi_3 \\
&\quad + (4f_0 f_8 + 4f_1 f_7 + 4f_2 f_6 - 5f_3 f_5) \xi_4 \\
&\quad + (-2f_1 f_8 - 2f_2 f_7 + 2f_3 f_6) \xi_6 + (4f_2 f_8 - 2f_3 f_7) \xi_7) \xi_1 \xi_8^2 + \dots \\
q_6 &= \xi_6 \xi_8^3 + (f_0(-2f_5 \xi_2 - 4f_6 \xi_3 + 8f_7 \xi_4 - 4f_8 \xi_6) \\
&\quad + f_1(f_5 \xi_3 + 2f_6 \xi_4 - 2f_8 \xi_7)) \xi_1 \xi_8^2 + \dots \\
q_7 &= \xi_7 \xi_8^3 + (4f_0(f_4 \xi_2 + f_6 \xi_4 - f_8 \xi_7) - f_1 f_3 \xi_2 - 2f_0 f_5 \xi_3) \xi_1 \xi_8^2 + \dots \\
q_8 &= \xi_8^4 + 16(f_1 f_8(f_1 \xi_2 - f_2 \xi_3 + f_3 \xi_4) + f_0 f_7(f_5 \xi_4 - f_6 \xi_6 + f_7 \xi_7)) \xi_1 \xi_8^2 + \dots \\
q_9 &= 2(f_7 \xi_6 - 4f_8 \xi_7) \xi_1 \xi_8^2 + \dots \\
q_{10} &= 2(f_5 \xi_4 - f_6 \xi_6 + f_7 \xi_7) \xi_1 \xi_8^2 + \dots \\
q_{11} &= 2(f_3 \xi_3 + 2f_4 \xi_4 - 2f_4 \xi_5 + f_5 \xi_6) \xi_1 \xi_8^2 + \dots \\
q_{12} &= 2(f_1 \xi_2 - f_2 \xi_3 + f_3 \xi_4) \xi_1 \xi_8^2 + \dots \\
q_{13} &= 2(-4f_0 \xi_2 + f_1 \xi_3) \xi_1 \xi_8^2 + \dots \\
q_{14} &= (3\xi_4 - \xi_5) \xi_1 \xi_8^2 + \dots \\
q_{15} &= \xi_1^2 \xi_8^2 + \dots = (\xi_1 \xi_8 - \xi_2 \xi_7 + \xi_3 \xi_6 - \xi_4 \xi_5)^2
\end{aligned}$$

FIGURE 1. A basis of the $\mathcal{J}[2]$ -invariant subspace of V_4 .

and that we get a subspace of dimension 7 of quartics vanishing on the Kummer variety.

It turns out[★] that the quartics in $V_4^{\mathcal{J}[2]}$ that vanish on \mathcal{K} are exactly those that do not contain terms cubic or quartic in ξ_8 . Forms spanning the complementary space are uniquely determined modulo $E_4^{\mathcal{J}[2]}$ by fixing the terms of higher degree in ξ_8 . We take $q_j = \xi_j \xi_8^3 + (\deg_{\xi_8} \leq 2)$ for $j = 1, \dots, 8$. Then the q_j can be chosen so that they have coefficients in $\mathbb{Z}[f_0, \dots, f_8]$. To fix q_j completely, it suffices to specify in addition the coefficients of $\xi_1 \xi_i \xi_8^2$ for $1 \leq i \leq 7$. One possibility is to choose them as given in Figure 1, which includes q_9, \dots, q_{15} in the

ideal of \mathcal{K} , where $E_4^{\mathcal{J}[2]} = \langle q_9, q_{10}, \dots, q_{15} \rangle$. These quartics can be obtained from `Kum3-invariants.magma` at [\[Data\]](#).

We can now identify the duplication map on \mathcal{K} .

Theorem 7.3. *The polynomials*

$$(\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8) = (4q_1, 4q_2, 4q_3, 4q_4, 4q_5, 4q_6, 4q_7, q_8).$$

in $V_4^{\mathcal{J}[2]}$ (with q_j as above) have the following properties.

- (1) $\delta_j \in \mathbb{Z}[f_0, f_1, \dots, f_8][\xi_1, \xi_2, \dots, \xi_8]$ for all $1 \leq j \leq 8$.
- (2) $(\delta_1, \delta_2, \dots, \delta_8)(0, 0, \dots, 0, 1) = (0, 0, \dots, 0, 1)$.
- (3) With y_T as defined earlier for an even 2-torsion point with image

$$(1 : \tau_2 : \tau_3 : \tau_4 : \tau_5 : \tau_6 : \tau_7 : \tau_8)$$

on \mathcal{K} , we have

$$y_T^2 \equiv \delta_8 - \tau_2\delta_7 + \tau_3\delta_6 - \tau_4\delta_5 - \tau_5\delta_4 + \tau_6\delta_3 - \tau_7\delta_2 + \tau_8\delta_1 = \langle \underline{\tau}, \underline{\delta} \rangle_S \bmod E_4^{\mathcal{J}[2]},$$

where $\underline{\tau} = (1, \tau_2, \dots, \tau_8)$ and $\underline{\delta} = (\delta_1, \dots, \delta_8)$.

- (4) The δ_j do not vanish simultaneously on \mathcal{K} .
- (5) The map $\delta: \mathcal{K} \rightarrow \mathcal{K}$ given by $(\delta_1 : \dots : \delta_8)$ is the duplication map on \mathcal{K} .

Proof.

- (1) This can be verified using the explicit polynomials.
- (2) This is obvious.
- (3) We compare the coefficients of $\xi_j \xi_8^3$ on both sides. Since by Corollary 6.6,

$$y_T = \xi_8^2 + 2\varepsilon_2\tau_2\xi_7\xi_8 + 2\varepsilon_3\tau_3\xi_6\xi_8 + \dots + 2\varepsilon_8\tau_8\xi_1\xi_8 + (\text{terms not involving } \xi_8),$$

we find

$$y_T^2 = \xi_8^4 + 4\varepsilon_2\tau_2\xi_7\xi_8^3 + \dots + 4\varepsilon_8\tau_8\xi_1\xi_8^3 + (\text{terms of degree } \leq 2 \text{ in } \xi_8)$$

and the right hand side has the same form. So the difference is a form in $V_4^{\mathcal{J}[2]}$ of degree at most 2 in ξ_8 , which implies that it is in $E_4^{\mathcal{J}[2]}$.

- (4) Let $\underline{\xi} \in k^8 \setminus \{0\}$ be coordinates of a point in \mathcal{K} . Then $\underline{\delta}(\underline{\xi}) = 0$ implies by (3) that $y_T(\underline{\xi}) = 0$ for all even 2-torsion points T (note that y_0 vanishes on all of \mathcal{K}). Lemma 6.8 then shows that $\underline{\xi} = 0$ as well, since $8r(T) \neq 0$ in k . This contradicts our choice of $\underline{\xi}$.
- (5) By (4), δ is a morphism $\mathcal{K} \rightarrow \mathbb{P}^7$, and by Lemma 7.1 (2) δ differs from the duplication map by post-composing with an automorphism α of \mathbb{P}^7 . We show[★] that on a generic point, δ coincides with the duplication map; this proves that α is the identity. We use the action of $\text{GL}(2)$ on (x, z) (and scaling on y) to reduce to the case that $F(x, 1)$ is monic of degree 7. A generic point P on \mathcal{J} can then be represented by (A, B, C) such that $A(x, 1)$ is monic of degree 3

and squarefree and $B(x, 1)$ is of degree ≤ 2 . After making a further affine transformation, we can assume that $A(x, 1) = x(x-1)(x-a)$ for some $a \in k$. The corresponding point on \mathcal{K} is then

$$\begin{aligned} \kappa(P) = & (1 : -a - 1 : a : 0 : -ac_3 - c_1 : -c_0 \\ & : (a+1)c_0 + 2b_0b_2 : -(a^2 + a + 1)c_0 - 2(a+1)b_0b_2), \end{aligned}$$

where $B(x, 1) = b_0 + b_1x + b_2x^2$, $C(x, 1) = c_0 + c_1x + c_2x^2 + c_3x^3 - x^4$. We compute $2P$ in terms of its Mumford representation using Cantor's algorithm as implemented in Magma and find $\kappa(2P)$. On the other hand, we compute $\delta(\kappa(P))$. Both points are equal, which proves the claim. \square

The quartics $\underline{\delta} = (\delta_1, \dots, \delta_8)$ are given in the file `Kum3-deltas.magma` at [\[Data\]](#).

The canonical map from $V_2 = \text{Sym}^2 L(2\Theta)$ to $L(4\Theta)$ has non-trivial one-dimensional kernel, spanned by the quadric y_0 vanishing on \mathcal{K} . Since the dimension of the even part $L(4\Theta)^+$ of $L(4\Theta)$ is $36 = \dim V_2$, the map $V_2 \rightarrow L(4\Theta)^+$ has a one-dimensional cokernel. Looking at the action of $\mathcal{J}[2]$ on $L(4\Theta)^+$, it is clear that this space splits as a direct sum of the image of V_2 and a one-dimensional invariant subspace. We will identify a generator of the latter.

Lemma 7.4. *The image of q_1 in $L(8\Theta)$ is the square of an element $\Xi \in L(4\Theta)^+$ that is invariant under the action of $\mathcal{J}[2]$.*

Proof. We pull back q_1 to a polynomial function on the affine space \mathbb{A}^{15} that parameterizes the triples of polynomials (A, B, C) . We find \star that this polynomial is the square of some other polynomial p that can be written as a quadratic in the components of $A_i \wedge B_i \wedge C_i$. So p is invariant under $\pm\Gamma$, which means that it gives an element Ξ of $L(4\Theta)^+$. \square

To make Ξ more explicit, we note that p can be expressed as a cubic in the ξ_j . Taking into account that $\xi_1 = 1$ on the affine space, we find that (up to the choice of a sign)

$$\begin{aligned} \xi_1 \Xi = & (-8f_0f_4f_8 + 2f_0f_5f_7 + 2f_1f_3f_8)\xi_1^3 - 4f_0f_6\xi_1^2\xi_2 + (-4f_0f_7 + 2f_1f_6)\xi_1^2\xi_3 \\ & + (-4f_0f_8 + 2f_1f_7 - 4f_2f_6 + f_3f_5)\xi_1^2\xi_4 + (12f_0f_8 - f_1f_7)\xi_1^2\xi_5 \\ & + (-4f_1f_8 + 2f_2f_7)\xi_1^2\xi_6 - 4f_2f_8\xi_1^2\xi_7 + 6f_0\xi_1\xi_2^2 - 3f_1\xi_1\xi_2\xi_3 + 6f_2\xi_1\xi_2\xi_4 \\ & - f_3\xi_1\xi_2\xi_6 - 2f_3\xi_1\xi_3\xi_4 + 2f_4\xi_1\xi_3\xi_6 - f_5\xi_1\xi_3\xi_7 + 4f_4\xi_1\xi_4^2 - 2f_4\xi_1\xi_4\xi_5 \\ & - 2f_5\xi_1\xi_4\xi_6 + 6f_6\xi_1\xi_4\xi_7 - 3f_7\xi_1\xi_6\xi_7 + 6f_8\xi_1\xi_7^2 - 11\xi_2\xi_4\xi_7 + \xi_2\xi_5\xi_7 + 2\xi_2\xi_6^2 \\ & + 2\xi_3^2\xi_7 + 5\xi_3\xi_4\xi_6 - 3\xi_3\xi_5\xi_6 + 2\xi_4^3 - 7\xi_4^2\xi_5 + 3\xi_4\xi_5^2 \end{aligned}$$

We obtain similar cubic expressions for $\xi_j \Xi$ with $j \in \{2, 3, \dots, 8\}$ by multiplying the polynomial above by ξ_j , then adding a suitable linear combination of the quartics vanishing on \mathcal{K} so that we obtain something that is divisible by ξ_1 . These

cubics are given in the file `Kum3-Xipols.magma` at [Data]. With this information, we can evaluate Ξ on any given set $\underline{\xi}$ of coordinates of a point on \mathcal{K} : we find an index j with $\xi_j \neq 0$ and evaluate Ξ as $(\xi_j \Xi)/\xi_j$.

This gives us a basis of $L(4\Theta)^+$ consisting of Ξ and the quadratic monomials in the ξ_j minus one of the monomials $\xi_j \xi_{9-j}$. Alternatively, we can use the basis consisting of Ξ and the y_T for the 35 nonzero even 2-torsion points T .

8. SUM AND DIFFERENCE ON THE KUMMER VARIETY

In this section, k continues to be a field of characteristic $\neq 2$ and F to be squarefree.

We consider the composition

$$\mathcal{J} \times \mathcal{J} \xrightarrow{(+,-)} \mathcal{J} \times \mathcal{J} \xrightarrow{(\kappa,\kappa)} \mathcal{K} \times \mathcal{K} \longrightarrow \mathbb{P}^7 \times \mathbb{P}^7 \xrightarrow{\text{Segre}} \mathbb{P}^{63} \xrightarrow{\text{symm.}} \mathbb{P}^{35}$$

where ‘symm.’ is the symmetrization map that sends a matrix A to $A + A^\top$ and we identify the Segre map with the multiplication map

$$(\text{column vectors}) \times (\text{row vectors}) \longrightarrow \text{matrices.}$$

Pulling back hyperplanes, we see that the map is given by sections of $4\Theta \times \{0\} + \{0\} \times 4\Theta$, hence symmetric bilinear forms on $L(4\Theta)$. The map is invariant under negation of either one of the arguments, therefore the bilinear forms only involve even sections. The map can be described by a symmetric matrix B of such bilinear forms such that in terms of coordinates (w_j) and (z_j) of the images $\kappa(P+Q)$ and $\kappa(P-Q)$ of $P \pm Q$ on \mathcal{K} , we have (up to scaling) $w_i z_j + w_j z_i = 2B_{ij}(\kappa(P), \kappa(Q))$. We normalize by requiring that $B_{88}(o, o) = 1$, where $o = (0, \dots, 0, 1)$.

We write \tilde{V}_2 for $L(4\Theta)^+$; then B can be interpreted as an element β of $\tilde{V}_2 \otimes \tilde{V}_2 \otimes V_2^*$. The last factor V_2^* is identified with the space of symmetric 8×8 matrices (whose entries are thought of representing $\frac{1}{2}(w_i z_j + w_j z_i)$ for coordinates \underline{w} and \underline{z} of points in \mathbb{P}^7) by specifying that a quadratic form $q \in V_2$ evaluates on such a matrix to $b(\underline{w}, \underline{z})$ where b is the bilinear form such that $q(\underline{x}) = b(\underline{x}, \underline{x})$. If M is the matrix of b and B is the matrix corresponding to the unordered pair $\{\underline{w}, \underline{z}\}$, then the pairing is $\text{Tr}(M^\top B) = 8\langle M, B \rangle$. Put differently, we obtain the (i, j) -entry of the matrix by evaluating at the quadratic form $\xi_i \xi_j$.

The 2-torsion group $\mathcal{J}[2]$ acts on each factor, and β must be invariant under the action of $\mathcal{J}[2] \times \mathcal{J}[2]$ such that (T, T') acts via $(T, T', T+T')$ on the three factors (shifting P by T and Q by T' shifts $P \pm Q$ by $T+T'$).

We use the basis of \tilde{V}_2 given by Ξ and y_T for the nonzero even 2-torsion points T (suitably extending k if necessary); for V_2^* we use the basis dual to $(y_T)_{T \text{ even}}$, which is given by the linear forms

$$y_T^*: v \longmapsto \frac{1}{r(T)} \langle z_T, v \rangle.$$

If T_1, T_2, T_3 are even 2-torsion points, then the effect of (T, T') acting on the corresponding basis element of the triple tensor product is to multiply it by

$$e_2(T, T_1)e_2(T', T_2)e_2(T + T', T_3) = e_2(T, T_1 + T_3)e_2(T', T_2 + T_3).$$

If this basis element occurs in β with a nonzero coefficient, then this factor must be 1 for all T, T' , which means that $T_1 = T_2 = T_3$. This shows that we must have

$$\beta = \sum_{T \neq 0} a_T (y_T \otimes y_T \otimes y_T^*) + a_0 (\Xi \otimes \Xi \otimes y_0^*).$$

If we evaluate at the origin in the first component, we obtain (using that Ξ vanishes there and that $y_T(o) = 1$ for $T \neq 0$ even)

$$\beta_o = \sum_{T \neq 0} a_T (y_T \otimes y_T^*).$$

This corresponds to taking $P = O$, resulting in the pair $\pm Q$ leading to $\{\kappa(Q), \kappa(Q)\}$. So, taking $\underline{\xi}$ as coordinates of Q and using $B_{88}(o, o) = 1$, the (i, j) -component of this expression, evaluated at $\underline{\xi}$ in the (now) first component of β_o , must be $\xi_i \xi_j$, up to a multiple of y_0 :

$$\xi_i \xi_j \equiv \sum_{T \neq 0} a_T y_T^*(\xi_i \xi_j) \cdot y_T \pmod{y_0}.$$

In other words, β_o , interpreted as a linear map $V_2 \rightarrow \tilde{V}_2$, is the canonical map; in particular, it sends y_T to y_T for all even $T \neq 0$, and so $a_T = 1$ for all $T \neq 0$. It only remains to find a_0 ; then β is completely determined. We consider the image of β in $\text{Sym}^2 \tilde{V}_2 \otimes V_2^*$, which corresponds to taking $P = Q$. This results in the unordered pair $\{2P, O\}$, represented (according to our normalization) by the symmetric matrix that is zero everywhere except in the last row and column, where it has entries $\frac{1}{2}\delta_1, \dots, \frac{1}{2}\delta_7, \delta_8$. We obtain (recall that $\Xi^2 = q_1$ and $\delta_1 = 4q_1$)

$$\sum_{T \neq 0} y_T^2 \otimes y_T^*(\xi_i \xi_j) + a_0 q_1 \otimes y_0^*(\xi_i \xi_j) = \begin{cases} 0 & \text{if } i, j < 8; \\ \frac{1}{2}\delta_i & \text{if } i < j = 8; \\ \delta_8 & \text{if } i = j = 8. \end{cases}$$

Evaluating at $y_0 = 2(\xi_1 \xi_8 - \xi_2 \xi_7 + \xi_3 \xi_6 - \xi_4 \xi_5)$, we find

$$a_0 q_1 = \delta_1 = 4q_1.$$

This shows that $a_0 = 4$. (Note that if we evaluate at y_T , we recover

$$y_T^2 = \sum_{j=1}^7 \frac{1}{2}\delta_j \cdot [\xi_j \xi_8] y_T + \delta_8 \cdot [\xi_8^2] y_T = \sum_{j=1}^7 \varepsilon_{9-j} \tau_{9-j} \delta_j + \delta_8).$$

We have shown:

Lemma 8.1. *The element $\beta \in \tilde{V}_2 \otimes \tilde{V}_2 \otimes V_2^*$ is given by*

$$\beta = \sum_{T \neq 0} y_T \otimes y_T \otimes y_T^* + 4\Xi \otimes \Xi \otimes y_0^*.$$

In terms of matrices, we have

$$(8.1) \quad 2B(\underline{\xi}, \underline{\zeta}) = \sum_{T \neq 0} \frac{y_T(\underline{\xi})y_T(\underline{\zeta})}{4r(T)} M_T S + \Xi(\underline{\xi})\Xi(\underline{\zeta})S.$$

To get the expression for B , note that y_T^* corresponds to the matrix

$$(y_T^*(\xi_i \xi_j))_{i,j} = \frac{1}{r(T)} (\langle z_T, \xi_i \xi_j \rangle)_{i,j} = \frac{1}{8r(T)} M_T S.$$

The resulting matrix of bi-quadratic forms corresponding to the first summand in (8.1) has entries that can be written as elements of $\mathbb{Z}[f_0, \dots, f_8][\underline{\xi}, \underline{\zeta}]$. The entries are given in the file `Kum3-biquforms.magma` at [Data]. More precisely, let

$$q = \xi_1(f_3 f_5 \xi_4 + f_1 f_7 \xi_5) + f_1 \xi_2 \xi_3 + f_3 \xi_2 \xi_6 + f_5 \xi_3 \xi_7 + f_7 \xi_6 \xi_7 + (\xi_4 + \xi_5) \xi_8,$$

then the entries of

$$B(\underline{\xi}, \underline{\zeta}) - \frac{1}{2}(q(\underline{\xi})q(\underline{\zeta}) + \Xi(\underline{\xi})\Xi(\underline{\zeta}))S$$

are (up to addition of multiples of $y_0(\underline{\xi})$ and $y_0(\underline{\zeta})$) in $\mathbb{Z}[f_0, \dots, f_8][\underline{\xi}, \underline{\zeta}]$. (Note that $q \equiv \Xi \pmod{(2, y_0)}$ so that the term in parentheses is divisible by 2.)

We can now use the matrix B to perform ‘pseudo-addition’ on \mathcal{K} in complete analogy to the case of genus 2 described in [FS]. This means that given $\kappa(P)$, $\kappa(Q)$ and $\kappa(P - Q)$, we can find $\kappa(P + Q)$. This in turn can be used to compute multiples of points on \mathcal{K} by a variant of the usual divide-and-conquer scheme (‘repeated squaring’).

We can make the upper left entry of B completely explicit.

Lemma 8.2. *Recall that $\langle \cdot, \cdot \rangle_S$ denotes the bilinear form corresponding to the matrix S . We have*

$$B_{11}(\underline{\xi}, \underline{\zeta}) \equiv \langle \underline{\xi}, \underline{\zeta} \rangle_S^2 \pmod{(y_0(\underline{\xi}), y_0(\underline{\zeta}))}.$$

Proof. This follows from $\langle z_T, \xi_1^2 \rangle = [\xi_8^2] y_T = 1$ (for $T \neq 0$) and Corollary 6.9:

$$B_{11}(\underline{\xi}, \underline{\zeta}) \equiv \sum_{T \neq 0} \frac{y_T(\underline{\xi})y_T(\underline{\zeta})}{8r(T)} = \langle \underline{\xi}, \underline{\zeta} \rangle_S^2. \quad \square$$

Corollary 8.3. *For two points $P, Q \in \mathcal{J}$ with images $\kappa(P), \kappa(Q) \in \mathcal{K}$, we have*

$$P \pm Q \in \Theta \iff \langle \kappa(P), \kappa(Q) \rangle_S = 0.$$

Proof. The bilinear form associated to S vanishes if and only if $B_{11}(\kappa(P), \kappa(Q))$ vanishes, which means that $\xi_1(P+Q)\xi_1(P-Q) = 0$, which in turn is equivalent to $P+Q \in \Theta$ or $P-Q \in \Theta$. \square

This is analogous to the duality between the Kummer Surface and the Dual Kummer Surface in the case of a curve of genus 2, see [CF, Thm. 4.3.1]. The difference is that here the Kummer variety is self-dual.

We can now also describe the locus of vanishing of y_T on \mathcal{K} .

Corollary 8.4. *Let $T \neq 0$ be an even 2-torsion point. Then for $P \in \mathcal{J}$, we have that $y_T(\kappa(P)) = 0$ if and only if $2P + T \in \Theta$.*

Proof. This is because $y_T^2 = \langle \kappa(T), \underline{\delta} \rangle_S$ (up to scaling). \square

For $T = 0$, we get that $\Xi(\kappa(P)) = 0$ if and only if $2P \in \Theta$. This is because $4\Xi^2 = \delta_1$.

9. FURTHER PROPERTIES OF THE DUPLICATION AND THE SUM-AND-DIFFERENCE MAPS

With a view of considering bad reduction later, we now allow k to be any field and $F \in k[x, z]$ to be any binary form of degree 8; in particular, $F = 0$ is allowed. Note that the relations deduced so far are valid over $\mathbb{Z}[f_0, \dots, f_8]$ and so can be specialized to any k and F . In this context, \mathcal{K} denotes the variety in \mathbb{P}_k^7 defined by the specializations of the quadric and the 34 quartics that define the Kummer variety in the generic case, and δ denotes the rational map (which now may have base points) from \mathcal{K} to itself given by the quartics $\underline{\delta}$. We can also still consider factorizations $F = GH$ into two factors of degree 4 (if $F = 0$, we take both of the factors to be the zero form of degree 4) and obtain points on \mathcal{K} that are specializations of the images of 2-torsion points. We will call equivalence classes of such factorizations (up to scaling) ‘nontrivial even 2-torsion points’ for simplicity, even though they do not in general arise from points of order 2 on some algebraic group. If T is such a nontrivial even 2-torsion point, then we denote the corresponding point on \mathcal{K} by $\kappa(T)$. We normalize the coordinates of $\kappa(T)$ such that the first coordinate is 1. We also have the associated quadratic form y_T . If $F = 0$, we obtain for example $\kappa(T) = (1 : 0 : \dots : 0)$ for the unique nontrivial even 2-torsion point, with associated quadratic form $y_T = \xi_8^2$.

We now state explicit criteria for the vanishing of $\underline{\delta}$ at a point on \mathcal{K} . We first exhibit a necessary condition. For the following, we assume k to be algebraically closed and of characteristic $\neq 2$.

Remark 9.1. Note that in characteristic 2 we have that $\delta_1 = \dots = \delta_7 = 0$ and $\delta_8 = y_T^2$ on \mathcal{K} for all T , where

$$y_T = \xi_8^2 + f_6 f_8 \xi_7^2 + f_4 f_8 \xi_6^2 + f_2 f_8 \xi_5^2 + f_4 f_6 \xi_4^2 + f_2 f_6 \xi_3^2 + f_2 f_4 \xi_2^2 + f_2 f_4 f_6 f_8 \xi_1^2,$$

which is the square of a linear form over k when k is perfect. Let \mathcal{L} denote the hyperplane defined by this linear form. Then δ restricts to a morphism on $\mathcal{K} \setminus \mathcal{L}$, which is constant with image the origin $(0 : \dots : 0 : 1)$.

Assume for now that $F \neq 0$ and write

$$F = F_0^2 F_1 \quad \text{with } F_1 \text{ squarefree.}$$

We define $\mathcal{T}(F)$ to be the set of nontrivial even 2-torsion points T associated to factorizations (G, H) with G and H both divisible by F_0 . So $\mathcal{T}(F)$ is in bijection with the unordered partitions of the roots of F_1 into two sets of equal size. We also define $\mathcal{T}(0)$ to be the one-element set $\{T\}$, where T corresponds to the factorization $0 = 0 \cdot 0$.

Lemma 9.2. *With the notation introduced above, the following statements are equivalent for a point on \mathcal{K} with coordinate vector $\underline{\xi}$:*

- (i) *For all $T \in \mathcal{T}(F)$, we have $\langle \kappa(T), \underline{\delta}(\underline{\xi}) \rangle_S = 0$.*
- (ii) *For all $T \in \mathcal{T}(F)$, we have $\langle \kappa(T), \underline{\xi} \rangle_S = 0$.*

In particular, $\underline{\delta}(\underline{\xi}) = 0$ implies $\langle \kappa(T), \underline{\xi} \rangle_S = 0$ for all $T \in \mathcal{T}(F)$.

Proof. By Theorem 7.3 (3), we have for all $T \in \mathcal{T}(F)$ that $y_T(\underline{\xi})^2 = \langle \kappa(T), \underline{\delta}(\underline{\xi}) \rangle_S$, so (i) is equivalent to $y_T(\underline{\xi}) = 0$ for all $T \in \mathcal{T}(F)$. When $F = 0$, we have $y_T = \xi_8^2$ and $\kappa(T) = (1 : 0 : \dots : 0)$ for the unique $T \in \mathcal{T}(F)$, so $y_T(\underline{\xi}) = 0$ is equivalent to $\xi_8 = 0$, which is equivalent to $\langle \kappa(T), \underline{\xi} \rangle_S = 0$. If, at the other extreme, F is squarefree, then one checks[★] that the coordinate vectors of the points in $\mathcal{T}(F)$ are linearly independent, which implies that (i) is equivalent to $\underline{\delta}(\underline{\xi}) = 0$ and (ii) is equivalent to $\underline{\xi} = 0$. The claim then follows from Theorem 7.3 (4).

We now assume that $F \neq 0$ and write $F = F_0^2 F_1$ as above with F_1 squarefree and F_0 non-constant. We check by an explicit computation[★] that

(*) *the y_T for $T \in \mathcal{T}(F)$ form a basis of the symmetric square of the space spanned by the linear forms $\langle \kappa(T), \cdot \rangle_S$ for $T \in \mathcal{T}(F)$.*

This implies that the vanishing of the y_T is equivalent to (ii). To verify (*), we can apply a transformation moving the roots of F_0 to an initial segment of $(0, \infty, 1, a)$ (where $a \in k \setminus \{0, 1\}$). The most involved case is when $\deg F_0 = 1$. We can then take $F_0 = x$ and find that the linear forms given by the $T \in \mathcal{T}(F)$ span $\langle \xi_4, \xi_6, \xi_7, \xi_8 \rangle$ and that the 10×10 matrix whose rows are the coefficient vectors of the y_T with respect to the monomials of degree 2 in these four variables has

determinant a power of two times a power of $\text{disc}(F_1)$, hence is invertible. The other cases are similar, but simpler. \square

This prompts the following definition.

Definition 9.3. We write $\mathcal{K}_{\text{good}}$ for the open subscheme

$$\mathcal{K} \setminus \{P : \langle \kappa(T), P \rangle_S = 0 \text{ for all } T \in \mathcal{T}(F)\}$$

of \mathcal{K} .

Lemma 9.2 now immediately implies the following.

Corollary 9.4. *The rational map $\delta: \mathcal{K} \rightarrow \mathcal{K}$ restricts to a morphism $\mathcal{K}_{\text{good}} \rightarrow \mathcal{K}_{\text{good}}$.*

We will now consider the ‘bad’ subset $\mathcal{K} \setminus \mathcal{K}_{\text{good}}$ of \mathcal{K} in more detail, in particular in relation to the base locus of δ , which it contains according to Corollary 9.4. We begin with a simple sufficient condition for a point to be in the base locus.

Lemma 9.5. *Assume that $F(x, z)$ is divisible by z^2 . Let $\underline{\xi}$ be the coordinate vector of a point on \mathcal{K} such that $\xi_2 = \xi_3 = \xi_4 = \xi_8 = 0$. Then $\underline{\delta}(\underline{\xi}) = 0$.*

Proof. Plugging $f_7 = f_8 = \xi_2 = \xi_3 = \xi_4 = \xi_8 = 0$ into the expressions for the δ_j gives zero \star . \square

We set

$$\mathcal{L}_\infty = \{(\xi_1 : \dots : \xi_8) \in \mathbb{P}^7 : \xi_2 = \xi_3 = \xi_4 = \xi_8 = 0\}.$$

Using the formulas given in Section 3 for the action on $\underline{\xi}$, one sees easily that \mathcal{L}_∞ is invariant under scaling of x and also under shifting $(x, z) \mapsto (x + \lambda z, z)$ (if $f_7 = f_8 = 0$), which together generate the stabilizer of ∞ in $\text{PGL}(2)$.

For F with a multiple root at some point $a \in \mathbb{P}^1$, let \tilde{F} be the result of acting on F by a linear substitution ϕ that moves a to ∞ ; then \tilde{F} is divisible by z^2 . We write $\mathcal{L}_a \subset \mathbb{P}^7$ for the image of \mathcal{L}_∞ under the automorphism of \mathbb{P}^7 induced by ϕ^{-1} . Since the stabilizer of ∞ in $\text{PGL}(2)$ leaves \mathcal{L}_∞ invariant, this definition of \mathcal{L}_a does not depend on the choice of ϕ . For example,

$$\mathcal{L}_0 = \{(\xi_1 : \dots : \xi_8) \in \mathbb{P}^7 : \xi_4 = \xi_6 = \xi_7 = \xi_8 = 0\}.$$

We write $A(F) \subset \mathbb{P}^1$ for the set of multiple roots of F . This is all of \mathbb{P}^1 when $F = 0$. Otherwise, $A(F)$ consists of the roots of F_0 when $F = F_0^2 F_1$ with F_1 squarefree.

Corollary 9.6. *If $P \in \mathcal{K} \cap \mathcal{L}_a$ for some $a \in A(F)$, then $\underline{\delta}(P) = 0$.*

Proof. This follows from Lemma 9.5 by applying a suitable automorphism of \mathbb{P}^1 . \square

So the base locus of δ contains $\mathcal{K} \cap \bigcup_{a \in A(F)} \mathcal{L}_a$. When F is not a nonzero square, we can show that this is exactly the ‘bad set’ $\mathcal{K} \setminus \mathcal{K}_{\text{good}}$.

Lemma 9.7. *Assume that F is not of the form $F = H^2$ with $H \neq 0$. Let P be in the ‘bad set’ $\mathcal{K} \setminus \mathcal{K}_{\text{good}}$. Then $P \in \mathcal{L}_a$ for some $a \in A(F)$. In particular,*

$$\mathcal{K}_{\text{good}} = \mathcal{K} \setminus \bigcup_{a \in A(F)} \mathcal{L}_a,$$

and $\mathcal{K} \setminus \mathcal{K}_{\text{good}} = \mathcal{K} \cap \bigcup_{a \in A(F)} \mathcal{L}_a$ is the base locus of δ .

Proof. Let $\underline{\xi}$ be a coordinate vector for P . We write $F = F_0^2 F_1$ with F_1 squarefree. We split the proof into various cases according to the factorization type of F_0 . If F_0 is constant, there is nothing to prove. Otherwise we move the roots of F_0 to an initial segment of $(0, \infty, 1)$.

1. $F_0 = x$. In this case the assumption is equivalent to $\xi_4 = \xi_6 = \xi_7 = \xi_8 = 0$ (compare the proof of Lemma 9.2), so that $P \in \mathcal{L}_0$.
2. $F_0 = x^2$. The assumption is $\xi_7 = \xi_8 = 0$; using the equations defining \mathcal{K} this implies \star $\xi_4 = \xi_6 = 0$, so $P \in \mathcal{L}_0$.
3. $F_0 = x^3$. The assumption is $\xi_8 = 0$, which in turn implies \star $\xi_7 = \xi_6 = \xi_4 = 0$, so $P \in \mathcal{L}_0$.
4. $F_0 = xz$. In this case the assumption is $\xi_4 = \xi_8 = 0$, which then implies \star $\xi_6 = \xi_7 = 0$ or $\xi_2 = \xi_3 = 0$, and so $P \in \mathcal{L}_0$ or $P \in \mathcal{L}_\infty$.
5. $F_0 = x^2z$. The assumption is $\xi_8 = 0$, which leads to \star $P \in \mathcal{L}_0$ or $P \in \mathcal{L}_\infty$.
6. $F_0 = xz(x - z)$. A similar computation shows \star that $P \in \mathcal{L}_0 \cup \mathcal{L}_1 \cup \mathcal{L}_\infty$.
7. $F = 0$. Here the assumption is $\xi_8 = 0$. The intersection $\mathcal{K} \cap \{\xi_8 = 0\}$ is defined \star by the 2×2 -minors of the matrix

$$\begin{pmatrix} \xi_2 & \xi_3 & \xi_4 \\ \xi_3 & \xi_4 + \xi_5 & \xi_6 \\ \xi_4 & \xi_6 & \xi_7 \end{pmatrix},$$

which therefore has rank 1 when evaluated on any point in $\mathcal{K} \cap \{\xi_8 = 0\}$. If $\xi_2 = 0$, then this implies that $\xi_3 = \xi_4 = 0$ as well, so that $P \in \mathcal{L}_\infty$. Otherwise, we can make a transformation shifting x/z by λ as in Section 3 that makes $\tilde{\xi}_7 = 0$ ($\tilde{\xi}_7$ is a polynomial of degree 4 in λ with leading coefficient ξ_2 , so we can find a suitable λ , since k is assumed to be algebraically closed). Then we get that $\tilde{\xi}_8 = \tilde{\xi}_7 = \tilde{\xi}_6 = \tilde{\xi}_4 = 0$, so the image point is in \mathcal{L}_0 , hence $P \in \mathcal{L}_\lambda$.

The last statement follows, since Corollary 9.4 shows that the base scheme of δ is contained in $\mathcal{K} \setminus \mathcal{K}_{\text{good}}$ and Corollary 9.6 shows that it contains the intersection of \mathcal{K} with the union of the \mathcal{L}_a . \square

We now consider the case $F = F_0^2 \neq 0$. Then the curve $y^2 = F(x, z) = F_0(x, z)^2$ splits into the two components $y = \pm F_0(x, z)$. The points on \mathcal{K} correspond to

linear equivalence classes of effective divisors of degree 4, modulo the action of the hyperelliptic involution. So there are three distinct possibilities how the points can be distributed among the two components: two on each, one and three, or all four on the same component. In the last case, we have $B \equiv \pm F_0 \pmod{A}$, and we can change the representative so that $B = \pm F_0$, which makes $C = 0$. So the two components of $\text{Pic}^4(\mathcal{C})$ consisting of classes of divisors whose support is contained in one of the two components of \mathcal{C} map to a single point $\omega \in \mathcal{K}$, which one can check[★] coincides with $\kappa(T)$ for the single $T \in \mathcal{T}(F)$; it satisfies $\underline{\delta}(\omega) = 0$.

Now a point P on the component of \mathcal{K} corresponding to the distribution of one and three points on the two components, if it is not in the base scheme of δ , must satisfy $\delta(P) = \omega$. So for such points we have $\underline{\delta}(\delta(P)) = 0$, but $\underline{\delta}(P) \neq 0$. Let $\underline{\xi}$ be coordinates for a point P with $\delta(P) = \omega = \kappa(T)$. Then $\langle \kappa(T), \underline{\delta}(\underline{\xi}) \rangle_S = \langle \kappa(T), \kappa(T) \rangle_S = 0$ (all points on \mathcal{K} satisfy $\langle \underline{\xi}, \underline{\xi} \rangle_S = y_0(\underline{\xi}) = 0$). By Lemma 9.2, this is equivalent to $\langle \kappa(T), \underline{\xi} \rangle_S = 0$. We write \mathcal{E} for the hyperplane given by $\langle \kappa(T), \underline{\xi} \rangle_S = 0$. So in this case $\mathcal{K}_{\text{good}} = \mathcal{K} \setminus \mathcal{E}$, and $P \in \mathcal{K} \cap \mathcal{E} = \mathcal{K} \setminus \mathcal{K}_{\text{good}}$ does not necessarily imply that $\underline{\delta}(P) = 0$. But we still have the following.

Lemma 9.8. *Assume that $F = F_0^2$ with $F_0 \neq 0$. If $P \in \mathcal{K}$ with $\underline{\delta}(P) = 0$, then $P \in \mathcal{L}_a$ for some $a \in A(F)$ (which here is simply the set of roots of F_0).*

Proof. We can again assume that the roots of F_0 are given by an initial segment of $(0, \infty, 1, a)$ (with $a \neq \infty, 0, 1$). We consider the various factorization types of F_0 in turn; they are represented by

$$F_0 = x^4, \quad x^3z, \quad x^2z^2, \quad x^2z(x-z) \quad \text{and} \quad xz(x-z)(x-az).$$

The computations[★] are similar to those done in the proof of Lemma 9.7. The most involved case is when F_0 has four distinct roots. To deal with it successfully, we make use of the Klein Four Group of automorphisms of the set of roots of F_0 . \square

We now have a precise description of the base scheme of the duplication map δ on \mathcal{K} , which is given by the quartic forms $\underline{\delta}$.

Proposition 9.9. *Let k be an algebraically closed field of characteristic $\neq 2$ and let $F \in k[x, z]$ be homogeneous of degree 8. We denote by \mathcal{K} and $\underline{\delta}$ the objects associated to F .*

- (1) *The base locus of δ is $\mathcal{K} \cap \bigcup_{a \in A(F)} \mathcal{L}_a$.*
- (2) *The base locus of $\delta \circ \delta$ is $\mathcal{K} \setminus \mathcal{K}_{\text{good}}$; δ can be iterated indefinitely on $\mathcal{K}_{\text{good}}$.*
- (3) *If F is not of the form $F = F_0^2$ with $F_0 \neq 0$, then the base locus of δ is $\mathcal{K} \setminus \mathcal{K}_{\text{good}}$.*

Proof.

- (1) Corollary 9.6 shows that the condition is sufficient. Conversely, if $\underline{\delta}(P) = 0$, then Lemmas 9.2, 9.7 and 9.8 show that $P \in \mathcal{L}_a$ for some multiple root a of F .

- (2) The second statement is Corollary 9.4. In view of (3), it is sufficient to consider the case $F = F_0^2 \neq 0$ for the first statement. If $P \in \mathcal{K} \setminus \mathcal{K}_{\text{good}}$ is not in the base locus of δ , then $\delta(P) = \omega$, which is in the base locus of δ , so P is in the base locus of $\delta \circ \delta$. Conversely, if P is in the base locus of $\delta \circ \delta$, then P cannot be in $\mathcal{K}_{\text{good}}$ by the second statement.
- (3) This follows from Corollary 9.4 and Lemma 9.7. \square

We can state a property of the ‘add-and-subtract’ morphism that is similar to that of δ given in Corollary 9.4. We write $\alpha: \text{Sym}^2 \mathcal{K} \rightarrow \text{Sym}^2 \mathcal{K}$ for the map given by the matrix B as defined in Section 8; this is defined for arbitrary $F \in k[x, z]$, homogeneous of degree 8. In general α is only a rational map.

Lemma 9.10. *Let k be an algebraically closed field of characteristic $\neq 2$ and let $F \in k[x, z]$ be homogeneous of degree 8. We denote by \mathcal{K} and $\underline{\delta}$ the objects associated to F . Then α restricts to a morphism $\text{Sym}^2 \mathcal{K}_{\text{good}} \rightarrow \text{Sym}^2 \mathcal{K}_{\text{good}}$.*

Proof. Note that generically, $\alpha \circ \alpha = \text{Sym}^2 \delta$ — this comes from the fact that

$$\{(P + Q) + (P - Q), (P + Q) - (P - Q)\} = \{2P, 2Q\}.$$

If we write $\underline{\xi} * \underline{\xi}'$ for the symmetric matrix $\underline{\xi}^\top \cdot \underline{\xi}' + \underline{\xi}'^\top \cdot \underline{\xi}$, then this relation shows that

$$(9.1) \quad \underline{\zeta} * \underline{\zeta}' = 2B(\underline{\xi}, \underline{\xi}') \implies \underline{\delta}(\underline{\xi}) * \underline{\delta}(\underline{\xi}') = 2B(\underline{\zeta}, \underline{\zeta}'),$$

up to a scalar factor, which we find to be 1 by taking $\underline{\xi} = \underline{\xi}' = (0, \dots, 0, 1)$. This is then a relation that is valid over $\mathbb{Z}[f_0, \dots, f_8]$.

Now let $\underline{\xi}$ and $\underline{\xi}'$ be projective coordinates of points in $\mathcal{K}_{\text{good}}$ and write $2B(\underline{\xi}, \underline{\xi}') = \underline{\zeta} * \underline{\zeta}'$ for suitable vectors $\underline{\zeta}, \underline{\zeta}'$. Then by Corollary 9.4, $\underline{\delta}(\underline{\xi})$ and $\underline{\delta}(\underline{\xi}')$ both do not vanish, so $\underline{\delta}(\underline{\xi}) * \underline{\delta}(\underline{\xi}') \neq 0$. This implies that $\underline{\zeta}, \underline{\zeta}' \neq 0$, which shows that α is defined on $\mathcal{K}_{\text{good}}$. If the point given by $\underline{\zeta} * \underline{\zeta}'$ were not in $\text{Sym}^2 \mathcal{K}_{\text{good}}$, then iterating α at most four more times would produce zero by Proposition 9.9 (2), contradicting the fact that δ can be iterated indefinitely on the points represented by $\underline{\xi}$ and $\underline{\xi}'$. \square

10. HEIGHTS

We now take k to be a number field (or some other field of characteristic $\neq 2$ with a collection of absolute values satisfying the product formula, for example a function field in one variable). We also assume again that $F \in k[x, z]$ is a squarefree binary octic form. Then \mathcal{C} is a curve of genus 2 over k , and we have the Jacobian \mathcal{J} and the Kummer variety \mathcal{K} associated to \mathcal{C} . We define the *naive height* on \mathcal{J} and on \mathcal{K}

to be the standard height on \mathbb{P}^7 with respect to the coordinates $(\xi_1 : \dots : \xi_8)$. We denote it by

$$h(P) = \sum_v n_v \log \max\{|\xi_1(P)|_v, \dots, |\xi_8(P)|_v\} \quad \text{for } P \in \mathcal{J}(k) \text{ or } \mathcal{K}(k)$$

where v runs through the places of k , the absolute values $|\cdot|_v$ extend the standard absolute values on \mathbb{Q} and $n_v = [K_v : \mathbb{Q}_w]$, where w is the place of \mathbb{Q} lying below v , so that we have the product formula

$$\prod_v |\alpha|_v^{n_v} = 1 \quad \text{for all } \alpha \in k^\times.$$

Then by general theory (see for example [HS, Part B]) the limit

$$\hat{h}(P) = \lim_{n \rightarrow \infty} \frac{h(nP)}{n^2}$$

exists and differs from $h(P)$ by a bounded amount. This is the *canonical height* of P . One of our goals in this section will be to find an explicit bound for

$$\beta = \sup_{P \in \mathcal{J}(k)} (h(P) - \hat{h}(P)).$$

We refer to [MS] for a detailed study of heights in the case of Jacobians of curves of genus 2, with input from [Sto1] and [Sto3]. We will now proceed to obtain some comparable results in our case of hyperelliptic genus 3 Jacobians. Most of this is based on the following telescoping series trick going back to Tate: we write

$$\hat{h}(P) = \lim_{n \rightarrow \infty} 4^{-n} h(2^n P) = h(P) + \sum_{n=0}^{\infty} 4^{-(n+1)} (h(2^{n+1} P) - 4h(2^n P))$$

and split the term $h(2P) - 4h(P)$ into local components as follows:

$$h(2P) - 4h(P) = \sum_v n_v (\max_j \log |\delta_j(\underline{\xi}(P))|_v - 4 \max_j \log |\xi_j(P)|_v) = \sum_v n_v \varepsilon_v(P)$$

with $\varepsilon_v(P) = \max_j \log |\delta_j(\underline{\xi}(P))|_v - 4 \max_j \log |\xi_j(P)|_v$, which is independent of the scaling of the coordinates $\underline{\xi}(P)$ and so can be defined for all $P \in \mathcal{J}(k_v)$ or $\mathcal{K}(k_v)$. Then $\varepsilon_v : \mathcal{K}(k_v) \rightarrow \mathbb{R}$ is continuous, so (since $\mathcal{K}(k_v)$ is compact) it is bounded. If $-\gamma_v \leq \inf_{P \in \mathcal{K}(k_v)} \varepsilon_v(P)$, then we have that

$$\beta \leq \sum_v n_v \sum_{n=0}^{\infty} 4^{-(n+1)} \gamma_v = \frac{1}{3} \sum_v n_v \gamma_v.$$

So we will now obtain estimates for γ_v . We follow closely the strategy of [Sto1]. Note that writing

$$\mu_v(P) = \sum_{n=0}^{\infty} 4^{-(n+1)} \varepsilon_v(2^n P) = \lim_{n \rightarrow \infty} 4^{-n} \max_j \log |\underline{\delta}^{\circ n}(\underline{\xi}(P))|_v - \max_j \log |\xi_j(P)|_v,$$

we also have that

$$\hat{h}(P) = h(P) + \sum_v n_v \mu_v(P).$$

We assume that the polynomial defining the curve \mathcal{C} has coefficients in the ring of integers of k . Then the matrices M_T defined in Section 5 for even 2-torsion points have entries that are algebraic integers. We use \mathcal{O} to denote the ring of all algebraic integers. Let $\underline{\xi}$ be coordinates of a point on \mathcal{K} . Then Theorem 7.3 (3) tells us that for all even 2-torsion points $T \neq 0$, we have that

$$y_T(\underline{\xi})^2 \in \mathcal{O}\delta_1(\underline{\xi}) + \mathcal{O}\delta_2(\underline{\xi}) + \dots + \mathcal{O}\delta_8(\underline{\xi})$$

and Lemma 6.8 tells us that (note that the coefficient of ξ_{9-j}^2 in y_0 is zero)

$$\xi_j^2 \in \sum_{T \neq 0, \text{even}} \frac{1}{8r(T)} \mathcal{O}y_T(\underline{\xi}).$$

Lemma 10.1. *Let v be a non-archimedean place of k . Then for $P \in \mathcal{K}(k_v)$, we have that*

$$\log |2^6 \text{disc}(F)|_v \leq \log \min_T |2^6 r(T)^2|_v \leq \varepsilon_v(P) \leq 0,$$

where T runs through the non-trivial even 2-torsion points.

Proof. Let $\underline{\xi}$ be coordinates for P and write $d_j = \delta_j(\underline{\xi})$ for $j = 1, \dots, 8$. Then for all even $T \neq 0$,

$$|y_T(\underline{\xi})|_v^2 \leq \max_j |d_j|_v$$

and

$$|\xi_j|_v^4 \leq \max_T |8r(T)|_v^{-2} |y_T(\underline{\xi})|_v^2 \leq \max_T |8r(T)|_v^{-2} \max_j |d_j|_v.$$

So

$$\varepsilon_v(P) = \log \max_j |d_j|_v - 4 \log \max_j |\xi_j|_v \geq \log \min_T |2^6 r(T)^2|_v.$$

Since $r(T)^2$ divides the discriminant $\text{disc}(F)$, the first inequality on the left also follows. The upper bound follows from the fact that the polynomials δ_j have integral coefficients. \square

Since $\varepsilon_v(P)$ is an integral multiple of the logarithm of the absolute value of a uniformizer π_v , we can sometimes gain a little bit by using

$$\varepsilon_v(P) \geq - \left\lfloor \max_T v(|2^6 r(T)^2|) \right\rfloor \log |\pi_v|_v,$$

where v denotes the v -adic additive valuation, normalized so that $v(\pi_v) = 1$.

Example 10.2. For the curve

$$y^2 = 4x^7 - 4x + 1,$$

over \mathbb{Q} and $v = 2$, the discriminant bound gives[★] $\varepsilon_2(P) \geq -22 \log 2$, since the discriminant of the polynomial on the right hand side (considered as a dehomogenized binary octic form) has 2-adic valuation 16. To get a better bound, we consider the resultants $r(T)$. If we write

$$f(x) = 4x^7 - 4x + 1 = 4g(x)h(x)$$

with g and h monic of degree 3 and 4, respectively, then $r(T) = 2^8 \text{Res}(g, h)$. From the Newton Polygon of f we see that all roots θ of f satisfy $v_2(\theta) = -2/7$. This gives $v_2(r(T)) \geq 32/7$. Since the product of all 35 resultants $r(T)$ is the tenth power of the discriminant, we must have equality. This gives the bound $\varepsilon_2(P) \geq -(15 + \frac{1}{7}) \log 2$, which can be improved to $-15 \log 2$, so that we get $-\mu_2 \leq 5 \log 2$.

Corollary 10.3. *Assume that $k = \mathbb{Q}$. Then we have that*

$$\beta \leq \frac{1}{3} \log |2^6 \text{disc}(F)| + \frac{1}{3} \gamma_\infty.$$

To get a bound on γ_∞ , we use the archimedean triangle inequality. We write $\tau_j(T)$ for the coordinates of a non-trivial even 2-torsion point T (with $\tau_1(T) = 1$) and $v_j(T)$ for the coefficients in the formula for ξ_j^2 , so that we have

$$\xi_j^2 = \sum_T v_j(T) y_T.$$

Lemma 10.4. *Let v be an archimedean place of k . Then we have that*

$$\gamma_v \leq \log \max_j \left(\sum_T |v_j(T)|_v \sqrt{\sum_{i=1}^8 |\tau_i(T)|_v} \right)^2.$$

Proof. Similarly as in the non-archimedean case, we have that

$$|y_T(\underline{\xi})|_v^2 \leq \sum_{j=1}^8 |\tau_j(T)|_v \max_j |d_j|_v$$

and

$$\max_j |\xi_j|_v^2 \leq \max_j \sum_T |v_j(T)|_v |y_T(\underline{\xi})|_v.$$

Combining these gives the result. □

As in [MS, Section 16B], we can refine this result somewhat. Define a function

$$f: \mathbb{R}_{\geq 0}^8 \longrightarrow \mathbb{R}_{\geq 0}^8, \quad (d_1, \dots, d_8) \longmapsto \left(\sqrt{\sum_{T} |v_j(T)|_v} \sqrt{\sum_{i=1}^8 |\tau_i(T) d_{9-i}|_v} \right)_{1 \leq j \leq 8}.$$

We write $\|(x_1, \dots, x_8)\|_{\infty} = \max\{|x_1|, \dots, |x_8|\}$ for the maximum norm.

Lemma 10.5. *Define a sequence (b_n) in $\mathbb{R}_{\geq 0}^8$ by*

$$b_0 = (1, \dots, 1) \quad \text{and} \quad b_{n+1} = f(b_n).$$

The (b_n) converges to a limit b , and we have that

$$-\mu_v(P) \leq \frac{4^N}{4^N - 1} \log \|b_N\|_{\infty}$$

for all $N \geq 1$ and all $P \in \mathcal{J}(\mathbb{C})$. In particular, $\sup -\mu_v(\mathcal{J}(\mathbb{C})) \leq \log \|b\|_{\infty}$.

Proof. See the proof of [MS, Lemma 16.1]. □

Example 10.6. For the curve

$$y^2 = 4x^7 - 4x + 1,$$

the bound $\gamma_{\infty}/3$ is 1.15134, whereas with $N = 8$, we obtain the considerably better bound $-\mu_{\infty} \leq 0.51852$.

We can improve this a little bit more if $k_v = \mathbb{R}$, by making use of the fact that the coordinates of the points involved are real, but the $\tau_i(T)$ may be non-real. This can give a better bound on

$$|y_T^2|_v \leq \max_{|\delta_i| \leq d_i} \left| \sum_{i=1}^8 \varepsilon_i \tau_i(T) \delta_{9-i} \right|_v.$$

For the curve above, this improves[★] the upper bound for $-\mu_{\infty}$ to 0.43829.

Now we show that in the most common cases of bad reduction, there is in fact no contribution to the height difference bound. This result is similar to [Sto3, Proposition 5.2].

Lemma 10.7. *Let v be a non-archimedean place of k of odd residue characteristic. Assume that the reduction of F at v has a simple root and that the model of \mathcal{C} given by $y^2 = F(x, z)$ is regular at v . Then $\mu_v(P) = \varepsilon_v(P) = 0$ for all $P \in \mathcal{J}(k_v)$.*

Note that the assumptions on the model are satisfied when $v(\text{disc}(F)) = 1$.

Proof. We work with a suitable unramified extension K of k_v , so that the reduction \bar{F} of F splits into linear factors over the residue field. We denote the ring of integers of K by \mathcal{O} . By assumption, \bar{F} has a simple root, which by Hensel's Lemma lifts to a root of F in $\mathbb{P}^1(K)$. We can use a transformation defined over \mathcal{O} to move this root of F to ∞ . Then we have $f_8 = 0$ and $v(f_7) = 0$. We can further scale F (at the cost of at most a further quadratic unramified extension) so that $f_7 = 1$.

Assume that $P \in \mathcal{J}(K)$ has $\varepsilon_v(P) \neq 0$ and let $\underline{\xi}$ be normalized coordinates for $\kappa(P) \in \mathcal{K}(K)$ (i.e., such that the coordinates are in \mathcal{O} and at least one of them is in \mathcal{O}^\times). By Proposition 9.9, the reduction of P must lie in some \mathcal{L}_a where $a \neq \infty$ is a multiple root of \bar{F} . We can shift a to 0; then the coordinates ξ_4, ξ_6, ξ_7 and ξ_8 have positive valuation. We also have $v(f_0) = 1$ (this is because the model is regular at the point $(0 : 0 : 1)$ in the reduction) and $v(f_1) \geq 1$ (since $a = 0$ is a multiple root of \bar{F}).

Now assume first that $v(\xi_1) = 0$; then we can scale $\underline{\xi}$ such that $\xi_1 = 1$. We consider the quantity μ_{034} introduced in Section 4; its value on P is in K . By (4.1), we have that

$$\mu_{034}^2 = \eta_{00}\eta_{34}^2 + \eta_{33}\eta_{04}^2 + \eta_{44}\eta_{03}^2 - 4\eta_{00}\eta_{33}\eta_{44} - \eta_{03}\eta_{04}\eta_{34} = f_0 + (f_6 - \xi_2)\xi_4^2 - \xi_6\xi_4$$

(note that $\eta_{44} = f_8 = 0$, $\eta_{34} = f_7 = 1$, $\eta_{33} = f_6 - \eta_{24}$, $\eta_{24} = \xi_2$, $\eta_{04} = \xi_4$, $\eta_{03} = \xi_6$). Now since $v(f_0) = 1$ and $v(\xi_4) \geq 1$, $v(\xi_6) \geq 1$, we find that $2v(\mu_{034}) = 1$, a contradiction.

So we must have $v(\xi_1) > 0$. One can check[★] that

$$\nu_1 = (\xi_4 - \xi_5)\mu_{013} + \xi_7\mu_{123}$$

$$\nu_2 = \xi_3\mu_{014} - \xi_4\mu_{024}$$

$$\nu_3 = \xi_2\mu_{024} - \xi_4\mu_{134}$$

are functions in $L(4\Theta)$, which are clearly odd, so their squares can be written as quartics in the ξ_j by Lemma 2.3. Let $I = (f_0, f_1, \xi_1, \xi_4, \xi_6, \xi_7, \xi_8)^2$; then anything in I has valuation at least 2. We find[★] that modulo I we have that

$$\nu_1^2 \equiv f_0\xi_5^4, \quad \nu_2^2 \equiv f_0\xi_3^4, \quad \nu_3^2 \equiv f_0\xi_2^4.$$

Since (at least) one of ξ_2, ξ_3, ξ_5 is a unit and $v(f_0) = 1$, we obtain a contradiction again.

Therefore $\varepsilon_v(P) = 0$ for all $P \in \mathcal{J}(K)$, which implies that $\mu_v(P) = 0$ as well. \square

Example 10.8. The discriminant of the curve

$$\mathcal{C}: y^2 = 4x^7 - 4x + 1,$$

is[★] $2^{28} \cdot 19 \cdot 223 \cdot 44909$. Lemma 10.7 now implies that $\varepsilon_v(P) = 0$ for all $P \in \mathcal{J}(\mathbb{Q}_v)$ for all places v except 2 and ∞ , including the bad primes 19, 223 and 44909. So,

using Examples 10.2 and 10.6, we obtain the bound

$$h(P) \leq \hat{h}(P) + 5 \log 2 + 0.43829 \leq \hat{h}(P) + 3.90403$$

for all $P \in \mathcal{J}(\mathbb{Q})$.

To compute the canonical height $\hat{h}(P)$ for some point $P \in \mathcal{J}(\mathbb{Q})$ (say, for a hyperelliptic curve \mathcal{C} of genus 3 defined over \mathbb{Q}), we can use any of the approaches described in [MS], except the most efficient one (building on Proposition 14.3 in loc. cit.), since we have so far no general bound on the denominator of $\mu_p/\log p$ in terms of the discriminant. A little bit of care is needed, since contrary to the genus 2 situation, $\varepsilon_v = 0$ and $\mu_v = 0$ are not necessarily equivalent — there can be a difference when the reduction of F is a constant times a square — so the criterion for a point to be in the subgroup on which $\mu_v = 0$ has to be taken as $\overline{\kappa(P)} \in \mathcal{K}_{\text{good}}(\mathbb{F})$, where $\overline{\kappa(P)}$ is the reduction of $\kappa(P)$ at v and \mathbb{F} is the residue class field.

We can describe the subset on which $\mu_v = 0$ and show that it is a subgroup and that μ_v factors through the quotient.

Theorem 10.9. *Let v be a non-archimedean place of k of odd residue characteristic. Write $\mathcal{J}(k_v)_{\text{good}}$ for the subset of $\mathcal{J}(k_v)$ consisting of the points P such that $\kappa(P)$ reduces to a point in $\mathcal{K}_{\text{good}}(\mathbb{F})$. Then $\mathcal{J}(k_v)_{\text{good}} = \{P \in \mathcal{J}(k_v) : \mu_v(P) = 0\}$ is a subgroup of finite index of $\mathcal{J}(k_v)$, and ε_v and μ_v factor through the quotient $\mathcal{J}(k_v)/\mathcal{J}(k_v)_{\text{good}}$.*

Proof. That $\mathcal{J}(k_v)_{\text{good}}$ is a group follows from Lemma 9.10: If P_1 and P_2 are in $\mathcal{J}(k_v)_{\text{good}}$, then $P_1 \pm P_2$ reduce to a point in $\mathcal{K}_{\text{good}}$ as well. This subgroup contains the kernel of reduction, which is of finite index, so it is itself of finite index. That $\mathcal{J}(k_v)_{\text{good}} = \{P \in \mathcal{J}(k_v) : \mu_v(P) = 0\}$ follows from the results of Section 9.

It remains to show that μ_v (and therefore also ε_v , since $\varepsilon_v(P) = 4\mu_v(P) - \mu_v(2P)$) factors through the quotient group. Let $P, P' \in \mathcal{J}(k_v)$ and let $\underline{\xi}$ and $\underline{\xi}'$ be coordinate vectors for $\kappa(P)$ and $\kappa(P')$, respectively. We can then choose coordinate vectors $\underline{\zeta}$ and $\underline{\zeta}'$ for $\kappa(P' + P)$ and $\kappa(P' - P)$, respectively, such that $\underline{\zeta} * \underline{\zeta}' = 2B(\underline{\xi}, \underline{\xi}')$. Iterating the implication in (9.1) then gives

$$\underline{\delta}(\underline{\zeta}) * \underline{\delta}(\underline{\zeta}') = 2B(\underline{\delta}(\underline{\xi}), \underline{\delta}(\underline{\xi}')),$$

and we can iterate this relation further. If $\underline{\alpha}$ is a vector or matrix, then we write $|\underline{\alpha}|_v$ for the maximum of the v -adic absolute values of the entries of α . Define

$$\varepsilon_v(P, P') = \log |2B(\underline{\xi}, \underline{\xi}')|_v - 2 \log |\underline{\xi}|_v - 2 \log |\underline{\xi}'|_v$$

(this does not depend on the scaling of the coordinate vectors) and note that $|\underline{\zeta} * \underline{\zeta}'|_v = |\underline{\zeta}|_v \cdot |\underline{\zeta}'|_v$ (here we use that the residue characteristic is odd). We then

see that $\mu_v(P) = 0$ implies $\mu_v(P + Q) = \mu_v(Q)$ for all $Q \in \mathcal{J}(k_v)$ in the same way as in the proof of [MS, Lemma 3.7]. \square

11. AN APPLICATION

We consider the curve

$$\mathcal{C}' : y^2 - y = x^7 - x,$$

which is isomorphic to the curve

$$\mathcal{C} : y^2 = 4x^7 - 4x + 1,$$

which we have been using as our running example. Our results can now be used to determine a set of generators for the Mordell-Weil group $\mathcal{J}(\mathbb{Q})$. This is the key ingredient for the method that determines the set of integral points on a hyperelliptic curve as in [BM+]. We carry out the necessary computations and thence find all the integral solutions of the equation $y^2 - y = x^7 - x$.

A 2-descent on the Jacobian \mathcal{J} of \mathcal{C} as described in [Sto2] and implemented in Magma [BCP] shows that the rank of $\mathcal{J}(\mathbb{Q})$ is at most 4. We have $\#\mathcal{J}(\mathbb{F}_3) = 94$ and $\#\mathcal{J}(\mathbb{F}_7) = 911$, which implies that $\mathcal{J}(\mathbb{Q})$ is torsion free (the torsion subgroup injects into $\mathcal{J}(\mathbb{F}_p)$ for p an odd prime of good reduction). We have the obvious points $(0, \pm 1)$, $(\pm 1, \pm 1)$, $(\pm \omega, \pm 1)$, $(\pm \omega^2, \pm 1)$ on \mathcal{C} , where ω denotes a primitive cube root of unity, together with the point at infinity. We can check that the rational divisors of degree zero on \mathcal{C} supported in these points generate a subgroup G of $\mathcal{J}(\mathbb{Q})$ of rank 4, which already shows that $\mathcal{J}(\mathbb{Q}) \cong \mathbb{Z}^4$. Computing canonical heights, either with an approach as in [MS] or with the more general algorithms due independently to Holmes [Hol] and Müller [Mü2], we find that an LLL-reduced basis of the lattice (G, \hat{h}) is given by

$$\begin{aligned} P_1 &= [(0, 1) - \infty], & P_2 &= [(1, 1) - \infty], & P_3 &= [(-1, 1) - \infty], \\ P_4 &= [(1, -1) + (\omega, -1) + (\omega^2, -1) - 3 \cdot \infty] \end{aligned}$$

with height pairing matrix

$$M \approx \begin{pmatrix} 0.17820 & 0.01340 & -0.05683 & 0.08269 \\ 0.01340 & 0.81995 & -0.34461 & -0.26775 \\ -0.05683 & -0.34461 & 0.98526 & 0.37358 \\ 0.08269 & -0.26775 & 0.37358 & 1.07765 \end{pmatrix}.$$

We can bound the covering radius ρ of this lattice by $\rho^2 \leq 0.50752$. Using Example 10.8, it follows that if $G \neq \mathcal{J}(\mathbb{Q})$, then there must be a point $P \in \mathcal{J}(\mathbb{Q}) \setminus G$ satisfying

$$h(P) \leq \rho^2 + \beta \leq 0.50752 + 3.90403 = 4.41155,$$

so that we can write $\kappa(P) = (\xi_1 : \xi_2 : \dots : \xi_8) \in \mathcal{K}(\mathbb{Q})$ with coprime integers ξ_j such that $|\xi_j| \leq \lfloor e^{4.41155} \rfloor = 82$. We can enumerate all points in $\mathcal{K}(\mathbb{Q})$ up to

this height bound and check that no such point lifts to a point in $\mathcal{J}(\mathbb{Q})$ that is not in G . (Compare [Sto3, §7] for this approach to determining the Mordell-Weil group.) We have therefore proved the following.

Proposition 11.1. *The group $\mathcal{J}(\mathbb{Q})$ is free abelian of rank 4, generated by the points P_1, P_2, P_3 and P_4 .*

A Mordell-Weil sieve computation as described in [BS] shows that any unknown rational point on \mathcal{C} must differ from one of the eleven known points

$$\infty, (-1, \pm 1), (0, \pm 1), \left(\frac{1}{4}, \pm \frac{1}{64}\right), (1, \pm 1), (5, \pm 559)$$

by an element of $B \cdot \mathcal{J}(\mathbb{Q})$, where

$$B = 2^6 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 \cdot 47 \cdot 53 \cdot 61 \cdot 71 \cdot 79 \cdot 83 \cdot 97 \approx 1.1 \cdot 10^{32}.$$

In particular, we know that every rational point is in the same coset modulo $2\mathcal{J}(\mathbb{Q})$ as one of the known points. For each of these cosets (there are five such cosets: the points with x -coordinate $1/4$ are in the same coset as those with x -coordinate 0), we compute a bound for the size of the x -coordinate of an integral point on \mathcal{C} with the method given in [BM+]. This shows that

$$\log |x| \leq 2 \cdot 10^{1229}$$

for any such point (x, y) . On the other hand, using the second stage of the Mordell-Weil sieve as explained in [BM+], we obtain a lattice $L \subset \mathbb{Z}^4$ of index $\approx 2.3 \cdot 10^{2505}$ such that the minimal squared euclidean length of a nonzero element of L is $\approx 2.55 \cdot 10^{1252}$ and such that every rational point on \mathcal{C} differs from one of the known points by an element in the image of L in $\mathcal{J}(\mathbb{Q})$ under the isomorphism $\mathbb{Z}^4 \xrightarrow{\cong} \mathcal{J}(\mathbb{Q})$ given by the basis above. This is more than sufficient to produce a contradiction to the assumption that there is an integral point we do not already know. We have therefore proved:

Theorem 11.2. *The only points in $\mathcal{C}(\mathbb{Q})$ with integral x -coordinate are*

$$(-1, \pm 1), (0, \pm 1), (1, \pm 1), (5, \pm 559).$$

In particular, the only integral solutions of the equation

$$y^2 - y = x^7 - x$$

are $(x, y) = (-1, 0), (-1, 1), (0, 0), (0, 1), (1, 0), (1, 1), (5, 280)$ and $(5, -279)$.

12. QUADRATIC TWISTS

Let F be a squarefree octic binary form over a field k not of characteristic 2 and let $c \in k^\times$. Then the Kummer varieties \mathcal{K} and $\mathcal{K}^{(c)}$ associated to F and to cF ,

respectively, are isomorphic, with an isomorphism from the former to the latter being given by

$$(\xi_1 : \xi_2 : \xi_3 : \dots : \xi_7 : \xi_8) \longmapsto (\xi_1 : c\xi_2 : c\xi_3 : \dots : c\xi_7 : c^2\xi_8).$$

We can therefore use \mathcal{K} as a model for the Kummer variety associated to the curve $\mathcal{C}^{(c)}: y^2 = cF(x, z)$. This will in general change the naive height of a point $P \in \mathcal{J}^{(c)}(\mathbb{Q})$, but will not affect the canonical height, which is insensitive to automorphisms of the ambient \mathbb{P}^7 . The duplication map is preserved by the isomorphism. This implies that the height difference bounds of Lemmas 10.1 and 10.5 for F apply to \mathcal{K} , even when \mathcal{K} is used as the Kummer variety of $\mathcal{C}^{(c)}$. This is because these bounds are valid for all k_v -points on \mathcal{K} , regardless of whether they lift to points in $\mathcal{J}(k_v)$ or not. Note, however, that the result of Lemma 10.7 does *not* carry over: in the interesting case, c has odd valuation at v , and so we are in effect looking at (certain) points on \mathcal{J} defined over a ramified quadratic extension of k_v . Since in terms of the original valuation, the possible values of the valuation on this larger field are now in $\frac{1}{2}\mathbb{Z}$, the argument in the proof of Lemma 10.7 breaks down.

When working with this model, one has to modify the criterion for a point to lift to $\mathcal{J}(k)$ by multiplying the μ_{ijk} by c .

As an example, consider the curve given by

$$\begin{pmatrix} y \\ 2 \end{pmatrix} = \begin{pmatrix} x \\ 7 \end{pmatrix}.$$

It is isomorphic to the curve

$$\mathcal{C}: y^2 = 70(x^7 - 14x^5 + 49x^3 - 36x + 630) = 70F(x, 1)$$

where F is the obvious octic binary form. The 2-Selmer rank of its Jacobian \mathcal{J} is 9, $\mathcal{J}(\mathbb{Q})$ is torsion free, and the subgroup G of $\mathcal{J}(\mathbb{Q})$ generated by differences of the 27 small rational points on \mathcal{C} has rank 9 with LLL-reduced basis

$$\begin{aligned} & [(-2, 210) - \infty], \quad [(1, 210) - \infty], \quad [(3, 210) - \infty], \\ & [(2, 210) - \infty], \quad [(-3, 210) - \infty], \quad [(4, 630) - \infty], \\ & [(-\frac{5}{2}, -\frac{1785}{8}) + (3, 210) + (4, 630) - 3\infty], \\ & [(0, 210) - \infty], \quad [(6, 3570) - \infty]. \end{aligned}$$

We would like to show that these points are actually generators of $\mathcal{J}(\mathbb{Q})$.

Using the Kummer variety associated to $70F$, we obtain the following bound for μ_v at the bad primes and infinity (using the valuations of the resultants $r(T)$, Lemma 10.7 and Lemma 10.5):

$$\begin{aligned} \mu_2 &\geq -6 \log 2, & \mu_3 &\geq -\frac{10}{3} \log 3, & \mu_5 &\geq -\frac{10}{3} \log 5, & \mu_7 &\geq -\frac{8}{3} \log 7, \\ \mu_{13} &= 0, & \mu_{17} &\geq -\frac{2}{3} \log 17, & \mu_{15717742643} &= 0, & \mu_\infty &\geq -0.6152. \end{aligned}$$

The resulting bound ≈ 20.88 for $h - \hat{h}$ is *much* too large to be useful.

However, using the Kummer variety associated to F , we find

$$\begin{aligned} \mu_2 &\geq -\frac{10}{3} \log 2, & \mu_3 &\geq -\frac{10}{3} \log 3, & \mu_5 &\geq -\frac{2}{3} \log 5, & \mu_7 &= 0, \\ \mu_{13} &= 0, & \mu_{17} &\geq -\frac{2}{3} \log 17, & \mu_{15717742643} &= 0, & \mu_\infty &\geq -0.6152. \end{aligned}$$

This gives a bound of ≈ 9.55 (now for a different naive height), which is already a lot better, but still a bit too large for practical purposes. Now one can check that for a point $P \in \mathcal{J}(\mathbb{Q}_p)$ with $p \in \{5, 17\}$, we always have $\kappa(2P) \in \mathcal{K}_{\text{good}}$. This implies that we get a better estimate

$$h(2P) \leq \hat{h}(2P) + \frac{10}{3} \log 6 + 0.6152 \leq \hat{h}(2P) + 6.588$$

for $P \in \mathcal{J}(\mathbb{Q})$. A further study of the situation at $p = 3$ reveals that μ_3 factors through the component group Φ of the Néron model of \mathcal{J} over \mathbb{Z}_3 , which has the structure $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and that the minimum of μ_3 on 2Φ is $-\frac{5}{3} \log 3$. This leads to

$$(12.1) \quad h(2P) \leq \hat{h}(2P) + 4.757.$$

We enumerate all points P in $\mathcal{J}(\mathbb{Q})$ such that $h(P) \leq \log 2000$ using a p -adic lattice-based approach with $p = 277$, as follows. For each of the 10 965 233 points $\kappa(0) \neq Q \in \mathcal{K}(\mathbb{F}_p)$ that are in the image of $\mathcal{J}(\mathbb{F}_p)$, we construct a sublattice L_Q of \mathbb{Z}^8 such that for every point $P \in \mathcal{J}(\mathbb{Q})$ such that $\kappa(P)$ reduces mod p to Q , every integral coordinate vector for $\kappa(P)$ is in L_Q and such that $(\mathbb{Z}^8 : L_Q) \geq p^{11}$. We then search for short vectors in L_Q , thus obtaining all points of multiplicative naive height ≤ 2000 . Note that all these points are smooth on \mathcal{K} over \mathbb{F}_p , since $\#\mathcal{J}(\mathbb{F}_p)$ is odd. This computation took about two CPU weeks. For points reducing to the origin, we see that the quadratic equation satisfied by points on \mathcal{K} forces ξ_1 to be divisible by $p^2 > 2000$, so $\xi_1 = 0$, and every such point must be on the theta divisor. A point $P = [P_1 + P_2 - 2 \cdot \infty] \in \mathcal{J}(\mathbb{Q})$ reduces to the origin if and only if the points P_1 and P_2 reduce to opposite points; in particular, the polynomial whose roots are the x -coordinates of P_1 and P_2 reduces to a square mod p . Since the coefficients are bounded by $7 = \lfloor 2000/p \rfloor$, divisibility of the discriminant by p implies that the discriminant vanishes, so that $P_1 = P_2$, and the point P does not reduce to the origin, after all.

We find no point P such that $0 < \hat{h}(P) < \hat{h}(P_1) \approx 1.619$, where P_1 is a known point of minimal positive canonical height, and no points P outside G such that $\hat{h}(P) < 2.844 \approx \log 2000 - 4.757$. Since the bound (12.1) is only valid on $2\mathcal{J}(\mathbb{Q})$, this implies that there are no points $P \in \mathcal{J}(\mathbb{Q})$ with $0 < \hat{h}(P) < 0.711 =: m$. Using the bound (see [FS])

$$I \leq \left\lfloor \sqrt{\frac{\gamma_9^9 \det(M)}{m^9}} \right\rfloor \leq 1787$$

for the index of the known subgroup in $\mathcal{J}(\mathbb{Q})$, where γ_9 denotes the Hermite constant for 9-dimensional lattices and M is the height pairing matrix of the basis of the known subgroup of $\mathcal{J}(\mathbb{Q})$, we see that it suffices to rule out all primes up to 1787 as possible index divisors. We therefore check that the known subgroup G is in fact saturated at all those primes with the method already introduced in [FS]: to verify saturation at p , we find sufficiently many primes q of good reduction such that $\#\mathcal{J}(\mathbb{F}_q)$ is divisible by p (usually nine such primes will suffice) and check that the kernel of the natural map

$$G/pG \longrightarrow \prod_q \mathcal{J}(\mathbb{F}_q)/p\mathcal{J}(\mathbb{F}_q)$$

is trivial. This computation takes a few CPU days; the most time-consuming task is to find $\#\mathcal{J}(\mathbb{F}_q)$ for all primes q up to $q = 322\,781$ (which is needed for $p = 1471$). This gives the following result.

Theorem 12.1. *The points $[P_j - \infty]$ freely generate $\mathcal{J}(\mathbb{Q})$, where the $P_j \in \mathcal{C}(\mathbb{Q})$ are the points with the following x -coordinates and positive y -coordinate:*

$$-3, -2, -\frac{5}{2}, 0, 1, 2, 3, 4, 6.$$

In principle, one could now try to determine the set of integral points on \mathcal{C} with the method we had already used for $y^2 - y = x^7 - x$. However, a Mordell-Weil sieve computation with a group of rank 9 is a rather daunting task, which we prefer to leave to the truly dedicated reader.

REFERENCES

- [BCP] W. BOSMA, J. CANNON and C. PLAYOUST: *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**, 235–265 (1997).
- [BS] N. BRUIN and M. STOLL: *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math. **13**, 272–306 (2010).
- [BM+] Y. BUGEAUD, M. MIGNOTTE, S. SIKSEK, M. STOLL and SZ. TENGYEL: *Integral points on hyperelliptic curves*, Algebra & Number Theory **2**:8, 859–885 (2008).
- [CF] J.W.S. CASSELS and E.V. FLYNN: *Prolegomena to a middlebrow arithmetic of curves of genus 2*, Cambridge University Press, Cambridge, UK, 1996.
- [Duq] S. DUQUESNE: *Calculs effectifs des points entiers et rationnels sur les courbes*, Thèse de doctorat, Université Bordeaux (2001).
- [FS] E.V. FLYNN and N.P. SMART: *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith. **79**:4, 333–352 (1997).
- [HS] M. HINDRY and J.H. SILVERMAN: *Diophantine Geometry. An Introduction*, Springer GTM **201**, Springer-Verlag, New York, 2000.
- [Hol] D. HOLMES: *Computing Néron-Tate heights of points on hyperelliptic Jacobians*, J. Number Theory **132**:6, 1295–1305 (2012).
- [Mü1] J.S. MÜLLER: *Computing canonical heights on Jacobians*, PhD thesis, University of Bayreuth (2010).
- [Mü2] J.S. MÜLLER: *Computing canonical heights using arithmetic intersection theory*, Math. Comp. **83**, 311–336 (2014).

- [Mü3] J.S. MÜLLER: *Explicit Kummer varieties of hyperelliptic Jacobian threefolds*, LMS J. Comput. Math. **17**, 496–508 (2014).
- [MS] J.S. MÜLLER and M. STOLL: *Canonical heights on genus two Jacobians*, Algebra & Number Theory **10**, No. 10, 2153–2234 (2016).
- [Mum] D. MUMFORD: *On the equations defining abelian varieties. I*, Invent. Math. **1**, 287–354 (1966).
- [Sto1] M. STOLL: *On the height constant for curves of genus two*, Acta Arith. **90**, 183–201 (1999).
- [Sto2] M. STOLL: *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98**, 245–277 (2001).
- [Sto3] M. STOLL: *On the height constant for curves of genus two, II*, Acta Arith. **104**, 165–182 (2002).
- [Data] M. STOLL: Magma files with relevant data, available at <http://www.mathe2.uni-bayreuth.de/stoll/magma/index.html>
- [Stu] A.G.J. STUBBS: *Hyperelliptic curves*, PhD thesis, University of Liverpool (2000).

MATHEMATISCHES INSTITUT, UNIVERSITÄT BAYREUTH, 95440 BAYREUTH, GERMANY.

E-mail address: Michael.Stoll@uni-bayreuth.de