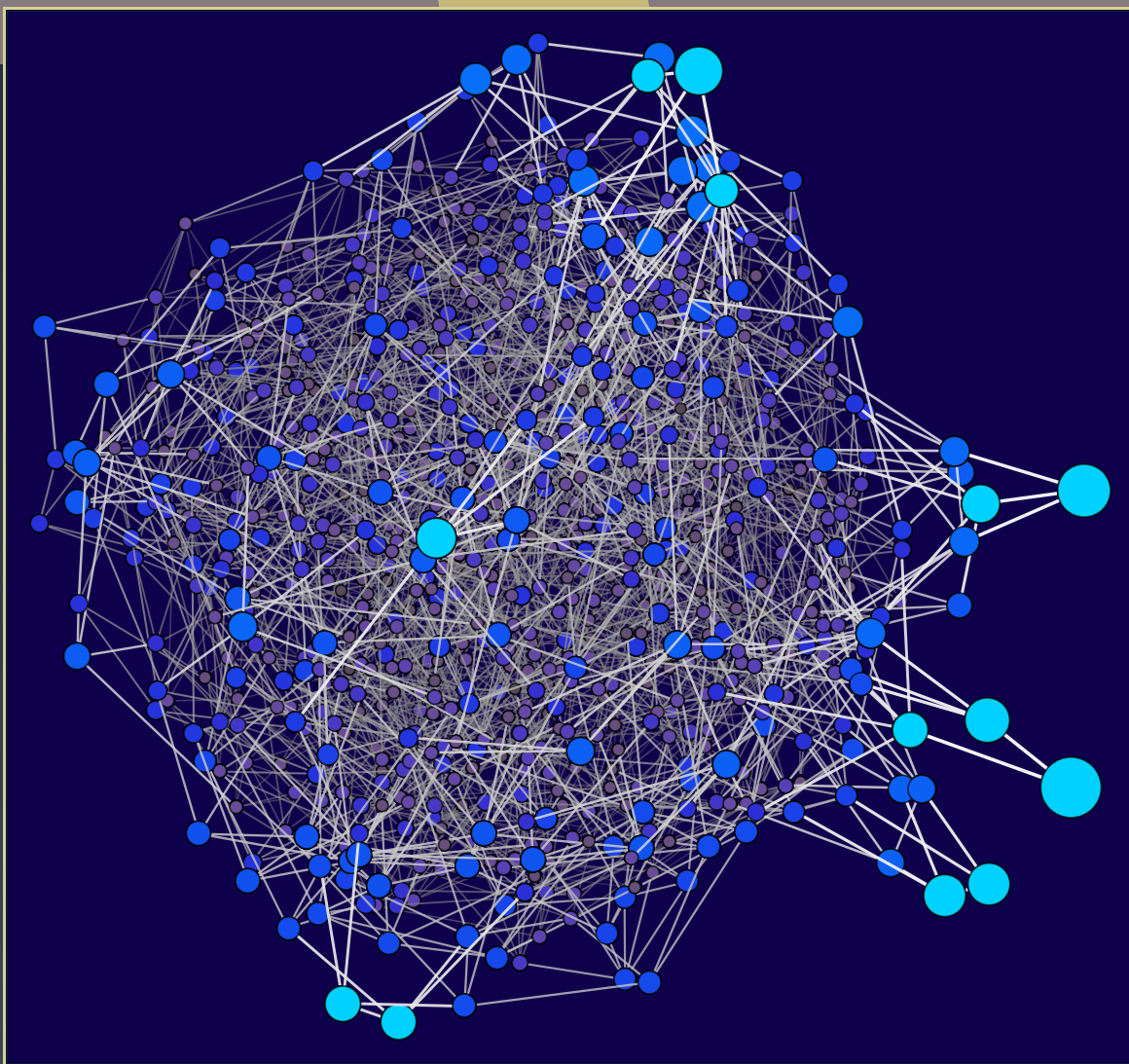# ANTS XIV
Proceedings of the Fourteenth
Algorithmic Number Theory Symposium

Cubic post-critically finite polynomials defined over $\mathbb{Q}$

Jacqueline Anderson, Michelle Manes, and Bella Tobin

msp

msp

Cubic post-critically finite polynomials defined over ℚ

Jacqueline Anderson, Michelle Manes, and Bella Tobin

We find all post-critically finite (PCF) cubic polynomials defined over $\mathbb{Q}$, up to conjugacy over $\mathrm{PGL}_2(\overline{\mathbb{Q}})$. We describe normal forms that classify equivalence classes of cubic polynomials while respecting the field of definition. Applying known bounds on the coefficients of post-critically bounded polynomials to these normal forms simultaneously at all places of $\mathbb{Q}$, we create a finite search space of cubic polynomials over $\mathbb{Q}$ that may be PCF. Using a computer search of these possibly PCF cubic polynomials, we find fifteen which are in fact PCF.

1. Introduction

Let K be a number field, and let $f(z) \in K[z]$ have degree $d \geq 2$. Consider iterates of f:

$$f^n(z) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}(z), \quad \text{and} \quad f^0(z) := z.$$

The orbit of a point $\alpha \in \overline{K}$ is the set $\mathcal{O}_f(\alpha) = \{f^n(\alpha) \mid n \geq 0\}$.

Rather than studying individual polynomials, we consider equivalence classes of polynomials under conjugation by affine elements $\phi \in \mathrm{PGL}_2(\overline{K})$. For $\phi(z) = az + b \in \overline{K}[z]$, we define

$$f^\phi = \phi \circ f \circ \phi^{-1}.$$

Note that f and f^ϕ have the same dynamical behavior over $\overline{K}$ in the sense that ϕ maps the orbit $\mathcal{O}_f(\alpha)$ to $\mathcal{O}_{f^\phi}(\phi(\alpha))$.

Critical points of f are the points $\alpha \in \overline{K}$ such that $f'(\alpha) = 0$. Branner and Hubbard write in [6] "the main question to ask about a rational map is: *what are the orbits under iteration of the critical points?*" Of particular interest are functions for which all critical points have either a bounded or finite orbit.

Definition 1.1. A polynomial f is *postcritically finite* (PCF) if the orbit of each critical point is finite. A polynomial is *postcritically bounded* with respect to a given absolute value if the orbit of each critical point is bounded with respect to that absolute value.

The study of PCF maps has a long history in complex dynamics, from Thurston's work in the early 1980s and continuing to the present day, for example [3; 9; 10; 11; 12; 13]. In [18], Silverman describes PCF maps as an analog of abelian varieties with complex multiplication, so these maps are of particular interest in arithmetic dynamics as well. For example, all quadratic post-critically finite rational maps over $\mathbb{Q}$ have been found in [15], and many cubic post-critically finite polynomials over $\mathbb{Q}$ have been found in [14].

Theorem. *There are exactly fifteen* $\overline{\mathbb{Q}}$ *conjugacy classes of cubic PCF polynomials defined over* $\mathbb{Q}$:

(1) z^3
(2) $-z^3 + 1$
(3) $-2z^3 + 3z^2 + \frac{1}{2}$

(4) $-2z^3 + 3z^2$
(5) $-z^3 + \frac{3}{2}z^2 + 1$
(6) $2z^3 - 3z^2 + 1$

(7) $2z^3 - 3z^2 + \frac{1}{2}$
(8) $z^3 - \frac{3}{2}z^2$
(9) $-3z^3 + \frac{9}{2}z^2$

(10) $-4z^3 + 6z^2 - \frac{1}{2}$
(11) $4z^3 - 6z^2 + \frac{3}{2}$
(12) $3z^3 - \frac{9}{2}z^2 + 1$

(13) $-z^3 + \frac{3}{2}z^2 - 1$
(14) $-\frac{1}{4}z^3 + \frac{3}{2}z + 2$
(15) $-\frac{1}{28}z^3 - \frac{3}{4}z + \frac{7}{2}$

Of these, (1), (4), (6), (8), (10), and (11) were found by Ingram in [14]. To complete the list, we adapt Ingram's techniques as described below.

Let K be a number field, and let $f(z) \in K[z]$ be a cubic polynomial. Critical points of f are roots of the quadratic polynomial $f'(z) \in K[z]$, so there are three possibilities:

(a) There are two distinct critical points: $\gamma_1 \neq \gamma_2$, and they are both K-rational.

(b) There are two distinct critical points $\gamma_1 \neq \gamma_2$ with $K(\gamma_1) = K(\gamma_2)$ a quadratic extension of K.

(c) There is exactly one critical point, $\gamma \in K$.

In the first two cases, we say that f is *bicritical*. In the third case, we say f is *unicritical*. In determining a complete list of cubic PCF polynomials defined over $\mathbb{Q}[z]$, we treat each of these cases separately:

(1) For each of cases (a)–(c) above, find a normal form for cubic polynomials such that every cubic polynomial over $\mathbb{Q}[z]$ is conjugate to a map in one of these forms, and the conjugation respects the field of definition for the given case.

(2) For a map to be PCF, it must be post-critically bounded in each absolute value. Find archimedean and p-adic bounds on the coefficients for maps in the normal forms to be post-critically bounded.

(3) Use the bounds in (2) to create a finite search space of possibly PCF maps.

(4) For each map in the finite search space, test if it is PCF or not.

1A. *Outline.* We begin in Section 2 by treating the special case of a polynomial with a unique critical point. In Section 3, we find the normal forms needed in Step (1) of the algorithm above. Section 4 provides the coefficient bounds described in Step (2). Finally, Section 5 describes the algorithms and provides the complete list of PCF cubic polynomials defined over $\mathbb{Q}$.

2. Unicritical PCF polynomials

We begin by considering unicritical PCF polynomials. First, we will determine a normal form for unicritical polynomials of arbitrary degree defined over a number field K. In [8], Buff studied unicritical polynomials from a complex dynamics point of view, and he used that work to answer questions of Milnor and of Baker and DeMarco. Some of his preliminary work overlaps with the work here, specifically the normal form in Theorem 2.1 and the bound on $|a|$ in Proposition 2.2. Because Buff was working over $\mathbb{C}$, he did not consider questions about field of definition. Therefore, we provide full proofs of these results from a more arithmetic point of view.

Theorem 2.1. *Let $f(z) \in K[z]$ be a degree d unicritical polynomial. Then either $f(z)$ is $\overline{K}$-conjugate to z^d, or f is conjugate to a unique polynomial of the form*

$$az^d + 1 \in K[z].$$

Proof. Without loss of generality, we may replace f by a conjugate map where the unique critical point γ is moved to 0. Since $\gamma \in K$, this does not change the field of definition. So we assume that $f(z) = bz^d + c \in K[z]$.

If $c = 0$, then $f(z) = bz^d$ for $b \in K^\times$. Letting $\phi(z) = b^{1/(d-1)}z$, we have $f^\phi(z) = z^d$.

Now, assume $c \neq 0$. Conjugating by $\phi(z) = z/c$ gives

$$f^\phi(z) = bc^{d-1}z^d + 1.$$

Since $b, c \in K^\times$, then $bc^{d-1} \in K^\times$. Letting $a = bc^{d-1}$ gives the result.

Finally, ϕ is the only affine map in $\mathrm{PGL}_2(\overline{K})$ fixing 0 and satisfying $f^\phi(0) = 1$. Therefore, $f(z)$ is $\overline{K}$-conjugate to $az^d + 1 \in K[z]$ for a unique $a \in K^\times$. $\square$

Theorem 2.1 implies that up to conjugacy every unicritical polynomial $f \in K[z]$ is a power map or of the form $az^d + 1$. In both cases $\mathrm{Crit}(f) = \{0\}$. If f is a power map then $f(0) = 0$, hence f is PCF. Therefore, in order to completely describe all other PCF unicritical polynomials in $\mathbb{Q}[z]$ (of any degree), we need only consider those of the form $f(z) = az^d + 1$ for $a \in \mathbb{Q}^\times$.

Proposition 2.2 [8, Corllary 8]. *If $f(z) = az^d + 1 \in K[z]$ is post-critically finite, then $|a| \leq 2$.*

Proof. Suppose $|a| > 2$ and $|\alpha| \geq 1$. Then

$$|f(\alpha)| = |a\alpha^d + 1| > |\alpha|.$$

Inductively, α must be a wandering point. Since $\mathrm{Crit}(f) = \{0\}$ and $f(0) = 1$, we see that f is not PCF. Therefore, if $f \in K[z]$ is PCF it must be that $|a| \leq 2$. $\square$

Theorem 2.3. *Let $f(z) = az^d + 1 \in \mathbb{Q}[z]$ and $d \geq 2$. For d even, f is PCF if and only if $a \in \{-2, -1\}$. For d odd, f is PCF if and only if $a = -1$.*

Proof. Suppose $|a|_p > 1$ for some prime p. If $|z|_p \geq 1$, then $|f(z)|_p = |az^d + 1|_p = |az^d|_p > |z|_p$, so α is a wandering point if there exists $n \geq 0$ such that $|f^n(\alpha)|_p \geq 1$. In particular, $f(0) = 1$, so the critical

point 0 is a wandering point and f is not PCF. We conclude that for all primes p, $|a|_p \leq 1$; hence $a \in \mathbb{Z}$. By Proposition 2.2, $|a| \leq 2$, so $a \in \{\pm 1, \pm 2\}$.

Suppose that $|\alpha| > 2$. Then

$$|f(\alpha)| = |a\alpha^d + 1| > 2^{d-1}|\alpha| - 1 > |\alpha|.$$

Inductively, α must be a wandering point for f.

If $a = 1$, then $f^3(0) = 2^d + 1$, so 0 must be a wandering point. If $a = 2$, then $f^2(0) = 3$, so 0 must be a wandering point. If $a = -1$, then $f^2(0) = 0$, so f is PCF.

Finally, consider the case $a = -2$. If d is even then $f^2(0) = f^3(0) = -1$, so f is PCF. If d is odd, then $f^3(0) = 3$, so 0 is a wandering point. $\qquad\square$

3. Normal forms for bicritical polynomials

Cubic polynomials have been studied extensively in complex dynamics, e.g., [5; 4; 6; 7; 16], and in arithmetic dynamics, e.g., [14]. All of these use the Branner–Hubbard normal form, sometimes also called the monic centered form:

$$F(z) = z^3 + Az + B \quad \text{with critical points } \pm\alpha \text{ where } \alpha = \sqrt{\frac{-A}{3}}.$$

This form may be preferred in complex dynamics, but it is not ideal in arithmetic dynamics because it does not preserve the field of definition of the polynomial. For example, in [14], Ingram shows that if K is a number field and $F(z) \in K[z]$ is PCF, then the pairs (A, B) are in a finite computable set, and he finds the set in the case $F(z) \in \mathbb{Q}(z)$. However, our Table 1 shows that fewer than half of the PCF cubic polynomials defined over $\mathbb{Q}$ are conjugate to some $F(z) \in \mathbb{Q}[z]$ in the Branner–Hubbard form.

Example 3.1. Consider the PCF polynomial $f \in \mathbb{Q}[z]$ given by $f(z) = 3z^3 - \frac{9}{2}z^2 + 1$. Conjugating by

$$\phi(z) = \sqrt{3}z - \frac{\sqrt{3}}{2} \text{ gives } f^\phi(z) = z^3 - \frac{9}{4}z - \frac{\sqrt{3}}{4} \notin \mathbb{Q}[z].$$

In this section, we describe normal forms for cubic bicritical polynomials, one for the case of rational critical points and one for the case of irrational critical points. These cases are not disjoint, but both are necessary to exhaustively list all PCF cubic polynomials. It is a simple matter to check that our final list of cubic polynomials contains no conjugate maps, so this is of no concern.

Example 3.2. Let

$$f_1(z) = \frac{z^3}{4} - \frac{3z}{2}, \quad \text{so } \text{Crit}(f_1) = \{\pm\sqrt{2}\}.$$

Moving the two critical points to 0 and 1 gives the polynomial $g_1(z) = 2z^3 - 3z^2 + 1$. These conjugate polynomials — one with rational critical points and one with irrational critical points — are both defined over $\mathbb{Q}$.

If $f(z) \in K[z]$ has two rational critical points, we may conjugate to move them to 0 and 1 without changing the field of definition. From [2, Proposition 2.3], we know that there is a *unique* conjugacy class of bicritical polynomials of degree $d \geq 3$ with fixed critical points γ_1 and γ_2, and with prescribed ramification at the two critical points. Moreover, we have a formula for this polynomial when $\{\gamma_1, \gamma_2\} = \{0, 1\}$. Call the polynomial $\mathcal{B}_{d,k}(z)$. Since the critical points are at 0 and 1 and the polynomial has degree d, we have

$$\mathcal{B}'_{d,k}(z) = cz^{d-k-1}(z-1)^k$$

for some $1 \leq k < d-1$ and some constant c. So $d-k$ is the ramification index of $\mathcal{B}_{d,k}(z)$ at the critical point 0, and $k+1$ is the ramification index at the critical point 1. Expanding with the binomial theorem, integrating term-by-term, and requiring that the two critical points are fixed gives

$$\mathcal{B}_{d,k}(z) = \left(\frac{1}{k!} \prod_{j=0}^{k} (d-j) \right) z^{d-k} \sum_{i=0}^{k} \frac{(-1)^i}{(d-k+i)} \binom{k}{i} z^i. \tag{3-1}$$

Since we are concerned with the case $d = 3$, necessarily $k = 1$, giving the polynomial

$$\mathcal{B}_{3,1}(z) = -2z^3 + 3z^2. \tag{3-2}$$

Proposition 3.3. *Let* $g \in K[z]$ *be a bicritical polynomial of degree* $d \geq 3$ *with* $\mathrm{Crit}(g) = \{\gamma_1, \gamma_2\} \subseteq K$. *There exists an element* $\phi \in \mathrm{PGL}_2(K)$ *such that* $g^\phi = a\mathcal{B}_{d,k} + c$ *for some* $k \in \mathbb{N}$ *and some* $a, c \in K$.

Proof. Let $g \in K[z]$ with critical points $\gamma_1, \gamma_2 \in K$. Choose $k \in \mathbb{N}$ such that $d-k$ is the ramification index of γ_1 and $k+1$ is the ramification index of γ_2. Define $\phi(z) = (z-\gamma_1)/(\gamma_2-\gamma_1) \in \mathrm{PGL}_2(K)$, which moves the critical points to 0 and 1, respectively.

If $f(z) = g^\phi(z)$, then f has critical points at 0 and 1 and degree d, so

$$f'(z) = \alpha z^{d-k-1}(z-1)^k = a\mathcal{B}'_{d,k}(z)$$

for some $a \in \overline{K}^\times$.

Then $f(z) = a\mathcal{B}_{d,k}(z) + c$, and since $f = g^\phi$ where both $g, \phi \in K[z]$, we have $a, c \in K$. $\square$

We now consider a normal form for cubic polynomials $g \in K[z]$ with critical points in a quadratic extension of K.

Let $D \in \mathcal{O}_K^\times$ and let $d \geq 3$ be odd. We define a polynomial $\mathcal{P}_{d,D}(z) \in K[z]$ by the following conditions:

- $\mathcal{P}'_{d,D}(z) = (z^2 - D)^{(d-1)/2}$.
- $\mathcal{P}_{d,D}(0) = 0$.

Then $\mathcal{P}_{d,D}(z)$ is a bicritical polynomial having critical points $\{\pm\sqrt{D}\}$ each with ramification index $(d+1)/2$. Just as with the polynomials $\mathcal{B}_{d,k}(z)$, we expand the derivative $\mathcal{P}'_{d,D}(z)$ using the binomial theorem, integrate term-by-term, and use the fact that 0 is fixed to find a formula for these polynomials:

$$\mathcal{P}_{d,D}(z) = \sum_{j=0}^{(d-1)/2} (-D)^{(d-1)/2-j} \binom{\frac{d-1}{2}}{j} \frac{z^{2j+1}}{2j+1}. \tag{3-3}$$

Of particular interest in the sequel is the cubic case

$$\mathcal{P}_{3,D}(z) = \frac{z^3}{3} - Dz. \tag{3-4}$$

Proposition 3.4. *Let $g(z) \in K[z]$ be a bicritical polynomial of degree $d \geq 3$. Suppose that $\mathrm{Crit}(g) = \{\gamma_1, \gamma_2\} \not\subset K$. Then g is conjugate to a map of the form $a\mathcal{P}_{d,D}(z) + c$ for some $a, c \in K$ and some $D \in \mathcal{O}_K^\times / \mathcal{O}_K^2$.*

Proof. By definition, $\{\gamma_1, \gamma_2\}$ are roots of the polynomial $g'(z) \in K[z]$. Since they are not in K, we must have $g'(z) = \alpha(h(z))^\beta$ where $h \in K[z]$ is an irreducible quadratic polynomial. Note: In this case, d is odd and the ramification index of each critical point is $(d+1)/2$.

Therefore there are $m, n \in K$ with $n \neq 0$ and $D \in \mathcal{O}_K^\times / \mathcal{O}_K^2$ such that $\gamma_1 = m + n\sqrt{D}$ and $\gamma_2 = m - n\sqrt{D}$. Consider

$$\phi(z) = \frac{z - m}{n} \in K[z], \quad \text{which satisfies } \phi(\gamma_1) = \sqrt{D} \text{ and } \phi(\gamma_2) = -\sqrt{D}.$$

Define $f(z) = g^\phi(z)$. Since $g, \phi \in K[z]$, we have $f(z) \in K[z]$. Hence $f'(z) \in K[z]$. Furthermore, $\mathrm{Crit}(f) = \mathrm{Crit}(g^\phi) = \phi(\mathrm{Crit}(g)) = \{\pm\sqrt{D}\}$. Therefore, $f'(z) = a(z^2 - D)^{(d-1)/2}$ for some $a \in K$, which means that $f(z) = a\mathcal{P}_{d,D}(z) + c \in K[z]$. $\qquad\square$

4. Coefficient bounds for PCF cubic polynomials over $\mathbb{Q}$

From Corollary 1.2 in [14], for any number field K there are finitely many conjugacy classes of post-critically finite polynomial maps of degree d in $K[z]$. We would like to use the normal forms in Section 3 to determine a representative of each conjugacy class of PCF cubic polynomials over $\mathbb{Q}$. Many of these results can be extended to bicritical maps of arbitrary degree (see [19]).

Let $f(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \in K[z]$. Following Ingram [14], we set the following notation:

$$(2d)_v = \begin{cases} 1 & v \text{ is nonarchimedean,} \\ 2d & v \text{ is archimedean,} \end{cases}$$

$$C_{f,v} = (2d)_v \max_{0 \leq i < d} \left\{ 1, \left| \frac{a_i}{a_d} \right|_v^{1/(d-i)}, |a_d|_v^{-1/(d-1)} \right\}.$$

The following lemma show that $C_{f,v}$ gives an effective v-adic bound for preperiodic points (points with finite orbit) of a polynomial $f(z) \in \mathbb{Q}[z]$. Applying this bound to the critical points will, in turn, give v-adic bounds on the coefficients for PCF polynomials. Ingram uses $C_{f,v}$ in exaclty this way in [14] without stating and proving a lemma of this sort. We provide Lemma 4.1 and its proof for clarity and completeness.

Lemma 4.1. *Let $f(z) \in \mathbb{Q}[z]$ be a polynomial of degree $d \geq 2$. For $\alpha \in \mathbb{Q}$, if there exists $v \in M_{\mathbb{Q}}$ and $n \in \mathbb{N}$ such that*

$$|f^n(\alpha)|_v > C_{f,v},$$

then α must be a wandering point (have infinite orbit) for f.

Proof. First, notice that α is a wandering point if and only if $f^n(\alpha)$ is a wandering point for all $n \in \mathbb{N}$, so without loss of generality, assume $|\alpha|_v > C_{f,v}$ for some $v \in M_K$. We will show that α is a wandering point by proving that whenever $|\alpha|_v > C_{f,v}$, we must have $|f(\alpha)|_v > |\alpha|_v$.

If v is nonarchimedean, then $|\alpha|_v > |a_i/a_d|_v^{1/(d-i)}$ guarantees that $|a_d \alpha^d|_v > |a_i \alpha^i|_v$ for all $i < d$, so we have

$$|f(\alpha)|_v = \left| \sum_{i=0}^{d} a_i \alpha^i \right|_v = |a_d \alpha^d|_v > |\alpha|_v.$$

The inequality above comes from the fact that $|\alpha|_v > C_{f,v} \geq |a_d|_v^{-1/(d-1)}$.

If v is archimedean, then starting with $|\alpha|_v > 2d|a_i/a_d|_v^{1/(d-i)}$, we see that

$$|a_d \alpha^d|_v > \max_{0 \leq i < d} \{(2d)^{d-i} |a_i \alpha^i|_v\} \geq 2d \max_{0 \leq i < d} \{|a_i \alpha^i|_v\},$$

and so we have

$$|f(\alpha)|_v = \left| \sum_{i=0}^{d} a_i \alpha^i \right|_v \geq |a_d \alpha^d|_v - d \max_{0 \leq i < d} |a_i \alpha^i|_v > \tfrac{1}{2}|a_d \alpha^d|_v.$$

Finally, it follows from $|\alpha|_v > 2d|a_d|_v^{-1/(d-1)}$ that

$$\tfrac{1}{2}|a_d \alpha^d|_v > \tfrac{1}{2}(2d)^{d-1}|\alpha|_v > |\alpha|_v,$$

as desired. $\qquad\square$

4A. *PCF cubics with rational critical points.* We begin by specializing Lemma 4.1 to bicritical cubic polynomials with rational critical points, using the normal form in Proposition 3.3.

Lemma 4.2. *Let*

$$f(z) = a\mathcal{B}_{3,1} + c = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$$

be a bicritical polynomial and let $\alpha \in \mathbb{Q}$. If there exist $v \in M_\mathbb{Q}$ and $n \in \mathbb{N}$ such that

$$|f^n(\alpha)|_v > C_{f,v} = (6)_v \max\left\{1, |\tfrac{3}{2}|_v, |\tfrac{1}{2a}|_v^{1/2}, |\tfrac{c}{2a}|_v^{1/3}\right\},$$

then α is a wandering point for f.

Proof. The result follows immediately from applying the definition of $C_{f,v}$ and Lemma 4.1 to the coefficients of $f(z)$. $\qquad\square$

Remark 4.3. Let $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$, so $\mathrm{Crit}(f) = \{0, 1\}$. If f is PCF then every element in the orbits of 0 and 1 must be bounded by $C_{f,v}$. In particular,

$$|f(1)|_v = |a + c|_v \leq C_{f,v} \quad \text{and} \quad |f(0)|_v = |c|_v \leq C_{f,v}.$$

Thus if f is PCF, then $\max\{|c|_v, |a+c|_v\} \leq C_{f,v}$ for all $v \in M_\mathbb{Q}$. For every nonarchimedean place v, this means $\max\{|a|_v, |c|_v\} \leq C_{f,v}$.

Using the bound given above, we can find bounds on the absolute values of the parameters a and c of a PCF polynomial of the form $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$. We begin with an archimedean bound on the parameter a.

Lemma 4.4. *Let* $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$. *If* f *is PCF, then* $|a| < 4$.

Proof. Suppose $|a| \geq 4$ and $|\alpha| \geq \max\{|c|, 2\}$. Then

$$|f(\alpha)| = |a\alpha^{d-1}(-(d-1)\alpha + d) + c|,$$

and a straightforward calculation shows that $|f(\alpha)| > |\alpha|$. If $|c| \geq 2$, then 0 must be a wandering point. If $|c| < 2$, then

$$|a + c| \geq |a| - |c| > 2,$$

so 1 must be a wandering point. Thus, if f is PCF, we must have $|a| < 4$. $\qquad\square$

The following lemmas give p-adic bounds on the parameters a and c when f is PCF.

Lemma 4.5. *If* $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$ *is PCF then for nonarchimedean* $v \in M_{\mathbb{Q}}$

$$C_{f,v} = \max\left\{1, \left|\tfrac{3}{2}\right|_v, \left|\tfrac{1}{2a}\right|_v^{1/2}\right\}.$$

Proof. Let $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$ and $v \in M_{\mathbb{Q}}$ be nonarchimedean. From Lemma 4.2,

$$C_{f,v} = \max\left\{1, \left|\tfrac{3}{2}\right|_v, \left|\tfrac{1}{2a}\right|_v^{1/2}, \left|\tfrac{c}{2a}\right|_v^{1/3}\right\}.$$

Suppose

$$C_{f,v} = \left|\tfrac{c}{2a}\right|_v^{1/3} > \left|\tfrac{1}{2a}\right|_v^{1/2}; \quad \text{then } |c|_v^2 > \left|\tfrac{1}{2a}\right|_v.$$

However, since f is PCF,

$$|c|_v \leq C_{f,v} = \left|\tfrac{c}{2a}\right|_v^{1/3}, \quad \text{so } |c|_v^2 \leq \left|\tfrac{1}{2a}\right|_v,$$

giving a contradiction. $\qquad\square$

Notice that the statement above holds for $a, c \in K$ and $v \in M_K$ for any number field K and the proof is identical.

Lemma 4.6. *Let* $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$ *be PCF, let* p *be an odd prime, and let* $|\cdot|_p$ *be the* p-adic *absolute value. Then* $|a|_p \leq 1$ *and* $|c|_p^2 \leq |a|_p^{-1}$.

Proof. From Lemma 4.5,

$$C_{f,p} = \max\left\{1, \left|\tfrac{3}{2}\right|_p, \left|\tfrac{1}{2a}\right|_p^{1/2}\right\} = \max\{1, |3|_p, |a|_p^{-1/2}\} = \max\{1, |a|_p^{-1/2}\}.$$

There are two distinct cases

(1) $C_{f,p} = 1$, or

(2) $C_{f,p} = |a|_p^{-1/2} > 1$.

First, suppose $C_{f,p} = 1 \geq |a|_p^{-1/2}$. Then $|a|_p \geq 1$. However, since f is PCF,

$$|a|_p, |c|_p \leq C_{f,p} = 1.$$

Therefore $|a|_p = 1$, $|a|_p^{-1} = 1$, and $|c|_p^2 \leq 1 = |a|_p^{-1}$.

Now, suppose $C_{f,p} = |a|_p^{-1/2} > 1$. Then $|a|_p < 1$, as desired. Furthermore, since f is PCF,

$$|c|_p \leq C_{f,p} = |a|_p^{-1/2}. \qquad \square$$

Lemma 4.7. *Let* $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$ *be PCF. Then*

$$|2a|_2 \leq 1 \quad and \quad |2c|_2 \leq 1.$$

In fact, $2a \in \mathbb{Z}$.

Proof. From Lemma 4.6, we have $|2a|_p \leq 1$ for all odd primes p, so $2a \in \mathbb{Z}$ will follow immediately once we know that $|2a|_2 \leq 1$.

From Lemma 4.5,

$$C_{f,2} = \max\left\{1, \left|\tfrac{3}{2}\right|_2, \left|\tfrac{1}{2a}\right|_2^{1/2}\right\} = \max\left\{2, \left|\tfrac{1}{2a}\right|_2^{1/2}\right\}. \tag{4-1}$$

Suppose $C_{f,2} = 2$: Since f is PCF, both $|a|_2$ and $|c|_2 \leq 2$. Therefore, both $|2a|_2$ and $|2c|_2 \leq 1$ as desired.

Suppose $C_{f,2} = |1/(2a)|_2^{1/2} > 2$: Then

$$|2a|_2 < \tfrac{1}{4} < 1. \tag{4-2}$$

By Lemma 4.4, $|a| < 4$, so since $2a \in \mathbb{Z}$, we must have

$$a \in \left\{\tfrac{n}{2} : 1 \leq |n| < 8\right\}. \tag{4-3}$$

However, all of these possible a-values fail to satisfy equation (4-2), so the case $C_{f,2} = \left|\tfrac{1}{2a}\right|_2^{1/2} > 2$ does not happen. Therefore, if f is PCF then $C_{f,2} = 2$, and both $|2a|_2$ and $|2c|_2 \leq 1$ as desired. $\qquad \square$

Proposition 4.8. *If* f *is a cubic PCF polynomial of the form* $a\mathcal{B}_{d,k}(z) + c \in \mathbb{Q}[z]$, *then*

$$\pm a \in \left\{\tfrac{1}{2}, 1, \tfrac{3}{2}, 2, \tfrac{5}{2}, 3, \tfrac{7}{2}\right\} \quad and \quad \pm c \in \left\{0, 1, \tfrac{1}{2}, \tfrac{3}{2}, 2\right\}.$$

Proof. The result for a follows from equation (4-3) and Lemma 4.7.

Given the list for a, we see that $|a|_p = 1$ for any prime $p \notin \{2, 3, 5, 7\}$. For $p \in \{3, 5, 7\}$, we have $|a|_p \geq \tfrac{1}{p}$, so $|a|_p^{-1} \leq p$. Using Lemma 4.6, we conclude that $|c|_p \leq 1$ in both cases. Combining this with the fact that $|2c|_2 \leq 1$ from Lemma 4.7, we see that $|2c|_p \leq 1$ for all primes p. That is, $2c \in \mathbb{Z}$.

We will show that $|c| < \tfrac{5}{2}$. Suppose that a is contained in the above list and $|\alpha| \geq |c| \geq \tfrac{5}{2}$. Then

$$|f(\alpha)| \geq |a||\alpha|^2|-2\alpha + 3| - |c|,$$

and this implies $|f(\alpha)| > |\alpha|$. Hence α is a wandering point for f. Then $c = f(0)$ must be a wandering point for f, in which case f would not be PCF. The result for c follows. $\qquad \square$

4B. PCF cubics with irrational critical points. As in Section 4A, we can use the bound $C_{f,\nu}$ to find bounds on the (archimedean and nonarchimedean) absolute values of the parameters a, c and D of a PCF polynomial of the form $f(z) = a\mathcal{P}_{3,D} + c \in \mathbb{Q}[z]$. Unlike in Section 4A, the bounds are not given explicitly. Instead, we will determine restrictions on the relationships between the three parameters. In Theorem 5.2, we use these relationships to implement an algorithm that determines a finite set of triples (D, a, c) for which the polynomial $f(z) = a\mathcal{P}_{3,D} + c \in \mathbb{Q}[z]$ is possibly PCF.

Proposition 4.9. *Let* $f(z) = a(z^3/3 - Dz) + c \in \mathbb{Q}[z]$. *If f is PCF, then*

$$\pm aD \in \left\{ \tfrac{3}{4}, \tfrac{3}{2}, \tfrac{9}{4}, 3, \tfrac{15}{4}, \tfrac{9}{2}, \tfrac{21}{4} \right\}.$$

Proof. Let $\phi(z) = (z - \sqrt{D})/(-2\sqrt{D})$. Then

$$f^\phi(z) = \frac{-2}{3}aD(-2z^3 + 3z^2) + \frac{aD}{3} - \frac{c - \sqrt{D}}{2\sqrt{D}}.$$

None of the bounds on a in the previous section depended on the fact that $c \in \mathbb{Q}$, so we may apply them to f^ϕ. From Proposition 4.8, we have that

$$\pm\tfrac{2}{3}aD \in \left\{ \tfrac{1}{2}, 1, \tfrac{3}{2}, 2, \tfrac{5}{2}, 3, \tfrac{7}{2} \right\}. \qquad \square$$

Lemma 4.10. *Let* $f(z) = a(z^3/3 - Dz) + c \in \mathbb{Q}[z]$ *with* $\pm aD \in \left\{ \tfrac{3}{4}, \tfrac{3}{2}, \tfrac{9}{4}, 3, \tfrac{15}{4}, \tfrac{9}{2}, \tfrac{21}{4} \right\}$. *If f is postcritically finite, then* $|c|^2 < 11|D|$.

Proof. $\mathrm{Crit}(f) = \{\pm\sqrt{D}\}$ and

$$f(\pm\sqrt{D}) = \mp\tfrac{2}{3}aD^{3/2} + c.$$

A calculation shows that if $|c|^2 \geq 11|D|$ and $\alpha \in \mathbb{C}$ with $|\alpha| > |c|$, then $|f(\alpha)| > |\alpha|$. Since $a \neq 0$ then at least one of the critical points γ must satisfy $|f(\gamma)| > |c|$. $\qquad \square$

Lemma 4.11. *Let* $f(z) = a(z^3/3 - Dz) + c \in \mathbb{Q}[z]$. *If f is p-adically post-critically bounded, then*

$$|c\sqrt{a}|_p \leq \begin{cases} 1 & \text{if } p \geq 5, \\ 3^{-1/2} & \text{if } p = 3, \\ 2^3 & \text{if } p = 2. \end{cases}$$

Proof. Let $g = f^\phi$ for some $\phi \in \mathrm{PGL}_2(\overline{\mathbb{Q}})$ so that f^ϕ is monic and has a fixed point at 0. Then g is of the form

$$g(z) = z^3 + 3\alpha z^2 + (3\alpha^2 - aD)z \tag{4-4}$$

where α is a root of the polynomial

$$z^3 - (aD + 1)z + c\sqrt{\frac{a}{3}}. \tag{4-5}$$

The critical points for g are now $-\alpha \pm \sqrt{aD/3}$.

From [1, Theorems 1.2 and 4.1], we know that if g is p-adically post-critically bounded, the critical points must satisfy

$$\left| -\alpha \pm \sqrt{\frac{aD}{3}} \right|_p \leq \begin{cases} 1 & \text{if } p > 2, \\ 2 & \text{if } p = 2. \end{cases}$$

First consider $p \geq 3$. Add the critical points to see that

$$|-2\alpha|_p \leq 1, \quad \text{so } |\alpha|_p \leq 1.$$

Therefore, the polynomial in equation (4-5) is monic and all three roots lie in the p-adic unit disk. A Newton polygon argument says that the coefficients of that polynomial must also lie in the p-adic unit disk: if any coefficient had negative valuation, some segment of the Newton polygon would have positive slope, which would imply that the polynomial has a root of absolute value greater than one.

Since the constant term lies in the p-adic unit disk,

$$\left| c\sqrt{\frac{a}{3}} \right|_p \leq 1.$$

That gives the following bounds for $p \neq 2$:

$$|c\sqrt{a}|_p \leq \begin{cases} 1 & \text{if } p \geq 5, \\ 3^{-1/2} & \text{if } p = 3. \end{cases}$$

Now consider the case $p = 2$. We have

$$\left| -\alpha \pm \sqrt{\frac{aD}{3}} \right|_2 \leq 2. \tag{4-6}$$

Using the list of possible aD values from Proposition 4.9, we see that

$$\left| \sqrt{\frac{aD}{3}} \right|_2 \leq 2.$$

Applying the ultrametric triangle inequality to equation (4-6) yields $|-\alpha|_2 \leq 2$. Therefore the Newton polygon for that polynomial at $p = 2$ can have a segment of slope at most 1. Since the polynomial in equation (4-5) is cubic, that means the constant term must satisfy

$$v_2\left(c\sqrt{\frac{a}{3}} \right) \geq -3.$$

So $|c\sqrt{a}|_2 \leq 2^3$, which completes the proof. $\qquad\square$

5. The algorithms

This section presents algorithms for finding all bicritical cubic PCF polynomials over $\mathbb{Q}[z]$; the algorithms depend on normal forms found in Section 3 and coefficient bounds proven in Section 4.

5A. *Case 1: Rational critical points.* Results in Section 4 give a finite set of coefficients to test, so the first algorithm is straightforward.

Theorem 5.1. *If $f(z) \in \mathbb{Q}[z]$ is a cubic bicritical PCF polynomial with rational critical points, then $f(z)$ is conjugate to $f_{a,c}(z) = a(-2z^3 + 3z^2) + c$ where*

$$(a, c) \in \left\{ (1, 0), \left(\pm 1, \tfrac{1}{2} \right), \left(\tfrac{1}{2}, \pm 1 \right), \left(2, -\tfrac{1}{2} \right), \left(\tfrac{3}{2}, 0 \right), (-1, 1), \left(-2, \tfrac{3}{2} \right), \left(-\tfrac{3}{2}, 1 \right), \left(-\tfrac{1}{2}, 0 \right) \right\}.$$

Proof. From Proposition 3.3, we know that every cubic polynomial in $\mathbb{Q}[z]$ with rational critical points is conjugate to a map of the form $f_{a,c}(z) = a(-2z^3 + 3z^2) + c$ for some $a, c \in \mathbb{Q}$.

From Proposition 4.8, if $f_{a,c}$ is post-critically bounded in every place, then

$$\pm a \in \left\{ \tfrac{1}{2}, 1, \tfrac{3}{2}, 2, \tfrac{5}{2}, 3, \tfrac{7}{2} \right\} \quad \text{and} \quad \pm c \in \left\{ 0, 1, \tfrac{1}{2}, \tfrac{3}{2}, 2 \right\}.$$

This gives 126 possibilities for (a, c). The authors used built-in Sage [17] functionality to test all such pairs.[1]   □

5B. *Case 3: Irrational critical points.* This case is more delicate. Results in Section 4 give relationships between absolute values of the coefficients for cubic PCF maps. We must disentangle these relationships to build a finite search space.

Theorem 5.2. *If $f(z) \in \mathbb{Q}[z]$ is a cubic bicritical PCF polynomial that is not conjugate to a polynomial with rational critical points, then $f(z)$ is conjugate to $f_{D,a,c}(z) = a(\tfrac{z^3}{3} - Dz) + c$ where*

$$(D, a, c) \in \left\{ \left(2, -\tfrac{3}{4}, 2 \right), \left(-7, -\tfrac{3}{28}, \tfrac{7}{2} \right) \right\}.$$

Proof. From Proposition 3.4, we know that every cubic polynomial in $\mathbb{Q}[z]$ with irrational critical points is conjugate to a map of the form

$$f_{D,a,c}(z) = a(z^3/3 - Dz) + c$$

for some $a, c \in \mathbb{Q}$ and a squarefree integer D.

Note that if $c = 0$, then $f_{D,a,c}(z)$ is conjugate to a cubic polynomial with rational critical points via conjugation by $\phi(z) = (a - \sqrt{D})/(-z\sqrt{D})$. Furthermore, $f_{D,a,-c}(z)$ is conjugate to $f_{D,a,c}(z)$, so we may assume that $c > 0$. Therefore, we build a list of triples (D, a, c) with $D, a, c > 0$, and each triple corresponds to four possibly PCF polynomials (varying the signs of D and a). We split the algorithm into two cases corresponding to D even and D odd.

Step 1: *Loop over possible aD values.* From Proposition 4.9, if $f_{D,a,c}$ is PCF then:

$$\pm aD \in \left\{ \tfrac{3}{4}, \tfrac{3}{2}, \tfrac{9}{4}, 3, \tfrac{15}{4}, \tfrac{9}{2}, \tfrac{21}{4} \right\}.$$

---

[1]Sage code is available with the arXiv distribution of this article.

Step 2: *Compute $|a|_2$.* We use the value of aD in Step 1 and the parity of D.

Step 3: *Find an upper bound for $|c|_p$ for each prime p.* From Lemma 4.11, we know that if $f_{D,a,c}(z)$ is p-adically post-critically bounded, then

$$|c\sqrt{a}|_p \leq \begin{cases} 1 & \text{if } p \geq 5, \\ 3^{-1/2} & \text{if } p = 3, \\ 2^3 & \text{if } p = 2. \end{cases} \tag{5-1}$$

So from Step 2 we can find $e \leq 3$ such that $|c|_2 \leq 2^e$. Also using the list in Step 1, we conclude that $|c|_p \leq 1$ for each prime $p \geq 3$.

Step 4: *Factor D and c.* Write $D = mP$ or $D = 2mP$, where m and P are relatively prime odd squarefree integers such that m divides the numerator of aD and P divides the denominator of a. By equation (5-1), P must also divide the numerator of c. Thus, $c = \frac{Pk}{2^e}$ for some positive integer k. Note: For a fixed aD from the list above, m comes from a finite set, but for now P and k can be arbitrarily large.

Step 5: *Bound the factors of D and c.* From Lemma 4.10, we know that if $f_{D,a,c}(z)$ is post-critically bounded at the archimedean place, then $|c|^2 < 11|D|$. Depending on the parity of D, this gives

$$\frac{P^2 k^2}{2^{2e}} < 11mP \quad \text{or} \quad \frac{P^2 k^2}{2^{2e}} < 22mP.$$

So $Pk^2 < B$ where $B = 11m \cdot 2^{2e}$ when D is odd, and $B = 11m \cdot 2^{2e+1}$ when D is even. We know e from Step 3, so for each m we have an explicit value for the upper bound B.

Step 6: *Loop over P values.* For all odd, squarefree integers $P < B$, we determine the set of possible k values such that $Pk^2 < B$.

Step 7: *Create the triple.* Each triple (m, P, k) yields a triple $(D, a, c) = (mP, aD/(mP), Pk/2^e)$ or $(D, a, c) = (2mP, aD/(2mP), Pk/2^e)$. Finally, check that $3 \mid ac$ to verify that the triple satisfies the 3-adic condition in equation (5-1). If so, add (D, a, c) to the list of possible PCF triples.

This algorithm yields a list of 5,957 triples corresponding to 23,828 possibly PCF polynomials. The authors used built-in Sage [17] functionality to test all such triples. Only the two listed in the theorem statement above are actually PCF and are not conjugate to a polynomial already found in Theorem 5.1. $\qquad\square$

Combining the results in Theorems 2.3, 5.1, and 5.2 yields a total of 15 conjugacy classes of PCF cubic polynomials over $\mathbb{Q}[z]$, and this list is exhaustive. In the table below, we provide one representative of each conjugacy class along with the critical portrait for the polynomial. In the portrait, the critical points are given by γ and other points in the post-critical set are denoted $\bullet$. The monic centered form is given when it is defined over $\mathbb{Q}[z]$; these appeared in [14].
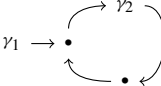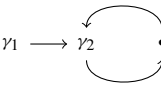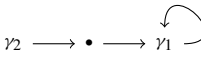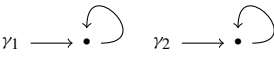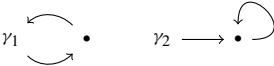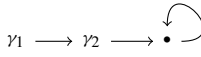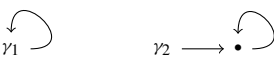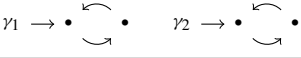
PCF polynomial	Critical portrait	Monic centered form
z^3	γ_1 (self-loop)	z^3
$-z^3 + 1$	γ_1	
$-2z^3 + 3z^2 + \frac{1}{2}$	$\gamma_1 \rightarrow \bullet$, γ_2	
$-z^3 + \frac{3}{2}z^2 + 1$	$\gamma_1 \longrightarrow \gamma_2$	
$-2z^3 + 3z^2$	γ_1, γ_2	$z^3 + \frac{3}{2}z$
$-3z^3 + \frac{9}{2}z^2$	$\gamma_2 \longrightarrow \bullet \longrightarrow \gamma_1$	
$-z^3 + \frac{3}{2}z^2 - 1$	$\gamma_1 \rightarrow \bullet \;\; \bullet$, $\gamma_2 \rightarrow \bullet$	
$-4z^3 + 6z^2 - \frac{1}{2}$	$\gamma_1 \rightarrow \bullet \;\; \bullet \leftarrow \gamma_2$	$z^3 + 3z$
$2z^3 - 3z^2 + 1$	$\gamma_1 \;\; \gamma_2$	$z^3 - \frac{3}{2}z$
$4z^3 - 6z^2 + \frac{3}{2}$	$\gamma_1 \longrightarrow \bullet$, $\gamma_2 \longrightarrow \bullet$	$z^3 - 3z$
$2z^3 - 3z^2 + \frac{1}{2}$	$\gamma_1 \;\; \bullet$, $\gamma_2 \longrightarrow \bullet$	
$3z^3 - \frac{9}{2}z^2 + 1$	$\gamma_1 \longrightarrow \gamma_2 \longrightarrow \bullet$	
$z^3 - \frac{3}{2}z^2$	γ_1, $\gamma_2 \longrightarrow \bullet$	$z^3 - \frac{3}{4}z + \frac{3}{4}$ and $z^3 - \frac{3}{4}z - \frac{3}{4}$
$-\frac{1}{4}z^3 + \frac{3}{2}z + 2$	$\gamma_1 \rightarrow \bullet \;\; \bullet$, $\gamma_2 \rightarrow \bullet \;\; \bullet$	
$-\frac{1}{28}z^3 - \frac{3}{4}z + \frac{7}{2}$	$\gamma_1 \;\; \bullet$, $\gamma_2 \;\; \bullet$	

Table 1. Critical Portraits of Cubic PCF Polynomials over $\mathbb{Q}$

References

[1] Jacqueline Anderson, *Bounds on the radius of the p-adic Mandelbrot set*, Acta Arith. **158** (2013), no. 3, 253–269. MR 3040666

[2] Jacqueline Anderson, Irene I. Bouw, Ozlem Ejder, Neslihan Girgin, Valentijn Karemaker, and Michelle Manes, *Dynamical Belyi maps*, Women in numbers Europe II, Assoc. Women Math. Ser., vol. 11, Springer, Cham, 2018, pp. 57–82. MR 3882706

[3] James Belk and Sarah Koch, *Iterated monodromy for a two-dimensional map*, In the tradition of Ahlfors-Bers. V, Contemp. Math., vol. 510, Amer. Math. Soc., Providence, RI, 2010, pp. 1–11. MR 2581826

[4] Araceli Bonifant, Jan Kiwi, and John Milnor, *Errata for "Cubic polynomial maps with periodic critical orbit, part II: Escape regions"*, Conform. Geom. Dyn. **14** (2010), 190–193. MR 2670510

[5] Araceli Bonifant, Jan Kiwi, and John Milnor, *Cubic polynomial maps with periodic critical orbit. II. Escape regions*, Conform. Geom. Dyn. **14** (2010), 68–112. MR 2600536

[6] Bodil Branner and John H. Hubbard, *The iteration of cubic polynomials. I. The global topology of parameter space*, Acta Math. **160** (1988), no. 3-4, 143–206. MR 945011

[7] Bodil Branner and John H. Hubbard, *The iteration of cubic polynomials. II. Patterns and parapatterns*, Acta Math. **169** (1992), no. 3-4, 229–325. MR 1194004

[8] Xavier Buff, *On postcritically finite unicritical polynomials*, New York J. Math. **24** (2018), 1111–1122. MR 3890968

[9] Laura De Marco, *Dynamical moduli spaces and elliptic curves*, Ann. Fac. Sci. Toulouse Math. (6) **27** (2018), no. 2, 389–420. MR 3831028

[10] C. Favre and T. Gauthier, *Distribution of postcritically finite polynomials*, Israel J. Math. **209** (2015), no. 1, 235–292. MR 3430241

[11] William Floyd, Walter Parry, and Kevin M. Pilgrim, *Modular groups, Hurwitz classes and dynamic portraits of NET maps*, Groups Geom. Dyn. **13** (2019), no. 1, 47–88. MR 3900764

[12] Thomas Gauthier and Gabriel Vigny, *Distribution of postcritically finite polynomials II: Speed of convergence*, J. Mod. Dyn. **11** (2017), 57–98. MR 3627118

[13] Thomas Gauthierand Gabriel Vigny, *Distribution of postcritically finite polynomials III: Combinatorial continuity*, Fund. Math. **244** (2019), no. 1, 17–48. MR 3874664

[14] Patrick Ingram, *A finiteness result for post-critically finite polynomials*, International Mathematics Research Notices (2010).

[15] David Lukas, Michelle Manes, and Diane Yap, *A census of quadratic post-critically finite rational functions defined over ℚ*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 314–329. MR 3240812

[16] John Milnor, *Cubic polynomial maps with periodic critical orbit. I*, Complex dynamics, A K Peters, Wellesley, MA, 2009, pp. 333–411. MR 2508263

[17] Inc. SageMath, *CoCalc: Collaborative Computation Online*, 2016, `https://cocalc.com/`.

[18] Joseph H. Silverman, *Moduli spaces and arithmetic dynamics*, CRM Monograph Series, vol. 30, American Mathematical Society, Providence, RI, 2012. MR 2884382

[19] Bella Tobin, *Arithmetic dynamics of bicritical polynomials*, In progress.

JACQUELINE ANDERSON: jacqueline.anderson@bridgew.edu
Department of Mathematics, Bridgewater State University, Bridgewater, MA, United States

MICHELLE MANES: mmanes@math.hawaii.edu
Department of Mathematics, University of Hawai'i at Mānoa, Honolulu, HI, United States

BELLA TOBIN: bella.tobin@okstate.edu
Department of Mathematics, Oklahoma State University, Stillwater, OK, United States

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS