TATE-SHAFAREVICH GROUPS AND $K3$ SURFACES

PATRICK CORN

ABSTRACT. This paper explores a topic taken up recently by Logan and van Luijk, finding nontrivial 2-torsion elements of the Tate-Shafarevich group of the Jacobian of a genus-2 curve by exhibiting Brauer-Manin obstructions to rational points on certain quotients of principal homogeneous spaces of the Jacobian, whose desingularizations are explicit $K3$ surfaces. The main difference between the methods used in this paper and those of Logan and van Luijk is that the obstructions are obtained here from explicitly constructed quaternion algebras, rather than elliptic fibrations.

1. INTRODUCTION

Let C be a curve of genus 2 over a number field k, with Jacobian J. In an effort to describe the (finite) set $C(k)$, we are led to the study of $J(k)$. To determine its rank, we refer to a well-known exact sequence

$$(1) \qquad 0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(k, J) \to \text{Ш}(k, J)[2] \to 0,$$

where the middle group is effectively computable. See [17] for a comprehensive description of the computation, which has been implemented in the computer algebra system MAGMA ([2]).

So computing the group on the left is more or less equivalent to computing the rather mysterious group on the right. In this paper, we find examples of curves C over $\mathbb{Q}$ such that $\text{Ш}(\mathbb{Q}, J)[2]$ is nonzero, by finding explicit elements of this group. Such elements can be represented by 2-coverings X of J which have points everywhere locally but no k-points. The strategy, as in [12], is to prove that the Hasse principle fails for X by exhibiting a Brauer-Manin obstruction to rational points on the desingularization of the quotient X/ι, where ι is the involution on X corresponding to multiplication by -1 on J. This desingularization is a $K3$ surface which can be given explicitly as the smooth complete intersection of 3 quadrics in $\mathbb{P}^5$.

The result is the following theorem.

Theorem 1.1. *Let S be the set of primes splitting completely in a certain finite extension $K/\mathbb{Q}$ (this extension is given explicitly in the statement of Proposition 5.3). For all n equal to the product of primes in S, the genus-2 curve*

$$C_n \colon y^2 = n(x^2 - 5x + 1)(x^3 - 7x + 10)(x + 1)$$

satisfies $\text{Ш}(\mathbb{Q}, \mathrm{Jac}(C))[2] \neq 0$.

The curve with $n = 1$ was originally obtained by a computer search over products of polynomials of degrees $2, 3, 1$ with small coefficients.

I thank Ronald van Luijk for introducing me to this topic and for many helpful conversations. I would also like to thank Bjorn Poonen for several enlightening comments, and in particular for the method of computing problematic smooth places outlined in the proof of the main theorem. Finally I thank the anonymous referee for his thoughtful comments and suggestions.

2. THE BRAUER-MANIN OBSTRUCTION

2.1. **Generalities.** First we briefly review the Brauer-Manin obstruction to the Hasse principle. Let V be a smooth proper k-variety, k a number field. Then the map $V(\mathbb{A}_k) \to \prod_v V(k_v)$ is a bijection ([16], pp. 98-99). We will suppose that this set $V(\mathbb{A}_k)$ is nonempty.

For any scheme V we can define the *Brauer group* $\operatorname{Br} V = H^2(V_{\mathrm{et}}, \mathbb{G}_m)$. If $P_v \in V(k_v)$, functoriality gives an evaluation map $\operatorname{Br} V \to \operatorname{Br} k_v$; it is natural to denote the image of an element $\mathcal{A} \in \operatorname{Br} V$ by $\mathcal{A}(P_v)$. For an element $\mathcal{A} \in \operatorname{Br} V$, define the set

$$V(\mathbb{A}_k)^{\mathcal{A}} = \{(P_v) \in V(\mathbb{A}_k) : \sum_v \operatorname{inv}_v \mathcal{A}(P_v) = 0\},$$

where the sum is over all places v of k, and define

$$(2) \qquad V(\mathbb{A}_k)^{\mathrm{Br}} = \bigcap_{\mathcal{A} \in \operatorname{Br} V} V(\mathbb{A}_k)^{\mathcal{A}}.$$

Here $\operatorname{inv}_v \colon \operatorname{Br} k_v \to \mathbb{Q}/\mathbb{Z}$ is an isomorphism if v is non-Archimedean, or the injection $\frac{1}{2}\mathbb{Z}/Z \to \mathbb{Q}/\mathbb{Z}$ if $k_v = \mathbb{R}$, or the zero map if $k_v = \mathbb{C}$. Class field theory shows that

$$V(k) \subseteq V(\mathbb{A}_k)^{\mathrm{Br}} \subseteq V(\mathbb{A}_k),$$

so we say that V has a Brauer-Manin obstruction to the Hasse principle if $V(\mathbb{A}_k)^{\mathrm{Br}}$ is empty, so that $V(k)$ is as well.

For many classes of varieties, it is believed that the Brauer-Manin obstruction to the Hasse principle is "the only one"; that is, if $V(\mathbb{A}_k)^{\mathrm{Br}}$ is nonempty, then so is $V(k)$. It is not known (even conjecturally) whether or not the Brauer-Manin obstruction to the Hasse principle is the only one for $K3$ surfaces.

2.2. **The key isomorphism.** The map $V \to \operatorname{Spec} k$ induces a map $\operatorname{Br} k \to \operatorname{Br} V$, which is injective if $V(\mathbb{A}_k)$ is nonempty. Elements in the image of this map are called *constant algebras*. Two elements of $\operatorname{Br} V$ which differ by a constant algebra cut out the same subset of $V(\mathbb{A}_k)$, so the intersection (2) defining $V(\mathbb{A}_k)^{\mathrm{Br}}$ need only be taken over a set of representatives of $\dfrac{\operatorname{Br} V}{\operatorname{Br} k}$.

Proposition 2.1. *For V a smooth projective geometrically integral k-variety, k a number field, with $V(\mathbb{A}_k) \neq \emptyset$, there is an isomorphism*

$$(3) \qquad \frac{\operatorname{Br}_1 V}{\operatorname{Br} k} \to H^1(k, \operatorname{Pic} \overline{V}),$$

where $\overline{V} = V \times_k \overline{k}$ and $\operatorname{Br}_1 V = \ker(\operatorname{Br} V \to \operatorname{Br} \overline{V})$ is the "algebraic part" of the Brauer group.

Proof. This is a standard consequence of the Hochschild-Serre spectral sequence; see for instance [16], Corollary 2.3.9. □

It is, unfortunately, very difficult in general to compute the inverse of the isomorphism (3) explicitly. The crux of the computation is an explicit use of the fact (due to Tate) that $H^3(k, \overline{k}^*) = 0$; that is, one must express an arbitrary 3-cocycle with values in $\overline{k}^*$ as a coboundary. In the next section, we discuss one way around this problem.

2.3. Quaternion algebras in $\mathrm{Br}_1(V)$.

One common way of constructing explicit elements of $\mathrm{Br}_1(V)$ is as follows:

Definition 2.2. For $c \in k^*$ and $g \in k(V)^*$, the quaternion algebra (c, g) is a four-dimensional central simple $k(V)$-algebra with $k(V)$-basis $1, i, j, ij$, satisfying $i^2 = c$, $j^2 = g$, and $ij = -ji$.

Of course, quaternion algebras are quite general objects; the reason we study the special quaternion algebras defined above is the following standard lemma:

Lemma 2.3. *For $c \in k^*$ and $g \in k(V)^*$, a quaternion algebra $(c, g) \in \mathrm{Br}\, k(V)$ is in the image of the map $\mathrm{Br}\, V \to \mathrm{Br}\, k(V)$ if and only if $\mathrm{div}(g) = D + \sigma D$, where D is a divisor defined over $k(\sqrt{c})$ and σ is the nontrivial element of $\mathrm{Gal}(k(\sqrt{c})/k)$. It is a constant algebra if and only if $\mathrm{div}(g) = D' + \sigma D'$, where D' is a principal divisor defined over $k(\sqrt{c})$.*

Proof. See [8], Proposition 2.2.3 or [4], Proposition 4.17. □

Note that the quaternion algebra (c, g) will always split over the quadratic extension $k(\sqrt{c})$, so its image in $H^1(k, \mathrm{Pic}\, \overline{V})$ will restrict to 0 in $H^1(k(\sqrt{c}), \mathrm{Pic}\, \overline{V})$. There is also a well-known formula for the local invariant of such a quaternion algebra in $\mathrm{Br}\, V$: for any point $P_v \in V(k_v)$, we have that

$$\mathrm{inv}_v(c, g)(P_v) = [c, g(P_v)]_v,$$

where $[a, b]_v$ is the Hilbert symbol of $a, b \in k_v^*$ expressed as an element of $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. So $[a, b]_v = 0$ if and only if $x^2 - ay^2 - bz^2$ represents 0 in k_v; otherwise, it equals $1/2$.

Algorithm 2.4. Given a class of varieties over k, here is how we look for varieties V in that class with quaternion algebras of the above type generating nonconstant elements in $\mathrm{Br}_1(V)$:

(1) Find a G_k-invariant generating set Γ for $\mathrm{Pic}\, \overline{V}$ (possibly a subgroup of $\mathrm{Pic}\, \overline{V}$ will work as well; see the comments).

(2) The action of the Galois group on Γ induces a map $G_k \to \mathrm{Aut}(\Gamma)$. By inflation-restriction, $H^1(k, \mathrm{Pic}\, \overline{V})$ will be isomorphic to $H^1(H, \mathrm{Pic}\, \overline{V})$, where H is the image of G_k inside $\mathrm{Aut}(\Gamma)$. List the cohomology groups $H^1(H, \mathrm{Pic}\, \overline{V})$ for every subgroup H of $\mathrm{Aut}(\Gamma)$; these are the possibilities for $H^1(k, \mathrm{Pic}\, \overline{V})$.

(3) Search the subgroups of $\mathrm{Aut}(\Gamma)$ to find H such that $H^1(H, \mathrm{Pic}\, \overline{V}) = \mathbb{Z}/2$ but $H^1(H', \mathrm{Pic}\, \overline{V}) = 0$ for some subgroup $H' \subset H$ of index 2.

(4) Give conditions on V such that the image of G_k in $\mathrm{Aut}(\Gamma)$ equals H.

(5) Let L be the fixed field of H'. Use the equality $H^1(H, \operatorname{Pic} \overline{V}) = \mathbb{Z}/2$ to find a nonzero divisor class $d \in \operatorname{Pic} V_L$ such that $d + \sigma d = 0$ in $\operatorname{Pic} V_L$, σ the nontrivial element of $\operatorname{Gal}(L/k)$.

(6) Given d and L, find a divisor D defined over L whose class is d. (Such a divisor is guaranteed to exist whenever V has points everywhere locally; see [8], Proposition 1.3.4.) Then our quaternion algebra is (c, g), where $L = k(\sqrt{c})$ and g is a function whose divisor is $D + \sigma D$.

Comments on the algorithm: Carrying out step (1) requires that we know quite a lot about the geometry of $\overline{V}$. Even for general $K3$ surfaces, this is too hard. Some previous attempts to carry out this algorithm explicitly have restricted themselves to Del Pezzo surfaces (e.g. [8], [10], [9]), or special $K3$ surfaces such as diagonal quartic hypersurfaces ([4]) or Kummer surfaces ([1]). As we will see, the $K3$ surfaces we examine in this paper come equipped with a G_k-invariant set Γ of 32 lines generating a subgroup of $\operatorname{Pic} \overline{V}$ which is free of rank 17. In general, we will want $\operatorname{Pic} \overline{V}$ to have no 2-torsion; see the comments for Step (5).

In Step (3), we usually search for the largest possible such H, so that we can study the broadest possible class of varieties V admitting a nonconstant quaternion algebra of the above type in $\operatorname{Br}_1 V$. The conditions on H and H' can be relaxed somewhat if need be: what we are looking for is a subgroup H and an index-2 subgroup H' of H such that the restriction of some order-2 element of $H^1(H, \operatorname{Pic} \overline{V})$ is zero in $H^1(H', \operatorname{Pic} \overline{V})$. In practice, the largest such H and H' usually satisfy the stronger conditions given in the algorithm.

We carry out Step (5) using the following procedure: let $\overline{P} = \operatorname{Pic} \overline{V}$. Then there is an isomorphism

$$\frac{(\overline{P}/2\overline{P})^{G_k}}{\overline{P}^{G_k}/2\overline{P}^{G_k}} \to H^1(k, \overline{P})[2]$$

sending a divisor class e representing an element of $(\overline{P}/2\overline{P})^{G_k}$ to the class of the cocycle $c_\tau = \frac{1}{2}(\tau e - e)$ (cf. [9], Lemma 3.1; here c_τ is well defined because $\overline{P}$ has no 2-torsion). Since we have computed $H^1(k, \overline{P})[2]$, we can find a nontrivial c_τ and hence a nontrivial e. If this cocycle trivializes upon restriction to G_L, then we can find an e on the left defined over L, and then the divisor class $d = \frac{1}{2}(\sigma e - e)$ satisfies $d + \sigma d = 0$ in $\operatorname{Pic} V_L$.

Moreover, in this case, the class in $\operatorname{Br}_1(V)/\operatorname{Br} k$ of the quaternion algebra (c, g) that we obtain at the end of the algorithm corresponds via the isomorphism (3) to the class of the cocycle c_τ, so if we know that this cocycle is not a coboundary, we are guaranteed that the quaternion algebra we have found is nonconstant.

In practice, we usually write down conditions on V in Step (4) in such a way that *generically* $H^1(k, \overline{P})[2]$ is nontrivial, because the image of $G_k \to \operatorname{Aut}(\Gamma)$ is the subgroup H we found in Step (3); but if the image of $G_k \to \operatorname{Aut}(\Gamma)$ is strictly contained in H, it might happen that the quaternion algebra (c, g) we construct is constant.

If Γ generates a subgroup Q of $\overline{P}$, then step (2) enumerates the possibilities for $H^1(k, Q)$, and the rest of the algorithm constructs a quaternion algebra whose corresponding cocycle in $H^1(k, Q)$ is not a coboundary. If Q is a proper subgroup of $\overline{P}$, then the restriction of this quaternion algebra to $H^1(k, \overline{P})$ might be zero. So in this case (and the problem case in the above paragraph), we will get a bona fide

element of $\mathrm{Br}\,V$ from the above algorithm, but it will not furnish a Brauer-Manin obstruction to rational points on V.

3. Genus-2 curves and $K3$ surfaces: A review of the theory

The material in this section is taken largely from [12].

3.1. **Construction of the $K3$ surface.** Let C be a genus-2 curve over a number field k and let J be its Jacobian. We wish to associate, to an element $\delta \in \mathrm{Sel}^{(2)}(k, J)$, a $K3$ surface V_δ with points everywhere locally, such that if δ is in the image of $J(k)/2J(k)$, then V_δ has a rational point.

Definition 3.1. For $f(x) \in k[x]$ of degree 6, set $A_f = k[x]/(f(x))$.

Definition 3.2. For any $\delta \in A_f^*$, define

$$\mathcal{V}_{f,\delta} = \{q \in A_f : \delta q^2 \equiv \text{quadratic mod } f\}.$$

If we write $q(x) = \sum_{i=0}^5 a_i x^i$, then q lies in $\mathcal{V}_{f,\delta}$ if and only if the coefficients of x^3, x^4, and x^5 in δq^2 all vanish. Considered as polynomials in the a_i, these coefficients C_3, C_4, C_5 are homogeneous of degree 2.

Definition 3.3. For $\delta \in A_f^*$, define V_δ to be the variety in $\mathbb{P}^5$ consisting of points $(a_0 : \cdots : a_5)$ such that $\sum_{i=0}^5 a_i x^i \in \mathcal{V}_{f,\delta}$. One shows ([12], Proposition 2.1.2) that V_δ is a smooth complete intersection of the three quadrics C_3, C_4, C_5, which makes it a $K3$ surface of degree 8.

Let H_f be the kernel of the norm map $A_f^*/(A_f^*)^2 k^* \to k^*/(k^*)^2$ (which is well defined because the degree of f is even). Then Lemma 5.1 of [17] describes a map $\Delta_k \colon J(k)/2J(k) \to H_f$ whose kernel has order 1 or 2; as usual, it is induced from the homomorphism $\mathrm{Div}^0_\perp(C)(k) \to A_f^*$ defined by $P \mapsto x(P) - x$, where $\mathrm{Div}^0_\perp(C)$ consists of divisors whose support is disjoint from that of $\mathrm{div}(y)$. In addition, the lemma gives necessary and sufficient conditions under which the kernel will have order 1. It suffices, for instance, for f to have a factor of odd degree. (See Theorem 13.2 of [15] for a generalization.) Following section 5 of [17], we say that "k satisfies condition ($\ddagger$)" (thinking of f as fixed) if the kernel has order 1.

If k satisfies condition ($\ddagger$), we can identify $\mathrm{Sel}^{(2)}(k, J)$ with the set of elements of H_f whose images in $H_f \otimes k_v$ lie in the image of Δ_{k_v} for all places v of k.[1]

Henceforth, we will assume that k satisfies ($\ddagger$), and we will think of $\mathrm{Sel}^{(2)}(k, J)$ as the subset of H_f described in the above paragraph. The goal is then to compute that set and to look for elements in it which are not in the image of Δ_k.

This is where the set $\mathcal{V}_{f,\delta}$ comes in: Proposition 3.2.6 of [12] shows that if $\delta \in \mathrm{Sel}^{(2)}(k, J)$ is in the image of Δ_k, then there is a polynomial $q \in \mathcal{V}_{f,\delta}$. For the sake of concreteness, we sketch the proof: δ will be congruent mod $(A_f^*)^2 k^*$ to $(x(P_1) - x)(x(P_2) - x)$ for some pair of points $P_1, P_2 \in C(\overline{k})$ that are either both defined over k, or defined and conjugate over a quadratic extension of k. We restate this fact:

---

[1] In general, this set is known as the "fake 2-Selmer group," but it is isomorphic with the 2-Selmer group if k satisfies condition ($\ddagger$); see [17], section 5.

Proposition 3.4. *Let C be a genus-2 curve given by $y^2 = f(x)$, $f(x) \in k[x]$ of degree 6, and let J be its Jacobian. Suppose that k satisfies (‡). If $\delta \in \mathrm{Sel}^{(2)}(k, J)$ is in the image of the map $J(k)/2J(k) \to \mathrm{Sel}^{(2)}(k, J)$ from (1), then the K3 surface V_δ has a rational point.*

We can view this result from another perspective as well: elements $\delta \in \mathrm{Sel}^{(2)}(k, J)$ correspond to 2-coverings X_δ of J, which are twists of J equipped with a map $\pi \colon X \to J$ defined over k which is a twist of multiplication by 2 on $J_{\overline{k}}$. Such 2-coverings inherit an involution defined over k descending from multiplication by -1 on J. Then the surface V_δ is the minimal nonsingular model of the quotient of X_δ by this involution. (It is a twist of the desingularized Kummer surface of J; cf. Chapter 16 of [7].)

The element δ comes from $J(k)/2J(k)$ if and only if X_δ is the trivial twist of J, which happens if and only if $X_\delta(k)$ is nonempty. But since $\delta \in \mathrm{Sel}^{(2)}(k, J)$, we must have that $X_\delta(k_v)$ is nonempty for all places v of k. Certainly if X_δ has a point in some field K, then V_δ will have a point in K as well. So V_δ has points everywhere locally, and $V_\delta(k) = \emptyset$ will imply that $X_\delta(k) = \emptyset$ and hence that δ does not come from $J(k)/2J(k)$, which is the same as saying that it maps to a nontrivial element of $\mathrm{III}(k, J)[2]$.

Remark 3.5. It may be true that $X_\delta(k)$ is empty while $V_\delta(k)$ is nonempty; since X_δ is really the surface in whose rational points we are interested, one might hope to work directly with it instead of V_δ. Of course, the reason we do not do this is that the usual explicit description of X_δ is as an intersection of 72 quadrics in $\mathbb{P}^{15}$ (just as it is for the Jacobian itself; see [7], Chapter 2 for the construction).

Remark 3.6. If $f(x)$ has a k-rational root, we can find a model C' for C of the form $w^2 = g(u)$, $\deg g = 5$. If we carry through the above constructions in A_g instead of A_f, we get a smooth complete intersection of two quadrics in $\mathbb{P}^4$, which is a Del Pezzo surface W_β of degree 4, where β is the element of $\mathrm{Sel}^{(2)}(k, \mathrm{Jac}\, C')$ corresponding to δ (see [6] and [3]). We will see later that V_δ is a double cover of W_β. Then, just as in the previous remark, it may be true that $W_\beta(k)$ is nonempty while $V_\delta(k)$ is empty; in fact, this happens for the curve given in Theorem 1.1 (assuming that the Brauer-Manin obstruction to the Hasse principle is the only one for Del Pezzo surfaces).

3.2. **The 32 lines and** $\mathrm{Pic}\, \overline{V_\delta}$**.** Here we review the construction of the 32 lines on $\mathrm{Pic}\, \overline{V_\delta}$ and analyze the structure of $\mathrm{Pic}\, \overline{V_\delta}$ as a G_k-module. The ideas are taken from [12], but the notation will be different.

For $\delta \in A_f^*$, let $r_1, \ldots, r_6$ be the roots of f in $\overline{k}$. Fix a choice of square roots z_i of $\delta(r_i)$ in $\overline{k}$.

For an element $s = (s_1, \ldots, s_6) \in (\mathbb{Z}/2)^6$, define γ_s to be the unique degree-5 polynomial satisfying $\gamma_s(r_i) = \dfrac{(-1)^{s_i}}{z_i}$ for $1 \leq i \leq 6$. Now define

$$\mathcal{L}_s = \{\gamma_s(x)(tx + u) \colon t, u \in \overline{k}\}$$

and notice that $\delta(x)q(x)^2 \equiv (tx+u)^2 \bmod f$, for any $q(x) \in \mathcal{L}_s$. The projectivization (as in Definition 3.3) of $\mathcal{L}_s$ is a line L_s on $\overline{V_\delta}$. Notice that if $s + s' = (1, 1, 1, 1, 1, 1)$, we have that $\gamma_s = -\gamma_{s'}$, so $L_s = L_{s'}$. Thus we have 32 lines L_s indexed by elements of $(\mathbb{Z}/2)^6/\langle(1, 1, 1, 1, 1, 1)\rangle$.

It is not hard to determine the intersection pairing as applied to the subgroup generated by these lines in $\operatorname{Pic} \overline{V_\delta}$; one obtains

$$L_{s_1} \cdot L_{s_2} = \begin{cases} -2 & \text{if } s_1 \text{ and } s_2 \text{ differ in 0 or 6 places,} \\ 1 & \text{if } s_1 \text{ and } s_2 \text{ differ in 1 or 5 places,} \\ 0 & \text{otherwise.} \end{cases}$$

The first line follows by the adjunction formula for $K3$ surfaces, and the second and third lines follow by direct calculations. From these intersection numbers we obtain

Proposition 3.7 ([12], Proposition 2.1.21). *The classes of the 32 lines on $\overline{V_\delta}$ generate a subgroup of $\operatorname{Pic} \overline{V_\delta}$ isomorphic to $\mathbb{Z}^{17}$.*

Remark 3.8. In the generic case this subgroup equals all of $\operatorname{Pic} \overline{V_\delta}$ (Proposition 2.1.30 of [12]). As noted above, even if V_δ is not generic, we can still use the subgroup Q generated by the classes of the lines to give us an element of $H^1(k, \operatorname{Pic} \overline{V_\delta})$, using the natural map $H^1(k, Q) \to H^1(k, \operatorname{Pic} \overline{V_\delta})$.

4. THE ALGORITHM FOR V_δ

Viewed in terms of Algorithm 2.4, the end of the previous section carries out Step (1) for the class of varieties of the form V_δ; then Γ is in our case the set of 32 lines on $\overline{V_\delta}$ defined earlier. We proceed to carry out the remaining steps of the algorithm.

Let G_Γ be the group $(\mathbb{Z}/2)^6/\langle(1,1,1,1,1,1)\rangle$ indexing the 32 lines. Then, by a straightforward analysis of the intersection pairing on Γ (which is Proposition 2.2.11 of [12]), $\operatorname{Aut}(\Gamma)$ is isomorphic to $G_\Gamma \rtimes S_6$, where the symmetric group acts on G_Γ by permuting indices (which corresponds to permuting the square roots z_i of $\delta(r_i)$), and G_Γ acts on itself by addition.

For $\delta \in \operatorname{Sel}^{(2)}(k, J)$, the image of $G_k \to \operatorname{Aut}(\Gamma)$ must lie in a subgroup of index 2 inside $\operatorname{Aut}(\Gamma)$, because the norm of δ is required to be a square in k (the 2-Selmer group is a subgroup of the kernel H_f of the norm map). Indeed, this index-2 subgroup is the semi-direct product of S_6 with the index-2 subgroup of G_Γ of elements whose sum is 0. This is a group G of order 11520 which acts on $\mathbb{Z}^{17}$ in a prescribed way. MAGMA can enumerate its subgroups H and compute $H^1(H, \mathbb{Z}^{17})$ for each one. This is Step (2).

We look in Step (3) for maximal subgroups H of G such that $H^1(H, \mathbb{Z}^{17}) = \mathbb{Z}/2$ and $H^1(H', \mathbb{Z}^{17}) = 0$ for some index-2 subgroup $H' \subset H$. MAGMA finds two conjugacy classes of such subgroups. One class consists of subgroups of order 96; the other consists of subgroups of order 128. Here we exhibit a Brauer-Manin obstruction coming from the first conjugacy class; presumably we could use the same techniques to try to find one coming from the second class.

4.1. The subgroup H_{96} and the shape of $f(x)$. Consider polynomials $f(x)$ of the shape

$$f(x) = f_2(x)f_3(x)(x - r_6),$$

where f_i is an irreducible polynomial of degree i. (Note that condition ($\ddagger$) is automatic, since f has a factor of odd degree.) Let C be the genus-2 curve $y^2 = f(x)$. Pick the ordering of the roots of f that lists the two roots of f_2, then the three roots of f_3, then r_6. Suppose also that $\delta \in \operatorname{Sel}^{(2)}(k, J)$ satisfies the condition that $\delta(r_1)$

is a square in $\mathbb{Q}(r_1)$, where r_1 is a root of $f_2(x)$. Then the image of $G_k \to \mathrm{Aut}(\Gamma)$ will sit inside the subgroup of $G_\Gamma \rtimes S_6$ generated by the elements

$$(0,0,1,0,0,1), (0,0,1,1,1,1), (12), (345), (34),$$

where the first two elements are in G_Γ and the last three elements are permutations in S_6.

It is not hard to check that this is a subgroup H_{96} of order 96. If we define H_{48} to be the index-2 subgroup consisting of elements which leave $z_6 = \sqrt{\delta(r_6)}$ unchanged, then MAGMA computes that $H^1(H_{96}, \mathbb{Z}^{17}) = \mathbb{Z}/2$ and $H^1(H_{48}, \mathbb{Z}^{17}) = 0$.

Now let us see where the nontrivial element of $H^1(H_{96}, \mathbb{Z}^{17})$ comes from: set

$$d = \left(\ell_{(0,0,0,1,1,0)} + \ell_{(0,0,0,1,1,1)} \right) - \left(\ell_{(0,0,1,0,0,0)} + \ell_{(0,0,1,0,0,1)} \right),$$

where ℓ_s is the divisor class of L_s. One computes that $\sigma d = d$ for all $d \in H_{48}$, and $\sigma d = -d$ for all $\sigma \in H_{96} \setminus H_{48}$. So d is the divisor class we referred to in Step (5) of Algorithm 2.4.

Now the fixed field of the intersection of H_{48} with the image of $G_k \to \mathrm{Aut}(\Gamma)$ will be $L = k(\sqrt{\delta(r_6)})$. The remaining step in the algorithm is to find a divisor $D \in \mathrm{Div}(V_\delta)_L$ whose divisor class is d. Of course we will have to use the fact that V_δ has points everywhere locally. The easiest way to solve this computational problem, generally speaking, is to reduce it to solving a certain norm equation which we are guaranteed has a solution by the Hasse Norm Theorem. We now show how this can be accomplished for V_δ.

4.2. The divisor D and the quaternion algebra.
The strategy is to take a divisor E in the class of d defined over a higher-degree extension of k, and then to subtract the divisor of a judiciously chosen rational function to E in order to obtain a divisor defined over L. That is, we want

$$\tau(E - (h)) = E - (h) \text{ for all } \tau \in G_L.$$

Here we begin with

$$E = \left(L_{(0,0,0,1,1,0)} + L_{(0,0,0,1,1,1)} \right) - \left(L_{(0,0,1,0,0,0)} + L_{(0,0,1,0,0,1)} \right).$$

The stabilizer H_{12} of the divisor E (not its class) in H_{96} is generated by $(0,0,1,1, 0,0) \cdot (34), (12), (45)$. It has order 12 and index 4 in H_{48}. We wish to find a function (h) such that $E - (h)$ is fixed by H_{48}. That is, for all $\tau \in H_{48}$, we want $E - \tau E = \mathrm{div}(h/\tau h)$.

There are four left cosets of H_{12} in H_{48}, and we first identify what the divisor of $h/\tau h$ must be for τ in each coset. For ease of notation, we identify an element $s \in G_\Gamma$ with the binary number $\sum_{i=1}^{6} 2^{6-i} s_i$. So, in this notation,

$$E = L_6 + L_7 - (L_8 + L_9).$$

So we get

$$\tau \in H_{12} \Rightarrow \operatorname{div}(h/\tau h) = 0,$$

$$\tau \in (0,0,1,1,0,0)H_{12} \Rightarrow \operatorname{div}(h/\tau h) = L_4 + L_5 + L_6 + L_7$$
$$- (L_8 + L_9 + L_{10} + L_{11}),$$

$$\tau \in (0,0,0,1,1,0)H_{12} \Rightarrow \operatorname{div}(h/\tau h) = L_6 + L_7 + L_{14} + L_{15}$$
$$- (L_0 + L_1 + L_8 + L_9),$$

$$\tau \in (0,0,1,0,1,0)H_{12} \Rightarrow \operatorname{div}(h/\tau h) = L_2 + L_3 + L_6 + L_7$$
$$- (L_8 + L_9 + L_{12} + L_{13}).$$

Proposition 4.1. *Fix an index set $I = i_1, i_2, i_3 \in \{1,2,3,4,5,6\}$. Fix a sequence $B = (b_1, b_2, b_3) \in \mathbb{Z}/2$. Let $E_{I,B}$ be the sum of the eight lines L_s, $s \in G_\Gamma$, where $s_{i_j} = b_j$. Then $E_{I,B}$ is a hyperplane section.*

Proof. This is a restatement of Lemma 2.1.24 in [12]. $\qquad\qquad\square$

The point of this proposition is that we can write the above divisors as differences of hyperplane sections. For $3 \le i \le 6$, define p_i to be a linear polynomial cutting out $E_{\{1,2,i\},\{0,0,0\}}$, and define q_i to be a linear polynomial cutting out $E_{\{1,2,i\},\{0,0,1\}}$. Then we see that

$$L_4 + L_5 + L_6 + L_7 - (L_8 + L_9 + L_{10} + L_{11}) = \operatorname{div}\left(\frac{p_3}{p_4}\right),$$

$$L_6 + L_7 + L_{14} + L_{15} - (L_0 + L_1 + L_8 + L_9) = \operatorname{div}\left(\frac{q_5}{p_4}\right),$$

$$L_2 + L_3 + L_6 + L_7 - (L_8 + L_9 + L_{12} + L_{13}) = \operatorname{div}\left(\frac{p_3}{p_5}\right).$$

Next we consider certain conditions on the p_i and q_i, which have so far only been defined up to scalar multiples. In the two propositions that follow, we show first that these conditions are sufficient to construct an explicit divisor in the divisor class of E which is defined over L, and then we verify that we can always find p_i and q_i satisfying these conditions.

Condition 1. We wish to choose p_i and q_i to have coefficients in $k(r_1, z_i, z_6)$ and to be defined so that $(0,0,1,1,1,1)p_i = q_i$. This condition will be immediate from the construction of the p_i and q_i we will outline below.

Condition 2. We wish to choose p_i and q_i so that $\sigma p_i = p_j$ and $\sigma q_i = q_j$ if $\sigma \in H_{96} \cap S_6$ sends i to j, and so that

$$\tau p_i = \begin{cases} p_i & \text{if } \tau \in H_{96} \cap G_\Gamma \text{ has a 0 in the } i\text{th spot,} \\ q_i & \text{if } \tau \in H_{96} \cap G_\Gamma \text{ has a 1 in the } i\text{th spot.} \end{cases}$$

This condition is easy to satisfy, as we will shortly see.

Condition 3. We also want that $p_i q_i = p_j q_j$ for $3 \le i, j \le 5$. This condition is more difficult to ensure; we will need to use the fact that V_δ has points everywhere locally.

Proposition 4.2. *Suppose that p_i and q_i satisfy Conditions 1,2,3. Let*

$$h = 1 + \frac{p_3}{p_4} + \frac{q_5}{p_4} + \frac{p_3}{p_5}.$$

Then the divisor $E - (h)$ is defined over the field $L = k(z_6)$.

Proof. By condition 1, the rational function h is defined over the field $k(r_1, z_3, z_4, z_5)$. Note that z_6 is automatically contained in this field extension because of the requirement that the product of the z_i is in k (and the requirement that $z_1 \in k(r_1)$). The Galois group of this field extension is a subgroup of H_{96}. So we must only show that $E - \tau E = \operatorname{div}(h/\tau h)$ for every $\tau \in H_{48}$.

First we show that $\tau h = h$ for $\tau \in H_{12}$. Clearly this is the case for $\tau = (12)$. Now

$$(45)h = 1 + \frac{p_3}{p_5} + \frac{q_4}{p_5} + \frac{p_3}{p_4} = 1 + \frac{p_3}{p_5} + \frac{p_4}{q_5} + \frac{p_3}{p_4} = h$$

and

$$((0,0,1,1,0,0) \cdot (34))h = (0,0,1,1,0,0)\left(1 + \frac{p_4}{p_3} + \frac{q_5}{p_3} + \frac{p_4}{p_5}\right)$$

$$= 1 + \frac{q_4}{q_3} + \frac{q_5}{q_3} + \frac{q_4}{p_5}$$

$$= 1 + \frac{p_3}{p_4} + \frac{p_3}{p_5} + \frac{p_4}{q_5} = h.$$

So $\operatorname{div}(h/\tau h)$ depends only on the left coset of H_{12} to which τ belongs. In the computations that follow, it will help to note that

$$h = \frac{p_4 p_5 + p_3 p_5 + p_3 p_4 + p_5 q_5}{p_4 p_5}$$

and to notice that the numerator is invariant under permutations of the coordinates $3, 4, 5$, by Condition 3. So we are reduced to three computations:

$$\frac{h}{(34)h} = \frac{p_3 p_5}{p_4 p_5} = \frac{p_3}{p_4},$$

$$\frac{h}{(0,0,0,1,1,0)h} = \frac{(p_4 p_5 + p_3 p_5 + p_3 p_4 + p_5 q_5)q_4 q_5}{(q_4 q_5 + p_3 q_5 + p_3 q_4 + p_5 q_5)p_4 p_5}$$

$$= \frac{q_5}{p_4} \frac{(p_4 q_4)p_5 + p_3 q_4 p_5 + (p_4 q_4)p_3 + (p_5 q_5)q_4}{(p_5 q_5)q_4 + (p_5 q_5)p_3 + p_3 q_4 p_5 + (p_5 q_5)p_5}$$

$$= \frac{q_5}{p_4} \text{ (using Condition 3 several times)},$$

$$\frac{h}{(35)h} = \frac{p_4 p_3}{p_4 p_5} = \frac{p_3}{p_5}.$$

In each case, $h/\tau h$ has the divisor we want. $\square$

Proposition 4.3. *In the above situation, we can construct functions p_i and q_i satisfying Conditions $1, 2, 3$.*

Proof. Define

$$p_i(a_0, a_1, a_2, a_3, a_4, a_5) = \sum_{j=0}^{5}\left(\frac{r_1^j(r_2 - r_i)}{z_2 z_i} + \frac{r_2^j(r_i - r_1)}{z_i z_1} + \frac{r_i^j(r_1 - r_2)}{z_1 z_2}\right)a_j.$$

Define q_i by replacing z_i with $-z_i$ everywhere. We must now show that the intersection divisor of the hyperplane cut out by p_i with V_δ is in fact $E_{\{1,2,i\},\{0,0,0\}}$.

To see this, let $q(x) = \sum_{j=0}^{5} a_j x^j$, and suppose that $q(r_m) = \dfrac{1}{z_m}(tr_m + u)$ for $m = 1, 2, i$. Then

$$p_i(a_0, a_1, a_2, a_3, a_4, a_5) = \frac{q(r_1)(r_2 - r_i)}{z_2 z_i} + \frac{q(r_2)(r_i - r_1)}{z_i z_1} + \frac{q(r_i)(r_1 - r_2)}{z_1 z_2}$$

$$= \frac{1}{z_1 z_2 z_i}\left((r_2 - r_i)(tr_1 + u) + (r_i - r_1)(tr_2 + u) + (r_1 - r_2)(tr_i + u)\right)$$

$$= 0.$$

Hence the lines whose classes appear in $E_{\{1,2,i\},\{0,0,0\}}$ all lie on the hyperplane cut out by p_i.

Similarly we can show that the intersection divisor of the hyperplane cut out by q_i with V_δ is $E_{\{1,2,i\},\{0,0,1\}}$. Now Conditions 1 and 2 are immediate from the construction of p_i and q_i. Note also that $p_i q_i$ actually has coefficients in $k(z_i^2)$, as it is invariant under the transposition of the indices $1, 2$ as well as the map $z_i \mapsto -z_i$.

Now we must arrange for Condition 3 to hold by multiplying the p's and q's by suitable constants. For $3 \le i \le 6$, consider the rational function $\dfrac{p_i q_i}{p_6 q_6}$ on $\overline{V}$. Note that its divisor is 0, so it is a nonzero constant u_i. To evaluate this constant, let $P_v \in V(k_v)$ be a point not in the support of this rational function, and note that

$$u_i = \frac{p_i(P_v) q_i(P_v)}{p_6(P_v) q_6(P_v)} = \frac{a_v}{b_v},$$

where a_v is a norm from $k_v(z_i)$ to $k_v(z_i^2)$ and b_v is a norm from $k_v(z_6)$ to k_v.

Lemma 4.4 ([13], VIII.1.11). *Let k be a field of characteristic $\ne 2$. An element $c \in k^*$ is the product of a norm from $k(\sqrt{a})$ and a norm from $k(\sqrt{b})$ if and only if, as an element of $k(\sqrt{ab})$, it is a norm from $k(\sqrt{a}, \sqrt{b})$.*

Let $L_i = k(z_i^2)$. For any place w of L_i, the expression $u_i = a_v(1/b_v)$ exhibits $u_i \in L_i$ as the product of a norm from $(L_i)_w(z_i)$ and a norm from $(L_i)_w(z_6)$. By Lemma 4.4, we see that u_i is a norm from $(L_i)_w(z_i, z_6)$ to $(L_i)_w(z_i z_6)$. By the Hasse Norm Theorem, it follows that u_i is a norm from $L_i(z_i, z_6)$ to $L_i(z_i z_6)$, say of $d_i \in L_i(z_i, z_6)$. Let $\sigma = (0, 0, 1, 1, 1, 1) \in G_\Gamma$. Then $d_i(\sigma d_i) = u_i$, and if we let d_j be the image of d_i under an element of $H_{96} \cap S_6$, transposing i and j, we see that

$$\frac{p_i q_i}{p_j q_j} = \frac{d_i \sigma d_i}{d_j \sigma d_j},$$

and thus if we replace p_i by p_i/d_i and q_i by $q_i/(\sigma d_i)$, we have found functions satisfying Condition (3). $\qquad\square$

Once we have constructed h such that $E - \tau E = \mathrm{div}(h/\tau h)$, the rational function g we want will be a function whose divisor is $(E - (h)) + \sigma(E - (h))$, where σ is *any* element of $H_{96} \setminus H_{48}$. The most convenient σ to choose is certainly $(0, 0, 1, 1, 1, 1) \in G_\Gamma$, because $\sigma E = -E$. Thus the rational function g we use is a function whose divisor is $-(h \cdot (0, 0, 1, 1, 1, 1)h)$. We can drop the negative sign, since we have a quaternion algebra, i.e. $(c, g) = (c, 1/g)$. So we can take

$$g = h \cdot (0, 0, 1, 1, 1, 1)h \text{ times a constant,}$$

where we know that we will be able to find a constant so that g is invariant under the action of the Galois group.

Remark 4.5. It appears at first glance that g will always be a norm from $k(z_6)$ to k, which would make the quaternion algebra we have constructed trivial in $\operatorname{Br} V$. But h is not itself defined over $k(z_6)$, so indeed this algebra is nontrivial in general.

Remark 4.6. Here is how we arrange for Condition 3 to hold in practice. We know from the proof above that there are constants $d_i \in k(z_i, z_6)$ (which are conjugate to each other under the action of S_3 on the indices $3, 4, 5$) such that $(p_i/d_i)\sigma(p_i/d_i)$ is independent of i, for $3 \le i \le 5$; here σ is the element $(0, 0, 1, 1, 1, 1) \in G_\Gamma$ sending $z_i \mapsto -z_i$ for $3 \le i \le 6$.

We consider the *normal form* N_i of $p_i q_i$ with respect to a Gröbner basis for the ideal generated by the defining equations of V_δ. The normal form is a uniquely determined representative of the equivalence class of $p_i q_i$ modulo this ideal; it is clear from the construction of the normal form that the normal forms of $p_i q_i$ and $p_j q_j$ are permuted just as $p_i q_i$ and $p_j q_j$ are, by the action of S_3 on the indices. Fixing a monomial appearing in N_i and calling its coefficient c_i, we note that $c_i \in k(z_i)$ should satisfy

$$\frac{c_i}{c_j} = \frac{p_i q_i}{p_j q_j} = \frac{N_\sigma(d_i)}{N_\sigma(d_j)}.$$

Note also that

$$\frac{N_\sigma(d_i)}{c_i}$$

is independent of i, but since this quantity is in $k(z_i^2, z_6)^*$ for each i, it follows that it lies in $k(z_6)^*$.

So we search for $n \in k(z_6)^*$ such that $c_i n$ is a norm from $k(z_i, z_6)$ to $k(z_i^2, z_i z_6)$; we are guaranteed that such n exist, and in practice we find them quickly (e.g. using the `NormEquation` function in MAGMA).

In fact, in every explicit example that the author has written down, he has been able to find a value of n lying in k^*, but the author does not know if it is always possible to find $n \in k^*$ in general.

5. Proof of the main theorem

Theorem 5.1. *Let C be the hyperelliptic curve $y^2 = (x^2 - 5x + 1)(x^3 - 7x + 10)(x + 1)$. Then $\text{Ш}(\mathbb{Q}, \operatorname{Jac}(C))[2] = \mathbb{Z}/2 \times \mathbb{Z}/2$.*

Proof. Let $J = \operatorname{Jac}(C)$. Let $f(x)$ be the sextic polynomial defining C. First note that it is easy to show that $J(\mathbb{Q})/2J(\mathbb{Q})$ is a vector space over $\mathbb{Z}/2$ of dimension at least 2; the quadratic factor of $f(x)$ gives a nontrivial 2-torsion element in $J(\mathbb{Q})$, and there is also an element of $J(\mathbb{Q})/2J(\mathbb{Q})$ induced by the point in $J(\mathbb{Q})$ coming from the point $(-1, 0) \in C(\mathbb{Q})$ (MAGMA checks easily that these elements are distinct). According to Stoll's algorithm from [17], now implemented in MAGMA as `TwoSelmerGroup`, we can compute $\operatorname{Sel}^{(2)}(\mathbb{Q}, J)$, and we find that it is a vector space over $\mathbb{Z}/2$ of dimension equal to 4. (As remarked above, condition (‡) is automatic because f has a factor of odd degree.) Moreover, since C has a rational point, its Jacobian is even (in the language of [14]); that is, the order of $\text{Ш}(\mathbb{Q}, J)[2]$ is a square. Hence it is either 1 or 4. So we need only exhibit one nontrivial element of $\text{Ш}(\mathbb{Q}, J)[2]$ to complete the proof.

Define $\delta \in A_f^*$ by

(4) $$\delta(x) = -\frac{7}{2965}(377x^5 - 706x^4 - 5200x^3 + 2061x^2 - 9086x - 12308).$$

Then MAGMA shows that δ gives an element of $\mathrm{Sel}^{(2)}(J)$. The $K3$ surface V_δ is given by the vanishing of the polynomials

$- 377a_0^2 - 1604a_0a_1 - 4310a_0a_2 - 9600a_0a_3 - 14130a_0a_4 - 24100a_0a_5 - 2155a_1^2$

$- 9600a_1a_2 - 14130a_1a_3 - 24100a_1a_4 + 3002a_1a_5 - 7065a_2^2 - 24100a_2a_3$

$+ 3002a_2a_4 - 3752a_2a_5 + 1501a_3^2 - 3752a_3a_4 + 380254a_3a_5$

$+ 190127a_4^2 + 505356a_4a_5 + 2697585a_5^2,$

$353a_0^2 + 1053a_0a_1 + 3820a_0a_2 + 12135a_0a_3 + 16210a_0a_4 + 49701a_0a_5 + 1910a_1^2$

$+ 12135a_1a_2 + 16210a_1a_3 + 49701a_1a_4 - 7880a_1a_5 + 8105a_2^2 + 49701a_2a_3$

$- 7880a_2a_4 + 197631a_2a_5 - 3940a_3^2 + 197631a_3a_4 - 507830a_3a_5 - 253915a_4^2$

$+ 1686873a_4a_5 - 2233480a_5^2,$

$1300a_0^2 + 6321a_0a_1 + 17920a_0a_2 + 34505a_0a_3 + 63708a_0a_4 + 62335a_0a_5 + 8960a_1^2$

$+ 34505a_1a_2 + 63708a_1a_3 + 62335a_1a_4 + 90560a_1a_5 + 31854a_2^2 + 62335a_2a_3$

$+ 90560a_2a_4 - 243597a_2a_5$

$+ 45280a_3^2 - 243597a_3a_4 - 202262a_3a_5 - 101131a_4^2$

$- 3623209a_4a_5 - 1919025a_5^2.$

Since $\delta(r_6) = -7$, we will be using the Azumaya algebra $(-7, g)$, where g is constructed as in the previous section. (Notice that the nontrivial element of the Galois group of $\mathbb{Q}(z_6)$ sends $z_6 \mapsto -z_6$.) The denominator G of g, which is a constant multiple of $h \cdot (0,0,1,1,1,1)h$, is $p_4p_5q_4q_5$. This is a constant multiple of $(p_6q_6)^2$. Plugging in any point in $V(k_v)$ to $(p_6q_6)^2$ yields a norm from $k_v(z_6)$ to k_v, so when we compute the invariant of g, we can ignore the contribution coming from its denominator. The numerator is a homogeneous polynomial F of degree 4, so we are reduced now to computing the expressions $(-7, F(P_v))_v$ for all places v of $\mathbb{Q}$ and all points $P_v \in V(k_v)$. (The value $F(P_v)$ is not invariant under projective scaling of the coordinates of P_v, but since F has even degree, it is invariant modulo squares. Thus we can use any choice of coordinates for P_v when we compute these expressions.)

We have fixed G, but notice that g, and hence F, are only defined up to multiplication by a rational constant; call it c_0. However, since $\sum_v (-7, c_0)_v = 0$, we are guaranteed to get the correct invariant sum no matter which choice of F we make (as long as this choice is uniform for all v).

Next we wish to compute the primes of bad reduction for V_δ, for the purposes of invariant computations. This is a standard computation using the minors of the matrix of partial derivatives; we can also note that the bad primes must divide the discriminant of the minimal Galois extension over which all the lines are defined. In our case, the bad primes are $2, 3, 7, 83, 739, \infty$. Note that if -7 is a square in $\mathbb{Q}_p$ we know automatically that the quaternion algebra $(-7, F/G)$ will have constant invariant 0 at p. So we do not have to analyze $p = 2, 739$.

These will not be the only primes to consider when we compute the possibilities for $\mathrm{inv}_p \mathcal{A}(P_p)$, $P_p \in V_\delta(\mathbb{Q}_p)$. Here we repeat a standard lemma that allows us to restrict our consideration to a finite set of primes.

Lemma 5.2. *Let V be a smooth projective geometrically integral k-variety, k a number field, $g \in k(V)^*$, and let $(L/k, g)$ be a quaternion algebra in $\mathrm{Br}\, V$. Let v be*

a non-Archimedean place of k and suppose that v does not ramify in L and that V has smooth reduction at v. Then $\mathrm{inv}_v(L/k, g)(P_v)$ is independent of the choice of $P_v \in V(k_v)$.

Proof. See Lemma 8.4, [9].   □

So if p is not a bad prime for V_δ and p does not ramify in $k(z_6)$, then the invariants of the quaternion algebra $(\delta(r_6), g)(P_p)$ will be independent of the choice of P_p. When will it be nonzero?

The proof of Lemma 8.4 of [9] implies that, if $\delta(r_6)$ is not a square mod p, the invariant of $(\delta(r_6), g)(P_p)$ will equal $m_p/2 \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, where m_p is the integer such that $m_p V_p$ appears in the divisor of g (here V_p denotes the special fiber of the smooth model $\mathcal{V}$ of V_δ over $\mathrm{Spec}\, \mathbb{Z}_p$).

Pick a point $P \in V_\delta(\overline{\mathbb{Q}})$. Write $g = F/G$, where F and G are as above; they are homogeneous polynomials in six variables with integer coefficients. Since G is a norm from $k(z_6)(V_\delta)$ to $k(V_\delta)$, we can ignore it for the purposes of invariant computations. If there is a prime $\mathfrak{p}$ over p not dividing $F(P)$, then $P_{\mathfrak{p}} \in V_p(\overline{\mathbb{F}_p})$ is not in the support of g (or some rational function obtained from g by multiplying the denominator by a norm from $k(z_6)(V_\delta)$), so the integer m must equal 0. So the set of primes at which $\mathrm{inv}_p(\delta(r_6), g)(P_p)$ is not always 0, independent of $P_p \in V_\delta(\mathbb{Q}_p)$, is contained in the union of the set of bad primes with the set of primes of $\mathbb{Z}$ dividing $N(F(P))$, where N denotes the absolute norm down to $\mathbb{Q}$.

This is true for all P, so after intersecting the set of prime divisors of $N(F(P))$ for various P, we obtain the set

$$\{5, 61, 347, 739, 3433, 4337, 6833, 663149189, 69804594311\}$$

of primes p at which V_δ has smooth reduction but the integer m_p is possibly nonzero. After throwing out the primes for which -7 is a square in $\mathbb{Q}_p^*$, we get

$$\{5, 61, 3433, 663149189\}.$$

For each p in this set, we find that m_p is odd. This is not hard to check: as the invariant is constant, we need only lift one point not in the support of F/G in $V_\delta(\mathbb{Q}_p)$ to high enough precision in order to evaluate F at it. Since the invariant at each of these primes is $1/2$ and there is an even number of them, their net contribution to the sum is 0. So we obtain

$$\sum_v \mathrm{inv}_v(-7, F/G)(P_v) = \mathrm{inv}_3(-7, F/G)(P_3) + \mathrm{inv}_7(-7, F/G)(P_7)$$

$$+ \mathrm{inv}_{83}(-7, F/G)(P_{83}) + \mathrm{inv}_\infty(-7, F/G)(P_\infty).$$

To carry out the invariant computation at ∞, we first show that the value of the function F on the points in $V_\delta(\mathbb{R})$ is either always positive or always negative. To see this, consider the polynomial whose roots are $\pm z_3, \pm z_4, \pm z_5$; this polynomial can be written as $h(x^2)$, where $h(x) = x^3 - 126x^2 + 7938x + 250047$. Notice that $h(x)$ has one real root, which is negative. Under any embedding of the splitting field of $h(x^2)$ into $\mathbb{C}$ such that the image of z_3^2 is the negative real root, the images of z_4^2 and z_5^2 are distinct and conjugate. Choose such an embedding so that z_4 and $-z_5$ are complex conjugates. Then consider the action of complex conjugation on the p_i and q_i; we see that it sends p_3 to q_3 and vice versa, while it sends p_4 to q_5 and p_5 to q_4.

Now F is a constant multiple of

$$(p_3p_5 + p_3p_4 + p_4p_5 + p_3q_3)(q_3q_5 + q_3q_4 + q_4q_5 + p_3q_3),$$

and if we plug in a point in $V_\delta(\mathbb{R})$ to both these factors, we see immediately that we get the product of a complex number and its conjugate. So if we can show that F is never zero on $V_\delta(\mathbb{R})$, we can deduce that it is either always positive or always negative. It can be easily verified, either by plugging in a specific real-valued point or noticing that F is actually a *positive* constant multiple of the above function, that F is always positive. This shows that the invariant is actually zero.

To see that F never vanishes on $V_\delta(\mathbb{R})$, note that if $F(P) = 0$ for some $P \in V_\delta(\mathbb{R})$, then both factors of F vanish at P (since they are complex conjugates). So P lies on the intersection of the $K3$ surface V_δ with the two hypersurfaces cut out by the factors of F; this intersection is zero-dimensional, and MAGMA computes that there are no real points on it.

At 83 we note that there is one singular $\mathbb{F}_{83}$-valued point in the special fiber V_{83}, but it does not lift to any points mod 83^2. By a theorem of Bright ([5], Theorem 1), the invariant is constant above any smooth $\mathbb{F}_{83}$-point, so we need merely write down all points in $V_\delta(\mathbb{F}_{83})$, and lift each one to high enough precision in order to evaluate F/G at it. (Hensel's lemma guarantees that any lift of a smooth $\mathbb{F}_{83}$-point to any larger finite field will lift to a $\mathbb{Z}_{83}$-point.) Doing this computation for each of the 6960 smooth points in $V_\delta(\mathbb{F}_{83})$, we find that each point has a lift P mod 83^5 such that the 83-adic valuation of $F(P)$ is either 2 or 4. The invariant at P is 0 or $1/2$ depending on whether or not $F(P)$ has even or odd valuation, respectively; so in all cases, we find that the invariant at 83 is zero.

At 7, we compute that $V(\mathbb{F}_7)$ has 71 points. One of these points, $P_s = (3\colon 6\colon 3\colon 1\colon 2\colon 1)$, is singular, and the set

$$\{P \in V(\mathbb{F}_7)\colon F(P) = 0\}$$

has 15 elements (including the singular point). For the other 56 points, we find that $F(P) = 1$, 2, or 4, which are the squares in $\mathbb{F}_7^*$, so the invariant is zero at all these points.

Again using Theorem 1 of [5], we find one lift P of each of the 14 remaining nonsingular points in $V(\mathbb{F}_7)$ to a point in $V(\mathbb{Z}_7)$ (at least one of whose coordinates is a unit; we will call such a P *normalized*) and compute $F(P)$ for each such lift. In particular, we see that $F(P) \equiv 7^2$, $2 \cdot 7^2$, or $4 \cdot 7^2$ mod 7^3 for each of these points, so $F(P)$ is a square in $\mathbb{Z}_7$, so the invariant is zero at these points as well.

Above the point P_s, Bright's theorem does not apply, and we must actually consider all possible lifts of P_s to $P \in V(\mathbb{Z}_7)$. A lengthy MAGMA computation shows that for any such normalized P, $F(P) \equiv 2 \cdot 7^4$ mod 7^5, so once again the invariant is zero at all these points, and hence the invariant is zero at all points in $V(\mathbb{Q}_7)$.

At 3, we compute that $V(\mathbb{F}_7)$ has 40 points. All of them are singular, so Bright's theorem does not apply. A MAGMA computation similar to the one at 7 shows that if P is any normalized point in $V(\mathbb{Z}_3)$, $v_3(F(P)) = 5$. So the invariant is $1/2$ at all points in $V(\mathbb{Q}_3)$.

Hence the sum $\sum \mathrm{inv}_v \mathcal{A}(P_v)$ is constant and equal to $1/2$ for all $(P_v) \in V_\delta(\mathbb{A}_\mathbb{Q})$, so $V_\delta(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$, so $V_\delta(\mathbb{Q}) = \emptyset$. So $\delta \in \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ maps to a nonzero element of $\text{Ш}(\mathbb{Q}, J)[2]$. $\square$

Proposition 5.3. *Let n be a (positive) product of primes splitting completely in the field*

$$L(\sqrt{2}, \sqrt{-739}),$$

where L is the field of definition of the 32 lines of the curve C given above (so L is the degree-96 splitting field of $(x^2 - 35x + 49)(x^6 - 126x^4 + 7938x^2 + 250047)$). Then the Jacobian J_n of the curve given by

$$y^2 = n(x^2 - 5x + 1)(x^3 - 7x + 10)(x + 1)$$

satisfies $\text{Ш}(\mathbb{Q}, J_n)[2] \neq 0$.

Proof. Let $f(x) = (x^2 - 5x + 1)(x^3 - 7x + 10)(x + 1)$. Again, condition (‡) is automatic since f has an odd-degree factor. Note that $A_f = A_{nf}$. We show that the element

$$\delta = -\frac{7}{2965}(377x^5 - 706x^4 - 5200x^3 + 2061x^2 - 9086x - 12308)$$

lies in $\text{Sel}^{(2)}(\mathbb{Q}, J_n)$. By Corollary 5.11 of [17], we must check this only at ∞, 2, and primes p such that p^2 divides the discriminant of $nf(x)$. So we must check ∞, 2, 7, 739, and primes dividing n. At primes p dividing n, we actually show that the image of δ lies in $(A_{nf}^*)^2 \mathbb{Q}_p^*$. Let r_1 and r_2 be the roots of $x^2 - 5x + 1$, let r_3, r_4, r_5 be roots of $x^3 - 7x + 10$, and let $r_6 = -1$. Consider the isomorphism

$$A_{nf} \to \mathbb{Q}(r_1) \oplus \mathbb{Q}(r_3) \oplus \mathbb{Q}$$

given by $g(x) \mapsto (g(r_1), g(r_3), g(r_6))$. The image of δ under this isomorphism is

$$(\delta(r_1), \delta(r_3), \delta(-1)) = (z_1^2, z_3^2, -7).$$

For primes p splitting completely in L, these three elements z_1^2, z_3^2, and -7 are actually in $(\mathbb{Q}_p^*)^2$ (their square roots z_1, z_3, and z_6 lie in L). So in fact the image of $g(x)$ lies in $((A_{nf} \otimes \mathbb{Q}_p)^*)^2$, so it is zero in $H_f \otimes \mathbb{Q}_p$; hence it is trivial in the image of $\Delta_{\mathbb{Q}_p}$.

At the primes $p = \infty, 2, 7, 739$, we notice that n is a square in $\mathbb{Q}_p^*$; so the fact that δ lies in $\Delta_{\mathbb{Q}_p}(J_n(\mathbb{Q}_p)/2J_n(\mathbb{Q}_p))$ follows from the fact that it lies in $\Delta_{\mathbb{Q}_p}(J_1(\mathbb{Q}_p)/2J_1(\mathbb{Q}_p))$. So δ does indeed lie in $\text{Sel}^{(2)}(\mathbb{Q}, J_n)$.

Finally, the associated surfaces X_δ and V_δ are the same for J_n as they are for J_1; since X_δ has no rational points, this shows as before that δ maps to a nontrivial element of $\text{Ш}(\mathbb{Q}, J_n)$. This completes the proof. $\square$

6. Connections with Del Pezzo surfaces of degree 4

In this section, we consider the odd-degree model C' of C obtained by sending the rational point $(-1, 0)$ to infinity. Its equation is

$$w^2 = (7u^2 - 7u + 1)(16u^3 - 4u^2 - 3u + 1),$$

via the change of variables $w = y/(x+1)^3$, $u = 1/(x+1)$. Here we prove a general lemma about the relationship between these two curves.

Lemma 6.1. *Consider a hyperelliptic curve C_1 over a number field k with equation*

$$y^2 = f_5(x)(x - a).$$

Let C_2 be the odd-degree model of this curve, given by the equation

$$w^2 = u^5 f_5\left(\frac{1}{u} + a\right),$$

where $w = y/(x-a)^3$, $u = 1/(x-a)$. Let $f(x)$ be the sextic polynomial defining C_1 and $g(u)$ the quintic polynomial defining C_2. Let $\delta \in \mathrm{Sel}^{(2)}(k, \mathrm{Jac}\, C_1)$, considered as in [17] as a subgroup of $A_f^*/(A_f^*)^2 k^*$, and let β be an element in $\mathrm{Sel}^{(2)}(k, \mathrm{Jac}\, C_2)$, considered as in [17] as a subgroup of $A_g^*/(A_g^*)^2$. There is a natural isomorphism $\mathrm{Sel}^{(2)}(k, \mathrm{Jac}\, C_1) \to \mathrm{Sel}^{(2)}(k, \mathrm{Jac}\, C_2)$; suppose it sends δ to β. Let W_β be the intersection of two quadrics obtained as the projectivization of the set

$$\mathcal{W}_{g,\beta} = \{s(u) \in A_g : \beta(u)s(u)^2 \equiv \text{quadratic (mod } g)\}$$

(cf. [6] and [3]). Then the K3 surface V_δ obtained from C_1 is a double cover of W_β, which is a smooth Del Pezzo surface of degree 4. It ramifies over the projectivization of

$$\{s(u) \in A_g : \beta(u)s(u)^2 \equiv \text{linear (mod } g)\}.$$

Proof. Note that $k[x]/(f_5(x)) \cong k[u]/(g(u))$. Now the Chinese Remainder Theorem gives a natural isomorphism between $A_f^*/(A_f^*)^2 \mathbb{Q}^*$ and $A_g/(A_g^*)^2$, as the first group is isomorphic to

$$\frac{(k[x]/f_5(x))^* \oplus k^*}{\text{squares} \cdot k^*}$$

and the second group is isomorphic to

$$\frac{(k[u]/(g(u)))^*}{\text{squares}}.$$

It is not hard to see that this isomorphism restricts to an isomorphism ϕ: $\mathrm{Sel}^{(2)}(k, \mathrm{Jac}\, C_1) \to \mathrm{Sel}^{(2)}(k, \mathrm{Jac}\, C_2)$ (where these Selmer groups are realized, as in [17], as subgroups of $A_f^*/(A_f^*)^2 k^*$ and $A_g/(A_g^*)^2$, respectively). (As usual, condition ($\ddagger$) is immediate from the factorization of f.)

The fact that W_β is a smooth Del Pezzo surface of degree 4 is Lemma 17 of [3]. Now suppose $q \in \mathcal{V}_{f,\delta}$, so that δq^2 is congruent to a quadratic polynomial c mod f. Let $c_1(u) = u^2 c(1/u + a)/\delta(a)$; then c_1 is also quadratic. If $\beta = \phi(\delta)$, then

$$\beta(u) \equiv u^6 \delta(1/u + a)/\delta(a) \text{ mod } (A_g^*)^2,$$

and if we choose this representative polynomial for the class of β, we see that the polynomial $s(u)$, defined by the formula

(5) $$s(u) \equiv u^{-2} q(1/u + a) \text{ mod } g(u),$$

is in $\mathcal{W}_{g,\beta}$, because $\beta(u)s(u)^2 \equiv c_1(u) \pmod{g(u)}$. Note that $s(u)$ is well defined, because u is invertible mod $g(u)$.

So (5) gives a map $\mathcal{V}_{f,\delta} \to \mathcal{W}_{g,\beta}$, which induces a map $V_\delta \to W_\beta$. Now consider $s(u) \in \mathcal{W}_{g,\beta}$, and suppose that $\beta s^2 \equiv c_1 \text{ mod } g$. Let $r_1, \ldots, r_6$ be the roots of f in $\overline{k}$, where $r_6 = a$. Now $q \in \mathcal{V}_{f,\delta}$ maps to s if and only if

$$q(r_i) = \frac{1}{(r_i - a)^2} s\left(\frac{1}{r_i - a}\right), \quad 1 \le i \le 5.$$

Note that the quadratic polynomial associated to q is $c(x) = \delta(a)(x-a)^2 c_1(1/(x-a))$. So if q is to lie in $\mathcal{V}_{f,\delta}$, we must have that $q(a)^2$ is the leading term of c_1. Generically there are two choices for the square root of this leading term (these choices coincide when the leading term is 0). The result follows. □

As mentioned above, the lemma implies that if W_β has a Brauer-Manin obstruction to rational points, then so does V_δ, and if W_β fails the Hasse principle, then so does V_δ. So the "$K3$ method" of exhibiting explicit elements of III[2] will work whenever the "Del Pezzo method" of [6] and [11] works. (Of course, the $K3$ method also works more generally; it applies to any genus-2 curve $y^2 = f(x)$, while the Del Pezzo method works only for curves with odd-degree models. The example given in [12] is an example of an application of the $K3$ method to a curve without an odd-degree model.)

For the curve $y^2 = (x^2 - 5x + 1)(x^3 - 7x + 10)(x+1)$ and specific choice of δ given in (4), this construction produces a Del Pezzo surface W_β with points everywhere locally. As it happens, however, Logan's program for Del Pezzo surfaces ([11]) shows that W_β has no Brauer-Manin obstruction to rational points. We expect that it satisfies the Hasse principle as well (although the size of the coefficients in the defining equations for W_β precludes a successful search for rational points of small naive height). In any case, this shows that the $K3$ method is in fact strictly stronger than the Del Pezzo method, even in the case when both methods apply.

References

1. Paola Argentin. *Sur certaines surfaces de Kummer*. Ph.D. thesis, Université de Genève, 2006.
2. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993), homepage at `http://magma.maths.usyd.edu.au/magma/`. MR1484478
3. M. J. Bright, N. Bruin, E. V. Flynn, and A. Logan. The Brauer-Manin obstruction and III [2]. *LMS J. Comp. Math.*, 10:354–377, 2007. MR2342713 (2008i:11087)
4. Martin Bright. *Computations on diagonal quartic surfaces*. Ph.D. thesis, Cambridge University, 2002.
5. Martin Bright. Efficient evaluation of the Brauer-Manin obstruction. *Math. Proc. Camb. Phil. Soc.*, 142(1):13–23, 2007. MR2296387 (2007k:14026)
6. Nils Bruin and E. V. Flynn. Exhibiting SHA[2] on hyperelliptic Jacobians. *J. Number Theory*, 118:266–291, 2006. MR2225283 (2006m:11091)
7. J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Cambridge University Press, 1996. London Math. Soc. Lecture Note Series 230. MR1406090 (97i:11071)
8. Patrick Corn. *Del Pezzo surfaces and the Brauer-Manin obstruction*. Ph.D. thesis, University of California, Berkeley, 2005.
9. Patrick Corn. The Brauer-Manin obstruction on Del Pezzo surfaces of degree 2. *Proc. London Math. Soc.*, 95(3):735–777, 2007. MR2368282 (2009a:14027)
10. Andrew Kresch and Yuri Tschinkel. On the arithmetic of del Pezzo surfaces of degree 2. Proc. London Math. Soc. (3) 89(3):545–569, 2004. MR2107007 (2005h:14060)
11. Adam Logan. MAGMA algorithm for computing the Brauer-Manin obstruction on a Del Pezzo surface of degree 4. `http://www.liv.ac.uk/∼adaml/math/index.html`, 2004.
12. Adam Logan and Ronald van Luijk. Nontrivial elements of Sha explained through $K3$ surfaces. *Math. Comp.*, 78:441–483, 2009. MR2448716
13. James Milne. Class field theory. Online lecture notes, `http://www.jmilne.org/math/CourseNotes/math776.pdf`, 1997.
14. B. Poonen and M. Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. Math.*, 150:1109–1149, 1999. MR1740984 (2000m:11048)
15. Bjorn Poonen and E. F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997. MR1465369 (98k:11087)

16. Alexei Skorobogatov. *Torsors and rational points*. Cambridge University Press, Cambridge, 2001. Cambridge Tracts in Mathematics, 144. MR1845760 (2002d:14032)

17. Michael Stoll. Implementing 2-descent on Jacobians of hyperelliptic curves. *Acta Arith.*, 98:245–277, 2001. MR1829626 (2002b:11089)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GEORGIA 30602-7403
  E-mail address: `corn@math.uga.edu`
  Current address: Department of Mathematics and Computer Science, St. Mary's College of Maryland, 18952 E. Fisher Road, St. Mary's City, Maryland 20686-3001
  E-mail address: `pkcorn@smcm.edu`