AN EXPLICIT THEORY OF HEIGHTS FOR HYPERELLIPTIC JACOBIANS OF GENUS THREE

MICHAEL STOLL

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. Such a curve $\mathcal{C}$ is given by an equation of the form $y^2 = f(x)$, where f is a squarefree polynomial of degree 7 or 8. We denote its Jacobian 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 $\mathcal{J} \to \mathbb{P}^7$ 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 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 $\mathcal{X} = \operatorname{Pic}^4(\mathcal{C})$ 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 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 $\mathcal{K}$.

The next task is to describe the maps $\mathcal{K} \to \mathcal{K}$ and $\operatorname{Sym}^2 \mathcal{K} \to \operatorname{Sym}^2 \mathcal{K}$ 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 $\mathcal{K}$. In analogy with [Sto1], we also obtain an estimate for the local 'loss of precision' under $\underline{\delta}$ in terms of the valuation of the discriminant of f. This in turn leads to an explicit upper bound for the difference $h - \hat{h}$ between the (logarithmic) naive and canonical heights on $\mathcal{J}$ over a number field. Such a bound is necessary if one wants to find generators of the full Mordell-Weil group when only a subgroup of finite index is known. We

Date: May 15, 2014.

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 [BMSST]. As a further illustration, we determine explicit generators of the Mordell-Weil group of the Jacobian of the curve given by the binomial coefficient equation

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

The necessary computations were performed using the MAGMA computer algebra system [Magma].

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

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

(We do not assume that $\mathcal{C}$ has a Weierstrass point at infinity.) 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 $\mathbb{P}^2_{1,4,1}$ given by $y^2 = F(x,z)$. 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 $\mathcal{J} = \operatorname{Pic}^0_{\mathcal{C}}$ is canonically isomorphic to $\mathcal{X} = \operatorname{Pic}^4_{\mathcal{C}}$. The theta divisor on Pic^0_C (given by 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 $\mathfrak{W} \sim 2\mathfrak{m}$) corresponds to the locus of points on $\mathcal{X}$ that are not represented by divisors in general position. An effective divisor $\mathfrak{D}$ on $\mathcal{C}$ is said to be *in general position* unless there is a point $P \in \mathcal{C}$ such that $\mathfrak{D} \geq (P) + (\iota P)$, where $\iota\colon \mathcal{C} \to \mathcal{C}$, $(x,y) \mapsto (x,-y)$ is the hyperelliptic involution.

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.

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 $\pi\colon \mathcal{C} \to \mathbb{P}^1$, $(x,y) \mapsto x$, together with another quartic binary form $B(x,z)$ such that $y = B(x,z)$ on the points in $\mathfrak{D}$. More precisely, we must have

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

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

We let $Q = x_2^2 - x_1x_3$, M_Q the associated symmetric matrix and

$$\Gamma = \mathrm{SO}(Q) = \{\gamma \in \mathrm{SL}(3) : \gamma M_Q \gamma^\top = M_Q\}\,,$$

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

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

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:

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

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 $-t_{-1} \in -\Gamma$. □

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 $a_0, \ldots, a_4, b_0 \ldots, b_4, c_0, \ldots, c_4$ as affine coordinates on $\mathbb{A}^{15}$. We let $\mathcal{V} \subset \mathbb{A}^{15}$ be the affine variety given by (2.1). The defining equations of $\mathcal{V}$ then read

$$\begin{aligned}
b_0^2 - a_0c_0 &= f_0 \\
2b_0b_1 - (a_0c_1 + a_1c_0) &= f_1 \\
2b_0b_2 + b_1^2 - (a_0c_2 + a_1c_1 + a_2c_0) &= f_2 \\
2b_0b_3 + 2b_1b_2 - (a_0c_3 + a_1c_2 + a_2c_1 + a_3c_0) &= f_3 \\
2b_0b_4 + 2b_1b_3 + b_2^2 - (a_0c_4 + a_1c_3 + a_2c_2 + a_3c_1 + a_4c_0) &= f_4 \\
2b_1b_4 + 2b_2b_3 - (a_1c_4 + a_2c_3 + a_3c_2 + a_4c_1) &= f_5 \\
2b_2b_4 + b_3^2 - (a_2c_4 + a_3c_3 + a_4c_2) &= f_6 \\
2b_3b_4 - (a_3c_4 + a_4c_3) &= f_7 \\
b_4^2 - a_4c_4 &= f_8\,.
\end{aligned}$$

By Lemma 2.1, $\mathcal{V}/\Gamma = \mathcal{U} := \mathcal{X} \setminus \Theta$. Therefore the functions in the Riemann-Roch space $L(n\Theta)$ will be represented by Γ-invariant polynomials in the a_i, b_i, c_i.

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 form

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

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. Modulo the relations defining $\mathcal{V}$, there are six independent such invariants. We choose

$$\begin{aligned} \eta_{02} &= 2b_0b_2 - (a_0c_2 + a_2c_0) \\ \eta_{03} &= 2b_0b_3 - (a_0c_3 + a_3c_0) \\ \eta_{04} &= 2b_0b_4 - (a_0c_4 + a_4c_0) \\ \eta_{13} &= 2b_1b_3 - (a_1c_3 + a_3c_1) \\ \eta_{14} &= 2b_1b_4 - (a_1c_4 + a_4c_1) \\ \eta_{24} &= 2b_2b_4 - (a_2c_4 + a_4c_2) \end{aligned}$$

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 $L(2\Theta)$. Since $\dim L(2\Theta) = 8$, we are missing one function. This should be given by some quadratic form in the η_{ij}, with the property that it does not grow faster than the η_{ij} when we approach Θ.

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

$$A(x,1) = A_0(x)\big(\lambda^2(x - x_0)^2 + \big(2\lambda\psi(x_0) - \varphi_+'(x_0)\big)(x - x_0) - \varphi_-(x_0) + O(\lambda^{-1})\big)\,,$$

shows that

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

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

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

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

$$\eta = \eta_{02}\eta_{24} - \eta_{03}\eta_{14} + \eta_{04}^2 + \eta_{04}\eta_{13}\,, \tag{2.2}$$

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

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

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

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

We use $(\xi_1, \dots, \xi_8)$ 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

$$\xi_1\xi_8 - \xi_2\xi_7 + \xi_3\xi_6 - \xi_4\xi_5 = 0\,. \tag{2.3}$$

The image $\mathcal{K}$ of the Kummer variety in $\mathbb{P}^7$ is given by a quadric and 34 quartic relations that are not multiples of the quadric. The quadric is just (2.3). There are 15 quartic relations in $(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6, \xi_7)$ coming from the fact that the quadratic form $B_l^2 - A_lC_l$ has rank (at most) 3. They are given by the 4×4 minors of the corresponding matrix

$$M = \begin{pmatrix} 2f_0\xi_1 & f_1\xi_1 & \xi_7 & \xi_6 & \xi_4 \\ f_1\xi_1 & 2(f_2\xi_1 - \xi_7) & f_3\xi_1 - \xi_6 & \xi_5 - \xi_4 & \xi_3 \\ \xi_7 & f_3\xi_1 - \xi_6 & 2(f_4\xi_1 - \xi_5) & f_5\xi_1 - \xi_3 & \xi_2 \\ \xi_6 & \xi_5 - \xi_4 & f_5\xi_1 - \xi_3 & 2(f_6\xi_1 - \xi_2) & f_7\xi_1 \\ \xi_4 & \xi_3 & \xi_2 & f_7\xi_1 & 2f_8\xi_1 \end{pmatrix} \tag{2.4}$$

Since these relations do not involve ξ_8, they cannot be multiples of the quadratic relation. We will see later how to obtain all quartic relations satisfied by the Kummer variety.

On a point $[(x_1, y_1) + (x_2, y_2) + \mathfrak{m}] \in \Theta$, the map restricts to

$$\left(0 : 1 : -(x_1 + x_2) : x_1x_2 : x_1^2 + x_1x_2 + x_2^2 : -(x_1 + x_2)x_1x_2 : (x_1x_2)^2 : \frac{2y_1y_2 - G(x_1, x_2)}{(x_1 - x_2)^2}\right).$$

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

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

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.)

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

$$(0 : 0 : 0 : 0 : 0 : 0 : 0 : 1)\,.$$

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

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

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

$$(0 : g_2^2 : g_1g_2 : g_0g_2 : g_1^2 - g_0g_2 : g_0g_1 : g_0^2 : g_0^3h_6 + g_0^2g_2h_4 + g_0g_2^2h_2 + g_2^3h_0)\,. \tag{2.5}$$

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

(2.6)
$$\begin{aligned}\bigl(1 &: g_2h_4 + g_4h_2 : g_1h_4 + g_4h_1 : g_0h_4 + g_4h_0 \\ &: g_0h_4 + g_4h_0 + g_1h_3 + g_3h_1 : g_0h_3 + g_3h_0 : g_0h_2 + g_2h_0 \\ &: (g_0h_4 + g_4h_0)^2 + (g_0h_2 + g_2h_0)(g_2h_4 + g_4h_2) + (g_1h_0 - g_0h_1)(g_4h_3 - g_3h_4)\bigr)\,.\end{aligned}$$

3. Lifting points to the Jacobian

In order to decide if a point on the Kummer variety lifts to the Jacobian $\mathcal{J}$, we have to consider odd functions on $\mathcal{J}$. In $L(3\Theta)$ of dimension $3^3 = 27$, the subspace of even functions has dimension 14 and is spanned by $\xi_1, \dots, \xi_8$, 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

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

The subspace of odd functions has dimension 13. We obtain a ten-dimensional subspace of the latter 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 $\mathrm{SL}(3)$ 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

$$L = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ b_0 & b_1 & b_2 & b_3 & b_4 \\ c_0 & c_1 & c_2 & c_3 & c_4 \end{pmatrix}\,. \tag{3.1}$$

If we denote the minor corresponding to $0 \le i < j < k \le 4$ by μ_{ijk} and use the notation $\eta_{ii} = b_i^2 - a_ic_i$ and $\eta_{ij} = 2b_ib_j - (a_ic_j + a_jc_i)$ for $i < j$, then we find

$$\mu_{ijk}^2 = \eta_{ii}\eta_{jk}^2 + \eta_{jj}\eta_{ik}^2 + \eta_{kk}\eta_{ij}^2 - 4\eta_{ii}\eta_{jj}\eta_{kk} - \eta_{ij}\eta_{ik}\eta_{jk}\,. \tag{3.2}$$

If L_{ijk} is the corresponding 3×3 submatrix of the matrix above, note that

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

with

$$D = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix}\,, \tag{3.3}$$

and that the entries of the product matrix $L^\top DL$ are of the form $2\eta_{ii}$ on the diagonal and η_{ij} off the diagonal, so $L^\top DL = M$, where M is the matrix corresponding to the quadratic form $B_l^2 - A_lC_l$ given in (2.4). 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'.

For a point 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 are squares, and it is sufficient that one of them is a nonzero square. 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 less than three). The dimension of the space spanned by A, B and C cannot be less than two, since this would imply that F is a constant times a square, which is not possible, since F is assumed to be 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 two-torsion point on $\mathcal{J}$, and it will always lift.

Let us now assume that not all the minors vanish, say $\mu_{ijk} \neq 0$. Then L has rank 3, so that its rows, or equivalently, the polynomials A, B, C are linearly independent. Since the rank of M is also 3, both L and M have the same two-dimensional kernel. We can compute the kernel from M and then we find the space generated by A, B, C as its annihilator; it is simply given by rows i, j, k of M. If we find an invertible 3×3 matrix U such that $M_{ijk} = U^\top DU$ (where M_{ijk} is the principal 3×3 submatrix of M given by rows and columns i, j, k), then we can find a matrix L whose rows are in the space generated by rows i, j, k of M and such that $L_{ijk} = U$. Then $L^\top DL = M$, and L provides us with a representative (A, B, C) of the point on $\mathcal{J}$ we are looking for. Finding U is equivalent to finding an isomorphism between the conic

$$(x_1, x_2, x_3) M_{ijk} (x_1, x_2, x_3)^\top = 0 \qquad \text{and} \qquad x_1 x_3 - x_2^2 = 0\,,$$

which comes down to finding a point on the conic and parametrizing it.

For points with $\xi_1 = 0$, we can use the explicit description of the image of Θ given in the previous section.

Remark 3.1. One can check that the following three expressions are a possible choice for the missing three basis elements of the odd subspace of $L(3\Theta)$:

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

4. 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 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 $\kappa_1, \kappa_2, \ldots, \kappa_8$ 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

$$\begin{aligned}
\tilde{\xi}_1 &= \xi_1 \\
\tilde{\xi}_2 &= \xi_2 + 3\lambda f_7\xi_1 + 12\lambda^2 f_8\xi_1 \\
\tilde{\xi}_3 &= \xi_3 + 2\lambda\xi_2 + 3\lambda^2 f_7\xi_1 + 8\lambda^3 f_8\xi_1 \\
\tilde{\xi}_4 &= \xi_4 + \lambda\xi_3 + \lambda^2\xi_2 + \lambda^3 f_7\xi_1 + 2\lambda^4 f_8\xi_1 \\
\tilde{\xi}_5 &= \xi_5 + \lambda(2f_5\xi_1 + 3\xi_3) + \lambda^2(6f_6\xi_1 + 3\xi_2) + 17\lambda^3 f_7\xi_1 + 34\lambda^4 f_8\xi_1 \\
\tilde{\xi}_6 &= \xi_6 + \lambda(3\xi_4 + \xi_5) + \lambda^2(f_5\xi_1 + 3\xi_3) + \lambda^3(2f_6\xi_1 + 2\xi_2) + 5\lambda^4 f_7\xi_1 + 8\lambda^5 f_8\xi_1 \\
\tilde{\xi}_7 &= \xi_7 + \lambda(f_3\xi_1 + 2\xi_6) + \lambda^2(2f_4\xi_1 + 3\xi_4 + \xi_5) + \lambda^3(4f_5\xi_1 + 2\xi_3) \\
&\qquad + \lambda^4(6f_6\xi_1 + \xi_2) + 9\lambda^5 f_7\xi_1 + 12\lambda^6 f_8\xi_1 \\
\tilde{\xi}_8 &= \xi_8 + \lambda(f_3\xi_2 + 2f_5\xi_4 + 3f_7\xi_7) \\
&\qquad + \lambda^2(3f_3f_7\xi_1 + 2f_4\xi_2 + f_5\xi_3 + 6f_6\xi_4 + 3f_7\xi_6 + 12f_8\xi_7) \\
&\qquad + \lambda^3((12f_3f_8 + 6f_4f_7)\xi_1 + 4f_5\xi_2 + 4f_6\xi_3 + 17f_7\xi_4 + f_7\xi_5 + 16f_8\xi_6) \\
&\qquad + \lambda^4((24f_4f_8 + 11f_5f_7)\xi_1 + 8f_6\xi_2 + 12f_7\xi_3 + 46f_8\xi_4 + 6f_8\xi_5) \\
&\qquad + \lambda^5((44f_5f_8 + 18f_6f_7)\xi_1 + 16f_7\xi_2 + 32f_8\xi_3) \\
&\qquad + \lambda^6((68f_6f_8 + 29f_7^2)\xi_1 + 32f_8\xi_2) + 148\lambda^7 f_7f_8\xi_1 + 148\lambda^8 f_8^2\xi_1
\end{aligned}$$

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

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

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 (3.1) 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 (3.3), we have $L^\top DL = M$ with M as in (2.4). 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 $\tilde{\xi}_2, \ldots, \tilde{\xi}_7$ 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' two-torsion point, see below in Section 5.

5. The action of the two-torsion subgroup

There is a natural bijection between the two-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 $[\sum_{\omega \in \Omega_1} (\omega, 0) - (\#\Omega_1/2)\mathfrak{m}]$. Since $\#\Omega = 8$ is divisible by four, 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' two-torsion points are the 35 points corresponding to a partition into two sets of four roots, together with the origin, and the 'odd' two-torsion points are the 28 points corresponding to a partition into subsets of sizes two and six. 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

$$e_2(T, T') = \varepsilon(T)\varepsilon(T')\varepsilon(T + T')\,. \tag{5.1}$$

Note that $\mathrm{Pic}^0_{\mathcal{C}}$ is canonically isomorphic to $\mathrm{Pic}^2_{\mathcal{C}}$ (by adding the class of $\mathfrak{m}$), which contains the theta characteristics. In this way, the theta characteristics are identified with the two-torsion points, and the odd (resp., even) theta characteristics correspond to the 'odd' (resp., 'even') two-torsion points.

Using the transformations described in the previous section and the matrices obtained by Duquesne [Duq] representing the translation by a two-torsion point, we find the corresponding matrices in our setting for an 'even' nontrivial two-torsion point. The matrices for 'odd' two-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 two-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

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

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 (2.3) satisfied by points on the Kummer variety. We will write $\langle \cdot, \cdot \rangle_S$ for the pairing given by S: for vectors $\underline{\xi} = (\xi_1, \ldots, \xi_8)$ and $\underline{\zeta} = (\zeta_1, \ldots, \zeta_8)$, 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

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

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' 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 two-torsion points, this entry is zero.

For a two-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 $S = S^\top = S^{-1}$)

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

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

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

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

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

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 $\mathbb{P}^7$:

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

6. The action on quadratic and quartic forms

We follow the approach taken in [Sto1] and study the action of the two-torsion subgroup on quadratic and quartic forms on $\mathbb{P}^7$. We work over an algebraically closed field of characteristic different from two.

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

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

induced by the standard sequence

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \operatorname{SL}(8) \longrightarrow \operatorname{PSL}(8) \longrightarrow 0$$

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

Proof. Let $T \in \mathcal{J}[2]$ and let $M_T \in \operatorname{GL}(8)$ 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 $\tilde{M}_T \in \operatorname{SL}(8)$, 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 only differ by scaling, $\tilde{M}_T$ is well-defined up to sign. Among the lifts of the class of M_T in $\operatorname{PSL}(8)$ to $\operatorname{SL}(8)$, $\pm\tilde{M}_T$ 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 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 $\tilde{M}_T \tilde{M}_{T'}$ must be $\zeta \tilde{M}_{T+T'}$ for some eighth root of unity ζ. 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 $\zeta = \pm 1$, so that $\tilde{M}_T \tilde{M}_{T'} \in G$. □

Remark 6.2. Note that the situation here is somewhat different from the situation in genus two, 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 two-torsion points. The effect is that there is no map $\varepsilon \colon \mathcal{J}[2] \to \mu_2$ that induces the Weil pairing as in (5.1), so that we have to use a fourfold covering of $\mathcal{J}[2]$ in 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

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

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.

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

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

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 Weil pairing with T, then the above implies that

$$\rho_2 = \bigoplus_{T \colon \varepsilon(T)=1} \chi_T \,. \tag{6.1}$$

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 (2.3); we define

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

Then y_0 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 6.3. *For every nontrivial 'even' two-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. □

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

Remark 6.4. Note that if T is an 'odd' two-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 6.5. *Let T be a nontrivial 'even' two-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

$$y_T = \xi_8^2 + 2\sum_{j=2}^{8} \varepsilon_j\tau_j\,\xi_j\xi_8 + (\textit{terms not involving } \xi_8)\,.$$

Note that this is still true for $T = 0$ if we replace the first coordinate by zero (and similarly in the formula for y_T).

Proof. The last column of M_T has entries $1, \tau_2, \ldots, \tau_8$ (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 6.3, the claim follows. □

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 $\xi_1, \dots, \xi_8$ of V_1, then $\langle \phi, \phi' \rangle = \frac{1}{8} \operatorname{Tr}(A^\top A')$ (the scaling has the effect of giving the standard quadratic form norm 1).

For an 'even' two-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 6.6. *For all 'even' two-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 $\operatorname{Tr}\big((S\tilde{M}_T^\top)^\top (S\tilde{M}_{T'})\big)$ is zero if $T \neq T'$ and equals 8 if $T = T'$. We have

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

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. □

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

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

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

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

Proof. We have by Lemma 6.6

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

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

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

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

Corollary 6.8. *We have*

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

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

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

Proof. We compute using Lemma 6.7,

$$\begin{aligned}&\sum_{T\colon \varepsilon(T)=1} \frac{1}{8r(T)} y_T(\underline{\xi}) y_T(\underline{\zeta}) \\ &\qquad = \sum_{i=1}^{8} \xi_i^2 \sum_{T\colon \varepsilon(T)=1} \frac{[\xi_i^2] y_T(\underline{\xi})}{8r(T)} y_T(\underline{\zeta}) + \sum_{1 \le i < j \le 8} \xi_i\xi_j \sum_{T\colon \varepsilon(T)=1} \frac{[\xi_i\xi_j] y_T(\underline{\xi})}{8r(T)} y_T(\underline{\zeta}) \\ &\qquad = \sum_{i=1}^{8} \xi_i^2 \zeta_{9-i}^2 + 2 \sum_{1 \le i < j \le 8} \varepsilon_i\varepsilon_j \, \xi_i\xi_j\zeta_{9-i}\zeta_{9-j} \\ &\qquad = \Bigl(\sum_{j=1}^{8} \varepsilon_j \, \xi_j\zeta_{9-j}\Bigr)^2 .\end{aligned}$$

□

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

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

This gives us

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

We deduce that

$$\rho_4 = \chi_0^{\oplus 15} \oplus \bigoplus_{T\neq 0} \chi_T^{\oplus 5} \,. \tag{6.2}$$

Let $\underline{\delta} = (\delta_1, \ldots, \delta_8)$ denote the quartic forms that give the duplication map on the Kummer variety $\mathcal{K}$, scaled in such a way that $\delta_8(0,0,0,0,0,0,0,1) = 1$ (and then determined up to adding a quartic form vanishing on $\mathcal{K}$). We write E_4 for the space 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 $\mathbb{A}^{15}$ and checking whether it vanishes on $\mathcal{V}$.

Lemma 6.9.

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 $\delta_1, \ldots, \delta_8$ 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, and a subspace of dimension 36 is given by $y_0 V_2$. The latter splits in the same way as ρ_2 does. Since for the generic curve, the Galois action is transitive on the 'odd' two-torsion points and on the nontrivial 'even' two-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 two-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 $\delta \colon K \to K$ 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. □

We see that the 36 quartic forms y_T^2 for T an 'even' two-torsion point are in the invariant subspace of V_4 of dimension 15. Let k denote a field of characteristic different from 2 such that $F \in k[x,z]$. We assume that F is squarefree, so that $\mathcal{C}$ is a smooth hyperelliptic curve of genus 3 over k. Let $\mathcal{T}_{\text{even}}$ denote the finite k-scheme whose geometric points are the 36 'even' two-torsion points, and denote by k_{even} its coordinate ring; it is an étale k-algebra of dimension 36. Then $y \colon T \mapsto y_T$ can be considered as a quadratic form with coefficients in k_{even} and $r \colon T \mapsto r(T)$ is an element of $k_{\text{even}}^\times$.

Lemma 6.10. *The 36 coefficients* $c_{ii} = [\xi_i^2]y$, *for* $1 \le i \le 8$, *and* $c_{ij} = \frac{1}{2}[\xi_i\xi_j]y$, *for* $1 \le i < j \le 8$, *constitute a* k*-basis of* k_{even}.

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

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

Lemma 6.7 can be interpreted as saying that

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

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

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 that they indeed span a space of this dimension 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 $q_j = \xi_j\xi_8^3 + (\deg_{\xi_8} \le 2)$ for $j = 1, \ldots, 8$. Then the q_j can be chosen so that they have coefficients in $\mathbb{Z}[f_0, \ldots, f_8]$. To fix q_j completely, it suffices to in addition specify the coefficients of $\xi_1\xi_i\xi_8^2$ for $1 \le i \le 7$. One possibility is to choose them as given in Figure 1, which includes $q_9, \ldots, q_{15}$ in the ideal of $\mathcal{K}$, where $E_4^{\mathcal{J}[2]} = \langle q_9, q_{10}, \ldots, q_{15}\rangle$.

We claim that we can take

$$(\delta_1, \delta_2, \ldots, \delta_8) = (4q_1, 4q_2, 4q_3, 4q_4, 4q_5, 4q_6, 4q_7, q_8)\,.$$

It can be checked that the induced basis of $V_4^{\mathcal{J}[2]}/E_4^{\mathcal{J}[2]}$ transforms in the same way under the action of SL(2) (by linear substitution of the homogeneous variables in A, B, C, F) as our coordinates $(\xi_1, \ldots, \xi_8)$. So we can apply an isomorphism to $\mathcal{C}$ and assume that $f_8 = 0$. We can then embed the curve into Pic^4 by adding $\mathfrak{m}$ and the Weierstrass point at infinity. The point (x_0, y_0) then maps to

$$(0 : 0 : 0 : 0 : 1 : -x_0 : x_0^2 : -f_7x_0^3)$$

and its double maps to

$$(0 : 1 : -2x_0 : x_0^2 : 3x_0^2 : -2x_0^3 : x_0^4 : *)$$

where $*$ is some polynomial in the f_j and x_0 divided by $4F(x_0, 1)$. We check that our δ_j restrict to this (up to scaling by $-4f_7^2F(x_0, 1)$) on the image of $\mathcal{C}$.

$$
\begin{aligned}
q_1 &= \xi_1\xi_8^3 + 2(-f_2\xi_2 + f_3\xi_3 - f_4\xi_4 - f_4\xi_5 + f_5\xi_6 - f_6\xi_7)\xi_1\xi_8^2 + \ldots \\
q_2 &= \xi_2\xi_8^3 + (4f_8(-f_0\xi_2 + f_2\xi_4 + f_4\xi_7) - 2f_3f_8\xi_6 - f_5f_7\xi_7)\xi_1\xi_8^2 + \ldots \\
q_3 &= \xi_3\xi_8^3 + (f_7(-2f_0\xi_2 + 2f_2\xi_4 + f_3\xi_6) \\
&\qquad\qquad + 2f_8(-2f_0\xi_3 + 4f_1\xi_4 - 2f_2\xi_6 - f_3\xi_7))\xi_1\xi_8^2 + \ldots \\
q_4 &= \xi_4\xi_8^3 + (-2f_0f_7\xi_3 + (12f_0f_8 + f_1f_7)\xi_4 - 2f_1f_8\xi_6)\xi_1\xi_8^2 + \ldots \\
q_5 &= \xi_5\xi_8^3 + ((4f_0f_6 - 2f_1f_5)\xi_2 + (-2f_0f_7 - 2f_1f_6 + 2f_2f_5)\xi_3 \\
&\qquad\qquad + (4f_0f_8 + 4f_1f_7 + 4f_2f_6 - 5f_3f_5)\xi_4 \\
&\qquad\qquad + (-2f_1f_8 - 2f_2f_7 + 2f_3f_6)\xi_6 + (4f_2f_8 - 2f_3f_7)\xi_7)\xi_1\xi_8^2 + \ldots \\
q_6 &= \xi_6\xi_8^3 + (f_0(-2f_5\xi_2 - 4f_6\xi_3 + 8f_7\xi_4 - 4f_8\xi_6) \\
&\qquad\qquad + f_1(f_5\xi_3 + 2f_6\xi_4 - 2f_8\xi_7))\xi_1\xi_8^2 + \ldots \\
q_7 &= \xi_7\xi_8^3 + (4f_0(f_4\xi_2 + f_6\xi_4 - f_8\xi_7) - f_1f_3\xi_2 - 2f_0f_5\xi_3)\xi_1\xi_8^2 + \ldots \\
q_8 &= \xi_8^4 + 16(f_1f_8(f_1\xi_2 - f_2\xi_3 + f_3\xi_4) + f_0f_7(f_5\xi_4 - f_6\xi_6 + f_7\xi_7))\xi_1\xi_8^2 + \ldots
\end{aligned}
$$

$$
\begin{aligned}
q_9 &= 2(f_7\xi_6 - 4f_8\xi_7)\xi_1\xi_8^2 + \ldots \\
q_{10} &= 2(f_5\xi_4 - f_6\xi_6 + f_7\xi_7)\xi_1\xi_8^2 + \ldots \\
q_{11} &= 2(f_3\xi_3 + 2f_4\xi_4 - 2f_4\xi_5 + f_5\xi_6)\xi_1\xi_8^2 + \ldots \\
q_{12} &= 2(f_1\xi_2 - f_2\xi_3 + f_3\xi_4)\xi_1\xi_8^2 + \ldots \\
q_{13} &= 2(-4f_0\xi_2 + f_1\xi_3)\xi_1\xi_8^2 + \ldots \\
q_{14} &= (3\xi_4 - \xi_5)\xi_1\xi_8^2 + \ldots \\
q_{15} &= \xi_1^2\xi_8^2 + \ldots = (\xi_1\xi_8 - \xi_2\xi_7 + \xi_3\xi_6 - \xi_4\xi_5)^2
\end{aligned}
$$

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

Since q_1 is the only invariant quartic (mod E_4) that vanishes on the image of $\mathcal{C}$, this shows that our δ_j are correct up to multiples of q_1. We can also check that $\delta_1\delta_8 - \delta_2\delta_7 + \delta_3\delta_6 - \delta_4\delta_5$ vanishes on $\mathcal{K}$. As this is the only quadratic relation that holds on $\mathcal{K}$, the multiples of q_1 must also be correct. We therefore find the following.

Theorem 6.11. *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) $\delta_j \in \mathbb{Z}[f_0, f_1, \ldots, f_8][\xi_1, \xi_2, \ldots, \xi_8]$ *for all* $1 \le j \le 8$.

(2) *The map $\delta \colon \mathcal{K} \to \mathcal{K}$ given by $(\delta_1 : \ldots : \delta_8)$ is the duplication map on $\mathcal{K}$.*
(3) $(\delta_1, \delta_2, \ldots, \delta_8)(0, 0, \ldots, 0, 1) = (0, 0, \ldots, 0, 1)$.
(4) *With y_T as defined earlier for an 'even' two-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 $\underline{\tau} = (1, \tau_2, \ldots, \tau_8)$ and $\underline{\delta} = (\delta_1, \ldots, \delta_8)$.

Proof.

(1) This can be verified using the explicit polynomials.
(2) See the discussion preceding the theorem.
(3) This is obvious.
(4) We compare the coefficients of $\xi_j\xi_8^3$ on both sides. Since by Corollary 6.5,

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

we find

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

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 $E_4^{\mathcal{J}[2]}$. □

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

Corollary 6.12. *Let $\underline{\xi}$ be coordinates of a point on $\mathcal{K}$ ($\underline{\xi} = 0$ is allowed).*

(1) *If $\underline{\delta}(\underline{\xi}) = 0$, then $y_T(\underline{\xi}) = 0$ for all 'even' two-torsion points T.*
(2) *If $\operatorname{disc}(F) \neq 0$, then $\underline{\delta}(\underline{\xi}) = 0$ implies $\underline{\xi} = 0$.*
(3) *If $\kappa(T)$ are coordinates of the image on $\mathcal{K}$ of a two-torsion point T, given by a factorization $F = GH$, as in (2.5) or (2.6), then $\delta_8(\kappa(T)) = \operatorname{Res}(G, H)^2$ (and the other δ_j vanish). So $\kappa(T)$ belongs to the base scheme of $\underline{\delta}$ if and only if G and H are not coprime.*

Proof.

(1) This follows from the last statement in Theorem 6.11.
(2) By the first part, $y_T(\underline{\xi}) = 0$ for all 'even' T. Since $\operatorname{disc}(F) \neq 0$, we also have $r(T) \neq 0$ for all T; then by Lemma 6.7 we obtain $\xi_j = 0$ for all j.
(3) This comes out of an explicit computation. □

Note that the action of $\mathrm{GL}(2)$ on (x, z) induces an action on the coefficients of F and on our coordinates $\underline{\xi}$. This induces a 'degree' coming from scaling F:

$$\deg(f_j) = 1, \quad \deg(\underline{\xi}) = (0, 1, 1, 1, 1, 1, 1, 2)$$

and a 'weight' coming from scaling x:

$$\mathrm{wt}(f_j) = j, \quad \mathrm{wt}(\underline{\xi}) = (0, 6, 5, 4, 4, 3, 2, 8)\,.$$

On the level of the coordinates a_j, b_j, c_j on $\mathbb{A}^{15}$, we have

$$\deg(a_j) = \deg(b_j) = \deg(c_j) = \frac{1}{2} \qquad \text{and} \qquad \mathrm{wt}(a_j) = \mathrm{wt}(b_j) = \mathrm{wt}(c_j) = j\,.$$

For example, the invariant quartics given above are homogeneous with respect to this degree and weight:

$$\begin{aligned} \deg(q_1, q_2, \ldots, q_{15}) &= (6, 7, 7, 7, 7, 7, 7, 8,\ 6, 6, 6, 6, 6,\ 5,\ 4) \\ \mathrm{wt}(q_1, q_2, \ldots, q_{15}) &= (24, 30, 29, 28, 28, 27, 26, 32,\ 26, 25, 24, 23, 22,\ 20,\ 16) \end{aligned}$$

We find 70 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:

$$\begin{aligned} \deg = 4\colon &\quad \mathrm{wt} = 12, 13, 14, 14, 15, 15, 16, 16, 16, 17, 17, 18, 18, 19, 20 \\ \deg = 5\colon &\quad \mathrm{wt} = 17, 18, 18, 19, 19, 20, 20, 20, 21, 21, 22, 22, 23 \\ \deg = 6\colon &\quad \mathrm{wt} = 22, 23, 24, 24, 25, 26 \end{aligned}$$

These quartics are given in the file `Kum3-quartics.magma` at [Data]. The 15 quartics of degree 4 are exactly those obtained as 4×4-minors of the matrix M in (2.4).

The canonical map from $V_2 = \mathrm{Sym}^2 L(2\Theta)$ 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 $V_2 \to L(4\Theta)^+$ 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 6.13. *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 that this polynomial is the square of some other polynomial p that can be written as a quadratic in the components of $A_l \wedge B_l \wedge C_l$. So p is invariant under $\pm\Gamma$, which means that it gives an element Ξ of $L(4\Theta)^+$. □

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 $j \in \{2, 3, \ldots, 8\}$ 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' two-torsion points T.

7. Further properties of the duplication map

We refine the statement of Corollary 6.12. We stress that the coefficients f_j of F are completely arbitrary; we do not assume that F has non-vanishing discriminant or even that F is nonzero. Since $\mathcal{K}$ and $\underline{\delta}$ are defined in terms of polynomials with coefficients in $\mathbb{Z}[f_0, \ldots, f_8]$, they make sense over any field (or even ring) and for any choice of the f_j.

Lemma 7.1. *Let k be a field, $f_0, \ldots, f_8 \in k$, and let $\mathcal{K}$ and $\underline{\delta}$ be the associated objects defined over k. If $\underline{\xi} \in k^8$ are coordinates of a point on $\mathcal{K}$, then we have*

$$\underline{\delta}(\underline{\xi}) = 0 \iff y_T(\underline{\xi}) = 0 \quad \textit{for all 'even' } T \neq 0 \quad \textit{and} \quad 2\Xi(\underline{\xi}) = 0\,.$$

Proof. The implication '$\Longrightarrow$' is Corollary 6.12, together with $(2\Xi)^2 = \delta_1$. So we only have to show the other implication. In characteristic 2, we have $\delta_j = 0$ for $j \neq 8$ and therefore $y_T^2 = \delta_8$ on $\mathcal{K}$ (for all T), which makes the claim obvious. If $F = 0$, we have $\delta_8 = \xi_8^4$ and $\delta_j = 4\xi_j\xi_8^3$ for $j < 8$. For all T, we have $\kappa(T) = (1 : 0 : \ldots : 0)$, so $y_T^2 = \delta_8$ on $\mathcal{K}$, and $y_T = 0$ implies $\delta_8 = 0$ and thence $\underline{\delta} = 0$. In the remaining case $F \neq 0$, $\operatorname{char}(k) \neq 2$, we can assume that F splits over k (otherwise we enlarge k). Acting on F by $\mathrm{GL}(2)$, we can move up to three roots to ∞, 0 and 1, and we can assume that $F(x, 1)$ is monic (perhaps after a further field extension). In the finitely many resulting cases, we check by an explicit computation that $\delta_2, \delta_3, \ldots, \delta_8$ vanish on the subvariety of $\mathcal{K}$ given by the vanishing of the y_T. The vanishing of Ξ implies the vanishing of δ_1 (it turns out that using Ξ is only necessary when F either has a root of multiplicity 8 or two roots of multiplicities 2 and 6). The most complicated cases (with many distinct roots) are more easily dealt with by observing that the coordinate vectors $\kappa(T)$ generate k^8, so by Theorem 6.11 the vanishing of all y_T implies the vanishing of $\underline{\delta}$. This applies whenever F has at most double roots. □

We now state explicit criteria for the vanishing of $\underline{\delta}$ at a point on $\mathcal{K}$. We first exhibit a sufficient condition. For the following, we fix an algebraically closed field k of characteristic $\neq 2$ and a homogeneous polynomial $F \in k[x, z]$ of degree 8. We continue to denote by $\mathcal{K}$ and $\underline{\delta}$ the objects associated to F via the polynomials constructed earlier.

Lemma 7.2. *Assume that $F(x, z)$ is divisible by x^2. Let $\underline{\xi}$ be the coordinate vector of a point on $\mathcal{K}$ such that $\xi_4 = \xi_6 = \xi_7 = \xi_8 = 0$. Then $\underline{\delta}(\underline{\xi}) = 0$.*

Proof. Plugging $f_0 = f_1 = \xi_4 = \xi_6 = \xi_7 = \xi_8 = 0$ into the expressions for the δ_j gives zero. □

We set

$$L_0 = \{(\xi_1 : \ldots : \xi_8) \in \mathbb{P}^7 : \xi_4 = \xi_6 = \xi_7 = \xi_8 = 0\}.$$

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 0; then $\tilde{F}$ is divisible by x^2. We write $L_a \subset \mathbb{P}^7$ for the image of L_0 under the automorphism of $\mathbb{P}^7$ induced by ϕ^{-1} (compare Section 4). It can be checked that L_a does not depend on ϕ. For example,

$$L_\infty = \{(\xi_1 : \ldots : \xi_8) \in \mathbb{P}^7 : \xi_2 = \xi_3 = \xi_4 = \xi_8 = 0\}.$$

We write $A(F) \subset \mathbb{P}^1$ for the set of multiple roots of F.

Corollary 7.3. *If $P \in \mathcal{K} \cap L_a$ for some $a \in A(F)$, then $\underline{\delta}(P) = 0$.*

Proof. This follows from Lemma 7.2 by applying a suitable automorphism of $\mathbb{P}^1$. □

Even when F is not squarefree, we still obtain a matrix M_T, a point on $\mathcal{K}$ and a quadratic form y_T associated to each factorization $F = G \cdot H$ of F into two binary forms of degree 4. Assume for now that $F \neq 0$ and write

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

We define $\mathcal{T}(F)$ to be the set of such T associated to factorizations (G, H) with G and H both divisible by F_0. We also set $\mathcal{T}(0)$ to be the one-element set $\{T\}$, where T corresponds to the factorization $0 = 0 \cdot 0$. We write $\kappa(T)$ for the corresponding point on $\mathcal{K}$ with first coordinate 1.

Lemma 7.4. *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 $\langle \kappa(T), \underline{\xi} \rangle_S = 0$.*

Proof. By Theorem 6.11 (4), 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 $T \in \mathcal{T}(F)$. One can 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 check the claim made above, 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 $\deg F_0 = 1$ (the case that F is squarefree itself being dealt with in Corollary 6.12). 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 $\operatorname{disc}(F_1)$, hence is invertible. The other cases are similar, but simpler. □

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 $\mathcal{K}$. Then the lemma immediately implies the following.

Corollary 7.5. *The duplication map $\delta \colon \mathcal{K} \to \mathcal{K}$ is defined on $\mathcal{K}_{\text{good}}$ and maps $\mathcal{K}_{\text{good}}$ into itself.*

When F is not a nonzero square, we can show a bit more.

Lemma 7.6. *Assume that F is not of the form $F = H^2$ with $H \neq 0$. Let $P \in \mathcal{K}$ be such that $\langle \kappa(T), P \rangle_S = 0$ for all $T \in \mathcal{T}(F)$. Then $P \in L_a$ for some $a \in A(F)$.*

Proof. Let $\underline{\xi}$ be a coordinate vector for P. We split the proof into various cases according to the factorization type of F_0. Note that we can move the roots of F_0 to 0, ∞ and 1.

1. $F_0 = x$. In this case the assumption is equivalent to $\xi_4 = \xi_6 = \xi_7 = \xi_8 = 0$, so that $P \in L_0$.
2. $F_0 = x^2$. The assumption is $\xi_7 = \xi_8 = 0$; this implies (using the equations defining $\mathcal{K}$) $\xi_4 = \xi_6 = 0$, so $P \in L_0$.
3. $F_0 = x^3$. The assumption is $\xi_8 = 0$, which in turn implies $\xi_7 = \xi_6 = \xi_4 = 0$, so $P \in L_0$.
4. $F_0 = xz$. In this case the assumption is $\xi_4 = \xi_8 = 0$, which then implies $\xi_6 = \xi_7 = 0$ or $\xi_2 = \xi_3 = 0$, and so $P \in L_0$ or $P \in L_\infty$.
5. $F_0 = x^2z$. The assumption is $\xi_8 = 0$, which leads to $\xi_4 = 0$ and then to $P \in L_0$ or $P \in L_\infty$.

6. $F_0 = xz(x - z)$. A similar computation shows that $P \in L_0 \cup L_1 \cup L_\infty$.
7. $F = 0$. Here the assumption is $\xi_8 = 0$. The scheme $\mathcal{K} \cap \{\xi_8 = 0\}$ is defined by the 2×2-minors of the matrix
$$\begin{pmatrix} \xi_2 & \xi_3 & \xi_4 \\ \xi_3 & \xi_4 + \xi_5 & \xi_6 \\ \xi_4 & \xi_6 & \xi_7 \end{pmatrix} ;$$
writing $(\xi_4 : \xi_3) = (\xi_3 : \xi_2) = \ldots = (\lambda : \mu)$, it follows that $P \in L_{(\lambda:\mu)}$. □

Corollary 7.7. *If F is not of the form $F = H^2$ with $H \neq 0$, then the base scheme of δ is exactly the complement of $\mathcal{K}_{\text{good}}$.*

Proof. Corollary 7.5 shows that the base scheme of δ is contained in $\mathcal{K} \setminus \mathcal{K}_{\text{good}}$. So let $P \in \mathcal{K} \setminus \mathcal{K}_{\text{good}}$. Then by Lemma 7.6, $P \in L_a$ for some $a \in A(F)$, so by Corollary 7.3, $\underline{\delta}(P) = 0$, so P is in the base scheme of δ. □

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 $B \equiv \pm F_0 \bmod A$, and we can change the representative so that $B = \pm F_0$, which makes $C = 0$. So the two components of $\operatorname{Pic}^4(\mathcal{C})$ 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 $T \in \mathcal{T}(F)$. Note that $\underline{\delta}(\kappa(T)) = 0$, since $r(T) = 0$. 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 7.4, this is equivalent to $\langle \kappa(T), \underline{\xi} \rangle_S = 0$. We write E for the hyperplane given by $\langle \kappa(T), \underline{\xi} \rangle_S = 0$. In this case, $P \in \mathcal{K} \cap E$ does not necessarily imply that $\underline{\delta}(P) = 0$. But we still have the following.

Lemma 7.8. *Assume that $F = F_0^2$ with $F_0 \neq 0$. If $P \in \mathcal{K}$ with $\underline{\delta}(P) = 0$, then $P \in L_a$ 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; the computations are similar to those done in the proof of Lemma 7.6. The most involved case is when F_0 has four distinct roots. □

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 7.9. *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. *A point $P \in \mathcal{K}$ is in the base scheme of δ (so that $\underline{\delta}(P) = 0$) if and only if $P \in L_a$ for some $a \in A(F)$.*
2. *Assume that F is not of the form $F = F_0^2$ with $F_0 \neq 0$. If $P \in \mathcal{K}$ is not in the base scheme of δ, then the same is true for $\delta(P)$.*
3. *Assume that $F = F_0^2$ with $F_0 \neq 0$. If $P \in \mathcal{K} \setminus E$, then P is not in the base scheme of δ and $\delta(P) \notin E$, so $\delta(P)$ is not in the base scheme of δ either.*

Proof.

1. Corollary 7.3 shows that the condition is sufficient. Conversely, if $\underline{\delta}(P) = 0$, then Lemmas 7.4, 7.6 and 7.8 show that $P \in L_a$ for some multiple root a of F.
2. This follows from Corollaries 7.5 and 7.7.
3. Recall that $P \notin E \iff \delta(P) \notin E$ by Lemma 7.4. In particular, $P \notin E$ implies that $\underline{\delta}(P) \neq 0$, so P is not in the base scheme of δ. The same argument can then be applied to $\delta(P)$. □

8. Sum and difference on the Kummer variety

We consider the composition

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

where 'symm.' is the symmetrization map that sends a matrix A to $A + A^\top$ (identifying 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 $o = (0, \ldots, 0, 1)$.

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 $\mathrm{Tr}(M^\top B) = 8\langle M, B\rangle$. Put differently, we obtain the (i, j)-entry of the matrix by evaluating at the quadratic form $\xi_i\xi_j$.

The two-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' two-torsion points T; for V_2^* we use the basis dual to $(y_T)_{T \text{ `even'}}$, which is given by the linear forms

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

If T_1, T_2, T_3 are 'even' two-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:

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

In other words, β_o, interpreted as a linear map $V_2 \to \tilde{V}_2$, 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 $\mathrm{Sym}^2 \tilde{V}_2 \otimes V_2^*$, 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 $\frac{1}{2}\delta_1, \ldots, \frac{1}{2}\delta_7, \delta_8$. 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

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

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

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

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

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

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

$$q = \xi_1(f_3f_5\xi_4 + f_1f_7\xi_5) + f_1\xi_2\xi_3 + f_3\xi_2\xi_6 + f_5\xi_3\xi_7 + f_7\xi_6\xi_7 + (\xi_4 + \xi_5)\xi_8\,,$$

then the entries of

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

are (up to addition of multiples of $y_0(\underline{\xi})$ and $y_0(\underline{\zeta})$) in $\mathbb{Z}[f_0, \ldots, f_8][\underline{\xi}, \underline{\zeta}]$. (Note that $q \equiv \Xi \bmod (2, y_0)$ 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 two 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*

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

Proof. This follows from $\langle z_T, \xi_1^2\rangle = [\xi_8^2]y_T = 1$ (for $T \neq 0$) and Corollary 6.8:

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

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 $P-Q \in \Theta$. □

This is analogous to the duality between the Kummer Surface and the Dual Kummer Surface in the case of a curve of genus two, 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' two-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). □

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

We formulate an important property of the 'add-and-subtract' morphism. We write $\alpha\colon \operatorname{Sym}^2\mathcal{K} \to \operatorname{Sym}^2\mathcal{K}$ for the map given by B; note that this is defined for arbitrary $F \in k[x,z]$, homogeneous of degree 8. Recall the definition of $\mathcal{K}_{\mathrm{good}}$ from Section 7.

Lemma 8.5. *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 is defined on $\operatorname{Sym}^2\mathcal{K}_{\mathrm{good}}$, and $\alpha(\operatorname{Sym}^2\mathcal{K}_{\mathrm{good}}) \subset \operatorname{Sym}^2\mathcal{K}_{\mathrm{good}}$.*

Proof. Note that $\alpha\circ\alpha = \operatorname{Sym}^2\delta$ — this comes from

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

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

$$\underline{\zeta} * \underline{\zeta}' = 2B(\underline{\xi},\underline{\xi}') \quad\Longrightarrow\quad \underline{\delta}(\underline{\xi}) * \underline{\delta}(\underline{\xi}') = 2B(\underline{\zeta},\underline{\zeta}')\,, \tag{8.2}$$

up to a scalar factor, which we find to be 1 by taking $\underline{\xi} = \underline{\xi}' = (0, \dots, 0, 1)$. 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 7.5, $\underline{\delta}(\underline{\xi})$ 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 $\operatorname{Sym}^2 \mathcal{K}_{\text{good}}$, then iterating α at most four more times would produce zero by the result of Section 7, but by the same results, this contradicts the fact that δ can be iterated indefinitely on the points represented by $\underline{\xi}$ and $\underline{\xi}'$. □

9. Heights

We now assume that the curve $\mathcal{C}$ (and therefore also the related objects) are defined over a number field k. We define the *naive height* on the Jacobian $\mathcal{J}$ and on the Kummer surface $\mathcal{K}$ to be the standard height on $\mathbb{P}^7$ with respect to the coordinates $(\xi_1 : \ldots : \xi_8)$. We denote it by

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

where v runs through the places of k and the absolute values $|\cdot|_v$ are normalized in such a way as to satisfy the product formula.

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

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

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

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

We follow the approach that was successful in other situations: we write

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

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

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

with $\varepsilon_v(P) = \max_j \log|\delta_j(\underline{\xi}(P))|_v - 4\max_j \log|\xi_j(P)|_v$, which can be defined for all $P \in \mathcal{J}(k_v)$ or $\mathcal{K}(k_v)$. Then $\varepsilon_v \colon \mathcal{K}(k_v) \to \mathbb{R}$ is continuous, so (since $\mathcal{K}(k_v)$ is compact) it is bounded. If $-\gamma_v \le \inf_{P\in\mathcal{K}(k_v)} \varepsilon_v(P)$, then we have

$$\beta \le \sum_v \sum_{n=0}^{\infty} 4^{-(n+1)}\gamma_v = \tfrac{1}{3}\sum_v \gamma_v\,.$$

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

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

we also have

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

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 earlier for 'even' two-torsion points have entries that are algebraic integers. We use $\mathcal{O}$ to denote the ring of all algebraic integers. Let $\underline{x} = (x_1, x_2, \ldots, x_8)$ be coordinates of a point on $\mathcal{K}$. Then Theorem 6.11 tells us that

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

and Lemma 6.7 tells us that

$$x_j^2 \in \sum_{T\neq 0} \frac{1}{8r(T)} \mathcal{O} y_T(\underline{x}) \,.$$

Lemma 9.1. *Let v be a non-archimedean place of k. Then for $P \in \mathcal{K}(k_v)$, we have*

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

where T runs through the non-trivial 'even' two-torsion points.

Proof. Let $(x_1 : \ldots : x_8)$ be coordinates for P and write $d_j = \delta_j(x_1, \ldots, x_8)$ for $j = 1, \ldots, 8$. Then for all 'even' $T \neq 0$

$$|y_T(x_1, \ldots, x_8)|_v^2 \le \max_j |d_j|_v$$

and

$$|x_j|_v^4 \le \max_T |8r(T)|_v^{-2} |y_T(x_1, \ldots, x_8)|_v^2 \le \max_T |8r(T)|_v^{-2} \max_j |d_j|_v \,.$$

So

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

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

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

$$\varepsilon_v(P) \ge -\Big\lfloor \max_T v\big(|2^6 r(T)^2|\big) \Big\rfloor \log |\pi_v|_v \,.$$

Example 9.2. For the curve

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

over $\mathbb{Q}$ and $v = 2$, the discriminant bound gives $\varepsilon_2(P) \ge -22\log 2$, since the discriminant of the polynomial on the right hand side (considered as a dehomogenized octic form) has 2-adic valuation 16. The resultants all have the same valuation $\frac{32}{7}$, leading to $\varepsilon_2(P) \ge -(15 + \frac{1}{7})\log 2$, which can be improved to $-15\log 2$, so that we get $-\mu_2 \le 5\log 2$.

Corollary 9.3. *Assume that $k = \mathbb{Q}$. Then we have*

$$\beta \le \tfrac{1}{3}\log|2^6\operatorname{disc}(F)| + \tfrac{1}{3}\gamma_\infty\,.$$

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' two-torsion point T (with $\tau_1(T) = 1$) and $\upsilon_j(T)$ for the coefficients in the formula for ξ_j^2, so that we have

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

Lemma 9.4. *Let v be an archimedean place of k. Then we have*

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

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

$$|y_T(x_1,\dots,x_8)|_v^2 \le \sum_{j=1}^{8} |\tau_j(T)|_v \max_j |d_j|_v$$

and

$$\max_j |x_j|_v^2 \le \max_j \sum_T |\upsilon_j(T)|_v |y_T(x_1,\dots,x_8)|_v\,.$$

Combining these gives the result. □

We can refine this result somewhat. Define a function

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

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

Lemma 9.5. *Define a sequence* (b_n) *in* $\mathbb{R}^8_{\geq 0}$ *by*

$$b_0 = (1, \dots, 1) \qquad \text{and} \qquad b_{n+1} = f(\|b_n\|_\infty^{-1} b_n)\,.$$

Then we have

$$\mu_v(P) \geq -\frac{1}{4^N - 1} \sum_{n=0}^{N-1} 4^{N-n} \log \|b_{N-n}\|_\infty$$

for all $N \geq 1$ *and all* $P \in J(\mathbb{C})$.

Proof. By our previous considerations, it is clear that $|\delta_j(\underline{x})|_v \leq d_j$ for all j implies $|x_j|_v \leq f_j(d_1, \dots, d_8)$ for all j. Since f is homogeneous of degree $1/4$, we can deduce by induction on N that

$$\log |\underline{x}|_v \leq \sum_{n=0}^{N-1} 4^{-n} \log \|b_{N-n}\|_\infty + \log |\delta^{\circ N}(\underline{x})|_v$$

for all $N \geq 1$. Writing

$$\mu_v = \sum_{m=0}^{\infty} 4^{-mN} \bigl(4^{-N} \log |\delta^{\circ mN}(\underline{x}(2^{mN} P))|_v - \log |\underline{x}(2^{mN} P)|_v\bigr)\,,$$

we obtain a lower bound of

$$-\sum_{n=0}^{N-1} 4^{-n} \log \|b_{N-n}\|_\infty$$

for each of the terms in parentheses. Plugging this estimate into the geometric series gives the result. □

Example 9.6. 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.

Lemma 9.7. *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 $v(\operatorname{disc}(F)) = 1$.

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 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 a further 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 7.9, the reduction of P must lie in some 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 3. By (3.2), we have

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

(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

$$\begin{aligned} \nu_1 &= (\xi_4 - \xi_5)\mu_{013} + \xi_7\mu_{123} \\ \nu_2 &= \xi_3\mu_{014} - \xi_4\mu_{023} \\ \nu_3 &= \xi_2\mu_{024} - \xi_4\mu_{134} \end{aligned}$$

are odd functions in $L(4\Theta)$, so their squares can be written as quartics in the ξ_j. It turns out that modulo $I = (f_0, f_1, \xi_1, \xi_4, \xi_6, \xi_7, \xi_8)^2$, we have

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

Since (at least) one of ξ_2, ξ_3, ξ_5 is a unit, $v(f_0) = 1$, and everything in I has valuation at least 2, 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. □

Example 9.8. The discriminant of the curve

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

is $2^{28} \cdot 19 \cdot 223 \cdot 44909$. Lemma 9.7 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 9.2 and 9.6, we obtain the bound

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

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]. The only caveat is that, 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 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.

Lemma 9.9. *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 8.5: 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 7.

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 (8.2) then gives

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

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 have

$$\begin{aligned}\varepsilon_v(P'+P)+\varepsilon_v(P'-P) &= \log\bigl|\underline{\delta}(\underline{\zeta}) * \underline{\delta}(\underline{\zeta}')\bigr|_v - 4\log|\underline{\zeta} * \underline{\zeta}'|_v \\ &= \log\bigl|2B\bigl(\underline{\delta}(\underline{\xi}), \underline{\delta}(\underline{\xi}')\bigr)\bigr|_v - 4\log\bigl|2B(\underline{\xi}, \underline{\xi}')\bigr|_v \\ &= \varepsilon_v(2P, 2P') + 2\log|\underline{\delta}(\underline{\xi})|_v + 2\log|\underline{\delta}(\underline{\xi}')|_v \\ &\qquad - 4\varepsilon_v(P, P') + 8\log|\underline{\xi}|_v + 8\log|\underline{\xi}'|_v \\ &= 2\varepsilon_v(P) + 2\varepsilon_v(P') + \varepsilon_v(2P, 2P') - 4\varepsilon_v(P, P')\,.\end{aligned}$$

Replacing P and P' by $2^n P$ and $2^n P'$, respectively, multiplying the relation by 4^{-n} and adding, we obtain

$$\mu_v(P'+P) + \mu_v(P'-P) = 2\mu_v(P) + 2\mu_v(P') - \varepsilon_v(P, P')\,. \tag{9.1}$$

Now assume that $\mu_v(P) = 0$. We have to show that $\mu_v(P'+P) = \mu_v(P')$. Note that $\varepsilon_v(\cdot,\cdot)$ is a locally constant function on the compact group $\mathcal{J}(k_v) \times \mathcal{J}(k_v)$, so it factors through a finite quotient. In particular, the sequence $\bigl(\varepsilon_v(P, P'+nP)\bigr)_{n\in\mathbb{Z}}$ is periodic. Replacing P' by $P'+nP$ in (9.1) above and adding, we get, for every $m \in \mathbb{Z}_{>0}$,

$$\begin{aligned}\mu_v(P'+(m+1)P) - \mu_v(P'+mP) - \mu_v(P'-mP) + \mu_v(P'-(m+1)P) \\ = -\sum_{n=-m}^{m} \varepsilon_v(P, P'+nP)\,.\end{aligned}$$

The left hand side is bounded independently of m. If $\varepsilon_v(P, P'+nP)$ were nonzero (and hence negative) for some n, then it would be < 0 for infinitely many n because of the periodicity, and this would lead to a contradiction for sufficiently large m. It follows that $\varepsilon_v(P, P'+nP) = 0$ for all n, so that

$$\mu_v(P'+(n+1)P) - 2\mu_v(P'+nP) + \mu_v(P'+(n-1)P) = 0 \qquad \text{for all } n.$$

The only bounded sequences $(a_n)_{n\in\mathbb{Z}}$ satisfying $a_{n+1} - 2a_n + a_{n-1} = 0$ for all n are the constant ones. In particular, it follows that $\mu_v(P'+P) = \mu_v(P')$ as desired. □

10. An application

We consider the curve

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

which isomorphic to the curve

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

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 [BMSST]. 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 [Magma] 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 the approach described in this paper 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

$$P_1 = [(0,1) - \infty]\,, \quad P_2 = [(1,1) - \infty]\,, \quad P_3 = [(-1,1) - \infty]\,,$$
$$P_4 = [(1,-1) + (\omega,-1) + (\omega^2,-1) - 3\cdot\infty]$$

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 $\rho^2 \le 0.50752$. Using Example 9.8, 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

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

so that we can write $\kappa(P) = (\xi_1 : \xi_2 : \ldots : \xi_8) \in \mathcal{K}(\mathbb{Q})$ with coprime integers ξ_j such that $|\xi_j| \le \lfloor e^{4.41155} \rfloor = 82$. 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 10.1. *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

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

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 [BMSST]. This shows that

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

for any such point (x, y). On the other hand, using the second stage of the Mordell-Weil sieve as explained in [BMSST], 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 10.2. *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* $(5, -279)$.

11. 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

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

We can therefore use $\mathcal{K}$ as a model for the Kummer variety associated to the curve $\mathcal{C}^{(c)} \colon y^2 = cF(x, z)$. 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 9.1 and 9.5 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 9.7 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 9.7 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

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

It is isomorphic to the curve

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

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

$$\begin{gathered}
(-2, 210) - \infty\,, \quad (1, 210) - \infty\,, \quad (3, 210) - \infty\,, \\
(2, 210) - \infty\,, \quad (-3, 210) - \infty\,, \quad (4, 630) - \infty\,, \\
(-\tfrac{5}{2}, -\tfrac{1785}{8}) + (3, 210) + (4, 630) - 3\infty\,, \\
(0, 210) - \infty\,, \quad (6, 3570) - \infty\,.
\end{gathered}$$

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 9.7 and Lemma 9.5):

$$\begin{gathered}
\mu_2 \ge -6\log 2\,, \quad \mu_3 \ge -\tfrac{10}{3}\log 3\,, \quad \mu_5 \ge -\tfrac{10}{3}\log 5\,, \quad \mu_7 \ge -\tfrac{8}{3}\log 7\,, \\
\mu_{13} = 0\,, \quad \mu_{17} \ge -\tfrac{2}{3}\log 17\,, \quad \mu_{15717742643} = 0\,, \quad \mu_\infty \ge -0.6152\,.
\end{gathered}$$

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

$$\begin{gathered}
\mu_2 \ge -\tfrac{10}{3}\log 2\,, \quad \mu_3 \ge -\tfrac{10}{3}\log 3\,, \quad \mu_5 \ge -\tfrac{2}{3}\log 5\,, \quad \mu_7 = 0\,, \\
\mu_{13} = 0\,, \quad \mu_{17} \ge -\tfrac{2}{3}\log 17\,, \quad \mu_{15717742643} = 0\,, \quad \mu_\infty \ge -0.6152\,.
\end{gathered}$$

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

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

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

$$h(2P) \le \hat{h}(2P) + 4.757\,. \tag{11.1}$$

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 $p = 277$: 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 (11.1) 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 11.1. *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:*

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

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

[Magma] 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).

[BMSST] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll and Sz. Tengely: *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 NéronTate 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*, Preprint (2012), arXiv:1211.6900 [math.AG].

[MS] J.S. Müller and M. Stoll: *Canonical heights on genus two Jacobians*, in preparation.

[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`