ACTA ARITHMETICA
169.1 (2015)

The arithmetic of curves defined by iteration

by

Wade Hindes (Providence, RI)

1. Introduction. The arithmetic properties of iterated rational maps (heights, integer points in orbits, preperiodic points etc.) provide many interesting problems, both directly and by analogy, in classical arithmetic geometry. In this paper, we study another object straddling both geometry and dynamics, the arboreal representation attached to a rational function. Specifically, in the case of quadratic polynomials $f = f_c(x) = x^2 + c$, we translate key problems regarding the size of the Galois groups of iterates of f into a geometric framework.

To state these results, we fix some notation. For $f = x^2 + c$, let f^n denote the nth iterate of f and let $G_n(f) = \mathrm{Gal}(f^n)$ be the Galois group of f^n. Moreover, let $\mathbb{T}_n$ denote the set of roots of $f, f^2, \dots, f^n$ together with 0, and set

$$\mathbb{T}_\infty := \bigsqcup_{n \geq 0} f^{-n}(0) \quad \text{and} \quad G_\infty = \varprojlim G_n(f). \tag{1}$$

If f is irreducible, then $\mathbb{T}_n$ carries a natural 2-ary rooted tree structure: $\alpha, \beta \in \mathbb{T}_n$ share an edge if and only if $f(\alpha) = \beta$. Furthermore, as f is a polynomial with rational coefficients, $G_n(f)$ acts via graph automorphisms on $\mathbb{T}_n$. Hence, we have injections $G_n \hookrightarrow \mathrm{Aut}(\mathbb{T}_n)$ and $G_\infty \hookrightarrow \mathrm{Aut}(\mathbb{T}_\infty)$ called the *arboreal representations* associated to f. A major problem in arithmetic dynamics, most notably because of its application to density questions in orbits [15], is to study the size of these images. For a nice exposition on the subject, as well as the formulation for rational functions $\phi \in \mathbb{Q}(x)$, see [14].

For a fixed stage n, a natural question to ask is which rational values of c supply a polynomial $x^2 + c$ whose nth iterate is the first to have smaller than expected Galois group. When $n = 4$, the only examples up to a very large height are $c = 2/3$ and $c = -6/7$. Moreover, we prove that there are no such integer values (in contrast to the $n = 3$ case in [11]) and formulate

2010 *Mathematics Subject Classification*: Primary 14G05; Secondary 37P55.
Key words and phrases: rational points on curves, arithmetic dynamics, Galois theory.

DOI: 10.4064/aa169-1-1

questions for larger n. Specifically, let

$$S^{(n)} = \{c \in \mathbb{Q} \mid |\mathrm{Aut}(\mathbb{T}_{n-1}) : G_{n-1}(f_c)| = 1 \quad \text{and} \quad |\mathrm{Aut}(\mathbb{T}_n) : G_n(f_c)| > 1\}.$$

Then we use techniques in the theory of rational points on curves (Chabauty's method, unramified coverings, the Mordell–Weil sieve, and bounds on linear forms in logarithms) to deduce the following maximality result for the fourth iterate of these quadratic polynomials.

THEOREM 1.1. *Let $f_c(x) = x^2 + c$ for some $c \in \mathbb{Q}$. Then all of the following statements hold:*

(i) *$S^{(4)} \cap \mathbb{Z} = \emptyset$. That is, if c is an integer and $G_3(f_c) \cong \mathrm{Aut}(\mathbb{T}_3)$, then $G_4(f_c) \cong \mathrm{Aut}(\mathbb{T}_4)$.*
(ii) *If $c \neq 3$ is an integer and $G_2(f_c) \cong \mathrm{Aut}(\mathbb{T}_2)$, then $G_4(f_c) \cong \mathrm{Aut}(\mathbb{T}_4)$.*
(iii) *If the curve $F_2 : y^2 = x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1$ has no rational points of Weil height greater than 10^{100}, then $S^{(4)} = \{2/3, -6/7\}$.*

In the proof of this and subsequent theorems, the key objects which parametrize the size of these dynamical Galois groups are the hyperelliptic curves

$$C_n : y^2 = f^n(x) \quad \text{and} \quad B_n : y^2 = (x - c)f^n(x).$$

Adding to the evidence for open image conjectures in dynamics (see [10], [11], and [14, Conjecture 3.11]), we use these curves defined by iteration and some standard conjectures in arithmetic geometry to prove the following theorem.

THEOREM 1.2. *Let $f(x) = x^2 + c$ for some integer c. If $c \neq -2$ and $-c$ is not a square, then both of the following statements hold:*

(i) *The Hall–Lang conjecture implies that $|\mathrm{Aut}(\mathbb{T}_\infty) : G_\infty(f)|$ is finite.*
(ii) *If the weak form of Hall's conjecture for the Mordell curves holds with $C = 100$ and $\epsilon = 4$, then when $f(x) = x^2 + 3$, we have $|\mathrm{Aut}(\mathbb{T}_\infty) : G_\infty(f)| = 2$.*

REMARK 1.1. This result is analogous to a theorem of Serre for non-CM elliptic curves [2]. Moreover, the analogy is particularly interesting since when $c = -2$, the relevant family of curves actually has CM; see Theorem 1.3 below. The author [11] and Gratton et al. [10] (independently) prove the conclusion of part (i) of Theorem 1.2 assuming the ABC conjecture holds over $\mathbb{Q}$ instead of the Hall–Lang conjecture.

We begin Section 2 by discussing some general arithmetic properties of C_n and B_n. Specifically, we address problems related to the torsion subgroups and simple factors of their Jacobians. For this, we extract information from the specific case when $c = -2$ and f is a Chebyshev polynomial.

In this case, the curves in this family have some very special properties. In particular, let $J(B_n)$ be the Jacobian of B_n. Then we have the following theorem.

THEOREM 1.3. *When $f(x) = x^2 - 2$, all of the following statements hold:*

(i) *$J(B_n)$ is an absolutely simple abelian variety that has complex multiplication by $\mathbb{Q}(\zeta + \zeta^d)$, where ζ is a primitive 2^{n+2}th root of unity and $d = 2^{n+1} - 1$.*

(ii) *Consider $B_n/\mathbb{F}_p$ and let $\chi(B_n, t)$ be the characteristic polynomial of Frobenius.*

  (a) *If $p \equiv 5 \bmod 8$, then $\chi(B_n, t) = t^{2^n} + p^{2^{n-1}}$ for all $n \geq 1$.*
  (b) *If $p \equiv 3 \bmod 8$, then $\chi(B_n, t) = t^{2^n} + p^{2^{n-1}}$ for all $n \geq 2$.*

(iii) *$J(B_n)(\mathbb{Q})_{Tor} \cong \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$. It follows that $\operatorname{rank}(J(B_n)(\mathbb{Q})) \geq 1$ for all $n \geq 2$. Furthermore, $\operatorname{rank}(J(C_n)(\mathbb{Q})) \geq n - 2$ for all $n \geq 1$.*

(iv) *$B_n(\mathbb{Q}) = \{\infty, (-2, 0), (0, \pm 2)\}$ for all $n \geq 2$.*

Note that in part (iv) of Theorem 1.3 we have determined the rational points on a family of curves whose Jacobians are of positive rank and geometrically simple, a usually difficult task. The key point is that our polynomial $f = x^2 - 2$ is equipped with a rational cycle (the fixed point 2), and we will discuss generalizations of this construction to other polynomials with similar dynamical properties (see (18)). Furthermore, as a corollary, we obtain the factorization (into simple factors) of the Jacobians of C_n for a large class of quadratic polynomials.

COROLLARY 1.1. *If $f(x) = x^2 + ax + b \equiv x^2 - 2 \bmod p$ for some $p \equiv \pm 3 \bmod 8$, then the decomposition*

$$J(C_n) \sim J(B_1) \times \cdots \times J(B_{n-1})$$

is indecomposable over $\mathbb{Q}$. In particular, whenever $c + 2$ has a prime factor $p \equiv \pm 3 \bmod 8$, then the decomposition above is indecomposable for $f_c(x) = x^2 + c$.

We close with a discussion of certain Galois uniformity questions, analogous to those for preperiodic points of rational polynomials (see [20] and [13]). For the sake of completeness, all Galois groups were computed with Sage [23], and the descent calculations were carried out with Magma [1]. Since the curves we study are hyperelliptic, the relevant codes may be easily found in the Magma handbook. Finally, we let $\operatorname{Res}(f, g)$ denote the resultant of two polynomials f and g.

2. Arithmetic properties of curves defined by iteration. Let $f = f_c(x) = x^2 + c$. As mentioned in the Introduction, the size of the Galois

group of f^n is encoded in the existence of certain rational points on the curve

$$C_n := \{(x, y) \mid y^2 = f_c^n(x)\} \tag{2}$$

and its quadratic twists (for now, we bracket the discussion of this correspondence and take it up in Section 3). In particular, to understand the Galois groups as we iterate f, we must study the arithmetic of these curves. As a first step, in this section we analyze the torsion subgroups and simple factors of their Jacobians.

When studying the rational points on a curve of large genus, one often attempts to find a map to a curve of lower genus, where the typical arithmetic procedures are more easily carried out. Note that by iterating f we obtain maps

$$C_n \xrightarrow{f} C_{n-1} \xrightarrow{f} \cdots \xrightarrow{f} C_1. \tag{3}$$

However, in order to completely decompose the Jacobians of C_n (and perhaps compute their endomorphism rings), it would be better to find maps to curves whose Jacobians are simple. Fortunately, for $m < n$ we also have the coverings $\pi_m : C_n \to B_m$ given by

$$B_m := y^2 = (x - c)f_c^m(x) \quad \text{and} \quad \pi_m(x, y) = \big(f_c^{n-m}(x), yf_c^{n-m-1}(x)\big). \tag{4}$$

Remark 2.1. Similar maps and curves, π_m and B_m, can be constructed for all quadratic polynomials $f = x^2 + bx + c$ simply by completing the square (see [11]).

From this we can deduce that the Jacobian of C_n decomposes as one might expect from our setup. For simplicity, we adopt the notation $J(C)$ for the Jacobian of any curve C throughout. Furthermore, we write $A \sim B$ when A and B are isogenous abelian varieties.

Proposition 2.1. *Let $f(x) = f_c(x) = x^2 + c$. If f^n is separable, then C_n is nonsingular and*

$$J(C_n) \sim J(B_1) \times \cdots \times J(B_{n-1}) \tag{5}$$

for all $n \geq 2$. In particular, we have such a decomposition when f is irreducible.

Proof. We will proceed by induction on n. If $n = 2$, then both C_2 and B_1 have genus 1. Moreover, $\pi_1 : C_2 \to B_1$ is nonconstant (f has degree two) and hence the induced map on Jacobians must be an isogeny.

Now for the general case: We fix n and let $f_m : C_n \to C_m$ be the map $(x, y) \mapsto (f^{n-m}(x), y)$. The maps f_{n-1} and π_{n-1} induce maps

$$\phi = (\pi_{n-1}, f_{n-1}) : C_n \to B_{n-1} \times C_{n-1}, \quad \phi_* : J(C_n) \to J(B_{n-1}) \times J(C_{n-1}).$$

We show that ϕ induces an isomorphism ϕ^* on the space of regular differentials on C_n and on $B_{n-1} \times C_{n-1}$, from which it follows that ϕ_* is an isogeny.

Note that $\text{genus}(C_n) = 2^{n-1} - 1$ and $\text{genus}(B_m) = 2^{m-1}$. It follows that for $0 \leq i \leq 2^{n-2} - 1$, the set $\{(x^i/y)dx\}$ is a basis of $H^0(B_{n-1}, \Omega)$. Similarly, $\{(x^j/y)dx\}$ is a basis of $H^0(C_{n-1}, \Omega)$ for $0 \leq j \leq 2^{n-2} - 2$. One computes

$$\pi_{n-1}^*\left(\frac{x^i}{y}dx\right) = \frac{f(x)^i}{xy}d(f(x)) = 2\frac{f(x)^i}{y}dx, \tag{6}$$

$$f_{n-1}^*\left(\frac{x^j}{y}dx\right) = \frac{f(x)^j}{y}d(f(x)) = \frac{2f(x)^j x}{y}dx. \tag{7}$$

Since

$$\begin{aligned}\dim_{\mathbb{Q}}(H^0(C_n, \Omega)) &= 2^{n-1} - 1 = 2^{n-2} + 2^{n-2} - 1 \\ &= \dim_{\mathbb{Q}}(H^0(B_{n-1}, \Omega)) + \dim_{\mathbb{Q}}(H^0(C_{n-1}, \Omega)),\end{aligned}$$

it suffices to show that ϕ^* is surjective, to infer that it is an isomorphism. To do this, it is enough to show that $\{(x^i/y)dx\}$ inside $H^0(C_n, \Omega)$ is in the span of the images of π_{n-1}^* and f_{n-1}^* for all $0 \leq i \leq 2^{n-1} - 2$. To establish this, we again proceed by induction.

Note that by (6) and (7), we have

$$\frac{dx}{y} = \frac{1}{2} \cdot \frac{2dx}{y} = \frac{1}{2}\pi_{n-1}^*\left(\frac{dx}{y}\right), \qquad \frac{xdx}{y} = \frac{1}{2} \cdot \frac{2xdx}{y} = \frac{1}{2}f_{n-1}^*\left(\frac{dx}{y}\right).$$

As for the inductive step, suppose that $(x^i/y)dx$ is in the span of π_{n-1}^* and f_{n-1}^* for all $i \leq t - 1$. Furthermore, assume that t is even and write $t = 2k$. If we write $f(x)^k = x^t + \sum_{i=0}^{t-1} c_i x^i$, then

$$\frac{x^t dx}{y} = \frac{1}{2}\pi_{n-1}^*\left(\frac{x^k dx}{y}\right) - \sum_{i=0}^{t-1} c_i \frac{x^i dx}{y}.$$

However, the tail sum is in the span of π_{n-1}^* and f_{n-1}^* by the induction hypothesis (note that t is even and $t \leq 2^{n-1} - 2$ implies that $k \leq 2^{n-2} - 1$, which is needed to force $(x^k/y)dx \in H^0(B_{n-1}, \Omega)$ as desired).

Similarly, if $t = 2k + 1$, then write $f(x)^k = x^{2k} + \sum_{i=0}^{t-2} s_i x^i$. We see that

$$\frac{x^t dx}{y} = \frac{xf(x)^k dx}{y} - \sum_{i=0}^{t-2} s_i \frac{x^{i+1} dx}{y} = \frac{1}{2}f_{n-1}^*\left(\frac{x^k dx}{y}\right) - \sum_{i=0}^{t-2} s_i \frac{x^{i+1} dx}{y}.$$

Again, the tail sum is in the intended span. To see this, note that $t \leq 2^{n-1} - 2$ implies that $k \leq 2^{n-2} - 3$, and hence $(x^k/y)dx$ is in $H^0(C_{n-1}, \Omega)$.

The argument above establishes that $J(C_n) \sim J(B_{n-1}) \times J(C_{n-1})$. However, by induction we deduce that

$$J(C_n) \sim J(B_{n-1}) \times J(B_{n-2}) \times \cdots \times J(B_1)$$

as claimed. ∎

In Corollary 1.1, we show that for many values of c and every m, the Jacobian $J(B_m)$ of B_m is simple. To do this, we extract information from the special case when $c = -2$. In this situation, $f = x^2 - 2$ is a Chebyshev polynomial of degree 2, often denoted T_2 elsewhere in the literature [21, 1.6]. More generally, f^n is the Chebyshev polynomial T_{2^n} of degree 2^n.

We consider the Chebyshev polynomials T_d as characterized by the equations

$$T_d(z + z^{-1}) = z^d + z^{-d} \quad \text{for all } z \in \mathbb{C}^*, \tag{8}$$

and T_d is known to be a degree d monic polynomial with integer coefficients. The classical Chebyshev polynomials $\tilde{T}_d$ were defined in the following way:

$$\text{if we write } z = e^{it}, \text{ then } \tilde{T}_d(2\cos(t)) = 2\cos(dt),$$

though we use the first characterization in (8), where T_d is monic. For a complete discussion of these polynomials, see [21, 1.6].

It has long been known that the dynamical behavior of the Chebyshev polynomials is particularly simple. We will harness this simplicity to deduce strong conclusions about the curves B_n in this case. However, the key insight is that a polynomial does not have to actually be a Chebyshev polynomial for parts of this analysis to work, but simply reduce to $x^2 - 2$ modulo some prime $p \equiv \pm 3 \bmod 8$.

In particular, we obtain arithmetic information for a large class of quadratic polynomials. Our first result in the Chebyshev case is the following.

THEOREM 2.1. *Let $f(x) = x^2 - 2$ and consider the curves $B_n/\mathbb{F}_p$.*

(i) *If $p \equiv 5 \bmod 8$, then B_n has characteristic polynomial $\chi(B_n, t) = t^{2^n} + p^{2^{n-1}}$ for all $n \geq 1$.*
(ii) *If $p \equiv 3 \bmod 8$, then B_n has characteristic polynomial $\chi(B_n, t) = t^{2^n} + p^{2^{n-1}}$ for all $n \geq 2$.*

In particular, $J(B_n)(\mathbb{F}_p) \cong \mathbb{Z}/(p^{2^{n-1}} + 1)\mathbb{Z}$ and $J(B_n)$ is supersingular for the n and p given above.

Proof. To compute $\chi(B_n, t)$, we consider the auxiliary curves

$$\mathfrak{C}_n : y^2 = x(x^{2^n} + 1) \quad \text{and} \quad B_n^{\pm} : y^2 = (x \pm 2)T_{2^n}(x). \tag{9}$$

Note that $\mathfrak{C}_{n+1}$ is equipped with the maps

$$\phi_{\pm} : \mathfrak{C}_{n+1} \to B_n^{\pm}, \qquad \phi_{\pm}(x, y) = \left(x + \frac{1}{x}, \frac{(x \pm 1)y}{x^{2^{n-1}+1}} \right), \tag{10}$$

and that $B_n^{\pm}/\mathbb{F}_p$ are nonsingular for every odd prime. The nonsingularity follows from the fact that $T_2 = f$ is critically finite: $\{f(0), f^2(0), f^3(0), \dots\}$ $= \{\pm 2\}$. Hence the discriminant of $(x \pm 2)f^n(x)$ is a power of 2. In general,

the discriminant Δ_m of f_c^m for any quadratic polynomial $f_c = x^2 + c$ is

$$\Delta_m = \pm \Delta_{m-1}^2 \cdot 2^{2^m} f_c^m(0) \tag{11}$$

(see [15, Lemma 2.6]). Before proceeding with the proof of Theorem 2.1, we are in need of a few lemmata.

LEMMA 2.1. *Let n be any positive integer. If $m < 2^n$ and $p \equiv \pm 3 \bmod 8$, then the field $\mathbb{F}_{p^m}$ contains an element α satisfying $\alpha^{2^{n+1}} = 1$, which is not a square in $\mathbb{F}_{p^m}$.*

Proof. Write $q = p^m$ and suppose that $m = 2^t$. Notice that $\mathbb{F}_q$ contains an element α of order 2^{t+2}, since $p^{2^t} - 1$ is divisible by 2^{t+2} and $\mathbb{F}_q^*$ is cyclic. To see this, write

$$(p^{2^t} - 1) = (p^{2^{t-1}} - 1)(p^{2^{t-1}} + 1) = (p-1)(p+1)(p^2+1)\cdots(p^{2^{t-1}} + 1),$$

inductively. As either $p + 1$ or $p - 1$ is $\equiv 0 \bmod 4$ and every other term in the product is even, we see that $p^{2^t} - 1$ is divisible by 2^{t+2}.

However, $p \equiv \pm 3 \bmod 8$ implies that no higher power of 2 can divide the product. Hence α is not a square in $\mathbb{F}_q$. Finally, the conditions on m force $t \leq n - 1$. Therefore, $\alpha^{2^{n+1}} = 1$ as desired.

In general we may write $m = 2^t a$ for some odd a. By applying the result in the 2-powered case to the subfield $\mathbb{F}_{p^{2^t}} \subset \mathbb{F}_q$, we may find an element $\alpha \in \mathbb{F}_{p^{2^t}}$ with the desired properties. Note that if such an element α were a square in $\mathbb{F}_q$, then it must be a square in $\mathbb{F}_{p^{2^t}}$ (otherwise there would be a proper quadratic extension of $\mathbb{F}_{p^{2^t}}$ contained in $\mathbb{F}_q$, contradicting the fact that a is odd). However, as was the case above, the fact that $p \equiv \pm 3 \mod 8$ implies that α is not a square in $\mathbb{F}_{p^{2^t}}$. ∎

LEMMA 2.2. *If $v_2(p+1) = k$, then $\#B_n^+(\mathbb{F}_q) = \#B_n^-(\mathbb{F}_q)$ for all $n \geq k$ and all $q = p^t$.*

Proof. Notice that when $q = p^{2t}$ or $p \equiv 1 \bmod 4$, the claim easily follows: Choose α in $\mathbb{F}_q$ such that $\alpha^2 = -1$. Then $(x, y) \mapsto (-x, \alpha y)$ is a bijection from $B_n^+(\mathbb{F}_q)$ to $B_n^-(\mathbb{F}_q)$.

When $q = p^{2t+1}$, we define the bijections

$$\pi_+ : B_n^+(\mathbb{F}_q) \to B_n^-(\mathbb{F}_q) \quad \text{and} \quad \pi_- : B_n^-(\mathbb{F}_q) \to B_n^+(\mathbb{F}_q) \tag{12}$$

using the following strategy: For π_+ we take $(a, b) \in B_n^+(\mathbb{F}_q)$ and pullback ϕ_+ defined in (10) to a point $(w, y) \in \mathfrak{C}_n(\mathbb{F}_{q^2})$. Next, apply the endomorphism $(w, y) \mapsto (\zeta^2 w, \zeta y)$ on $\mathfrak{C}_n(\mathbb{F}_{q^2})$ for a suitably chosen root of unity ζ. Finally, apply ϕ_- to get a point on $B_n^-(\mathbb{F}_q)$. Define π_- in a similar fashion.

Specifically, let $a \in \mathbb{F}_q$ and write $a = w + w^{-1}$ for some $w \in \mathbb{F}_{q^2}^*$. Moreover, since $v_2(p+1) = k$, we may choose a primitive 2^{k+1}th root of

unity $\zeta \in \mathbb{F}_{p^2} \subseteq \mathbb{F}_{q^2}$. Define the maps π_+ and π_- as follows:

$$\pi_+(a,b) := \begin{cases} (2,0), & (a,b) = (-2,0), \\ \left(a, \frac{w-1}{w+1}b\right), & a \neq -2,\ a^2-4 \in \mathbb{F}_q^2, \\ \left(\zeta^2 w + (\zeta^2 w)^{-1}, \frac{\zeta^2 w - 1}{w+1} \cdot \frac{-1}{\zeta} b\right), & a \neq -2,\ a^2-4 \notin \mathbb{F}_q^2, \\ \infty, & (a,b) = \infty, \end{cases}$$

and

$$\pi_-(a,b) := \begin{cases} (-2,0), & (a,b) = (2,0), \\ \left(a, \frac{w+1}{w-1}b\right), & a \neq -2,\ a^2-4 \in \mathbb{F}_q^2, \\ \left(\zeta^2 w + (\zeta^2 w)^{-1}, \frac{\zeta^2 w - 1}{w+1} \cdot -\zeta \cdot b\right), & a \neq -2,\ a^2-4 \notin \mathbb{F}_q^2, \\ \infty, & (a,b) = \infty. \end{cases}$$

One easily checks that π_+ and π_- are inverses, that $\pi_+(B_n^+(\mathbb{F}_q)) \subset B_n^-(\mathbb{F}_{q^2})$, and that $\pi_-(B_n^-(\mathbb{F}_q)) \subseteq B_n^+(\mathbb{F}_{q^2})$. The content which remains to be checked is that the respective images of π_+ and π_- are in fact defined over $\mathbb{F}_q$. We complete the argument for π_+ only, as the argument for π_- is identical.

Suppose that $a^2 - 4 \in \mathbb{F}_q^2$ and that $(a,b) \in B_n^+(\mathbb{F}_q)$. Since $w + w^{-1} = a$ (or equivalently $w^2 - aw + 1 = 0$), the quadratic formula tells us that $w \in \mathbb{F}_q$. Hence $\frac{w+1}{w-1}b \in \mathbb{F}_q$ and $\pi_+(a,b) \in B_n^-(\mathbb{F}_q)$ as claimed.

On the other hand, if $a^2 - 4 \notin \mathbb{F}_q^2$, then the Frobenius map $x \mapsto x^q$ acts nontrivially on w, and must send it to w^{-1}, the only other root of $x^2 - ax + 1 = 0$. Note that

$$(\zeta^2)^q = (\zeta^2)^{(p^{2t+1})} = ((\zeta^2)^{p^{2t}})^p = (\zeta^2)^p = \zeta^{-2},$$

since ζ^2 is in $\mathbb{F}_{p^2}$ (hence is fixed by applying $x \mapsto x^p$ an even number of times) and $2(p+1) \equiv 0 \bmod 2^{k+1}$. It follows that $(\zeta^2 w)^q = (\zeta^2 w)^{-1}$ and $(\zeta^2 w) + (\zeta^2 w)^{-1} \in \mathbb{F}_q$.

For the second coordinate, we compute

$$\left(\frac{\zeta^2 w - 1}{w+1} \cdot \frac{-1}{\zeta} \cdot b\right)^q = \frac{\frac{1}{\zeta^2 w} - 1}{\frac{1}{w} + 1} \cdot \frac{-1^q}{\zeta^q} b^q = \frac{1}{\zeta^{q+2}} \cdot \frac{\zeta^2 w - 1}{w+1} b.$$

It suffices to show that $\zeta^{q+1} = -1$. To see this, write $q = p^{2t+1}$ and use the fact that $(\zeta)^{p^{2t}} = \zeta$, since $\zeta \in \mathbb{F}_{q^2}$. In particular, $\zeta^{q+1} = \zeta(\zeta^{p^{2t}})^p = (\zeta)^{p+1} = -1$ as desired. Hence $\pi_+(a,b) \in B_n^-(\mathbb{F}_q)$. ∎

Now for the proof of Theorem 2.1: One checks that $\phi_\pm$ is a quotient map for the involution

$$\psi_\pm(x,y) = \left(\frac{1}{x}, \frac{\pm y}{x^{2^n+1}}\right)$$

of $\mathfrak{C}_{n+1}$ defined in (9). If $G = \mathrm{Aut}(\mathfrak{C}_{n+1})$, then a result of Kani and Rosen [19] on the equivalence of idempotents in the group algebra $\mathbb{Q}[G]$ implies

that the Jacobian of the curve $\mathfrak{C}_{n+1}$ has a decomposition

$$J(\mathfrak{C}_{n+1}) \sim J(B_n^+) \times J(B_n^-) \tag{13}$$

over the rationals. Moreover, since every odd prime is a prime of good reduction, we have a similar decomposition of $J(\mathfrak{C}_n)$ over $\mathbb{F}_p$.

Therefore, it suffices to compute the characteristic polynomial of Frobenius for $\mathfrak{C}_{n+1}$ to find that of B_n. In keeping with our earlier notation, we denote this characteristic polynomial by $\chi(\mathfrak{C}_{n+1}, t)$. We refer the reader to [6, §14.1] for the formulas relating the coefficients of this polynomial to the number of points on the curve over $\mathbb{F}_q$.

Note that the genus of $\mathfrak{C}_{n+1}$ is $g = 2^n$, and so to compute the coefficients of the Euler polynomial of $\mathfrak{C}_{n+1}$, we need to find

$$N_m = \#\mathfrak{C}_{n+1}(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)\left(\frac{x^{2^{n+1}} + 1}{q}\right)$$

for $q = p^m$ and $m \leq 2^n$. To do this, suppose that $m < 2^n$ and apply Lemma 2.1 to find a nonsquare $\alpha \in \mathbb{F}_{p^m}$ satisfying $\alpha^{2^{n+1}} = 1$. We compute

$$\begin{aligned} N_m - (q+1) &= \sum_{x \in S} \sum_{i=1}^{2^{n+1}} \left(\frac{x \cdot \alpha^i}{q}\right)\left(\frac{(\alpha^i \cdot x)^{2^{n+1}} + 1}{q}\right) \\ &= \sum_{x \in S} \left(\sum_{i=1}^{2^{n+1}} \left(\frac{\alpha^i}{q}\right)\right)\left(\frac{x}{q}\right)\left(\frac{x^{2^{n+1}} + 1}{q}\right) = 0, \end{aligned} \tag{14}$$

where S is a set of coset representatives for $\mathbb{F}_q^*/\langle\alpha\rangle$; the final equality follows from the fact that $\left(\frac{\alpha}{p}\right) = -1$.

It is known that χ can be expressed as

$$\chi(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g + p a_{g-1} + \cdots + p^g,$$

where for $i \leq g$ one has

$$i a_i = (N_i - p^i - 1) + (N_{i-1} - p^{i-1} - 1)a_1 + \cdots + (N_1 - p - 1)a_{i-1}. \tag{15}$$

This recurrence relation for the coefficients a_i follows from Newton's formula expressing the elementary power polynomials in terms of the elementary symmetric functions (see [7, p. 619]).

It can be seen from the character sum on (14) and the expression in (15) that

$$\chi(\mathfrak{C}_n, t) = t^{2^{n+1}} + a t^{2^n} + p^{2^n} \quad \text{and} \quad 2^n a = N_{2^n} - p^{2^n} - 1. \tag{16}$$

Note that the Hasse–Weil bound implies that $a \leq 2p^{2^{n-1}}$. We show that this is an equality.

From Lemma 2.2, it follows that $J(\mathfrak{C}_{n+1}) \sim J(B_n^+)^2$ and $\chi(\mathfrak{C}_n, t) = \chi(B_n^+, t)^2$ for the n designated in Theorem 2.1. If we write

$$a = 2p^{2^{n-1}} + 2b_1^2 p^{2^{n-1}-1} + \cdots + b_{2^{n-2}}^2,$$

where the b_i's are the coefficients of the characteristic polynomial of $J(B_n)$, then the bound on a implies that

$$2b_1^2 p^{2^{n-1}-1} + \cdots + b_{2^{n-2}}^2 = 0.$$

We conclude that $b_i = 0$ for all i, and that $\chi(B_n, t) = t^{2^n} + p^{2^{n-1}}$ as claimed. The group structure of $J(B_n)(\mathbb{F}_p)$ follows from a theorem of Zhu, which may be found in [12, §45]. ∎

As mentioned in the Introduction, we can extract global information for a large class of quadratic polynomials from the local data in the Chebyshev case. We restate this information here.

Corollary 1.4. *If $f(x) = x^2 + ax + b \equiv x^2 - 2 \bmod p$ for some $p \equiv \pm 3 \bmod 8$, then the decomposition*

$$J(C_n) \sim J(B_1) \times \cdots \times J(B_{n-1})$$

is indecomposable over $\mathbb{Q}$. In particular, whenever $c+2$ has a prime factor $p \equiv \pm 3 \bmod 8$, then the decomposition above is indecomposable for $f_c(x) = x^2 + c$.

Remark 2.2. We can also use Theorem 2.1 to extract global torsion data. For instance, let $f(x) = x^2 + 63$. Then one can prove that $J(B_n)(\mathbb{Q})_{\mathrm{Tor}} \cong \mathbb{Z}/2\mathbb{Z}$ for all $n \leq 30$. This follows from Theorem 2.1 and the fact that $\gcd(5^{2^n} + 1, 13^{2^n} + 1) = 2$ for all $n \leq 30$.

In the Chebyshev case, the positive density of primes at which $J(B_n)$ has supersingular reduction suggests the presence of latent symmetries. Indeed, one sees that $J(B_1)$ is an elliptic curve which has complex multiplication by $\mathbb{Z}[\sqrt{-2}]$:

$$[\sqrt{-2}](x, y) = \left(-\frac{1}{2} \cdot \frac{x^2 - 2}{x - 2} + 2, \frac{1}{-2\sqrt{-2}} \cdot \frac{y((x-2)^2 - 2)}{(x-2)^2} \right).$$

Moreover, by checking Igusa invariants against known examples, one sees that $J(B_2)$ also has complex multiplication by $\mathbb{Q}(\sqrt{\sqrt{2} - 2})$. Statement (i) of Theorem 1.3, which follows from the work of Carocca, Lange, and Rodriguez [4], shows that these examples are no accident and provides a construction of hyperelliptic curves, defined over the rational numbers, which have complex multiplication.

There is much more we can prove in the Chebyshev case, especially about statements pertaining to rational points. In fact, the technique which we use to determine $B_n(\mathbb{Q})$ for all $n \geq 2$ generalizes to polynomials having

a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-stable cycle, which we discuss after restating and proving the following consolidated theorem.

THEOREM 1.3. *When $f(x) = x^2 - 2$, all of the following statements hold:*

(i) *$J(B_n)$ is an absolutely simple abelian variety that has complex multiplication by $\mathbb{Q}(\zeta + \zeta^d)$, where ζ is a primitive 2^{n+2}th root of unity and $d = 2^{n+1} - 1$.*

(ii) *Consider $B_n/\mathbb{F}_p$ and let $\chi(B_n, t)$ be the characteristic polynomial of Frobenius.*

  (a) *If $p \equiv 5 \bmod 8$, then $\chi(B_n, t) = t^{2^n} + p^{2^{n-1}}$ for all $n \geq 1$.*
  (b) *If $p \equiv 3 \bmod 8$, then $\chi(B_n, t) = t^{2^n} + p^{2^{n-1}}$ for all $n \geq 2$.*

(iii) *$J(B_n)(\mathbb{Q})_{\mathrm{Tor}} \cong \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$. It follows that $\mathrm{rank}(J(B_n)(\mathbb{Q})) \geq 1$ for all $n \geq 2$. Furthermore, $\mathrm{rank}(J(C_n)(\mathbb{Q})) \geq n - 2$ for all $n \geq 1$.*

(iv) *$B_n(\mathbb{Q}) = \{\infty, (-2, 0), (0, \pm 2)\}$ for all $n \geq 2$.*

Proof. For the first statement, note that $\mathfrak{C}_{n+1}$ defined in (9) has complex multiplication by $\mathbb{Q}(\zeta)$, induced by the map

$$[\zeta] : \mathfrak{C}_{n+1} \to \mathfrak{C}_{n+1}, \qquad [\zeta](x, y) = (\zeta^2 x, \zeta y).$$

We have already seen that the quotient curve of $\mathfrak{C}_{n+1}$ by the automorphism ψ is B_n and that $J(\mathfrak{C}_n) \sim J(B_n)^2$ over $\bar{\mathbb{Q}}$. It follows that the simple factors of $J(B_n)$ have complex multiplication by some subfield of $\mathbb{Q}(\zeta)$; see [17, Theorem 3.3].

In [4, Theorem 2] it was shown that $\mathfrak{C}'_{n+1} : y^2 = x(x^{2^{n+1}} - 1)$ has a quotient X with the property that $J(X)$ has complex multiplication by $\mathbb{Q}(\zeta + \zeta^d)$. Moreover, since $\mathbb{Q}(\zeta + \zeta^d)$ does not contain any proper CM fields, $J(X)$ must be absolutely simple (see [17, Theorem 3.3]).

However, note that $\mathfrak{C}_{n+1}$ and $\mathfrak{C}'_{n+1}$ are twists, becoming isomorphic over $\mathbb{Q}(\zeta)$. Since any decomposition of an abelian variety is unique up to isogeny, we must have $J(X) \sim J(B_n)$. Hence, $\mathrm{End}_0(J(X)) \cong \mathrm{End}_0(J(B_n))$ and $J(B_n)$ has CM as claimed.

REMARK 2.3. [4, Theorem 2] was established by studying the general case of metacyclic Galois coverings $Y \to \mathbb{P}^1$ branched at three points, building upon previous work of Ellenberg. To translate, the relevant Galois covering group is

$$G = \langle [\zeta], \psi \mid [\zeta]^{2^{n+1}} = \psi^2 = 1,\ \psi \circ [\zeta] \circ \psi = [\zeta^d] \rangle, \tag{17}$$

and one can take Y to be $\mathfrak{C}'_{n+1}$.

The second statement of Theorem 1.3 is a restatement of Theorem 2.1. For the third statement, we use the fact that $J(B_n)(\mathbb{Q})_{\mathrm{Tor}}$ injects into

$J(B_n)(\mathbb{F}_p)$ via the reduction map [16]. Hence, $J(B_n)(\mathbb{Q})_{\mathrm{Tor}} \cong \mathbb{Z}/2\mathbb{Z}$ follows from the fact that

$$\gcd(5^{2^n}+1, 13^{2^n}+1, 29^{2^n}+1, \dots) = 2 \quad \text{for all } n,$$

where the above set ranges over all (or almost all) primes $p \equiv 5 \bmod 8$. To see this, fix n and suppose that p^* is an odd prime which divides $p^{2^n}+1$ for almost all $p \equiv 5 \bmod 8$. In particular $p^{2^n} \equiv -1 \bmod p^*$, and hence $p^* \equiv 1 \bmod 4$.

Now note that $\gcd(4p^*+1, 8p^*) = 1$, so that Dirichlet's theorem on arithmetic progressions implies that there exist infinitely many primes p_0 with $p_0 = 4p^*+1+8p^*k_0$ for some integer k_0. Moreover, since $4p^*+1 \equiv 5 \bmod 8$, we have $p_0 \equiv 5 \bmod 8$. Hence, we may choose p_0 such that $p_0^{2^n}+1 \equiv 0 \bmod p^*$ by our assumption on p^*.

Finally, one sees that $1 \equiv 4p^*+1+8p^*k_0 \equiv p_0 \bmod p^*$ and $2 \equiv p_0^{2^n}+1 \equiv 0 \bmod p^*$. This is a contradiction since p^* is odd.

On the other hand $f^n(0) = 2$ for all $n \geq 2$, from which it follows that $(0,2) \in B_n(\mathbb{Q})$. Moreover, by the argument above, this point (after embedding it into the Jacobian) is not a torsion point. Hence, $J(B_n)(\mathbb{Q})$ has positive rank. The statement regarding the rank of the rational points of $J(C_n)$ follows from Proposition 2.1.

Finally, we prove statement (iv) of Thereom 1.3. If $n \geq 2$, then C_n maps to $B_1 : y^2 = (x+2)(x^2-2)$. However, B_1 is an elliptic curve, and a 2-descent shows that $B_1(\mathbb{Q})$ has rank zero. It follows that $B_1(\mathbb{Q}) = \{\infty, (-2,0)\}$, and after computing preimages, we see that $C_n(\mathbb{Q})$ contains only the infinite points.

If $n = 2$, a 2-descent shows that the rank of $J(B_2)(\mathbb{Q})$ is one. Moreover, after running the Chabauty function in Magma [1], we see that $B_2(\mathbb{Q}) = \{\infty, (-2,0), (0,\pm 2)\}$. This matches our claim for larger n. For the remaining $n \geq 3$, we use covering collections to determine $B_n(\mathbb{Q})$.

Since the resultant of $x+2$ and f^n is equal to 2 (for all n), the rational points on B_n are covered by the rational points on the curves

$$D_n^{(d)} : du^2 = x+2, \quad dv^2 = f^n(x) \quad \text{for } d \in \{\pm 1, \pm 2\}$$

(see [25, Example 9]). We will proceed by examining the second defining equation $C_n^{(d)} : dv^2 = f^n(x)$ of $D_n^{(d)}$. If $d = 1$, then our description of $C_n(\mathbb{Q})$ implies that $D_n(\mathbb{Q})$ has only the points at infinity. If $d = -2$, then $C_n^{(-2)}$ maps to the elliptic curve $B_1^{(-2)} : -2v^2 = (x+2)(x^2-2)$ via $(x,y) \mapsto (f^{n-1}(x), -2f^{n-2}(x)y)$. A descent shows that $B_1^{(-2)}(\mathbb{Q})$ has rank zero, from which it easily follows that $B_1^{(-2)}(\mathbb{Q}) = \{\infty, (-2,0)\}$. By computing preimages, we find that $C_n^{(-2)}$ and $D_n^{(-2)}$ have no rational points.

For the remaining cases when $d = -1$ and $d = 2$, we map $C_n^{(d)}$ to $B_2^{(d)}$ via $(x,y) \mapsto (f^{n-1}(x), df^{n-2}(x)y)$. However, in either scenario, we find that

$J(B_2^{(d)})(\mathbb{Q})$ has rank one, and moreover, we can compute a generator using bounds between the Weil and canonical heights. After running the Chabauty function in Magma [1] and computing preimages, we find that

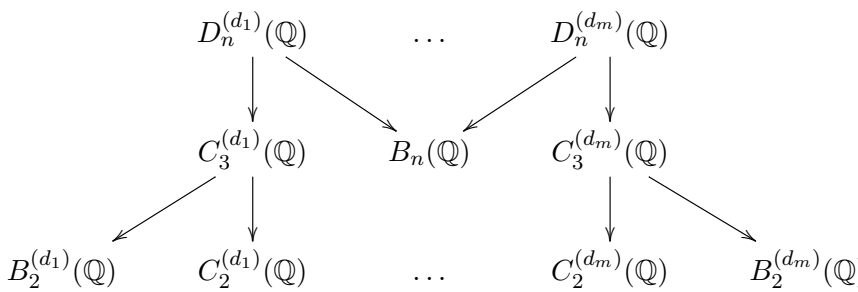
$$C_n^{(2)}(\mathbb{Q}) = \{(0,\pm 1),(\pm 2,\pm 1)\}, \quad C_n^{(-1)}(\mathbb{Q}) = \{(\pm 1,\pm 1)\} \quad \text{for all } n \geq 3.$$

Consequently, $D_n^{(2)}(\mathbb{Q}) = \{(0,\pm 1,\pm 1),(-2,0,\pm 1)\}$ and $D_n^{(-1)}(\mathbb{Q}) = \emptyset$. Moreover, we see that $B_n(\mathbb{Q}) = \{\infty,(-2,0),(0,\pm 2)\}$ as claimed. ∎

Notice that we have determined the rational points on infinitely many curves B_n, each of which does not cover any lower genus curves (their Jacobians have complex multiplication by a CM field with no proper CM subfields).

This is a normally difficult task. However, because -2 has finite orbit under application of the polynomial $x^2 - 2$, the rational points on B_n are covered by finitely many computable twists of a curve D_n. Moreover, the twists are independent of n. Furthermore, each of the finitely many $D_n^{(d)}$ maps to many lower genus curves where standard rational point techniques may be applied (e.g. Chabauty's method, covering collections, rank zero Jacobians) more reasonably.

We illustrate this situation in the following diagram:



A general way to construct examples of families of curves with this stability behavior is to use rational polynomials f with a finite $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-stable cycle.

For instance, if $f(x) = x^2 - 31/48$, then f has a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-stable 4-cycle:

$$\begin{array}{ccc} 1/4+\sqrt{-15}/6 & \xrightarrow{\ f\ } & -1+\sqrt{-15}/12 \\ \uparrow f & & \downarrow f \\ -1-\sqrt{-15}/12 & \xleftarrow{\ f\ } & 1/4-\sqrt{-15}/6. \end{array}$$

We construct a polynomial g from this cycle. Set $\alpha = 1/4+\sqrt{-15}/6$ and let $\bar{\alpha} = 1/4-\sqrt{-15}/6$ be its Galois conjugate. Similarly, set $\beta = -1+\sqrt{-15}/12$

and $\bar{\beta} = -1 - \sqrt{-15}/12$. Now, if one considers

$$g(x) = x^2 - x/2 + 23/48 = (x-\alpha)(x-\bar{\alpha}) \quad \text{or}$$
$$g(x) = x^2 + 2x + 53/48 = (x-\beta)(x-\bar{\beta}),$$

then $\mathrm{Supp}(\mathrm{Res}(g, f^n)) \subseteq \{2, 3, 23, 53\}$ for either choice of g.

Hence, to determine the rational points on

$$y^2 = g(x)f^n(x) \quad \text{for all } n \geq 1,$$

it suffices to compute the rational points on

$$D_g^{(d)}(f^n) : du^2 = g(x), \quad dv^2 = f^n(x),$$

where $d = \pm 2^{e_0} \cdot 3^{e_1} \cdot 23^{e_2} \cdot 53^{e_3}$ and $e_i \in \{0, 1\}$ for all $i \geq 0$. However, the equation $dv^2 = f^n(x)$ maps to $dv^2 = f^m(x)$ for all $m < n$, and a strategy for determining $D_g^{(d)}(f^n)(\mathbb{Q})$ is to choose an m for which the Jacobian of $dv^2 = f^m(x)$ has rank zero, or at least satisfies Chabauty's condition.

One can use this to show that

$$A_n : y^2 = g(x)f^n(x) \text{ satisfies } A_n(\mathbb{Q}) = \{\infty^{\pm}\} \text{ for all } n \geq 1. \tag{18}$$

Now that we have studied these curves defined by quadratic iteration in some detail, we use them and the theory of rational points on curves to classify Galois behavior in the dynamical setting.

3. Dynamical Galois groups and curves. In order to probe how the curves C_n and their quadratic twists relate to the Galois theory of f^n, we must first discuss the necessary background. Let $f \in \mathbb{Q}[x]$ be a polynomial of degree d whose iterates are separable. That is, we assume that the polynomials obtained from successive composition of f have distinct roots in an algebraic closure.

We recall some notation. Let $\mathbb{T}_n$ denote the set of roots of $f, f^2, \ldots, f^n$ together with 0, and let $G_n(f)$ be the Galois group of f^n over the rationals. Furthermore, set

$$\mathbb{T}_\infty := \bigsqcup_{n \geq 0} f^{-n}(0) \quad \text{and} \quad G_\infty = \varprojlim G_n(f). \tag{19}$$

Note that $\mathbb{T}_n$ (respectively $\mathbb{T}_\infty$) carries a natural d-ary rooted tree structure: $\alpha, \beta \in \mathbb{T}_n$ share an edge if and only if $f(\alpha) = \beta$. Moreover, as f is a polynomial with rational coefficients, $G_n(f)$ acts via graph automorphisms on $\mathbb{T}_n$. Hence, we have injections $G_n \hookrightarrow \mathrm{Aut}(\mathbb{T}_n)$ and $G_\infty \hookrightarrow \mathrm{Aut}(\mathbb{T}_\infty)$. Such a framework is called the *arboreal representation* associated to f and we can ask about the size of the image $G_\infty \leq \mathrm{Aut}(T_\infty)$. For a nice exposition, see [14].

REMARK 3.1. Note that $\mathrm{Aut}(\mathbb{T}_n)$ is the n-fold iterated wreath product of the symmetric group S_d. We will use this characterization when useful.

In the quadratic case, it has been conjectured that the image of $G_\infty(f)$ is "large" under mild assumptions on f; see [14, Conjecture 3.11] for a more general statement.

CONJECTURE 3.1 (Finite index). Let $f \in \mathbb{Q}[x]$ be a quadratic polynomial. If all iterates of f are irreducible and f is post-critically infinite, then $|\mathrm{Aut}(\mathbb{T}_\infty) : G_\infty(f)|$ is finite.

Here *post-critically infinite* means that the orbit of the unique root of f's derivative, also known as *critical point*, is infinite. This is an analog of Serre's result for the Galois action on the prime-powered torsion points of a non-CM elliptic curve. For a discussion of this analogy, see [2].

The hypotheses of Conjecture 3.1 are easily satisfied in the case when $f(x) = x^2 + c$ and c is an integer: If $c \neq -2$ and $-c$ is not a square, then f^n is irreducible for all n, and the set $\{f(0), f^2(0), \dots\}$ is infinite. Stoll [24] has given congruence relations on c which ensure that the Galois groups of iterates of $f(x) = x^2 + c$ are maximal (i.e. $G_n(f) \cong \mathrm{Aut}(\mathbb{T}_n)$ for all n). However, much is unknown as to the behavior of integer values not satisfying Stoll's congruences, not to mention the more general setting of rational c (for instance $c = 3$ and $2/3$).

In order to attack the finite index conjecture for more general values of c, we use the following fundamental lemma (due to Stoll), which gives a criterion for the maximality of the Galois groups of iterates in terms of rational points; see [24, Corollary 1.3] for the case when $f = x^2 + c$ and c is an integer, or [15, Lemma 3.2] for the result concerning all rational quadratic polynomials:

LEMMA 3.1. *Let $f \in \mathbb{Q}[x]$ be a quadratic polynomial, let $\gamma \in \mathbb{Q}$ be such that $f'(\gamma) = 0$, and let K_m be a splitting field for f^m. If $f, f^2, \dots, f^n$ are all irreducible polynomials, then the subextension K_n/K_{n-1} is not maximal if and only if $f^n(\gamma)$ is a square in K_{n-1}.*

REMARK 3.2. Let $f(x) = x^2 + c$. Note that with the hypotheses of Lemma 3.1, K_n/K_{n-1} is not maximal if and only in $(0, y) \in C_n(K_{n-1})$ for some $y \in K_{n-1}$. Furthermore, $|\mathbb{Q}(y) : \mathbb{Q}| = 2$ as $f \in \mathbb{Q}[x]$.

As promised, we use quadratic twists of C_n and the Hall–Lang conjecture on integral points of elliptic curves to prove the finite index Conjecture 3.1 in this case when c is an integer. Before we restate and prove Theorem 1.2, we remind the reader of the aforementioned conjectures.

CONJECTURE 3.2 (Hall). For all $\epsilon > 0$ there is a constant C_ϵ (depending only on ϵ) such that for all nonzero $D \in \mathbb{Z}$ and all $x, y \in \mathbb{Z}$ satisfying $y^2 = x^3 + D$, we have

$$|x| \leq C_\epsilon D^{2+\epsilon}.$$

Conjecture 3.2 is often referred to as the weak form of Hall's conjecture. The original conjecture was made with $\epsilon = 0$, and though not yet disproven, is no longer believed to be true. Lang would later generalize Hall's conjecture to the following.

CONJECTURE 3.3 (Hall–Lang). There are absolute constants C and κ such that for every elliptic curve $E/\mathbb{Q}$ given by a Weierstrass equation

$$y^2 = x^3 + Ax + B \quad \text{with } A, B \in \mathbb{Z}$$

and for every integral point $P \in E(\mathbb{Q})$ we have

$$|x(P)| \leq C \max\{|A|, |B|\}^{\kappa}.$$

See [22, 9.7] for a discussion of these conjectures as well as the relevant background material. Assuming these conjectures, we have the following dynamical corollaries.

THEOREM 1.2. *Let $f(x) = x^2 + c$ for some integer c. If $c \neq -2$ and $-c$ is not a square, then both of the following statements hold:*

(i) *The Hall–Lang conjecture implies that $|\mathrm{Aut}(\mathbb{T}_\infty) : G_\infty(f)|$ is finite.*
(ii) *If the weak form of Hall's conjecture for the Mordell curves holds with $C = 100$ and $\epsilon = 4$, then when $f(x) = x^2 + 3$, we have $|\mathrm{Aut}(\mathbb{T}_\infty) : G_\infty(f)| = 2$.*

Proof. Let $f(x) = x^2 + c$ and suppose that the subextension K_n/K_{n-1} is not maximal. We will show that such an $n \geq 2$ is bounded.

Since c is an integer such that $-c$ is not a square, [24, Corollary 1.3] implies that $f^n(0)$ is not a square, and that $f^1, \ldots, f^n$ are irreducible polynomials. Lemma 3.1 implies that $f^n(0)$ is a square in K_{n-1}. Hence, there is some $y \in \mathbb{Z}$ such that

$$dy^2 = f^n(0) \quad \text{for } \mathbb{Q}(\sqrt{d}) \subset K_{n-1} \text{ and } d \text{ square-free.}$$

Moreover, d is a product of distinct primes p_i dividing $2\prod_{j=1}^{n-1} f^j(0)$. To see this latter fact, we use the formula for the discriminant Δ_m of f^m,

$$\Delta_m = \pm \Delta_{m-1}^2 2^{2^m} f^m(0),$$

given in [15, Lemma 2.6]. It follows that the rational primes that ramify in K_{n-1} must divide $2\prod_{j=1}^{n-1} f^j(0)$. Since the primes which divide d must ramify in K_{n-1}, we obtain the desired description of the p_i. Also note that if $p_i \,|\, f^j(0)$ and $p_i \,|\, f^n(0)$ (which is the case since $p_i \,|\, d$), then it divides $f^{n-j}(0)$.

In any case, we may assume that $d = \prod_i p_i$, where the p_i's are distinct primes dividing $2\prod_{j=1}^{\lfloor n/2 \rfloor} f^j(0)$. Here $\lfloor x \rfloor$ denotes the floor function.

A rational point on the curve $C_n^{(d)} : dy^2 = f^n(x)$ maps to $B_1^{(d)} : dy^2 = (x - c)f(x)$ via $(x, y) \mapsto (f^{n-1}(x), yf^{n-2}(x))$. Transforming $B_1^{(d)}$ into stan-

dard form, we get

$$E_1^{(d)} : y^2 = x^3 + 598752(c^2 - 3c)d^2x + 161243136(c^3 - 18c^2)d^3,$$

via $(x, y) \mapsto (d(x - 12c), 2d^2y)$. In particular, if K_n/K_{n-1} is not maximal, then we obtain an integer point

$$\big(d(f^{n-1}(0) - 12c), 2yd^2f^{n-2}(0)\big) \in E_1^{(d)}(\mathbb{Q}). \tag{20}$$

If we assume the Hall–Lang conjecture on integral points of elliptic curves, then there exist constants C and κ such that

$$d(f^{n-1}(0) - 12c) < C \max\{|598752(c^2 - 3c)d^2|, |161243136(c^3 - 18c^2)d^3|\}^\kappa.$$

See [22] or [5] for the relevant background on elliptic curves. In either case

$$|f^{n-1}(0)| < C'|d|^{\kappa'} \le C'|f(0)f^2(0)\cdots f^{\lfloor n/2\rfloor}(0)|^{\kappa'} \tag{21}$$

for some new constants C' and κ'. However, this implies that n is bounded.

For example, if $c > 0$, then $f^m(0) > f(0)f^2(0)\cdots f^{m-1}(0)$ for all m. Hence, if we let $t = \lfloor n/2\rfloor + 1$ and suppose $\kappa' < 2^s$, then

$$f^{n-1}(0) < C'(f^t(0))^{\kappa'} < C'f^{t+s}(0). \tag{22}$$

Since 0 is not preperiodic, the result follows. A similar argument works in the case when $c \le -3$: we simply use the fact that $|f^m(0)| \ge (f^{m-1}(0) - 1)^2$ (see [24, Corollary 1.3]).

Explicitly, when $c = 3$ the j invariant of $B_1^{(d)}$ is zero, and we may transform $B_1^{(d)}$ into the Mordell curve $M^{(-2d)^3} := y^2 = x^3 - (2d)^3$. In particular, a point $(0, y) \in C_n^{(d)}(\mathbb{Q})$ yields a point

$$\big((f^{n-1}(0) - 1)d, d^2yf^{n-2}(0)\big) \in M^{(-2d)^3}(\mathbb{Q}).$$

If the weak form of Hall's conjecture for the Mordell curves holds with $\epsilon = 4$ and $C(\epsilon) = 100$, then for $f(x) = x^2 + 3$ we have

$$|(f^{n-1}(0) - 1)d| < 100|(-2d)^3|^6.$$

This implies that

$$f^{n-1}(0) < 26214400d^{17} + 1 \le 26214400(f^{\lfloor n/2\rfloor+1}(0))^{17} + 1. \tag{23}$$

However, such a bound implies that $n \le 13$. Moreover, one checks that the only $n \le 13$ with $dy^2 = f^n(0)$ and d equal to a product of distinct primes dividing $2\prod_{j=1}^{n-1} f^j(0)$ is $n = 3$. In this case, $f^3(0) = 7^2 \cdot 3 = 7^2 f(0)$ and $|\mathrm{Aut}(\mathbb{T}_3) : G_3(f)| = 2$. It follows that the index of the entire family, $|\mathrm{Aut}(\mathbb{T}_\infty) : G_\infty(f)|$, must also equal 2. ∎

REMARK 3.3. For $\epsilon = 4$, our constant $C = 100$ safely fits the data pitting the known integer points on the Mordell curves against the size of their defining coefficients (see [9]). In fact, even for Elkies' large examples [8], our

choice of C works (thus far) for the strong form of Hall's conjecture ($\epsilon = 0$), though our proof will also work if one insists on a much larger constant.

We now take a different approach to studying these dynamical Galois groups. In Theorem 1.2, we used the curves coming from $f_c(x) = x^2 + c$ to analyze the Galois theory of f's iterates (viewing $c \in \mathbb{Q}$ as fixed), investigating the stability as n grows. We now change our perspective slightly. Suppose that we fix a stage n, and ask for which rational values of c the Galois group of f_c^n is smaller than $\mathrm{Aut}(\mathbb{T}_n)$. Of course this question needs to be refined, as there will be many trivial values of c (for instance if $-c$ is a square). A natural adjustment then is to ask for which rational numbers, $G_n(f_c)$ is smaller than expected for the first time at stage n. As noted in Theorem 1.2, an interesting example is $c = 3$ and $n = 3$:

$$\mathrm{Gal}((x^2+3)^2+3) \cong D_4 \cong \mathrm{Aut}(\mathbb{T}_2), \tag{24}$$

yet one computes that $|\mathrm{Gal}(((x^2+3)^2+3)^2+3)| = 64 < 2^{2^3-1}$, and hence the third iterate of $f = x^2 + 3$ is the first of f's iterates to have a Galois group which is not maximal. This leads to the following definition:

Definition 3.1. Let c be a rational number and let $n \geq 2$. If $f_c = x^2 + c$ is a quadratic polynomial such that

$$G_{n-1}(f_c) \cong \mathrm{Aut}(\mathbb{T}_{n-1}) \quad \text{and} \quad G_n(f_c) \ncong \mathrm{Aut}(\mathbb{T}_n),$$

then we say that f_c has a *newly small* nth *iterate*. Furthermore, let

$$S^{(n)} := \{c \in \mathbb{Q} \mid f_c \text{ has a newly small } n\text{th iterate}\}$$

be the set of rational values of c supplying a polynomial with a newly small nth iterate.

Our refined question then becomes to describe $S^{(n)}$. In the case when $n = 3$, we completely characterized $S^{(3)}$ in terms of the x-coordinates of two rank-one elliptic curves (see [11, Theorem 3.1]). In particular, using bounds on linear forms in elliptic logarithms, we concluded that $S^{(3)} \cap \mathbb{Z} = \{3\}$ (see [11, Corollary 3.1]). Hence, $x^2 + 3$ is the only integer polynomial in the family $x^2 + c$ with this particular Galois degeneracy.

Furthermore, in [11] we use this characterization to compute many new examples of polynomials with newly small third iterate by adding together the points corresponding to known examples on the elliptic curve: e.g. $f(x) = x^2 - 2/3$, $x^2 + 6/19$, $x^2 - 17/14$. Moreover, since generators of both curves are easily computed and since the complement of $S^{(3)}$ and the points on the curves are explicit [11, Theorem 3.1], we have in some sense found all examples.

It is natural to ask what happens for larger n. As an illustration, consider the case when $n = 4$ and $c = -6/7$. One computes with Sage [23] that

$$\big|\mathrm{Gal}\big(((x^2 - 6/7)^2 - 6/7)^2 - 6/7\big)\big| = 2^{2^3-1},$$
$$\big|\mathrm{Gal}\big(\big(((x^2 - 6/7)^2 - 6/7)^2 - 6/7\big)^2 - 6/7\big)\big| = 8192.$$

Since $8192 < 2^{2^4-1}$, we see that $-6/7 \in S^{(4)}$. Are there any other examples? Although not entirely satisfactory, we have the following theorem which we restate from the Introduction:

THEOREM 1.1. *Let $f_c(x) = x^2 + c$ for some $c \in \mathbb{Q}$. Then all of the following statements hold:*

(i) *$S^{(4)} \cap \mathbb{Z} = \emptyset$. That is, if c is an integer and $G_3(f_c) \cong \mathrm{Aut}(\mathbb{T}_3)$, then $G_4(f_c) \cong \mathrm{Aut}(\mathbb{T}_4)$.*
(ii) *If $c \neq 3$ is an integer and $G_2(f_c) \cong \mathrm{Aut}(\mathbb{T}_2)$, then $G_4(f_c) \cong \mathrm{Aut}(\mathbb{T}_4)$.*
(iii) *If the curve $F_2 : y^2 = x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1$ has no rational points of Weil height greater than 10^{100}, then $S^{(4)} = \{2/3, -6/7\}$.*

Proof. As in [11], we associate values in $S^{(n)}$ with the rational points on certain curves. To continue, we need the following lemma:

LEMMA 3.2. *Let $f_c(x) = f(x) = x^2 + c$ and let K_m be the splitting field of f^m over $\mathbb{Q}$. If $c \in S^{(4)}$, then f^4 is irreducible and*

$$\mathbb{Q}(\sqrt{-c}), \quad \mathbb{Q}(\sqrt{f^2(0)}), \quad \mathbb{Q}\left(\sqrt{-\frac{f^2(0)}{c}}\right), \quad \mathbb{Q}(\sqrt{f^3(0)}),$$
$$\mathbb{Q}\left(\sqrt{-\frac{f^3(0)}{c}}\right), \quad \mathbb{Q}\left(\sqrt{\frac{f^3(0)}{f^2(0)}}\right), \quad \mathbb{Q}\left(\sqrt{-\frac{f^3(0)}{c+1}}\right)$$

are the distinct quadratic subfields of K_3.

Proof. First note that if $\mathrm{Gal}(f^m) \cong \mathrm{Aut}(\mathbb{T}_m)$, then K_m contains exactly $2^m - 1$ quadratic subfields. The reason is that the number of quadratic subfields is the number of subgroups of $\mathrm{Gal}(K_m)$ whose quotient is $\mathbb{Z}/2\mathbb{Z}$. Now $\mathrm{Aut}(\mathbb{T}_m)$ is the m-fold wreath product of $\mathbb{Z}/2\mathbb{Z}$, and one can show that the maximal abelian quotient of exponent 2 of this group is $(\mathbb{Z}/2\mathbb{Z})^m$ (see [24]). This quotient group, by its maximality property, will contain as a subgroup any quotient that is abelian of exponent 2, and hence the quotients that are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ are in one-to-one correspondence with the subgroups of $(\mathbb{Z}/2\mathbb{Z})^m$ of order 2. However, that is the same as the number of distinct elements of order 2, which is $2^m - 1$.

Now for the proof of Lemma 3.2: Suppose that $c \in S^{(4)}$. Then $\mathrm{Gal}(f^j) \cong \mathrm{Aut}(\mathbb{T}_j)$ for all $1 \leq j \leq 3$, and the subextensions K_3/K_2, K_2/K_1, and

$K_1/\mathbb{Q}$ are all maximal. In particular $-f(0) = -c$ is not a rational square and $K_1 = \mathbb{Q}(\sqrt{-c})$. Since $\mathrm{Aut}(\mathbb{T}_2)$ acts transitively on the roots of f^2, it follows that f^2 is irreducible. Then Lemma 3.1 implies that $f^2(0) \notin (K_1)^2$. In particular, the distinct quadratic subfields of K_2 are

$$\mathbb{Q}(\sqrt{-c}), \quad \mathbb{Q}(\sqrt{f^2(0)}), \quad \mathbb{Q}\left(\sqrt{\frac{f^2(0)}{-c}}\right). \tag{25}$$

Note that when $m \geq 2$, then the discriminant formula (11) implies that $\sqrt{f^m(0)} \in K_m$. By the opening remarks in this proof, there must be exactly $2^2 - 1 = 3$ such subfields. Hence our list is exhaustive for K_2.

One simply repeats this argument for the third iterate, obtaining the claimed list of quadratic subfields of K_3. In particular the set $\{-f(0), f^2(0), f^3(0)\}$ does not contain a rational square. It suffices to show that $f^4(0)$ is not a rational square either to deduce that f^4 is irreducible (see [15]). However, a 2-descent on the curve

$$F_0 : y^2 = f_c^4(0) = ((c^2 + c)^2 + c)^2 + c$$

shows that its Jacobian has rank zero. After reducing modulo several primes of good reduction, one finds that any torsion must be 2-torsion. Hence $F_0(\mathbb{Q}) = \{\infty^{\pm}, (0,0), (-1,0)\}$, and $c \in S^{(4)}$ implies that $c \neq 0, -1$. ∎

With Lemma 3.2 in place, we are ready to relate the elements of $S^{(4)}$ with the rational points on certain curves. If $c \in S^{(4)}$ then f_c^4 is irreducible and $f_c^4(0)$ is not a rational square (see the proof of the lemma). However, since the extension K_4/K_3 is not maximal by assumption, Lemma 3.1 implies that $\sqrt{f_c^4(0)} \in K_3$. Hence $\sqrt{f_c^4(0)}$ must live in one of the seven quadratic subfields of K_3 listed in Lemma 3.2. Thus, there must exist $y \in \mathbb{Q}$ such that (c, y) is a rational point on one of the following curves:

$$\begin{aligned}
F_1 : y^2 &= \frac{f_x^4(0)}{-x} = -(x^7 + 4x^6 + 6x^5 + 6x^4 + 5x^3 + 2x^2 + x + 1),\\
F_2 : y^2 &= \frac{f_x^4(0)}{f_x^2(0)} = x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1,\\
F_3 : y^2 &= \frac{f_x^4(0)}{-(x+1)} = -x(x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1),\\
F_4 : y^2 &= \frac{f_x^4(0)}{x} \cdot \frac{f_x^3(0)}{x}\\
&= (x^7 + 4x^6 + 6x^5 + 6x^4 + 5x^3 + 2x^2 + x + 1)(x^3 + 2x^2 + x + 1),\\
F_5 : y^2 &= f_x^4(0)\frac{f_x^3(0)}{-x}\\
&= (x^8 + 4x^7 + 6x^6 + 6x^5 + 5x^4 + 2x^3 + x^2 + x) \cdot -(x^3 + 2x^2 + x + 1),
\end{aligned}$$

$$\begin{aligned} F_6 : y^2 &= \frac{f_x^4(0)}{f_x^2(0)} f_x^3(0) \\ &= (x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1)(x^4 + 2x^3 + x^2 + x), \\ F_7 : y^2 &= \frac{f_x^4(0)}{-(f_x^2(0))} \cdot \frac{f_x^3(0)}{x} \\ &= -(x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1)(x^3 + 2x^2 + x + 1) \end{aligned}$$

(after dividing out the finite singularities coming from $c = 0, -1$ when necessary).

Note that all of these curves are hyperelliptic, and so at least in principle, their arithmetic (ranks, integer points etc.) is more easily computable. Also note that the interesting rational points corresponding to known elements of $S^{(4)}$ both come from $F_2(\mathbb{Q})$:

$$\{\infty^+, \infty^-, (0, \pm 1), (2/3, \pm 53/27), (-6/7, \pm 377/343)\} \subseteq F_2(\mathbb{Q}). \tag{26}$$

Therefore, to describe $S^{(4)}$ it suffices to characterize $F_i(\mathbb{Q})$ for all $1 \leq i \leq 7$. We will do this sequentially, employing standard methods in the theory of rational points on curves. For a nice overview of these techniques, see [25].

Case 1. A 2-descent with Magma [1] shows that the rational points on the Jacobian of F_1 have rank one. Moreover, reducing modulo various primes of good reduction, one sees that the order of any rational torsion point must divide 4. However, the only 2-torsion point is $Q = [(-1, 0) - \infty]$, and by examining the image of Q via the 2-descent map, one sees that Q is not a double in $J(F_1)(\mathbb{Q})$. It follows that $J(F_1)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$. Since F_1 has genus three, we can apply the method of Chabauty and Coleman to bound the rational points (in fact, find them all).

To do this we change variables to obtain an equation which is more amenable to the computations to come: send $(x, y) \mapsto (-x - 2, y)$ to map to the curve

$$F_1' : y^2 = x^7 + 10x^6 + 42x^5 + 94x^4 + 117x^3 + 76x^2 + 21x + 1.$$

A naive point search yields $\{\infty, (-1, 0), (0, \pm 1)\} \subseteq F_1'(\mathbb{Q})$, and we will show that this set is exhaustive.

Let $J = J(F_1')$ and use the point $P_0 = (0, 1)$ to define an embedding of $F_1'(\mathbb{Q}) \subseteq J(\mathbb{Q}) \subseteq J(\mathbb{Q}_3)$ via $P \mapsto [P - P_0]$. Then given a 1-form ω on $J(\mathbb{Q}_3)$, one can integrate to form the function

$$J(\mathbb{Q}_3) \to \mathbb{Q}_3 \quad \text{given by} \quad P \mapsto \int_0^P \omega.$$

Coleman's idea was to notice that if we restrict this function to a residue class of $F_1'(\mathbb{Q}_3) \subset J(\mathbb{Q}_3)$, then this function can be computed explicitly in terms of power series (using a parametrization coming from a uniformizer

for the class). Moreover, when the genus is larger than the rank of the group $J(\mathbb{Q})$, as is the case in our example, one can find an ω where the above function vanishes on $J(\mathbb{Q})$. Finally, using Newton polygons, one can bound the number of rational points in each residue class by bounding the number of zeros of a power series in $\mathbb{Z}_3$. This is what we will do. For a nice exposition of this method, see [18].

We will follow the notation and outline of Example 1 in Section 9 of Wetherell's thesis [26]. In particular, we use x as a local coordinate system on the residue class at $(0,1)$ and the basis $\eta_0 = (1/y)dx$, $\eta_1 = (x/y)dx$, and $\eta_2 = (x^2/y)dx$ for the global forms on F_1'. Expanding $1/y$ in a power series in terms of x we get

$$\begin{aligned}\eta_0 &= \tfrac{dx}{y}\\ &= 1 - \tfrac{21}{2}x + \tfrac{1019}{8}x^2 - \tfrac{28089}{16}x^3 + \tfrac{3292019}{128}x^4 - \tfrac{99637707}{256}x^5 + \tfrac{6153979535}{1024}x^6 - \cdots.\end{aligned}$$

Furthermore, it is known that the η_i are in $\mathbb{Z}_3[[x]]$. Then we have the integrals λ_i for the η_i in the residue class of $(0,1)$, that is,

$$\lambda_i(P) = \int_{(0,1)}^{P} \eta_i.$$

From our formulas for the η_i, we have

$$\lambda_0 = x - \tfrac{21}{4}x^2 + \tfrac{1019}{24}x^3 - \tfrac{28089}{64}x^4 + \tfrac{3292019}{640}x^5 - \tfrac{33212569}{512}x^6 + \tfrac{6153979535}{7168}x^7 - \cdots,$$

$$\lambda_1 = \tfrac{1}{2}x^2 - \tfrac{7}{2}x^3 + \tfrac{1019}{32}x^4 - \tfrac{28089}{80}x^5 + \tfrac{3292019}{768}x^6 - \tfrac{99637707}{1792}x^7 + \tfrac{6153979535}{8192}x^8 - \cdots,$$

$$\lambda_2 = \tfrac{1}{3}x^3 - \tfrac{21}{8}x^4 + \tfrac{1019}{40}x^5 - \tfrac{9363}{32}x^6 + \tfrac{3292019}{896}x^7 - \tfrac{99637707}{2048}x^8 + \tfrac{6153979535}{9216}x^9 + \cdots.$$

Let ω_i be the differentials on J corresponding to the η_i on F_1', i.e. the pullbacks relative to the inclusion $F_1'(\mathbb{Q}_3) \subseteq J(\mathbb{Q}_3)$ given by $P \mapsto [P - (0,1)]$. Finally, let λ_i' be the homomorphism from $J(\mathbb{Q}_3)$ to $\mathbb{Q}_3$ obtained by integrating the ω_i. We will calculate the λ_i' on $J_1(\mathbb{Q}_3)$, the kernel of the reduction map.

Let $a \in J_1(\mathbb{Q}_3)$, so that a may be represented as $a = [P_1 + P_2 + P_3 - 3P_0]$ with $P_i \in C(\bar{\mathbb{Q}}_3)$ and $\overline{P_i} = \overline{P_0} = (0,1)$. If $s_j = \sum_{i=1}^{3} x(P_i)^j$, then from the expression

$$\int_0^a \omega_i = \sum_j \int_{(0,1)}^{P_j} \eta_i$$

we see that

$$\lambda_0 = s_1 - \tfrac{21}{4}s_2 + \tfrac{1019}{24}s_3 - \tfrac{28089}{64}s_4 + \tfrac{3292019}{640}s_5 - \tfrac{33212569}{512}s_6 + \tfrac{6153979535}{7168}s_7 - \cdots,$$

$$\lambda_1 = \tfrac{1}{2}s_2 - \tfrac{7}{2}s_3 + \tfrac{1019}{32}s_4 - \tfrac{28089}{80}s_5 + \tfrac{3292019}{768}s_6 - \tfrac{99637707}{1792}s_7 + \tfrac{6153979535}{8192}s_8 - \cdots,$$

$$\lambda_2 = \tfrac{1}{3}s_3 - \tfrac{21}{8}s_4 + \tfrac{1019}{40}s_5 - \tfrac{9363}{32}s_6 + \tfrac{3292019}{896}s_7 - \tfrac{99637707}{2048}s_8 + \tfrac{6153979535}{9216}s_9 - \cdots.$$

We wish to find an ω whose integral kills $J(\mathbb{Q})$. However, since $\log(J(\mathbb{Q}))$ has rank one in $T_0(J(\mathbb{Q}_3))$, the dimension of such differentials is 2, and so we have some freedom with our choice. We will exploit this freedom to bound the number of points in each residue field.

Note that if $U = [\infty - P_0]$, then $12U$ is in $J_1(\mathbb{Q}_3)$. Furthermore, a 1-form kills $J(\mathbb{Q})$ if and only if it kills $12U$, since the index of the subgroup generated by the rational torsion and U is coprime to $|J(\mathbb{F}_3)| = 24$. Using Magma, we calculate the divisor $12U$ represented as $[P_1 + P_2 + P_3 - 3P_0]$, where the three symmetric functions in the $x(P_i)$ are

$$\sigma_1 = \frac{5688167583876464940561144764011383197382945288}{55289396017060746454134095281856012324660431 21} \equiv 2 \cdot 3^4 \bmod 3^5,$$

$$\sigma_2 = \frac{-2183647192786560140353830791558556354713308560}{55289396017060746454134095281856012324660431 21} \equiv 2^2 \cdot 3^3 \bmod 3^5,$$

$$\sigma_3 = \frac{4352156372570507181684433225178910249832181376}{55289396017060746454134095281856012324660431 21} \equiv 2^3 \cdot 3^3 \bmod 3^5.$$

Choosing a precision of 3^5 was arbitrary, though sufficient for our purposes. Note that the valuation of every $x(P_i)$ is at least $\min\{v(\sigma_i)/i\} = \min\{4, 3/2, 1\} = 1$. It follows that $v(s_j) \geq j$. Moreover, one verifies that every term past $j = 3$ of $\lambda_i(12U)$ is congruent to 0 mod 3^5.

After calculating the s_j in terms of the σ_i, one finds that

$$\lambda_0(12U) \equiv 2 \cdot 3^3 \bmod 3^5,$$
$$\lambda_1(12U) \equiv 3^3 \bmod 3^5,$$
$$\lambda_2(12U) \equiv 2^3 \cdot 3^3 \bmod 3^5.$$

As the integral is linear in the integrand, there exist global 1-forms α and β such that

$$\int_0^P \alpha = 0 \quad \text{and} \quad \int_0^P \beta = 0 \quad \text{for all } P \in J(\mathbb{Q}),$$

with $\alpha \equiv 2\lambda_1 - \lambda_0 \bmod 3^5$ and $\beta \equiv 2\lambda_2 - 4\lambda_0 \bmod 3^5$. Moreover, $\alpha = (x-1)dx/y$ and $\beta = (x^2-1)dx/y$ when we view them over $\mathbb{F}_3$. However, for every $P \in F_1'(\mathbb{F}_3)$, either α or β does not vanish at P: see the table below.

$P \in F_1'(\mathbb{F}_p)$	$\mathrm{ord}_P(\alpha)$	$\mathrm{ord}_P(\beta)$
$\overline{\infty}$	2	0
$\overline{(0,1)}$	0	0
$\overline{(0,-1)}$	0	0
$\overline{(-1,0)}$	0	1

It follows that every residue class in $F_1'(\mathbb{Q}_3)$ contains at most one rational point, and hence exactly one rational point as claimed.

Case 2. We first use Runge's method to find $F_2(\mathbb{Z})$. This involves completing the square. Suppose we have an integer solution x. We rewrite our

equation as

$$y^2 - \left(x^3 + \tfrac{3}{2}x^2 + \tfrac{3}{8}x + \tfrac{15}{16}\right)^2 = -\tfrac{61}{64}x^2 - \tfrac{45}{64}x + \tfrac{31}{256},$$

and then multiply by 256 to clear denominators. Write

$$g = 16x^3 + 24x^2 + 6x + 15, \quad h = -244x^2 - 180x + 31, \quad Y = 16y.$$

Then $(Y-g)(Y+g) = h$, and (unless one of the factors is zero) $|Y-g| \le |h|$ and $|Y+g| \le |h|$. Note that neither factor can be zero since h has no integer roots. After combining our inequalities, we see that

$$|2g| = |(Y+g) - (Y-g)| \le 2|h|. \tag{27}$$

Hence $|g| \le |h|$. As the degree of g is larger than h, we get a small bound on x. A naive point search shows that $F_2(\mathbb{Z}) = \{\infty^{\pm}, (-1, \pm 1), (0, \pm 1), (-2, \pm 1)\}$.

As for the full rational points, this is (at the moment) beyond reach; for an explanation, see Remark 3.4 at the end of this section. At best, we can be sure that the unknown rational points must be of very large height (on the order of 10^{100}) by running the Mordell–Weil sieve. Since our curve is of genus 2, we can use explicit bounds between the Weil and canonical heights to compute a basis of $J(F_2)(\mathbb{Q})$. It follows that $J(F_2)(\mathbb{Q})$ has basis

$$\begin{aligned} P_1 &= [(0,-1) + (-1,-1) - \infty^- - \infty^+], \\ P_2 &= [(0,-1) + (0,-1) - \infty^- - \infty^+], \\ P_3 &= [(0,1) + (-2,1) - \infty^- - \infty^+], \end{aligned}$$

which we use while sieving with Magma (see [3] for a full discussion of the Mordell–Weil sieve, or [25] for a basic introduction). On the other hand, a point search with Magma can be used to list all points of height at most 10^7 with little work.

Case 3. For F_3 and subsequent curves, we use unramified covers to determine the rational points. Note that $\mathrm{Res}(x^6+3x^5+3x^4+3x^3+2x^2+1, -x) = 1$, and we study the curves

$$D^{(d)} : du^2 = x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1, \quad dv^2 = -x, \quad d \in \{\pm 1\},$$

which are $\mathbb{Z}/2\mathbb{Z}$-covers of F_3. Moreover, every rational point on F_3 lifts to one on some $D^{(d)}$ (see [25, Example 9]). If $d = -1$, then the curve $du^2 = x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 1$ has no rational points, since it has no points in $\mathbb{F}_3$. Hence $D^{(-1)}$ has no rational points. On the other hand, if $d = 1$, then our description of $F_2(\mathbb{Z})$ shows that $F_3(\mathbb{Z}) = \{\infty, (-1, \pm 1), (0,0)\}$. Moreover, if we assume that there are no unknown points in $F_2(\mathbb{Q})$, then we have found all of the rational points on F_3. In any case $0, -1 \notin S^{(4)}$. Hence, F_3 contributes no integers to $S^{(4)}$.

CASE 4. Similarly for F_4 we have the covers

$$D^{(d)} : du^2 = (x+1)(x^3+2x^2+x+1),$$
$$dv^2 = x^6+3x^5+3x^4+3x^3+2x^2+1, \quad d \in \{\pm 1\}.$$

Again, if $d=-1$, then one sees that there are no rational points on $D^{(d)}$ by looking in $\mathbb{F}_3$. When $d=1$, the second defining equation of D is that of F_2, and so we use our description of $F_2(\mathbb{Z})$ to show that $F_4(\mathbb{Z}) = \{\infty^{\pm}, (-1,0), (0,\pm 1), (-2,\pm 1)\}$. Under the assumption that there are no unknown rational points on F_2, we can conclude that $F_4(\mathbb{Z}) = F_4(\mathbb{Q})$. In any event $0, -1, -2$ are not in $S^{(4)}$, and so F_4 also contributes nothing to $S^{(4)}$.

CASE 5. The Jacobian of F_5 has rank zero, and we easily determine that $F_5(\mathbb{Q}) = \{\infty^{\pm}, (0,0)\}$. Since $0 \notin S^{(4)}$, we conclude that F_5 contributes no integers to $S^{(4)}$.

CASE 6. Since $\mathrm{Res}(x^6+3x^5+3x^4+3x^3+2x^2+1, x^4+2x^3+x^2+x) = -1$, the rational points on F_6 are covered by the points on

$$D^{(d)} : du^2 = x^6+3x^5+3x^4+3x^3+2x^2+1,$$
$$dv^2 = x^4+2x^3+x^2+x, \quad d \in \{\pm 1\}.$$

If $d=1$, then the equation $u^2 = x^4+2x^3+x^2+x$ represents an elliptic curve of rank zero having rational points $\{\infty^{\pm}, (0,0)\}$. It follows that $D^{(1)}(\mathbb{Q})$ has only the points at infinity and those corresponding to $x=0$. If $d=-1$, then $D^{(-1)}$ has no points over $\mathbb{F}_3$. We conclude that $F_6(\mathbb{Q}) = \{\infty^{\pm}, (0,0)\}$ unconditionally, and nothing new is added to $S^{(4)}$ in this case.

CASE 7. The rational points on the final curve F_7 are covered by the points on

$$D^{(d)} : du^2 = x^6+3x^5+3x^4+3x^3+2x^2+1,$$
$$dv^2 = -(x^3+2x^2+x+1), \quad d \in \{\pm 1\}.$$

As in previous cases, if $d=-1$, then $D^{(-1)}$ has no points over $\mathbb{F}_3$. On the other hand, when $d=1$ we use our description of $F_2(\mathbb{Z})$ and $F_2(\mathbb{Q})$ do determine that $F_7(\mathbb{Z}) = \{\infty, (-2,\pm 1)\}$. As before, if there are no unknown rational points on F_2, then we will have given a complete list of points on F_7. Note that $-2 \notin S^{(4)}$ and so, in combination with the previous cases, we have shown that $S^{(4)} \cap \mathbb{Z} = \emptyset$.

Finally, if $c \neq 3$ is an integer such that $G_2(f_c) \cong \mathrm{Aut}(T_2)$, then $G_3(f_c) \cong \mathrm{Aut}(T_3)$ by [11, Corollary 3.1]. However, since $S^{(4)} \cap \mathbb{Z} = \emptyset$, we deduce that also $G_4(f_c) \cong \mathrm{Aut}(T_4)$.

This finishes the proof of Theorem 1.1. ∎

REMARK 3.4. At the moment, proving that we have determined $F_2(\mathbb{Q})$ is far beyond reach. For one, the Galois group of $x^6+3x^5+3x^4+3x^3+$

$2x^2 + 1$ is S_6, from which it follows that $\mathrm{End}(J(F_2)) \cong \mathbb{Z}$; see [27]. In particular, F_2 does not map to any lower genus (elliptic) curves. Moreover, the rank of $J(F_2)(\mathbb{Q})$ is 3, and so the method of Chabauty and Coleman is not applicable. Furthermore, in order to use a covering collection coming from the pullback of the multiplication by 2 map on the Jacobian, one would need to determine generators of the Mordell–Weil group $E(K)$, where E is an elliptic curve defined over a number field K of degree 17, followed by elliptic Chabauty. This is currently not feasible.

A naive point search on the relevant curves suggests that $S^{(5)}$ and $S^{(6)}$ are probably empty. In fact, if $n = 5$, then the 15 curves, corresponding to the $2^4 - 1$ quadratic subfields of K_4, satisfy the Chabauty condition (small rank), and so proving that $S^{(5)}$ is empty may be doable. This begs the question as to whether all n sufficiently large satisfy $S^{(n)} = \emptyset$. Is it true for all $n \geq 5$?

This seems beyond reach at the moment. However, the weaker statement that $S^{(n)} \cap \mathbb{Z} = \emptyset$ may be attackable if one assumes standard conjectures on the height of integer points on hyperelliptic curves relative to the size of the defining coefficients. If true, this would amount to a nice Galois uniformity principle. Namely, outside of the small exception $x^2 + 3$, it seems as though $G_2(f_c) \cong \mathrm{Aut}(\mathbb{T}_2)$ already implies that $G_n(f_c) \cong \mathrm{Aut}(\mathbb{T}_n)$ for all $n \geq 1$ whenever c is an integer.

Acknowledgements. It is a pleasure to thank my advisor, Joe Silverman, as well as Michael Stoll, Rafe Jones, Samir Siksek, Reinier Broker, Daniel Hermes, and Vivian Olsiewski Healey for the many useful discussions while this work was in progress. I also thank the referee for helpful comments.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system 1: The user language*, J. Symbolic Comput. 24 (1997), 235–265 (also see Magma homepage at http://magma.maths.usyd.edu.au/magma/handbook/text/1398).

[2] N. Boston and R. Jones, *The image of an arboreal Galois representation*, Pure Appl. Math. Quart. 5 (2009), 213–225.

[3] N. Bruin and M. Stoll, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. 13 (2010), 272–306.

[4] A. Carocca, H. Lange, and R. Rodriguez, *Jacobians with complex multiplication*, Trans. Amer. Math. Soc. 363 (2011), 6159–6175.

[5] H. Cohen, *Number Theory. Vol. 1: Tools and Diophantine Equations*, Grad. Texts in Math. 239, Springer, 2007.

[6] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2006.

[7] D. Dummit and R. Foote, *Abstract Algebra*, 3rd ed., Wiley, 2004.
[8] N. Elkies, *List of integers x, y with $x < 10^{18}$ and $0 < |x^3 - y^2| < x^{1/2}$*, http://www.math.harvard.edu/~elkies/hall.html.
[9] J. Gebel, A. Pethő, and H. Zimmer, *Computing integral points on Mordell's elliptic curves*, Collect. Math. 48 (1997), 115–136.
[10] C. Gratton, K. Nguyen, and T. Tucker, *ABC implies primitive prime divisors in arithmetic dynamics*, Bull. London Math. Soc. 45 (2013), 1194–1208.
[11] W. Hindes, *Points on elliptic curves parametrizing dynamical Galois groups*, Acta Arith. 159 (2013), 149–167.
[12] N. Hurt, *Many Rational Points: Coding Theory and Algebraic Geometry*, Math. Appl. 564, Kluwer, 2003.
[13] B. Hutz and P. Ingram, *On Poonen's conjecture concerning rational preperiodic points of quadratic maps*. Rocky Mountain J. Math. 43 (2013), 193–204.
[14] R. Jones, *Galois representations from pre-image trees: an arboreal survey*, in: Publ. Math. Besançon Algèbre Théor. Nombres, Presses Univ. Franche-Comté, 2013, 107–136.
[15] R. Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. London Math. Soc. 78 (2008), 523–544.
[16] N. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. 62 (1981), 481–502.
[17] S. Lang, *Abelian Varieties*, Springer, 1983.
[18] W. McCallum and B. Poonen, *The Method of Chabauty and Coleman*, in: Explicit Methods in Number Theory, Panor. Synthèses 36, Soc. Math. France, 2012, 99–117; also available at http://www-math.mit.edu/~poonen/papers/chabauty.pdf.
[19] J. Paulhus, *Decomposing Jacobians of curves with extra automorphisms*, Acta Arith. 132 (2008), 231–244.
[20] B. Poonen, *The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture*, Math. Z. 228 (1998), 11–29.
[21] J. Silverman, *The Arithmetic of Dynamical Systems*, Grad. Texts in Math. 241, Springer, 2007.
[22] J. Silverman, *Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986; 2nd ed., 2009.
[23] W. Stein, *Sage: Open Source Mathematical Software (Version 2.10.2)*, The Sage Group, 2008, http://www.sagemath.org.
[24] M. Stoll, *Galois groups over $\mathbb{Q}$ of some iterated polynomials*, Arch. Math. (Basel) 59 (1992), 239–244.
[25] M. Stoll, *Rational points on curves*, J. Théor. Nombres Bordeaux 23 (2011), 257–277.
[26] J. Wetherell, *Bounding the number of points on certain curves of high rank*, Ph.D. thesis, Univ. of California at Berkeley, 1997.
[27] Yu. G. Zarhin, *Hyperelliptic Jacobians without complex multiplication*, Math. Res. Lett. 7 (2000), 123–132.

Wade Hindes
Department of Mathematics
Brown University
Providence, RI 02912, U.S.A.
E-mail: whindes@math.brown.edu

Received on 19.6.2013
and in revised form on 25.12.2014 (7487)