TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 357, Number 11, Pages 4329–4347
S 0002-9947(05)03954-1
Article electronically published on June 22, 2005

TOWERS OF 2-COVERS OF HYPERELLIPTIC CURVES

NILS BRUIN AND E. VICTOR FLYNN

Abstract. In this article, we give a way of constructing an unramified Galois-cover of a hyperelliptic curve. The geometric Galois-group is an elementary abelian 2-group. The construction does not make use of the embedding of the curve in its Jacobian, and it readily displays all subcovers. We show that the cover we construct is isomorphic to the pullback along the multiplication-by-2 map of an embedding of the curve in its Jacobian.

We show that the constructed cover has an abundance of elliptic and hyperelliptic subcovers. This makes this cover especially suited for covering techniques employed for determining the rational points on curves. In particular the hyperelliptic subcovers give a chance for applying the method iteratively, thus creating towers of elementary abelian 2-covers of hyperelliptic curves.

As an application, we determine the rational points on the genus 2 curve arising from the question of whether the sum of the first n fourth powers can ever be a square. For this curve, a simple covering step fails, but a second step succeeds.

1. Introduction

The motivation for the techniques we develop in this paper is the problem of finding sharp bounds on the number of rational points on an algebraic curve over a number field. An important instrument for that is a method conceived by Chabauty [7] based on p-adic analytic intersections in the Jacobian of the curve. For this method to succeed, one should have that the Mordell-Weil rank of the Jacobian is small compared to its dimension.

If Chabauty's method does not apply directly to a curve C, or is too difficult to apply, one may try to construct a finite set of curves that cover the original curve, such that each rational point of C lifts to a rational point on one of the covers, a so-called *covering collection*. It then suffices to find the rational points on each of the covering curves. Chabauty's method may apply to each of those covers independently.

The covering curves will in general be of much higher genus than the original curve. Folklore suggests that Mordell-Weil ranks of simple abelian varieties tend to

Received by the editors July 9, 2001 and, in revised form, September 22, 2002.

2000 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.

Key words and phrases. Covers of curves, hyperelliptic curves, rational points, descent, method of Chabauty.

The first author was supported by the Pacific Institute for the Mathematical Sciences, Simon Fraser University and the University of British Columbia.

The second author received financial support from EPSRC Grant Number GR/R82975/01.

be moderate. Thus, if the Jacobian of the covering curve consists of few, high dimensional simple factors, then one would generally expect that Chabauty's method should be applicable.

At the other end of the spectrum, things look grim at first. Suppose we have a curve C over a number field K with $\mathrm{rkJac}(C)(K) \geq \mathrm{genus}(C)$ and a cover D such that $\mathrm{Jac}(D)$ is isogenous over K to $\mathrm{Jac}(C) \oplus E_1 \oplus \cdots \oplus E_n$, where the E_i are elliptic curves over K. We have that D covers each E_i. If there is a truly non-trivial point $\overline{P} \in C(K)$ that lifts to $P \in D(K)$, then there is no reason for the image of P in any of the $E_i(K)$ to be a torsion point. If all the E_i have positive Mordell-Weil rank, then the cover D/C is essentially useless from the point of view of Chabauty's method. One encounters this situation if one considers a hyperelliptic curve C of genus 2 with $\mathrm{Jac}(C)[2]$ pointwise defined over K and D a pullback of an embedding of C in $\mathrm{Jac}(C)$ along multiplication by two. For hyperelliptic curves of higher genus with full rational 2-torsion, the situation is similar.

In this paper, we show that D covers other hyperelliptic curves C' besides C. If one knows $C'(K)$, then one can find $D(K)$ by examining the fibers of D above $C'(K)$. We propose to repeat the construction used to obtain D from C, but now for C'. We thus obtain a finite set of covers D'/C' such that the rational points of C' are covered by those of the D'. The curves C' may be more suitable for covering methods (and if they are not, then one may consider further covering steps).

Furthermore, the construction in this paper gives a very explicit description of the simple factors of $\mathrm{Jac}(D)$ as Weil-restrictions of Jacobians of hyperelliptic curves. This makes $\mathrm{Jac}(D)$ computationally reasonably accessible.

Note the complementary nature of both techniques. In general one would expect that one 2-covering step should suffice if the 2-torsion has a high degree field of definition. On the other hand, if the 2-torsion is defined over a small field, then a second covering step is probably feasible.

Whether we can actually carry out the necessary computations depends on whether we can find a finite index subgroup of the Mordell-Weil groups of the relevant abelian varieties. Unfortunately, the known methods for that are only conjecturally effective.

As an example of utilising towers of covers to find the rational points on hyperelliptic curves, we prove

Theorem 1.1. *The rational points on*

$$y^2 = \frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{1}{3}x^3 - \frac{1}{30}x$$

have

$$x \in \{-\frac{5}{4}, -\frac{6}{5}, -1, -\frac{1}{2}, -\frac{1}{9}, 0, \frac{1}{2}, 1, \infty\}.$$

It follows that the only integral points have $x \in \{0, 1\}$. We obtain an alternative proof to [15], that the sum of the first x fourth powers is not a square for $x > 1$.

2. Preliminaries

Let K be a number field. We write $\overline{K}$ for its algebraic closure and $\mathrm{Gal}(K) = \mathrm{Gal}(\overline{K}/K)$ for the Galois group of $\overline{K}$ over K. Let M be a $\mathrm{Gal}(K)$-module. For $i = 0, 1$, we write $H^i(K, M) = H^i(\mathrm{Gal}(K), M)$ for the Galois-cohomology groups

of M. Following [16, Theorem X.1.1(c)] we write

$$K(S,m) = \{b \in K^*/K^{*m} : \mathrm{ord}_v(b) \equiv 0 \mod m \text{ for all } v \notin S\}$$

and we extend the notation to semi-simple commutative algebras over K component-wise, where $v \notin S$ should be interpreted as "v is a prime not above a prime in S".

A curve C/K is a smooth, complete, absolutely irreducible variety of dimension 1 over K. Let D and C be two curves. We call D/C a *cover* if there is a non-constant morphism $D \to C$ defined over K. We consider the choice of the morphism to be fixed if we refer to the cover D/C.

The group $\mathrm{Aut}(D)$ is the group of degree 1 maps $D \to D$ defined over $\overline{K}$. Let D/C be a cover with the morphism $\phi : D \to C$. The group $\mathrm{Aut}(D/C) \subset \mathrm{Aut}(D)$ consists of $\psi \in \mathrm{Aut}(D)$ such that $\phi \circ \psi = \phi$. If $\#\mathrm{Aut}(D/C) = \deg(\phi)$, then D/C is a *Galois* cover.

A curve D' over K that is isomorphic to D over $\overline{K}$, is called a *twist* of D. We write $\mathrm{Twist}_K(D)$ for the set of K-isomorphism classes that contain a twist of D.

Theorem 2.1. *Let D be a curve over a number field K. Then we have*

$$\mathrm{Twist}_K(D) = H^1(K, \mathrm{Aut}(D)).$$

See [16, Theorem X.2.2].

Recall that $\xi \in H^1(K, \mathrm{Aut}(D))$ is represented by a 1-cocycle $\mathrm{Gal}(K) \to \mathrm{Aut}(D)$, denoted by $\sigma \mapsto \xi_\sigma$. A 1-cocycle satisfies $\xi_{\sigma\tau} = {}^\sigma\xi_\tau \circ \xi_\sigma$ for any $\sigma, \tau \in \mathrm{Gal}(K)$.

Let $\xi = (\sigma \mapsto \xi_\sigma) \in H^1(K, \mathrm{Aut}(D))$. Using ξ, we define a new $\mathrm{Gal}(K)$-action on $D(\overline{K})$. Let $P \in D(\overline{K})$ and $\sigma \in \mathrm{Gal}(K)$. Then the new action is given by ${}^{\sigma *}P = \xi_\sigma^{-1}({}^\sigma P)$. It is easily checked that ${}^{\sigma\tau *}P = {}^{\sigma *}({}^{\tau *}P)$. The set $D(\overline{K})$ equipped with this new action is again the set of $\overline{K}$-points of an algebraic curve over K. This is the curve D twisted by ξ. We denote this new curve by $\xi * D$. This construction gives a natural set-theoretic bijection $\psi_\xi : D(\overline{K}) \to \xi * D(\overline{K})$. It is induced by an isomorphism ψ_ξ of curves defined over $\overline{K}$. Of course, if ξ is non-trivial, then ψ_ξ is not defined over K. If ψ_ξ is represented by a coboundary, which means that there is a $\psi \in \mathrm{Aut}(D)$ such that $\xi_\sigma = {}^\sigma\psi^{-1} \circ \psi$, then $\psi_\xi = \psi$ and $\xi * D = D$.

3. Chabauty methods

3.1. **The original idea.** Let K be a number field and let C be an algebraic curve over K of genus $g > 1$. We know that $C(K)$ is finite, but all the known proofs are ineffective. The known proofs do give a bound on the size of $C(K)$, but usually those bounds are not attained.

If $C(K_\mathfrak{p})$ is empty for some completion $K_\mathfrak{p}$ of K at a prime $\mathfrak{p}$, then the subset $C(K)$ is empty too. The first problem is effectively decidable. Unfortunately, the Hasse principle, which states the converse, does not hold for all curves of positive genus.

If we have $P_0 \in C(K)$, then, by the Abel-Jacobi map $P \mapsto [P - P_0]$, we can view C as a subvariety of $J = \mathrm{Jac}(C)$ over K. In the absence of such a point P_0, we can still choose a canonical divisor ω and consider the non-constant map $C \to \mathrm{Jac}(C)$ defined by $P \mapsto [(2g-2)P - \omega]$. Provided that $\mathrm{Pic}^0(C/K) \simeq J(K)$, which is the case if $C(K_\mathfrak{p}) \neq \emptyset$ for all primes $\mathfrak{p}$, the argument applies. The map $P \mapsto [(2g-2)P - \omega]$ has a singular image, which introduces some extra technical

difficulties. We will concentrate on the case where we have a rational Abel-Jacobi map at our disposal.

Let $\mathfrak{p}$ be a prime of K over a finite rational prime p. The set $C(K)$ is contained in $J(K)$ and in $C(K_\mathfrak{p}) \subset J(K_\mathfrak{p})$. Let $\overline{J(K)}$ denote the p-adic topological closure of $J(K) \subset J(K_\mathfrak{p})$. Then $C(K) \subset C(K_\mathfrak{p}) \cap \overline{J(K)}$. The latter is the intersection of two p-adic analytic varieties. Therefore, we have analytic methods at our disposal to bound the size of the intersection. In particular, one can show that it is finite if $\dim(\overline{J(K)}) < \dim(J(K_\mathfrak{p}))$. This is always the case if $\mathrm{rk}(J(K)) < g$.

In practice, if $\mathrm{rk}(J(K)) < g$, one can often find a prime $\mathfrak{p}$ such that $\#C(K) = \#(C(K_\mathfrak{p}) \cap \overline{J(K)})$. Thus, if we know a subset of $C(K)$ that attains this size bound, then we know $C(K)$ itself. See [7] for the first mention of this idea and [8] for a more modern treatment. See [10] and [18] for detailed descriptions for an application to specific curves.

3.2. **Subcovers.** In order to carry out the construction suggested in Section 3.1, we have to know $J(K)$, or at least a subgroup of finite index. In practice this is one of the most difficult steps. Furthermore, these computations become rapidly more cumbersome with growing genus g. So, while from the theoretical point of view large genus is good because that leaves room for the Mordell-Weil rank of J being large while still satisfying $\mathrm{rk}(J(K)) < \mathrm{genus}(C)$, it is bad for actually carrying out the computations.

Suppose that C is a cover of another curve E over K. That means there is a non-constant morphism $\pi : C \to E$ over K. Then $\pi(C(K)) \subset E(K)$. If $E(K)$ is known and finite, then we only have to search the finite set $\pi^{-1}(E(K))$ for rational points to determine $C(K)$.

In particular, if E is an elliptic curve of (provable) rank 0 or a curve of genus 0 with no rational points (which, by the Hasse principle, can be shown by local means), then this construction gives a particularly easy way of finding $C(K)$.

A slightly more difficult case occurs if there is a subcover $\pi : C \to E$ over $\overline{K}$ that is only defined over some extension L of K. Let A be the Weil restriction $\Re_{L/K}(\mathrm{Jac}(E))$ in the sense of [2, §7.6]. Then, by definition, $\mathrm{Mor}_L(C, \mathrm{Jac}(E)) \simeq \mathrm{Mor}_K(C, A)$. Therefore, the non-constant map $C \to \mathrm{Jac}(C) \xrightarrow{\pi_*} \mathrm{Jac}(E)$ induces a non-constant map $\pi' : C \to A$ defined over K. We can now try to determine $\pi'(C)(K)$ using the same techniques as in Section 3.1 and then use the fact that C is a cover of $\pi'(C)$.

In carrying out this process, we have to determine (something close to) $A(K)$. However, this is isomorphic to $\mathrm{Jac}(E)(L)$. So, in this special case, we can get information on the Mordell-Weil group of an abelian variety of dimension $[L : K] \cdot \mathrm{genus}(E)$ by analysing the Mordell-Weil group of the $\mathrm{genus}(E)$-dimensional Jacobian of E over a degree $[L : K]$ extension of the base field of A. Thus, we interchange geometric dimensions for arithmetic degree. Given the present state of knowledge of number fields, this is desirable from a computational point of view.

Instead of translating information about $E(L)$ into information about $A(K)$, we might also go the other way and formulate our problem directly in terms of E. Suppose that C covers a curve S over K and that there is a cover $\phi : E \to S$ over L such that $\Phi : C \to S$ factors as $\phi \circ \pi$ over L. Note that, by choosing $S = \mathbb{P}^1$, there is an abundance of maps Φ, ϕ that satisfy this criterion. Since $\Phi(C(K)) \subset S(K)$ and $\pi(C(K)) \subset E(L)$, we see that if we can determine $\{P \in E(L) : \phi(P) \in S(K)\}$

and it is finite, then we can obtain $C(K)$ with a finite amount of work. If E is a genus 1 curve, then this set is computationally quite accessible. See [3] and [4] for details.

4. Covering techniques

It may happen that the methods described in Section 3.1 do not apply. As pointed out in [18], one may try to construct a set $\{D_\delta\}$ of covers of C such that the images of $D_\delta(K)$ together cover $C(K)$. We call such a set a *covering collection*. If one can find all $D_\delta(K)$, possibly with methods that failed on C, then one obtains $C(K)$ by taking the union of the images of $D_\delta(K)$. Obviously, it is desirable to construct *finite* covering collections. An unramified Galois cover of C gives rise to a finite covering collection.

Theorem 4.1 (Wetherell)**.** *Let $\phi : D \to C$ be an unramified Galois cover over a number field K. Then there is a finite set $\{\xi * D\}$ of twists of D, unramified outside the primes of bad reduction of the cover D/C, such that*

$$C(K) = \bigcup (\xi * \phi)(\xi * D(K)).$$

Proof. We repeat the proof from [18] to fix notation. Suppose we have a point $P \in D(\overline{K})$ with $\phi(P) \in C(K)$. Let $\sigma \in \mathrm{Gal}(K)$. Then

$$\phi({}^\sigma P) = {}^\sigma\phi({}^\sigma P) = {}^\sigma(\phi(P)) = \phi(P).$$

We see that $\mathrm{Gal}(K)$ permutes the $\overline{K}$-points of the fiber of ϕ above $\phi(P)$. Since D/C is Galois, it follows that there is a $\xi_\sigma \in \mathrm{Aut}(D/C)$ such that ${}^\sigma P = \xi_\sigma(P)$. Since

$$\xi_{\sigma\tau}(P) = {}^{\sigma\tau}P = {}^\sigma({}^\tau P) = {}^\sigma(\xi_\tau(P)) = {}^\sigma\xi_\tau({}^\sigma P) = {}^\sigma\xi_\tau \circ \xi_\sigma(P),$$

we see that $\xi = (\sigma \mapsto \xi_\sigma) \in H^1(K, \mathrm{Aut}(D/C))$. The cocycle representing ξ is a coboundary (i.e., ξ is trivial) if there is a $\psi \in \mathrm{Aut}(D/C)$ (or $\psi \in \mathrm{Aut}(D)$ if we are interested in twists of D alone as opposed to twists of the cover D/C) such that $\xi_\sigma = {}^\sigma\psi^{-1}\psi$ for all $\sigma \in \mathrm{Gal}(K)$. In that case we see that ${}^\sigma\psi({}^\sigma P) = \psi(P)$. Therefore, $\psi(P) \in D(K)$. If $\psi \in \mathrm{Aut}(D/C)$, then $\phi \circ \psi = \phi$ and thus that there is a rational point in the fiber of ϕ above $\phi(P)$.

Furthermore, if $\phi : D \to C$ has good reduction at a prime $\mathfrak{p}$ of K, then ξ is unramified at $\mathfrak{p}$. Let S be a finite set of primes containing the primes of bad reduction of D/C and the primes at infinity. Following [16], we write

$$H^1(K, \mathrm{Aut}(D/C); S)$$

for the classes of cocycles that are unramified outside S. This is a finite set. We have that $\psi_\xi(P) \in \xi * D(K)$. Furthermore, $\xi * \phi = \phi \circ \psi_\xi^{-1}$ is defined over K. Therefore, $\xi * D/C$ is again a cover over K. Furthermore, we see that the rational point $\psi_\xi(P)$ maps to $\phi(P)$ under $\xi * \phi$. This proves that $C(K)$ is covered by the rational points of a finite number of twists of D. □

This construction is easiest to carry out if $\mathrm{Aut}(D/C)$ is abelian. Furthermore, in order to keep the computations on the covers manageable, it is desirable that $\mathrm{Aut}(D/C)$ has many subgroups. This makes unramified elementary abelian 2-covers a natural choice for initial investigation.

5. Elementary 2-covers of $\mathbb{P}^1$, unramified outside a fixed set

As we show in Lemma 5.5, an unramified elementary abelian 2-cover of a hyperelliptic curve is an elementary abelian 2-cover of $\mathbb{P}^1$. We study the latter objects first.

We show that there is a unique maximal curve C_V over $\overline{K}$ with a prescribed ramification locus V, Galois and with an automorphism group of exponent 2. Furthermore, we show that this curve can be defined over the field of definition of the ramification locus, and we will determine its twists. By choice of coordinates, we can assume that ∞ is not in the ramification locus. However, the description of C_V is easier if $\infty \in V$, and in fact, if $\infty \notin V$, our approach will be to first construct $C_{V\cup\{\infty\}}$ and then identify C_V as a subcover.

Definition 5.1. A cover D/C is called an elementary abelian 2-cover if $\deg(D/C) = 2^n$ and $\mathrm{Aut}(D/C) \simeq \mathbb{F}_2^n$.

We use the term *locus* for a reduced subscheme of a variety. We mainly use the term for a 0-dimensional subscheme on a curve, which we will happily confuse with its point-set over the algebraic closure of the base field, as a Galois-set. In this special case, we define the degree to be the cardinality of the point set over the algebraic closure. If the locus is defined over a number field, then there is a notion of reduction at a prime, depending on the choice of model over the ring of integers. We say a locus has *good reduction* at a prime p if there is a model, relative to which the reduction is non-singular. Otherwise p is a prime of *bad reduction*.

Lemma 5.2. *Let $D/\mathbb{P}^1$ be an elementary abelian 2-cover of degree 2^n and let W be the locus of $\mathbb{P}^1$ above which $D/\mathbb{P}^1$ is ramified. We have*

$$\mathrm{genus}(D) = 2^{n-2}(\deg(W) - 4) + 1.$$

Proof. Apply Riemann-Hurwitz [16, Theorem II.5.9]. □

The following lemma is a restatement of the main result of Kummer theory ([1]) for exponent 2 in the case of algebraic curves.

Lemma 5.3. *Let D be an elementary abelian 2-cover of a curve C over an algebraically closed field $\overline{K}$ of characteristic 0. Then D is a fibre-product of double covers of C.*

Proof. We prove this by induction on $\deg(D) = 2^n$. For $n = 1$ the statement is obviously true. Suppose now that the statement is true for $n-1$. The group $\mathrm{Aut}(D/C)$ has $2^n - 1$ subgroups of index 2 and the same number of subgroups of order 2. The index 2 subgroups correspond to double covers, and the order 2 subgroups correspond to degree 2^{n-1} subcovers. Pick one of the degree 2^{n-1} subcovers C_1. By induction, C_1 is a fibre product of double covers. The curve C_1 has $2^{n-1} - 1$ degree 2 subcovers. Therefore, there is a degree 2 subcover C_2 of D that is not a subcover of C_1. That means that the fibre product $C_1 \times_{\mathbb{P}^1} C_2$ is a proper cover of C_1. On the other hand, D covers both C_1 and C_2, so it covers $C_1 \times_{\mathbb{P}^1} C_2$. From the degrees it follows that they are equal. □

Lemma 5.3 shows that double covers are the building blocks of elementary abelian 2-covers. The geometry of a double cover of $\mathbb{P}^1$ is entirely determined by its ramification locus. We define some notation for such double covers.

Let the *weight* of a vector $\mathbf{v}$ of an $\mathbb{F}_2$ vector space with basis be the number of non-zero coordinates of $\mathbf{v}$.

Definition 5.4. Let $V \subset \mathbb{P}^1$ be a 0-dimensional locus over an algebraically closed field $\overline{K}$. We write

$$\mathcal{V} := \{\text{even-weight vectors in the } \mathbb{F}_2\text{-vector space with basis } V(\overline{K})\}.$$

For non-zero $\mathbf{v} \in \mathcal{V}$, let $C_{\mathbf{v}}$ be the double cover of $\mathbb{P}^1$ that is ramified exactly at the points occurring in the support of $\mathbf{v}$.

Let x be a coordinate on $\mathbb{P}^1$. If $\{t_1, \ldots, t_{n-1}, \infty\} = V$, then we can identify $\mathcal{V}$ with the $\mathbb{F}_2$-vector space on $t_1, \ldots, t_{n-1}$ and we have

$$\overline{K}(C_{\mathbf{v}}) = \overline{K}(x)[y_{\mathbf{v}}]/(y_{\mathbf{v}}^2 - \prod_{i=1}^{n-1}(x - t_i)^{v_i}).$$

If $\infty \notin V$ and $\{t_1, \ldots, t_n\} = V$, then we have

$$\overline{K}(C_{\mathbf{v}}) = \overline{K}(x)[y_{\mathbf{v}}]/(y_{\mathbf{v}}^2 - \prod_{i=1}^{n}(x - t_i)^{v_i}).$$

In either case, let $\mathbf{v}, \mathbf{w} \in \mathcal{V}$ be independent vectors. By multiplying the relations for $y_{\mathbf{v}}^2$ and $y_{\mathbf{w}}^2$ we find

$$(y_{\mathbf{v}} y_{\mathbf{w}})^2 = \prod_{i=1}^{n}((x - t_i)^{v_i w_i})^2 (x - t_i)^{v_i + w_i}.$$

It follows that $\overline{K}(x, y_{\mathbf{v}} y_{\mathbf{w}}) \simeq \overline{K}(C_{\mathbf{v}+\mathbf{w}})$. Thus, the fibre product $C_{\mathbf{v}} \times_{\mathbb{P}^1} C_{\mathbf{w}}$ covers $C_{\mathbf{v}+\mathbf{w}}$. It follows that a curve that covers $C_{\mathbf{v}_1}, \ldots, C_{\mathbf{v}_r}$ covers all $C_{\mathbf{v}}$ with $\mathbf{v} \in \langle \mathbf{v}_1, \ldots, \mathbf{v}_r \rangle$. Lemma 5.3 shows that elementary abelian 2-covers of $\mathbb{P}^1$, unramified outside V, are in bijective correspondence with subspaces of $\mathcal{V}$. Let $\mathcal{W} \subset \mathcal{V}$ be a subspace with basis $\mathbf{v}_1, \ldots, \mathbf{v}_r$. We write

$$C_{\mathcal{W}} = C_{\mathbf{v}_1} \times_{\mathbb{P}^1} \cdots \times_{\mathbb{P}^1} C_{\mathbf{v}_r}.$$

Lemma 5.5. *Let $\overline{K}$ be an algebraically closed field of characteristic 0. Let $C/\mathbb{P}^1$ be a double cover over $\overline{K}$ and let D/C be an unramified elementary abelian 2-cover over $\overline{K}$. Then $D/\mathbb{P}^1$ is an elementary abelian 2-cover.*

Proof. By Lemma 5.3 it is sufficient to show the lemma for double covers D/C. We have that $\overline{K}(D) \simeq \overline{K}(C)(\sqrt{f})$ for some function $f \in \overline{K}(C)$. Since D is unramified over C, we have that f has an even order everywhere. Equivalently, $(f) = 2N$ for some $N \in \mathrm{Div}^0(C)$, so $[N] \in \mathrm{Pic}(C)[2]$.

For any $g \in \overline{K}(C)$ we have $\overline{K}(D) \simeq \overline{K}(C)(\sqrt{g^2 f})$ and $(fg^2) = 2(N + (g))$. Note that C is a hyperelliptic curve and that the 2-torsion of $\mathrm{Pic}^0(C)$ can be represented by linear combinations of the branch points of the double cover. Therefore, we can assume that N is supported entirely on branch points. It follows that for $\sigma \in \mathrm{Aut}(C)/\mathbb{P}^1$ we have that $({}^{\sigma}f) = (f)$, but then f is a lift of a function on $\mathbb{P}^1$, so it follows that $\overline{K}(D)$ is the composite of two quadratic extensions of $\mathbb{P}^1$. □

Lemma 5.6. *Let $\overline{K}$ be an algebraically closed field of characteristic 0 and let V be a 0-dimensional locus of $\mathbb{P}^1$ over $\overline{K}$. Choose a coordinate x on $\mathbb{P}^1$. Let $\{t_1, \ldots, t_n\}$*

be the part of V away from ∞. Then:

- *There is a maximal elementary abelian 2-cover C_V of $\mathbb{P}^1$, unramified outside V.*
- *We have* $\deg(C_V/\mathbb{P}^1) = 2^{\deg(V)-1}$.

Let $y_i^2 = x - t_i$ for $i = 1, \dots, n$.

- *If $\infty \in V$, then*
$$\overline{K}(C_V) = \overline{K}(x)(y_1, \dots, y_n).$$
- *If $\infty \notin V$, then*
$$\overline{K}(C_V) = \overline{K}(x)(\{y_i y_j : i, j \in \{1, \dots, n\}\}).$$

Proof. By Lemma 5.3, if we can find a cover that has all degree 2 covers, unramified outside V as subcovers, then this curve covers any fibre product of such curves and thus any elementary abelian 2-cover unramified outside V.

First, assume that $\infty \in V$. Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ be a basis of $\mathcal{V}$ and define
$$C_V = C_{\mathbf{v}_1} \times_{\mathbb{P}^1} \cdots \times_{\mathbb{P}^1} C_{\mathbf{v}_n}.$$
Then, as remarked above, C_V covers all elementary 2-covers, unramified outside ∞ and V. By choosing the standard basis, we see that
$$\overline{K}(C_V) = \overline{K}(x)(y_1, \dots, y_n) = \overline{K}(x)(\sqrt{x - t_1}, \dots, \sqrt{x - t_n}).$$
The latter expression clearly exhibits $\overline{K}(C_V)$ as a field of degree $2^n = 2^{\deg(V)-1}$.

If $\infty \notin V$, then $\overline{K}(C_V)$ is the subfield of $\overline{K}(C_{\{\infty\}\cup V})$ of functions that are unramified at ∞. This subfield is generated by $\{y_i y_j : i, j \in \{1, \dots, n\}\}$. We have that $\overline{K}(C_{\{\infty\}\cup V})$ is of relative degree 2 over $\overline{K}(C_V)$, so we have $\deg(C_V/\mathbb{P}^1) = 2^{\deg(V)-1}$. This proves the lemma. □

We now investigate which arithmetic structures can be supported by C_V. Suppose that V is a 0-dimensional locus of $\mathbb{P}^1$ defined over a number field K. We classify the $\mathrm{Gal}(K)$-module structures supported by $\overline{K}(C_V)$ such that $\overline{K}(x) \subset \overline{K}(C_V)$ with its usual Galois action is a sub-Galois-module. Choose a coordinate on $\mathbb{P}^1$ over K. Let $\{t_1, \dots, t_n\} \subset \mathbb{P}^1(\overline{K})$ be the part of V away from ∞. Define $F(x) = (x - t_1) \cdots (x - t_n) \in K[x]$.

First, we assume that $\infty \in V$. Note that the Galois-action on the functions y_i given by $y_i^2 = (x - t_i)$ is already largely determined, since
$$\left(\frac{{}^\sigma y_i}{y_{\sigma(i)}}\right)^2 = \frac{{}^\sigma(x - t_i)}{x - t_{\sigma(i)}} = 1.$$
Therefore, we already have that ${}^\sigma y_i = \pm y_{\sigma(i)}$. Without loss of generality, we will fix the choice of sign such that ${}^\sigma y_i = y_{\sigma(i)}$.

In view of the arithmetic considerations that we are to consider shortly, we study a slightly more general set of models of C_V, by considering $\delta_i y_i^2 = (x - t_i)$. Using this, we obtain the following representations of $\overline{K}(C_V)$:
$$I_\delta = (\delta_i y_i^2 - (x - t_i) : i = 1, \dots, n); \quad \overline{K}(C_V) = \overline{K}(x)[y_1, \dots, y_n]/I_\delta,$$
where
$$\delta = (\delta_1, \dots, \delta_n) \in \overline{K}^* \times \cdots \times \overline{K}^*.$$
The latter is a Galois-module under
$${}^\sigma(\delta_{\sigma(1)}, \dots, \delta_{\sigma(n)}) = ({}^\sigma(\delta_1), \dots, {}^\sigma(\delta_n)).$$

Given the action of $\mathrm{Gal}(\overline{K}/K)$ we have prescribed on $\overline{K}[y_1,\dots,y_n]$, the ideal I_δ is Galois-invariant precisely if ${}^\sigma\delta_i = \delta_{\sigma(i)}$, i.e., if δ is Galois-invariant.

Lemma 5.7 ([14, p. 450])**.** *Let K be a number field. Let $F(x) \in K[x]$ be a square-free monic polynomial. Let $\overline{K}$ be the algebraic closure of K and let $t_1,\dots,t_n \in \overline{K}$ be the roots of F in $\overline{K}$. For $\sigma \in \mathrm{Gal}(K)$, write ${}^\sigma t_i = t_{\sigma(i)}$. Let*

$$\overline{A}^* = \underbrace{\overline{K}^* \times \cdots \times \overline{K}^*}_{n}$$

be the Galois-module with

$${}^\sigma(\delta_{\sigma(1)},\dots,\delta_{\sigma(n)}) = ({}^\sigma(\delta_1),\dots,{}^\sigma(\delta_n)).$$

Let $A = K[x]/F(x)$. We have

$$H^0(K,\overline{A}^*) = A^*.$$

Proof. Let $F(x) = F_1(x)\cdots F_r(x)$ be the factorisation of F into monic irreducible polynomials over K and let $K_j = K[x]/F_j(x)$. Then $A = K_1 \oplus \cdots \oplus K_r$ and each of the $K(t_i)$ is isomorphic to some K_j. Suppose we have $\delta \in H^0(K,\overline{A}^*)$ and $\sigma \in \mathrm{Gal}(K)$ with $\sigma(i) = i$. Then ${}^\sigma\delta_i = \delta_i$. It follows that $\delta_i \in K(t_i)$. On the other hand, if $\sigma(i) = j$, then $\delta_j = {}^\sigma\delta_i \in {}^\sigma K(t_i)$. Therefore, the value of δ_j is completely determined by δ_i. This establishes the isomorphism. □

We are now in a position to describe the possible Galois-descents of $C_V/\mathbb{P}^1$ relative to $\overline{K}/K$. It is straightforward to see that if $\infty \in V$, then any model over $C_V/\mathbb{P}^1$ over K is isomorphic over K to a model of the form $K(x)[y_1,\dots,y_n]/I_\delta$. This allows us to give a partial description of $H^1(K,\mathrm{Aut}(C_V/\mathbb{P}^1))$ in Lemmas 5.8 and 5.9.

In the special situation where V is the ramification locus of a hyperelliptic curve C, i.e., $\#V$ is even, then because of the maximality of C_V, we have that over $\overline{K}$, the curve C_V covers C as well. In Section 6, we will see that if $C(K)$ is non-empty, then C_V can be descended to a pullback along the multiplication-by-2 map of an embedding of C in its Jacobian. As such, $H^1(K,\mathrm{Aut}(C_V/C)) = H^1(K,\mathrm{Jac}(C)[2])$ maps to $H^1(K,\mathrm{Aut}(C_V/\mathbb{P}^1))$ by composition of covers. In the case that $\infty \in V$, this map is an injection and the image has been identified in [13, Theorem 1.1].

Lemma 5.8. *Let K be a number field. Let V be a 0-dimensional locus of $\mathbb{P}^1$ over K with $\infty \in V$. Then the maximal elementary abelian 2-cover C_V of $\mathbb{P}^1$ unramified outside V can be defined over K. Choose a coordinate x on $\mathbb{P}^1$ over K. Let $\{t_1,\dots,t_n\} \subset \mathbb{P}^1(\overline{K})$ be the finite part of V. Define $F(x) = (x-t_1)\cdots(x-t_n)$ and $A = K[x]/F(x)$. We have*

$$H^1(K,\mathrm{Aut}(C_V/\mathbb{P}^1)) \simeq A^*/A^{*2}.$$

Let S be a finite set of primes containing the primes above $2,\infty$ and the primes of bad reduction of V. Then $H^1(K,C_V;S) \simeq A(S,2)$.

Proof. In the discussion above we have established that any Galois-module isomorphic to $\overline{K}(C_V)$ as a field is isomorphic to $\overline{K}(x)[y_1,\dots,y_n]/I_\delta$, where $\delta \in A^* \subset \overline{K}^* \times \cdots \times \overline{K}^*$ according to Lemma 5.7. Over $\overline{K}(x)$, the fields $\overline{K}(x)[y_1,\dots,y_n]/I_\delta$ and $\overline{K}(x)[y_1,\dots,y_n]/I_{\delta'}$ are isomorphic by $y_i \mapsto \sqrt{\delta_i'/\delta_i}\,y_i$. Consequently, the two curves are isomorphic over K exactly when $\delta/\delta' \in A^{*2}$. This also shows that a twist δ becomes trivial over an extension L of K exactly if $\delta \in (A\otimes L)^{*2}$. The twists of

C_V unramified outside S are exactly the twists that become trivial over a base field extension unramified outside S. This implies that $H^1(K, C_V; S) \simeq A(S, 2)$. □

It remains to describe $H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))$ if $\infty \notin V$. If there is a rational degree 1 point in V, then we can simply move it to ∞ and apply Lemma 5.8. Joe Wetherell pointed out to us that a similar argument should hold if there is an odd degree point in V. Since we are mainly interested in constructing covering collections, we are primarily interested in those twists of C_V that have a rational point. Although we fail in describing $H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))$ completely in the general case, we can at least identify a subgroup that contains twists with rational points.

Again, in the special case where V is the ramification locus of a hyperelliptic curve C with a rational point, we find $H^1(K, \mathrm{Jac}_C[2]) \to H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))$. In fact from the exact sequence of Galois modules

$$0 \to \mathrm{Aut}(C_V/C) \to \mathrm{Aut}(C_V/\mathbb{P}^1) \to \mathrm{Aut}(C/\mathbb{P}^1) \to 0$$

we obtain by cohomology

$$\mathrm{Aut}_K(C_V/\mathbb{P}^1) \to \mathrm{Aut}_K(C/\mathbb{P}^1) \to H^1(K, \mathrm{Aut}(C_V/C)) \to H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1)).$$

Therefore, $H^1(K, \mathrm{Jac}_C[2]) \hookrightarrow H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))$ precisely if there is a K-rational automorphism of $C_V/\mathbb{P}^1$ that induces the hyperelliptic involution on C. This is exactly the case if V contains an odd degree point over K. See [12, Theorem 11.3] for a more general description of the kernel of $H^1(K, \mathrm{Pic}^0(C/K)) \to A^*/K^*A^{*2}$.

Lemma 5.9. *Let K be a number field. Let V be a 0-dimensional locus of $\mathbb{P}^1$. Then the maximal elementary abelian 2-cover C_V of $\mathbb{P}^1$ unramified outside V can be defined over K. Choose x on $\mathbb{P}^1$ such that $\infty \notin V$. Let $F(x)$ be the monic polynomial that vanishes exactly at V and define $A = K[x]/F(x)$. We have*

$$H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1)) \supset A^*/K^*A^{*2}.$$

Furthermore, if $P_0 \in \delta * C_V(K)$, then $\delta \in A^*/K^*A^{*2}$. Let S contain the primes above $2, \infty$ and the primes of bad reduction of $V \cup \{\infty\}$. The map

$$A(S, 2) \to H^1(K, C_V; S) \cap A^*/K^*A^{*2}$$

is surjective.

Proof. Let $W = V \cup \{\infty\}$. By Lemma 5.8, we have that C_W is defined over K. By definition, C_V is a subcover over $\overline{K}$. $\mathrm{Aut}(C_W/C_V) \simeq \mathbb{F}_2$ is a normal subgroup of $\mathrm{Aut}(C_W/\mathbb{P}^1)$. The involution $\tau \in \mathrm{Aut}(C_W/C_V)$ is the only involution that has exactly the points above ∞ as fixed points. Consequently, τ is defined over K and so is $\langle\tau\rangle\backslash C_W \simeq C_V$. We have the exact sequences

$$0 \to \mathrm{Aut}(C_W/C_V) \to \mathrm{Aut}(C_W/\mathbb{P}^1) \to \mathrm{Aut}(C_V/\mathbb{P}^1) \to 0$$

and

$$H^1(K, \mathrm{Aut}(C_W/C_V)) \to H^1(K, \mathrm{Aut}(C_W/\mathbb{P}^1)) \to H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1)).$$

Since C_W has degree 2 over C_V we have that $H^1(K, \mathrm{Aut}(C_W/C_V)) = K^*/K^{*2}$. Combined with Lemma 5.8, we see that A^*/K^*A^{*2} is a part of $H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))$.

It remains to prove that all twists of $C_V/\mathbb{P}^1$ with a rational point P_0 are in the trivial class of $H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))/(A^*/K^*A^{*2})$.

Note that for points $P_1, P_2 \in C_V(\overline{K})$ mapping to the same $x \in \mathbb{P}^1(K)$, the cocycles $\sigma \mapsto {}^\sigma P_1$ and $\sigma \mapsto {}^\sigma P_2$ differ by a coboundary because $C_V/\mathbb{P}^1$ is abelian Galois. Therefore, if we have two twists of $C_V/\mathbb{P}^1$ having a rational point above a

fixed x, then these twists are isomorphic over K. This establishes that for any twist $\delta_0 * C_V$ with a K-rational point P_0, we only have to show that there exists some twist $\delta * C_V$ with $\delta \in A^*/K^*A^{*2}$ and a rational point above $x(P_0)$. To this end, we take the twist of C_W that has a rational point above $x(P_0)$. The corresponding twist $\delta * C_V$ of C_V has a rational point above $x(P_0)$ too. But then this curve must be isomorphic to $\delta_0 * C_V$. Since this twist is induced by a twist of C_W, we naturally have $\delta \in A^*/K^*A^{*2}$.

Finally, it is straightforward to check that $A(S,2) \to A^*/K^*A^{*2}$ surjects onto the the elements that become trivial upon base field extension unramified outside S. □

Lemma 5.10. *Let V be a 0-dimensional locus of $\mathbb{P}^1$ of degree at least 2 defined over a number field K. Let x be a coordinate on $\mathbb{P}^1$ over K such that $\infty \notin V$. The functions $y_1, \dots, y_n$ give rise to a smooth projective model of $\delta * C_V$ defined by*

$$J_\delta = ((t_l - t_k)(\delta_i y_i^2 - \delta_j y_j^2) - (t_j - t_i)(\delta_k y_k^2 - \delta_l y_l^2) : i,j,k,l \in \{1,\dots,n\}),$$

where for any distinct $i, j \in \{1, \dots, n\}$ we have

$$x = \frac{t_j \delta_i y_i^2 - t_i \delta_j y_j^2}{\delta_i y_i^2 - \delta_j y_j^2}.$$

The group $\mathrm{Aut}(C_V/\mathbb{P}^1)$ is generated by the involutions $\tau_i : y_i \mapsto -y_i$, subject to the relation $\tau_1 \circ \cdots \circ \tau_n = \mathrm{id}$.

Proof. Let $W = V \cup \{\infty\}$. The map $C_W \to \mathbb{P}^{n-1}$ given by $(x, y_1, \dots, y_n) \mapsto (y_1 : \cdots : y_n)$ maps $\delta * C_W$ onto the locus of J_δ, denoted by C'. This shows that J_δ indeed defines a curve covered by C_W. It is a simple verification that $C' \subset \mathbb{P}^{n-1}$ is indeed smooth.

Since C' is a subcover of $\delta * C_W/\mathbb{P}^1$, we have that $C' = G\backslash \delta * C_W$ for some subgroup $G \subset \mathrm{Aut}(\delta * C_W/\mathbb{P}^1)$. The involutions $\tau_i : y_i \to -y_i$ generate $\mathrm{Aut}(C_W/\mathbb{P}^1)$ and it follows that $C' = \langle \tau_1 \circ \cdots \circ \tau_n \rangle \backslash C_W$. Therefore, $\tau_1, \dots, \tau_n$ induce non-trivial automorphisms of $C'/\mathbb{P}^1$. Since τ_i has fixed points above $x = t_i$, we see that C' is ramified above V and thus is covered by $\delta' * C_V$. On the other hand, $\delta * C_W$ is a double cover of both $\delta * C_V$ and C'. It follows that $C' = \delta' * C_V = \delta * C_V$. □

Note that both the subgroups of $\mathrm{Aut}(C_V/\mathbb{P}^1)$ and the subspaces of $\mathcal{V}$ as in Definition 5.4 classify the subcovers of C_V. Both are $\mathbb{F}_2$-vector spaces. As we have seen, an element $\mathbf{v}$ of $\mathcal{V}$ corresponds to a function $y_{\mathbf{v}}$ on C_V.

In terms of these spaces, we can give a completely explicit description of the Kummer pairing on $\mathcal{V} \times \mathrm{Aut}(C_V/\mathbb{P}^1)$. We take $(\mathbf{v}, \tau) = 1$ if $y_{\mathbf{v}} \circ \tau = -y_{\mathbf{v}}$ and $(\mathbf{v}, \tau) = 0$ if $y_{\mathbf{v}} \circ \tau = y_{\mathbf{v}}$. It is easy to check that this is a non-degenerate bilinear pairing and thus that $\mathcal{V}$ can be identified with the dual space of $\mathrm{Aut}(C_V/\mathbb{P}^1)$. Let $\mathcal{W} = \langle \mathbf{v}_1, \dots, \mathbf{v}_r \rangle \subset \mathcal{V}$ be a subspace of dimension r. Write

$$\mathcal{W}^\perp = \{\tau \in \mathrm{Aut}(C_V/\mathbb{P}^1) : (\mathcal{W}, \tau) = 0\}.$$

Then $C_{\mathcal{W}} = \mathcal{W}^\perp \backslash C_V$, where $C_{\mathcal{W}}$ is as defined above.

Note that $\mathcal{V}$ is a $\mathrm{Gal}(K)$-module, both as the dual space of the $\mathrm{Gal}(K)$-module $\mathrm{Aut}(\delta * C_V/\mathbb{P}^1)$ and as a vector space over the $\mathrm{Gal}(K)$-set $V(\overline{K})$. It is easy to see that these structures are compatible. Consequently, $\mathcal{W} \subset \mathcal{V}$ is $\mathrm{Gal}(K)$-stable if and only if $\mathcal{W}^\perp$ is. If this is the case, then $C_{\mathcal{W}}$ can be defined over K as well. We write $\delta * C_{\mathcal{W}}$ for the corresponding quotient of $\delta * C_V$ over K.

6. Hyperelliptic subcovers

Note that, since $\mathrm{Aut}(C_V/\mathbb{P}^1)$ has exponent 2, we have that C_V is an unramified cover of any subcover that is ramified above all of V. In particular, if V is the ramification locus of a hyperelliptic curve, then we have an alternative geometric description of C_V.

Let C be a hyperelliptic curve of genus g over a number field K with a point $P_0 \in C(K)$. Write $\hat{\cdot} : P \mapsto \hat{P}$ for the hyperelliptic involution. We fix C as a double cover of $\mathbb{P}^1 = \langle\hat{\cdot}\rangle\backslash C$. Via the Abel-Jacobi map $\iota_{P_0} : C \to \mathrm{Jac}(C)$ defined by $P \mapsto [P - P_0]$, we can view C as a subvariety of $\mathrm{Jac}(C)$. The involution $D \mapsto [\hat{P}_0 - P_0] - D$ on $\mathrm{Jac}(C)$ restricts to $\hat{\cdot}$ on $C \subset \mathrm{Jac}(C)$.

The multiplication-by-two map $[2] : \mathrm{Jac}(C) \to \mathrm{Jac}(C)$ is unramified and of degree 2^{2g}. Let $[2]^{-1}(\iota_{P_0}(C))$ be the pullback of $\iota_{P_0}(C)$ along $[2]$. Since it is an unramified cover of the smooth variety $\iota_{P_0}(C) \simeq C$, it is smooth itself. By [11, Proposition 9.1] it is connected.

We have $\mathrm{Aut}([2]^{-1}(\iota_{P_0}C)/C) = \mathrm{Jac}(C)[2]$, so $[2]^{-1}(\iota_{P_0}C)/C$ is an unramified elementary abelian 2-cover. By Lemma 5.5 we have that $[2]^{-1}(\iota_{P_0}C)/\mathbb{P}^1$ is an elementary abelian 2-cover of degree 2^{2g+1}, unramified outside the ramification-locus V of $C/\mathbb{P}^1$.

Lemma 6.1. *Let $C/\mathbb{P}^1$ be a hyperelliptic curve over a number field K. Let $V \subset \mathbb{P}^1$ be the ramification locus of $C/\mathbb{P}^1$. If $P_0 \in C(K)$, then there is a $\delta_{P_0} \in H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))$ such that $\delta_{P_0} * C_V \simeq [2]^{-1}\iota_{P_0}C$.*

In accordance with the notation introduced in Lemmas 5.8 and 5.9, we can assume $\delta_{P_0} \in A^*/A^{*2}$ if $\infty \in V$ and $\delta_{P_0} \in A^*/A^{*2}K^*$ otherwise.

Proof. Since $[2]^{-1}(\iota_{P_0}(C))$ is geometrically connected and, via $[2]^{-1}(\iota_{P_0}(C)) \to C \to \mathbb{P}^1$, is an elementary abelian 2-cover of $\mathbb{P}^1$ of degree 2^{2g+1} and unramified outside V, we have that $[2]^{-1}(\iota_{P_0}(C))$ is isomorphic to C_V over $\overline{K}$. Since both curves are defined over K, they are twists. This implies the existence of δ_{P_0}. Note that $[2]^{-1}(\iota_{P_0}(C))$ passes through $0 \in \mathrm{Jac}(C)$ and thus has a rational point. From Lemmas 5.8 and 5.9 it follows that δ_{P_0} can be taken as stated. □

The curve C_V gives rise to a covering collection of a hyperelliptic curve that is particularly rich in subcovers. Let C be a hyperelliptic curve over a number field K defined by

$$C : y^2 = F(x)$$

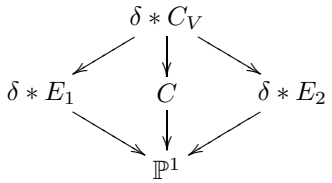
with F a square-free polynomial with integral coefficients and of degree at least 5. Let V be the ramification locus of the double cover $C/\mathbb{P}^1$.

Let S contain all primes where $2\mathrm{Disc}(F)$ is not a unit. According to Lemma 5.6, there is a twist of C_V that covers C. By Theorem 4.1, the twists of C_V unramified outside S contain a covering collection of C_V. Since we only need to include curves with rational points, Lemmas 5.8 and 5.9 show that we only need to consider the twists represented by the finite set $A(S, 2)$, where $A = K[x]/F(x)$. Note that the set of twists to be considered can be reduced even further by observing that we only need to consider twists that induce the trivial twist of C.

We recall that if C' is a subcover of C_V over $\overline{K}$, we write $\delta * C'$ for the corresponding twist of C' that is a subcover of $\delta * C$, considered over the field of definition of C'.

A first set of hyperelliptic subcovers can be obtained by splitting V into two disjoint loci of even degree. One may need a field extension for this. We obtain $F(x) = R_1(x)R_2(x)$, where $R_1(x)$ is defined over a finite extension L of K. We get the subcovers

$$E_1 : y_1^2 = R_1(x), \quad E_2 : y_2^2 = R_2(x),$$



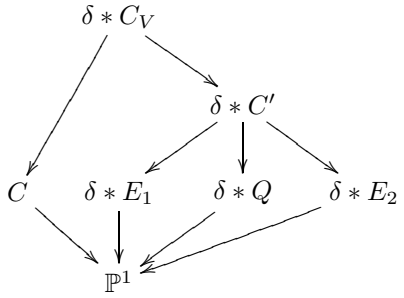
We can now determine the rational points on $\delta * C_V$ if we can find the L-rational points on either $\delta * E_1$ or $\delta * E_2$ that have a K rational image on $\mathbb{P}^1$ as suggested in Section 3.2. See [4] for a description of how one may proceed if the curve E_1 or E_2 under consideration is of genus 1.

A second level of hyperelliptic subcovers can be accessed in the following way. Assume that $F(x)$ factors as $F(x) = Q(x)R(x)R_0(x)$, where $\deg(Q) = 2$ and $\deg(R)$ is odd. If the degree of F is odd, we can also let R represent a locus that contains ∞, so in that situation we can also allow R to be of even degree as a polynomial. Note further that we may need a field extension to realise this factorisation. However, this construction is also useful if it exists over K, so for simplicity, we restrict to that case here.

Let $Q(x) = (x - q_1)(x - q_2)$. Here, either $q_1, q_2 \in K$ or q_1, q_2 are quadratic over K and conjugate. We consider

$$\begin{array}{rcl} Q & : & y_0^2 = Q(x), \\ E_1 & : & y_1^2 = (x - q_1)R(x), \\ E_2 & : & y_2^2 = (x - q_2)R(x). \end{array}$$

Note that from the discussion in Section 5, it follows that the subcover $\delta * C'$ of $\delta * C$, corresponding to $\delta * E_1 \times_{\mathbb{P}^1} \delta * E_2$, is defined over K and covers $\delta * Q$. We have



Note that $\delta * Q$ is a genus 0 curve. Therefore, either $\delta * Q(K)$ is empty, which we can determine by local means according to the Hasse principle, or we can parametrise $\mathbb{P}^1 \xrightarrow{\sim} \delta * Q$ over K and express $\delta * C'$ as a double cover of a $\mathbb{P}^1$. We can then re-apply the construction to get a covering collection of C'.

7. An example

As an application of the techniques described in Section 5 we consider the following problem.

Question 7.1. Is there an $n > 1$ such that the sum of the first n fourth powers is a square?

This question can be answered by determining the integral solutions to

$$z^2 = \sum_{i=1}^{n} i^4 = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n.$$

This has been done by Schäffer [15] using techniques for finding integral points on special genus 1 curves. We will determine all rational points. It turns out there are quite a few rational, non-integral solutions. As a result, we obtain a new, perhaps somewhat more systematic and insightful (although less elementary) proof than in [15].

We work with a slightly modified model by putting $(n, z) = (\frac{x}{1-x}, \frac{y}{30(1-x)^3})$. This gives us the slightly more attractive model

$$C : y^2 = 30x(x-1)(x+1)(x^2-5x+1) = F(x).$$

Lemma 7.2. *The Mordell-Weil rank of* $\mathrm{Jac}(C)$ *over* $\mathbb{Q}$ *is* 3. *We have* $\mathrm{Jac}(C)(\mathbb{Q}) \simeq \mathbb{Z}^3 \oplus (\mathbb{Z}/2\mathbb{Z})^3$.

Proof. A 2-descent as described in [6] and implemented by Michael Stoll ([17]) in MAGMA gives an upper bound of 3 for the rank. The rational points ∞, $(\frac{1}{2}, \frac{15}{4})$, $(\frac{1}{3}, \frac{20}{9})$, $(5, 60)$ generate a free rank-3 subgroup of $\mathrm{Jac}(C)(\mathbb{Q})$. Therefore, the rank is exactly 3. □

So, directly applying Chabauty's method to C as in Section 3.1 will not be successful. We construct a covering collection of C by considering twists of the maximal elementary abelian 2-cover of $\mathbb{P}^1$, unramified outside $F(x)$. We apply the ideas explained in Section 6.

Let $\alpha^2 - 5\alpha + 1 = 0$ and let $L = \mathbb{Q}(\alpha)$. The curve C is a double cover of $\mathbb{P}^1$, ramified above $V = \{\infty, 0, 1, -1, \alpha, 5-\alpha\}$. We consider the coverings $\delta * C_V/\mathbb{P}^1$ defined by

$$\delta * C_V : \begin{cases} \delta_1 y_1^2 &= 30x &=: P_1(x), \\ \delta_2 y_2^2 &= x-1 &=: P_2(x), \\ \delta_3 y_3^2 &= x+1 &=: P_3(x), \\ \delta_4(y_{4,0} + \alpha y_{4,1})^2 &= x-\alpha &=: P_4(x), \\ \delta_5(y_{4,0} + (5-\alpha)y_{4,1})^2 &= x-(5-\alpha) &=: P_5(x), \end{cases}$$

where $\delta_5 = \mathrm{norm}_{L/\mathbb{Q}}(\delta_4)/\delta_4$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts trivially on $y_1, y_2, y_3, y_{4,0}, y_{4,1}$ and

$$\delta = (\delta_1, \delta_2, \delta_3, \delta_4) \in A(S, 2) \subset (\mathbb{Q}^*/\mathbb{Q}^*)^2 \times (\mathbb{Q}^*/\mathbb{Q}^*)^2 \times (\mathbb{Q}^*/\mathbb{Q}^*)^2 \times L^*/(L^*)^2.$$

Note that the identification of δ with elements of $H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1))$ is shifted by 30 with respect to the identification in Lemma 5.8.

The subcovers of $\delta * C_V$ of degree 2 are naturally indexed by the non-zero vectors in $\mathbb{F}_2^5 = \mathcal{V}$, the dual vector space of $\mathrm{Aut}(C_V/\mathbb{P}^1)$ as explained in Section 5. For

TABLE 1. Productive twists of C_V

i	$x(P_i)$	$\delta^{(i)}$
1	∞	$(1, 30, 30, 10\alpha)$
2	0	$(-1, -1, 1, -\alpha)$
3	6	$(5, 5, 7, -1 + 6\alpha)$
4	1/2	$(15, -2, 6, 2 - 4\alpha)$
5	$-1/8$	$(-15, -2, 14, -2 - 16\alpha)$
6	1/3	$(10, -6, 3, 2 - \alpha)$
7	5	$(6, 1, 6, \alpha)$
8	1	$(30, -5, 2, 1 - \alpha)$
9	-1	$(-30, -2, 105, -1 - \alpha)$

$\mathbf{v} \in \mathbb{F}_2^5$ we define

$$\delta * C_{\mathbf{v}} : \left(\prod_{i=1}^{5} \delta_i^{\mathbf{v}_i}\right) y_{\mathbf{v}}^2 = \prod_{i=1}^{5} P_i^{\mathbf{v}_i}.$$

The cover $\delta * C_{\mathbf{v}}/\mathbb{P}^1$ is ramified at infinity precisely if $\mathbf{v}_i = 1$ for an odd number of values for i. If $\mathbf{v}_4 \neq \mathbf{v}_5$, then $C_{\mathbf{v}}$ is only defined over $\mathbb{Q}(\alpha)$ and $\delta * C_{(0,0,0,1,1)+\mathbf{v}}$ is conjugate to $\delta * C_{\mathbf{v}}$.

Finally, due to the identification of δ with elements of $H^1(K, \mathrm{Aut}(C_V/\mathbb{P}^1)$ we chose above, we have, writing $\mathbf{1} = (1, 1, 1, 1, 1)$, that $C_{\mathbf{1}} = C$, so that $1 * C_V$ is an unramified cover of C over K.

Let S contain the primes above $2, 3, 5, 7, \infty$. Since $\mathrm{Disc}(F) = 2^{10}3^{11}5^87^3$, we see that $\{\delta * C_V : \delta \in A^*(S, 2);\ \mathrm{norm}_{A/\mathbb{Q}}(\delta) \in (\mathbb{Q}^*)^2\}$ forms a covering collection for C. Note that $\mathbb{Q}(S, 2) = \langle -1, 2, 3, 5, 7\rangle$ and that $L(S, 2) = \langle -1, \alpha, 2, 3, 3 - \alpha, \alpha - 2, 7\rangle$. It is therefore sufficient to determine the rational points on $\delta * C_V$ for those values of δ.

First we determine which twists of C_V have rational points everywhere locally. This is a straightforward but tedious procedure. Note that $\#A(S, 2) = 2^{4\cdot 5+7}$. Also if one restricts to those twists that restrict to the trivial twist of C, then this is too large a set to simply enumerate. However, if one proves that a subcover has no points locally, then all twists that restrict to that subcover have no points locally either. By combining this information, one can cut down considerably on the amount of work. Additionally, one can use the fact that one only has to consider those twists corresponding to the 2-Selmer group of $\mathrm{Jac}(C)$ over K. This follows from the fact that $\mathrm{Aut}(C_V/C) = \mathrm{Jac}(C)[2]$ in a natural way.

Using either technique, one finds that only the twists with known rational points have points everywhere locally. See Table 1.

Suppose we have a subcover E of $\delta^{(i)} * C_V$ such that E has only a finite number of rational points over its field of definition. If we explicitly know these points, then we can find the rational points on $\delta^{(i)} * C_V$ by lifting these points. Alternatively, since we are really only interested in $C(\mathbb{Q})$, we can map these points down to $\mathbb{P}^1$ and see if they lift to rational points on C. Attractive candidates for E are genus 1 curves. From Lemma 5.2 we can deduce that any genus 1 subcover covers a degree 2 genus 1 subcover. We can therefore restrict our attention to the genus 1 curves

TABLE 2. Indices of genus 1 subcovers of C_V

j	$\mathbf{v}_j$	field of definition
1	$(1,1,1,0,0)$	$\mathbb{Q}$
2	$(1,0,0,1,1)$	$\mathbb{Q}$
3	$(0,1,0,1,1)$	$\mathbb{Q}$
4	$(0,0,1,1,1)$	$\mathbb{Q}$
5	$(1,1,0,1,1)$	$\mathbb{Q}$
6	$(1,0,1,1,1)$	$\mathbb{Q}$
7	$(0,1,1,1,1)$	$\mathbb{Q}$
8	$(0,1,1,1,0)$	$\mathbb{Q}(\alpha)$
9	$(1,0,1,1,0)$	$\mathbb{Q}(\alpha)$
10	$(1,1,0,1,0)$	$\mathbb{Q}(\alpha)$
11	$(1,1,1,1,0)$	$\mathbb{Q}(\alpha)$

TABLE 3. Rank bounds for the Mordell-Weil group of $\delta^{(i)} * E_j$

i	$j=1$	2	3	4	5	6	7	8	9	10	11
1	1	1	1	2	1	1	1	2	2	0	2
2	1	1	1	1	1	1	1	2	1	1	0
3	2	1	2	1	2	2	2	2	2	3	2
4	1	2	1	1	1	2	1	1	1	2	0
5	1	2	2	2	1	2	1	2	2	3	0
6	1	1	1	2	1	1	1	1	1	1	0
7	1	1	1	2	1	2	1	2	1	1	2
8	0	1	0	1	0	1	1	2	1	0	1
9	2	0	1	0	1	2	1	1	1	1	1

$E_j = C_{\mathbf{v}_j}$ where the $\mathbf{v}_j$ run through the weight 3 and 4 vectors of $\mathcal{V} = \mathbb{F}_2^5$ according to Table 2.

Note that each of $\delta^{(i)} * E_j$ has a point over its field of definition, coming from the rational point on $\delta^{(i)} * C_V$ indicated in Table 1. These curves are therefore isomorphic to their Jacobians. Using all 2-isogeny descents available to us, we obtain the rank bounds in Table 3. It is interesting to note that for these curves the 2-isogeny Selmer ranks are remarkably often not sharp, as can be exposed by choosing another 2-isogeny. The bounds in Table 3 are easily proved sharp by a simple search for points.

Inspection of Table 3 shows that $\delta^{(i)} * C_V$ cover an elliptic curve of rank 0 for $i \neq 3, 7$. Each of those curves has only 2-torsion, which is easy to determine. These points only give rise to rational points on C that are already listed.

For $\delta^{(7)} * C_V$ we determine the $\mathbb{Q}(\alpha)$ rational points on $\delta^{(7)} * E_9$ that map to a $\mathbb{Q}$-rational point. Note that $\langle (5,1), (0,0), (1,0) \rangle$ generates a subgroup of odd index in $\delta^{(7)} * E_9(\mathbb{Q}(\alpha))$. A standard computation as explained in [4] shows, using an argument at 37, that $x(\delta^{(7)} * E_9(\mathbb{Q}(\alpha))) = \{\infty, 1, 0, -1, 5\}$. We also see that the rational points of $\delta^{(7)} * C_V$ lead only to already-listed rational points of C.

The only case left is $\delta^{(3)} * C_V$. An inspection of Table 3 shows that no elliptic curve covered by $\delta^{(3)} * C_V$ satisfies the rank criterion for a Chabauty-argument. Since $\mathrm{Jac}(C_V)$ is isogenous to the direct sum of all elliptic curves covered by it, we see that in fact a genuine Chabauty-argument on $\delta^{(3)} * C_V$ would fail.

Consider the genus 2 subcover $D : \delta^{(3)} * E_9 \times_{\mathbb{P}^1}{}^{\sigma}(\delta^{(3)} * E_9)$ of $\delta^{(3)} * C_V$. Note that D is a quotient of $\delta^{(3)} * C_V$ by a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subgroup of $\mathrm{Aut}(\delta^{(3)} * C_V/\mathbb{P}^1)$. Therefore, D is defined over $\mathbb{Q}$. Furthermore, it is a double cover of the genus 0 curve $Q : 7y_0^2 = x^2 - 5x + 1$. We have

$$D : \left\{ \begin{array}{lcccc} E_1 & : & 5(6\alpha-1)y_1^2 & = & 30x(x+1)(x-\alpha), \\ E_2 & : & 5(29-6\alpha)y_2^2 & = & 30x(x+1)(x+\alpha-5), \\ Q & : & 7y_0^2 & = & x^2-5x+1, \\ & & y_0 & = & \frac{7y_1y_2}{6x(x+1)}. \end{array} \right.$$

We parametrise Q by

$$(x, y_0) = (-\frac{u^2-14u+21}{u^2+14u+21}, -\frac{u^2-21}{u^2+14u+21}).$$

We find that

$$(y_1+y_2)^2 = 6x(x+1)(4x-1+2y_0).$$

Let $w = \frac{(u^2+14u+21)^2}{4(u-3)}$. We have

$$D : w^2 = 42u(u^2-14u+21)(u^2+14u+21).$$

Obviously, the representation of D as a double cover of Q is not unique. The automorphism $u \mapsto \frac{21}{u}$ of $Q/\mathbb{P}^1$ changes D/Q. In fact, it sends D to

$$w^2 = 2u(u^2-14u+21)(u^2+14u+21),$$

which shows that the quadratic twist by 21 of D is in fact trivial.

Naturally, the Mordell-Weil rank of $\mathrm{Jac}(D)$ is equal to the Mordell-Weil rank of $\delta^{(3)} * E_9$ over $\mathbb{Q}(\alpha)$. Therefore, a Chabauty argument on D directly will be as unsuccessful as on $\delta^{(3)} * E_9$. However, D itself is a hyperelliptic curve, so we can reapply the covering techniques we have developed to D.

Rather than bore the reader with an indigestible amount of detail, we will quickly record the essential information necessary to reconstruct the computations. A transcript of the computations is available electronically from [5].

Let D' denote the maximal unramified elementary abelian 2-cover of D. We have $B = \mathbb{Q}[u]/(42u(u^2-14u+21)(u^2+14u+21)) = \mathbb{Q} \oplus \mathbb{Q}(\sqrt{7}) \oplus \mathbb{Q}(\sqrt{7})$ and $H^1(\mathbb{Q}, \mathrm{Aut}(D'/Q)) = B^*/(B^*)^2$. The only twists of D' covering D that have local points everywhere have a known rational point. They are

$u(P)$	δ_P
∞	$(1, 24+9\sqrt{7}, 24+9\sqrt{7})$
0	$(1, -7-2\sqrt{7}, 7-2\sqrt{7})$
-7	$(-6, -77-29\sqrt{7}, -21-8\sqrt{7})$
21	$(2, 35+13\sqrt{7}, 7-2\sqrt{7})$

For $u(P) = 0, \infty$, we have that $\delta_P * D'$ covers the curve

$$w^2 = (u^2-14u+21)(u^2+14u+21).$$

It is isomorphic to an elliptic curve of rank 0 with 4 rational points.

For $u(P) = 21$ we have that $\delta_P * D'$ covers

$$F_1 : (24 - 9\sqrt{7})w^2 = (u - 7 - 2\sqrt{7})(u - 7 + 2\sqrt{7})(u + 7 - 2\sqrt{7}).$$

The points $(21-8\sqrt{7}, 70-26\sqrt{7})$, $(7+2\sqrt{7}, 0)$ and $(7-2\sqrt{7}, 0)$ generate a subgroup of odd finite index in the Mordell-Weil group. It is of rank 1, which is smaller than $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}]$. A Chabauty-argument at 19 shows that $u(F_1(\mathbb{Q}(\sqrt{7}))) \cap Q(\mathbb{Q}) = \{\infty, 21\}$.

For $u(P) = -7$ we have that $\delta_P * D'$ covers

$$F_2 : (126 - 48\sqrt{7})w^2 = (u - 7 - 2\sqrt{7})(u - 7 + 2\sqrt{7})(u + 7 - 2\sqrt{7}).$$

The points $(-7, 14 + 6\sqrt{2})$, $(7 + 2\sqrt{7}, 0)$ and $(7 - 2\sqrt{7}, 0)$ generate a subgroup of odd index in the Mordell-Weil group. A Chabauty-argument at 19 and 5 shows that $u(F_2(\mathbb{Q}(\sqrt{7}))) \cap Q(\mathbb{Q}) = \{\infty, -7\}$.

Taken together, we see that $u(D(\mathbb{Q})) = \{0, \infty, -7, 21\}$. These points map to $x(D(\mathbb{Q})) = \{-1, 6, -\frac{2}{9}\}$. The point $x = -\frac{2}{9}$ does not lift to a rational point on C, while the other points lift to rational points already listed. We have proved

Theorem 7.3. *Let*

$$C : y^2 = 30x(x - 1)(x + 1)(x^2 - 5x + 1).$$

We have $x(C(\mathbb{Q})) = \{\infty, 0, 6, \frac{1}{2}, -\frac{1}{8}, \frac{1}{3}, 5, 1, -1\}$.

Note that these values map to $\{-1, 0, -\frac{6}{5}, 1, -\frac{1}{9}, \frac{1}{2}, -\frac{5}{4}, \infty, -\frac{1}{2}\}$ for n in Question 7.1 . Consequently, we find that only the sum of the first 0 or 1 fourth powers is a square.

Acknowledgements

We thank Ed Schaefer for posing the question answered in the example. We especially thank him for not pointing out to us that the problem was already solved. Had we known, this paper would probably not have been written. Furthermore, we thank Joe Wetherell for many inspiring and clarifying discussions. In particular his comments on Lemma 5.9 have been of vital importance. We are also grateful to the Mathematical Sciences Research Institute in Berkeley, California, for its facilities. Part of the research in this paper was done there. Finally, we greatly appreciate the efforts of the developers of the KANT/KASH package for number theory (see [9]). It proved a very reliable platform for the extensive computations for the example.

References

1. B. J. Birch, *Cyclotomic fields and Kummer extensions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 85–93. MR0219507 (36:2588)
2. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)
3. Nils Bruin, *Chabauty methods and covering techniques applied to generalised Fermat equations*, Ph.D. thesis, Universiteit Leiden, 1999.
4. Nils Bruin, *Chabauty methods using elliptic curves*, Tech. Report W99–14, Leiden, 1999.
5. Nils Bruin and Victor Flynn, *Transcript of computations*, available from `ftp://ftp.liv.ac.uk/pub/genus2/bruinflynn/tow2cov` or `http://www.cecm.sfu.ca/~bruin/tow2cov`, 2001.
6. J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, LMS–LNS 230, Cambridge University Press, Cambridge, 1996. MR1406090 (97i:11071)
7. Claude Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. Acad. Sci. Paris **212** (1941), 1022–1024. MR0011005 (6:102e)

8. Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR0808103 (87f:11043)
9. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, available from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash`. MR1484479 (99g:11150)
10. E. V. Flynn, *A flexible method for applying Chabauty's theorem*, Compositio Mathematica **105** (1997), 79–94. MR1436746 (97m:11083)
11. J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, Eds. G. Cornell and J.H. Silverman, pp. 167–212. MR0861976
12. Bjorn Poonen and Edward F. Schaefer, *Explicit descent for jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188. MR1465369 (98k:11087)
13. Edward F. Schaefer, *2-descent on the jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), 219–232. MR1326746 (96c:11066)
14. Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471. MR1612262 (99h:11063)
15. Juan J. Schäffer, *The equation* $1^p + 2^p + 3^p + \cdots + n^p = m^q$, Acta Math. **95** (1956), 155–189. MR0078395 (17:1187a)
16. Joseph H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986. MR0817210 (87g:11070)
17. Michael Stoll, *Implementing 2-descent for jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277. MR1829626 (2002b:11089)
18. Joseph L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, U.C. Berkeley, 1997.

Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, Canada V5A 1S6
E-mail address: `bruin@member.ams.org`

Mathematical Institute, University of Oxford, Oxford OX1 3LB, United Kingdom
E-mail address: `flynn@maths.ox.ac.uk`