HOMOGENEOUS SPACES AND DEGREE 4 DEL PEZZO SURFACES

E.V. FLYNN

Abstract. It is known that, given a genus 2 curve $\mathcal{C} : y^2 = f(x)$, where $f(x)$ is quintic and defined over a field K, of characteristic different from 2, and given a homogeneous space $\mathcal{H}_\delta$ for complete 2-descent on the Jacobian of $\mathcal{C}$, there is a V_δ (which we shall describe), which is a degree 4 del Pezzo surface defined over K, such that $\mathcal{H}_\delta(K) \neq \emptyset \implies V_\delta(K) \neq \emptyset$. We shall prove that every degree 4 del Pezzo surface V, defined over K, arises in this way; furthermore, we shall show explicitly how, given V, to find $\mathcal{C}$ and δ such that $V = V_\delta$, up to a linear change in variable defined over K. We shall also apply this relationship to Hürlimann's example of a degree 4 del Pezzo surface violating the Hasse principle, and derive an explicit parametrised infinite family of genus 2 curves, defined over $\mathbb{Q}$, whose Jacobians have nontrivial members of the Shafarevich-Tate group. This example will differ from previous examples in the literature by having only two $\mathbb{Q}$-rational Weierstrass points.

1. Introduction

Consider a curve $\mathcal{C}$ of genus 2 defined over a field K, of characteristic different from 2, with a K-rational Weierstrass point. This can be written in the form

$$\mathcal{C} : y^2 = f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \tag{1}$$

where $f(x) \in K[x]$ is a separable polynomial; furthermore, let $J = \mathrm{Jac}(\mathcal{C})$ be the Jacobian of $\mathcal{C}$. Note that $\mathcal{C}$ has a unique point at infinity, which will be denoted ∞. Following Chapter 1 of [5], any member of $J(K)$ may be represented by a divisor class in $\mathrm{Pic}^0_K(\mathcal{C})$ of the form $[P_1 + P_2 - 2\infty]$, where P_1, P_2 are (not necessarily distinct) points on $\mathcal{C}$ (including ∞) and either P_1, P_2 are both K-rational or P_1, P_2 are quadratic over K and conjugate. For convenience, we shall abbreviate such a divisor class by $\{P_1, P_2\}$. This representation gives a 1-1 correspondence with $J(K)$, except that everything of the form $\{(x, y), (x, -y)\}$ and $\{\infty, \infty\}$ must be identified into a single equivalence class $\mathcal{O}$, which serves as the group identity in $J(K)$. Define $\mathcal{A} = K[x]/(f(x))$; let θ be the image of x in $\mathcal{A}$, so that $\mathcal{A} = K[\theta]$ and $\{1, \theta, \ldots, \theta^4\}$ is a basis of $\mathcal{A}$ as a K-vector space, and define

$$\mathcal{A}' = \mathrm{Ker}(N_{\mathcal{A}/K} : \mathcal{A}^* \to K^*/K^{*2}). \tag{2}$$

Date: 20 March, 2009.

1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.

Key words and phrases. Higher Genus Curves, Jacobians, Visualisation, Brauer-Manin obstruction, Shafarevich-Tate Group.

The author thanks EPSRC for support: grant number EP/F060661/1.

Then (see the introduction of [17] or p.152 of [19]) $H^1(K, J[2]) \simeq \mathcal{A}'/\mathcal{A}^{*2}$ and, making this identification, the coboundary embedding can be given (see Theorem 1.1 of [17]) as

$$\begin{array}{rccc} \mu: & J(K) & \to & H^1(K,J[2]) \\ & \{P_1,P_2\} = \{(x_1,y_1),(x_2,y_2)\} & \mapsto & (x_1-\theta)(x_2-\theta), \end{array} \tag{3}$$

except for the special cases when P_1 or $P_2 = \infty$ or when y_1 or $y_2 = 0$. When $P_i = \infty$, $x_i - \theta$ should be replaced with 1; see Prop. 3.2 of [17] for what $x_i - \theta$ should be replaced with, when $y_i = 0$. Note that $H^1(K, J[2])$ is a standard shorthand notation for $H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), J[2](K^{\mathrm{sep}}))$.

We recall (see Sec III.1 of [18] or 2.11.2 of [15]) that, given a projective variety X over K, and given a Galois extension K'/K, there is a natural map

$$\psi : \{K'/K\text{-twists of } X\}/K\text{-isomorphisms} \to H^1(\mathrm{Gal}(K'/K), \mathrm{Aut}(X_{K'})), \tag{4}$$

where $X_{K'}$ denotes X base-extended to K'. This natural map ψ can be described as follows. If Y is a K'/K-twist of X (which comes together with a K'-isomorphism $f : Y_{K'} \to X_{K'}$) then the corresponding cocycle is $\sigma \mapsto f \circ \sigma(f^{-1})$. It can be shown (see Sec III.1 of [18]) that ψ is bijective.

Now let $\delta \in H^1(K, J[2])$. Note that there is a map $J[2](K^{\mathrm{sep}}) \to \mathrm{Aut}(J_{K^{\mathrm{sep}}})$ which sends P to translation-by-P, and this induces a map from $H^1(K, J[2])$ to $H^1(K, \mathrm{Aut}(J))$; let $\bar{\delta}$ denote the image of δ under this map. Let $\mathcal{H}_\delta$ be a homogeneous space in the isomorphism class that corresponds to δ under ψ. Note that $\mathcal{H}_\delta$ is defined over K and comes together with a K^{sep}-isomorphism $f : \mathcal{H}_\delta \to J$ (where we are using $\mathcal{H}_\delta, J$ as shorthand for their base extensions to K^{sep}). An explicit model for $\mathcal{H}_\delta$ is given in [9] for the case when all Weierstrass points are defined over K.

Assume that there is a point $D \in J(K)$ such that $\mu(D) = \delta$. Then there exists $Q \in J(K^{\mathrm{sep}})$ such that $2Q = D$ and such that $\bar{\delta}$ can be represented by the cocycle: $\sigma \mapsto T_{\sigma(Q)-Q}$, where $T_{\sigma(Q)-Q}$ denotes translation by $\sigma(Q) - Q$. Then $f^{-1}(-Q) \in \mathcal{H}_\delta(K)$. Similarly, any member of $\mathcal{H}_\delta(K)$ gives $D \in J(K)$ such that $\mu(D) = \delta$. It follows that

$$\mathcal{H}_\delta(K) \neq \emptyset \iff \{D \in J(K) : \mu(D) = \delta\} \neq \emptyset. \tag{5}$$

To simplify notation, we shall let $\delta \in \mathcal{A}'$ or $\mathcal{A}^*$ but will also use δ to denote its class in $\mathcal{A}'/\mathcal{A}^{*2}$ or $\mathcal{A}^*/\mathcal{A}^{*2}$, respectively, in expressions such as: $\mathcal{H}_\delta$, $\delta \in \mu(J(K)), \delta = \mu(D)$. The variety V_δ, which we shall shortly define, strictly speaking depends on the choice of representative δ; however, changing δ modulo $\mathcal{A}^{*2}$ only alters V_δ by an invertible linear change of variables over K, and we are ultimately interested (for our main result) only in V_δ modulo invertible linear change of variables over K.

Let $\delta = \delta_0 + \ldots + \delta_4\theta^4 \in \mathcal{A}'$ and suppose that $\mathcal{H}_\delta(K) \neq \emptyset$ so that, by (5), there exists $D = \{(x_1, y_1), (x_2, y_2)\}$ which satisfies $D \in J(K)$ and $\mu(D) = \delta$. Then there exist $u_0, \dots, u_4 \in K$ such that

$$(x_1 - \theta)(x_2 - \theta) = \delta \left(\sum_{i=0}^{4} u_i \theta^i \right)^2 . \tag{6}$$

For $\delta \in \mathcal{A}'$ we define $Q_{\delta,i} \in K[\underline{u}] = K[u_0, \dots, u_4]$ by

$$\delta \left(\sum_{i=0}^{4} u_i \theta^i \right)^2 = \sum_{i=0}^{4} Q_{\delta,i}(\underline{u}) \theta^i .$$

For $\delta \in \mu(J(K))$ there must then be points on the projective variety

$$V_\delta : \left\{ \begin{array}{rcl} Q_{\delta,3}(u_0,u_1,u_2,u_3,u_4) & = & 0, \\ Q_{\delta,4}(u_0,u_1,u_2,u_3,u_4) & = & 0. \end{array} \right. \tag{7}$$

The above gives that $\{D \in J(K) : \mu(D) = \delta\} \neq \emptyset \implies V_\delta(K) \neq \emptyset$. Using (5), this also gives that $\mathcal{H}_\delta(K) \neq \emptyset \implies V_\delta(K) \neq \emptyset$. As we shall soon note, in Lemma 1, V_δ is a smooth intersection of two quadrics in $\mathbb{P}^4$, and so is a degree 4 del Pezzo surface.

In the next section, we shall not need to appeal to any of the structure of J as an abelian variety, and indeed we shall need only think of the above as a map that sends a pair $\mathcal{C}, \delta$ to V_δ. Our main aim will be to show how, given any degree 4 del Pezzo surface V, to find $\mathcal{C}, \delta$ such that V is the same as V_δ (up to linear change in variable); the algorithm in the next section will not require anything of the geometry of $\mathcal{H}_\delta$ or J. For a description of the underlying geometry, see [12],[20] and Lemma 6.1 of [8].

As stated previously, even without mentioning homogeneous spaces the above construction associates to a pair $\mathcal{C}, \delta$, for $\delta \in \mathcal{A}'$, a degree 4 del Pezzo surface V_δ. Note also that this can be extended to any $\delta \in \mathcal{A}^*$; that is, we can define V_δ, as above, derived from $\mathcal{C}, \delta$, for any $\delta \in \mathcal{A}^*$. We recall the following result (Lemma 17 in [3]).

Lemma 1. *Let $\mathcal{C}$ be a curve of genus 2 of the form (1), defined over K, let $\delta \in \mathcal{A}^*$, where $\mathcal{A} = K[\theta] = K[x]/(f(x))$, let V_δ be as in (7), and let $M_{\delta,3}, M_{\delta,4}$ be the symmetric matrices representing the quadrics $Q_{\delta,3}, Q_{\delta,4}$, respectively. Then V_δ is smooth, and so is a degree 4 del Pezzo surface. Furthermore, $\det(xM_{\delta,3} - M_{\delta,4})$, the characteristic polynomial of V_δ, is $f(x)$, up to multiplication by a nonzero constant and invertible linear change in variable.*

Our first aim will be to prove the following converse.

Theorem 2. *Let V be any degree 4 del Pezzo surface, defined over K, given as the smooth intersection of quadrics*

$$V : \left\{ \begin{array}{rcl} G(u_0,u_1,u_2,u_3,u_4) & = & 0, \\ H(u_0,u_1,u_2,u_3,u_4) & = & 0. \end{array} \right. \tag{8}$$

Then there exists a genus 2 curve $\mathcal{C}$ of the form (1), defined over K, and $\delta \in \mathcal{A}^*$ such that V is the V_δ of (7), up to a linear change in variable which is defined over K. Furthermore, there exist such $\mathcal{C}, \delta$ with $\delta \in \mathcal{A}'$, where $\mathcal{A}'$ is as in (2).

We shall first give the following short proof, due to Alexei Skorobogatov (personal communication; see also [20]), and then describe the algorithm in the next section. *Proof* Let K be a field of characteristic not equal to 2 with separable closure $\bar{K}$, and Galois group $\Gamma = \mathrm{Gal}(\bar{K}/K)$. Let V be a del Pezzo surface of degree 4, that is, a smooth intersection of two quadrics in $\mathbb{P}^4_K$. Choose the coordinates in the pencil of quadrics through V so that the characteristic polynomial $f(x) = \prod(x - \theta_i)$, $\theta_i \in \bar{K}$, has degree 5. Then $\mathcal{A} = K[x]/\big(f(x)\big)$ is a 5-dimensional étale K-algebra, that is, $\mathcal{A} = \oplus\, K_j$ for some field extensions K_j/K.

Consider the finite étale abelian group K-scheme (that is, an abelian group with an action of Γ) $G = R_{\mathcal{A}/K}(\mu_2)/\mu_2$, where $R_{\mathcal{A}/K}$ is the Weil restriction of scalars. The abelian group $G(\bar{K}) \cong \big(\mathbb{Z}/2\big)^4$ is generated by five elements of order 2 whose product is the identity. These generators are permuted by Γ in the same way as the θ_i.

Over $\bar{K}$ the quadrics of the pencil can be simultaneously diagonalized (Prop. 2.1 of [16]). More precisely, we can write $\mathbb{P}^4_K = \mathbb{P}\big(R_{\mathcal{A}/K}\mathbb{A}^1_{\mathcal{A}}\big)$, and let u be a variable in $\mathbb{A}^1_{\mathcal{A}}$. For an arbitrary del Pezzo surface V of degree 4 with characteristic polynomial $f(x)$ there exist $\alpha, \beta \in \mathcal{A}^*$ such that V is given by the equations

$$(9) \quad \mathrm{Tr}_{\mathcal{A}/K}\big(\alpha u^2\big) = \mathrm{Tr}_{\mathcal{A}/K}\big(\beta u^2\big) = 0, \text{ or, equivalently, } \sum_{i=0}^{4} \alpha_i v_i^2 = \sum_{i=0}^{4} \beta_i v_i^2 = 0,$$

where $(\alpha_i) \in (\bar{K})^5$ is the image of α in $\mathcal{A} \otimes_K \bar{K} = (\bar{K})^5$, and similarly for β. Here Γ acts on the α_i, the β_i and the $\bar{K}$-coordinates v_i in the same way it acts on the θ_i. We have $\theta_i = \alpha_i^{-1}\beta_i$, hence $\theta = \alpha^{-1}\beta \in \mathcal{A}^*$. The K-group G acts on $\mathbb{P}^4_K$ by changing the signs of x_i, so G leaves invariant every quadric that contains V, and thus preserves V.

From (9) it is clear that the natural morphism $V \to V/G$ sends u to u^2, so that V/G is a subset of $\mathbb{P}^4_K = \mathbb{P}\big(R_{\mathcal{A}/K}\mathbb{A}^1_{\mathcal{A}}\big)$ with $\mathcal{A}$-coordinate $w = u^2$, given by

$$(10) \qquad \mathrm{Tr}_{\mathcal{A}/K}(\alpha w) = \mathrm{Tr}_{\mathcal{A}/K}(\alpha\theta w) = 0.$$

In particular, $V/G \cong \mathbb{P}^2_K$. The linear span $\mathcal{L}$ of $1, \theta, \theta^2, \theta^3$ in the vector space $\mathcal{A}$ over K has codimension 1, hence up to a constant from K^* there is a unique $\delta \in \mathcal{A}^*$ such that $\mathrm{Tr}_{\mathcal{A}/K}(\alpha\delta^{-1}\ell) = 0$ for any $\ell \in \mathcal{L}$. Then the 3-dimensional subspace of $R_{\mathcal{A}/K}\mathbb{A}^1_{\mathcal{A}}$ given by (10) is spanned by $\delta^{-1}, \delta^{-1}\theta, \delta^{-1}\theta^2$, that is, we can write $w = \delta^{-1}(t_0 + t_1\theta + t_2\theta^2)$, where t_0, t_1, t_2 are coordinates over K. Therefore, V is given by the vanishing of the θ^3 and θ^4 terms in

$$(11) \qquad t_0 + t_1\theta + t_2\theta^2 = \delta u^2 = \delta\Big(\sum_{i=0}^{4} u_i\theta^i\Big)^2,$$

which is equivalent to (6). Now let $\mathcal{C}$ be the curve of genus two given by $y^2 = f(x)$; then V is defined by $\mathcal{C}$ and δ as in the statement of the theorem. Thus all del Pezzo surfaces of degree 4 are obtained in this way.

It only remains to show that we can choose $\delta \in \mathcal{A}'$. Note that replacing δ with $k\delta$, for any $k \in K$, does not affect V_δ; in particular, we can take $k = N_{\mathcal{A}/K}(\delta)$, so that $N_{\mathcal{A}/K}(k\delta) = k^6$, giving $k\delta \in A'$, as required. □

Our aim in the next section will be to provide an explicit and straightforward route from any such V to $\mathcal{C}, \delta$; this will ease the work of others who wish to use the literature on degree 4 del Pezzo surfaces and apply it to Shafarevich-Tate groups of Jacobians. To illustrate this, we shall then consider an example of Hürlimann (given in [10] and Example 15.7 of [7]), and derive an explicit parametrised infinite family of genus 2 curves, defined over $\mathbb{Q}$, whose Jacobians have nontrivial members of the Shafarevich-Tate group.

2. Deriving $\mathcal{C}$ and δ from the Degree 4 del Pezzo Surface

Given V as in (8), a degree 4 del Pezzo surface defined over K, we know from Lemma 1 that when V does arise as claimed in Theorem 2 then we should use the curve $\mathcal{C} : y^2 = f(x)$, where $f(x)$ is the characteristic polynomial of V. We shall describe in this section an algorithm to derive both $\mathcal{C}$ and δ; note that this section also provides an independent proof of Theorem 2.

The defining equations for V might not immediately be in the form V_δ for a given $\mathcal{C}, \delta$; it might first be necessary to change variables and change defining equations. Our strategy is fairly straightforward; given V, we first change variables over a field extension L so that the defining equations are simultaneously diagonalised; we then show $\mathcal{C}, \delta$ exist over L; we then change variables again to force $\mathcal{C}, \delta$ to be defined over K; finally we force $\delta \in \mathcal{A}'$, rather than merely $\mathcal{A}^*$. There will be a small amount of finesse here; the standard proof of simultaneous diagonalisability of two symmetric matrices uses orthonormal changes of basis, which require unnecessary field extensions. We shall instead use a initial change of basis over K so that one of the matrices is diagonalised, and then use only the splitting field of $f(x)$ to perform the simultaneous diagonalisation. It will then be clear how to perform a further change of variable to obtain $\mathcal{C}, \delta$ which are defined over K. We first see, given $\mathcal{C}, \delta$, how V_δ appears when diagonalised (see also the proof of Lemma 17 in [3]).

Lemma 3. *Let $\mathcal{C} : y^2 = f(x), K, \delta \in \mathcal{A}^*, V_\delta, Q_{\delta,3}, Q_{\delta,4}, M_{\delta,3}, M_{\delta,4}$ be as in Lemma 1. Let L be the splitting field of the quintic $f(x)$, and let $f(x) = (x - \theta_0) \dots (x - \theta_4)$, where all $\theta_i \in L$. Then a linear change of variable over L, from $u_0, \dots, u_4$ to $v_0, \dots, v_4$, makes V_δ of (7) become:*

$$\sum_{i=0}^{4} d_i v_i^2 / E_i = \sum_{i=0}^{4} d_i \theta_i v_i^2 / E_i = 0, \tag{12}$$

where each $E_i = \prod_{j \neq i}(\theta_i - \theta_j)$ *and each* $d_i = \delta_0 + \delta_1\theta_i + \ldots + \delta_4\theta_i^4$*, for* $i = 0, \ldots, 4$*.*

Note that (12) is the same as (9), with $\alpha_i = d_i/E_i$, $\beta_i = d_i\theta_i/E_i$.

Proof Let N denote the 5×5 Van der Monde matrix (θ_j^i), that is,

$$N = \begin{pmatrix} \theta_0^0 & \theta_1^0 & \theta_2^0 & \theta_3^0 & \theta_4^0 \\ \theta_0^1 & \theta_1^1 & \theta_2^1 & \theta_3^1 & \theta_4^1 \\ \theta_0^2 & \theta_1^2 & \theta_2^2 & \theta_3^2 & \theta_4^2 \\ \theta_0^3 & \theta_1^3 & \theta_2^3 & \theta_3^3 & \theta_4^3 \\ \theta_0^4 & \theta_1^4 & \theta_2^4 & \theta_3^4 & \theta_4^4 \end{pmatrix}, \tag{13}$$

so that $(d_0, \ldots, d_4) = (\delta_0, \ldots, \delta_4)N$, and define v_i by $(v_0, \ldots, v_4) = (u_0, \ldots, u_4)N$, for $i = 0, \ldots 4$. This linear change in variable (defined over L) puts the two defining equations for V_δ into the required form. □

The following proves our desired direction, from V to $\mathcal{C}, \delta$ for the special case when we are given defining equations of V which are both diagonal.

Lemma 4. *Let* V *be a degree 4 del Pezzo surface, defined by* G, H*, as in (8), and suppose that* G, H *are both diagonal and defined over some field* L*, of characteristic different from 2. Then* V *is, up to a linear change in variable defined over* L*, the same as* V_δ *of (7) for some* $\mathcal{C} : y^2 = f(x)$*, where* $f(x)$ *is quintic in* x *and defined over* L*, and some* $\delta = \delta_0 + \ldots + \delta_4\theta^4 \in L[\theta]^*$*, with* $\delta_0, \ldots, \delta_4 \in L$*.*

Proof Let $G(\underline{u}) = g_0u_0^2 + \ldots + g_4u_4^2$ and $H(\underline{u}) = h_0u_0^2 + \ldots + h_4u_4^2$ be the diagonal defining equations of V. Since V is nonsingular, we can arrange that all $g_i \neq 0$. For $i = 0, \ldots, 4$, let $\theta_i = h_i/g_i$, let d_i denote g_iE_i where $E_i = \prod_{j \neq i}(\theta_i - \theta_j)$, and define δ_i by: $(\delta_0, \ldots, \delta_4) = (d_0, \ldots, d_4)N^{-1}$ where, as usual, N is the 5×5 Van der Monde matrix (θ_j^i), as in (13). It now follows from Lemma 3 that the given V is (up to a linear change in variable defined over L) the V_δ of (7) for the curve $\mathcal{C} : y^2 = f(x) = (x - \theta_0)\ldots(x - \theta_4)$ and $\delta = \delta_0 + \ldots + \delta_4\theta^4$. □

We are now in a position to describe our algorithm for any degree 4 del Pezzo surface; the following gives explicitly the steps which derive $\mathcal{C}, \delta$ from V.

Description of the algorithm. Let V be any degree 4 del Pezzo surface, given as the smooth intersection of quadrics G, H in (8), each defined over K, represented by the symmetric matrices A_0, B_0, respectively.

Step 1. First check that A_0 has nonzero determinant; if not, then replace A_0 by some $A_0 + kB_0$ with nonzero determinant for some $k \in K$ (which must exist, by the nonsingularity of V). Now perform a congruence diagonalisation of A_0 (see Algorithm 12.1 on p.379 of [13]), in which one forms $(A_0|I)$ and applies at each stage both a row operation and its corresponding column operation to the left hand matrix, with only the column operation applied to the right hand matrix, until we obtain $(A|P)$, with A diagonal. This gives $A = P^TA_0P$; the method guarantees a change of basis which is defined over K. Also define $B = P^TB_0P$, which is symmetric.

Step 2. Let $\theta_0, \ldots, \theta_4$ be the eigenvalues of $A^{-1}B$, with corresponding eigenvectors $z_0, \ldots, z_4$ (in column form) chosen so that $\{(\theta_i, z_i) : i = 0, \ldots, 4\}$ is invariant under the action of the Galois group. Note that the nonsingularity of V guarantees that $\theta_0, \ldots, \theta_4$ are distinct and so $z_0, \ldots, z_4$ are linearly independent. Let Q be the 5×5 matrix $(z_0 \ldots z_4)$, let D_1 be the 5×5 diagonal matrix with diagonal entries $\theta_0, \ldots, \theta_4$, and let D_2 be the diagonal matrix with diagonal entries $z_0^T A z_0, \ldots, z_4^T A z_4$. Fix A_1 to be any choice of diagonal matrix such that $A_1^2 = A^{-1}$. The $A_1^{-1} z_i$, for $i = 0, \ldots, 4$, are the eigenvectors of the symmetric matrix $A_1 B A_1$. Then $(PQ)^T A_0 (PQ) = Q^T A Q = (A_1^{-1} Q)^T (A_1^{-1} Q) = D_2$ and $(PQ)^T B_0 (PQ) = Q^T B Q = D_2 D_1$ are simultaneously diagonal, and are defined over L, the splitting field of $\det(xA - B)$; in particular, the field of definition of A_1 is not required.

Step 3. Now apply Lemma 4 to our diagonalised pair $(PQ)^T A_0 (PQ) = D_2$ and $(PQ)^T B_0 (PQ) = D_2 D_1$, defined over L. Following the proof of Lemma 4, for $i = 0, \ldots 4$ define N as usual to be the Van der Monde matrix (θ_j^i) as in (13), and define

$$M = PQN^T, \quad f(x) = \det(xI - A^{-1}B) = \prod_{i=0}^{4} (x - \theta_i),$$

$$d_i = (z_i^T A z_i) \prod_{j \neq i} (\theta_i - \theta_j), \quad (\delta_0, \ldots, \delta_4) = (d_0, \ldots, d_4) N^{-1}, \quad \delta = \delta_0 + \ldots + \delta_4 \theta^4.$$

Then $f(x), M$ and all δ_i are symmetric in $\theta_0, \ldots, \theta_4$ and so are defined over K (the original field of definition of A_0, B_0), and it follows from Lemma 4 that $M^T B_0 M$, $M^T A_0 M$ give the V_δ for $y^2 = f(x)$ and $\delta \in \mathcal{A}^*$, as required.

As already mentioned, we can finally take $k = N_{\mathcal{A}/K}(\delta)$, so that $N_{\mathcal{A}/K}(k\delta) = k^6$, giving $k\delta \in A'$, as required. □

When $f(x)$ is an irreducible quintic, one should leave the θ_i as variables; the above steps will then give the δ_i as symmetric polynomials in the θ_i, which will then be polynomials in the coefficients of $f(x)$.

Suppose that $\mathcal{C} : y^2 = f(x)$, δ and $\mathcal{C}' : y^2 = g(x)$, δ' give the same del Pezzo surface (up to K-rational linear change of variable), where $f(x), g(x)$ are quintic and defined over K. Then it can be checked that these are related by $g(x) = \ell(cx + d)^5 f\big(\phi(x)\big)$, where $\ell \in K^*$ and $\phi(x) = (ax + b)/(cx + d)$ is an invertible fractional linear transformation, defined over K, and δ' is the image of δ under the isomorphism from $K[x]/\big(f(x)\big)$ to $K[x]/\big(g(x)\big)$ induced by $x \mapsto \phi(x)$. That is to say, if $K[\theta] = K[x]/\big(f(x)\big)$ and $K[\theta'] = K[x]/\big(g(x)\big)$ then $\delta = \delta_0 + \delta_1\theta + \ldots + \delta_4\theta^4$ maps to $\delta' = \delta_0 + \delta_1\phi(\theta') + \ldots + \delta_4\phi(\theta')^4$.

Note that the above description includes, up to birational equivalence, the curves in sextic form $y^2 = \ell(x - s)f(x)$, for any $\ell \in K^*$, $s \in K$ such that $f(s) \neq 0$; these are birationally equivalent to $y^2 = \ell x^5 f\big((sx+1)/x\big)$. Different values of $\ell \in K$ give quadratic twists (geometrically the same curve), whereas different values of $s \in K$ can give geometrically distinct curves.

3. Worked Examples and a Family of $\text{Ш}(J/Q)[2]$

As motivation, we first give the following result from [10] (see also Example 15.7 of [7]).

Lemma 5. *The Hasse principle is violated by the following degree* 4 *del Pezzo surface, defined over* $\mathbb{Q}$*:*

$$u_0^2 - 17u_1^2 + 386u_2^2 - 34u_3^2 - 3u_4^2 = 0, \qquad u_0u_2 - 17u_1u_3 = 0. \tag{14}$$ □

For other examples, due to the Brauer-Manin obstruction, see [1],[11]. The first equation is already in diagonal form, so that Step 1 is not required. Letting A, B denote the symmetric matrices for these equations, we apply Step 2 and note that $A^{-1}B$ has characteristic equation $f(x) = (x^2-1/1544)(x^2-1/8)x$ with eigenvalues $\theta_0 = 1/(2\sqrt{386}), \theta_1 = 1/(2\sqrt{2}), \theta_2 = -1/(2\sqrt{386}), \theta_3 = -1/(2\sqrt{2}), \theta_4 = 0$; we use corresponding eigenvectors $z_0 = (1,0,1/\sqrt{386},0,0)^T, z_1 = (0,1,0,1/\sqrt{2},0)^T$, $z_2 = (1,0,-1/\sqrt{386},0,0)^T, z_3 = (0,1,0,-1/\sqrt{2},0)^T, z_4 = (0,0,0,0,1)^T$. After substituting $u_0 = v_0+v_2, u_2 = (v_0-v_2)/\sqrt{386}, u_1 = v_1+v_3, u_3 = (v_1-v_3)/\sqrt{2}, u_4 = v_4$, we obtain the following simultaneous diagonalisation, defined over the splitting field of $f(x)$.

$$\begin{array}{l} 2v_0^2 + 2v_2^2 - 34v_1^2 - 34v_3^2 - 3v_4^2 = 0, \\ (1/\sqrt{386})v_0^2 - (1/\sqrt{386})v_2^2 - (17/\sqrt{2})v_1^2 + (17/\sqrt{2})v_3^2 = 0. \end{array} \tag{15}$$

Applying Step 3, the d_i are: $d_0 = -12/37249, d_1 = -204/193, d_2 = -12/37249, d_3 = -204/193, d_4 = -3/12352$, and computing $(\delta_0,\ldots,\delta_4) = (d_0,\ldots,d_4)N^{-1}$, where $N = (\theta_j^i)$ as in (13), gives

$$\underline{\delta} = -\frac{3}{12352} + \frac{60456960}{37249}\theta + \frac{697228131}{148996}\theta^2 - \frac{93373857792}{37249}\theta^3 - \frac{280065062019}{37249}\theta^4.$$

This is not in $\mathcal{A}'$, as $N_{\mathcal{A}/K}(\underline{\delta}) = -579$ modulo squares; so we take instead $\delta = -579\,\underline{\delta} \in \mathcal{A}'$, which gives the same V_δ. We now have $y^2 = (x^2-1/1544)(x^2-1/8)x$ and δ for which the example in (14) arises as V_δ. Furthermore, the same V_δ will arise from $y^2 = (x^2-1/1544)(x^2-1/8)x(x-s)$, for any $s \in \mathbb{Q}^*$. Replacing (x,y) with $(1/2x, y/8x^3)$, letting $t = 1/s \in \mathbb{Q}^*$, and noting that V_δ is unaffected by multiplying the quintic by a member of $\mathbb{Q}^*$, we see that we can take instead the curve

$$y^2 = F_{\ell,t}(X) = \ell(x^2-386)(x^2-2)(x-t).$$

Note that $\mathcal{A} = \mathbb{Q}[\theta] \simeq \mathbb{Q}(\sqrt{386}) \times \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}$. In this representation we obtain, for $\{(x_1,y_1),(x_2,y_2)\} \in J(\mathbb{Q})$,

$$\begin{array}{ll} \mu: & \{(x_1,y_1),(x_2,y_2)\} \\ & \mapsto [(x_1-\sqrt{386})(x_2-\sqrt{386}),\ (x_1-\sqrt{2})(x_2-\sqrt{2}),\ (x_1-t)(x_2-t)]. \end{array} \tag{16}$$

Using this representation, we can take $\delta = [193, 17, 1]$, giving the following result.

Lemma 6. *Let $\mathcal{C}_{\ell,t} : Y^2 = F_{\ell,t}(x)$, with Jacobian $J_{\ell,t}$, and δ be given by*

$$Y^2 = F_{\ell,t}(x) = \ell(x^2 - 386)(x^2 - 2)(x - t), \quad \delta = [193, 17, 1] \in \mathcal{A}'. \tag{17}$$

Let μ be as defined in (16). Then $\delta \notin \operatorname{im} \mu = \mu\big(J_{\ell,t}(\mathbb{Q})\big)$.

Proof The existence of $D \in J_{\ell,t}(\mathbb{Q})$ such that $\mu(D) = \delta$ would imply $V_\delta(\mathbb{Q}) \neq \emptyset$. However, as we have seen, this would give a $\mathbb{Q}$-rational point on (14) which we know to be impossible from Lemma 5. Hence $\delta \notin \operatorname{im} \mu$. □

This means that $\delta \in \text{Ш}(J_{\ell,t}/\mathbb{Q})[2]$ precisely when, for all primes p of bad reduction, at least one of the local solutions to V_δ lifts to a local solution of $\mathcal{H}_\delta$. For example, this happens when $\ell = 17, t = 1/3$.

Lemma 7. *Let $\mathcal{C}_{17,\frac{1}{3}}$ and δ be as in Lemma 6 with $\ell = 17, t = 1/3$:*

$$\mathcal{C}_{17,\frac{1}{3}} : y^2 = F_{17,\frac{1}{3}}(x) = 17\Big(x^2 - 386\Big)\Big(x^2 - 2\Big)\Big(x - \frac{1}{3}\Big), \quad \delta = [193, 17, 1].$$

Then $\delta \in \text{Ш}(J_{17,\frac{1}{3}}/\mathbb{Q})[2]$.

Proof We first show that $\delta \in S^{(2)}(J_{17,\frac{1}{3}}/\mathbb{Q})$, the 2-Selmer group, equivalent to $\mathcal{H}_\delta$ having points every locally. It is sufficient to check the primes of bad reduction $p = 2, 3, 17, 23, 151, 193, \infty$. For any prime p, let $\mu_p : J_{17,\frac{1}{3}}(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, J_{17,\frac{1}{3}}[2])$ denote the map of (3), with K replaced by $\mathbb{Q}_p$; also let q_p denote the natural injection $q_p : H^1(\mathbb{Q}, J_{17,\frac{1}{3}}[2]) \to H^1(\mathbb{Q}_p, J_{17,\frac{1}{3}}[2])$. Rather than writing out the equations of $\mathcal{H}_\delta$ explicitly, a simpler approach is to check, for each p, that there exists $D_p \in J_{17,\frac{1}{3}}(\mathbb{Q}_p)$ such that $\mu_p(D_p) = q_p(\delta)$. For $p = 2, 3, 151, \infty$, we can take D_p to be the identity $\mathcal{O}$. For $p = 17$, take $D_{17} = \{(-s_{17}, 0), (1/3, 0)\} \in J_{17,\frac{1}{3}}(\mathbb{Q}_{17})$, where $s_{17} \in \mathbb{Q}_{17}$ satisfies $s_{17}^2 = 2, s_{17} \equiv 6 \pmod{17}$. For $p = 23$, take $D_{23} = \{(s_{23}, 0), (4, \beta)\}$ where $s_{23} \in \mathbb{Q}_{23}$ satisfies $s_{23}^2 = 2, s_{23} \equiv 5 \pmod{23}$ and $\beta \in \mathbb{Q}_{23}$ satisfies $\beta^2 = F_{17,\frac{1}{3}}(4) = -968660/3$. For $p = 193$, take $D_{193} = \{(s_{193}, 0), (10, \gamma)\}$ where $s_{193} \in \mathbb{Q}_{193}$ satisfies $s_{193}^2 = 2, s_{193} \equiv 52 \pmod{193}$ and $\gamma \in \mathbb{Q}_{193}$ satisfies $\gamma^2 = F_{17,\frac{1}{3}}(10) = -13817804/3$. All of these satisfy $\mu_p(D_p) = q_p(\delta)$, so that $\delta = [193, 17, 1] \in S^{(2)}(J_{17,\frac{1}{3}}/\mathbb{Q})$. Furthermore, we already know, from Lemma 6, that $\delta \notin \operatorname{im} \mu$, so that $\delta \in \text{Ш}(J_{17,\frac{1}{3}}/\mathbb{Q})[2]$, as required. □

This gives rise to the following infinite family of Jacobians with Ш[2].

Lemma 8. *Let $\mathcal{C}_{\ell,t} : y^2 = \ell(x^2 - 386)(x^2 - 2)(x - t)$, and let $J_{\ell,t}$ be the Jacobian of $\mathcal{C}_{\ell,t}$. Let $S = \{2, 3, 17, 23, 151, 193, \infty\}$. There exists a nontrivial member of $\text{Ш}(J_{17k,\frac{1}{3}}/\mathbb{Q})[2]$ when $k \in \mathbb{Q}^*$ satisfies:*

- *(i) For all primes $q \notin S$, such that $v_q(k)$ is odd: $\left(\frac{193}{q}\right) = \left(\frac{17}{q}\right) = 1$.*
- *(ii) For all $p \in S$, $k \in (\mathbb{Q}_p^*)^2$. [including $k > 0$ from $p = \infty$].*

Proof From Lemma 6, we have that $\delta = [193, 17, 1] \notin \operatorname{im} \mu$ for any k and, from Lemma 7, that $\delta \in S^{(2)}(J_{17k,\frac{1}{3}}/\mathbb{Q})$ when $k = 1$. It is therefore only necessary to choose k so that $\mathcal{H}_\delta$ continues to have solutions at members of S, and at any new bad primes introduced by k. Since the map μ is only affected by translating some entries multiplicatively by k, the above conditions on k are sufficient. □

Note that, when $k = q$ prime, (i),(ii) are equivalent to a congruence condition on q, which immediately gives infinitely many such k (and indeed k can be taken to be any product of distinct such primes). For curves of this form there is also the available alternative of trying to show the existence of members of $Ш(J_{17k,\frac{1}{3}}/\mathbb{Q})[2]$ by finding the curve $\mathcal{D}_{17k,\frac{1}{3}}$ with Richelot isogenous Jacobian (see [2]), when there might be a difference between the 2-Selmer bounds on the ranks of the Mordell-Weil groups of the Jacobians of $\mathcal{C}_{17k,\frac{1}{3}}$ and $\mathcal{D}_{17k,\frac{1}{3}}$. We find that this applies to the case $k = 1$ in the above family; however, it does not apply to the case $k = 577$, when there exist nontrivial members of $Ш[2]$ on both Jacobians.

We can now find a parametrised family of curves $y^2 = F_{17k,\frac{1}{3}}(x)$ all of which are guaranteed to contain a nontrivial member of $Ш(J_{17k,\frac{1}{3}}/\mathbb{Q})[2]$. The following example is the first using this method to have only two Weierstrass points (whereas the examples in [3],[4] have three Weierstrass points; see also the examples in [6],[12],[14]).

Proposition 9. *Let* $\mathcal{C}_{\ell,t} : y^2 = \ell(x^2 - 386)(x^2 - 2)(x - t)$ *and let* $J_{\ell,t}$ *be the Jacobian of* $\mathcal{C}_{\ell,t}$. *There exists a nontrivial member of* $Ш(J_{17k,\frac{1}{3}}/\mathbb{Q})[2]$ *for any* k *of the form*

$$k = (w^m - w + 1)^8 + 105N(w^m - w + 1)^6 + 2064N^2(w^m - w + 1)^4 + 6720N^3(w^m - w + 1)^2 + 4096N^4, \tag{18}$$

for any $w \in \mathbb{Q}$, *where* $N = 8 \cdot 3 \cdot 17 \cdot 23 \cdot 151 \cdot 193 = 273477912$ *and* $m = 52801$. *Furthermore,* $J_{17k,\frac{1}{3}}$ *is absolutely simple.*

Proof From Lemma 8, it is sufficient to show that k satisfies conditions (i),(ii). For reasons which soon will become apparent, we first parametrise $r^2 = s^2 - 176$, using $r_0 = 7, s_0 = 15$ as a basepoint. This gives: $r(z) = (7z^2 - 30z + 7)/(z^2 - 1)$ and $s(z) = (15z^2 - 14z + 15)/(z^2 - 1)$. Now take:

$$k = \big((7z^2 - 30z + 7)^2 - 17(z^2 - 1)^2\big)/2 = 16z^4 - 210z^3 + 516z^2 - 210z + 16. \tag{19}$$

Note that $k > 0$ as long as $z < 0$. Suppose q is prime, not in S, such that $v_q(k)$ is odd. Then $v_q(z) \geq 0$ (since if $v_q(z) < 0$ then $v_q(16z^4) < v_q(210z^3), v_q(516z^2), v_q(210z), v_q(16)$ and so, by (19), $v_q(k) = v_q(16z^4) = 4v_q(2z)$, giving $4|v_q(k)$, a contradiction). Now, $v_q(z^2 - 1) = v_q(7z^2 - 30z + 7)$, since otherwise $v_q(k)$ would be even; say that $r = v_q(z^2 - 1) = v_q(7z^2 - 30z + 7)$. Then $v_q(k) \geq 2r$ and so $v_q(k) \geq 2r + 1$, since $v_q(k)$ is odd. So, $17 \equiv ((7z^2 - 30z + 7)/(z^2 - 1))^2 \pmod q$, giving $\left(\frac{17}{q}\right) = 1$. Also,

$$193 = 17 + 176 \equiv \left(\frac{7z^2 - 30z + 7}{z^2 - 1}\right)^2 + 176 = \left(\frac{15z^2 - 14z + 15}{z^2 - 1}\right)^2,$$

giving $\left(\frac{193}{q}\right) = 1$, so that any k in (19) satisfies (i) in Lemma 8. For (ii), it is sufficient that $z < 0$ (so that $k > 0$), $z \in p\mathbb{Z}_p$ for all $p \in S\backslash\{2\}$ (so that, from (19), $k \in \mathbb{Z}_p^*$ and $k \equiv 16 \bmod p$, giving $k \in (\mathbb{Q}_p^*)^2$), and $z \in 64\mathbb{Z}_2$ (so that $k = 16k'$, where $k' \in \mathbb{Z}_2^*$ and $k' \equiv 1 \pmod 8$, giving $k \in (\mathbb{Q}_2^*)^2$). It is sufficient to take $z = -64 \cdot 3 \cdot 17 \cdot 23 \cdot 151 \cdot 193 \cdot u^2$, as long as $u \in \mathbb{Z}_p$ for all $p \in S$. It is then sufficient to take $u = 1/(w^m - w + 1)$, where $m = 52801$, which is obtained by taking the smallest integer $m > 1$ satisfying $m \equiv 1 \pmod{p-1}$, for all $p \in S$, that is to say: $m = 1 + \mathrm{lcm}(2-1, 3-1, 17-1, 23-1, 151-1, 193-1) = 52801$. Substituting these into (19) and multiplying by $\frac{1}{4}(w^m - w + 1)^8 \in (\mathbb{Q}^*)^2$ gives (18), as required.

The fact that $J_{17k,\frac{1}{3}}$ is absolutely simple can be shown, using the method in [21] (also described on p.158 of [5]) at $p = 29$. □

The author thanks Ronald van Luijk, Ed Schaefer, Alexei Skorobogatov and Damiano Testa for helpful discussions.

References

[1] B.J. Birch and H.P.F. Swinnerton-Dyer. The Hasse problem for rational surfaces. *J. Reine Angew. Math.*, 274/275:164–174, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.

[2] J–B. Bost and J–F. Mestre. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math.*, 38:36–64, 1988.

[3] M.J. Bright, N. Bruin, E.V. Flynn and A. Logan. The Brauer–Manin Obstruction and Ш[2] *LMS J. Comput. Math.*, 10:1–24, 2007.

[4] N. Bruin and E.V. Flynn. Exhibiting SHA[2] on hyperelliptic Jacobians. *J. Number Theory.*, 118:266–291, 2006.

[5] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[6] J–L. Colliot-Thélène and B. Poonen. Algebraic families of nonzero elements of Shafarevich-Tate groups. *J. Amer. Math. Soc.*, 13(1):83–99, 2000.

[7] J–L. Colliot-Thélène, J–J. Sansuc, and P. Swinnerton-Dyer. Intersections of two quadrics and Châtelet surfaces. II. *J. Reine Angew. Math.*, 374:72–168, 1987.

[8] P. Corn. Tate-Shafarevich groups and K3 surfaces. arXiv: 0711.4436.

[9] D.M. Gordon and D. Grant. Computing the Mordell-Weil rank of Jacobians of curves of genus 2. *Trans. Amer. Math. Soc.*, 337:807–824, 1993.

[10] W. Hürlimann. Brauer group and Diophantine geometry: a cohomological approach. In *Brauer groups in ring theory and algebraic geometry (Wilrijk, 1981)*, volume 917 of *Lecture Notes in Math.*, pages 43–65. Springer, Berlin, 1982.

[11] V.A. Iskovskih. A counterexample to the Hasse principle for systems of two quadratic forms in five variables. *Mat. Zametki*, 10:253–257, 1971.

[12] A. Logan and R. van Luijk. Nontrivial elements of Sha explained through K3 surfaces. *Math. Comp.* 78:441–483, 2009.

[13] S. Lipschutz and M. Lipson. *Linear Algebra*, Third Edition. McGraw-Hill, 2001.

[14] B. Poonen. An explicit algebraic family of genus-one curves violating the Hasse principle. *J. Théor. Nombres Bordeaux*, 13(1):263–274, 2001. 21st Journées Arithmétiques (Rome, 2001).

[15] B. Poonen. *Rational points on varieties,* 2003. Available at:
http://math.berkeley.edu/~poonen/papers/Qpoints.pdf

[16] M. Reid. *The complete intersection of two or more quadrics,* Cambridge PhD Thesis, 1972. Available at:
http://www.warwick.ac.uk/~masda/3folds/qu.pdf

[17] E.F. Schaefer. 2-Descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51:219–232, 1995.

[18] J.P. Serre. *Galois Cohomology.* Springer-Verlag, New York, 1972.

[19] J.P. Serre. *Local Fields.* Springer-Verlag, New York, 1979.

[20] A. Skorobogatov. Del Pezzo surfaces of degree 4 and their relation to Kummer surfaces. http://www.ma.imperial.ac.uk/~anskor/DP4.PDF

[21] M. Stoll. Two simple 2-dimensional abelian varieties defined over **Q** with Mordell-Weil group of rank at least 19. *C. R. Acad. Sci. Paris Sér. I Math.*, 321(10):1341–1345, 1995.

Mathematical Institute, University of Oxford, 24–29 St. Giles, Oxford OX1 3LB, United Kingdom

E-mail address: `flynn@maths.ox.ac.uk`