N-COVERS OF HYPERELLIPTIC CURVES

N. BRUIN AND E.V. FLYNN

Abstract. For a hyperelliptic curve $\mathcal{C}$ of genus g with a divisor class of order $n = g + 1$, we shall consider an associated covering collection of curves $\mathcal{D}_\delta$, each of genus g^2. We describe, up to isogeny, the Jacobian of each $\mathcal{D}_\delta$ via a map from $\mathcal{D}_\delta$ to $\mathcal{C}$, and two independent maps from $\mathcal{D}_\delta$ to a curve of genus $g(g-1)/2$. For some curves, this allows covering techniques that depend on arithmetic data of number fields of smaller degree than standard 2-coverings; we illustrate this by using 3-coverings to find all $\mathbb{Q}$-rational points on a curve of genus 2 for which 2-covering techniques would be impractical.

1. Description of the Jacobian of the Covering Curves

We shall consider a hyperelliptic curve of genus $g = n - 1 \geq 1$, of the form

$$\mathcal{C} : Y^2 = F(X) = G(X)^2 + kH(X)^n, \quad \text{where } G(X) \text{ is of degree } n = g+1 \text{ and } H(X) \text{ is of degree } 2, \tag{1}$$

and where $G(X), H(X), k$ are defined over the ring of integers $\mathcal{O}$ of a number field K. Here, and elsewhere, we shall adopt the usual convention that $\mathcal{C}$ is used to denote the non-singular curve, even though the equation given in (1) is singular; for the practical purpose of points on $\mathcal{C}$, we can take these to be the affine (X, Y) satisfying (1), together with ∞^+, ∞^-, which will be distinct points on this non-singular curve. We shall assume that $F(X)$ has nonzero discriminant, which implies that resultant$(G(X), H(X))$ is also nonzero. Equation (1) is a classical model of a hyperelliptic curve whose Jacobian J has an element of order n defined over K, namely the divisor class $D = [(X_1, G(X_1)) + (X_2, G(X_2)) - \infty^+ - \infty^-] \in J(K)$, where X_1, X_2 are the roots of $H(X)$. This can be seem immediately from the fact that nD is the divisor of the function $Y - G(X)$. By rewriting (1) as $(Y + G(X))(Y - G(X)) = kH(X)^n$, we see that each factor of the left hand side is 'almost' an nth power, which gives rise to the following covering curves.

Lemma 1. *Let $\mathcal{C}$ be as in (1), with $G(X), H(X), k$ defined over $\mathcal{O}$, the ring of integers of a number field K. Let S be the smallest set of primes of $\mathcal{O}$ for which* resultant$(2G(X), kH(X)) \in \mathcal{O}_\mathfrak{p}^*$ *for all $\mathfrak{p} \notin \mathcal{O}$, and let $K(S, n) = \{\delta \in K^*/(K^*)^n : v_\mathfrak{p}(\delta) \bmod n = 0, \text{ for all } \mathfrak{p} \notin S\}$. If $(X, Y) \in \mathcal{C}(K)$ then there exist $\delta \in K(S, n)$, $U \in K$ such that (X, U) lies on the curve of genus g^2:*

$$\mathcal{D}_\delta : 2\delta U^n G(X) = \delta^2 U^{2n} - kH(X)^n. \tag{2}$$

The map $\phi : (X, U) \mapsto (X, \delta U^n - G(X))$ is from $\mathcal{D}_\delta$ to $\mathcal{C}$, and is an unramified cover of degree n.

Proof The condition on resultant$(2G(X), kH(X))$ gives, for any $(X, Y) \in \mathcal{C}(K)$ and any $\mathfrak{p} \notin \mathcal{O}$:

Date: July 12, 2001.
1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.
Key words and phrases. Coverings of Curves, Descent, Curves of Genus 2, Method of Chabauty.
N. Bruin is supported by grants from the Pacific Institute for the Mathematical Sciences, Simon Fraser University and the University of British Columbia. E.V. Flynn is supported by EPSRC Grant GR/R82975/01.

$$\begin{aligned} X \in \mathcal{O} &\implies \min(v_{\mathfrak{p}}(2G(X)), v_{\mathfrak{p}}(kH(X))) = 0 \implies \min(v_{\mathfrak{p}}(2G(X)), v_{\mathfrak{p}}(kH(X)^n)) = 0 \\ &\implies \min(v_{\mathfrak{p}}((Y+G(X)) - (Y-G(X))), v_{\mathfrak{p}}((Y+G(X))(Y-G(X)))) = 0 \\ &\implies \min(v_{\mathfrak{p}}(Y+G(X)), v_{\mathfrak{p}}(Y-G(X))) = 0. \end{aligned}$$

Since also $v_{\mathfrak{p}}(k) = 0$ and $(Y+G(X))(Y-G(X)) = kH(X)^n$, we must have $v_{\mathfrak{p}}(Y+G(X)), v_{\mathfrak{p}}(Y-G(X)) \in n\mathbb{Z}$. A similar argument applied to $1/X$ shows the same to be true when $X \notin \mathcal{O}$. It follows that there exist $\delta \in K(S,n)$, $U \in K$ for which $Y+G(X) = \delta U^n$, and so $Y-G(X) = kH(X)^n/(\delta U^n)$. Taking the difference of these equations, and then multiplying through by δU^n, gives the equation (2) above for $\mathcal{D}_\delta$. Finally, the curve $\mathcal{D}_\delta$ can be rewritten as: $(\delta U^n - G(X))^2 = G(X)^2 + kH(X)^n$, so that the given map ϕ is from $\mathcal{D}_\delta$ to $\mathcal{C}$ and is clearly unramified and of degree $n = g+1$. We can apply Hurwitz' formula (see [17], Theorem II.5.9): $2(\mathrm{genus}(\mathcal{D}_\delta) - 1) = 2\deg(\phi)(\mathrm{genus}(\mathcal{C}) - 1)$ to conclude that the genus of $\mathcal{D}_\delta$ is g^2. □

The map ϕ above gives that, up to isogeny, the Jacobian of $\mathcal{C}$ occurs as a factor of the Jacobian of D_δ. In [16], this cofactor is studied in an analytic setting. In [15], algebraic tools are developed to describe isogeny factors of more general abelian varieties.

Let us for the moment consider a general hyperelliptic curve $C/\mathbb{P}^1$ over an algebraically closed field $\overline{K}$ with an unramified cyclic degree n cover D/C. Then the cover $D/\mathbb{P}^1$ can be obtained by composing the covers D/C and $C/\mathbb{P}^1$. The hyperelliptic involution of $C/\mathbb{P}^1$ induces involutions $\tau_0, \ldots, \tau_{n-1}$ on $D/\mathbb{P}^1$. Besides these, we have $\langle\zeta\rangle = \mathrm{Aut}(D/C) \subset \mathrm{Aut}(D/\mathbb{P}^1)$. We see that $\mathrm{Aut}(D/\mathbb{P}^1)$ is the dihedral group of order $2n$. We label the τ_i so that $\tau_{i+1} = \zeta \circ \tau_i$, where the indices should be taken modulo n.

We have subcovers $F_i = D/\langle\tau_i\rangle$. Note that $\tau_{i+2} = \zeta \circ \tau_i \circ \zeta^{-1}$, so if n is odd, then all τ_i are conjugate and if n is even, then the τ_i fall in one of two conjugacy classes, depending on the parity of i. The automorphism $D \xrightarrow{\zeta} D$ induces an isomorphism $F_i \to F_{i+2}$. Furthermore, we see that τ_i and τ_{i+1} generate $\mathrm{Aut}(D/\mathbb{P}^1)$, as do ζ and τ_i. From [15, Theorem C], it follows that

$$\mathrm{Jac}(D) \sim_{\overline{K}} \mathrm{Jac}(C) \times \mathrm{Jac}(F_i) \times \mathrm{Jac}(F_{i+1}), \text{ for } i = 0, \ldots, n-2.$$

Returning now to the special case of $\mathcal{C}$ given by (1) and $\mathcal{D}_\delta$ given by (2), with $n = \mathrm{genus}(\mathcal{C}) + 1$, we shall in the next lemma make this decomposition explicit. Furthermore, we shall show that, for n odd, the F_i can be defined and are isomorphic over the base field.

Lemma 2. *Let $\mathcal{D}_\delta$ be as in (2). Define $S_n(s,t) \in \mathbb{Z}[s,t]$ by $u^n + v^n = S_n(u+v, uv)$, let $c_0 \in \overline{K}$ be a fixed nth root of $-k/\delta^2$, let $\zeta \in \overline{K}$ be a fixed primitive nth root of unity, and let $c_i = \zeta^i c_0$, for $i = 0, \ldots, n-1$. Then, for any $0 \le i \le n-1$, the map $\phi_i : (X,U) \mapsto (X,V)$, where $V = U + c_i H(X)/U$, gives $\mathcal{D}_\delta$ as a degree 2 cover of the genus $g(g-1)/2$ curve:*

$$\mathcal{F}_{\delta,c_i} : 2G(X) = \delta S_n(V, c_i H(X)). \tag{3}$$

When n is odd, the map $\phi_i' : (X,U) \mapsto (X,W)$, where $W = -c_i^{(n-1)/2}\delta V$, gives $\mathcal{D}_\delta$ as a degree 2 cover of the genus $g(g-1)/2$ curve defined over K:

$$\mathcal{F} : 2(-k)^{(n-1)/2}G(X) = S_n(-W, -kH(X)). \tag{4}$$

Furthermore, whether n is even or odd, $Jac(\mathcal{D}_\delta)$ is isogenous over $\overline{K}$ to $Jac(\mathcal{C}) \times Jac(\mathcal{F}) \times Jac(\mathcal{F})$.

Proof On dividing through by δU^n, equation (2) can be rewritten as $2G(X) = \delta(U^n + (-k/\delta^2)H(X)^n/U^n)$, and so

$$2G(X) = \delta(U^n + (c_i H(X)/U)^n) = \delta S_n(V, c_i H(X)), \tag{5}$$

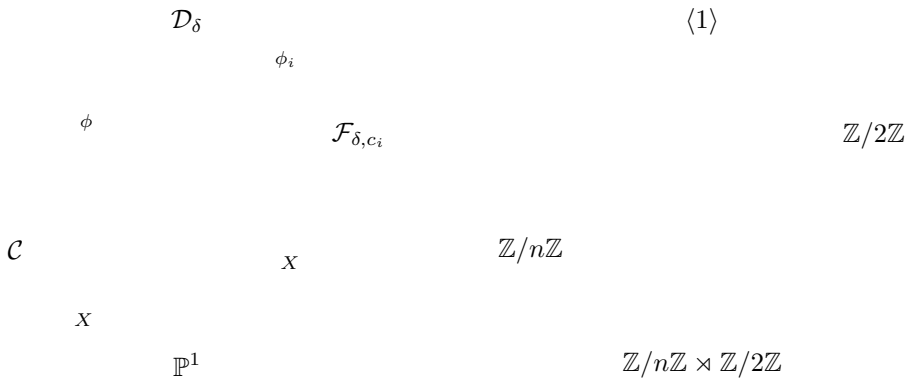
giving (3), since $U + c_i H(X)/U = V$ and $U c_i H(X)/U = c_i H(X)$. For odd n, multiplying both sides by $\delta^{n-1} c_i^{n(n-1)/2} = (-k)^{(n-1)/2}$ gives $2(-k)^{(n-1)/2} G(X) = (c_i^{(n-1)/2}\delta U)^n + (c_i^{(n+1)/2}\delta H(X)/U)^n$, from which (4) follows.

When n is even, the map ϕ_i is ramified at the points $(X_k, \pm U_k)$, for $k = 1, \ldots, n$, where the X_k are the roots of $G(X) - \delta c_i^{n/2} H(X)^{n/2}$, and each $U_k^2 = c_i H(X)$. When n is odd, ϕ_i is ramified at the points (X_k, U_k), for $k = 1, \ldots, 2n$, where the X_k are the roots of $F(X)$ in (1), and each $U_k = G(X_k)/(\delta c_i^{(n-1)/2} H(X)^{(n-1)/2})$. In either case, ϕ_i is ramified at $2n = 2g+2$ points $P_1, \ldots, P_{2g+2}$, and the ramification index $e_{P_k}(\phi_i)$ is 2 at each of these points. Again applying the Hurwitz formula

$$2(\text{genus}(\mathcal{D}_\delta) - 1) = 2\text{deg}(\phi_i)(\text{genus}(\mathcal{F}_{\delta,c_i}) - 1) + \sum_{k=1}^{2g+2} (e_{P_k}(\phi_i) - 1), \tag{6}$$

gives $2(g^2 - 1) = 2 \cdot 2(\text{genus}(\mathcal{F}_{\delta,c_i}) - 1) + 2g + 2$ so that $\mathcal{F}_{\delta,c_i}$, and hence $\mathcal{F}$, has genus $g(g-1)/2$.

We now have the following diagram of maps between curves over $\overline{K}$, together with the corresponding Galois diagram.



Consider the automorphisms $\tau_i : (X, U) \mapsto (X, c_i H(X)/U)$ and $\zeta^i : (X, U) \mapsto (X, \zeta^i U)$, which are both in $\text{Aut}(\mathcal{D}_\delta/\mathbb{P}^1)$. We see from degrees that $\langle \tau_i, \zeta^i \rangle$, which is isomorphic to the Dihedral group $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, is the Galois group of $\mathcal{D}_\delta/\mathbb{P}^1$ and that $\mathcal{D}_\delta/\mathbb{P}^1$ is indeed Galois. Furthermore $\mathcal{C} = \langle \zeta \rangle \backslash \mathcal{D}_\delta$ and $\mathcal{F}_{\delta,i} = \langle \tau_i \rangle \backslash \mathcal{D}_\delta$. For any i, j, let $(\tau_i)_*$ and $(\tau_j)_*$ denote, respectively, the action on $\text{Jac}(\mathcal{D}_\delta)$ given by τ_i and τ_j pointwise on divisors. Map $\text{Jac}(\mathcal{C})$ to $\text{Jac}(\mathcal{D}_\delta)$ by ϕ^*. The image of ϕ^* in $\text{Div}(\mathcal{D}_\delta)$ is spanned by the $\sum_{i=0}^{n-1} \zeta^i(P)$ for P on $\mathcal{D}_\delta$. If a divisor class D is mapped to zero in both $\text{Jac}(\mathcal{F}_{\delta,c_i})$ and $\text{Jac}(\mathcal{F}_{\delta,c_j})$ then we must have that $(\tau_i)_*(D) = -D$ and $(\tau_j)_*(D) = -D$; in other words, $D = (\tau_i)_*(\tau_j)_*(D)$. Furthermore, $(\tau_i)_*(\tau_j)_* = \zeta^{(i-j)}$. Therefore, if $i - j$ generates $\mathbb{Z}/n\mathbb{Z}$ then $D = \zeta(D)$. Since ζ is unramified, all points have an orbit of size n. Therefore, D is a linear combination of divisor classes of the form the $[\sum_i \zeta^i(P)]$. Consequently, D is a pullback from $\text{Jac}(\mathcal{C})$. It is clear that $\text{Jac}(\mathcal{C})$ indeed maps to 0 in $\text{Jac}(\mathcal{F}_{\delta,c_i}) \times \text{Jac}(\mathcal{F}_{\delta,c_j})$ and so the following

sequence

$$\mathrm{Jac}(\mathcal{C}) \xrightarrow{\phi^*} \mathrm{Jac}(\mathcal{D}_\delta) \xrightarrow{(\phi_i)_*\times(\phi_j)_*} \mathrm{Jac}(\mathcal{F}_{\delta,c_i}) \times \mathrm{Jac}(\mathcal{F}_{\delta,c_j}) \longrightarrow 0$$

is exact, and $\mathrm{Jac}(\mathcal{D}_\delta)$ is isogeneous over $\overline{K}$ to $\mathrm{Jac}(\mathcal{C}) \times \mathrm{Jac}(\mathcal{F}_{\delta,c_i}) \times \mathrm{Jac}(\mathcal{F}_{\delta,c_j})$. When n is odd, the map $(X,V) \mapsto (X,W)$ is a birational transformation over $K(c_i)$ from $\mathcal{F}_{\delta,c_i}$ to $\mathcal{F}$, and similarly for n even, it gives a birational transformation over $K(c_i^{1/2})$. In either case, $\mathcal{F}$ and all $\mathcal{F}_{\delta,c_i}$ are birationally equivalent over $\overline{K}$, so that $\mathrm{Jac}(\mathcal{D}_\delta)$ is isogeneous over $\overline{K}$ to $\mathrm{Jac}(\mathcal{C}) \times \mathrm{Jac}(\mathcal{F}) \times \mathrm{Jac}(\mathcal{F})$. □

As an aside, note that, if we let $\phi^* : \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{D}_\delta)$ and $\phi_* : \mathrm{Jac}(\mathcal{D}_\delta) \to \mathrm{Jac}(\mathcal{C})$ be the maps on Jacobians induced by the map $\phi : \mathcal{D}_\delta \to \mathcal{C}$ of Lemma 1, then $\phi_*\phi^*$ is the multiplication by n map on $\mathrm{Jac}(\mathcal{C})$, and $\mathcal{D}_\delta$ is geometrically a pullback of an embedding of $\mathcal{C}$ in $\mathrm{Jac}(\mathcal{C})$ via the restriction of ϕ_* to $\mathrm{im}\phi^*$.

Note that the hyperelliptic involution on $\mathcal{C}$ acts on $\mathrm{Jac}[n]$ and therefore on $H^1(K, \mathrm{Jac}[n])$, part of which classifies the twists D_δ. The induced involution on the the covers $\mathcal{D}_\delta$ is given by $\delta \mapsto k/\delta$. This has a computational benefit that, apart from at most one value of δ invariant under $\delta \mapsto k/\delta$, the number of curves $\mathcal{D}_\delta$ to be considered can be cut in half.

2. Application in Genus 2

In the special case where $n = 3$ and $g = 2$ in (1), the curve $\mathcal{D}_\delta$ of Lemma 2 has genus 4. The following lemma constrains the possible images of the maps ϕ_i' of Lemma 2.

Corollary 1. *Let (X,Y) be a K-rational point on the genus 2 curve $\mathcal{C} : Y^2 = F(X) = G(X)^2 + kH(X)^3$, where $G(X), H(X)$ are cubic and quadratic polynomials in X, respectively, and let $K(S,3)$ be as described in Lemma 1. Then, for some $\delta \in K(S,3)$, there exists $U \in K$ such that (X,U) is a K-rational point on the genus 4 curve $\mathcal{D}_\delta : 2\delta U^3 G(X) = \delta^2 U^6 - kH(X)^3$, and there exists $W \in L = K((k\delta)^{1/3})$ such that (X,W) is an L-rational point on the genus 1 curve $\mathcal{F} : 2kG(X) = W^3 + 3kH(X)W$. Let $\phi_0', \phi_1', \phi_2'$ be as in Lemma 2, and $(X,Y), (X_0,Y_0) \in \mathcal{C}(K)$; then $\sum_{i=0}^2 [\phi_i'(X,Y) - \phi_i'(X_0,Y_0)]$ is the identity element in $Jac(\mathcal{F})(L)$. If $t^3 - k\delta$ is irreducible in $K[t]$ and if $(X,W), (X_0,W_0)$ are the members of $\mathcal{F}(L)$ corresponding to $(X,Y), (X_0,Y_0)$ in $\mathcal{C}(K)$ under any choice of ϕ_i', then $Trace_{L/K}[(X,W) - (X_0,W_0)]$ is the identity element in $Jac(\mathcal{F})(L)$.*

Proof When $n = 3, g = 2$, the curves (1), (2) and (4) become the curves $\mathcal{C}$, $\mathcal{D}_\delta$ and $\mathcal{F}$ above, on noting that $S_n(s,t)$, defined in Lemma 2, becomes $S_3(s,t) = s^3 - 3st$. Finally, note that the three images (X,W) under $\phi_0', \phi_1', \phi_2'$ in Lemma 2 all have the same X-coordinate, since X is K-rational, and so are collinear, as are the three images (X_0,W_0) under $\phi_0', \phi_1', \phi_2'$, giving that $\sum_{i=0}^2 [\phi_i'(X,Y) - \phi_i'(X_0,Y_0)]$ is the identity element in $\mathrm{Jac}(\mathcal{F})(L)$. If $t^3 - k\delta$ is irreducible in $K[t]$, then the $\phi_i'(X,Y)$ are all in the same Galois orbit, as are the $\phi_i'(X_0,Y_0)$); hence $\sum_{i=0}^2 [\phi_i'(X,Y) - \phi_i'(X_0,Y_0)]$ is the same as $\mathrm{Trace}_{L/K}[(X,W) - (X_0,W_0)]$, which again is the identity element in $\mathrm{Jac}(\mathcal{F})(L)$. □

This gives a new approach for trying to find all points on a genus 2 curve in the form of $\mathcal{C}$ above. For each $\delta \in K(S,3)$ one first tries to show by a local argument that no such (X,U) exist on the genus 4 curve $\mathcal{D}_\delta$.

There is a second chance to deal with a given δ by analysing the trace 0 points which, modulo 3-torsion, are contained in $\mathrm{Jac}(\mathcal{F})(L)/\mathrm{Jac}(\mathcal{F})(K)$. If the rank of $\mathrm{Jac}(\mathcal{F})(L)$ is at most 1 greater than the rank of $\mathrm{Jac}(\mathcal{F})(K)$, then there is a chance to bound the number of solutions using local power series in the style of [1],[2],[12], [14], using the arithmetic restriction that $X \in K$. Things become simpler if $\mathcal{F}$ is an elliptic curve over K, since we can then use $\mathcal{F}$ itself, or an easily derived Weierstrass equation $\mathcal{E}$, as a model for $\mathrm{Jac}(\mathcal{F})$; our worked example below will be of this type. As will be apparent in our example, the arguments will differ slightly from those in the literature, since X is an odd degree function on $\mathcal{F}$, whereas the techniques in [1],[2],[12],[14] use the multiplication by 2 map and even degree functions, and since we shall need to describe the trace 0 group for our elliptic curve.

Example 1. *Let* $\mathcal{C} : Y^2 = F(X) = G(X)^2 + kH(X)^3$, *where* $G(X) = X^3 + 2$, $H = X^2 + X + 1$ *and* $k = 1$. *Then* $\mathcal{C}(\mathbb{Q}) = \{(1, \pm 6)\}$.

Proof Using the standard techniques in [6],[11] and (as a check) the MAGMA implementation of [18], we find that the rank of $\mathrm{Jac}(\mathcal{C})(\mathbb{Q})$ is exactly 2, with divisor classes of infinite order given by $[2(1,6) - \infty^+ - \infty^-]$ and $[(-\frac{3}{2} + \frac{\sqrt{5}}{2}, 11 - 4\sqrt{5}) + (-\frac{3}{2} - \frac{\sqrt{5}}{2}, 11 + 4\sqrt{5}) - \infty^+ - \infty^-]$, which are independent in $\mathrm{Jac}(\mathcal{C})(\mathbb{Q})$ modulo torsion. Therefore, we cannot apply directly to $\mathcal{C}$ the Chabauty techniques in [7],[10], which require the rank of $\mathrm{Jac}(\mathcal{C})(\mathbb{Q})$ to be less than the genus of $\mathcal{C}$.

We first compute $\mathrm{resultant}(2G(X), kH(X)) = 36$, and so by Lemma 1 we need only consider $\delta \in \langle 2, 3\rangle$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^3$, that is: $\delta = 1, 2, 3, 4, 6, 9, 12, 18, 36$. For $\delta = 1, 2, 4$, we find that $\mathcal{D}_\delta$ of Corollary 1 has no $\mathbb{Q}_3$-rational points, and for $\delta = 6, 12, 18, 36$, we find that $\mathcal{D}_\delta$ has no $\mathbb{Q}_2$-rational points, leaving only $\delta = 3, 9$ to be considered. For $\delta = 3$, there is the point $(X_0, U_0) = (1, -1) \in \mathcal{D}_3(\mathbb{Q})$, which is a preimage of $(1, -6) \in \mathcal{C}(\mathbb{Q})$ under the map ϕ of Lemma 1. In Lemma 2, we can see that $(1, -1)$ maps to $(X_0, W_0) = (1, \alpha^2 - \alpha) \in \mathcal{F}(L)$, where $L = \mathbb{Q}(\alpha)$ and $\alpha = 3^{1/3}$; in this example, (4) is the genus 1 curve

$$\mathcal{F} : 2(X^3 + 2) = W^3 + 3(X^2 + X + 1)W. \tag{7}$$

Similarly, for $\delta = 9$, there is the point $(1, -1) \in \mathcal{D}_9(\mathbb{Q})$, which is a preimage of $(1, 6) \in \mathcal{C}(\mathbb{Q})$ under the map ϕ of Lemma 1. This maps to the same point on $\mathcal{F}$ as before. Since the hyperelliptic involution on $\mathcal{C}$ swaps $\delta = 3$ and $\delta = k/3 = 9$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^3$, it is sufficient to solve the case $\delta = 3$.

In view of Corollary 1, it is sufficient to show that $(X, W) = (1, \alpha^2 - \alpha)$ is the only member of $\mathcal{F}(L)$ with $\mathrm{Trace}_{L/\mathbb{Q}}[(X, W) - (X_0, W_0)] = 0$ and $X \in \mathbb{Q}$. There is also the $\mathbb{Q}$-rational point $(0, 1)$ on $\mathcal{F}$, and by taking this as a base point (using the technique in [5], p.35) we map $\mathcal{F}$ over $\mathbb{Q}$ to the Weierstrass form

$$\mathcal{E} : y^2 = x^3 + 1485x - 75762. \tag{8}$$

The birational transformation over $\mathbb{Q}$ from $\mathcal{F}$ to $\mathcal{E}$ and its inverse are described by

$$\begin{aligned} x(X, W) &= (39X^2 + 48X + 96 - 12XW + 24W + 24W^2)/X^2, \\ y(X, W) &= (-288X^3 - 720X^2 - 576X - 1152 + 108X^2W + 144XW - 288W - 288W^2)/X^3, \\ X(x, y) &= (4104x + 47304 - 12xy - 468y)/(x^3 + 27x^2 + 675x - 137079), \\ W(x, y) &= (x^3 - 27x^2 - 729x + 134595 + 6xy - 810y)/(x^3 + 27x^2 + 675x - 137079). \end{aligned} \tag{9}$$

Note that we have mapped $(0,1)$ on $\mathcal{F}$ to ∞ on $\mathcal{E}$. It is straightforward to show that both $\mathrm{Jac}(\mathcal{E})(\mathbb{Q})$ and $\mathrm{Jac}(\mathcal{E})(L)$ have trivial torsion, and that $\mathrm{Jac}(\mathcal{E})(\mathbb{Q})$ has rank 2, with generators $[(x,y)-\infty] = [(31,8)-\infty]$ and $[(43,260)-\infty]$. Standard techniques, as in [2],[3],[8], show that the rank of $\mathrm{Jac}(\mathcal{E})(L)$ is bounded above by 3, using the 2-Selmer bound, a computation which requires working in the degree 9 field $L(\beta)$, where β is a root of $x^3+1485x-75762$. There are now several places in the literature describing how to compute 2-Selmer bounds on ranks of elliptic curves over number fields (for example, [2],[3],[8],[9]), and so we do not give the details here; they descibed in the file `covdeg3.g`, available at [4].

The image of our known point $\mathfrak{P}_0 = (X_0, W_0) = (1, \alpha^2-\alpha) \in \mathcal{F}(L)$ maps under the birational transformation (9) to the point $P_0 = (36\alpha^2+60\alpha+39, -324\alpha^2-828\alpha-1008) \in \mathcal{E}(L)$. This gives a third independent member $[P_0-\infty] \in \mathrm{Jac}(\mathcal{E})(L)$ of infinite order, and so the rank of $\mathrm{Jac}(\mathcal{E})(L)$ is 3. It is sufficient to find all $(x,y) \in \mathcal{E}(L)$ such that $[(x,y)-P_0]$ has trace 0 and such that $X(x,y) \in \mathbb{Q}$. Note that $[(x,y)-P_0] = [(x,y)-\infty]-[P_0-\infty]$. From now on, we shall use the standard identification between $\mathrm{Jac}(\mathcal{E})$ and $\mathcal{E}$ by using (x,y) on $\mathcal{E}$ as the standard abbreviation for $[(x,y)-\infty]$ in $\mathrm{Jac}(\mathcal{E})$. So, it is now sufficient to find all $(x,y) \in \mathcal{E}(L)$ such that $(x,y) = P_0 + \mathrm{P}$, where $P \in \mathcal{E}(L)$ has trace 0, and such that $X(x,y) \in \mathbb{Q}$.

A member of $\mathcal{E}(\mathbb{Q})$ can only have trace 0 if it is 3-torsion; since $\mathcal{E}(\mathbb{Q})$ has only trivial torsion, it follows that the trace 0 group of $\mathcal{E}(L)$ is described by $\mathcal{E}(L)/\mathcal{E}(\mathbb{Q})$. We can compute that

$$\mathrm{Trace}_{L/\mathbb{Q}} P_0 = (3823/9, -237232/27) = -(31,8)+(43,260) \notin 3\mathcal{E}(\mathbb{Q}). \tag{10}$$

If $(31,8),(43,260),P_0$ were generators for $\mathcal{E}(L)$, this would show that

$$\begin{aligned} R_1 &= 3P_0 - \mathrm{Trace}_{L/\mathbb{Q}} P_0 \\ &= \left(\tfrac{265305648}{46471489} - \tfrac{902606639}{139414467}\alpha + \tfrac{2769472739}{139414467}\alpha^2, -\tfrac{48831440094572}{950388421539} + \tfrac{8488112833156}{316796140513}\alpha - \tfrac{26044121637556}{316796140513}\alpha^2\right) \end{aligned} \tag{11}$$

is a generator of the trace 0 group, and that any $P \in \mathcal{E}(L)$ of trace 0 satisfies $P = MR_1$ for some $M \in \mathbb{Z}$. This would require a substantial height computation which we have not attempted. Note that $\mathrm{Trace}_{L/\mathbb{Q}}(\langle (31,8),(43,260),R_1\rangle) = \langle 3(31,8), 3(43,260)\rangle$. Any $P \in \mathcal{E}(L)$ satisfies $dP \in \langle (31,8),(43,260),R_1\rangle$ for some $d \in \mathbb{Z}$ and if P is of trace 0 then $dP = mR_1$, for some $m \in \mathbb{Z}$. We cannot have $|m/d|_{17} > 1$ since $16R_1$ is in the kernel of reduction modulo either prime above 17, and the local parameter $s(16R_1) = -x(16R_1)/y(16R_1)$ has valuation 1 at either prime above 17. We can now say that any $P \in \mathcal{E}(L)$ of trace 0 satisfies $P = MR_1$ for some $M \in \mathbb{Z}_{17}$, which is sufficient for our purposes, since our remaining argument is 17-adic.

The following general type of argument has appeared before in the 2-covers literature (see [2],[12],[13],[14]), but we shall nevertheless give some details, to illustrate how to deal with the arithmetic restriction on the function X, which is not even. We first recall the standard local power series associated to an elliptic curve of the form $y^2 = g_3x^3+g_2x^2+g_1x+g_0$. Imitating Chapter IV of [17], we introduce the variables $s = -x/y, w = -1/y$. Then $w = g_3s^3+g_2s^2w+g_1sw^2+g_0w^3$, and recursive substitution gives $w = w(s)$, a power series in the local parameter s, with initial term g_3s^3. If (x_0,y_0) is any point on $\mathcal{E}$, then the x and y

coordinates of $(x_0, y_0) + (x, y)$ are power series in s over $\mathbb{Z}[g_0, g_1, g_2, g_3, x_0, y_0]$.

$$\begin{array}{l} x\text{-coord of } \big((x_0,y_0)+(x,y)\big) = x_0 + 2y_0 s + (3g_3x_0^2 + 2g_2x_0 + g_1)s^2 + O(s^3), \\ y\text{-coord of } \big((x_0,y_0)+(x,y)\big) = y_0 + (3g_3x_0^2 + 2g_2x_0 + g_1)s + 2(3g_3x_0 + g_2)y_0 s^2 + O(s^3) \end{array} \tag{12}$$

If $(s, w(s)), (t, w(t))$ are two points in s-w coordinates then the s-coordinate of the sum can be written as $\mathcal{F}(s,t) \in \mathbb{Z}[g_0, g_1, g_2, g_3][\![s, t]\!]$, the *formal group*. There are then power series

$$\log(t) = t + \frac{1}{3}g_2t^3 + \frac{1}{5}(g_2^2 + 2g_1g_3)t^5 + O(t^7) \in \mathbb{Q}[g_0, g_1, g_2, g_3][\![t]\!], \tag{13}$$

$$\exp(t) = t - \frac{1}{3}g_2t^3 + \frac{1}{15}(2g_2^2 - 6g_1g_3)t^5 + O(t^7) \in \mathbb{Q}[g_0, g_1, g_2, g_3][\![t]\!], \tag{14}$$

satisfying $\log(\mathcal{F}(s,t)) = \log(s)+\log(t)$, $\mathcal{F}(\exp(s), \exp(t)) = \exp(s+t)$. In either power series, the denominator of the coefficient of t^k divides $k!$.

Let γ be the unique member of $\mathbb{Q}_{17}$ such that $\gamma^3 = 3$, and let ω be such that $\omega^2 + \omega + 1 = 0$. Embed $L = \mathbb{Q}(\alpha)$ into $\mathbb{Q}_{17}(\omega)$ via $\alpha \mapsto \gamma\omega$. Then, one finds that $R = 16R_1$ is in the kernel of reduction and so $s(R) = -x(R)/y(R) \equiv 3315 + 2244\omega \pmod{17^3}$ is divisible by 17. Standard arguments (see the file `covdeg3.g` in [4]) show that we can disregard all $M \not\equiv 0 \pmod{16}$; that is, it is sufficient to find all $N \in \mathbb{Z}_{17}$ such that $X(P_0 + NR) \in \mathbb{Q}$. We can compute $s(NR)$, the s-coordinate of NR, using (13),(14), as $\exp(N\log(s(R)))$, which is a power series in N. Substituting this power series for s, and substituting $x(P_0), y(P_0)$ for x_0, y_0 in (12), gives $x(P_0 + NR)$ and $y(P_0 + NR)$ as members of $\mathbb{Z}_{17}[\omega][\![N]\!]$.

$$\begin{array}{rcl} x(P_0+NR) & \equiv & 638 + 561N + 1734N^2 + (662 + 3434N + 867N^2)\omega \pmod{17^3} \\ y(P_0+NR) & \equiv & 3427 + 3281N + 289N^2 + (2583 + 1700N + 2601N^2)\omega \pmod{17^3} \end{array} \tag{15}$$

It is clear, from the standard estimate $|k!|_p \geq p^{-(k-1)/(p-1)}$ for any prime p, that the coefficients of the N^k in the above power series are indeed in $\mathbb{Z}_{17}[\alpha]$, and converge to 0 as $k \to \infty$. Substituting these powers series for x, y into the third equation of (9) gives

$$X(P_0 + NR) = \big(\theta_1(N) + \theta_2(N)\omega\big)/\big(\theta_3(N) + \theta_4(N)\omega\big), \tag{16}$$

where $\theta_i(N) \in \mathbb{Z}_{17}[\![N]\!]$ for each i and

$$\begin{array}{l} \theta_1(N) \equiv 1584 + 1207N + 4046N^2, \quad \theta_2(N) \equiv 599 + 3298N + 2312N^2, \\ \theta_3(N) \equiv 1584 + 3332N + 2601N^2, \quad \theta_4(N) \equiv 599 + 4811N + 867N^2 \pmod{17^3}. \end{array} \tag{17}$$

Any $N \in \mathbb{Z}_{17}$ such that $X(P_0 + NR) \in \mathbb{Q} \subset \mathbb{Q}_{17}$ must then be a root of

$$\theta(N) = \theta_1(N)\theta_4(N) - \theta_2(N)\theta_3(N) \equiv 3553N + 2601N^2 \equiv 11 \cdot 17 \cdot 19N + 3^2 \cdot 17^2N^2 \pmod{17^3}. \tag{18}$$

Since $X(P_0) \in \mathbb{Q}$, we know that $N = 0$ is a root of $\theta(N)$ and so the constant term of $\theta(N)$ is genuinely 0, not merely 0 modulo 17^3. Furthermore, the 17-adic norm of leading coefficient has 17-adic norm strictly greater than all subsequent coefficients, so that $N = 0$ is the only root. Therefore, $N = 0$ is the only $N \in \mathbb{Z}_{17}$ such that $X(P_0 + NR) \in \mathbb{Q}$, as required. □

In principle, we could have tried to apply a standard 2-cover, as in [2],[14]; but then, since $\mathrm{Gal}(G(X)^2 + kH(X)^3) = \mathrm{Sym}(6)$, a number field of degree 45 (a cubic extension of a degree 15 number field) would be required to define the elliptic curves associated to those techniques and to perform a 2-descent on them. The class field information would have been unobtainable, and so standard 2-covers are not viable for examples of the above type, where $F(X)$ has full Galois group. Therefore, the 3-covering technique used above genuinely

provides a line of attack for some curves which would be computationally too difficult for 2-covers. Any curve of genus 2 can be written in the form $\mathcal{C} : Y^2 = F(X) = G(X)^2 + kH(X)^3$ of Corollary 1 over an extension of the ground field for which $\mathrm{Jac}(\mathcal{C})$ contains a point of order 3, so that the 3-covering method applied to the above example is, in principle, applicable to any curve of genus 2. In practice, for each curve, it will depend on the smallest field over which a point of order 2 or 3 is defined as to whether conventional 2-covers as in [2],[14] or the 3-covers presented here will be computationally superior.

We thank Armand Brumer and Jaap Top for drawing our attention to [15] and [16]. We thank Joe Wetherell for many helpful discussions.

References

[1] N. Bruin. The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. *Compositio Math.*, 118:305–321, 1999.
[2] N. Bruin. Chabauty methods using covers on curves of genus 2. http://www.math.leidenuniv.nl/reports/1999-15.shtml
[3] N. Bruin. KASH-based program for performing 2-descent on elliptic curves over number fields. Available from: http://www.math.uu.nl/people/bruin/ell.shar
[4] N. Bruin and E.V. Flynn. Transcripts of Computations for Example 1. Availalable from: `http://www.cecm.sfu.ca/~bruin/covdeg3/` or: `www.maths.ox.ac.uk/~flynn/genus2/bruinflynn/Ncovers/`
[5] J.W.S. Cassels. *Lectures on elliptic curves*. LMS–ST 24. Cambridge University Press, Cambridge, 1991.
[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.
[7] C. Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212:1022–1024, 1941.
[8] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Comput.*, 24(3-4):267–283, 1997. Available from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash`.
[9] Z. Djabri, E.F. Schaefer, and N.P. Smart. Computing the p-Selmer group of an elliptic curve. *Trans. Amer. Math. Soc.*, 352(12):5583–5597, 2000.
[10] E.V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Mathematica*, 105:79–94, 1997.
[11] E.V. Flynn, B. Poonen and E.F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-two curve. *Duke Math. J.*, 90:435–463, 1997.
[12] E.V. Flynn and J.L. Wetherell. Finding Rational Points on Bielliptic Genus 2 Curves. *Manuscripta Math.*, 100:519–533, 1999.
[13] E.V. Flynn. On Q-Derived Polynomials. *Proc. Edinburgh Math. Soc.*, 44:103–110, 2001.
[14] E.V. Flynn and J.L. Wetherell. Covering Collections and a Challenge Problem of Serre. *Acta Arith.*, 98(2):197–205, 2001.
[15] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.
[16] J. Ries. The Prym variety for a cyclic unramified cover of a hyperelliptic Riemann surface. *J. Reine Angew. Math.*, 340:59–69, 1983.
[17] J.H. Silverman. *The Arithmetic of Elliptic Curves*. GTM 106. Springer-Verlag, 1986.
[18] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245-277, 2001.

Department of Mathematics & Statistics, Simon Fraser University, Burnaby, BC, Canada, V5A 1S6
E-mail address: `bruin@cecm.sfu.ca`

Mathematical Institute, University of Oxford, 24–29 St. Giles, Oxford OX1 3LB, England
E-mail address: `flynn@maths.ox.ac.uk`