AN APPLICATION OF "SELMER GROUP CHABAUTY" TO ARITHMETIC DYNAMICS

MICHAEL STOLL

ABSTRACT. We describe how one can use the "Selmer group Chabauty" method developed by the author to show that certain hyperelliptic curves of the form

$$C\colon y^2 = x^{2g+1} + h(x)^2\,,$$

with $h \in \mathbb{Z}[x]$ such that $\deg h \le g$ and $h(0)$ is odd, have only the "obvious" rational points ∞ (the unique point at infinity on the smooth projective model of the curve) and $(0, \pm h(0))$.

Let $c \in \mathbb{Q}$ and write $f_c(x) = x^2 + c$. We denote the iterates of f_c by $f_c^{\circ n}$; i.e., we set $f_c^{\circ 0}(x) = x$ and $f_c^{\circ(n+1)}(x) = f_c(f_c^{\circ n}(x))$. As an application of the method, we prove that if $f_c^{\circ 2}$ is irreducible, then $f_c^{\circ 6}$ is also irreducible. Assuming the Generalized Riemann Hypothesis (GRH), it also follows that $f_c^{\circ 10}$ is irreducible.

1 Introduction

We describe how one can use the "Selmer group Chabauty" method developed by the author in [Sto17] to show that certain hyperelliptic curves of the form

$$C\colon y^2 = x^N + h(x)^2\,, \tag{1.1}$$

where $N = 2g+1$ is odd, $h \in \mathbb{Z}[x]$ with $\deg h \le g$ and $h(0)$ odd, have only the "obvious" rational points ∞ (the unique point at infinity on the smooth projective model of the curve) and $P_0 = (0, h(0))$, $(0, -h(0))$.

We note that curves of the form (1.1) can be characterized by a nice property.

Lemma 1.1. *Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of genus g over a field k with $\operatorname{char}(k) \neq 2$ such that f is monic of odd degree $2g+1$. We use the unique point ∞ at infinity to define an embedding $i\colon C \to J$, where J is the Jacobian variety of C.*

(1) *If $P \in C(k)\setminus\{\infty\}$ is such that $i(P) \in J(k)$ has finite order n, then $n = 2$ or $n \ge 2g+1$.*

(2) *If $P \in C(k)$ is such that $i(P)$ has order $2g+1$ and $x(P) = 0$, then $f = x^{2g+1} + h(x)^2$ with a polynomial $h \in k[x]$ of degree $\le g$ such that $P = (0, h(0))$. Conversely, if f is of this form and $P = (0, h(0))$, then $i(P)$ has order $2g+1$.*

Proof.

(1) The divisor $n\cdot(P-\infty)$ is principal; let ϕ denote a function in $C(k)^\times$ with this divisor. Then $\phi \in L(n\cdot\infty)$. If $n \le 2g$, then this Riemann-Roch space is generated by powers of x. The divisor of a function of x alone is invariant under the hyperelliptic involution. This forces P to be a Weierstrass point on C, but then $i(P)$ has order 2.

Date: November 17, 2026.

2020 *Mathematics Subject Classification.* 14G05, 11G30, 37P15; 11Y50, 14Q05, 11R09.

Key words and phrases. Hyperelliptic curve, rational points, Selmer group Chabauty, quadratic iteration.

(2) Taking ϕ as in (1), we now have $\phi \in L((2g+1)\cdot\infty)$, which has basis $1, x, \dots, x^g, y$. As we have just seen, ϕ cannot be a function of x alone, so (up to scaling), $\phi = y - h(x)$ with $h \in k[x]$ of degree $\leq g$. The fact that $P = (0, h(0))$ is a zero of order $2g+1$ of ϕ implies that x^{2g+1} divides $f(x) - h(x)^2$. Since f is monic of degree $2g+1$ (and $\deg h \leq g$), it follows that $f(x) = x^{2g+1} + h(x)^2$. For the converse, we check that the divisor of $y - h(x)$ is $(2g+1)\cdot(P - \infty)$. Since $P \neq \infty$ and $2g+1$ is odd, the claim then follows from (1). □

As an application of the method, we prove the following result.

Theorem 1.2. *Let $c \in \mathbb{Q}$ and write $f_c(x) = x^2 + c$. We denote the iterates of f_c by $f_c^{\circ n}$; i.e., we set $f_c^{\circ 0}(x) = x$ and $f_c^{\circ(n+1)}(x) = f_c(f_c^{\circ n}(x))$. If $f_c^{\circ 2}$ is irreducible, then $f_c^{\circ 6}$ is also irreducible. Assuming the Generalized Riemann Hypothesis (GRH), it also follows that $f_c^{\circ 10}$ is irreducible.*

This is based on the following observation. Define the polynomial $A_n(c) = f_c^{\circ n}(0)$, for $n \geq 1$; i.e., $A_1(c) = c$ and $A_{n+1}(c) = A_n(c)^2 + c$. The following implication holds when $n \geq 2$ (see [Sto92, Lemma 1.2]).

$$f_c^{\circ(n-1)} \text{ irreducible and } A_n(c) \text{ not a square } \implies f_c^{\circ n} \text{ irreducible}$$

See also [Jon13] for a survey on related questions. By results in [DHJ+20], we know that $A_3(c)$ and $A_4(c)$ are never squares unless $c = 0$, or $c = -1$ in the case of A_4, but then $f_c = x^2$ or $x^2 - 1$ is already reducible. So the theorem follows if we can show that both $A_5(c)$ and $A_6(c)$ (and $A_7(c)$, $A_8(c)$, $A_9(c)$, $A_{10}(c)$, where we will need to assume GRH for A_7) can never be a square for $c \neq 0, -1$. We note that $\deg A_n = 2^{n-1}$ and that $A_n(0) = 0$. The curve $y^2 = A_n(x)$, whose rational points are of interest to us, is isomorphic to the curve $y^2 = a_n(x)$, where

$$a_n(x) = x^{2^{n-1}} A_n(x^{-1}),$$

so

$$a_1(x) = 1 \qquad \text{and} \qquad a_{n+1}(x) = x^{2^n - 1} + a_n(x)^2.$$

This shows that the curves under consideration have the form studied in this paper. For $n = 5$, we have the explicit equation

$$\begin{aligned} y^2 = a_5(x) = x^{15} + x^{14} + 2x^{13} + 5x^{12} + 14x^{11} + 26x^{10} + 44x^9 + 69x^8 \\ + 94x^7 + 114x^6 + 116x^5 + 94x^4 + 60x^3 + 28x^2 + 8x + 1. \end{aligned}$$

Our method shows that this curve has only the three obvious rational points ∞, $(0, 1)$ and $(0, -1)$, which is equivalent to saying that $A_5(c)$ can never be a square for $c \neq 0$.

We also show that $A_6(c)$ is a square only for $c = 0$ and $c = -1$ using by now standard methods for rational points on curves of genus 2.

We show that $A_7(c)$ can only be a square when $c = 0$ by computing the 2-Selmer group of the Jacobian of the curve $y^2 = a_7(x)$; this Selmer group turns out to be trivial. We need to assume GRH to verify that the class group of the number field obtained by adjoining a root of a_7 to $\mathbb{Q}$ is trivial.

We can reduce the question whether $A_n(c)$ can be a square for a given $c \in \mathbb{Q}$ to the analogous question for $A_p(c)$, $\pm A_p(c)$, or $A_4(c)$, where p is an odd prime divisor of n, for n odd, n twice an odd number, and n divisible by 4, respectively. Thus we can deal with A_8 and A_9 by reducing the question to A_4 and A_3, respectively. We show, again using Selmer group Chabauty, that $-A_5(c)$ can be a square only for $c = 0, -1$,

which, together with our result on A_5, also deals with A_{10}. We note that it is only the implication

$$f_c^{\circ 6} \text{ irreducible} \implies f_c^{\circ 7} \text{ irreducible}$$

that depends on GRH, whereas the implication

$$f_c^{\circ 7} \text{ irreducible} \implies f_c^{\circ 10} \text{ irreducible}$$

is unconditional, since it follows from the unconditional results on A_8, A_9, and A_{10}.

We describe the method in detail in Section 2, prove the claims on the various $A_n(c)$ in Section 3, and give some further examples and statistics in Section 4.

2 Selmer group Chabauty for a family of hyperelliptic curves

Fix $g \geq 1$. We consider the hyperelliptic curve

$$C\colon y^2 = f(x) := x^{2g+1} + h(x)^2\,,$$

where $h \in \mathbb{Z}[x]$, and we make the following assumptions (we will make additional assumptions later).

Assumptions 2.1.

(A1) $\deg h \leq g$, so f is monic of degree $2g+1$.

(A2) $h(0)$ is odd.

By considering f and its derivative $f'(x) = (2g+1)x^{2g} + 2h(x)h'(x)$ modulo 2, we see that f is squarefree over $\mathbb{F}_2$, hence f is squarefree and the discriminant of f is odd, and so C is a hyperelliptic curve of genus g. Since $\deg f = 2g+1$ is odd, there is a unique (and hence rational) point at infinity on (the smooth projective model of) C with respect to the given affine equation. We denote this point by ∞. We write J for the Jacobian variety of C; we have the embedding $\imath\colon C \to J$, $P \mapsto [P - \infty]$, defined over $\mathbb{Q}$. We note that C has at least the three obvious rational points ∞ and $(0, \pm h(0))$. We write $P_0 = (0, h(0))$; if $\iota\colon C \to C$, $(x, y) \mapsto (x, -y)$, denotes the hyperelliptic involution on C, then the third point is $\iota(P_0)$.

Lemma 2.2. *C has potentially good reduction at 2. More precisely, let $\pi = 2^{1/(2g+1)}$; then C is isomorphic to*

$$C'\colon \eta^2 + h(\pi^2\xi)\eta = \xi^{2g+1}$$

over $\mathbb{Q}(\pi)$, with reduction mod π given by

$$\tilde{C}\colon \eta^2 + \eta = \xi^{2g+1}\,,$$

which is a hyperelliptic curve of genus g over $\mathbb{F}_2$.

Proof. We set

$$y = 2\eta + h(\pi^2\xi) \qquad \text{and} \qquad x = \pi^2\xi$$

in the equation defining C; some elementary manipulations then give us the equation of C'. Since $h(0)$ is odd by Assumption (A2), we have that $h(\pi^2\xi) \equiv 1 \bmod \pi$, and so we get the indicated reduction $\tilde{C}$ mod π. The affine part of the reduction is smooth, since the partial derivative of the equation with respect to η is constant $= 1$, so $\tilde{C}$ is a curve of genus g. Since the genus does not drop, C' has good reduction at the prime above 2 of $\mathbb{Q}(\pi)$. □

Let $C(\mathbb{Q})_{\mathrm{odd}}$ denote the set of points $P \in C(\mathbb{Q})$ such that $\mathfrak{i}(P)$ has odd finite order; similarly for $C(\mathbb{Q}_2)_{\mathrm{odd}}$.

Lemma 2.3. $C(\mathbb{Q})_{\mathrm{odd}} = C(\mathbb{Q}_2)_{\mathrm{odd}} = \{\infty, P_0, \iota(P_0)\}$.

Proof. By Lemma 2.2, we have the following commutative diagram

$$\begin{array}{ccccccc} C(\mathbb{Q}) & \hookrightarrow & C(\mathbb{Q}_2) & \hookrightarrow & C(\mathbb{Q}_2(\pi)) & \xhookrightarrow{\mathfrak{i}} & J(\mathbb{Q}_2(\pi)) \\ & & & \searrow^{\alpha} & \downarrow & & \downarrow \\ & & & & \tilde{C}(\mathbb{F}_2) & \xhookrightarrow{\mathfrak{i}} & \tilde{J}(\mathbb{F}_2)\ , \end{array}$$

where $\tilde{J}$ denotes the Jacobian of $\tilde{C}$. The right-most vertical map is injective on the torsion points of odd order. This implies that $\alpha\colon C(\mathbb{Q}_2)_{\mathrm{odd}} \to \tilde{C}(\mathbb{F}_2)$ is also injective. Since $\tilde{C}(\mathbb{F}_2) = \{\infty, (0,0), (0,1)\}$ consists of three points, this already shows that $\#C(\mathbb{Q}_2)_{\mathrm{odd}}$ has at most three elements. On the other hand, $\mathfrak{i}(\infty) = 0$ has order 1 and $\mathfrak{i}(P_0)$ and $\mathfrak{i}(\iota(P_0)) = -\mathfrak{i}(P_0)$ have odd order $2g+1$ (see Lemma 1.1). So

$$\{\infty, P_0, \iota(P_0)\} \subset C(\mathbb{Q})_{\mathrm{odd}} \subset C(\mathbb{Q}_2)_{\mathrm{odd}} \qquad \text{and} \qquad \#C(\mathbb{Q}_2)_{\mathrm{odd}} \leq 3\,,$$

which proves the claim. □

We note that $\tilde{J}[2] = 0$ (the hyperelliptic involution on $\tilde{C}$ is given by $\eta \mapsto \eta + 1$; the point at infinity is the only fixed point), so that $J(\mathbb{Q}_2)[2]$ maps into the kernel of reduction in $J(\mathbb{Q}_2(\pi))$.

For later use, we now consider regular differentials on C and their formal integrals over $\mathbb{Q}_2$. We write $v_2\colon \bar{\mathbb{Q}}_2 \to \mathbb{Q} \cup \{\infty\}$ for the 2-adic valuation normalized such that $v_2(2) = 1$.

Lemma 2.4. *We set, for $j = 0, 1, \ldots, g-1$, $\omega_j = x^j\,dx/y \in \Omega^1(C)$. Then the following holds.*

(1) *Let $t = x$ be a uniformizer at P_0 and write $\omega_j = w_j(t)\,dt$ with power series $w_j \in \mathbb{Q}_2[\![t]\!]$. Let $\ell_j(t) = \int_0^t w_j(\tau)\,d\tau \in \mathbb{Q}_2[\![t]\!]$ be the formal integral. Then the coefficient of t^n in ℓ_j has 2-adic valuation at least $\frac{2}{2g+1} - \frac{2}{2g+1}n - \log_2 n$. In particular, the series $\ell_j(t)$ converge when $v_2(t) > \frac{2}{2g+1}$.*

(2) *Let $\tilde{t} = (y - h(x))/x^{g+1}$; this is a uniformizer at ∞. Write $\omega_j = \tilde{w}_j(\tilde{t})\,d\tilde{t}$ with $\tilde{w}_j \in \mathbb{Q}_2[\![\tilde{t}]\!]$ and let $\tilde{\ell}_j(\tilde{t}) = \int_0^{\tilde{t}} \tilde{w}_j(\tau)\,d\tau \in \mathbb{Q}_2[\![\tilde{t}]\!]$. Then the coefficient of $\tilde{t}^n$ in $\tilde{\ell}_j$ has 2-adic valuation at least $\frac{2}{2g+1} + \frac{1}{2g+1}n - \log_2 n$. In particular, the series $\tilde{\ell}_j(\tilde{t})$ converge when $v_2(\tilde{t}) > -\frac{1}{2g+1}$.*

Proof. Since C' has good reduction, the differentials $\omega'_j = \xi^j\,d\xi/(2\eta + h(\pi^2\xi))$, for $j = 0, 1, \ldots, g-1$, form a basis of the Néron differentials on C' over $\mathbb{Z}_2[\pi]$. In terms of the isomorphism between C and C' given in the proof of Lemma 2.2, we find that $\omega_j = \pi^{2j+2}\omega'_j$.

To prove (1), we observe that the ω'_j reduce to regular differentials on $\tilde{C}$, which implies that we can write $\omega'_j(\tau) = u_j(\tau)\,d\tau$ with $u_j \in \mathbb{Z}_2[\pi][\![\tau]\!]$, where $\tau = \xi = \pi^{-2}t$ is a

uniformizer at the image of P_0 on C' that reduces to a uniformizer at the reduction of this point on $\tilde{C}$. Then

$$w_j(t)\,dt = \omega_j = \pi^{2j+2}\omega_j' = \pi^{2j+2}u_j(\tau)\,d\tau = \pi^{2j}u_j(\pi^{-2}t)\,dt\,,$$

so the coefficient of t^n in w_j has valuation $\geq (2j-2n)v_2(\pi) \geq -\frac{2}{2g+1}n$. The claim follows.

The proof of (2) is similar. $\tilde{\tau} = \eta/\xi^{g+1} = \pi\tilde{t}$ is a uniformizer at ∞ on C' that reduces to a uniformizer at ∞ on $\tilde{C}$. As before, we have that $\omega_j'(\tilde{\tau}) = \tilde{u}_j(\tilde{\tau})\,d\tilde{\tau}$ with $\tilde{u}_j \in \mathbb{Z}_2[\pi][\![\tilde{\tau}]\!]$. Then

$$\tilde{w}_j(\tilde{t})\,d\tilde{t} = \omega_j = \pi^{2j+2}\omega_j' = \pi^{2j+2}\tilde{u}_j(\tilde{\tau})\,d\tilde{\tau} = \pi^{2j+3}\tilde{u}_j(\pi\tilde{t})\,d\tilde{t}\,,$$

so the coefficient of $\tilde{t}^n$ in $\tilde{w}_j$ has valuation $\geq (2j+3+n)v_2(\pi) \geq \frac{1}{2g+1}(3+n)$, and the claim follows. □

One can show that $(\omega_0/2, \ldots, \omega_{g-1}/2)$ is a basis of the $\mathbb{Z}_2$-module of Néron differentials on C over $\mathbb{Z}_2$, but we will not need this. We set $\underline{\omega} = (\omega_0, \ldots, \omega_{g-1})$.

Recall that pull-back under i induces a canonical isomorphism between the space of regular (equivalently, invariant) 1-forms on J and the space of regular differentials on C. We write $\underline{\omega}_J$ for the basis of $\Omega^1(J_{\mathbb{Q}_2})$ corresponding under this isomorphism to $\underline{\omega}$. On the compact commutative 2-adic Lie group $J(\mathbb{Q}_2)$ we have the logarithm homomorphism $J(\mathbb{Q}_2) \to T_0J(\mathbb{Q}_2)$, where the target is the tangent space at the origin. Since the space of invariant differentials on $J_{\mathbb{Q}_2}$ is canonically isomorphic to the cotangent space at the origin, the logarithm corresponds to a pairing between $J(\mathbb{Q}_2)$ and the space of invariant differentials. Using the isomorphism mentioned above, the pairing is given by

$$J(\mathbb{Q}_2) \times \Omega^1(C_{\mathbb{Q}_2}) \ni \Big(\sum_{j=1}^m i(P_j), \omega\Big) \longmapsto \sum_{j=1}^m \log_\omega P_j := \sum_{j=1}^m \int_\infty^{P_j} \omega\,,$$

where the P_j are points in $C(\bar{\mathbb{Q}}_2)$ and the integral here is the Berkovich-Coleman integral on C over $\mathbb{Q}_2$; see [Ber07]. (It agrees with the abelian integral, since the Berkovich space of C over $\mathbb{C}_2$ is simply connected; this comes from the fact that C has potentially good reduction.) We define $\log\colon J(\mathbb{Q}_2) \to \mathbb{Q}_2^g$ as the g-tuple of homomorphisms given in this way by pairing with $\underline{\omega}$. Then log induces a $\mathbb{Z}_2$-linear map on the kernel of reduction in $J(\mathbb{Q}_2)$. In particular, its image Λ is a full $\mathbb{Z}_2$-lattice. We fix an isomorphism $\Lambda \simeq \mathbb{Z}_2^g$ of $\mathbb{Z}_2$-modules and define $\log'\colon J(\mathbb{Q}_2) \to \mathbb{Z}_2^g$ to be the composition of log with this isomorphism. This induces an $\mathbb{F}_2$-linear surjective map $\overline{\log'}\colon J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \to \mathbb{F}_2^g$. Its kernel is the image of $J(\mathbb{Q}_2)[2^\infty]$ in $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ (the kernel of $\log'$ is the same as the kernel of log, which is $J(\mathbb{Q}_2)_{\mathrm{tors}}$, and torsion of odd order is mapped to zero in the quotient).

To make use of $\overline{\log'}$ later, we will need to know $\Lambda = \log(J(\mathbb{Q}_2))$. We note that Lemma 2.4 shows that when $P = (x, y)$ is a point on C with $v_2(x) < \frac{2}{2g+1}$, then its image P' on C' has $v_2(\xi) = v_2(x) - \frac{2}{2g+1} < 0$, so it reduces to ∞ on $\tilde{C}$, and we have that $\tilde{t}(P) = \pi^{-1}\tilde{\tau}(P')$ has valuation $> -\frac{1}{2g+1}$. We can then evaluate $\log i(P) = \int_\infty^P \underline{\omega} \in \mathbb{Q}_2^g$ numerically by evaluating the series $\tilde{\ell}_j$ at $\tilde{t}$ to any desired 2-adic accuracy. Similarly, if $v_2(x) > \frac{2}{2g+1}$, we can evaluate $\log i(P)$ numerically by evaluating the series ℓ_j at x, since we have that $\log i(P) = \log i(P) - \log i(P_0) = \int_{P_0}^P \underline{\omega}$ ($i(P_0)$ has finite order and so is killed by the logarithm). We recall that every point $Q \in J(\mathbb{Q}_2)$ is represented by a divisor of the

form $D - d \cdot \infty$, where D is an effective divisor of degree $d \leq g$ defined over $\mathbb{Q}_2$. This implies that $J(\mathbb{Q}_2)$ is generated by points of the form $\mathrm{Tr}_{K/\mathbb{Q}_2} i(P)$ where $P \in C(K)$ and K is an extension of $\mathbb{Q}_2$ of degree $\leq g$. Since the ramification index of K is at most g, it follows that $v_2(x(P)) \neq \frac{2}{2g+1}$, so that we can evaluate $\log i(P)$ for all relevant P in the way sketched above.

Write $A = \mathbb{Q}[x]/\langle f \rangle$; we denote the image of x in A by θ, so that $A = \mathbb{Q}[\theta]$. Then A is an étale algebra over $\mathbb{Q}$; it is a product of algebraic number fields corresponding to the irreducible factors of f. Recall that the 2-Selmer group of J can be identified with a subgroup of $A^\times/A^{\times 2}$; more precisely, a subgroup of elements of $A(S,2)$ with trivial norm in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Here S is the set of primes of A above prime numbers p such that p^2 divides the discriminant of f, and $A(S,2)$ is the (finite) subgroup of $A^\times/A^{\times 2}$ consisting of elements whose valuation at all primes outside S is even; see [Sch95, Sto01]. We let H denote the subgroup of $A(S,2)$ consisting of elements with trivial norm. We identify the 2-Selmer group $\mathrm{Sel}_2(J)$ with its image in H. (Usually, we would have to include the primes above 2 in S, but here we can leave them out, since f has odd discriminant. The standard argument then shows that elements in the image of the Selmer group must have even valuation at the primes above 2. See also the proof of Lemma 2.12 (2), which shows that enough images of points land in H_2 to span the full image.)

We have the 2-adic local analogue

$$H_2 = \mathbb{Z}_2[\theta]^\times/\mathbb{Z}_2[\theta]^{\times 2}$$

(note that $\mathbb{Z}_2[\theta]$ is the ring of integers of $A_2 = \mathbb{Q}_2[x]/\langle f \rangle = A \otimes_{\mathbb{Q}} \mathbb{Q}_2$) and the canonical homomorphism $\rho_2 \colon H \to H_2$. Write δ_2 for the map $J(\mathbb{Q}_2) \to H_2$ given by the "$x - T$ map" on $J(\mathbb{Q}_2)$. It lands in H_2 by the parenthesized remark above. We note that by definition, ρ_2 maps the 2-Selmer group into the image of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ in H_2 under the local descent map. So we can define (slightly abusing notation) the $\mathbb{F}_2$-linear map $\overline{\log'} \circ \rho_2 \colon \mathrm{Sel}_2(J) \to \mathbb{F}_2^g$.

Remark 2.5. We note that we can use knowledge of the image J_2 of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ in H_2 to determine $\mathrm{Sel}_2(J)$ from the "relaxed" 2-Selmer group $\widetilde{\mathrm{Sel}}$ of J, where we leave out the local condition at 2. This is because $\mathrm{Sel}_2(J) = \widetilde{\mathrm{Sel}} \cap \rho_2^{-1}(J_2)$. This can give a faster way of determining the Selmer group compared to the standard implementation in Magma. See also [Sto17, Remark 4.2].

We write δ for the global descent map $J(\mathbb{Q}) \to \mathrm{Sel}_2(J) \subseteq H$. Its kernel is $2J(\mathbb{Q})$, and we have $\delta_2 = \rho_2 \circ \delta$ on $J(\mathbb{Q})$. We need a further assumption.

Assumption 2.6.

(A3) The map $\overline{\log'} \circ \rho_2 \colon \mathrm{Sel}_2(J) \to \mathbb{F}_2^g$ has kernel $\delta\big(J(\mathbb{Q})[2^\infty]\big)$.

Since we will exclusively deal with vector spaces over $\mathbb{F}_2$ in the following, all dimensions will be $\mathbb{F}_2$-dimensions.

Note that $\delta\big(J(\mathbb{Q})[2^\infty]\big)$ is always contained in the kernel of $\overline{\log'} \circ \rho_2$. Since we have $\dim \delta\big(J(\mathbb{Q})[2^\infty]\big) = \dim J(\mathbb{Q})[2]$, the assumption is equivalent to

$$\dim \mathrm{Sel}_2(J) - \dim J(\mathbb{Q})[2] = \dim \overline{\log'}\big(\rho_2(\mathrm{Sel}_2(J))\big) .$$

The term on the left is the upper bound on the rank of $J(\mathbb{Q})$ that we obtain from the 2-Selmer group. In the applications, we need to compute $\overline{\log'}$ on $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ in any case, so the assumption is easy to check.

Remark 2.7. If $J(\mathbb{Q})[2] = 0$ (which is equivalent to f being irreducible over $\mathbb{Q}$), then the assumption reduces to saying that $\overline{\log'} \circ \rho_2$ is injective, which in particular implies that ρ_2 is injective on the Selmer group, but the condition is in general stronger than this.

Define $\rho\colon \mathbb{Z}_2^g \setminus \{0\} \to \mathbb{F}_2^g \setminus \{0\}$, $\underline{a} \mapsto \overline{2^{-v_2(\underline{a})}\underline{a}}$.

Proposition 2.8. *Assume* (A3) *and let* $Q \in J(\mathbb{Q})$ *with* $\log' Q \neq 0$ *(i.e.,* $Q \notin J(\mathbb{Q})_{\mathrm{tors}}$*). Then* $\rho \log' Q \in \overline{\log'}\big(\rho_2(\mathrm{Sel}_2(J))\big)$.

Proof. Since $\log'\big(2^k J(\mathbb{Q}) + J(\mathbb{Q})_{\mathrm{tors}}\big) \subset 2^k\mathbb{Z}_2^g$ and $\log' Q \neq 0$, there is a largest $k \geq 0$ with $Q \in 2^k J(\mathbb{Q}) + J(\mathbb{Q})_{\mathrm{tors}}$. Write $Q = 2^k Z + T$ with $T \in J(\mathbb{Q})_{\mathrm{tors}}$; then $Z \notin 2J(\mathbb{Q}) + J(\mathbb{Q})_{\mathrm{tors}}$. So $\delta(Z) \in \mathrm{Sel}_2(J)$ is not in $\delta(J(\mathbb{Q})_{\mathrm{tors}}) = \delta(J(\mathbb{Q})[2^\infty])$ (odd torsion lies in $2J(\mathbb{Q})$), and by (A3), $\overline{\log'}(\delta_2(Z)) \neq 0$, that is, $\log' Z \notin 2\mathbb{Z}_2^g$. Hence

$$\rho \log' Q = \rho(2^k \log' Z) = \log' Z \bmod 2 = \overline{\log'}\big(\rho_2(\delta(Z))\big) \in \overline{\log'}\big(\rho_2(\mathrm{Sel}_2(J))\big)\,. \qquad \square$$

This has the following consequence, which we will use in our applications. It is the essence of the "Selmer group Chabauty" method from [Sto17] for the determination of the rational points on C.

Corollary 2.9. *Assume* (A3). *If* $\rho \log' i(Q) \notin \overline{\log'}\big(\rho_2(\mathrm{Sel}_2(J))\big)$ *for every* $Q \in C(\mathbb{Q}_2)$ *such that* $i(Q) \notin J(\mathbb{Q}_2)_{\mathrm{tors}}$*, then* $i(P) \in J(\mathbb{Q})_{\mathrm{tors}}$ *for every* $P \in C(\mathbb{Q})$. *In particular, if in addition* f *is irreducible, then* $C(\mathbb{Q}) = C(\mathbb{Q})_{\mathrm{odd}}$.

Proof. Let $P \in C(\mathbb{Q})$. If $\log' i(P) = 0$, then $i(P) \in J(\mathbb{Q})_{\mathrm{tors}}$ as claimed (and if f is irreducible, every torsion point has odd order, so $P \in C(\mathbb{Q})_{\mathrm{odd}}$). Otherwise, Proposition 2.8 with $Q = i(P)$ gives a contradiction. $\square$

Here is a variant that is more convenient when there are other rational points (we will need it for the proof of Proposition 3.7).

Corollary 2.10. *Assume* (A3). *Let* $B \in C(\mathbb{Q})$ *and* $X \subseteq C(\mathbb{Q}_2)$ *be such that* $\log'[P - B] \neq 0$ *and* $\rho(\log'[P - B]) \notin \overline{\log'}\big(\rho_2(\mathrm{Sel}_2(J))\big)$ *for all* $P \in X \setminus \{B\}$. *Then* $X \cap C(\mathbb{Q}) \subseteq \{B\}$.

Proof. Apply Proposition 2.8 to $Q = [P - B]$ for $P \in X \cap C(\mathbb{Q})$ with $P \neq B$. $\square$

We now come back to determining the image of log for the family of curves considered in this paper. By Nakayama's Lemma, $\log(J(\mathbb{Q}_2))$ is generated as a $\mathbb{Z}_2$-module by the images of representatives of a basis of (the $\mathbb{F}_2$-vector space) $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$. We know that $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = g + \dim J(\mathbb{Q}_2)[2]$, and $\dim J(\mathbb{Q}_2)[2]$ is one less than the number of irreducible factors of f over $\mathbb{Q}_2$; see [Sto01]. Also, we have the injective homomorphism $\delta_2\colon J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \to H_2$, which we can compute fairly easily.

A more thorough analysis allows us to pin down $\log(J(\mathbb{Q}_2))$ precisely without having to search for suitable points in $J(\mathbb{Q}_2)$. First we need a handle on H_2.

Lemma 2.11. *We denote reduction mod 2 by a bar. Note that $\mathbb{F}_2[\bar\theta] = F_1 \times \cdots \times F_m$ is a direct product of finite field extensions of $\mathbb{F}_2$ (this is because the discriminant of f is odd). For $\alpha \in \mathbb{Z}_2[\theta]$, we let $\bar\alpha_j \in F_j$ denote the jth component of $\bar\alpha \in \mathbb{F}_2[\bar\theta]$. Let $R \subset \mathbb{Z}_2[\theta]$ be a complete set of representatives of $\mathbb{F}_2[\bar\theta]$.*

(1) *Let $\alpha \in \mathbb{Z}_2[\theta]$. Then $1+4\alpha$ is a square in $\mathbb{Z}_2[\theta]$ if and only if $\operatorname{Tr}_{F_j/\mathbb{F}_2} \bar\alpha_j = 0$ for all j. We define $\operatorname{Tr}\colon \mathbb{F}_2[\bar\theta] \to \mathbb{F}_2^m$ as $\operatorname{Tr}(\bar\alpha) = (\operatorname{Tr}_{F_j/\mathbb{F}_2} \bar\alpha_j)_{j=1,\dots,m}$.*

(2) *Let $B \subset R$ be representatives of an $\mathbb{F}_2$-basis of $\mathbb{F}_2[\bar\theta]$ and let $B' \subset R$ be representatives of an $\mathbb{F}_2$-basis of $\mathbb{F}_2[\bar\theta]/\ker\operatorname{Tr}$. Then $(1+2\beta)_{\beta\in B}$ together with $(1+4\beta')_{\beta'\in B'}$ is an $\mathbb{F}_2$-basis of H_2.*

Proof. Let $\Pi = 1+2\mathbb{Z}_2[\theta]$ be the group of principal units. Since $\mathbb{Z}_2[\theta]^\times/\Pi \simeq F_1^\times \times \cdots \times F_m^\times$ is finite of odd order, the inclusion $\Pi \hookrightarrow \mathbb{Z}_2[\theta]^\times$ induces an isomorphism $\Pi/\Pi^2 \simeq H_2$.

(1) If $1+4\alpha$ is a square, it must be the square of an element of the form $1+2\beta$ with $\beta \in \mathbb{Z}_2[\theta]$. Now $(1+2\beta)^2 = 1+4(\beta+\beta^2)$, so the condition is that $\alpha = \beta+\beta^2$ for some $\beta \in \mathbb{Z}_2[\theta]$. Since $\operatorname{Tr}\bar\beta = \operatorname{Tr}\bar\beta^2$, every such α satisfies $\operatorname{Tr}\bar\alpha = 0$. Conversely, if $\operatorname{Tr}\bar\alpha = 0$, there is $\bar\beta \in \mathbb{F}_2[\bar\theta]$ such that $\bar\alpha = \bar\beta + \bar\beta^2$. Then $1+4\alpha \equiv (1+2\beta)^2 \bmod 8\mathbb{Z}_2[\theta]$, which implies that $1+4\alpha$ is a square as well.

(2) We clearly have that $\Pi^2 \subset 1+4\mathbb{Z}_2[\theta]$. The result of (1) implies that $1+4\alpha \mapsto \operatorname{Tr}\bar\alpha$ induces an isomorphism $(1+4\mathbb{Z}_2[\theta])/\Pi^2 \simeq \mathbb{F}_2^m$. In particular, $(1+4\beta')_{\beta'\in B'}$ is a basis of the $\mathbb{F}_2$-vector space on the left. Also, $1+2\beta \mapsto \bar\beta$ induces an isomorphism $\Pi/(1+4\mathbb{Z}_2[\theta]) \simeq \mathbb{F}_2[\bar\theta]$, so that $(1+2\beta)_{\beta\in B}$ gives a basis of the space on the left. Combining these two bases gives the result. □

Now we can use this information to get at the image of log.

Lemma 2.12. *We write $\Sigma\operatorname{Tr}\bar\alpha$ for $\sum_{j=1}^m \operatorname{Tr}_{F_j/\mathbb{F}_2} \bar\alpha_j \in \mathbb{F}_2$, with notation as in Lemma 2.11.*

(1) *We have that $\Sigma\operatorname{Tr}\bar\theta^{-d} = 0$ for $1 \le d \le 2g$.*

(2) *The image in H_2 of $J(\mathbb{Q}_2)$ under δ_2 has basis represented by $(1-2\theta^{-d})_{d=1,\dots,g}$ and $(1+4\theta^{-d})_{d\in I}$, where $I \subset \{1,3,5,\dots,2g-1\}$ is such that $(\bar\theta^{-d})_{d\in I}$ is a basis of $\ker\Sigma\operatorname{Tr}/\ker\operatorname{Tr}$.*

(3) *Let $\underline\omega = \sum_{n=0}^\infty t^n \underline a_n\,dt$ with $t = x$ a uniformizer at $P_0 = (0,h(0))$ and $\underline a_n \in \mathbb{Q}_2^g$ with $v_2(\underline a_n) \ge \lceil -\frac{2n}{2g+1} \rceil$. Then*

$$\log(J(\mathbb{Q}_2)) = \Big\langle \sum_{n=1}^\infty \frac{2^n}{n} \underline a_{dn-1} : d = 1,\dots,g \Big\rangle_{\mathbb{Z}_2} + \Big\langle \sum_{n=1}^\infty \frac{4^n}{n} \underline a_{dn-1} : d \in I \Big\rangle_{\mathbb{Z}_2}.$$

Proof. To prove (1), recall that if p is the reciprocal characteristic polynomial of $\alpha \in L$, where L is an étale algebra over a field K, then we have the following identity of formal power series over K.

$$\sum_{n=1}^\infty (\operatorname{Tr}_{L/K} \alpha^n) z^n = \frac{-zp'(z)}{p(z)}.$$

(We have that $p(z) = z^{[L:K]}c(z^{-1}) = 1 - (\operatorname{Tr}_{L/K}\alpha)z + \dots$ when c is the characteristic polynomial of α.) We apply this to $\alpha = \bar\theta^{-1} \in \mathbb{F}_2[\bar\theta] = L$ and $K = \mathbb{F}_2$. In this case,

$p(z) = \bar{f}(z) = \bar{h}(z)^2 + z^{2g+1} \in \mathbb{F}_2[z]$, so that

$$\frac{-zp'(z)}{p(z)} = \frac{z(2\bar{h}(z)\bar{h}'(z) + (2g+1)z^{2g})}{\bar{f}(z)} = \frac{z^{2g+1}}{\bar{f}(z)} \in \mathbb{F}_2[\![z]\!]\,,$$

which shows that $\Sigma\mathrm{Tr}\,\bar{\theta}^{-d} = \mathrm{Tr}_{\mathbb{F}_2[\bar{\theta}]/\mathbb{F}_2}\,\bar{\theta}^{-d} = 0$ when $1 \le d \le 2g$.

We know that $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = \dim J(\mathbb{Q}_2)[2] + g$. Since

$$\#I = \dim(\ker \Sigma\mathrm{Tr}/\ker \mathrm{Tr}) = m - 1 = \dim J(\mathbb{Q}_2)[2]\,,$$

to show (2) it is enough to show that the given elements are in the image of δ_2, since their number is correct and they are linearly independent according to Lemma 2.11. (Note that the reductions of θ^{-d}, $0 \le d \le 2g$, form a basis of $\mathbb{F}_2[\bar{\theta}]$, so by (1), we can select representatives of a basis of $\ker \Sigma\mathrm{Tr}/\ker \mathrm{Tr}$ from powers of θ. Also note that $\Sigma\mathrm{Tr}\,1 = 1$ and $\mathrm{Tr}\,\bar{\theta}^{-2d} = \mathrm{Tr}\,\bar{\theta}^{-d}$, so it is sufficient to consider powers with odd exponents.)

Let K be a finite extension of $\mathbb{Q}_2$ and take $\alpha \in K$ with $v_2(\alpha) > \frac{2}{2g+1}$. Then

$$f(\alpha) = \alpha^{2g+1} + h(\alpha)^2 \equiv h(\alpha)^2 \bmod 4\pi_K\,,$$

where π_K is a uniformizer of K, so $f(\alpha)$ is a square in K (note that $h(\alpha)$ is a unit), and there is a point $P = (\alpha, \beta) \in C(K)$. Then $\mathrm{Tr}_{K/\mathbb{Q}_2}\,i(P) \in J(\mathbb{Q}_2)$, and if c is the characteristic polynomial of α, then $\delta_2(\mathrm{Tr}_{K/\mathbb{Q}_2}\,i(P)) = (-1)^{\deg c} c(\theta)$ (we specify elements of H_2 by representatives in $\mathbb{Z}_2[\theta]^\times$).

Now consider $\alpha = 2^{1/d} \in \mathbb{Q}_2(2^{1/d})$ for $1 \le d \le g$. Then $v_2(\alpha) = \frac{1}{d} > \frac{2}{2g+1}$, so we obtain a point $Q_d \in J(\mathbb{Q}_2)$ with

$$\delta_2(Q_d) = (-1)^d(\theta^d - 2) = (-\theta)^d(1 - 2\theta^{-d})\,.$$

Since $-\theta = (\theta^{-g}h(\theta))^2$ is a square in $\mathbb{Z}_2[\theta]$, this shows that $1 - 2\theta^{-d}$ is in the image of δ_2. Similarly, taking $\alpha = 4^{1/d} \in \mathbb{Q}_2(2^{1/d})$ with d odd and $d \le 2g-1$, we again have $v_2(\alpha) > \frac{2}{2g+1}$, and we find that $1 + 4\theta^{-d}$ is in the image of δ_2. This proves (2).

To see (3), we recall that the image of log is the $\mathbb{Z}_2$-span of the logarithms of elements of $J(\mathbb{Q}_2)$ that give generators of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$. By the reasoning above, such elements are given by divisors of the form (the y-coordinates $*$ are chosen so that the point lies in the residue disk of P_0)

$$\sum_{k=0}^{d-1} (\zeta_d^k 2^{1/d}, *) - d\cdot\infty\,, \quad 1 \le d \le g, \qquad \text{and} \qquad \sum_{k=0}^{d-1} (\zeta_d^k 4^{1/d}, *) - d\cdot\infty\,, \quad d \in I\,.$$

Here ζ_d denotes a primitive dth root of unity in $\bar{\mathbb{Q}}_2$. The claim follows by noting that

$$\log[(\alpha, *) - \infty] = \sum_{n=1}^{\infty} \frac{\alpha^n}{n} \underline{a}_{n-1}$$

when $v_2(\alpha) > \frac{2}{2g+1}$ and that $\mathrm{Tr}_{\mathbb{Q}_2(2^{1/d})/\mathbb{Q}_2}(2^{k/d}) = 0$ when $d \nmid k$ and $= d2^{k/d}$ otherwise. (We use that d is odd when $d \in I$, so that $x^d - 4$ is irreducible over $\mathbb{Q}_2$.) □

Note that in (3) we can replace I by any larger set contained in $\{1, 3, \ldots, 2g-1\}$, since we get the logarithm of some element of $J(\mathbb{Q}_2)$ for any such d. So to determine the image of log, we first compute the $(2g \times g)$-matrix L whose rows are given by the individual logarithms specified in the lemma (computed to sufficient precision), but with $I = \{1, 3, 5, \ldots, 2g-1\}$. Then we echelonize this matrix over $\mathbb{Z}_2$, which gives us a

$\mathbb{Z}_2$-basis of the image. If the precision turns out to be insufficient for the echelonization process, we have to recompute the logarithms to higher precision. We obtain a matrix $U \in \mathrm{GL}(g, \mathbb{Z}[\frac{1}{2}])$ such that the rows of LU generate $\mathbb{Z}_2^g$. Then $\log' \colon Q \mapsto (\log Q)U$ is a logarithm on $J(\mathbb{Q}_2)$ with image $\mathbb{Z}_2^g$ (we consider $\log Q$ as a row vector here), which is what we need.

Remark 2.13. Lemma 2.12 shows, among other things, that $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ can be generated by classes represented by divisors $[D - (\deg D) \cdot \infty]$ with D reducing to a multiple of $\bar{P}_0$. This can be seen independently as follows. Recall that $\tilde{J}(\mathbb{F}_2)$ has odd order. Let $Q \in J(\mathbb{Q}_2)$ be arbitrary. Then an odd multiple of Q is in the kernel of reduction in $J'(\mathbb{Q}_2(\pi))$ (where J' is the Jacobian of C' as in Lemma 2.2), hence we can assume that Q is in this kernel of reduction to begin with. We can represent Q by a divisor of the form $D - (\deg D) \cdot P_0$ with $\deg D \leq g$. Since $\bar{P}_0$ is not a Weierstrass point, the reduction of D, considered as a divisor on C', must be $(\deg D) \cdot \bar{P}_0$ (because Q is in the kernel of reduction). We can add $(\deg D) \cdot [P_0 - \infty]$ without changing the image mod $2J(\mathbb{Q}_2)$, since $[P_0 - \infty]$ is a torsion point of odd order.

In the following, we will outline an algorithm that can be used to verify the assumption in Corollary 2.9 for a given curve C and thus enable us to determine $C(\mathbb{Q})$. Recall that we first need to verify Assumption (A3). This can be done once we can compute $\overline{\log'}$ on a basis of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$. Then we need to show that $\rho \log' i(P) \notin \overline{\log'}\big(\rho_2(\mathrm{Sel}_2(J))\big)$ for every $P \in C(\mathbb{Q}_2)$ such that $i(P) \notin J(\mathbb{Q}_2)_{\mathrm{tors}}$.

We first consider points $P \in C(\mathbb{Q}_2)$ such that $x(P) \in \mathbb{Z}_2^\times$.

Lemma 2.14. *Assume that $h(1)$ is even. Then all points $P \in C(\mathbb{Q}_2)$ such that $x(P) \in \mathbb{Z}_2^\times$ have $x(P) \equiv 1 - h(1)^2 \bmod 8$, and such points exist. If $\delta_2(i(P)) = x(P) - \theta$ is not in the image of $\mathrm{Sel}_2(J)$ under ρ_2 for one of them, then $C(\mathbb{Q})$ does not contain points P such that $x(P) \in \mathbb{Z}_2^\times$.*

Proof. We first note that $f'(a) = (2g+1)a^{2g} + 2h(a)h'(a) \in \mathbb{Z}_2^\times$ when $a \in \mathbb{Z}_2^\times$, which implies that $f(a + 2^m k) \equiv f(a) + 2^m k \bmod 2^{m+1}$ for $k \in \mathbb{Z}_2$.

Since $h(1)$ is even by assumption, we have $f(1) = 1 + h(1)^2 \in 1 + 4\mathbb{Z}$. Then $f(1 - h(1)^2) \equiv 1 \bmod 8$, hence there is $P \in C(\mathbb{Q}_2)$ with $x(P) = 1 - h(1)^2$.

If $P' \in C(\mathbb{Q}_2)$ is any other point such that $x(P') \in \mathbb{Z}_2^\times$, write $x(P') = x(P) + 2k$ with $k \in \mathbb{Z}_2$. Then $f(x(P')) \equiv 1 + 2k \bmod 4$, so k must be even for $f(x(P'))$ to be a square. We can then write $x(P') = x(P) + 4k$ with $k \in \mathbb{Z}_2$. Then $f(x(P')) \equiv 1 + 4k \bmod 8$, so k must again be even, and we have that $x(P') \equiv x(P) \bmod 8$.

Write $f = f_1 \cdots f_m$ with the f_j the monic irreducible factors of f in $\mathbb{Q}_2[x]$. Then $\mathbb{Q}_2[\theta]$ is isomorphic to the product of the m (unramified) extensions of $\mathbb{Q}_2$ obtained by adjoining a root of $f_1, \ldots, f_m$. Since $f(1)$ and $x(P)$ are odd, $f_j(x(P)) \in \mathbb{Z}_2^\times$ for all j, hence $x(P) - \theta$ is a 2-adic unit in each component of this product. Then $x(P') \equiv x(P) \bmod 8$ implies that the square classes of $x(P') - \theta$ and $x(P) - \theta$ are the same, and so $\delta_2(i(P')) = \delta_2(i(P))$. Since by assumption, $\delta_2(i(P)) \notin \rho_2(\mathrm{Sel}_2(J))$, none of these points can be in $C(\mathbb{Q})$. □

Remark 2.15. If $h(1)$ is odd (hence $f(1)$ is even), dealing with points P such that $x(P) \in \mathbb{Z}_2^\times$ can be more involved, depending on the precise behavior of h. We do not discuss this here.

It remains to consider points whose x-coordinate has either strictly positive or strictly negative 2-adic valuation. We consider rational points P with $v_2(x(P)) > 0$ first. We can

assume that P is 2-adically closer to P_0 than to $\iota(P_0)$. Then $\log' i(P) = (\int_{P_0}^{P} \underline{\omega}) \cdot U$, and we can express the right hand side as a vector of power series in the uniformizer $t = x$ at P_0. So we need to determine the set

$$Z(P_0) := \{\rho \log' i(\tau, *) : 0 \neq \tau \in 2\mathbb{Z}_2\} \subset \mathbb{F}_2^g,$$

where the y-coordinate is chosen so that the point is close to P_0. This is a finite problem, since ρ is locally constant and $\rho \log' i(\tau, *)$ is given by the reduction of the coefficient of t in the series vector whenever the valuation of τ is large enough for the first term in the series to dominate all others. We then check that $Z(P_0)$ has empty intersection with the image of the Selmer group. (See also [PS14], where this kind of argument is used to show that most odd degree hyperelliptic curves have the point at infinity as their only rational point.)

When $v_2(x(P)) < 0$, then P is in the residue disk of ∞. We express $\log' i(P) = (\int_{\infty}^{P} \underline{\omega}) \cdot U$ as power series in $t = y/x^{g+1}$, which is a uniformizer at ∞. Since ∞ is a Weierstrass point and t is odd with respect to the hyperelliptic involution, the series giving $\underline{\omega}$ involve only even powers of t, so no loss of precision is introduced by the formal integral. We then compute $Z(\infty)$ in an analogous way as we did $Z(P_0)$ and check that it does not meet the image of the Selmer group. We obtain the following general statement.

Theorem 2.16. *Assume* (A1)–(A3) *and that* $h(1)$ *is even. If* $1 - h(1)^2 - \theta \notin \rho_2(\mathrm{Sel}_2(J))$ *and neither* $Z(P_0)$ *nor* $Z(\infty)$ *meets* $\overline{\log'}(\rho_2(\mathrm{Sel}_2(J)))$*, and* $\log' i(P) \neq 0$ *for all* $P \in C(\mathbb{Q}_2)$ *with* $v_2(x(P)) \neq 0$ *other than* P_0*,* $\iota(P_0)$ *and* ∞*, then* $C(\mathbb{Q}) = \{\infty, P_0, \iota(P_0)\}$.

We have implemented the procedure described above in Magma [BCP97]. This implementation is available at [Code, `SelChabDyn/`].

3 An application to arithmetic dynamics

As an application of the method described above, we show that the curve

$$\begin{aligned} C\colon y^2 = a_5(x) = x^{15} + x^{14} + 2x^{13} + 5x^{12} + 14x^{11} + 26x^{10} + 44x^9 + 69x^8 \\ + 94x^7 + 114x^6 + 116x^5 + 94x^4 + 60x^3 + 28x^2 + 8x + 1 \end{aligned}$$

of genus 7 has exactly the three rational points ∞, $(0, 1)$ and $(0, -1)$. As usual, we write J for its Jacobian variety. Since $a_5(x) = x^{15} + a_4(x)^2$ with $\deg a_4 = 7$, $a_4(0) = 1$ and $a_4(1) = 26$, Assumptions 2.1 and the assumption in Lemma 2.14 are satisfied. We can also check that a_5 is irreducible and that

$$\mathrm{disc}(a_5) = 13 \cdot 24554691821639909$$

is squarefree. Let θ be a root of a_5 and let $K = \mathbb{Q}(\theta)$. Then the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\theta]$. One checks (using Magma [BCP97], say) that $\mathcal{O}_K$ has trivial narrow class group (the Minkowski bound is less than 10^4, so this can easily be done unconditionally). This implies that both the usual class group and the narrow class group of $\mathcal{O}_K[\frac{1}{2}]$ are trivial, as they both are quotients of the narrow class group of $\mathcal{O}_K$. From this one can deduce that ρ_2 is injective.

Over $\mathbb{F}_2$, a_5 splits into a product of three irreducible factors of degree 5. So $A \otimes \mathbb{Q}_2$ is a product of three copies of the unramified extension of $\mathbb{Q}_2$ of degree 5. In particular, $\dim J(\mathbb{Q}_2)[2] = 2$. We set up H_2 and compute the image of $J(\mathbb{Q}_2)$ under δ_2 using Lemma 2.12. The set I can be taken to be $\{3, 5\}$. We intersect this image with the image of $\widetilde{\mathrm{Sel}}$, which is the subgroup of $\mathcal{O}_K^\times/\mathcal{O}_K^{\times 2}$ consisting of the classes of units with square

norm whose images under the real embeddings corresponding to the two largest roots of a_5 have the same sign. This intersection, which is isomorphic to the 2-Selmer group, has dimension 2. This latter fact was already observed in [DHJ+20]. We will identify the Selmer group with its image in H_2. Since there is no rational 2-torsion, this implies that the rank of $J(\mathbb{Q})$ is at most 2. However, we were unable to find any point of infinite order in $J(\mathbb{Q})$. So we cannot use the standard Chabauty method to determine $C(\mathbb{Q})$.

Points $P \in C(\mathbb{Q}_2)$ with $x(P) \in \mathbb{Z}_2^\times$ have $x(P) \equiv -3 \bmod 8$. We check that the image of $-3-\theta$ in H_2 is not in the Selmer group. This already shows that there are no rational points on C whose x-coordinate is a 2-adic unit; see Lemma 2.14.

We then compute the image of log, again using Lemma 2.12. The transformation matrix U can be taken to be

$$U = \begin{pmatrix} 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 0 & -1/4 & 0 \\ 0 & 0 & 0 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 0 & -1/4 \\ 0 & 0 & 0 & 0 & 0 & 1/4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1/4 \end{pmatrix}.$$

In terms of the corresponding basis of $\mathbb{F}_2^g = (\operatorname{im}\log')/2(\operatorname{im}\log')$, the image of the Selmer group is generated by $(0,1,0,0,0,1,0)$ and $(0,0,1,1,1,1,0)$. This shows that $\overline{\log'} \circ \rho_2$ is injective, so (A3) holds.

Then $\log' i(2t, *)$ is given by the vector of power series

$$\begin{aligned}&\big(t - 2^2t^2 + 2^2t^4 + O(2^3), \quad t^2 + 2^2t^4 + O(2^3), \quad 2^2t^3 + O(2^3),\\ &\quad 2t^4 + O(2^3), \quad O(2^3), \quad 5\cdot 2t^3 + 2^2t^4 + O(2^3), \quad O(2^3)\big).\end{aligned}$$

For odd t, this gives $\rho\log' i(2t,*) = (1,1,0,0,0,0,0)$. For even t, the linear term is dominant and gives $\rho\log' i(2t,*) = (1,0,0,0,0,0,0)$. Both these vectors are not in the image of the Selmer group.

For points near ∞, we write $P(2t)$ for the point with $y/x^8 = 2t$. Then the corresponding series are

$$\big(O(2^2),\ O(2^2),\ O(2^2),\ O(2^2),\ O(2^2),\ O(2^2),\ -t + O(2^2)\big).$$

So $\rho\log' i(P(2t)) = (0,0,0,0,0,0,1)$ for all $0 \neq t \in \mathbb{Z}_2$, which is also not in the image of the Selmer group.

We see that the method is successful and shows that there are no unexpected rational points on C. Since $A_5(x) = x^{16}a_5(1/x)$, this proves the following.

Proposition 3.1. *The only rational number c such that $A_5(c)$ is a square in $\mathbb{Q}$ is $c = 0$.*

We now discuss how to deal with $A_n(x) = y^2$ for composite $n \geq 6$. We begin with an auxiliary result.

Lemma 3.2. *There is a sequence $(B_n)_{n\geq 1}$ of monic polynomials $B_n \in \mathbb{Z}[c]$ such that $A_n(c) = \prod_{d|n} B_d(c)$ for all $n \geq 1$. If $m \neq n$, then the resultant of B_m and B_n is ± 1.*

Proof. (See also [BEK20, Lemma 9.5], which the authors attribute to Bjorn Poonen. The polynomials A_n are known as Gleason polynomials; the complex roots of the B_n are the centers of period exactly n in the Mandelbrot set.) We define $B_n = \prod_{d|n} A_d^{\mu(n/d)} \in \mathbb{Q}(c)$,

where μ is the Möbius function. Then the relation between the A_n's and the B_n's is satisfied. The proof of Lemma 1.1(b) in [Sto92], which gives a similar result for the values $A_n(c)$ when c is an integer, works in the same way over $\mathbb{F}_p[c]$ in place of $\mathbb{Z}$ (it uses that we have a PID with finite residue fields). It shows that the reduction mod p of B_n is a (monic) polynomial and that the reductions of B_m and B_n are coprime when $m \neq n$. Since this holds for every prime p, the first shows that $B_n \in \mathbb{Z}[c]$. The second means that the resultant is not divisible by p for any p, so the resultant must be a unit in $\mathbb{Z}$. □

From the recurrence defining A_n, we find that

$$A_n(0) = 0\,, \qquad A_n(-1) = \begin{cases} -1, & n \text{ odd} \\ 0, & n \text{ even} \end{cases} \quad \text{and} \quad A_n(-2) = \begin{cases} -2, & n = 1\,, \\ 2, & n > 1\,. \end{cases}$$

We also find that $A_n'(0) = 1$, $A_n'(-1) = (-1)^{n-1}$. This implies that

$$B_n(0) = \begin{cases} 0, & n = 1, \\ 1, & n > 1, \end{cases} \quad B_n(-1) = \begin{cases} -1, & n = 1, \\ 0, & n = 2, \\ 1, & n > 2, \end{cases} \quad B_n(-2) = \begin{cases} -2, & n = 1, \\ -1, & n > 1 \text{ squarefree}, \\ 1, & \text{else}. \end{cases}$$

Lemma 3.3. *Assume that $m \geq 2$ divides n and that m is even when n is even. If $c \in \mathbb{Q}$ is such that $A_n(c)$ is a square in $\mathbb{Q}$, then $A_m(c)$ is also a square in $\mathbb{Q}$.*

Proof. We write $A_n = A_m B$ where B is the product of the B_d with d a divisor of n that is not a divisor of m. Our assumptions imply that all these d are > 2. This shows that $B(0) = B(-1) = 1$ and also $B(-2) = A_n(-2)/A_m(-2) = 1$. In addition, B is monic of even degree. Together, these imply that $B(c)$ is a nonzero 3-adic square.

When $A_m(c) = 0$, the claim is trivially true. Otherwise, since the resultant of A_m and B is ± 1 by Lemma 3.2 and the multiplicativity of the resultant, and since both A_m and B have even degree, either both $A_m(c)$ and $B(c)$ are squares or both their negatives are squares. Since $B(c)$ is a nonzero 3-adic square, its negative is a non-square and it follows that $B(c)$ and $A_m(c)$ must both be squares. □

Corollary 3.4.

(1) *Assume that n is odd, p is a prime divisor of n and that $c \in \mathbb{Q}$ is such that $A_n(c)$ is a square. Then $A_p(c)$ is also a square.*

(2) *Assume that $4 \mid n$. Then the only $c \in \mathbb{Q}$ such that $A_n(c)$ is a square are $c = 0$ and $c = -1$.*

(3) *Assume that $n = 2m$ with m odd. If $A_n(c)$ is a square and p is a prime divisor of m, then $A_p(c)$ is a square or $-A_p(c)$ is a square. Also, $A_2(c) = c(c+1)$ is a square.*

Proof.

(1) Take $m = p$ in Lemma 3.3.

(2) Take $m = 4$ in Lemma 3.3 and use that $A_4(c)$ is a square only for $c = 0, -1$; see [DHJ+20].

(3) The first statement follows as in the proof of Lemma 3.3; the difference is that in this case, we cannot show that $B(c)$ must be a square. For the second statement, take $m = 2$ in Lemma 3.3. □

Since each of $A_3(c)$ and $A_5(c)$ is a square only for $c = 0$ and $A_4(c)$ is a square only for $c = 0$ and $c = -1$, this already implies that $A_n(c)$ cannot be a square when $c \neq 0, -1$ and n is an odd multiple of 3 or 5, or a multiple of 4. We now consider A_6.

Proposition 3.5. *Let $c \in \mathbb{Q}$ be such that $A_6(c)$ is a square. Then $c = 0$ or $c = -1$.*

Proof. By the corollary above, $A_2(c)$ is a square. This implies that $c = 0$ or $c = 1/(t^2-1)$ for some $t \in \mathbb{Q} \setminus \{\pm 1\}$. We also know that $c = 0$ when $A_3(c)$ is a square. So we can assume that $-A_3(c)$ is a square. Substituting $c = 1/(t^2 - 1)$ into $-A_3(c) = y^2$ and writing $u = y(t^2 - 1)^2$, we obtain the equation

$$u^2 = -t^6 + 2t^4 - 3t^2 + 1\,;$$

this defines a curve of genus 2 over $\mathbb{Q}$. A 2-descent on its Jacobian as implemented in Magma and described in [Sto01] shows that its Mordell-Weil rank is at most 1. The difference of the two rational points on the curve with t-coordinate zero is a point of infinite order on the Jacobian. Applying Magma's `Chabauty` function (based on [BS10, Section 4.4]) to it shows that these two are the only rational points on the curve. They correspond to $c = -1$; this completes the proof. (The fairly new Magma function `RationalPointsGenus2` takes about 0.1 seconds to obtain this result. See [Sto26] for a description of how it works.) □

This implies that $A_n(c)$ is never a square for $c \neq 0, -1$ when n is any multiple of 3.

We now consider A_7. We will work with the curve $y^2 = a_7(x)$ instead, which is isomorphic to $y^2 = A_7(x)$. When n is odd, $a_{n-1}(0) = 1$ and $a_{n-1}(-1) = 0$ (and so $a_{n-1}(1) \equiv a_{n-1}(-1) = 0 \bmod 2$), so the assumptions that $h(0)$ is odd and $h(1)$ is even are always satisfied for $f(x) = a_n(x) = x^{2g+1} + a_{n-1}^2$ with $g = 2^{n-2} - 1$. The discriminant of a_7 is squarefree,

$$\begin{aligned}\operatorname{disc}(a_7) = -&8291 \cdot 9137 \cdot 420221 \cdot 189946395389 \cdot 4813162343551332730513\\ &\cdot 2837919018511214750008829\\ &\cdot 1858730157152877176856713108209153714699601\,,\end{aligned}$$

and a_7 is irreducible. Let $K = \mathbb{Q}(\theta)$ with θ a root of a_7. Assuming GRH, we can verify with Magma that K has trivial class group. (The Minkowski bound is way too large to make an unconditional computation of the class group feasible. Under GRH, it takes about two and a half hours on the author's current laptop.) So the 2-Selmer group is contained in the units modulo squares. We can then get generators of the unit group quickly as power products on a factor base of elements of K (using Magma's `SUnitGroup` with the optional parameter `Raw`). This allows us to compute the signs of these units in the nine different real embeddings of K and thus to find the subgroup of the group of units modulo squares consisting of elements whose sign vectors are in the image of $J(\mathbb{R})$ under the local descent map δ_∞. This subgroup U_∞ has dimension $35 + 1 - 5 = 31$ as an $\mathbb{F}_2$-vector space (the unit rank is 35, as there are 9 real embeddings and 27 pairs of complex embeddings of K; we add 1 for the torsion subgroup, and the local conditions at infinity cut out a subspace of codimension 5, as the computation shows). We then compute the image of δ_2 as in Lemma 2.12 and the map $\rho_2 \colon U_\infty \to H_2$ and find that ρ_2 is injective and that its image intersects the image of δ_2 trivially. This means that the 2-Selmer group, which is isomorphic to this intersection, is trivial, so the three obvious points are the only rational points on $y^2 = a_7(x)$. This implies the following.

Proposition 3.6. *If* K *as above has odd class number (which is true assuming GRH), then the only rational number* c *such that* $A_7(c)$ *is a square in* $\mathbb{Q}$ *is* $c = 0$.

We can also deal with $n = 10$.

Proposition 3.7. *Let* $c \in \mathbb{Q}$ *be such that* $A_{10}(c)$ *is a square. Then* $c = 0$ *or* $c = -1$.

Proof. Assume that $A_{10}(c)$ is a square. By Corollary 3.4, it follows that $A_5(c)$ is a square or $-A_5(c)$ is a square. In the first case, $c = 0$ by Proposition 3.1. So we consider the second case. If $-A_5(c)$ is a square, then there is a rational point with x-coordinate $-1/c$ on the curve

$$C_- \colon y^2 = -a_5(-x) = x^{15} - a_4(-x)^2 \,.$$

This curve is isomorphic to the quadratic twist by -1 of the curve C discussed earlier; in particular, C and C_- are isomorphic over $\mathbb{Q}(i)$. We use this isomorphism for the computation of logarithms.

First, we compute the 2-Selmer group of the Jacobian J_- of C_-, which turns out to have dimension 3. By searching, we find that the points in $J_-(\mathbb{Q}_2)$ whose a-polynomials in the Mumford representation are in the list given below give a basis of $J_-(\mathbb{Q}_2)/2J_-(\mathbb{Q}_2)$.

$$x^2 + 2x + 2\,, \quad x^4 + 2x^3 + 2\,, \quad x^4 + 2x^2 + 2\,, \quad x^6 + 2x^3 + 2\,, \quad x^6 + 2x^5 + 2x^4 + 2x^3 + 2\,,$$
$$x - 1\,, \quad x^2 + x + 1\,, \quad x^3 - 2x^2 + 3x - 1\,, \quad x^6 + 2x^5 - 2x^3 - 3x - 3$$

The first five of these have roots α satisfying $v_2(\alpha) \geq 1/6$. Their logarithms can be computed using the expansion around $(0, i)$ in a similar way as for C. (The polynomials split into two factors over $\mathbb{Q}_2(i)$ corresponding to the two branches $y \sim \pm i h(x)$ near $x = 0$; one has to take the difference of the logarithms computed for the two factors to make sure the same base-point $(0, i)$ is used. Note that the image of this point under the usual embedding is torsion.) The remaining four have roots that are 2-adic units. They fall into the domain of convergence of the logarithm expansions around ∞ in terms of $t = (y + i h(x))/x^8$ (with $h(x) = a_4(-x)$). As a consistency check, the logarithms we obtain are indeed in $\mathbb{Q}_2$ (to the target precision), even though the computation involves $\mathbb{Q}_2(i)$ in a nontrivial way. We then proceed as for C. We find that the image of the Selmer group under $\overline{\log}' \circ \rho_2$ has dimension 3, which verifies (A3).

We note that there are no rational (not even 2-adic) points P on C_- with $v_2(x(P)) > 0$, since for even x, we have that $-a_5(-x) \equiv -1 \bmod 8$. To deal with points that have $v_2(x(P)) = 0$ and $y(P) \equiv 1 \bmod 4$, we use the base point $(1, 1)$: we expand the logarithms of $[P - (1, 1)]$ at $(1, 1)$ in terms of $t = x - 1$. It is easy to check that $v_2(t)$ must be at least 3 to give a $\mathbb{Q}_2$-point on the curve. For such t, $\rho(\log'[P - (1, 1)])$ is always the same vector, which is not in the image of the Selmer group. By Corollary 2.10 with $B = (1, 1)$ (and similarly, with $B = (1, -1)$ for the points with $y(P) \equiv -1 \bmod 4$), $(1, \pm 1)$ are the only rational points with $v_2(x(P)) = 0$. Note that $[(1, 1) - \infty]$ has infinite order here and in particular non-vanishing logarithm, so just looking at $\rho(\log' i(P))$ would not give a contradiction (the value is that for B, which is in the image of the Selmer group, coming from a rational point).

For points with $v_2(x(P)) < 0$, we proceed in the same way as for C; again, the only image under ρ that occurs is not in the image of the Selmer group. We conclude that $C_-(\mathbb{Q}) = \{\infty, (1, 1), (1, -1)\}$, which means that $c \in \{-1, 0\}$. □

We conclude that for $c \in \mathbb{Q}\backslash\{0,-1\}$, $A_n(c)$ is not a square in $\mathbb{Q}$ when n is a multiple of 3, 4 or 5 or (assuming GRH) an odd multiple of 7. This implies that when $f_c^{\circ 2}$ is irreducible, then so is $f_c^{\circ 6}$, and under GRH, $f_c^{\circ 10}$ is irreducible as well. This proves Theorem 1.2.

We remark that it appears to be hopeless to use the method presented here to show that $A_{11}(c)$ is never a square for $0 \neq c \in \mathbb{Q}$, as this would require showing that the class number of the number field of degree 1023 given by adjoining a root of a_{11} (which is irreducible) to $\mathbb{Q}$ is odd.

A Magma program verifying the computational claims of this section is available at the author's GitHub site [Code, `SelChabDyn/`]. It uses the implementation of the algorithm described in Section 2.

4 Further examples

We take $h(x) = x + 1$ and consider

$$C_g\colon y^2 = x^{2g+1} + (x+1)^2$$

for $g \geq 1$. Then Assumptions 2.1 are satisfied. We ran our algorithm for $g = 1, 2, \ldots, 12$. In each case, (A3) can be checked to be satisfied (and $h(1) = 2$ is even), so that our method can be used. The following table summarizes the results; the entries in the second row give the $\mathbb{F}_2$-dimension of the 2-Selmer group, and a $+$ or $-$ in the third row says whether the method was successful or not in showing that $C_g(\mathbb{Q}) = C_g(\mathbb{Q})_{\mathrm{odd}}$. (We assume GRH for the class group computations when $g \geq 11$.)

g	1	2	3	4	5	6	7	8	9	10	11	12
dim Sel	0	1	0	1	0	2	1	1	2	1	0	2
success?	+	−	+	+	+	+	+	+	+	+	+	+

For $g = 2$, we are not successful, and indeed, $C_2(\mathbb{Q})$ contains further points with x-coordinate 12. Since the Selmer group is one-dimensional, the Mordell-Weil rank is 1, with $[(12, 499) - \infty]$ a rational point of infinite order on the Jacobian. A combination of Chabauty's method with the Mordell-Weil Sieve, as implemented in Magma, allows us to determine $C_2(\mathbb{Q})$; see [BS10, Section 4.4] and [Sto26]. We obtain the following result.

Proposition 4.1. *Let $g \in \{1, 2, \ldots, 12\}$ and let $C_g\colon y^2 = x^{2g+1} + (x+1)^2$. If $g \neq 2$, then $C_g(\mathbb{Q}) = \{\infty, (0,1), (0,-1)\}$ (for $g \geq 11$, this assumes GRH), whereas*

$$C_2(\mathbb{Q}) = \{\infty, (0,1), (0,-1), (12,499), (12,-499)\}.$$

We note that C_1 is the curve $y^2 = a_3(x)$, where a_n is defined as in the preceding section.

We have also run the algorithm systematically for several values of the genus g with all polynomials $h \in \mathbb{Z}[x]$ of degree $\leq g$, with coefficients bounded in absolute value by a quantity depending on g and such that $h(0)$ is odd and $h(1)$ is even. We can restrict to polynomials with positive leading coefficient. We did the computations assuming GRH to speed up the determination of the class groups. The results are summarized in the tables below.

The curves are partitioned according to the dimension of the 2-Selmer group and sorted into three buckets, according to whether our algorithm was successful in proving that there are only the three obvious rational points, the curve has more than these three

rational points (up to a naive x-coordinate height of $4 \log 10$, extended to $7 \log 10$ for the curves where the algorithm was unsuccessful), or the algorithm was unsuccessful, but no additional points were found. We also give the average size of the Selmer group. We note that the total average is reasonably close to 3, which is consistent with the result of [BG13], even though their result does not apply to our restricted family of curves.

For curves with an additional pair of points, one would expect an average of 6 (for all odd degree curves of fixed genus with a marked non-Weierstrass point; see [Sha19, Theorem 1.1], which shows it is at most 6, and equality is expected, see p. 270 there), which is consistent with the trend as g grows in our tables. It is to be expected, and also visible in the data, that the algorithm is more likely to be successful when the Selmer group is small. The increasing success rate as the genus grows is consistent with the result of [PS14, Theorem 10.6], which says that for not too small genus, the method will be successful most of the time in showing that a general hyperelliptic curve of odd degree has the point at infinity as its only rational point, with the probability of failure bounded by $(12g + 20)2^{-g}$ in that larger family. We note that our assumption (A3) is exactly the condition in [PS14, Proposition 6.2] when $J(\mathbb{Q})[2] = 0$ (which is the case with probability 1).

Genus 2, coefficients bounded by 25.

dim Sel	0	1	2	3	4	5	avg. # Sel	total	perc.
success	4208	18	0	0	0	0	1.004	4226	25.0%
more pts.	0	1138	1390	469	36	2	4.029	3035	18.0%
failure	0	6325	2882	414	18	0	2.882	9639	57.0%
total	4208	7481	4272	883	54	2	2.618	16900	100.0%

Genus 3, coefficients bounded by 9.

dim Sel	0	1	2	3	4	5	avg. # Sel	total	perc.
success	4004	2963	161	0	0	0	1.483	7128	41.6%
more pts.	0	760	1150	569	59	2	4.598	2540	14.8%
failure	0	3795	3093	556	37	1	3.346	7482	43.6%
total	4004	7518	4404	1125	96	3	2.757	17150	100.0%

Genus 4, coefficients bounded by 5.

dim Sel	0	1	2	3	4	5	avg. # Sel	total	perc.
success	4806	6317	1715	38	0	0	1.911	12876	58.6%
more pts.	0	731	1218	666	120	9	5.055	2744	12.5%
failure	0	2381	2969	898	91	1	3.992	6340	28.9%
total	4806	9429	5902	1602	211	10	2.905	21960	100.0%

Genus 5, coefficients bounded by 3.

dim Sel	0	1	2	3	4	5	avg. # Sel	total	perc.
success	3307	5708	2447	282	5	0	2.285	11749	69.9%
more pts.	0	693	1204	644	133	6	5.102	2680	15.9%
failure	0	746	1110	463	59	1	4.461	2379	14.2%
total	3307	7147	4761	1389	197	7	3.042	16808	100.0%

Genus 6, coefficients bounded by 3.

dim Sel	0	1	2	3	4	5	6	avg. # Sel	total	perc.
success	22093	41016	22072	4096	204	4	0	2.554	89485	76.1%
more pts.	0	3783	7629	4539	1116	109	7	5.598	17183	14.6%
failure	0	2792	4990	2673	497	28	0	5.080	10980	9.3%
total	22093	47591	34691	11308	1817	141	7	3.235	117648	100.0%

Genus 7, 1000 random polynomials h with coefficients bounded by 10.

dim Sel	0	1	2	3	4	5	avg. # Sel	total	perc.
success	199	398	222	56	4	0	2.725	879	87.9%
more pts.	0	11	20	14	4	0	5.673	49	4.9%
failure	0	19	26	19	7	1	6.083	72	7.2%
total	199	428	268	89	15	1	3.111	1000	100.0%

References

[BG13] Manjul Bhargava and Benedict H. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and L-functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91. MR3156850 ↑4

[Ber07] Vladimir G. Berkovich, *Integration of one-forms on p-adic analytic spaces*, Annals of Mathematics Studies, vol. 162, Princeton University Press, Princeton, NJ, 2007. MR2263704 ↑2

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478 ↑2, 3

[BS10] Nils Bruin and Michael Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, DOI 10.1112/S1461157009000187. MR2685127 ↑3, 4

[BEK20] Xavier Buff, Adam L. Epstein, and Sarah Koch, *Eigenvalues of the Thurston operator*, J. Topol. **13** (2020), no. 3, 969–1002, DOI 10.1112/topo.12145. MR4100123 ↑3

[DHJ+20] David DeMark, Wade Hindes, Rafe Jones, Moses Misplon, Michael Stoll, and Michael Stoneman, *Eventually stable quadratic polynomials over* $\mathbb{Q}$, New York J. Math. **26** (2020), 526–561. MR4103000 ↑1, 3, 2

[Jon13] Rafe Jones, *Galois representations from pre-image trees: an arboreal survey*, Actes de la Conférence "Théorie des Nombres et Applications", Publ. Math. Besançon Algèbre Théorie Nr., vol. 2013, Presses Univ. Franche-Comté, Besançon, 2013, pp. 107–136 (English, with English and French summaries). MR3220023 ↑1

[PS14] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7. MR3245014 ↑2, 4

[Sch95] Edward F. Schaefer, *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232, DOI 10.1006/jnth.1995.1044. MR1326746 ↑2

[Sha19] Ananth N. Shankar, *2-Selmer groups of hyperelliptic curves with marked points*, Trans. Amer. Math. Soc. **372** (2019), no. 1, 267–304, DOI 10.1090/tran/7546. MR3968769 ↑4

[Sto92] Michael Stoll, *Galois groups over* **Q** *of some iterated polynomials*, Arch. Math. (Basel) **59** (1992), no. 3, 239–244, DOI 10.1007/BF01197321. MR1174401 ↑1, 3

[Sto01] ———, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626 ↑2, 2, 3

[Sto17] ———, *Chabauty without the Mordell-Weil group*, Algorithmic and experimental methods in algebra, geometry, and number theory (G. Böckle, W. Decker, and G. Malle, eds.), Springer, Cham, 2017, pp. 623–663, DOI 10.1007/978-3-319-70566-8_28. MR3792746 ↑1, 2.5, 2

[Sto26] ———, *Determining the rational points on a curve of genus 2 and Mordell-Weil rank 1*, Proceedings of the International Congress of Mathematicians 2026 — Volume 3: Invited Lectures (Sections 1–4), Society for Industrial and Applied Mathematics, 2026, pp. 484–498, DOI 10.1137/25M1804650. https://epubs.siam.org/doi/abs/10.1137/25M1804650. ↑3, 4

[Code] ———, *Magma scripts implementing the algorithms in this paper*, 2026. https://github.com/MichaelStollBayreuth/Verification. ↑2, 3

MATHEMATISCHES INSTITUT, UNIVERSITÄT BAYREUTH, 95440 BAYREUTH, GERMANY.

Email address: Michael.Stoll@uni-bayreuth.de