Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Number Theory 118 (2006) 266–291
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Exhibiting SHA[2] on hyperelliptic Jacobians

N. Bruin [a,*,1], E.V. Flynn [b,2]

[a] *Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6*
[b] *Mathematical Institute, University of Oxford, 24–29 St. Giles, Oxford OX1 3LB, UK*

Received 8 July 2005
Available online 1 December 2005
Communicated by Nils Bruin

Abstract

We discuss approaches to computing in the Shafarevich–Tate group of Jacobians of higher genus curves, with an emphasis on the theory and practice of visualisation. Especially for hyperelliptic curves, this often enables the computation of ranks of Jacobians, even when the 2-Selmer bound does not bound the rank sharply. This was previously only possible for a few special cases. For curves of genus 2, we also demonstrate a connection with degree 4 del Pezzo surfaces, and show how the Brauer–Manin obstruction on these surfaces can be used to compute members of the Shafarevich–Tate group of Jacobians. We derive an explicit parametrised infinite family of genus 2 curves whose Jacobians have nontrivial members of the Shafarevich–Tate group. Finally, we prove that under certain conditions, the visualisation dimension for order 2 cocycles of Jacobians of certain genus 2 curves is 4 rather than the general bound of 32.

MSC: primary 11G30; secondary 11G10; 14H40

Keywords: Higher genus curves; Jacobians; Visualisation; Brauer–Manin obstruction; Shafarevich–Tate group

* Corresponding author.
E-mail addresses: nbruin@cecm.sfu.ca, nbruin@sfu.ca (N. Bruin), flynn@maths.ox.ac.uk (E.V. Flynn).
[1] Partially supported by an NSERC grant.
[2] Supported by EPSRC grant GR/R82975/01.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2005.10.007

1. Introduction

In this article, we concern ourselves with the problem of determining the free rank of the Mordell–Weil group $J(K)$ of an Abelian variety J over a number field K. There are two main methods available for this problem:

(1) *Analytic methods*. When $K = \mathbb{Q}$ and $\dim J = 1$ then J is known to be *modular*. Furthermore, if the analytic rank of $J(\mathbb{Q})$ is at most 1 then, due to work of Kolyvagin, Gross and Zagier (see [15,16,19]), the Birch and Swinnerton-Dyer conjecture (BSD) is known to hold and therefore $\operatorname{rk} J(\mathbb{Q})$ can be read off from the L-series associated to J. If the analytic rank of $J(\mathbb{Q})$ is greater than 1, BSD still predicts that $\operatorname{rk} J(\mathbb{Q})$ should be computable via this analytic route.
For $\dim J > 1$ or $K \neq \mathbb{Q}$, the Abelian variety J is not necessarily modular. When it is, however, one can get some information conditional on BSD, see [1].
While analogues of BSD can still be conjectured to hold for non-modular Abelian varieties, we are far from making such analytic methods unconditional.
(2) *Descent methods*. Let $m \in \mathbb{Z}_{>1}$. Apart from torsion, $\operatorname{rk} J(K)$ can be read off from $\#J(K)/mJ(K)$. The group $J(K)/mJ(K)$ can be approximated by a local (or adelic) analogue, the *Selmer group* $S^{(m)}(J/K)$, which is effectively computable. Since $\#J(K)/mJ(K) \leqslant \#S^{(m)}(J/K)$, the Selmer group can provide an upper bound on $\operatorname{rk} J(K)$.

Due to failures of the local-to-global principle, the bounds obtained from Selmer groups need not be sharp. The Shafarevich–Tate group of J over K measures this failure and the standard exact sequence

$$0 \to J(K)/mJ(K) \to S^{(m)}(J/K) \to Ш(J/K)[m] \to 0$$

gives the relation between the Selmer group and $J(K)/mJ(K)$.

If $\delta \in S^{(m)}(J/K)$ does come from an element in $J(K)/mJ(K)$, one can show this by exhibiting a point $P \in J(K)$ that maps to δ. Since such a point is of finite height, one can find it in finite time.

The converse is harder to decide. Suppose that $\delta \in S^{(m)}(J/K)$ represents a suspected nontrivial element in $Ш(J/K)[m]$. Since we do not have an upper bound on the smallest height of a possible point $P \in J(K)$ that maps to δ, a failure to find such a point does not prove that δ is not in the image of $J(K)$.

Several methods are available to refine the bounds on $\#J(K)/mJ(K)$ and thus possibly decide if $\delta \in S^{(m)}(J/K)$ represents a nontrivial element in $Ш(J/K)$.

(1) *Different descents.* Choose n distinct from m (say coprime), and compute $S^{(n)}(J/K)$. If $Ш(J/K)[n]$ is trivial, then the ensuing bound on $J(K)/nJ(K)$ will be sharp. This will then give an upper bound on $\operatorname{rk} J(K)$ that is lower than the previous one, and show that $Ш(J/K)[m]$ is nontrivial. If one can find points in $J(K)$ that generate the image in $S^{(m)}(J/K)$ then one can show that δ is not in it and therefore represents a nontrivial element of $Ш(J/K)[m]$ (see [22]).

One problem is that, while in principle Selmer groups are effectively computable, in practice it is very computationally intensive. For general elliptic curves only $m = 2, 3$ are feasible. Another problem is that it is only conjectured that $Ш(J/K)$ is finite. In principle it could have torsion of all orders.

The computational complexity can be alleviated in special cases, using isogeny-Selmer groups. For example, following [26,28], the $(1-\zeta_5)$-Selmer group shows that the Mordell–Weil group of the Jacobian J of $Y^2 = X^5 - 13$ has rank 0, where ζ_5 is a primitive fifth root of unity. On the other hand, using the techniques in [27], the 2-Selmer bound on the rank is 2, proving the existence of a nontrivial member of $Ш(J/\mathbb{Q})[2]$.

(2) *Deeper descents.* Choose $n = m^e$ for some $e > 1$ and compute $S^{(n)}(J/K)$. If $Ш(J/K)[m]/(m^{e-1})Ш(J/K)[m^e]$ is nontrivial then this leads to a sharper bound on $\operatorname{rk} J(K)$. By comparing $S^{(m)}(J/K)$ and $m^{e-1}S^{(m^e)}(J/K)$ one can immediately recognise elements that represent nontrivial elements in $Ш(J/K)[m]/(m^{e-1})Ш(J/K)[m^e]$. The same computational restrictions as for the method above apply. However, for elliptic curves over number fields, 4-descent (or second descent) is practically feasible (see [8,20, 29]).

(3) *Isogenous Abelian varieties.* If J and J' are isogenous Abelian varieties then $\operatorname{rk} J(K) = \operatorname{rk} J'(K)$. One may well have that $Ш(J/K)[m] \not\simeq Ш(J'/K)[m]$ if the degree of the isogeny is not coprime to m. Therefore, the bounds on $\operatorname{rk} J(K)$ from $S^{(m)}(J/K)$ and $S^{(m)}(J'/K)$ may well be distinct. Since Abelian varieties generally have very few isogenies apart from the multiplication maps, which yield no useful information in this setting, this method is rather limited in its applicability.

For elliptic curves, it is fairly easy to obtain these isogenies. For more general Abelian varieties, say Jacobians of curves, not all isogenous Abelian varieties will again be Jacobians of curves. That can make computations rather complicated. For hyperelliptic curves of genus 2, there are *Richelot isogenies*. In particular, for a curve

$$\begin{aligned} C\colon\quad Y^2 &= G_1G_2G_3 \\ &= \big(g_{12}X^2 + g_{11}X + g_{10}\big)\big(g_{22}X^2 + g_{21}X + g_{20}\big)\big(g_{32}X^2 + g_{31}X + g_{30}\big), \end{aligned} \tag{1}$$

the Jacobian of C is isogenous to the Jacobian of

$$D\colon\quad \Delta Y^2 = \big(G_2'G_3 - G_2G_3'\big)\big(G_3'G_1 - G_3G_1'\big)\big(G_1'G_2 - G_1G_2'\big), \tag{2}$$

where $\Delta = \det(g_{ij})$. See [6] for a description of this isogeny. If one performs a complete 2-descent on both $\operatorname{Jac}(C)$ and $\operatorname{Jac}(D)$ then one can sometimes demonstrate a nontrivial member of $Ш(\operatorname{Jac}(C)/\mathbb{Q})$. For example, consider the curve $C\colon Y^2 = (X^2+4)(X^2-45)(2X^2-98X-41)$. The 2-Selmer group bounds the rank of $\operatorname{Jac}(C)(\mathbb{Q})$ by 4, whereas the same computation on the Richelot-isogenous Jacobian of the curve $\mathcal{D}$: $Y^2 = X(X^2+X-4)(X^2-X+45)$ bounds the rank by 0, proving that $Ш(\operatorname{Jac}(C)/\mathbb{Q})[2]$ has order 16 (see also [14] for other examples of $Ш(\operatorname{Jac}(C)/\mathbb{Q})[2]$ killed by isogenies, and [23, Section 6], for a Selmer group computation using isogenies).

(4) *Visualisation.* Since Abelian varieties in general have very few isogenies, the idea above has only very limited applicability. However, given an Abelian variety J, we can construct another Abelian variety B such that the product $J \times B$ does have a nontrivial isogenous Abelian variety A. The relevant groups for product varieties are easily expressed in terms of the factors:

$$(J \times B)(K) \simeq J(K) \times B(K)$$
$$S^{(m)}(J \times B/K) \simeq S^{(m)}(J/K) \times S^{(m)}(B/K)$$
$$Ш(J \times B/K) \simeq Ш(J/K) \times Ш(B/K).$$

It follows that $\operatorname{rk} A(K) = \operatorname{rk} J(K) + \operatorname{rk} B(K)$. By comparing $S^{(m)}(A/K)$ and $S^{(m)}(J \times B/K)$ one may be able to conclude that $Ш(J \times B/K)[m]$ is nontrivial and a further analysis may allow the conclusion that $Ш(J/K)[m]$ is nontrivial.

For applications of these methods to modular Abelian varieties, see [1,2,13]. For applications to elliptic curves over number fields, see [7,14].

(5) *Annihilation by base field extension.* This is really just a special case of method (4), where A is taken to be the Weil restriction of scalars of J with respect to a suitable extension L of K in the following way. Let $\delta \in S^{(m)}(J/K)$ represent a nontrivial element $\overline{\delta} \in Ш(J/K)[m]$. As we will see in Section 2, we have $Ш(J/K) \subset H^1(K, J)$. We take L to be an extension such that the restriction of $\overline{\delta}$ from $\operatorname{Gal}(\bar{K}/K)$ to $\operatorname{Gal}(\bar{K}/L)$ is trivial. See [7] for a full account of the situation where $m = 2$ and $\dim J = 1$.

Remark 1. The term *visualisation* under method (4) originates from Mazur and refers to the fact that the homogeneous spaces represented by the relevant elements of $S^{(m)}(J/K)$ occur as *fibres* of the map $A \to B$. This description of the homogeneous spaces is considered so explicit that the homogeneous space is *visualised*. Given a short exact sequence of Abelian varieties

$$0 \to J \to A \to B \to 0,$$

one defines the *visualised subgroup* of $H^1(K, J)$ by

$$0 \to \operatorname{Vis}_K(J \to A) \to H^1(K, J) \to H^1(K, A) \to H^1(K, B).$$

It is straightforward to check that for $\delta \in S^{(m)}(J/K)$, one can only expect to prove that the class $\bar{\delta}$ of δ in $Ш(J/K)$ is nontrivial via comparison with $S^{(m)}(A/K)$ if $\bar{\delta} \in \operatorname{Vis}_K(J \to A)$. If that is the case, by abuse of terminology we will say that δ is *visualised* in A.

In this article we will be concerned with extending explicit versions of the methods (4) and (5) to Jacobians of hyperelliptic curves. In Section 4 we develop some general tools to extract information on visualised elements of $Ш(J/K)[m]$. Proposition 6 gives the most powerful relation between $S^{(m)}(J/K)$ and $S^{(m)}(A/K)$.

Independently of visualisation methods, in Sections 5 and 6 we show that if C is a curve of genus 2 with a rational Weierstrass point then $\delta \in H^1(K, J[2])$ has a degree 4 del Pezzo surface V_δ related to it. If $\delta \in S^{(2)}(J/K)$ and V_δ has no rational points then δ represents a nontrivial element of $Ш(J/K)[2]$. We can use the Brauer–Manin obstruction on del Pezzo surfaces of degree 4 to infer information about $Ш(\mathrm{Jac}(C)/K)[2]$ for curves C of genus 2. In fact, in Section 6 we shall find the following explicit infinite family.

Proposition 2. *Let*

$$\mathcal{C}_{\ell,\lambda}: \quad Y^2 = \ell\big(X^2-2\big)\left(X-\frac{\lambda+2}{\lambda+1}\right)(X-\lambda)\left(X-\frac{3\lambda+4}{2\lambda+3}\right),$$

and let $J_{\ell,\lambda}$ be the Jacobian of $\mathcal{C}_{\ell,\lambda}$. There exists a nontrivial member of $Ш(J_{-2k,-13/8}/\mathbb{Q})[2]$ for any k of the form

$$k = 80\big(t^5-t+1\big)^2\big(\big(t^5-t+1\big)^2+10\big)^2+\big(\big(t^5-t+1\big)^2-10\big)^4, \tag{3}$$

for any $t \in \mathbb{Q}$. Furthermore, $J_{-2k,-13/8}$ is absolutely simple.

There are also infinite families of nontrivial $Ш(J/\mathbb{Q})[2]$ in [10,21], but the nature of our examples (being a family of twists) and the method of proof (using the Brauer–Manin obstruction on degree 4 del Pezzo surfaces) is quite different.

In Section 7 we study the applicability of method (5) to Jacobians J of hyperelliptic curves C of genus d with a rational Weierstrass point.

As a consequence, we recover a proof of [2, Proposition 2.3] that any element of $H^1(K, J)$ represented by $\delta \in H^1(K, J[2])$ can be visualised in an Abelian variety of dimension at most $d2^{2d}$. In fact, we prove the small improvement that if $\delta \in S^{(2)}(J/K)$ and C has at least $\dim J$ rational Weierstrass points then it can be visualised in an Abelian variety of dimension at most $d2^{2d-1}$.

Finally, in Section 8, we consider visualising varieties that are Jacobians of hyperelliptic curves, obtained via a fibre product construction. We prove:

Proposition 3. *Let C_1: $y^2 = f(x)$ be a curve of genus 2 over a number field K, with a rational Weierstrass point at $x = \infty$ and let $J = \mathrm{Jac}(C_1)$. Let $\delta \in H^1(K, J[2])$ be such that V_δ has a rational point. Then δ can be visualised in the Jacobian of a genus 4 hyperelliptic curve.*

Conditional on the conjecture that the Brauer–Manin obstruction is the only obstruction for del Pezzo surfaces having rational points, it would follow that one can either show that δ represents a nontrivial element in $H^1(K, J)$ by local methods or the Brauer–Manin obstruction on V_δ, or δ can be visualised in an Abelian variety of dimension 4. This is better than than the general bound of 32 on the visualisation dimension.

2. Review of Selmer groups

Let K be a number field and let J be an Abelian variety over K of dimension g. The Mordell–Weil theorem asserts that $J(K)$ is a finitely generated Abelian group:

$$J(K) \simeq \mathbb{Z}^r \times J(K)^{\mathrm{tor}}.$$

Furthermore, the finite subgroup $J(K)^{\mathrm{tor}}$, consisting of the rational points of finite order, is in theory effectively computable and is quite easily determined in many practical cases. Therefore, from the basic observation that:

$$\#J(K)/mJ(K) = m^r \cdot \#\big(J(K)^{\mathrm{tor}}/mJ(K)^{\mathrm{tor}}\big),$$

it is clear that the free rank r of $J(K)$ can be read off from $J(K)/mJ(K)$. The latter has a cohomological interpretation in terms of Galois cohomology, via the standard exact sequence

$$0 \to J(K)/mJ(K) \to H^1\big(K, J[m]\big) \to H^1(K, J).$$

Therefore, if we can determine $\mathrm{Ker}(H^1(K, J[m]) \to H^1(K, J))$, we can compute the free rank r of $J(K)$. Unfortunately, there is no known algorithm to compute this kernel. We can, however, approximate it everywhere locally. Let p be a prime (finite or infinite) of K and consider the restriction map $H^1(K, J) \to H^1(K_p, J)$. Taking the product over all possible primes p, we can define the *m-Selmer group* of J over K as

$$S^{(m)}(J/K) := \mathrm{Ker}\left(H^1\big(K, J[m]\big) \to \prod_p H^1(K_p, J)\right).$$

This group is finite, effectively computable and $J(K)/mJ(K) \hookrightarrow S^{(m)}(J/K)$. Therefore, we can effectively compute an upper bound for r.

The obstruction for this bound to equal the actual rank is contained in the K-cocycles that restrict to trivial ones at all primes p. This is defined to be the *Shafarevich–Tate group* of J over K:

$$Ш(J/K) := \mathrm{Ker}\left(H^1(K, J) \to \prod_p H^1(K_p, J)\right).$$

The m-torsion of this group is easily seen to be the exact obstruction. We have the exact sequence

$$0 \to J(K)/mJ(K) \to S^{(m)}(J/K) \to Ш(J/K)[m] \to 0.$$

3. Isogenies and Selmer groups

Let J be an Abelian variety over a number field K and let $\phi: J \to A$ be an isogeny, defined over K. Let $\hat{\phi}: A \to J$ be an isogeny such that $\phi \circ \hat{\phi} = (mn)|A$ and $\hat{\phi} \circ \phi = (mn)|J$. If J and A are principally polarised then one can take $\hat{\phi}$ to be the isogeny dual to ϕ. Otherwise, one has to compose with the appropriate polarisations.

It is easy to see that if J and A are isogenous Abelian varieties, then $\operatorname{rk} J(K) = \operatorname{rk} A(K)$. The same does not hold for Selmer-groups. In fact, the maps $\phi, \hat{\phi}$ also induce the commutative diagram

$$\begin{array}{ccc} H^1(K,J) & \xrightarrow{\phi} & H^1(K,A) \\ & \searrow^{mn} & \downarrow{\scriptstyle \hat{\phi}} \\ & & H^1(K,J) \end{array}$$

which suggests one may well have that

$$Ш(J/K)[m] \subset \operatorname{Ker}\bigl(H^1(K,J) \to H^1(K,A)\bigr).$$

Therefore, it may well happen that $\#Ш(J/K)[m] \neq \#Ш(A/K)[m]$ and therefore that $S^{(m)}(J/K)$ and $S^{(m)}(A/K)$ yield different bounds on the free rank.

Indeed, examples of this happening abound.

Example 4. Let $K = \mathbb{Q}$ and consider the isogeny

$$\begin{aligned} \phi: \quad J:\ y^2 = x^3 - 8x^2 + x \quad &\to \quad A:\ v^2 = u^3 + 16u^2 + 60u, \\ (x, y) \quad &\mapsto \quad \left(\frac{x^2 - 8x + 1}{x}, \frac{x^2 y - y}{x^2}\right). \end{aligned}$$

One can show that

$$\begin{aligned} S^{(2)}(J/\mathbb{Q}) &= (\mathbb{Z}/2\mathbb{Z})^3, & S^{(2)}(A/\mathbb{Q}) &= (\mathbb{Z}/2\mathbb{Z})^2, \\ J(\mathbb{Q})^{\mathrm{tor}} &= (\mathbb{Z}/2\mathbb{Z}), & A(\mathbb{Q})^{\mathrm{tor}} &= (\mathbb{Z}/2\mathbb{Z})^2. \end{aligned}$$

It follows that $\operatorname{rk} J(\mathbb{Q}) = \operatorname{rk} A(\mathbb{Q}) = 0$ and that $Ш(J/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$, while $Ш(A/\mathbb{Q})[2] = 0$.

4. Abelian product varieties

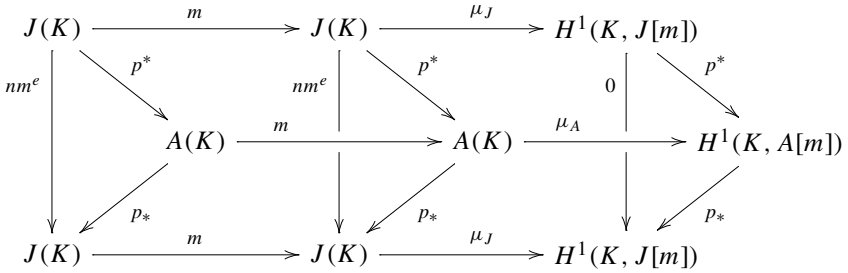
As we have seen in the previous section, one way to exhibit nontrivial elements of $Ш(J/K)$ is by comparing information obtained from isogenous Abelian varieties. This is a rather limited strategy, since in general, Abelian varieties have no nontrivial isogenies

defined over the base field. One can interpret the phenomenon that Cremona and Mazur (see [13]) labelled as *visualisation* as a generalisation of the construction discussed in Section 3, where one no longer requires the maps to be isogenies. Therefore, consider we have Abelian varieties J and A, such that we have two morphisms

$$p^*: J \to A \quad \text{and} \quad p_*: A \to J$$

such that $p_* \circ p^* = (nm^e)|_J$. We will assume that n is coprime to m. In most applications, m will be prime (in fact, m will be 2). We will also assume that p^* is injective.

These maps link the m-descent sequences of J and A:



We consider the subgroup $G \subset H^1(K, J[m])$ such that for all $\delta \in G$, there exists a point $b \in A(K)$ with $p_*(b) = 0$ and $\mu_A(b) = p^*(\delta)$.

Note that for $j \in J[nm^e](K)$, $\delta = \mu_J(j)$ and $b = p^*(j)$, we have $\mu_A(b) = p^*\delta$ and $p_*(b) = 0$, so $\mu_J(J[nm^e](K)) \subset G$ is not a restriction. We write $B(K) = \{a \in A(K)\colon\ p_*(a) = 0\}$.

Remark 5. In the situation where $n = e = 1$ and J and B are both Abelian subvarieties of A and $J \times B$ is isogenous to A, we have that G represents exactly the *visible* part of $H^1(K, J)$, as defined in Remark 1. If we write $q_*: A \to B$ for the relevant projection onto B, we have that an element $\bar{\delta} \in \mathrm{Vis}_K(J \to A)$, interpreted as a principal homogeneous space of J, is isomorphic to $q_*^{-1}(b)$. In fact our goal will be to minimize references to B and express all relevant data in terms of J and A.

The general idea is that $\operatorname{rk} A(K) \geqslant \operatorname{rk} B(K) + \operatorname{rk} J(K)$. Thus, a lower bound on $\operatorname{rk} B(K)$ together with an upper bound on $\operatorname{rk} A(K)$ yields an upper bound on $\operatorname{rk} J(K)$. In the following propositions we make this relation a little more precise. When $e = 1$ there is a very close relation between $G \cap \mu_J(J(K))$ and $\mu_A(A(K))$. We get a very satisfying result:

Proposition 6. *With the notation as above and with $e = 1$, we have*

$$G \cap \mu_J\big(J(K)\big) \subset p_*\mu_A\big(A(K)\big) + \mu_J\big(J[m](K)\big).$$

Proof. Suppose that $\delta \in \mu_J(J(K)) \cap G$. Then there is a point $j \in J(K)$ with $\mu_J(j) = \delta$ and a point $b \in A(K)$ with $p_*(b) = 0$ and $\mu_A(b) = p^*(\delta)$. It follows that there is a point $a \in A(K)$ such that

$$ma = p^*(j) - b.$$

It follows that $mp_*(a) = mnj$ and hence that $nj \in p_*(a) + J[m](K)$. The statement follows by applying μ_J and by noting that multiplication by n is an invertible operation on $H^1(K, J[m])$. □

One can use this proposition in the following way. Suppose one suspects that $\delta \in S^{(m)}(J/K)$ represents some nontrivial element of $Ш(J/K)$. If one can design an Abelian variety $A \xrightarrow{p_*} J$ such that $\delta \in G$, then one can test if $\delta \in p_*\mu_A(A(K)) + \mu_J(J[m](K))$. If not, then Proposition 6 guarantees that $\delta \notin \mu_J(J(K))$. See Example 19 for an application.

When $e > 1$, control is less complete. The assumptions in the following theorem are often met in practice. It is also possible to get similar results for other conditions.

Proposition 7. *With the notation above and with the assumption that* $A[m](K) \subset p^*(J(K)) + \mathrm{Ker}(p_*)$*, we have*

$$\#J(K)/mJ(K) \leqslant \frac{\#(\mu_A(A(K)) \cap p_*^{-1}(G)) \cdot \#\mathrm{Ker}(p^*|_{\mu_J(J(K))}) \cdot \#J[m](K)}{\#p^*G}.$$

Proof. First note that $p^*(J(K))$ gives rise to a subgroup with $\mu_A(p^*(J(K))) = p^*(\mu_J(K))$. Note furthermore that $p_*(\mu_A(p^*(J(K)))) = 0 \subset G$.

Writing $B = \mathrm{Ker}(p_*|_A)$, we have $p^*(G) \subset \mu_K(B(K))$. Note that $B(K) \cap p^*(J(K)) = p^*(J[nm^e](K))$. Therefore, writing $V' = B(K) + p^*J(K)$, we see that

$$\#V'/mV' \geqslant \frac{\#p^*(\mu_J(J(K))) \cdot \#p^*(G)}{\#p^*(J[nm^e](K))/mp^*(J[nm^e](K))}.$$

Let V be the m-saturation of $V' \subset A(K)$, that is,

$$V = \left\{a \in A(K)\colon \text{ there is an exponent } f \geqslant 0 \text{ such that } m^f a \in V'\right\}.$$

It easy to see that $\#V/mV \geqslant \#V'/mV'$. Because V is m-saturated in $A(K)$, it follows that $\mu_A(V) \simeq V/mV$. It remains to show that $p_*(\mu_A(V)) \subset G + \mu_J(J[nm^e](K))$.

Suppose that $a \in V$, i.e., $m^f a = b - p^*(j)$ for some $b \in B(K)$ and $j \in J(K)$. Applying p_*, we find $m^f p_*(a) = nm^e j$.

We see that if $f < e$ then $\mu_J(nm^{e-f} j) = 0$ and thus $p_*(\mu_A(a)) \in \mu_J(J[m^f](K))$.

For $f \geqslant 1$ we need $\mu_A(b - p^*(j)) = 0$, and thus $p^*(\mu_J(j)) = \mu_A(b) \in p^*(G)$. This implies that $\mu_J(j) \in G$.

If $f = e$ we find $m^e p_*(a) = nm^e j$, so $\mu_A(p_*(a)) \in n\mu_J(j) + \mu_J(J[m^e](K)) \subset G$.

If $f > e$ we define $\tilde{j} = -p_*a$ and $\tilde{b} = nm^e a - p^*p_*a \in B(K)$, we have $m(\tilde{b} - p^*\tilde{j}) = nm^{e+1}a$. Using that $A[m](K) \subset p^*J(K) + B(K)$, it follows that $nm^e a \in p^*J(K) + B(K)$. □

In order to get a cleaner statement, we make some further assumptions that often apply.

Corollary 8. *With the notation above, suppose that* $p^*: S^{(m)}(J/K) \to S^{(m)}(A/K)$ *is injective. Suppose furthermore that* $J[m](K) = \{0\}$ *and* $A[m](K) = \{0\}$. *Then*

$$\#J(K)/mJ(K) \leqslant \frac{\#(S^{(m)}(A/K) \cap p_*^{-1}(G))}{\#p^*G}.$$

Proof. Of course, the corollary follows by specialising Proposition 7. We give an independent proof as well. Using that $p_*p^*\mu_J(J(K)) = \{0\} \subset G$, it follows that

$$\mu_J\big(J(K)\big) \simeq p^*\mu_J\big(J(K)\big) \subset \mu_A\big(A(K)\big) \cap p_*^{-1}(G).$$

On the other hand, note that $p_*(B(K)) = \{0\}$, whereas $p_*p^*J(K) = nm^eJ(K)$. Since $A(K)$ is assumed to be torsion-free, it follows that $B(K)$ is independent of $p^*J(K)$ and that $B(K)$ is saturated in $A(K)$. Hence, we have an exact sequence

$$0 \to \mu_J\big(J(K)\big) \to \mu_A\big(A(K)\big) \to \mu_A\big(B(K)\big).$$

From the definition of G it follows that $p^*G \subset \mu_A(B(K))$. The corollary follows by observing that $\mu_A(A(K)) \subset S^{(m)}(A/K)$. □

Remark 9. The main feature of the corollary above is that it is not the entire group $S^{(m)}(A/K)$ which appears, but only the part that is mapped onto G by p_*. Should $A(K)$ be unexpectedly larger, or should $Ш(A/K)[m]$ be nontrivial, but represented by elements not in $p_*^{-1}(G)$, then the bounds obtained from the corollary are indeed stronger than what could be obtained from a mere rank bound comparison between A, B and J.

In order to use the corollary one needs information on G. Trivial bounds one can use are $S^{(m)}(A/K) \cap p_*^{-1}(G) \subset S^{(m)}(A/K)$ and $p^*G \supset \{0\}$. By exhibiting points in $B(K)$, one can improve these bounds. Points might be there by construction or one can search for them. See Example 17 for an application of Corollary 8.

5. 2-Selmer groups of hyperelliptic Jacobians

In order to apply the results of Section 4 to Jacobians of hyperelliptic curves, we need a detailed description of their Selmer-groups. We limit our study to curves with a model

$$C: \quad y^2 = f(x) = x^n + f_n x^{n-1} + \cdots + f_0, \quad \text{where } n = 2d+1$$

and $f \in K[x]$ is a square-free polynomial. We allow $d = 1$ as well, so our results apply to elliptic curves and hyperelliptic curves with a rational Weierstrass point.[3]

[3] The advantage being that with a rational Weierstrass point, a nice description of $H^1(K, J[2])$ is readily available. Without it, the analogous construction only yields a quotient of $H^1(J, J[2])$. See [27].

We write $J = \mathrm{Jac}(C)$. Note that a nonzero element $D \in J(K)$ can be represented by polynomials $g_D, h_D \in K[x]$, where g_D is monic and $0 \leqslant \deg h_D < \deg g_D \leqslant d$ such that

$$D = \big(g(x) = 0,\ y = h(x)\big) \cdot C - \big(\deg(g)\big)\infty.$$

We define $A = K[\theta] = K[x]/(f(x))$ and

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

Then $H^1(K, J[2]) \simeq A'/A^{*2}$ and the connecting homomorphism can be given as

$$\begin{aligned} \mu\colon\quad & J(K) \to H^1\big(K, J[2]\big) \\ & D \mapsto (-1)^{\deg(g_D)} g_D(\theta) \quad \text{if } \gcd(g_D, f) = 1. \end{aligned} \tag{4}$$

Note that $\{1, \theta, \ldots, \theta^{2d}\}$ is a basis of A as a K-vector space. If $\delta = \sum \delta_i \theta^i \in A$ represents an element in $\mu(J(K))$, then there exists a monic $g \in K[x]$ of degree $\leqslant d$ and $u_0, \ldots, u_{2d} \in K$ such that

$$g(\theta) = (-1)^{\deg(g)} \delta \left(\sum_{i=0}^{2d} u_i \theta^i \right)^2, \tag{5}$$

and such that there is an $h(x) \in K[x]$ for which

$$\big(g(x) = 0\big) \cdot C = \big(g(x) = 0,\, y = h(x)\big) \cup \big(g(x) = 0,\, y = -h(x)\big).$$

Remark 10. Our goal is to develop methods that allow us to decide whether $\delta \in S^{(2)}(J/K)$ lies in $\mu(J(K))$. Since we assume that $J(K)^{\mathrm{tor}}$ is easy to determine, only the class of δ in $S^{(2)}(J/K)/\mu(J(K)^{\mathrm{tor}})$ is important. In particular, we can multiply δ by elements from $J[2](K)$ if we want. This allows us to ensure that $\gcd(g, f) = 1$.

Furthermore, if $\delta \notin \mu(J(K)^{\mathrm{tor}})$ then δ can only be in $\mu(J(K))$ if $\mathrm{rk}\, J(K) > 0$. This implies that there are infinitely many points $D \in J(K)$ such that $\mu(D) = \delta$ and not all of them will meet the closed condition $\deg(g) < d$. Therefore, we may as well assume that $\deg(g) = d$.

For $\delta \in A^*$ we define $Q_{\delta,i} \in K[u_0, \ldots, u_{2d}]$ by

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

From the discussion above it follows that if $\delta \in \mu(J(K))$ then we can find a rational point on the projective variety

$$V_\delta\colon\ Q_{\delta,d+1}(\underline{u}) = \cdots = Q_{\delta,2d}(\underline{u}) = 0.$$

In order to capture the other conditions, we introduce some notation. We write

$$g(x) = x^d + \frac{Q_{\delta,d-1}(\underline{u})}{Q_{\delta,d}(\underline{u})}x^{d-1} + \cdots + \frac{Q_{\delta,0}(\underline{u})}{Q_{\delta,d}(\underline{u})}$$

and β for the image of x in $K(\underline{u})[x]/(g(x))$. Using the relation $g(\beta) = 0$, we define the rational functions $F_{\delta,i} \in K(\underline{u})$ by

$$f(\beta) = F_{\delta,0}(\underline{u}) + F_{\delta,1}(\underline{u})\beta + \cdots + F_{\delta,d-1}(\underline{u})\beta^{d-1}.$$

Similarly, we expand

$$\left(\sum_{i=0}^{d-1} y_i\beta^i\right)^2 = \sum_{i=0}^{d-1} Y_{\delta,i}(\underline{u}, \underline{y})\beta^i.$$

The remaining conditions on the leading coefficient of g and the fact that g should define a locus on the x-line that splits when pulled back to C can now be expressed as

$$T_\delta: \quad \begin{cases} (u_0 : \cdots : u_{2d}) \in V_\delta, \\ F_{\delta,i}(\underline{u}) = Y_{\delta,i}(\underline{u}, \underline{y}) \quad \text{for } i = 0, \ldots, d-1. \end{cases} \tag{6}$$

Since we divided by the leading coefficient $Q_{\delta,d}(\underline{u})$ to obtain $g(x)$, it would seem we need an additional condition on its square class to ensure that a rational point on T_δ leads to a divisor $D \in J(K)$ with $\mu(D) = \delta$. In fact, this condition is already implied:

Lemma 11. *Suppose that $(\underline{u}, \underline{y}) \in T_\delta(K)$ and that $N_{A/K}\delta \in K^{*2}$. Then there is a $z \in K$ such that*

$$(-1)^d Q_{\delta,d}(\underline{u}) = z^2.$$

Proof. First note that if $Q_{\delta,d}(\underline{u}) = 0$ then $z = 0$ works. However, in that case we would have bigger trouble elsewhere. We assume the conditions of Remark 10.

Note that

$$Q_{\delta,d}(\underline{u})g(\theta) = \sum_{i=0}^{d} Q_{\delta,i}(\underline{u})\theta^i \equiv \delta \pmod{A^{*2}}$$

and, since δ has square norm, it follows that

$$Q_{\delta,d}(\underline{u})^{2d+1} N_{A/K}\big(g(\theta)\big) = N_{A/K}\big(Q_{\delta,d}(\underline{u})g(\theta)\big) \in K^{*2}.$$

On the other hand, we have

$$N_{A/K}\big(g(\theta)\big) = N_{A[\beta]/K}(\theta - \beta) = (-1)^d N_{K[\beta]/K}\big(f(\beta)\big).$$

Since the equations for T_δ imply that $f(\beta)$ is a square in $K[\beta]$, we see that

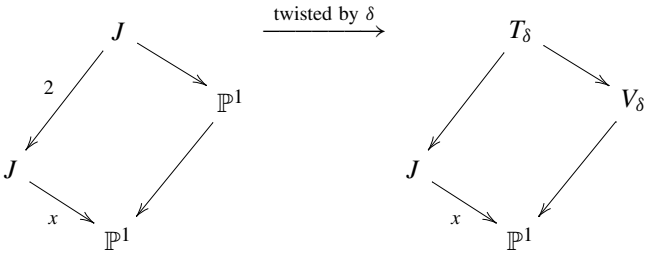
$$(-1)^d N_{A/K}\big(g(\theta)\big) \in K^{*2}.$$

The lemma follows. □

It is clear that if $D \in J(K)$ with $\mu(D) = \delta$ satisfying the conditions of Remark 10 then there is a rational point on T_δ corresponding to D. Conversely, we can write down $g \in K(\underline{u})[x]$ and $h \in K(\underline{u}, \underline{y})[x]$ such that a rational point on T_δ corresponds to a rational divisor given by g, h, provided that $Q_{\delta,d}(\underline{u}) \neq 0$ and that g is coprime to f. Since the latter are open conditions and the construction of T_δ is functorial, one can conclude that T_δ is birational to the homogeneous space corresponding to the class of δ in $H^1(K, J)[2]$, if T_δ is indeed irreducible.

We illustrate the construction in the case of elliptic curves and genus 2 curves.

Example 12. If $d = 1$ we recover the traditional construction of homogeneous spaces for full 2-descent.



We find

$$V_\delta: \quad Q_{\delta,2}(u_0, u_1, u_2) = 0$$

and homogenizing the equations

$$T_\delta: \quad \begin{cases} Q_{\delta,2}(\underline{u}) = 0, \\ Q_{\delta,1}(\underline{u}) = -z^2. \end{cases}$$

We conclude that T_δ can be described as the fibre product $T_\delta = J \times_{\mathbb{P}^1} V_\delta$.

If $\delta \in S^{(2)}(J/K)$ then T_δ has points everywhere locally and therefore V_δ has points everywhere locally as well. Together with Hasse–Minkowski, this implies that V_δ is isomorphic to $\mathbb{P}^1$ over K. Substituting a parametrization of V_δ into T_δ realizes T_δ as the familiar

$$v^2 = \text{quartic} \quad \text{in } u.$$

Example 13. For $d = 2$ the configuration is slightly more complicated. We write $J = \mathrm{Jac}(C)$ and $\mathcal{K} = J/\langle -1 \rangle$ for the associated Kummer surface. We write

$$\iota : C \to C$$
$$(x, y) \mapsto (x, -y)$$

for the hyperelliptic involution on C. A model of the Jacobian J can be obtained by blowing down an exceptional line on $\mathrm{Sym}^2(C)$, the symmetric square of C. We have the following diagram:

$$\begin{array}{ccccc}
C \times C & \longrightarrow & \mathrm{Sym}^2(C) & \xrightarrow{\text{blow down}} & J \\
\downarrow & & \downarrow & & \downarrow \\
C \times C/\langle \iota \times \iota \rangle & \longrightarrow & \mathrm{Sym}^2(C)/\langle \iota \times \iota \rangle & \longrightarrow & \mathcal{K} \\
\downarrow & & \downarrow & & \vdots \\
\mathbb{P}^1 \times \mathbb{P}^1 & \longrightarrow & \mathrm{Sym}^2(\mathbb{P}^1) & = & \mathbb{P}^2
\end{array}$$

The line that is blown down is the image of the antisymmetric embedding

$$C \to C \times C$$
$$P \mapsto (P, x^\iota P).$$

Since the images of the symmetric and the antisymmetric embedding of C coincide in $\mathbb{P}^2$, we see that the induced map $\mathcal{K} \to \mathbb{P}^2$ is only a rational map, because the image of the blown down component is indeterminate. Representing elements of J by divisors of the form

$$\left[\left\{g(x) = g_0 + g_1 x + g_2 x^2 = 0,\ y = h_0 + h_1 x\right\} \cdot C - 2\infty\right]$$

taken with the right kind of multiplicities, coordinates on $\mathbb{P}^2$ can be taken to be $(g_0 : g_1 : g_2)$. We assume for now that $g_2 = 1$ (see Remark 10) and write β for a formal root of g. If $g(x)$ indeed belongs to a point in $J(K)$ then there are $y_0, y_1 \in K$ such that

$$f(\beta) = (y_0 + \beta y_1)^2.$$

Expanding this equation with respect to the K basis $\{1, \beta\}$ and taking a resultant with respect to y_0 yields the equation

$$\begin{aligned}
&\left(g_1^2 - 4g_0\right)y_1^4 + \left(-4f_0 + 2f_1g_1 + 4f_2g_0 - 2f_2g_1^2 - 6f_3g_0g_1 + 2f_3g_1^3 - 4f_4g_0^2\right. \\
&\quad \left. + 8f_4g_0g_1^2 - 2f_4g_1^4 + 10g_0^2g_1 - 10g_0g_1^3 + 2g_1^5\right)y_1^2 \\
&\quad + f_1^2 - 2f_1f_2g_1 - 2f_1f_3g_0 + 2f_1f_3g_1^2 + 4f_1f_4g_0g_1 - 2f_1f_4g_1^3 + 2f_1g_0^2 - 6f_1g_0g_1^2 \\
&\quad + 2f_1g_1^4 + f_2^2g_1^2 + 2f_2f_3g_0g_1 - 2f_2f_3g_1^3 - 4f_2f_4g_0g_1^2 + 2f_2f_4g_1^4 - 2f_2g_0^2g_1
\end{aligned}$$

$$+6f_2g_0g_1^3-2f_2g_1^5+f_3^2g_0^2-2f_3^2g_0g_1^2+f_3^2g_1^4-4f_3f_4g_0^2g_1+6f_3f_4g_0g_1^3$$
$$-2f_3f_4g_1^5-2f_3g_0^3+8f_3g_0^2g_1^2-8f_3g_0g_1^4+2f_3g_1^6+4f_4^2g_0^2g_1^2-4f_4^2g_0g_1^4$$
$$+f_4^2g_1^6+4f_4g_0^3g_1-14f_4g_0^2g_1^3+10f_4g_0g_1^5-2f_4g_1^7+g_0^4-6g_0^3g_1^2+11g_0^2g_1^4$$
$$-6g_0g_1^6+g_1^8=0.$$

This equation expresses (up to birationality), J as a degree 4 cover of $\mathbb{P}^2$. As one can see, the equation above is quadratic in y_1^2. Putting

$$y_1^2=X+f_2-f_3g_1+f_4g_1^2+g_0g_1-g_1^3$$

therefore gives a double cover of $\mathbb{P}^2$, corresponding to $\mathcal{K}$. In fact, this particular substitution yields a quartic equation in g_0, g_1, X that corresponds to the standard model of the associated Kummer surface.

Note that if two points $[P_1+Q_1-2\infty]$ and $[P_2+Q_2-2\infty]$ map to the same point on $\mathbb{P}^2$, then in fact we must have (up to relabelling) $\{P_2,Q_2\}=\{P_1,{}^\iota Q_1\}$ or $\{P_2,Q_2\}=\{{}^\iota P_1,{}^\iota Q_1\}$. It follows that $[P_1+Q_1-P_2-Q_2]=2[Q_1-\infty]$ or $[P_1+Q_1-P_2-Q_2]=2[P_1+Q_1-2\infty]$. We see that the class of $D\in J(K)$ in $J(K)/2J(K)$ can already be read off from its image in $\mathbb{P}^2$. The variety

$$V_\delta:\quad\begin{cases}Q_{\delta,3}(u_0,u_1,u_2,u_3,u_4)=0,\\ Q_{\delta,4}(u_0,u_1,u_2,u_3,u_4)=0\end{cases}\tag{7}$$

encodes that, with the map

$$V_\delta\to\mathbb{P}^2$$
$$(\underline{u})\mapsto\big(Q_{\delta,0}(\underline{u}):Q_{\delta,1}(\underline{u}):Q_{\delta,2}(\underline{u})\big).$$

Thus, in this situation, we also get, up to birationality,

$$T_\delta\simeq V_\delta\times_{\mathbb{P}^2}J.$$

Note however that V_δ is a degree 4 del Pezzo surface and it is known that these do not necessarily satisfy the Hasse principle. That is to say, even if $\delta\in S^{(2)}(J/K)$ and therefore T_δ has points everywhere locally, it does not follow that V_δ has a rational point (in which case it would be birational to $\mathbb{P}^2$ over K). If $V_\delta(K)=\emptyset$, however, it does follow that $\delta\notin\mu(J(K))$. See Section 6 for an example of this.

On can define an interesting intermediate object

$$\mathcal{K}_\delta=V_\delta\times_{\mathbb{P}^2}\mathcal{K}.$$

Rational points on $\mathcal{K}_\delta$ (outside some well-defined bad locus, see Remark 10) correspond to points D on some quadratic twist $J^{(d)}(K)$ such that $\mu(D)=\delta$ in $H^1(K,J^{(d)}[2])=H^1(K,J[2])$.

6. Using the Brauer–Manin obstruction to exhibit Ш(J/K)[2]

In this section we expand on the remark at the end of Example 13 that for Jacobians J of curves of genus 2, the variety V_δ need not satisfy the Hasse principle. This gives us a way to show that $\mu(J(K)) \neq S^{(2)}(J/K)$ that does not occur for elliptic curves, because there V_δ does satisfy the Hasse principle.

The following result from [4] is an example of a degree 4 del Pezzo surface defined over $\mathbb{Q}$, which violates the Hasse principle.

Lemma 14. *The Hasse principle is violated by the degree* 4 *del Pezzo surface*

$$v_0v_1 - \left(v_2^2 - 5v_3^2\right) = 0, \qquad (v_0+v_1)(v_0+2v_1) - \left(v_2^2 - 5v_4^2\right) = 0. \tag{8}$$

For other examples, see [11,12,17,18,24], all of which are due to the Brauer–Manin obstruction. We now backwards-construct a genus 2 curve $C : Y^2 = F(X)$ and value of $\delta \in S^{(2)}(\mathrm{Jac}(C)/K)$ such that V_δ is isomorphic to (8).

It is straightforward to check that C should admit a model of the form

$$C_{b,t}\colon\ y^2 = b(x-t)\det(Q_3 + xQ_4),$$

where Q_3, Q_4 are identified with the symmetric matrices representing the quadrics defining the surface in Lemma 14. We substitute $x = \frac{2tX+3t+1}{2X-t-3}$, $t = \frac{-1}{3+2\lambda}$ and, remembering that $C_{b,t}$ is ramified at $x = \infty$, obtain a model:

$$\begin{aligned} Y^2 = F_{\ell,\lambda}(X) &= \ell\left(X^2 - e_1\right)(X-e_2)(X-e_3)(X-e_4), \\ \text{where}\quad e_1 = 2,\quad e_2 &= \frac{\lambda+2}{\lambda+1},\quad e_3 = \lambda,\quad e_4 = \frac{3\lambda+4}{2\lambda+3}. \end{aligned} \tag{9}$$

We find that

$$K[\theta] = K[X]/F_{\ell,\lambda}(X) \simeq \mathbb{Q}\left(\sqrt{2}\right) \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}.$$

We denote elements $\delta \in K[\theta]^*$ by $\delta = [\delta_0 + \delta_1\sqrt{e_1}, \delta_2, \delta_3, \delta_4]$ with the $\delta_i \in \mathbb{Q}$. In this representation, we obtain

$$\mu : J_{l,\lambda} \to H^1\left(\mathbb{Q}, J_{l,\lambda}[2]\right) : (g,h) \mapsto l^{\deg(g)}\left[g\left(\sqrt{e_1}\right), g(e_2), g(e_3), g(e_4)\right],$$

or, more explicitly,

$$\begin{aligned} \mu : \left[(x_1,y_1) + (x_2,y_2) - 2\infty\right] \mapsto \big[&\left(x_1 - \sqrt{e_1}\right)\left(x_2 - \sqrt{e_1}\right), (x_1-e_2)(x_2-e_2), \\ &(x_1-e_3)(x_2-e_3), (x_1-e_4)(x_2-e_4)\big]. \end{aligned} \tag{10}$$

If we now let the u_i be as introduced in (5), and perform a linear change of variable to the w_i defined by

$$w_0 + w_1\sqrt{e_1} = \sum_{i=0}^{4} u_i\big(\sqrt{e_1}\big)^i, \qquad w_j = \sum_{i=0}^{4} u_i e_j^i, \quad \text{for } j = 2,3,4, \tag{11}$$

then the existence of $w_i \in \mathbb{Q}$ for which

$$\begin{aligned} w_5^2\big(x_1 - \sqrt{e_1}\big)\big(x_2 - \sqrt{e_1}\big) &= \big(\delta_0 + \delta_1\sqrt{e_1}\big)\big(w_0 + w_1\sqrt{e_1}\big)^2, \\ w_5^2(x_1 - e_j)(x_2 - e_j) &= \delta_j w_j^2, \quad \text{for } j = 2,3,4, \end{aligned} \tag{12}$$

is a prerequisite for $\delta \in \operatorname{im}\mu$. On eliminating x_1, x_2, w_5, one is left with the quadratic forms $Q_{\delta,3}$, $Q_{\delta,4}$ of V_δ in (7). On solving for these to be the same as (8) up to a linear change of variable, we obtain the following curves and value of δ.

Lemma 15. *Let $\mathcal{C}_{\ell,\lambda}\colon Y^2 = F_{\ell,\lambda}(X)$, a curve of genus 2, and δ be given by*

$$\begin{aligned} Y^2 = F_{\ell,\lambda}(X) &= \ell\big(X^2 - 2\big)\left(X - \frac{\lambda+2}{\lambda+1}\right)(X - \lambda)\left(X - \frac{3\lambda+4}{2\lambda+3}\right), \\ \delta &= \big[1 - \sqrt{2}, -1, 5, 5\big] \in A = K[X]/F_{\ell,\lambda}(X). \end{aligned} \tag{13}$$

Let μ be as defined in (10). *Then $\delta \notin \operatorname{im}\mu$.*

Proof. First note that $(2\lambda^2 + 8\lambda + 4) - (2\lambda^2 + 4\lambda + 4)\sqrt{2} = (1 - \sqrt{2})(2 - \lambda\sqrt{2})^2$, so that $(2\lambda^2 + 8\lambda + 4) - (2\lambda^2 + 4\lambda + 4)\sqrt{2}$ is interchangeable with $1 - \sqrt{2}$ modulo squares. Substituting

$$\delta_0 = 2\lambda^2 + 8\lambda + 4, \qquad \delta_1 = -\big(2\lambda^2 + 4\lambda + 4\big), \qquad \delta_3 = -1, \qquad \delta_4 = 5, \qquad \delta_5 = 5$$

into (12) and eliminating x_1, x_2, w_5, one is left with the quadratic forms $Q_{\delta,3}$, $Q_{\delta,4}$ of V_δ in (7), expressed in terms of the variables w_i of (11). On further performing the linear change of variable to the v_i given by

$$\begin{aligned} v_0 = 2(\lambda^2 - 2)u_0, \qquad v_1 = 2(\lambda^2 - 2)u_1, \qquad v_3 = u_3, \\ v_2 = (\lambda + 1)u_2, \qquad v_4 = (2\lambda + 3)u_4, \end{aligned}$$

these quadratic forms become (8), which by Lemma 14 has no $\mathbb{Q}$-rational point. Therefore V_δ, and so T_δ of (6), has no $\mathbb{Q}$-rational point, giving that $\delta \notin \operatorname{im}\mu$. □

Of course, the above result does not guarantee members of $Ш(J/\mathbb{Q})[2]$ for all values of ℓ, λ. We are guaranteed that $\delta \notin \operatorname{im}\mu$ and that V_δ has points everywhere locally. This means that $\delta \in Ш(J/\mathbb{Q})[2]$ 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 T_δ. This does not happen for

$\ell = 1$, $\lambda = 1$, when there are no members of $Ш(J/\mathbb{Q})[2]$, but it does happen for $\ell = -2$, $\lambda = -13/8$.

Lemma 16. *Let $\mathcal{C}_{-2,-13/8}$ and δ be as in Lemma 15 with $\ell = -2$, $\lambda = -13/8$:*

$$\mathcal{C}_{-2,-13/8}\colon Y^2 = F_{-2,-13/8}(X) = -2\big(X^2-2\big)\left(X+\frac{3}{5}\right)\left(X+\frac{13}{8}\right)\left(X-\frac{7}{2}\right),$$
$$\delta = \big[1-\sqrt{2},-1,5,5\big].$$

Then $\delta \in Ш(J_{-2,-13/8}/\mathbb{Q})[2]$.

Proof. We first show that $\delta \in S^{(2)}(J_{-2,-13/8}/\mathbb{Q})$, the 2-Selmer group, equivalent to T_δ having points every locally. It is sufficient to check the primes of bad reduction $p = 2, 5, 41, \infty$. Rather than writing out the equations of T_δ explicitly, a simpler approach is to check, for each p, that there exists a member of $J_{-2,-13/8}(\mathbb{Q}_p)$ which maps under μ_p to δ modulo local squares, where μ_p is as defined in (10), except with $\mathbb{Q}$ replaced by $\mathbb{Q}_p$. Let $\epsilon, \varsigma \in \mathbb{Q}_2$ be such that $\epsilon^2 = F_{-2,-13/8}(3/2)$ and $\varsigma^2 = F_{-2,-13/8}(17)$; these both exist, since $F_{-2,-13/8}(3/2) = \frac{1}{16}105$ and $F_{-2,-13/8}(17) = -12700611/5$, with 105 and $-12700611/5$ both $\equiv 1 \pmod 8$. We now compute

$$\mu_\infty : \big[(-3/5,0)+(7/2,0)-2\infty\big] \mapsto \left[-\frac{2}{5}-\frac{58\sqrt{2}}{5}, -\frac{2825761}{50000}, \frac{1681}{80}, \frac{2825761}{1600}\right],$$
$$\mu_{41} : \mathcal{O} \mapsto [1,1,1,1],$$
$$\mu_5 : \big[(-13/8,0)+(7/2,0)-2\infty\big] \mapsto \left[-\frac{59}{4}-\frac{15\sqrt{2}}{2}, -\frac{1681}{100}, -\frac{2825761}{81920}, \frac{2825761}{1280}\right],$$
$$\mu_2 : \left[\left(\frac{3}{2},\epsilon\right)+(17,\varsigma)-2\infty\right] \mapsto \left[\frac{55}{2}-\frac{37\sqrt{2}}{2}, \frac{924}{25}, \frac{3725}{64}, -27\right],$$

where $\mathcal{O}$ is the identity element in $J_{-2,-13/8}(\mathbb{Q})$. Each of the above members of the image of μ_p is equal to $[1-\sqrt{2},-1,5,5]$ modulo local squares at p. Hence $\delta = [1-\sqrt{2},-1,5,5] \in S^{(2)}(J_{-2,-13/8}/\mathbb{Q})$. Furthermore, we already know, from Lemma 15, that $\delta \notin \operatorname{im}\mu$, so that $\delta \in Ш(J_{-2,-13/8}/\mathbb{Q})[2]$, as required. □

For curves of the form $Y^2 = F_{\ell,\lambda}(X)$ there is also the available alternative of trying to show the existence of members of $Ш(J_{\ell,\lambda}/\mathbb{Q})[2]$ using the Richelot isogeny (1), (2), when there might be a difference between the 2-Selmer bounds for $\mathcal{C}$ and $\mathcal{D}$. For the above example δ can alternatively be shown to be a member of $Ш(J_{-2,-13/8}/\mathbb{Q})[2]$ by comparing the 2-Selmer bound of 3 for the rank of $J_{-2,-13/8}(\mathbb{Q})$, with the 2-Selmer bound of 1 for the Richelot-isogenous Jacobian of the curve $Y^2 = -205(80X^2+260X-209)(29X^2+2X+58)(4X^2+13X+8)$, obtained from (1), (2) with $G_1 = -2(X^2-2)$, $G_2 = X+13/8$, $G_3 = (X+3/5)(X-7/2)$. Note, however, that Ш persists when one uses the Richelot isogeny with $G_1 = -2(X^2-2)$, $G_2 = X+3/5$, $G_3 = (X+13/8)(X-7/2)$. It would be

interesting to see the methods in [4] extended to degree 4 del Pezzos for which $\det(M+tN)$ has an irreducible factor of degree >2.

One nice consequence of our approach in Lemma 16, which has an advantage over case by case attempts via Richelot isogenies, is that we can find a parametrised family of curves $Y^2 = F_{-2k,-13/8}(X)$ all of which are guaranteed to contain a nontrivial member of $Ш(J_{-2k,-13/8}/\mathbb{Q})[2]$, provided that k comes from a family for which the local properties of δ are not affected.

Proof of Proposition 2. We already know, from Lemma 15, that $\delta = [1-\sqrt{2}, -1, 5, 5] \notin \operatorname{im}\mu$ for any k and, from Lemma 16, that $\delta \in S^{(2)}(J_{-2k,-13/8}/\mathbb{Q})$ when $k=1$. It is therefore only necessary to choose k so that T_δ of (6) continues to have solutions at $2, 5, 41, \infty$, and at any new bad primes introduced by k. Since the map μ is only affected by translating some entries multiplicatively by k, the following conditions on k are sufficient.

$$\begin{aligned}&\text{(i)}\quad k \in (\mathbb{R}^*)^2, \qquad \text{(ii)}\quad k \in \left(\mathbb{Q}_2^*\right)^2, \qquad \text{(iii)}\quad k \in \left(\mathbb{Q}_5^*\right)^2,\\ &\text{(iv)}\quad -1 \in \left(\mathbb{Q}_p^*\right)^2, \qquad \text{(v)}\quad 1\pm\sqrt{2} \in \left(\mathbb{Q}_p\left(\sqrt{2}\right)^*\right)^2, \qquad \text{(vi)}\quad 5 \in \left(\mathbb{Q}_p^*\right)^2,\\ &\text{for } p = 41 \text{ and any } p \neq 2, 5 \text{ with } v_p(k) \text{ odd.}\end{aligned} \tag{14}$$

First note that $-1, 5 \in (\mathbb{Q}_{41}^*)^2$ and $1\pm\sqrt{2} \in (\mathbb{Q}_{41}(\sqrt{2})^*)^2 = (\mathbb{Q}_{41}^*)^2$, so that (iv), (v), (vi) need only be checked for all $p \neq 2, 5$ with $v_p(k)$ odd. Condition (v) is satisfied when $1\pm\sqrt{2} = (u+v\sqrt{2})^2$, for some $u, v \in \mathbb{Q}_p$, giving $u^2+2v^2 = \pm 2uv = 1$; after eliminating v, we have $(2u^2-1)^2+1=0$, for some $u \in \mathbb{Q}_p$. So let

$$k = \frac{1}{2}\left(\left(2r^2-1\right)^2+1\right) = 2r^2\left(r^2-1\right)+1, \quad \text{for } r \in \mathbb{Q}. \tag{15}$$

For any odd prime p with $v_p(k)$ odd, we clearly have $r \in \mathbb{Z}_p$ and $(2r^2-1)^2+1 \equiv 0 \pmod{p}$, which lifts to a solution in $\mathbb{Z}_p$ of $(2u^2-1)^2+1=0$. Hence (v) is satisfied, as clearly is (iv), applying a similar argument to $\gamma^2+1 \equiv 0 \pmod{p}$, where $\gamma = 2r^2-1$. Furthermore, $k>0$, so that (i) is also satisfied. In order to ensure that (vi) is satisfied, it is equivalent (in view of (iv)) to force $-5 \in (\mathbb{Q}_p^*)^2$, for which it is sufficient that $10(r^2-1)$ is square, since then we would have $20r^2(\text{square}) \equiv -1 \pmod{p}$, and could apply the same argument as before. The genus 0 curve, $10(r^2-1) = \text{square}$, can be parametrised as $r = (1+10s^2)/(1-10s^2)$. Substituting this into (15) gives

$$\begin{aligned}k &= 2\left(\frac{1+10s^2}{1-10s^2}\right)^2\left(\frac{40s^2}{(1-10s^2)^2}\right)+1\\ &= 80s^2\left(1+10s^2\right)^2+\left(1-10s^2\right)^4 \quad \text{modulo squares.}\end{aligned} \tag{16}$$

So far, we have guaranteed that (i), (iv), (v), (vi) are always satisfied for any k in (16) and any $s \in \mathbb{Q}$. Furthermore

$$k = 80a^2\left(b^2 + 10a^2\right)^2 + \left(b^2 - 10a^2\right)^4 \quad \text{modulo squares,}$$
$$\text{where} \quad s = a/b, \quad \text{with } a, b \in \mathbb{Z} \text{ and } \gcd(a, b) = 1. \tag{17}$$

The right-hand side of (17) is congruent to 1 both modulo 8 and modulo 5, giving (ii), (iii), provided that $\gcd(2, b) = \gcd(5, b) = 1$, that is, provided $s \in \mathbb{Q} \cap \mathbb{Z}_2 \cap \mathbb{Z}_5$. In order to obtain a family with an unrestricted parameter $t \in \mathbb{Q}$, we can take $s = 1/(t^5 - t + 1)$, which satisfies $|s|_2, |s|_5 \leq 1$ for any $t \in \mathbb{Q}$. Substituting this into (16) gives the family (3), as required.

We finally note that $J_{-2k,-13/8}$ can be shown to have absolutely simple Jacobian, using the method in [25] (also described in [9, p. 158]) at $p = 13$. □

The family of Lemma 15 typically gives rise to absolutely simple examples of $J_{\ell,\lambda}$ (as in the example above), but there are the values $\lambda = 1, -2, -7/5$ where $J_{\ell,\lambda}$ is reducible. For example, a virtually identical argument shows that the family of reducible Jacobians $J_{2k,1}$ has $\delta \in Ш(J_{2k,1}/\mathbb{Q})[2]$ for all k of the form (3).

The above family of examples used Lemma 14, which was the application in [4] of the Brauer–Manin obstruction to a specific degree 4 del Pezzo surface. The general method for applying the Brauer–Manin obstruction to any degree 4 del Pezzo surface is outlined in [3].

7. Visualisation via Weil-restriction

We consider a curve C with its Jacobian J over a number field K of the type described in Section 5. Given a cocycle $\delta \in H^1(K, J[2])$, we construct an Abelian variety A of the type described in Section 4.

There is a finite extension L of K such that the restriction $\mathrm{res}^K_L(\delta) \in \mu(J(L))$. In the language of Section 5, $T_\delta(L) \neq \emptyset$, and subject to Remark 10, we can assume that the rational point lies outside certain bad loci. We take $A = \Re_{L/K}(J)$, the *Weil restriction* of J with respect to L/K (see [5, Section 7.6]). Base extension gives us an injection p^*: $J \to A$ and the norm map with respect to L/K gives a morphism $p_* : A \to J$. Writing $[L : K] = nm^e$, we have $p_* \circ p^* = (nm^e)|_J$. By design, we now have a point $b \in A(K)$ with $\mu_A(b) = p^*(\delta)$. In practice, nearly all constructions of b and L guarantee that $p_*(b) = 0$. In fact, in case $p_*(b) \neq 0$, we have constructed a nontrivial point on J, which may yield new information on $J(K)$.

For the case of elliptic curves (Example 12), we get T_δ as an intersection of two quadrics. Hence, any hyperplane section would yield points on T_δ of degree at most 4. In fact, if $\delta \in S^{(2)}(J/K)$ then due to the Hasse principle, T_δ is a double cover of a $\mathbb{P}^1$, so we can always choose L to be a quadratic extension of K. This is extremely fortunate, because this allows us to apply Proposition 6 to obtain new information about whether $\delta \in \mu(J(K))$. See [7] for a detailed description of this approach.

Since for higher genus we do not have a proof that T_δ has quadratic points, we avoid using that $V_\delta \simeq \mathbb{P}^1$ and demonstrate how one can use Corollary 8 to infer extra information about $\mathrm{rk}\, J(K)$.

Example 17. The elliptic curve

$$E\colon\ y^2 = x^3 - 7x^2 - 1$$

has rank 0 over $\mathbb{Q}$.

Proof. Of course, this statement can be proved by analytic methods (see [15,16]). However, for the purpose of illustration, we will ignore this fact and use Weil restriction together with Corollary 8. Writing $\theta^3 - 7\theta^2 - 1 = 0$, we have that

$$S^{(2)}(E/\mathbb{Q}) \simeq \langle \theta^2 - 7\theta, \theta^2 - 6\theta - 7 \rangle.$$

Taking $\delta = \theta^2 - 6\theta - 7$, we find

$$T_\delta\colon\ v^2 = -u^4 + 3u^3 - u^2 - 4u - 1.$$

As announced, we ignore that T_δ has many obvious quadratic points here and use a quartic extension, generated by α, given by $\alpha^4 - 3\alpha^3 + \alpha^2 + 4\alpha + 2$. It is clear that $(\alpha, 1) \in T_\delta(K)$. This leads to the rational point

$$\big((-17\alpha^3 + 3\alpha^2 + 4\alpha + 10)/4, (-41\alpha^3 + 292\alpha^2 + 490\alpha + 220)/8\big) \in E(K).$$

Subject to the Generalised Riemann Hypothesis, we find that

$$S^{(2)}(E/K) \simeq \langle \theta^2 - 7\theta, \theta^2 - 6\theta - 7 \rangle.$$

It is straightforward to verify that $E[2](\mathbb{Q}) = E[2](K) = \{0\}$. What is more, by construction we have $\#p^*G \geqslant 2$, where G is as defined in Section 4, just before Remark 5. Therefore, we already see that $\#E(\mathbb{Q})/2E(\mathbb{Q}) \leqslant 2$ and hence that $\#Ш(E/\mathbb{Q})[2] \geqslant 2$. If we assume that $Ш(E/\mathbb{Q})$ is always a square, then it follows that in fact $\operatorname{rk} E(\mathbb{Q}) = 0$. In fact we can prove this, because for $\delta = \theta^2 - 7\theta$ we find

$$T_\delta\colon\ v^2 = -4u^4 + 8u^3 + 8u^2 - 8u - 11$$

and

$$\big((\alpha^3 - 3\alpha^2 - \alpha + 6)/4, (3\alpha^3 - 8\alpha^2 + 4\alpha + 11)/4\big) \in T_\delta(K).$$

This yields

$$\big((-7039\alpha^3 + 160198\alpha^2 - 174306\alpha - 17232)/30625,$$
$$(-8419849\alpha^3 - 61373757\alpha^2 + 126116579\alpha + 102767863)/5359375\big) \in E(K).$$

It follows that $p^*(G) = S^{(2)}(E/K)$ and thus that $\operatorname{rk} E(\mathbb{Q}) = 0$. Note that in order to get this result, we unfortunately had to search for the second point above; only the first point

was there by construction. This problem does not arise when one can apply Proposition 6 (see [7]). □

The question arises whether we can bound the degree $[L : K]$ necessary to visualise a given $\delta \in H^1(K, J[2])$ in $A = \Re_{L/K} J$. An answer is given by the proof of [2, Proposition 2.3]. It should not come as a surprise that our present setup, which is an explicit version of the construction used by Agashe and Stein [1], allows us to give a simpler proof and, sometimes, a slight improvement.

Proposition 18. *Let $J, \delta, T_\delta, V_\delta$ be as in Section* 5.

(a) *There are extensions L/K with $[L : K] \leqslant 2^d$ such that $V_\delta(L)$ is non-empty.*
(b) *If $P \in V_\delta(L)$ satisfies the conditions of Remark* 10 *and M is the field of definition of a point on T_δ above P, then $[M : L] \leqslant 2^d$.*
(c) *If $\delta \in S^{(2)}(J/K)$ and f has at least $d-1$ linear factors then there are extensions L/K with $[L : K] \leqslant 2^{d-1}$ such that $V_\delta(L)$ is non-empty.*

Proof. (a) V_δ is a complete intersection of d quadrics in $\mathbb{P}^{2d}$. Intersecting V_δ with a d-plane yields points of degree at most 2^d.

(b) This is an exercise in Galois theory. For the generic point $P \in V_\delta(K(V_\delta))$, the splitting field of $K(V_\delta)[\beta]$ over $K(V_\delta)$ has Galois group S_d. Write $\beta_1, \ldots, \beta_d$ for the conjugates. The variety T_δ would definitely have a point above P over the field $K(V_\delta)[\sqrt{\beta_1}, \ldots, \sqrt{\beta_d}]$. This has Galois group $S_d \ltimes (S_2)^d$. Since we do not have to be able to distinguish the β_i individually but only need to be able to tell their square roots apart, we can take a subfield corresponding to some $S_d \subset S_d \ltimes (S_2)^d$. Since $[S_d \ltimes (S_2)^d : S_d] = 2^d$, we see we need a degree 2^d extension of $K(V_\delta)$. For any particular point, we would get a specialization of these function field extensions and hence a degree of at most 2^d.

(c) Let $\theta_1, \ldots, \theta_{d-1}$ be roots of f in K. As a K-algebra, we have $A \simeq K^{d-1} \times \tilde{A}$, where $\tilde{A}$ is some cofactor. It is straightforward to check that with a linear change of variables from $\underline{u}$ to $\underline{v}$, we can ensure that $Q_{\delta,i}(\underline{v})$ are all diagonal in, say, $v_0, \ldots, v_{d-2}$. It follows that V_δ is contained in a quadric W that involves only $v_{d-1}, \ldots, v_{2d}$. Since $v_0^2, \ldots, v_{d-2}^2$ are quadratic forms in $v_{d-1}, \ldots, v_{2d}$, we see that V_δ is a degree 2^{d-1} cover of W considered as a quadric in $\mathbb{P}^d$. From $\delta \in S^2(J/K)$ it follows that V_δ and hence W are everywhere locally solvable. Since W satisfies the Hasse principle, we see that W has rational points and therefore V_δ has points of degree 2^{d-1}. □

Finally, we give an example to illustrate that, even though in the case $d = 2$ we cannot prove a degree 2 extension will always work, it may still sometimes work because $\mathcal{K}_\delta$ may have a rational point.

Example 19. Let J be the Jacobian over $\mathbb{Q}$ of

$$C\colon\ y^2 = x^5 - 81x - 243.$$

Then $J(\mathbb{Q}) = \{0\}$ and $Ш(J/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. It is straightforward to verify that $S^{(2)}(J/\mathbb{Q}) = \langle \theta^2+9, \theta/3\rangle$ and that $\#J(\mathbb{Q})^{\mathrm{tor}} = 1$. We first consider $\delta = \theta^2 + 9$. We find

$$V_\delta\colon \begin{cases} 2u_0u_1 + 18u_0u_3 + 18u_1u_2 + 162u_1u_4 + 162u_2u_3 \\ \quad + 486u_2u_4 + 243u_3^2 + 1458u_3u_4 + 2187u_4^2 = 0, \\ 2u_0u_2 + 18u_0u_4 + u_1^2 + 18u_1u_3 + 9u_2^2 + 162u_2u_4 + 81u_3^2 + 486u_3u_4 + 729u_4^2 = 0. \end{cases}$$

From the presentation of δ it already follows that $P = (1:0:0:0:0) \in V_\delta(\mathbb{Q})$. Specializing the equation for T_δ from Section 5 we find

$$y_1^2\big(y_1^2 - 27\big) = 0.$$

By solving for y_0^2, y_1^2, we find that $\mathcal{K}_\delta$ has a rational point above P, with $(y_0^2, y_1^2) = (-243, 0)$ or $(y_0^2, y_1^2) = (0, 27)$. Furthermore, it shows that over $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{-3})$, the variety T_δ has a rational point as well. We choose $L = \mathbb{Q}(\sqrt{-3})$. We find $S^{(2)}(J/L) = \langle \theta^2 + 9, \theta/3\rangle$. Therefore $N_{L/K}(S^{(2)}(J/L)) = \{1\}$ and we see that $\delta \notin N_{L/K}(S^{(2)}(J/L))$. By Proposition 6 it follows that $\delta \notin \mu(J(\mathbb{Q}))$ and thus represents a nontrivial element in $Ш(J/\mathbb{Q})[2]$. Note that the only ingredients we needed were a rational point on V_δ and the computation of $S^{(2)}(J/L)$. This involves computing class group and unit information for $\mathbb{Q}(\theta, \sqrt{-3})$ and some local computations. We do not have to look for rational points on any twists of J or on $J(L)$.

In fact, for $\delta = \theta/3$, we find

$$\theta^2 + 18\theta + 27 = \delta\left(\frac{1}{9}\theta^3 + \frac{1}{3}\theta^2 + \theta - 3\right)^2$$

and $\mathcal{K}_\delta$ has a rational point above $P = (-3:1:1/3:1/9:0) \in V_\delta(\mathbb{Q})$ with $(y_0^2, y_1^2) = (-3\cdot 63^2, -3^2\cdot 42^2)$ or $(y_0^2, y_1^2) = (-189^2/2, -105^2/2)$. Hence, also δ gets visualised in $S^{(2)}(J/L)$ and therefore the computation above also verifies that $\theta/3 \notin \mu(J(\mathbb{Q}))$.

Another way to see that $\operatorname{rk} J(\mathbb{Q}) = 0$ is by considering $J^{(-3)}$, the Jacobian of $C^{(-3)}\colon\ y^2 = -3(x^5 - 81x - 243)$. It is easily checked that $g_1(x) = x^2 + 9$ and $g_2(x) = x$ give rise to two independent points on $J^{(-3)}(\mathbb{Q})$ and hence that $\operatorname{rk} J^{(-3)}(\mathbb{Q}) \geqslant 2$. Since $J^{(-3)}$ and J are isomorphic over $L = \mathbb{Q}(\sqrt{-3})$, it follows that

$$\operatorname{rk} J(L) = \operatorname{rk} J(\mathbb{Q}) + \operatorname{rk} J^{(-3)}(\mathbb{Q}).$$

The Selmer group computation above implies that $\operatorname{rk} J(L) \leqslant 2$ and therefore that $\operatorname{rk} J(\mathbb{Q}) = 0$. □

8. Visualisation using fibre products

In this section we consider a slightly more general construction of visualising Abelian varieties for hyperelliptic Jacobians. The construction from Section 7 with quadratic extensions can be considered a degenerate limit case (with $c \to \infty$) of the construction presented here.

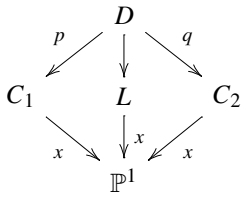
Let K be a number field. We consider a hyperelliptic curve of genus d with a model

$$C = C_1\colon\ y_1^2 = f(x),$$

where $f \in K[x]$ is a monic polynomial of degree $2d+1$. For parameters $b \in K^*$ and $c \in K$ such that $f(c) \neq 0$, we consider the curve

$$C_2\colon\ y_2^2 = b(x-c)f(x).$$

We consider the fibre product $D = C_1 \times_{\mathbb{P}^1} C_2$. These curves fit in the diagram below.



$$\begin{aligned} &C_1\colon\ y_1^2 = f(x),\\ &C_2\colon\ y_2^2 = b(x-c)f(x),\\ &L\colon\ y_0^2 = b(x-c),\\ &D\colon\ y_1^2 = f(y_0^2/b + c). \end{aligned}$$

It follows that D is a hyperelliptic curve of genus $2d$. We write $J = \mathrm{Jac}(C_1)$, $B = \mathrm{Jac}(C_2)$ and $A = \mathrm{Jac}(D)$. It is straightforward to check that J, A, B together with the pullback and push forward maps p^* and p_* fit the description in Section 4, with $p_* \circ p^* = 2|_J$.

In fact $J[2] = B[2]$ as Galois-modules, and $A = J \times B/\Delta$ where Δ is the antidiagonal embedding of $J[2]$ into $J[2] \times B[2]$. As a consequence, we also have $H^1(K, J[2]) \simeq H^1(K, B[2])$. One can see this isomorphism in the following way. By considering the coordinates

$$(u, v) = \left(\frac{bf(c)}{x-c}, \frac{b^d f(c)^{d+1}}{x-c}y\right)$$

we obtain a model

$$C_2\colon\ v^2 = \tilde{f}(u)$$

with $\tilde{f} \in K[u]$ monic and of degree $2d+1$. Note that points $D \in B(K)$ can be represented as divisors on C_2. If the divisor is supported outside $x = \infty$ then $D \in B(K)$ can be described as $[\{g(x) = 0, y = h(x)\} \cdot C_2 - \deg(g)(c, 0)]$. In this representation, we get the map[4]

$$\begin{aligned} \mu_2\colon\quad & B \mapsto H^1\big(K, J[2]\big),\\ & (g, h) \mapsto b^{\deg(g)} g(c) g(\theta). \end{aligned}$$

[4] The fact that modulo K^*, the map should be $(g, h) \mapsto g(\theta)$ is fairly easy to see. The scalar factor can be computed from the fact that the image should have square norm and a calculation like the one in the proof of Lemma 11.

This generalises the case where C_1 is an elliptic curve, which is discussed at length in [7]. It is proved there that, for a given $\delta \in H^1(K, J[2])$, the V_δ that belongs to B is actually isomorphic to the V_δ belonging to J. Hence, to construct a B such that $\delta \in \mu_2(B(K))$ it is sufficient to have a point $P \in V_\delta(K)$. One maps P to $x(P) \in \mathbb{P}^1$ below and solves b, c such that $x(P)$ is in $x(C_2(K))$. Then $\tilde{T}_\delta = C_2 \times_{\mathbb{P}^1} V_\delta$ has a rational point.

For curves of genus 2 we can proceed similarly.

Proof of Proposition 3. We follow the notation of Section 5. The statement that V_δ has a rational point means that there are $\delta_i \in K$ such that

$$\delta \equiv \delta_0 + \delta_1\theta + \delta_2\theta^2 \pmod{A^{*2}}.$$

If $\delta_1 = \delta_2 = 0$ then $\delta_0 \in K^{*2}$ (δ is invertible and of square norm, after all), so $\delta \equiv 1 \pmod{A^{*2}}$. In this case there is nothing to visualise. We can take any valid pair of values for c, b.

If $\delta_2 = 0$, write $\beta = -\delta_0/\delta_1$. Pick any $c \in K$ such that $f(c) \neq 0$ and put $b = (\beta - c)f(\beta)$. Now $g = x - \beta$ and $h = b$ specify a point in $B(K)$ with $\mu_2(g, h) = \delta$, and therefore δ is visualised in A.

If $\delta_2 \neq 0$ then we define $g = x^2 + \delta_1/\delta_2 x + \delta_0/\delta_2$, so that $\delta = \delta_2 g(\theta)$. Writing $K[\beta] = K[x]/(g(x))$, we pick $y_0, y_1 \in K$ such that $y_0 + \beta y_1 \in K[\beta]^*$. We solve $b, c \in K$ from the equation

$$b(\beta - c)f(\beta) = (y_0 + \beta y_1)^2.$$

It follows that with these choices, B indeed has a point over K with the given g and that $g(c) \equiv \delta_2 \pmod{K^{*2}}$. Therefore δ is visualised in A. □

We finally summarise the resulting procedure for attempting to show that a given $\delta \in S^{(2)}(J/K)$ represents a nontrivial element of $Ш(J/K)[2]$:

(1) Compute the Brauer–Manin obstruction for V_δ to have rational points. If there is such an obstruction, then T_δ has no rational points and hence δ represents a nontrivial element of $Ш(J/K)[2]$ and we are done.
(2) Search for a rational point on V_δ. If the Brauer–Manin obstruction is the only obstruction for rational points on del Pezzo surfaces, then this step succeeds in finite time.
(3) Use Proposition 3 to construct a visualising Abelian variety A and, appealing to Proposition 6, test whether $\delta \in p_* S^{(2)}(A/K)$. One can compute $S^{(2)}(A/K)$ using [27], or at least a quotient of it, the *fake Selmer group*. This is good enough, since p_* will factor through it (see [7]). Even if $\delta \notin 2Ш(J/K)[4]$, there is no guarantee this will actually show that $\delta \notin \mu(J(K))$. However, note that multiple choices for b, c are possible.

References

[1] A. Agashe, W. Stein, Visible evidence in the Birch and Swinnerton-Dyer conjecture for modular Abelian varieties of analytic rank zero, Math. Comp. 74 (249) (2005) 455–484 (electronic).

[2] A. Agashe, W. Stein, Visibility of Shafarevich–Tate groups of Abelian varieties, J. Number Theory 97 (1) (2002) 171–185.
[3] A.O. Bender, H.P.F. Swinnerton-Dyer, Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in $\mathbb{P}^4$, Proc. London Math. Soc. 83 (2001) 299–329.
[4] B.J. Birch, H.P.F. Swinnerton-Dyer, The Hasse problem for rational surfaces, J. Reine Angew. Math. 274/275 (1975) 164–174, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.
[5] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3)), vol. 21, Springer, Berlin, 1990.
[6] J.-B. Bost, J.-F. Mestre, Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2, Gaz. Math. 38 (1988) 36–64.
[7] N. Bruin, Visualising Sha[2] in Abelian surfaces, Math. Comp. 73 (247) (2004) 1459–1476 (electronic).
[8] J.W.S. Cassels, Second descents for elliptic curves, J. Reine Angew. Math. 494 (1998) 101–127, dedicated to Martin Kneser on the occasion of his 70th birthday.
[9] J.W.S. Cassels, E.V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, London Math. Soc. Lecture Note Ser., vol. 230, Cambridge Univ. Press, Cambridge, 1996.
[10] J.-L. Colliot-Thélène, B. Poonen, Algebraic families of nonzero elements of Shafarevich–Tate groups, J. Amer. Math. Soc. 13 (1) (2000) 83–99.
[11] J.-L. Colliot-Thélène, J.-J. Sansuc, P. Swinnerton-Dyer, Intersections of two quadrics and Châtelet surfaces. I, J. Reine Angew. Math. 373 (1987) 37–107.
[12] J.-L. Colliot-Thélène, J.-J. Sansuc, P. Swinnerton-Dyer, Intersections of two quadrics and Châtelet surfaces. II, J. Reine Angew. Math. 374 (1987) 72–168.
[13] J.E. Cremona, B. Mazur, Visualizing elements in the Shafarevich–Tate group, Experiment. Math. 9 (1) (2000) 13–28.
[14] E.V. Flynn, J. Redmond, Application of covering techniques to families of curves, J. Number Theory 101 (2) (2003) 376–397.
[15] B.H. Gross, Kolyvagin's work on modular elliptic curves, in: L-functions and Arithmetic, Durham, 1989, in: London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.
[16] B.H. Gross, D.B. Zagier, Heegner points and derivatives of L-series, Invent. Math. 84 (2) (1986) 225–320.
[17] W. Hürlimann, Brauer group and Diophantine geometry: A cohomological approach, in: Brauer Groups in Ring Theory and Algebraic Geometry, Wilrijk, 1981, in: Lecture Notes in Math., vol. 917, Springer, Berlin, 1982, pp. 43–65.
[18] V.A. Iskovskih, A counterexample to the Hasse principle for systems of two quadratic forms in five variables, Mat. Zametki 10 (1971) 253–257.
[19] V.A. Kolyvagin, On the structure of Shafarevich–Tate groups, in: Algebraic Geometry, Chicago, IL, 1989, in: Lecture Notes in Math., vol. 1479, 1991, pp. 94–121.
[20] J.R. Merriman, S. Siksek, N.P. Smart, Explicit 4-descents on an elliptic curve, Acta Arith. 77 (4) (1996) 385–404.
[21] B. Poonen, An explicit algebraic family of genus-one curves violating the Hasse principle, J. Théor. Nombres Bordeaux 13 (1) (2001) 263–274, 21st Journées Arithmétiques, Rome, 2001.
[22] E.F. Schaefer, M. Stoll, How to do a p-descent on an elliptic curve, Trans. Amer. Math. Soc. 356 (3) (2004) 1209–1231 (electronic).
[23] E.F. Schaefer, J.L. Wetherell, Computing the Selmer group of an isogeny between Abelian varieties using a further isogeny to a Jacobian, J. Number Theory 115 (1) (2005) 158–175.
[24] A. Skorobogatov, Torsors and Rational Points, Cambridge Tracts in Math., vol. 144, Cambridge Univ. Press, Cambridge, 2001.
[25] M. Stoll, Two simple 2-dimensional Abelian varieties defined over $\mathbf{Q}$ with Mordell–Weil group of rank at least 19, C. R. Acad. Sci. Paris Sér. I Math. 321 (10) (1995) 1341–1345.
[26] M. Stoll, On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians, J. Reine Angew. Math. 501 (1998) 171–189.
[27] M. Stoll, Implementing 2-descent for Jacobians of hyperelliptic curves, Acta Arith. 98 (3) (2001) 245–277.
[28] M. Stoll, On the arithmetic of the curves $y^2 = x^l + A$. II, J. Number Theory 93 (2) (2002) 183–206.
[29] T. Womack, Four descent on elliptic curves over Q, PhD thesis, University of Nottingham, 2003.