ANSWER TO A QUESTION OF BRUIN AND STOLL

BRENDAN CREUTZ

1. Introduction

Let K be a field of characteristic not equal to 2 and let C be a non-singular hyperelliptic curve over K. Fix an affine model for C of the form $C : y^2 = c \cdot f(x)$, with $c \in K^\times$ and $f(x) \in K[x]$ monic and of even degree. Use F to denote the algebra $F = K[x]/f(x)$. Since C is non-singular, $f(x)$ is square-free, and so F is an étale K-algebra.

In performing 2-descents on C or its Jacobian, one typically considers the sets (see [BrSt], [MSS], [PoSc], [Sch])

$$H_K = \{\delta \in F^\times/K^\times F^{\times 2} \,:\, c \cdot N_{F/K}(\delta) \in K^{\times 2}\}\,, \text{ and}$$
$$H^0_K = \{\delta \in F^\times/K^\times F^{\times 2} \,:\, N_{F/K}(\delta) \in K^{\times 2}\}\,.$$

When K is a number field, these sets contain the fake 2-Selmer set and fake 2-Selmer group of C and its Jacobian, respectively. These fake 2-Selmer objects parameterize pairs of (possibly isomorphic) everywhere locally solvable 2-coverings. In [BrSt] it is shown that H_K parameterizes pairs of (possibly isomorphic) 2-coverings of C which have a model in projective space of a particular form. We answer the following question of Bruin and Stoll (loc. cit. 7.2).

Question 1.1. *Can a hyperelliptic curve defined over a number field K be everywhere locally solvable and yet have H_K empty?*

When C is of genus one, it may be considered as a 2-covering of its Jacobian $E = \mathrm{Jac}(C)$. In this case question 1.1 is equivalent to asking whether C can be everywhere locally solvable yet fail to admit a lift to a 4-covering with trivial obstruction (in the sense of [CFOSS, Section 2]). We show that this is not possible.

Theorem 1.2. *Let $C \to E$ be an everywhere locally solvable 2-covering of an elliptic curve E defined over a number field K. Then there exists a lift of C to a 4-covering $D \to E$ with trivial period-index obstruction.*

In the higher genus situation, the question is answered by the following example.

Theorem 1.3. *Let C be the Hyperelliptic curve of genus 2 defined over $\mathbb{Q}$ by*

$$C : y^2 = 3(x^2+1)(x^2+17)(x^2-17)\,.$$

Then C is everywhere locally solvable, yet $H_{\mathbb{Q}}$ is empty.

Having written down the curve, the proof is rather elementary. The majority of what follows is devoted to the genus one case. We also address the obvious reformulation of theorem 1.2 for an arbitrary prime p.

Question 1.4. *Can a p-covering of an elliptic curve defined over a number field be everywhere locally solvable and yet fail to admit a lift to a p^2-covering with trivial obstruction?*

For $p \leq 11$, we are able to show that if the p-torsion in the Mordell-Weil group is trivial, then such lifts always exist. The restriction on p is an artifact of our method of proof. We reduce the problem to a machine computation that can, in principle, be carried out for any given p; $p = 11$ being about the limit our machine could handle. The hypothesis on the p-torsion of the Jacobian can be made more precise, but cannot be removed using our methods. At the very least, this places strong restrictions on what a potential counterexample can look like.

2. Proof of theorem 1.3

First we check that C is everywhere locally solvable. In fact, it has a $\mathbb{Q}_p$-rational Weierstrass point for each $p \leq \infty$. Indeed, $x^2 - 17$ splits over $\mathbb{Q}_2$ and $\mathbb{R}$, $x^2 + 1$ splits over $\mathbb{Q}_{17}$ and, for odd $p \neq 17$, the equation $\left(\frac{17}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{-17}{p}\right)$ shows that at least one of the three polynomials must split in $\mathbb{Q}_p$.

The Weierstrass algebra splits as $F \simeq \mathbb{Q}(\sqrt{-1}) \oplus \mathbb{Q}(\sqrt{17}) \oplus \mathbb{Q}(\sqrt{-17})$. We must show that 3 is not in the image of $N_{F/\mathbb{Q}}$ modulo squares. Suppose there is some $\delta \in F^\times$ and $s \in \mathbb{Q}^\times$ such that $N_{F/\mathbb{Q}}(\delta) = 3s^2$. Under

the splitting of F, let $\delta = (\delta_1, \delta_2, \delta_3)$ and denote the norm in each corresponding factor by N_i. By assumption we have $N_1(\delta_1)N_2(\delta_2)N_3(\delta_3) = 3s^2$. Scaling we may assume that $\delta_1 = a_1 + b_1\sqrt{-1}$, $\delta_2 = a_2 + b_2\sqrt{17}$ and $\delta_3 = a_3 + b_3\sqrt{-17}$ with $a_i, b_i, s \in \mathbb{Z}$.

$N_1(\delta_1) = a_1^2 + b_1^2$ is a sum of two squares, so every prime $p \equiv 3 \bmod 4$ occurs in its factorization with even multiplicity. Similarly we have the following two claims, whose verification we leave as an easy excercise for the reader.

- 3 appears in the factorization of $N_2(\delta_2)$ with even multiplicity.
- If $N_3(\delta_3) = 2^n m$ with m odd, then $m \equiv 1 \bmod 4$.

From $N_1(\delta_1)N_2(\delta_2)N_3(\delta_3) = 3s^2$ and the claims above, it follows that there is some prime $p \neq 3$ with $p \equiv 3 \bmod 4$ appearing with odd multiplicity in the factorizations of both $N_3(\delta_3)$ and $N_2(\delta_2)$. From this we can conclude that both 17 and -17 are squares modulo p, which is absurd since $p \equiv 3 \bmod 4$.

Remark: Note that $(x, y) \mapsto (x^2, y)$ gives a nonconstant map from $C : y^2 = 3(x^2+1)(x^2+17)(x^2-17)$ to the elliptic curve $E : y^2 = 3(x+1)(x+17)(x-17)$ which has Mordell-Weil group $E(\mathbb{Q}) = E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The preimages of the 2-torsion points on E are clearly not defined over $\mathbb{Q}$, so $C(\mathbb{Q}) = \emptyset$. A result of Siksek extending ideas of Scharaschkin shows that this failure of the Hasse principle is explained by a Brauer-Manin obstruction [Sik, V.Sc]. It is thus natural that there is an appeal to quadratic reciprocity in the final line of the proof above.

3. Background for the genus one case

In all that follows, K is a field, p is a prime and $m, n \geq 2$ are integers. We assume p, m and n are not divisible by the characteristic of K. An n-covering of a smooth curve Y is a non-singular, absolutely irreducible covering $Z \to Y$ which is unramified and Galois over the separable closure $\bar{K}$ of K, with group $\mathrm{Aut}(Z/Y) \simeq \mathrm{Jac}(Y)[n]$, where $\mathrm{Jac}(Y)[n]$ denotes the n-torsion subgroup of the Jacobian variety. We denote the set of isomorphism classes of n-coverings of Y by $\mathrm{Cov}^{(n)}(Y/K)$, two n-coverings being considered isomorphic if they are K-isomorphic as Y-schemes.

Let E be an elliptic curve over K and let $C \xrightarrow{\rho} E$ be an n-covering of $E = \mathrm{Jac}(C)$, also defined over K. The isomorphism class of (C, ρ) can be identified with an element of $\mathrm{H}^1(K, E[n])$. When no confusion can arise, we will supress mention of the covering map and use C also to denote the corresponding element of $\mathrm{H}^1(K, E[n])$.

Tate's result. We investigate the existence of a lift of C to an mn-covering of E with certain additional properties. First one must ask if there exists a lift at all. When K is a number field, C is everywhere locally solvable and m is prime, Tate has shown ([Cas, Section 5]) that this is indeed the case. We begin by reviewing this result.

There is an exact sequence, $0 \to E[m] \xrightarrow{i} E[nm] \xrightarrow{m} E[n] \to 0$. Galois cohomology then gives an exact sequence,

$$\mathrm{H}^1(K, E[m]) \xrightarrow{i_*} \mathrm{H}^1(K, E[mn]) \xrightarrow{m_*} \mathrm{H}^1(K, E[n]) \xrightarrow{\delta} \mathrm{H}^2(K, E[m]) \,.$$

We call any $D \in \mathrm{H}^1(K, E[mn])$ such that $m_*D = C$ a lift of C to an mn-covering. There is a canonical map $\mathrm{Cov}^{(m)}(C/K) \to \mathrm{H}^1(K, E[mn])$, given by composing the covering maps. The image of this map is the set of all lifts of C to an mn-covering.

From the exactness of the sequence above, one sees that $\delta(C) \in \mathrm{H}^2(K, E[m])$ presents an obstruction to lifting C to an mn-covering. One simple, but important, observation is that this obstruction vanishes if C has a K-rational point. When $K = k$ is a number field and C is everywhere locally solvable, this means that the obstruction vanishes everywhere locally. What Tate proves is that, for m prime, $\mathrm{H}^2(k, E[m])$ satisfies the Hasse principle. So, for C everywhere locally solvable, the obstruction vanishes globally.

Our proof of theorem 1.2 is similar. First we identify the relevant obstruction to having a lift to a covering of the desired form. This is given in proposition 3.1 below. Then for $p = 2$ we show that over a number field this obstruction satisfies the Hasse principle. This is proposition 3.4. Theorem 1.2 then follows. It is worth noting that our proof requires Tate's result; in order to properly interpret the obstruction given in proposition 3.1, we require the existence of some p-covering of C.

The period-index obstruction map. The n-coverings with 'trivial obstruction' are those that can be represented as so-called genus one normal curves of degree n. Such an object is a smooth genus one curve, together with the map to $\mathbb{P}^{n-1}$ associated to some K-rational divisor of degree n. When $n = 2$, this gives a double cover of $\mathbb{P}^1$, for $n > 2$ it is an embedding of degree n.

An n-covering $\pi : C \to E$ is a twist of the multiplication by n isogeny on E. Hence there is an isomorphism $\phi : C \to E$, defined over some extension of K, such that $\pi = [n] \circ \phi$. Pulling back the divisor $n.0_E$ along ϕ gives

a K-rational divisor class on C. If this class can be represented by a K-rational divisor, then it can be used to give a model for C as a genus one normal curve of degree n. In general, however, not every K-rational divisor class can be represented by a K-rational divisor. One has an exact sequence (see [CFOSS, Section 2] and [Lic])

$$0 \to K^\times \to K(C)^\times \to \mathrm{Div}_K(C) \to \mathrm{Pic}_K(C) \xrightarrow{\delta_C} \mathrm{Br}(K)\,.$$

The map δ_C gives the obstruction to a K-rational divisor class being represented by a K-rational divisor.

Following [CFOSS] we use $\mathrm{Ob}_n : \mathrm{H}^1(K, E[n]) \to \mathrm{Br}(K)$ to denote the map sending an n-covering C to $\delta_C([\phi^* n.0_E])$. We refer to $\mathrm{Ob}_n(C)$ as the obstruction algebra of C and say that C has trivial period-index obstruction if $\mathrm{Ob}_n(C) = 0$. Composing Ob_{mn} with the canonical map $\mathrm{Cov}^{(m)}(C/K) \to \mathrm{H}^1(K, E[mn])$, gives a map which, as a slight abuse of notation, we also denote by Ob_{mn}. We say that an m-covering of C has trivial *period-index obstruction* if its image under this map is trivial. We denote the set of isomorphism classes of m-coverings of C with trivial period-index obstruction by $\mathrm{Cov}_0^{(m)}(C/K)$. It is worth noting that the set $\mathrm{Cov}^{(m)}(C/K)$ does not depend on the structure of C as an n-covering, but the map Ob_{mn} and the set $\mathrm{Cov}_0^{(m)}(C/K)$ do.

Remark: We use the term 'period-index obstruction' to distinguish this from the other obstructions under consideration in this paper. The period of a smooth genus one curve may be defined as its order in the Weil-Châtelet group of its Jacobian, while its index is the minimal positive degree of a K-rational divisor. A curve of period dividing n can be given the structure of an n-covering. If this covering has trivial period-index obstruction, then the index of the underlying curve also divides n. Conversely, any curve of index dividing n can be given the structure of an n-covering of its Jacobian which has trivial period-index obstruction.

O'Neil has shown [O'N] that the obstruction map is quadratic. This means that $\mathrm{Ob}_n(aC) = a^2\,\mathrm{Ob}_n(C)$, for $a \in \mathbb{Z}$, and that the map $(C, C') \mapsto \mathrm{Ob}_n(C + C') - \mathrm{Ob}_n(C) - \mathrm{Ob}_n(C')$ is bilinear. In fact the pairing is the cup product induced by the Weil pairing on $E[n]$. Another important property is that the image of Ob_n is contained in the n-torsion subgroup of $\mathrm{Br}(K)$. The following diagram relates the obstruction maps of various levels (see [ClSh, Proposition 6] for a proof)

$$\begin{array}{ccccc}
\mathrm{H}^1(K, E[m]) & \xrightarrow{i_*} & \mathrm{H}^1(K, E[mn]) & \xrightarrow{m_*} & \mathrm{H}^1(K, E[n]) \\
\downarrow{\scriptstyle \mathrm{Ob}_m} & & \downarrow{\scriptstyle \mathrm{Ob}_{mn}} & & \downarrow{\scriptstyle \mathrm{Ob}_n} \\
\mathrm{Br}(K)[m] & \xrightarrow{n} & \mathrm{Br}(K)[mn] & \xrightarrow{m} & \mathrm{Br}(K)[n]
\end{array}$$

Before proceeding we make the following observation. If $C(K) \neq \emptyset$, then $\mathrm{Cov}_0^{(m)}(C/K) \neq \emptyset$. Indeed, any rational point of C must lift to a rational point on some m-covering of C and any mn-covering of E which contains a rational point has trivial period-index obstruction.

Step 1: The obstruction to $\mathrm{Cov}_0^{(p)}(C/K) \neq \emptyset$

We assume now that C is a p-covering of its Jacobian and that $\mathrm{Ob}_p(C) = 0$. Furthermore we will assume that $\mathrm{Cov}^{(p)}(C/K)$ is nonempty. These assumptions are satisfied if $C(K) \neq \emptyset$ or if K is a number field and C is everywhere locally solvable. We use i_* to denote the map $\mathrm{H}^1(K, E[p]) \to \mathrm{H}^1(K, E[p^2])$ induced by the inclusion $E[p] \to E[p^2]$.

Let X denote the set of flex points of C. We simply define this to be the preimage of 0_E under the covering map. In the terminology of [CFOSS] this is the $E[p]$-torsor corresponding the class of C in $\mathrm{H}^1(K, E[p])$. In particular, the action of E on C restricts to give a simply transitive action of $E[p]$ on X. If one chooses an appropriate model for C as a genus one normal curve of degree p, the set of flex points can be given a geometric interpretation. In the case $p = 2$, X is the set of Weierstrass points of C considered as a double cover of $\mathbb{P}^1$. For odd p, the flex points are the points C where there is some hyperplane meeting C with multiplicity p.

We define $\mathrm{Aff}(X, \mu_p)$ to be the G_K-module of affine maps from X to μ_p (we consider X as the affine space underlying the $\mathbb{F}_p$-vector space $E[p]$). This is a sub-G_K-module of the space of all maps, $\mathrm{Map}(X, \mu_p)$. In the case $p = 2$, $\mathrm{Aff}(X, \mu_p)$ is the kernel of the norm map $N : \mathrm{Map}(X, \mu_p) \to \mu_p$ sending a map to the product of its values at the points of X.

The constant maps form a subgroup $\mu_p \subset \mathrm{Aff}(X, \mu_p)$. The quotient can be identified with the group of linear maps $\mathrm{Hom}(E[p], \mu_p)$, which in turn can be identified with $E[p]$ via the Weil pairing. This gives an exact sequence

$$1 \to \mu_p \to \mathrm{Aff}(X, \mu_p) \to E[p] \to 0\,.$$

Taking Galois cohomology yields an exact sequence

$$\mathrm{H}^1(K, \mathrm{Aff}(X, \mu_p)) \to \mathrm{H}^1(K, E[p]) \xrightarrow{\Upsilon} \mathrm{Br}(K)[p] \xrightarrow{\alpha} \mathrm{H}^2(K, \mathrm{Aff}(X, \mu_p))\,.$$

We will interpret α as the relevant obstruction to having $\mathrm{Cov}_0^{(p)}(C/K) \neq \emptyset$. First note that the obstruction algebra associated to any $D \in \mathrm{Cov}^{(p)}(C/K)$ is actually p-torsion. This follows from the compatibility of Ob_p and Ob_{p^2}, since we have assumed $\mathrm{Ob}_p(C) = 0$.

Proposition 3.1. *The composition $\alpha \circ \mathrm{Ob}_{p^2} : \mathrm{Cov}^{(p)}(C/K) \to \mathrm{H}^2(K, \mathrm{Aff}(X, \mu_p))$ is constant. Moreover, $\alpha \circ \mathrm{Ob}_{p^2} = 0$ if and only if $\mathrm{Cov}_0^{(p)}(C/K) \neq \emptyset$.*

The proposition follows from the next 2 lemmas. Given a p-covering $\pi : D \to C$, and a cocycle $\xi \in Z^1(K, E[p])$, the twist $\pi_\xi : D_\xi \to C$ of $D \to C$ by ξ is also a p-covering of C. This gives an action of $\mathrm{H}^1(K, E[p])$ on $\mathrm{Cov}^{(p)}(C/K)$ which is simply transitive. The first lemma identifies how Ob_{p^2} changes under this action; the second relates this to α.

Lemma 3.2. *Let $D \in \mathrm{Cov}^{(p)}(C/K)$ and $\xi \in \mathrm{H}^1(K, E[p])$. Then $\mathrm{Ob}_{p^2}(D_\xi) - \mathrm{Ob}_{p^2}(D) = C \cup_p \xi$, where $\cup_n$ denotes the cup product associated to the Weil pairing on $E[n]$.*

Proof: The image in $\mathrm{H}^1(K, E[p^2])$ of D_ξ is the sum $D + i_*(\xi)$. The bilinear pairing associated to Ob_{p^2} is the cup product pairing $\cup_{p^2}$. So

$$D \cup_{p^2} i_*\xi = \mathrm{Ob}_{p^2}(D + i_*\xi) - \mathrm{Ob}_{p^2}(D) - \mathrm{Ob}_{p^2}(i_*\xi)\,.$$

Since $\mathrm{Ob}_{p^2} \circ i_* = p\,\mathrm{Ob}_p = 0$, the final term vanishes. Using the compatibility of the Weil pairings of levels p and p^2 (e.g. [Sil, III.8.1e]), we see that the cup product appearing is equal to $pD \cup_p \xi = C \cup_p \xi$. This completes the proof. □

Lemma 3.3. $\Upsilon(\xi) = C \cup_p \xi$.

Proof: Use $\rho : C \to E$ to denote the covering map and fix isomorphism $\phi : C \to E$ (defined over some extension of K) such that $[p] \circ \phi = \rho$. We use e_p to denote the Weil pairing and G_K for the absolute Galois group of K. For any $\sigma \in G_K$, ${}^\sigma\phi - \phi$ may be identified with an element of $E[p]$ and the class of C in $\mathrm{H}^1(K, E[p])$ is given by the cocycle $\sigma \mapsto ({}^\sigma\phi - \phi)$. Then the value of the cup product $C \cup_p \xi$ on a pair $(\sigma, \tau) \in G_K \times G_K$ is $e_p({}^\sigma\phi - \phi, {}^\sigma\xi_\tau)$.

Now let $\xi \in \mathrm{H}^1(K, E[p])$. Υ is a connecting homomorphism, so to compute $\Upsilon(\xi)$ we first lift to a cochain with values in $\mathrm{Aff}(X, \mu_p)$. For given $P \in E[p]$, the map $X \ni x \mapsto e_p(\phi(x), P) \in \mu_p$ is affine and its image under $\mathrm{Aff}(X, \mu_p) \to E[p]$ is P. So lifting ξ we get the cochain $\sigma \mapsto e_p(\phi(-), {}^\sigma\xi) \in \mathrm{Aff}(X, \mu_p)$. Now we compute the coboundary of this cochain. Its value on a pair $(\sigma, \tau) \in G_K \times G_K$ is given by

$$\frac{{}^\sigma e_p(\phi, \xi_\tau) \cdot e_p(\phi, \xi_\sigma)}{e_p(\phi, \xi_{\sigma\tau})} = \frac{e_p({}^\sigma\phi, {}^\sigma\xi_\tau)}{e_p(\phi, {}^\sigma\xi_\tau)} = e_p({}^\sigma\phi - \phi, {}^\sigma\xi_\tau)\,.$$

This is the same as the cup product computed above, so the lemma is proven.

□

Together the lemmas show that the image $\mathrm{Ob}_{p^2}(\mathrm{Cov}^{(p)}(C/K)) \subset \mathrm{Br}(K)[p]$ is a coset of the kernel of α. On the other hand, $\mathrm{Cov}_0^{(p)}(C/K) \neq \emptyset$ if and only if this coset contains $0 \in \mathrm{Br}(K)[p]$. This proves the proposition.

Step 2: The Hasse principle

Assume now that $K = k$ is a number field and that C is everywhere locally solvable. Then $\alpha \circ \mathrm{Ob}_{p^2}$ is constant, equal to say $a \in \mathrm{H}^2(k, \mathrm{Aff}(X, \mu_p))$, and a vanishes everywhere locally. So theorem 1.2 is a consequence of the following proposition.

Proposition 3.4. *A class in $\mathrm{H}^2(k, \mathrm{Aff}(X, \mu_2))$ is trivial if it is everywhere locally trivial.*

For the moment we will continue to work with an arbitrary prime p. To ease notation let $M = \mathrm{Aff}(X, \mu_p)$. By Poitou-Tate duality, the Hasse principle holds or fails simultaneously for $\mathrm{H}^2(k, M)$ and $\mathrm{H}^1(k, M^\vee)$, where $M^\vee = \mathrm{Hom}(M, \mu_p)$. Our strategy is to write down a map from $\mathrm{H}^1(k, M^\vee)$ to a group known to satisfy the Hasse principle. The kernel of this map is finite and depends only on the action of G_k on the flex points of C. For fixed p there are only finitely many possibilities for the action, and for each, the kernel can be computed. For $p = 2$ it turns out that the map is always injective. For odd p this is no longer the case.

Let $R = \mathrm{Map}_k(M, \bar{k})$ be the algebra of all G_k-equivariant maps from M to $\bar{k}$. This is the étale k-algebra corresponding to the G_k-set M under the usual categorical (anti-)equivalence between G_k-sets and étale k-algebras. We have $\bar{R} = R \otimes \bar{k} = \mathrm{Map}(M, \bar{k})$ and $\mu_p(\bar{R}) = \mathrm{Map}(M, \mu_p)$.

Let Q denote the quotient of $\mu_p(\bar{R}) = \mathrm{Map}(M, \mu_p)$ by the subspace consisting of maps that are homomorphisms. Then we have an exact sequence

$$0 \to M^\vee \to \mu_p(\bar{R}) \xrightarrow{q} Q \to 0\,.$$

Taking the Galois cohomology of this sequence over k and its completions we obtain a diagram with exact rows

$$\begin{array}{ccccccc}
\mu_p(R) & \xrightarrow{q} & \mathrm{H}^0(k, Q) & \longrightarrow & \mathrm{H}^1(k, M^\vee) & \longrightarrow & R^\times/R^{\times p} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\prod \mu_p(R_v) & \xrightarrow{q} & \prod \mathrm{H}^0(k_v, Q) & \longrightarrow & \prod \mathrm{H}^1(k_v, M^\vee) & \longrightarrow & \prod R_v^\times/R_v^{\times p}
\end{array}$$

The Grunwald-Wang theorem ([CoN, Theorem 9.1.11]), implies that the rightmost vertical map is injective. So if $\mathrm{H}^1(k, M^\vee) \to R^\times/R^{\times p}$ is injective, then the Hasse principle holds for $\mathrm{H}^1(k, M^\vee)$.

The action of G_k on X factors through the affine general linear group $\mathrm{AGL}_2(\mathbb{F}_p)$ and determines the action on μ_p. The actions of G_k on X, μ_p and any modules derived from the two (e.g. $M^\vee$ and $\mu_p(\bar{R})$) depend only on its image in $\mathrm{AGL}_2(\mathbb{F}_p)$. If this is denoted by G, then we have a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\mathrm{H}^0(k, \mu_p(\bar{R})) & \xrightarrow{q} & \mathrm{H}^0(k, Q) & \longrightarrow & \mathrm{H}^1(k, M^\vee) & \longrightarrow & \mathrm{H}^1(k, \mu_p(\bar{R})) \\
\| & & \| & & & & \\
\mathrm{H}^0(G, \mu_p(\bar{R})) & \xrightarrow{q} & \mathrm{H}^0(G, Q) & \longrightarrow & \mathrm{H}^1(G, M^\vee) & \longrightarrow & \mathrm{H}^1(G, \mu_p(\bar{R}))
\end{array}$$

The kernel of the map $\mathrm{H}^1(k, M^\vee) \to R^\times/R^{\times p}$ is thus isomorphic to $\mathrm{H}^0(G, Q)/q(\mathrm{H}^0(G, \mu_p(\bar{R})))$. Note also that this only depends only on the conjugacy class of G in $\mathrm{AGL}_2(\mathbb{F}_p)$. For a subgroup $H \subset \mathrm{AGL}_2(\mathbb{F}_p)$, let us use $\mathcal{R}(H)$ to denote $\mathrm{H}^0(H, Q)/q(\mathrm{H}^0(H, \mu_p(\bar{R})))$. Thus injectivity of the map $\mathrm{H}^1(k, M^\vee) \to R^\times/R^{\times p}$ is equivalent to $\mathcal{R}(G) = 0$.

We can now verify the Hasse principle for $\mathrm{H}^2(k, \mathrm{Aff}(X, \mu_2))$.

Lemma 3.5. *For any subgroup $H \subset \mathrm{AGL}_2(\mathbb{F}_2) = S_4$ we have $\mathcal{R}(H) = 0$.*

Proof: Up to conjugacy there are 11 subgroups of S_4. For each $\mathcal{R}(H)$ is a combinatorial object that we can compute using linear algebra over $\mathbb{F}_2$. This was done using MAGMA. We give details in the appendix. □

For odd p, this Hasse principle can fail - we have the following example. The cubic curve

$$C : x^3 + x^2z + 5xy^2 - 4xyz - 9xz^2 + 2y^3 - 2y^2z + 9yz^2 - 6z^3 = 0$$

(together with an appropriate covering map) represents a class in $\mathrm{Sel}^{(3)}(\mathrm{Jac}(C)/\mathbb{Q})$. If F' denotes the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all flex points of C, then its Galois group $G = \mathrm{Gal}(F'|\mathbb{Q})$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The subgroup $G' = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ acts transitively on X and the quotient corresponds to adjoining the cube roots of unity to $\mathbb{Q}$. A computation as in the lemma shows that $\mathcal{R}(G) \simeq \mathcal{R}(G') \neq 0$ and that up to conjugacy these are the only subgroups of $\mathrm{AGL}_2(\mathbb{F}_3)$ with this property. Above any p there are at least 3 primes of F' (only the ramified primes need to be checked), so all decomposition groups are of index ≥ 3 in G. In particular, none of them are isomorphic to G or G'. So, for each p, $\mathcal{R}(G_p) = 0$ and the Hasse principle must fail. Indeed, the kernels of $\mathcal{R}(G) \to \prod \mathcal{R}(G_p)$ and $\mathrm{H}^1(\mathbb{Q}, \mathrm{Aff}(X, \mu_3)^\vee) \to \prod \mathrm{H}^1(\mathbb{Q}_p, \mathrm{Aff}(X, \mu_3)^\vee)$ are isomorphic.

Of course this does not tell us that there are no 3-coverings of C with trivial obstruction, and it is in fact not the case. In the author's PhD thesis it is (will be) shown how $\mathrm{Cov}_0^{(p)}(C/K)$ can be represented as an algebraic object analogous to the set H_K defined in the hyperelliptic case. For the curve above, we can explicitly exhibit classes in the corresponding set. One might be able to use this as in the hyperelliptic case to find a counter-example. But in practice one would end up having to disprove solvability of a 'norm configuartion' that is significantly more complicated than that describing H_K.

We performed a similar computation for all odd $p \leq 11$; a notable pattern emerges. With respect to inclusion, there are unique (up to conjugacy) minimal and maximal subgroups G' and G in $\mathrm{AGL}_2(\mathbb{F}_p)$ for which $\mathcal{R} \neq 0$. G' acts transitively on X, trivially on μ_p and is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. G is an extension of G' by $\mathbb{Z}/(p-1)\mathbb{Z}$, acting nontrivially on μ_p and $E[p]^G = E[p]^{G'} \simeq \mathbb{Z}/p\mathbb{Z}$. Assuming G is realized as the image of an

absolute Galois group, the intermediate groups $G \supset G'' \supset G'$ correspond to the intermediate fields of the p-th cyclotomic extension of the base field. If K is a field containing μ_p, then there is an essentially unique action on the flex points for which the Hasse principle above can fail.

REMARK: One can perform similar computations in the hyperelliptic case. The analogue of $\mathrm{Aff}(X, \mu_p)$ is the space $\mathcal{N}$ of maps, from the set of Weierstrass points to μ_2, that take the value -1 at an even number of points. Provided $\mathrm{Cov}^{(2)}(C) \neq \emptyset$, one should be able to interpret the obstruction to $H_k \neq \emptyset$ as an element of $\mathrm{H}^2(k, \mathcal{N})$. In this way one is lead to consider the validity of the Hasse principle for $\mathrm{H}^1(k, \mathcal{N}^\vee)$, which can be attacked exactly as in the genus one case.

The action of G_k on the Weierstrass points factors through the symmetric group S_{2g+2}, where g is the genus. For $g = 2$, this leads to 56 conjugacy classes of subgroups. A computation as in lemma 3.5 can prove that the Hasse principle holds for all but three. The remaining groups are isomorphic to A_5, A_4 (both acting transitively on the Weierstrass points) and the Klein 4-group, respectively. The last is the relevant group for the curve considered in theorem 1.3; it was this potential failure of the Hasse principle that initially lead us to consider such curves.

Appendix: description of the computation

Since the proof of several statements above relies entirely on a machine computation, we feel it appropriate to give some details. We describe how $\mathcal{R}(G)$ (as defined above) can be computed for an arbitrary subgroup $G \subset \mathrm{AGL}_2(\mathbb{F}_p)$. So that we may use additive notation, we will identify μ_p with $\mathbb{Z}/p\mathbb{Z}$. Note however, that $\mathrm{AGL}_2(\mathbb{F}_p)$ then acts on $\mathbb{Z}/p\mathbb{Z}$ nontrivially.

We fix a labelling for the set of flex points $X = \{x_1, \dots, x_{p^2}\}$. We can then identify the action of $\mathrm{AGL}_2(\mathbb{F}_p)$ on X with that of a subgroup of S_{p^2} on $\{1, \dots, p^2\}$. We fix a basis $\{e_1, \dots, e_{p^2}\}$ for $\mathrm{Map}(X, \mu_p)$ consisting of the maps $e_i(x_j) = \delta_{i,j}$. The action of $g \in \mathrm{AGL}_2(\mathbb{F}_p)$ on e_i is, by definition, $g \cdot e_i : x \mapsto e_i(g^{-1}(x))^g$. The determinant on $\mathrm{AGL}_2(\mathbb{F}_p)$ is the cyclotomic character, so we can write this more succintly as $g \cdot e_i = \det(g) e_{g(i)}$. Using this, we can write down, for $g \in \mathrm{AGL}_2(\mathbb{F}_p)$, a matrix A_g giving the action of g on $\mathrm{Map}(X, \mu_p)$.

We also need to write down the 3-dimensional subspace $\mathrm{Aff}(X, \mu_p) \subset \mathrm{Map}(X, \mu_p)$. When $p = 2$, a map is affine if and only if the product, over $x \in X$, of its values is 1. For example, we may take the basis $\{e_1 + e_2, e_1 + e_3, e_1 + e_4\}$. In the case $p = 3$, one can check that a map is affine if and only if the product of its values on any affine line in X is 1 (we consider X as the affine space underlying $\mathbb{F}_p^2$). Using this we have no difficulty choosing a basis. For larger p, one can give a similar description.

The elements of $\mathrm{Aff}(X, \mu_p)$ give us a basis for $\mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p)$. Namely, we choose $\{f_\phi : \phi \in \mathrm{Aff}(X, \mu_p)\}$, where $f_\phi \in \mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p)$ is the map $f_\phi(\phi') = \delta_{\phi,\phi'}$. We fix a labelling $\phi_1, \dots, \phi_{p^3}$ for the affine maps. The action of $\mathrm{AGL}_2(\mathbb{F}_p)$ on $\mathrm{Aff}(X, \mu_p)$ can then be identified with that of a subgroup of S_{p^3} on $\{1, \dots, p^3\}$. Then as above, the action of $g \in \mathrm{AGL}_2(\mathbb{F}_p)$ is given by $g \cdot \phi_i = \det(g)\phi_{g(i)}$ and we can write down a matrix B_g giving the corresponding automorphism of $\mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p)$.

Given a basis for $\mathrm{Aff}(X, \mu_p)$, one has no difficulty writting down a basis for the 3-dimensional subspace $\mathrm{Aff}(X, \mu_p)^\vee = \mathrm{Hom}(\mathrm{Aff}(X, \mu_p), \mu_p) \subset \mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p)$. We then write down a matrix M giving the canonical map

$$M : \mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p) \to \mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p) / \mathrm{Hom}(\mathrm{Aff}(X, \mu_p), \mu_p) = Q\,.$$

Let I be the $p^3 \times p^3$ identity matrix. A map $\psi \in \mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p)$ is invariant under the action of g if and only if $\psi \in \ker(B_g - I)$. Similarly $\psi \in \mathrm{Map}(\mathrm{Aff}(X, \mu_p), \mu_p)$ represents a g-invariant class in Q if and only if $\psi \in \ker(M \cdot (B_g - I))$. So if $G \subset \mathrm{AGL}_2(\mathbb{F}_p)$ is a subgroup, then

$$\mathcal{R}(G) = \frac{M\left(\bigcap_{g \in G} \ker(M \cdot (B_g - I))\right)}{M\left(\bigcap_{g \in G} \ker(B_g - I)\right)}\,.$$

Note also that it suffices to compute the intersection over a set of generators of G.

References

[BrSt] N. Bruin and Michael Stoll: Two-cover descent on hyperelliptic curves, *Math. Comp.* **78** (2009) 2347-2370.

[Cas] J.W.S. Cassels: Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. reine angew. Math.* **221** (1962) 95-112.

[ClSh] P.L. Clark and S. Sharif: Period, index and potential Sha, *preprint* (2010).

[CFOSS] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll: Explicit n-descent on elliptic curves. I. Algebra, *J. reine angew. Math.* **615** (2008) 121-155.

[Lic] S. Lichtenbaum: The period-index problem for elliptic curves, *Amer. J. Math.* **90** (1968) 1209-1223.

[MSS] J. Merriman, S. Siksek and N.P. Smart: Explicit 4-descents on an elliptic curve, *Acta. Arith.* **77** (1996) no.4, 385-404.
[CoN] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of number fields. *Grundlehren der math. Wissenschaften* **323**, Springer-Verlag, 2000.
[O'N] C. O'Neil: The period-index obstruction for elliptic curves, *J. Number Theory.* **95** (2002) 329-339.
[PoSc] B. Poonen and E.F. Schaefer: Explicit descent for Jacobians of cyclic covers of the projective line. *J. reine angew. Math.* **448** (1997) 141-188.
[Sch] E.F. Schaefer: 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory.* **51** (1995) 219-232.
[V.Sc] V. Scharaschkin: The Brauer-Manin obstruction for curves. Manuscript 1998.
[Sik] S. Siksek: On the Brauer-Manin obstruction for curves havin split Jacobians, *Journal de théorie des nombres de Bordeaux* **16**, (2004) 773-777.
[Sil] J. Silverman: The arithmetic of elliptic curves. *Graduate Texts in Mathematics* **106**, Springer-Verlag, 1986.