Canad. J. Math. Vol. 71 (4), 2019 pp. 773–817
http://dx.doi.org/10.4153/CJM-2018-026-x

Powers in Orbits of Rational Functions: Cases of an Arithmetic Dynamical Mordell–Lang Conjecture

Jordan Cahn, Rafe Jones, and Jacob Spear

Abstract. Let K be a finitely generated field of characteristic zero. For fixed $m \geq 2$, we study the rational functions ϕ defined over K that have a K-orbit containing infinitely many distinct m-th powers. For $m \geq 5$ we show that the only such functions are those of the form $cx^j(\psi(x))^m$ with $\psi \in K(x)$, and for $m \leq 4$ we show that the only additional cases are certain Lattès maps and four families of rational functions whose special properties appear not to have been studied before.

With additional analysis, we show that the index set $\{n \geq 0 : \phi^n(a) \in \lambda(\mathbb{P}^1(K))\}$ is a union of finitely many arithmetic progressions, where ϕ^n denotes the n-th iterate of ϕ and $\lambda \in K(x)$ is any map Möbius-conjugate over K to x^m. When the index set is infinite, we give bounds on the number and moduli of the arithmetic progressions involved. These results are similar in flavor to the dynamical Mordell–Lang conjecture, and motivate a new conjecture on the intersection of an orbit with the value set of a morphism. A key ingredient in our proofs is a study of the curves $y^m = \phi^n(x)$. We describe all ϕ for which these curves have an irreducible component of genus at most 1, and show that such ϕ must have two distinct iterates that are equal in $K(x)^*/K(x)^{*m}$.

1 Introduction

Let K be a field and let $\phi \in K(x)$ be a rational function with coefficients in K. We denote by ϕ^n the n-th iterate of ϕ, which we emphasize is distinct from the n-th power of ϕ. A fundamental object in dynamics is the (forward) orbit[1]

$$O_\phi^+(a) = \{\phi^n(a) : n \geq 0\}$$

of $a \in \mathbb{P}^1(K)$ under the map ϕ; note that $\phi^0(x) = x$ by convention, and so $a \in O_\phi^+(a)$. An overarching goal is to classify the orbits of a given map ϕ in terms of salient features of K, such as a metric or arithmetic structure. A related goal, which has attracted a large body of work, is to understand the collection of maps that can possess an orbit with certain very special properties. For example, when $K = \mathbb{C}$, Ghioca, Tucker, and Zieve [9,10] show that if $f \in \mathbb{C}[x]$ has degree at least two, then for each $g \in \mathbb{C}[x]$ with degree at least two and such that an orbit of g has infinite intersection with an orbit

Received by the editors September 26, 2017; revised April 25, 2018.
Published electronically December 3, 2018.
Authors J. C. and J. S. research was supported by Carleton College's HHMI grant for undergraduate science education and the Carleton College department of Mathematics and Statistics.
AMS subject classification: **37P05**, 11G05, 37P15.
Keywords: arithmetic dynamics, iteration of rational functions, special orbits of rational function, genus of variables-separated curve, Lattès map.

[1] We generally drop the word "forward" in this article, but we wish to avoid confusion with the backwards orbit $O_\phi^-(a)$, which we use frequently (see Definition 3.4). We thus prefer the notation $O_\phi^+(a)$ for the forward orbit rather than the more standard $O_\phi(a)$.

of f, it follows that f has a common iterate with g. Thus the existence of a special orbit of f has global implications for f; in particular, it implies functional properties of the map f. Another example of such a result is due to Silverman [21, Theorem A]. Recall that the degree of ϕ can be defined by writing $\phi(x) = A_1(x)/A_2(x)$, with $A_1, A_2 \in K[x]$ relatively prime polynomials, and taking the maximum of the degrees of A_1 and A_2. Silverman shows that if $\phi(x) \in \mathbb{Q}(x)$ has degree at least two, and there is an orbit of $\phi(x)$ containing infinitely many integers, then $\phi^2(x)$ is a polynomial (a more general result is given in [21, Theorem B]). This theme is taken much further in the dynamical Mordell–Lang conjecture [5, Conjecture 1.5.0.1], which posits that if Φ is an endomorphism of a quasiprojective variety X defined over $\mathbb{C}$, a is any point in $X(\mathbb{C})$, and $V \subset X$ is any subvariety, then $\{n \geq 0 : \Phi^n(a) \in V(\mathbb{C})\}$ is a union of finitely many arithmetic progressions (note that singletons are considered arithmetic progressions, and thus any finite set is a union of arithmetic progressions). In particular, if $O_\phi^+(a) \cap V(\mathbb{C})$ is infinite, then V contains a positive-dimensional subvariety that is periodic under the action of f. Indeed, let $M > 0$ and $\ell \geq 0$ be such that $\Phi^{kM+\ell}(a) \in V(\mathbb{C})$ for all $k \geq 0$; then the Zariski closure of $\{\Phi^{kM+\ell}(a) : k \geq 0\}$ is positive-dimensional and invariant under Φ^M. For a summary of the extensive recent work surrounding this conjecture, see [5].

From this point forward, we let K be a finitely generated field of characteristic zero, that is, an extension of $\mathbb{Q}$ generated by a finite set of (possibly transcendental) elements; all such fields can be embedded in the complex numbers, and throughout this article we consider K as a subfield of $\mathbb{C}$. Fix an integer $m \geq 2$. Our goal is a study of the $\phi \in K(x)$ possessing a K-orbit containing infinitely many distinct m-th powers in K. The existence of such an orbit implies infinitely many distinct K-rational solutions to the equation $\phi^n(x) = y^m$ for each $n \geq 1$, and hence by Faltings' Theorem the curve $C_n : \phi^n(x) = y^m$ must have an irreducible component of genus at most one, for all $n \geq 1$ (throughout, we take the curve given by rational functions $A_1(x)/A_2(x) = B_1(y)/B_2(y)$ to be that given by $A_1(x)B_2(y) - B_1(y)A_2(x) = 0$). It is easy to see that every irreducible component of C_n has the same genus (Proposition 2.2), and we denote this quantity by g_n. We are thus interested in the maps ϕ such that g_n is at most one for all $n \geq 1$; our first two results (Theorems 1.1 and 1.2) deal with the a priori more general situation where g_n is bounded as n grows. These results, together with Corollary 1.3, show that the existence of an *arithmetically* special orbit of ϕ implies strong conclusions about the global structure of the function.

Theorem 1.1 *Fix $m \geq 2$ and let $\phi \in \mathbb{C}(x)$ have degree at least two. Then g_n is bounded as $n \to \infty$ if and only if*

(1.1) *there exist integers $r > s \geq 0$ such that*

$$\phi^r(x) = \phi^s(x)(\psi(x))^m \text{ for some } \psi \in \mathbb{C}(x).$$

In that case, the following hold.

(i) *If $\phi \in K(x)$ for some subfield K of $\mathbb{C}$, then (1.1) holds for some $\psi \in K(x)$.*
(ii) *We have $g_n \leq 1$ for all $n \geq 1$.*
(iii) *One can take $r \leq m$ if $m \geq 3$, and $r \leq 6$ if $m = 2$.*

A full accounting of the possible values of r and s that occur when (1.1) holds can be found in Section 8.

As a primary part of our proof of Theorem 1.1, we show the following theorem. Recall that the post-critical set $\operatorname{Postcrit}(\phi)$ of a rational function $\phi \in \mathbb{C}(x)$ is $\bigcup_{n\geq 1} \phi^n(C)$, where C is the critical set for ϕ, *i.e.*, the set of points in $\mathbb{P}^1(\mathbb{C})$ at which ϕ is not locally one-to-one. A map $\phi \in \mathbb{C}(x)$ of degree at least two is a *Lattès map* if there is a linear map $L(t) = at + b$ acting on a complex torus $\mathbb{C}/\Lambda$ and a finite-to-one holomorphic map $\Theta\colon \mathbb{C}/\Lambda \to \mathbb{P}^1(\mathbb{C})$ satisfying $\phi \circ \Theta = \Theta \circ L$. Denote by $e_\phi(z)$ the ramification index, or local degree, of ϕ at $z \in \mathbb{P}^1(\mathbb{C})$; when $z \neq \infty$ and $\phi(z) \neq \infty$, this coincides with the multiplicity of z as a root of $\phi(x) - \phi(z)$ (see [22, p. 12] for a full discussion). Usefully, the Lattès maps are precisely those rational functions $\phi \in \mathbb{C}(x)$ such that there exists a function $r\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{Z}$ satisfying

$$r(\phi(z)) = e_\phi(z) \cdot r(z) \text{ for all } z \in \mathbb{P}^1(\mathbb{C}) \quad \text{and} \quad r(z) = 1 \text{ for } z \notin \operatorname{Postcrit}(\phi). \tag{1.2}$$

Such a function r is unique; see Theorem 7.2 or [15, Section 4] for details. When there exists such a function r, the collection of values of r on $\operatorname{Postcrit}(\phi)$ is called the *signature* of ϕ, and the only possible signatures are (2,2,2,2), (3,3,3), (2,4,4), and (2,3,6) [15, Corollary 4.5].

Theorem 1.2 *Fix $m \geq 2$ and let $\phi \in \mathbb{C}(x)$ have degree at least two. Then g_n is bounded as $n \to \infty$ if and only if one of the following holds:*

(1) *$\phi(x) = cx^j(\psi(x))^m$ with $\psi \in \mathbb{C}(x)$, $0 \leq j \leq m-1$, $c \in \mathbb{C}^*$;*

(2) *$m = 4$ and ϕ is a Lattès map of signature $(2,4,4)$, with $\{0,\infty\}$ in the post-critical set and $r(0) = r(\infty) = 4$, where r is the function satisfying* (1.2)*;*

(3) *$m = 3$ and ϕ is a Lattès map of signature $(3,3,3)$, with $\{0,\infty\}$ in the post-critical set;*

(4) *$m = 2$ and ϕ is a Lattès map of signature $(2,2,2,2)$ with $\{0,\infty\}$ in the post-critical set;*

(5) *$m = 2$ and either $\phi(x)$ or $1/\phi(1/x)$ can be written in one of the following ways, where $B, C \in \mathbb{C}^*$, $f, g, h \in \mathbb{C}[x] \smallsetminus \{0\}$, and the numerator and denominator of each fraction have no common roots in $\mathbb{C}$:*

   (a) $-\frac{f(x)^2}{(x-C)g(x)^2}$ *with* $f(x)^2 + C(x-C)g(x)^2 = Cxh(x)^2$*;*

   (b) $-\frac{(x-C)f(x)^2}{g(x)^2}$ *with* $(x-C)f(x)^2 + Cg(x)^2 = xh(x)^2$*;*

   (c) $B\frac{(x-C)f(x)^2}{g(x)^2}$ *with* $B(x-C)f(x)^2 - Cg(x)^2 = -Ch(x)^2$*;*

   (d) $B\frac{x(x-C)f(x)^2}{g(x)^2}$ *with* $Bx(x-C)f(x)^2 - Cg(x)^2 = -Ch(x)^2$*.*

Moreover, if K is a subfield of $\mathbb{C}$ with $\phi \in K(x)$, then we can take

$$\psi \in K(x) \text{ and } c \in K^* \text{ in case } (1) \tag{1.3}$$

$$B, C \in K^* \text{ and } f, g, h \in K[x] \smallsetminus \{0\} \text{ in case } (5). \tag{1.4}$$

The maps in part (5) of Theorem 1.2 appear not to have been studied before in general. We discuss how to give explicit parameterizations of all such maps in Proposition 7.4 and the paragraphs following. Important examples of these maps are closely related to the degree-d monic Chebyshev polynomial T_d, defined by the equation

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

$T_d(x+x^{-1}) = x^d + x^{-d}$; see [15, Section 2] or [22, Section 6.2] for further properties. The map $(-1)^d(T_d(x+2))-2$ satisfies (5b) when d is odd and (5d) when d is even (see Corollary 1.8 for more on these maps). Note that maps of type (5a) and (5c) cannot be Möbius-conjugate to polynomials (see the proof of Theorem 1.2 in Section 7).

Combining Faltings' theorem with Theorems 1.1 and 1.2, we obtain the main result of this paper. Denote by $\mathbb{P}^1(K)^m$ the set $\{k^m : k \in K\} \cup \{\infty\}$.

Corollary 1.3 *Let K be a finitely generated field of characteristic zero field, let $\phi \in K(x)$ have degree at least two, and fix $m \geq 2$. If there exists $a \in \mathbb{P}^1(K)$ such that $O^+_\phi(a) \cap \mathbb{P}^1(K)^m$ is infinite, then ϕ falls into one of the cases in Theorem 1.2 and satisfies (1.3) and (1.4), and ϕ also satisfies (1.1) with $\psi \in K(x)$.*

Thus, the infinitude of $O^+_\phi(a) \cap \mathbb{P}^1(K)^m$ implies strong functional properties of ϕ, similar to the results of [9, 10, 21] mentioned at the beginning of this section.

The proofs of Theorems 1.1 and 1.2 unfold in two steps. The first is geometric and involves studying $\phi \in \mathbb{C}(x)$ for which g_n is bounded. The second is arithmetic and consists of showing that various quantities in the two theorems can be defined over a subfield K of $\mathbb{C}$, when ϕ was initially defined over K. In the geometric part, our study of the genus of C_n is a case of a problem with a long history, which remains largely unresolved: determine all pairs A, B of complex rational functions such that the curve $A(x) = B(y)$ has an irreducible component of genus at most one. In the case where A and B are polynomials, a complete solution is given in [6] for irreducible components of genus zero with at most two points at infinity (see [6, pp. 264, 281] for discussion and references regarding the extensive past work on this problem). Partial results exist for irreducible components of genus one, *e.g.*, [1, 2], again assuming A and B are polynomials. When A and B are allowed to be non-polynomial rational functions, there are many fewer results available. One example is [18], which classifies all A, B with no common critical values such that $A(x) = B(y)$ has an irreducible component of genus at most one.

While the general problem is far from resolution, we propose the following variant, which our Theorem 1.2 resolves for $B(y) = y^m$, $m \geq 2$.

Problem 1.4 *Given $B \in \mathbb{C}(x)$, explicitly determine all $\phi \in \mathbb{C}(x)$ such that*

(1.5) *for all $n \geq 1$ the curve $\phi^n(x) = B(y)$*
has an irreducible component of genus at most one.

One can also fix ϕ and study rational functions B for which (1.5) holds. This is the approach taken in the recent preprint [17], where it is shown, among other results, that if ϕ is not a power map, Chebyshev polynomial, or Lattès map, and (1.5) holds, then there is a rational Galois covering $h\colon \mathbb{P}^1 \to \mathbb{P}^1$ (depending only on ϕ) and rational functions V, V' satisfying $\phi \circ h = h \circ V'$ and $\phi^\ell \circ h = B \circ V$ for some $\ell \geq 1$.

The work of Ghioca, Tucker, and Zieve in [9, 10] addresses a question of similar flavor to Problem 1.4, though still quite distinct. There, the authors classify all pairs f, g of complex polynomials such that for every $m, n \geq 1$ the curve $f^n(x) = g^m(y)$ has an irreducible component of genus zero with at most two points at infinity. To do

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

so, they rely on the classification of Bilu and Tichy [6] mentioned above; thus, they already know precisely which curves $A(x) = B(y)$ have the desired property, but they must determine when A and B arise from iteration of lower-degree polynomials. This requires significant and novel results on polynomial decomposition.

Taking $B(y) = y^m$, as in Theorem 1.2, greatly eases the generally difficult problem of determining the irreducible components of $A(x) = B(y)$ and leads to a considerably simpler genus formula than the one for general curves of the form $A(x) = B(y)$ (see Propositions 2.2 and 2.3). Nonetheless, similar to the situation of [9, 10], we are left with the a priori difficult problem of determining the maps ϕ such that A can be taken to be an arbitrary iterate of ϕ.

The arithmetic part of the proofs of Theorems 1.1 and 1.2 can be found mainly in Section 6. This aspect of our results, in particular, the part of Theorem 1.1 where ψ can be defined over K when ϕ is defined over K, leads to a result whose conclusion is the same as that of the dynamical Mordell–Lang conjecture. When the intersection set is infinite, we are able to prove the far stronger conclusion that three arithmetic progressions suffice, and we give information on their moduli. Throughout, we denote by $\mathbb{N}_0$ the set of nonnegative integers.

Theorem 1.5 *Let K be a finitely generated field of characteristic zero, let $\phi, \lambda \in K(x)$ each have degree at least two, and suppose that λ is Möbius-conjugate (over K) to a power map. Then for every $a \in \mathbb{P}^1(K)$, the set*

$$\{n \in \mathbb{N}_0 : \phi^n(a) \in \lambda(\mathbb{P}^1(K))\} \tag{1.6}$$

is a finite union of arithmetic progressions. If $O^+_\phi(a) \cap \lambda(\mathbb{P}^1(K))$ is infinite, then the set (1.6) is a union of at most three arithmetic progressions, each with modulus M satisfying $M \le m$ if $m \ge 3$ and $M \le 6$ if $m = 2$.

We emphasize again that we take singletons to be arithmetic progressions of modulus 0, and so Theorem 1.5 holds trivially when the set (1.6) is finite. If $O^+_\phi(a) \cap \lambda(\mathbb{P}^1(K))$ is finite, then either $O^+_\phi(a)$ is infinite and the set (1.6) is finite or $O^+_\phi(a)$ is finite; in either case Theorem 1.5 holds trivially. In Section 10 we give an example where $O^+_\phi(a) \cap \lambda(\mathbb{P}^1(K))$ is infinite and the set (1.6) cannot be written as a union of two arithmetic progressions, showing that three is best possible. The bound on M in Theorem 1.5 is best possible for $m \ge 3$, regardless of the choice of K (see Lemma 8.1); for $m = 2$ the bound can be reduced to $M \le 4$ using an analysis of the field of definition of Lattès maps, which we plan to describe in a future article.

The proof of Theorem 1.5 quickly reduces to the case $\lambda(x) = x^m$. Indeed, let $\mu \in \mathrm{PGL}_2(K)$ and put $\phi^\mu = \mu^{-1} \circ \phi \circ \mu$. If $\phi^n(a) = \lambda(b)$ for $a, b \in \mathbb{P}^1(K)$, then $(\phi^\mu)^n(\mu^{-1}(a)) = \lambda^\mu(\mu^{-1}(b))$, giving

$$\{n \in \mathbb{N}_0 : \phi^n(a) \in \lambda(\mathbb{P}^1(K))\} = \{n \in \mathbb{N}_0 : (\phi^\mu)^n(\mu^{-1}(a)) \in \lambda^\mu(\mathbb{P}^1(K))\}. \tag{1.7}$$

Hence, if Theorem 1.5 can be established for λ^μ and arbitrary ϕ and a, it must also hold for λ and arbitrary ϕ and a. Thus, if μ conjugates λ to a power map, we have reduced to the case $\lambda(x) = x^m$, as desired. Note that if λ is not conjugate over K to a power map, we cannot take advantage of the special geometric properties of the

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

curve $\phi^n(x) = y^m$ mentioned in the discussion following Problem 1.4, and thus new methods would be required.

The dynamical Mordell–Lang conjecture asserts that once there exist infinitely many instances of the intersection between the geometric object $V(\mathbb{C})$ and the arithmetic dynamical object $O_\phi^+(a)$ (using the notation from the first paragraph of the introduction), then the intersection must have a structure: its index set must be given by finitely many arithmetic progressions. Theorem 1.5 proves this assertion in the case where $X = \mathbb{P}^1$ and the geometric object V is replaced by an arithmetic object, namely the set of K-values of the morphism $\lambda : X \to X$. We conjecture that a similar conclusion holds for the set of K-values of more general morphisms:

Conjecture 1.6 (Arithmetic dynamical Mordell–Lang conjecture for $\mathbb{P}^1$) *Let $X = \mathbb{P}^1$ and let Y be a curve defined over a finitely generated field of characteristic zero K. Suppose that $\lambda\colon Y \to X$ is a finite K-morphism and $\phi\colon X \to X$ is a morphism of degree at least two. Then for any $a \in X(K)$, the set $\{n \in \mathbb{N}_0 : \phi^n(a) \in \lambda(Y(K))\}$ is a finite union of arithmetic progressions.*

Shortly after this paper was posted to the arXiv, Hyde and Zieve sent us a proof of Conjecture 1.6. Their short argument makes use of the pigeonhole principle, as well as the finiteness of the number of topological covers of a compact Riemann surface with specified degree and branch points. It also yields a proof of Theorem 1.2 in the case where the curve $\phi^n(x) = y^m$ is irreducible for all $n \geq 1$.

It is interesting to consider whether a similar conclusion to that of Conjecture 1.6 holds for $X = \mathbb{P}^j$ with $j \geq 1$, where Y is a projective variety and λ is finite onto its image; indeed, one can extend the question further to the case where X and Y are any quasi-projective varieties, and ϕ is an endomorphism of X. To see why such a generalization of Conjecture 1.6 is plausible, let Z_n $(n \geq 1)$ be the subvariety of $X \times Y$ where the morphisms $\phi^n\colon X \to X$ and $\lambda\colon Y \to X$ agree. Then there is a natural K-morphism $Z_{n+1} \to Z_n$ taking (x, y) to $(\phi(x), y)$, which we again denote by ϕ. Thus, for any $i > j$ there is a finite map $\phi^{i-j}\colon Z_i(K) \to Z_j(K)$. Suppose that $O_\phi^+(a) \cap \lambda(Y(K))$ is infinite; otherwise, the conclusion of Conjecture 1.6 holds trivially, as in the paragraph following Theorem 1.5. Thus, $O_\phi^+(a)$ must be infinite, and hence $\phi^i(a) \neq \phi^j(a)$ for $i \neq j$. We label the next observation for future reference:

$$\text{(1.8)}\quad \text{for any fixed } n \geq 1, \qquad \text{there are infinitely many } i > n \text{ with } \phi^n\big(\phi^{i-n}(a)\big) \in \lambda\big(Y(K)\big),$$

implying that there are infinitely many points in $Z_n(K)$ for all $n \geq 1$. If these points are Zariski-dense in Z_n, then the Bombieri–Lang conjecture [12, Conjecture F.5.2.1] predicts that Z_n is not a variety of general type. We speculate that under suitable hypotheses this implies a functional relationship among iterates of ϕ and λ, for instance $\phi^r = \lambda \circ g$ for some $r \geq 1$ and some K-morphism $g\colon X \to Y$.

The previous paragraph furnishes an outline for our proof of Theorem 1.5. In the situation of that theorem, Z_n is a curve, and thus any infinite subset is Zariski dense, and the Bombieri–Lang conjecture is Faltings' famous theorem [14, Corollary 2.2, p. 12] (see [12, Theorem E.0.1] for an exposition of the number field case). We are

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

left with the problem of determining for which maps ϕ the curve Z_n is not of general type, *i.e,* when $g_n \leq 1$ for all $n \geq 1$. Theorem 1.1 gives the desired functional relationship under the hypothesis that $\deg \phi \geq 2$, and a close analysis of the various cases encountered in the proof of Theorem 1.1 gives the bound of three arithmetic progressions found in Theorem 1.5, together with the information on M.

We close this introduction with three additional results related to Corollary 1.3. Denote by K^m the set $\{k^m : k \in K\}$.

Corollary 1.7 *Let K be a finitely generated field of characteristic zero and let $\phi \in K(x)$ have degree $d \geq 2$. Suppose that there exists $a \in \mathbb{P}^1(K)$ with $O^+_\phi(a) \cap \mathbb{P}^1(K)^m$ infinite, for some $m \geq 5$ with $m \mid d$. Then $\phi(x) = (\psi(x))^m$ for some $\psi \in K(x)$.*

Corollary 1.7 follows immediately from Corollary 1.3 and the observation that if $\phi(x) = c(\psi(x))^m$ with $c \notin K^m$, then for all $a \in K$, $O^+_\phi(a) \cap \mathbb{P}^1(K)^m \subseteq \{a, 0, \infty\}$, and thus is finite.

When ϕ is a polynomial, we can give a particularly concrete version of Corollary 1.3.

Corollary 1.8 *Let K be a finitely generated field of characteristic zero, let $\phi \in K[x]$ have degree $d \geq 2$, and fix $m \geq 2$. If there exists $a \in \mathbb{P}^1(K)$ with $O^+_\phi(a) \cap K^m$ infinite, then one of the following holds:*

(i) *$\phi(x) = cx^j(g(x))^m$ for some $g \in K[x]$, $0 \leq j \leq m-1$, and $c \in K^*$;*

(ii) *$m = 2$ and there is $c \in K^*$ such that $c\phi(x/c)$ is*

$$(-1)^d (T_d(x+2)) - 2, \tag{1.9}$$

where T_d is the degree-d monic Chebyshev polynomial.

Note that cases (i) and (ii) of Corollary 1.8 are mutually exclusive, unlike the cases in Theorem 1.2. Indeed, for all $d \geq 2$, we have that T_d maps -2 to $2 \cdot (-1)^d$ with multiplicity 1, implying that the map in case (ii) maps -4 to 0 with multiplicity 1, and hence is not of the form given in case (i). The polynomials of the form (1.9) are conjugates of T_d that contain 0 in their post-critical set but do not belong to case (i). For $d = 2, 3, 4, 5$ these maps are: $x(x+4), -(x+4)(x+1)^2, x(x+4)(x+2)^2$, and $-(x+4)(x^2+3x+1)^2$, respectively.

Our final corollary shows that when $K = \mathbb{Q}$ and $\deg \phi = 2$, we obtain very strong consequences when there is $a \in \mathbb{Q}$ with $O^+_\phi(a) \cap \mathbb{Q}^2$ infinite.

Corollary 1.9 *A quadratic polynomial $\phi \in \mathbb{Q}[x]$ has a rational orbit containing infinitely many distinct squares if and only if either*

(i) *ϕ is the square of a linear polynomial with rational coefficients, or*

(ii) *$\phi(x) = cx^2 + 4x$ with $c \in \mathbb{Q}^*$.*

The paper is organized as follows. Sections 2–5 contain the geometric portion of the proofs of Theorems 1.1 and 1.2. In Section 2 we study the genera of irreducible components of super-elliptic curves, and show in Corollary 2.5 that g_n remains bounded

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

as n grows if and only if 0 and ∞ satisfy a ramification condition on iterated preimages that we call m-branch abundance (see Definition 2.1). We also show that if g_n is unbounded, then it grows exponentially with n (Theorem 2.6). In Section 3, we study rational functions with two m-branch abundant points in $\mathbb{P}^1(\mathbb{C})$ when $m \geq 5$. In Section 4 we study ramification among iterated preimages of m-branch abundant points when m is prime, with a view to understanding the most complicated cases $m = 2$ and $m = 3$; this culminates in two classification results (Theorems 4.6 and 4.7). In Section 5 we study maps with two 4-branch abundant points. In Section 6 we give the results that handle the arithmetic portion of the proofs of Theorems 1.1 and 1.2. In Section 7 we state useful results of Milnor [15] on Lattès maps, and combine them with material from the five previous sections to prove Theorem 1.2. In Section 8 we give the proof of Theorem 1.1, which involves checking numerous cases. In Section 9 we give the proofs of the remaining results from the introduction. In Section 10 we present the example mentioned after Theorem 1.5.

2 m-branch Abundant Points and the Genus of $\phi^n(x) = y^m$

Recall from the discussion before Theorem 1.2 the definition of the ramification index $e_\phi(z)$ of a rational function $\phi \in \mathbb{C}(x)$ at $z \in \mathbb{P}^1(\mathbb{C})$. We refer to $z \in \mathbb{P}^1(\mathbb{C})$ as a *ramification point* for ϕ if $e_\phi(z) > 1$. An easy argument on compositions of power series gives the following special case of the chain rule for ramification indices (see [4, Section 2.5]):

$$e_{\phi^n}(z) = \prod_{i=0}^{n-1} e_\phi(\phi^i(z)), \tag{2.1}$$

and hence $e_{\phi^n}(z)$ "remembers" the ramification of the map ϕ at each of $z, \phi(z), \dots, \phi^{n-1}(z)$. An essential tool throughout this paper comes in the form of the Riemann–Hurwitz formula (see *e.g.*, [4, Section 2.7] for a proof):

$$\sum_{z \in \mathbb{P}^1(\mathbb{C})} (e_\phi(z) - 1) = 2d - 2.$$

For $\alpha \in \mathbb{C}$, $\phi \in \mathbb{C}(x)$, and $n \geq 0$, we use the standard notation of $\phi^{-n}(\alpha)$ to denote the set $\{\beta \in \mathbb{C} : \phi^n(\beta) = \alpha\}$. We introduce the following terminology.

Definition 2.1 Fix $m \geq 2$, let $\phi \in \mathbb{C}(x)$ be non-constant, and let $\alpha \in \mathbb{P}^1(\mathbb{C})$. Define $\rho_n(\alpha)$ to be the number of $z \in \phi^{-n}(\alpha)$ with $e_{\phi^n}(z)$ not divisible by m. We say that α is *m-branch abundant* for ϕ if $\rho_n(\alpha)$ is bounded as $n \to \infty$.

Note that if $m_1 \mid m_2$, then $m_1 \nmid e_{\phi^n(z)}$ implies $m_2 \nmid e_{\phi^n(z)}$, and hence if and α is m_2-branch abundant for ϕ, then α is also m_1-branch abundant for ϕ. We remark that in [11], the authors call $\alpha \in \mathbb{P}^1(\mathbb{C})$ *dynamically ramified* for ϕ if the set $\bigcup_{n \geq 1} \{z \in \phi^{-n}(\alpha) : e_{\phi^n}(z) = 1\}$ is finite. The definition of an m-branch abundant point is weaker in that it only considers $z \in \phi^{-n}(\alpha)$ with $m \nmid e_{\phi^n}(z)$, and, moreover, it only asserts a bounded number of such points as n grows, rather than finiteness of the full set of such points as n varies.

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

A primary goal of this section is to establish a relationship between the existence of m-branch abundant points for ϕ and the genus of (irreducible factors of) $C_n : \phi^n(x) = y^m$. For curves of this form, the irreducible factors are easily found.

Proposition 2.2 *Let C be the curve defined (over $\mathbb{C}$) by $\psi(x) = y^m$, where $\psi(x) = c\prod_{i=1}^{k}(x - \alpha_i)^{e_i} \in \mathbb{C}(x)$ and $e_i \in \mathbb{Z} \smallsetminus \{0\}$ for all i. Let a be the greatest positive integer dividing m and all the e_i, and put $\lambda(x) = \sqrt[a]{c}\prod_{i=1}^{k}(x - \alpha_i)^{e_i/a} \in \mathbb{C}(x)$ for some fixed choice of $\sqrt[a]{c}$. Let ζ_a be a primitive a-th root of unity. Then the irreducible factors of C are the curves*

$$y^{m/a} = \zeta_a^k \lambda(x), \qquad k = 0, \ldots, a-1. \tag{2.2}$$

Proof We show that each curve is irreducible, and then it follows by comparing the degrees in y that they must comprise all the irreducible components of C. By assumption, $\zeta_a^k\lambda(x)$ is not a p-th power in $\mathbb{C}(x)$ for any prime p dividing m, and it follows that $y^{m/a} - \zeta_a^k\lambda(x)$ is irreducible as a polynomial in y, whence each of the curves in (2.2) is irreducible. ■

We can determine the genus of every curve of the form (2.2) quite explicitly.

Proposition 2.3 *Let C and a be as in Proposition 2.2, and put $m' = m/a$ and $e_i' = e_i/a$. Then every irreducible factor of C has the same genus g, given by*

$$g = 1 + \Big(\frac{k-1}{2}\Big)m' - \frac{1}{2}\Big(\gcd(m', e_1' + \cdots + e_k') + \sum_{i=1}^{k}\gcd(m', e_i')\Big). \tag{2.3}$$

Proof This follows from a straightforward application of Proposition 2.2 and a genus formula for irreducible curves given by variables-separated rational functions, first used by Ritt [19]. The first explicit statement and proof of the formula in the general situation seems to be [8, Proposition 2]; for another statement and proof, see [6, Proposition 4.1]. Many other authors have used various versions of this formula, *e.g.*, [3, Proposition 2.6] and [18, Corollary 2.1]. Another proof of this proposition can be given by noting that the genus of each irreducible factor is equal to the genus of the function field $\mathbb{C}(x, \sqrt[m']{\lambda(x)})$. Then one can directly apply the formula in [23, Proposition 3.7.3] for the genus of a Kummer extension of function fields. ■

Corollary 2.4 *Let g be as in Proposition 2.3, and denote by t the number of $i \in \{1, \ldots, k\}$ such that $m \nmid e_i$. If $t = 0$, then $g = 0$, and if $t > 0$, then*

$$\lceil (t/2) - 1 \rceil \le g \le (m-1)(t-1)/2, \tag{2.4}$$

where $\lceil \cdot \rceil$ denotes the ceiling function.

Remark The bounds are sharp, as evidenced by the hyperelliptic curves $y^2 = x^t - 1$.

Proof First note that $t = 0$ if and only if $m' = 1$, and in this case (2.3) reduces to $g = 0$. Assume now that $t \ge 1$ and $m' \ge 2$. If $m \nmid e_i$, then $m' \nmid e_i'$, giving us

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

$\gcd(m', e'_i) \le m'/2$. From (2.3), we obtain

$$g \ge 1 + \Big(\frac{k-1}{2}\Big)m' - \frac{1}{2}\Big(m'(1+(k-t)) + t\frac{m'}{2}\Big) = 1 + m'\Big(\frac{t}{4} - 1\Big), \tag{2.5}$$

with equality if and only if $m' \mid e'_1 + \cdots + e'_k$ and $\gcd(m', e'_i) = m'/2$ for each i with $m' \nmid e'_i$. Because $m' \ge 2$, (2.5) gives $g \ge (t/2) - 1$. This establishes the lower bound of (2.4) when t is even. Assume then that t is odd. Then if (2.5) is an equality, we have $\gcd(m', e'_i) = m'/2$ for an odd number of values of i and $\gcd(m', e'_i) = m'$ for the rest. Thus $e'_1 + \cdots + e'_k \equiv m'/2 \bmod m'$, and therefore $m' \nmid (e'_1 + \cdots + e'_k)$, a contradiction. We have shown that (2.5) is a strict inequality, giving $g > (t/2) - 1$. As g is an integer, we conclude $g \ge \lceil (t/2) - 1 \rceil$.

To prove the upper bound of (2.4), note that (2.3) gives

$$g \le 1 + \Big(\frac{k-1}{2}\Big)m' - \frac{1}{2}\Big(m'(k-t) + t + 1\Big) = \frac{(m'-1)(t-1)}{2} \le \frac{(m-1)(t-1)}{2},$$

as desired. ■

Write $\phi^n(x) = c\prod_{i=1}^k (x - \alpha_i)^{e_i}$, and take t_n to be the number of $i \in \{1, \dots, k\}$ such that $m \nmid e_i$. Then t_n is closely related to the quantity $\rho_n(0) + \rho_n(\infty)$, where ρ_n is defined in Definition 2.1. Indeed, $\rho_n(0) + \rho_n(\infty) = t_n$ unless $\infty \in \phi^{-n}(\infty) \cup \phi^{-n}(0)$ and $m \nmid e_{\phi^n}(\infty)$, in which case $\rho_n(0) + \rho_n(\infty) = t_n + 1$. We thus obtain the following corollary.

Corollary 2.5 *Let $\phi \in \mathbb{C}(x)$ have degree $d \ge 2$. For $n \ge 1$, let C_n be the curve defined (over $\mathbb{C}$) by $\phi^n(x) = y^m$, let g_n be the genus of every irreducible factor of C_n, and put $\rho_n(\phi) := \rho_n(0) + \rho_n(\infty)$, where $\rho_n(0)$ and $\rho_n(\infty)$ are as in Definition 2.1. Then either $\rho_n(\phi) = g_n = 0$ or*

$$\lceil (\rho_n(\phi) - 3)/2 \rceil \le g_n \le (m-1)(\rho_n(\phi) - 1)/2.$$

In particular, g_n is bounded as $n \to \infty$ if and only if both 0 and ∞ are m-branch abundant for ϕ.

A consequence of Corollary 2.5 is a result on the growth rate of g_n as $n \to \infty$ in the case where g_n is unbounded.

Theorem 2.6 *Let ϕ, C_n, and g_n be as in Corollary 2.5. If g_n is unbounded as $n \to \infty$, then $g_n \ge \kappa d^n$ for some constant κ.*

Proof Because g_n is unbounded, we have that $\rho_n(\phi)$ is unbounded, and without loss of generality say that $\rho_n(0)$ is unbounded. If $\rho_n(\phi) \ge \kappa d^n$, then after possibly adjusting κ the same conclusion holds for g_n, whence it suffices to give an exponential lower bound for $\rho_n(0)$.

Because $\rho_n(0)$ is unbounded, the set

$$Z = \Big\{ z \in \mathbb{P}^1(\mathbb{C}) : \phi^k(z) = 0 \text{ and } m \nmid e_{\phi^k}(z) \text{ for some } k \ge 1 \Big\}$$

is infinite. Observe that $O^+_\phi(0) \cap Z$ must be finite: if 0 is periodic, then $O^+_\phi(0)$ is itself finite, while if 0 is not periodic, then $O^+_\phi(0) \cap Z = \varnothing$. Consider the set

$$R = \Big\{ c \in \mathbb{P}^1(\mathbb{C}) : e_\phi(c) > 1 \text{ and } \phi^i(c) = 0 \text{ for some } i \ge 0 \Big\}.$$

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

Now $O^+_\phi(c) \smallsetminus O^+_\phi(0)$ is finite for each $c \in R$, and as $O^+_\phi(0) \cap Z$ is finite, we have that $O^+_\phi(c) \cap Z$ is finite. But R is finite by Riemann–Hurwitz, and thus $\bigcup_{c \in R} O^+_\phi(c)$ contains only finitely many elements of Z. Therefore, there exists $z \in Z$ that is not in the orbit of any ramification point of ϕ. From the definition of Z, $\phi^k(z) = 0$ for some $k \geq 1$. Then for all $n \geq k$, $\rho_n(0) \geq (\frac{1}{d^k})(d^n)$, furnishing the desired exponential lower bound. ∎

Observe that when combined with Theorem 1.1, Theorem 2.6 yields the result that the sequence $(g_n)_{n \geq 1}$ is either bounded by 1 or grows exponentially.

3 Maps with Two m-branch Abundant Points, $m \geq 5$

We begin with a definition and proposition that will be useful in proving Theorem 1.2.

Definition 3.1 For a fixed integer $m \geq 2$, rational function $\phi \in \mathbb{C}(x)$, and distinct $\alpha_1, \alpha_2 \in \mathbb{P}^1(\mathbb{C})$, we call ϕ *m-trivial with respect to* $\{\alpha_1, \alpha_2\}$ if we have $m \mid e_\phi(z)$ for all $z \in \phi^{-1}(\{\alpha_1, \alpha_2\}) \smallsetminus \{\alpha_1, \alpha_2\}$.

Proposition 3.2 *For any integer $m \geq 2$, a rational function $\phi \in \mathbb{C}(x)$ is m-trivial with respect to $\{0, \infty\}$ if and only if it is of the form*

$$cx^j(\psi(x))^m \qquad \text{with } \psi(x) \in \mathbb{C}(x),\ 0 \leq j \leq m-1, \text{ and } c \in \mathbb{C}^*.$$

Proof Let ϕ be m-trivial with respect to $\{0, \infty\}$. For each $z \in \phi^{-1}(0) \smallsetminus \{0, \infty\}$, the factor $(x - z)$ appears in the numerator of ϕ with multiplicity $e_\phi(z)$. The same holds for $z \in \phi^{-1}(\infty) \smallsetminus \{0, \infty\}$ and the denominator of ϕ. Letting $U = \phi^{-1}(0) \smallsetminus \{0, \infty\}$ and $V = \phi^{-1}(\infty) \smallsetminus \{0, \infty\}$, we can write

$$\phi(x) = c \cdot x^j \cdot \frac{\prod_{u \in U}(x-u)^m}{\prod_{v \in V}(x-v)^m}$$

for some $c \in \mathbb{C}^*$ (we cannot have $c = 0$, since ϕ is non-constant). Thus, $\phi(x) = cx^j\psi(x)^m$ with $\psi(x) = \prod_{u \in U}(x-u) / \prod_{v \in V}(x-v)$. If necessary, we can absorb m-th powers of x into $(\psi(x))^m$, allowing us to assume $0 \leq j \leq m-1$.

Suppose now that $\phi(x) = cx^j(\psi(x))^m$. Then $m \mid e_{\phi(z)}$ for all

$$z \in \phi^{-1}(\{0, \infty\}) \smallsetminus \{0, \infty\},$$

and it follows that ϕ is m-trivial with respect to $\{0, \infty\}$. ∎

In light of Proposition 3.2 and Corollary 2.5, in order to prove Theorem 1.2 we wish to show that in many cases a map for which 0 and ∞ are m-branch abundant must in fact be m-trivial with respect to $\{0, \infty\}$. The purpose of this section is to prove this in the case $m \geq 5$, which is done in Theorem 3.8. There is no special advantage to assuming that ϕ has 0 and ∞ as m-branch abundant points, and so we assume only that ϕ has two distinct m-branch abundant points α_1 and α_2.

We begin with several preparatory lemmas, which will be of use in later sections as well as this one. The first shows that when m is a prime power, m-branch abundance of $\alpha \in \mathbb{P}^1(\mathbb{C})$ propagates to certain iterated preimages of α.

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

Lemma 3.3 *Let $\phi \in \mathbb{C}(x)$ and p be prime. Suppose that $\alpha \in \mathbb{P}^1(\mathbb{C})$ is p^r-branch abundant for ϕ, where $r \geq 1$, and let $\beta \in \mathbb{P}^1(\mathbb{C})$ satisfy $\phi^k(\beta) = \alpha$ for some $k \geq 1$. If $p^r \nmid e_{\phi^k}(\beta)$, then β is p-branch abundant for ϕ. Furthermore, if $p \nmid e_\phi(\phi^i(\beta))$ for each $i = 0, 1, \dots, k-1$, then β is p^r-branch abundant for ϕ.*

Proof Consider $z \in \phi^{-n}(\beta)$, implying in particular that $z \in \phi^{-(n+k)}(\alpha)$. Note that

$$e_{\phi^{n+k}}(z) = e_{\phi^k}\big(\phi^n(z)\big) \cdot e_{\phi^n}(z) = e_{\phi^k}(\beta) \cdot e_{\phi^n}(z). \tag{3.1}$$

If $p^r \nmid e_{\phi^k}(\beta)$, then (3.1) and the primality of p give

$$\#\{z \in \phi^{-n}(\beta) : p \nmid e_{\phi^n}(z)\} \leq \#\{z \in \phi^{-(n+k)}(\alpha) : p^r \nmid e_{\phi^{n+k}}(z)\}. \tag{3.2}$$

Because α is p^r-branch abundant, the right-hand side of (3.2) is bounded as n grows, and thus β is p-branch abundant.

If $p \nmid e_\phi(\phi^i(\beta))$ for $i = 0, 1, \dots, k-1$, then $p \nmid e_{\phi^k}(\beta)$ by (2.1). Arguing as in the previous paragraph, it follows that β is p^r-branch abundant. ■

For $\alpha \in \mathbb{P}^1(\mathbb{C})$ and $\phi \in \mathbb{C}(x)$, we often wish to consider the union of the sets $\phi^{-n}(\alpha)$ for $n \geq 0$. We thus introduce the following standard definition.

Definition 3.4 Let $\phi \in \mathbb{C}(x)$ and $\alpha \in \mathbb{P}^1(\mathbb{C})$. The *backwards orbit* of α under ϕ is

$$O_\phi^-(\alpha) := \{\beta \in \mathbb{P}^1(\mathbb{C}) : \text{there exists } n \geq 0 \text{ with } \phi^n(\beta) = \alpha\}.$$

For $S \subset \mathbb{P}^1(\mathbb{C})$, the backwards orbit $O_\phi^-(S)$ of S is the union of $O_\phi^-(\alpha)$ over $\alpha \in S$.

Note that, as in the case with forward orbits, we have $\alpha \in O_\phi^-(\alpha)$.

The next lemma is crucial in our analysis. We often apply it to a preimage of a p-branch abundant point, and hence we use β instead of α in the statement.

Lemma 3.5 *Let S be a finite subset of $\mathbb{P}^1(\mathbb{C})$, and suppose that $\phi \in \mathbb{C}(x)$, p is prime, and $\beta \in \phi^{-1}(S) \setminus S$ is p-branch abundant for ϕ. Then there exists $y \in O_\phi^-(\beta)$ satisfying the following conditions:*

(i) *If $n \geq 0$ is minimal such that $\phi^n(y) = \beta$, then $S \cap \{y, \phi(y), \dots, \phi^n(y)\}$ is empty.*
(ii) *$p \mid e_\phi(z)$ for all $z \in \phi^{-1}(y) \setminus S$.*

Moreover, suppose that there are distinct $\{\beta_1, \dots, \beta_k\} \subseteq \phi^{-1}(S) \setminus S$ and (not necessarily distinct) primes $p_1, \dots, p_k$ such that for all $i = 1, \dots, k$, we have that β_i is p_i-branch abundant for ϕ, and y_i satisfies conditions (i) *and* (ii) *with respect to β_i and S. Then $y_i \neq y_j$ for all $i \neq j$.*

Proof If each $z \in \phi^{-1}(\beta) \setminus S$ satisfies $p \mid e_\phi(z)$, then we can take $y = \beta$ (note $\beta \notin S$ by assumption). Otherwise, construct a (possibly finite) sequence $\gamma_1, \gamma_2, \dots$ in $\mathbb{P}^1(\mathbb{C})$ as follows. Choose $\gamma_1 \in \phi^{-1}(\beta) \setminus S$ with $p \nmid e_\phi(\gamma_1)$. If γ_i is chosen for $i \geq 1$, then select $\gamma_{i+1} \in \phi^{-1}(\gamma_i) \setminus S$ with $p \nmid e_\phi(\gamma_{i+1})$. If no such γ_{i+1} exists, then the sequence terminates with γ_i, and thus we can take $y = \gamma_i$ to satisfy conditions (i) and (ii) of the theorem.

By construction, $\gamma_i \notin S$ for all i. Therefore, all the γ_i are distinct, for if $\gamma_i = \gamma_j$ for $i > j$, then γ_i is periodic under ϕ and its orbit is $\{\gamma_i, \gamma_{i-1}, \dots, \gamma_{j+1}\}$. But $\gamma_i \in O_\phi^-(S)$,

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

and so $O_\phi^+(\gamma_i)$ intersects S, implying that $\gamma_\ell \in S$ for some $j < \ell \le i$, which is a contradiction.

It thus suffices to show that the set $\{\gamma_i : i \ge 1\}$ is finite. Note that by Lemma 3.3, each γ_i is p-branch abundant for ϕ. Consider the set R of all $c \in \mathbb{P}^1(\mathbb{C})$ with $e_\phi(c) > 1$ and $c \in O_\phi^-(S)$. Observe that

$$\bigcup_{c\in R} O_\phi^+(c) \subseteq \Big(\bigcup_{c \in R} \big(O_\phi^+(c) \smallsetminus O_\phi^+(S) \big) \Big) \cup O_\phi^+(S), \tag{3.3}$$

where $O_\phi^+(S) = \bigcup_{s\in S} O_\phi^+(s)$. Now for each $c \in R$, we have that $O_\phi^+(c) \smallsetminus O_\phi^+(S)$ is finite, since $c \in O_\phi^-(S)$. We claim that only finitely many of the γ_i lie in $O_\phi^+(S)$. Otherwise, the finiteness of S and the pigeonhole principle imply that infinitely many of the γ_i lie in a single orbit $O_\phi^+(s)$ for some $s \in S$. Because each γ_i maps into S under enough iterations of ϕ, the orbit $O_\phi^+(s)$ visits S infinitely often. The finiteness of S then gives $\phi^{n_1}(s) = \phi^{n_2}(s)$ for some $n_1 \ne n_2$, and hence $O_\phi^+(s)$ is finite, contradicting our supposition that it contains infinitely many γ_i. Now from (3.3) we have that only finitely many of the γ_i lie in $\bigcup_{c\in R} O_\phi^+(c)$. This implies there are only finitely many γ_i, since otherwise there is some γ_i with no ramification point of ϕ in $O_\phi^-(\gamma_i)$, contradicting the p-branch abundance of γ_i.

To prove the last assertion of the lemma, assume to the contrary that $\gamma_i = \gamma_j$ for some $i \ne j$. Let $n_i \ge 0$ be minimal such that $\phi^{n_i}(\gamma_i) = \beta_i$ and let $n_j \ge 0$ be minimal such that $\phi^{n_j}(\gamma_j) = \beta_j$. Since $\gamma_i = \gamma_j$, we cannot have $n_i = n_j$, for then $\beta_i = \beta_j$. Assume without loss of generality that $n_i > n_j$, and note that $\gamma_i = \gamma_j$ implies

$$\begin{aligned}\big\{\beta_j, \phi(\beta_j), \dots \phi^{n_i - n_j}(\beta_j)\big\} &= \big\{\phi^{n_j}(\gamma_i), \phi^{n_j+1}(\gamma_i), \dots \phi^{n_i}(\gamma_i)\big\} \\ &\subseteq \big\{\gamma_i, \phi(\gamma_i), \dots, \phi^{n_i}(\gamma_i)\big\}.\end{aligned}$$

But $S \cap \{\gamma_i, \phi(\gamma_i), \dots, \phi^{n_i}(\gamma_i)\} = \varnothing$ by condition (i). Because $n_i - n_j \ge 1$, we have $\phi(\beta_j) \notin S$, a contradiction. ∎

Our next preparatory lemma is an elementary lower bound on ramification indices.

Lemma 3.6 *Let $m \in \mathbb{Z}$ with $m \ge 2$, let T be a finite subset of $\mathbb{P}^1(\mathbb{C})$ with $\#T = t$, and let $\phi \in \mathbb{C}(x)$ have degree $d \ge 2$. Let $U = \{z \in \phi^{-1}(T) : m \nmid e_\phi(z)\}$, and put $u = \#U$. Then*

$$\sum_{z\in\phi^{-1}(T)} (e_\phi(z) - 1) \ge (dt - u)\Big(\frac{m-1}{m}\Big),$$

where equality holds if and only if $e_\phi(z) \in \{1, m\}$ for all $z \in \phi^{-1}(T)$.

Proof Let $U' = \phi^{-1}(T) \smallsetminus U$. Because $\sum_{z\in\phi^{-1}(w)} e_\phi(z) = d$ for all $w \in \mathbb{P}^1(\mathbb{C})$, we have

$$\begin{aligned} dt = \sum_{z\in\phi^{-1}(T)} e_\phi(z) &= \sum_{z\in U} e_\phi(z) + \sum_{z\in U'} e_\phi(z) \\ &= \sum_{z \in U} (e_\phi(z) - 1) + u + m\Big(\sum_{z\in U'} (r_z - 1) + \#U'\Big),\end{aligned}$$

from which we have that $\#U' \le \frac{dt-u}{m}$, with equality if and only if $e_\phi(z) = 1$ for all $z \in U$ and $r_z = 1$ for all $z \in U'$. The lemma then follows from the observation that

$$\sum_{z\in\phi^{-1}(T)} \big(e_\phi(z)-1\big) = dt - \#\big(\phi^{-1}(T)\big) = dt - u - \#U'. \qquad \blacksquare$$

Let α_1 and α_2 be m-branch abundant points for ϕ. Put

$$B = \big\{\beta \in \mathbb{P}^1(\mathbb{C}) : \beta \in \phi^{-1}(\{\alpha_1,\alpha_2\}) \smallsetminus \{\alpha_1,\alpha_2\}, m \nmid e_\phi(\beta)\big\}. \tag{3.4}$$

From Definition 3.1, one sees immediately that ϕ is m-trivial with respect to $\{\alpha_1,\alpha_2\}$ if and only if B is empty. Now because $m \nmid e_\phi(\beta)$ for each $\beta \in B$, there must be some prime p_β and some $r \ge 1$ with $p_\beta^r \mid m$, but $p_\beta^r \nmid e_\phi(\beta)$. Because α_1 and α_2 are m-branch abundant, they are also p_β^r-branch abundant, and so by Lemma 3.3, β is p_β-branch abundant. We can then apply Lemma 3.5 with $S = \{\alpha_1,\alpha_2\}$ to find for each $\beta \in B$ some $y_\beta \in O_\phi^-(\beta)$ with $p_\beta \mid e_\phi(z)$ for each $z \in \phi^{-1}(y_\beta) \smallsetminus \{\alpha_1,\alpha_2\}$. We then set

$$Y = \{y_\beta : \beta \in B\}. \tag{3.5}$$

By the last assertion of Lemma 3.5, Y has the same number of elements as B.

Lemma 3.7 *Let $m \in \mathbb{Z}$ with $m \ge 2$, let $\phi \in \mathbb{C}(x)$ have degree $d \ge 2$, and let $\alpha_1,\alpha_2 \in \mathbb{P}^1(\mathbb{C})$ be distinct m-branch abundant points for ϕ. Let B and Y be as in (3.4) and (3.5), respectively. Put $b = \#B$ and $\ell_Y = \#(\phi^{-1}(Y) \cap \{\alpha_1,\alpha_2\})$. Then*

$$b(dm-2m+2) + \ell_Y(m-2) \le 4d-4.$$

Proof Let p be the smallest prime dividing m, so $p_\beta \ge p$ for all $\beta \in B$. By Lemma 3.5 we have $\#Y = \#B = b$. Applying Lemma 3.6 with $T = Y$ yields

$$\sum_{z\in\phi^{-1}(Y)} (e_\phi(z)-1) \ge (bd-\ell_Y)\Big(\frac{p-1}{p}\Big) \ge \frac{bd-\ell_Y}{2}.$$

Now let $u_i = \#\{z \in \phi^{-1}(\alpha_i) : m \nmid e_\phi(z)\}$ for $i \in \{1,2\}$. Note that $\#\phi^{-1}(\alpha_i) \le u_i + (d-u_i)/m$, whence

$$\sum_{z\in\phi^{-1}(\alpha_i)} (e_\phi(z)-1) = d - \#\phi^{-1}(\alpha_i) \ge d - \Big(u_i + \frac{d-u_i}{m}\Big).$$

By Lemma 3.5(i), we have that $Y \cap \{\alpha_1,\alpha_2\} = \varnothing$. Hence, $\#(\phi^{-1}(\{\alpha_1,\alpha_2\}) \cap \{\alpha_1,\alpha_2\}) \le 2 - \ell_Y$, and it follows that $u_1 + u_2 \le b + 2 - \ell_Y$. Thus,

$$\begin{aligned}
2d-2 = \sum_{z\in\mathbb{P}^1(\mathbb{C})} (e_\phi(z)-1) &\ge \sum_{z\in\phi^{-1}(\{\alpha_1,\alpha_2\}\cup Y)} \big(e_\phi(z)-1\big)\\
&\ge d - \Big(u_1 + \frac{d-u_1}{m}\Big) + d - \Big(u_2 + \frac{d-u_2}{m}\Big) + \frac{bd-\ell_Y}{2}\\
&= \big(2d - (u_1+u_2)\big)\frac{m-1}{m} + \frac{bd-\ell_Y}{2}\\
&\ge \big(2d - (b+2-\ell_Y)\big)\frac{m-1}{m} + \frac{bd-\ell_Y}{2}.
\end{aligned}$$

Multiplying through by $2m$ and regrouping terms yields the desired inequality. ■

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

We now prove the main theorem of this section.

Theorem 3.8 *Let $m \in \mathbb{Z}$ with $m \geq 5$. Then every rational function $\phi \in \mathbb{C}(x)$ with two m-branch abundant points α_1, α_2 in $\mathbb{P}^1(\mathbb{C})$ is m-trivial with respect to $\{\alpha_1, \alpha_2\}$.*

Proof We use the notation of Lemma 3.7, and assume $b \geq 1$ in order to derive a contradiction. If $\ell_Y \geq 1$, then applying Lemma 3.7 with $m \geq 5$ gives $b(5d - 8) + 3 \leq 4d - 4$. But $b \geq 1$, so this yields $5d - 5 \leq 4d - 4$, which is impossible, because $d \geq 2$.

If $\ell_Y = 0$, then Lemma 3.7 and $b \geq 1$ give $5d - 8 \leq 4d - 4$, which implies $d \leq 4$. Hence, $m > d$, implying $\phi^{-1}(\{\alpha_1, \alpha_2\}) \subseteq B \cup \{\alpha_1, \alpha_2\}$, and therefore $\#\phi^{-1}(\{\alpha_1, \alpha_2\}) \leq b + 2$. Moreover, since $\ell_Y = 0$, for each $y_\beta \in Y$, all elements of $\phi^{-1}(y_\beta)$ must have ramification index divisible by p_β, and in particular every element of $\phi^{-1}(Y)$ has ramification index greater than 1. When $d = 3$, this implies $e_\phi(z) = 3$ for all $z \in \phi^{-1}(Y)$, while for $d = 4$ we have $e_\phi(z) \geq 2$ for all $z \in \phi^{-1}(Y)$. In either case, $\sum_{z \in \phi^{-1}(Y)} (e_\phi(z) - 1) \geq 2b$. Hence for $d \in \{3, 4\}$, we obtain

$$\sum_{z \in \phi^{-1}(Y \cup \{\alpha_1, \alpha_2\})} \big(e_\phi(z) - 1 \big) \geq \big(2d - (b + 2) \big) + (2b) = 2d - 2 + b.$$

Because $b \geq 1$ we have a contradiction to the Riemann–Hurwitz formula. When $d = 2$, we have only $\sum_{z \in \phi^{-1}(Y)} (e_\phi(z) - 1) \geq b$, and so

$$\sum_{z \in \phi^{-1}(Y \cup \{\alpha_1, \alpha_2\})} \big(e_\phi(z) - 1 \big) \geq \big(2d - (b + 2) \big) + b = 2d - 2.$$

Hence, the inequality $\#\phi^{-1}(\{\alpha_1, \alpha_2\}) \geq b + 2$ is in fact an equality, and it follows that $\phi^{-1}(\{\alpha_1, \alpha_2\}) = B \cup \{\alpha_1, \alpha_2\}$. In particular, $\phi(\{\alpha_1, \alpha_2\}) \subseteq \{\alpha_1, \alpha_2\}$, implying that $O_\phi^+(\{\alpha_1, \alpha_2\}) \subseteq \{\alpha_1, \alpha_2\}$. Thus no element of B can be periodic under ϕ, for otherwise $B \cap O_\phi^+(\{\alpha_1, \alpha_2\}) \neq \varnothing$, contradicting the fact that by definition $B \cap \{\alpha_1, \alpha_2\} = \varnothing$. Now let $\beta \in B$, and for $n \geq 1$, let $\gamma_n \in \phi^{-n}(\beta)$. Because β is not periodic under ϕ, we must have that $\gamma_n, \phi(\gamma_n), \dots, \phi^n(\gamma_n)$ are all distinct. But

$$e_{\phi^n}(\gamma_n) = \prod_{i=0}^{n-1} e_\phi(\phi^i(\gamma_n)),$$

and there can be at most two i with $e_\phi(\phi^i(\gamma_n)) = 2$, with $e_\phi(\phi^i(\gamma_n)) = 1$ for the rest. It follows that $e_{\phi^n}(\gamma_n) \leq 4$. This holds for arbitrary n and γ_n, and thus β cannot be m-branch abundant, because $m \geq 5$. This contradiction completes the proof of the theorem. ∎

4 Preimage Trees of p-branch Abundant Points

In this section we study m-fold ramification among preimages of an m-branch abundant point.

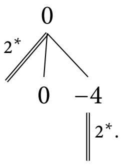
Definition 4.1 Fix $m \in \mathbb{Z}$ with $m \geq 2$, $\phi \in \mathbb{C}(x)$, and $\alpha \in \mathbb{P}^1(\mathbb{C})$. Given $z \in \mathbb{P}^1(\mathbb{C})$, denote by $r_\phi(z)$ the unordered tuple whose entries are $e_\phi(y)$ as y varies over $\phi^{-1}(z)$. For $n \geq 0$, let S_n be the set of $z \in \phi^{-n}(\alpha)$ with $m \nmid e_{\phi^n}(z)$. The *m-ramification* *structure of* $O^-_\phi(\alpha)$ is

$$\bigsqcup_{n\geq 0}\left\{(z, r_\phi(z)) : z \in S_n\right\}.$$

For example, let T_6 be the degree-6 monic Chebyshev polynomial, let $m = 2$, $\phi(x) = T_6(x+2) - 2$, and $\alpha = 0$. Then $S_0 = \{0\}$, $S_n = \{-4, 0\}$ for all $n \geq 1$, and the 2-ramification structure of $O^-_\phi(0)$ is

$$\begin{aligned}\{(0,(1,1,2,2))\} &\sqcup \{(-4,(2,2,2)),(0,(1,1,2,2))\} \\ &\sqcup \{(-4,(2,2,2)),(0,(1,1,2,2))\} \sqcup \cdots \end{aligned} \tag{4.1}$$

It is often convenient to represent m-ramification structures pictorially. We do this by constructing a diagram whose n-th row consists of the elements of S_n, and where a line between $\gamma \in S_{n+1}$ and $\beta \in S_n$ indicates that $\phi(\gamma) = \beta$. We label such a line with $e_\phi(\gamma)$ in the case where $e_\phi(\gamma) > 1$. To eliminate clutter, we indicate with a double line labeled by n (resp. n^*) a set of points each of which has ramification index divisible by n (resp. exactly n). To further simplify our diagrams, we omit repetition when it does not add novel information, such as when S_{n+1} is identical to S_n. For example, a diagram representing the 2-ramification structure in (4.1) is



If we replace the two occurrences of 2^* by 2, then the resulting diagram still describes the 2-ramification structure in (4.1), though it also describes others, *e.g.*,

$$\begin{aligned}\{(0,(1,1,2,4,6))\} &\sqcup \{(-4,(4,4,6)),(0,(1,1,2,4,6))\} \\ &\sqcup \{(-4,(4,4,6)),(0,(1,1,2,4,6))\} \sqcup \cdots \end{aligned}$$

The main goal of this section is to study maps $\phi \in \mathbb{C}(x)$ for which 0 and ∞ are m-branch abundant with $m \in \{2,3\}$, which we do in Theorems 4.6 and 4.7. Our main tool is a classification of the p-ramification structures of $O^-_\phi(\alpha)$, where p is prime and α is a p-branch abundant point for ϕ. This is done in Theorems 4.3 and 4.5.

Lemma 4.2 *Let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, let p be a prime with $p \nmid d$, and suppose that $\alpha \in \mathbb{P}^1(\mathbb{C})$ is p-branch abundant for ϕ. Then α is periodic under ϕ and there is exactly one $\beta \in \phi^{-1}(\alpha)$ with $p \nmid e_\phi(\beta)$. Moreover, β must be p-branch abundant for ϕ, and β must lie in $O^+_\phi(\alpha)$.*

Proof Because $p \nmid d$, there must be at least one $\beta \in \phi^{-1}(\alpha)$ with $p \nmid e_\phi(\beta)$. If $\beta = \alpha$, then evidently α is periodic under ϕ and $\beta \in O^+_\phi(\alpha)$. Assume $\beta \in \phi^{-1}(\alpha) \smallsetminus \{\alpha\}$. By Lemma 3.3 we have that β is p-branch abundant for ϕ. Applying Lemma 3.5 with $S = \{\alpha\}$, there exists $y \in O^-_\phi(\beta)$ with $p \mid e_\phi(z)$ for each $z \in \phi^{-1}(y) \smallsetminus \{\alpha\}$. If $\alpha \notin \phi^{-1}(y)$, then from $d = \sum_{z\in\phi^{-1}(y)} e_\phi(z)$ we have $p \mid d$, contrary to assumption. Hence, $\phi(\alpha) = y$, and so α is periodic under ϕ and $\beta \in O^+_\phi(\alpha)$.

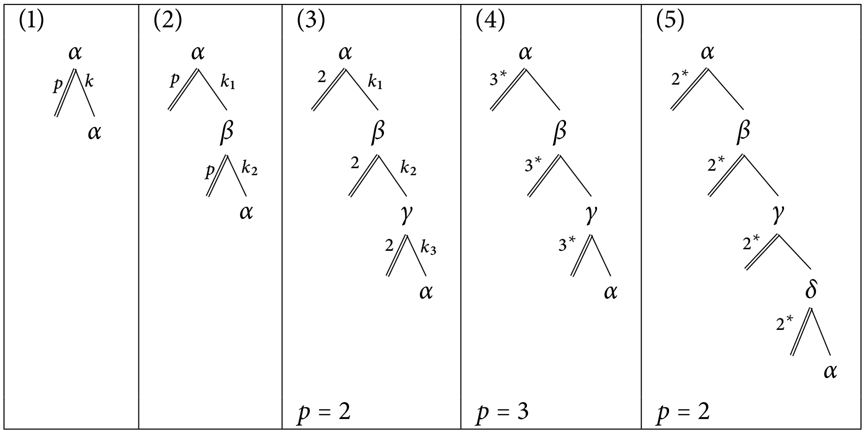


Figure 1

It remains to show that β is the unique element of $\phi^{-1}(\alpha)$ with ramification index not divisible by p. If β' is another such element, then by the previous paragraph we have $\beta' \in O^+_\phi(\alpha)$. Thus, both β and β' lie in the cycle C to which α belongs. But the action of ϕ on C is one-to-one, so $\phi(\beta) = \alpha = \phi(\beta')$ implies $\beta = \beta'$. ■

Theorem 4.3 *Let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, let p be a prime with $p \nmid d$, and suppose that $\alpha \in \mathbb{P}^1(\mathbb{C})$ is p-branch abundant for ϕ. Then the p-ramification structure for $O^-_\phi(\alpha)$ is one of those in Figure 1, where k_1, k_2, and k_3 are positive integers not divisible by p, and points named with distinct letters within a given diagram are distinct.*

Proof Put $\alpha_1 = \alpha$, and note that by Lemma 4.2 there is a unique $\alpha_2 \in \phi^{-1}(\alpha_1)$ with $p \nmid e_\phi(\alpha_{i+1})$ and $\alpha_2 \in O^+_\phi(\alpha_1)$. By Lemma 3.3 we have that α_2 is p-branch abundant for ϕ, and so we can apply Lemma 4.2 to α_2. Continuing in this fashion, we obtain a sequence $(\alpha_i)_{i\geq 1}$ in $\mathbb{P}^1(\mathbb{C})$ of p-branch abundant points for ϕ that satisfy $\phi(\alpha_{i+1}) = \alpha_i$ and $\alpha_{i+1} \in O^+_\phi(\alpha_i)$ for all $i \geq 1$. The latter condition implies $O^+_\phi(\alpha_{i+1}) \subseteq O^+_\phi(\alpha_i)$ for all $i \geq 1$, and so $O^+_\phi(\alpha_{i+1}) \subseteq O^+_\phi(\alpha_1)$, implying $\alpha_{i+1} \in O^+_\phi(\alpha_1)$. But Lemma 4.2 shows that α_1 is periodic under ϕ. Hence, $\alpha_i = \alpha_j$ for some $i > j$, which implies that $\alpha_1 = \alpha_{i-j+1}$. Let $n > 0$ be minimal such that $\alpha_1 = \alpha_{n+1}$. Note that $n = 1$ gives p-ramification structure (1), while $n = 2$ gives p-ramification structure (2).

Assume that $n \geq 3$. Applying Lemma 3.6 with $T = \{\alpha_i\}$ and summing over i yields

$$\sum_{i=1}^{n} \sum_{z \in \phi^{-1}(\alpha_i)} (e_\phi(z) - 1) \geq n(d-1)\frac{(p-1)}{p} \geq 3(d-1)\frac{(p-1)}{p}. \tag{4.2}$$

If $p > 3$, we obtain a contradiction to Riemann–Hurwitz. If $p = 3$, then we obtain a similar contradiction unless both the inequalities in (4.2) are equalities. This holds only when $n = 3$ and $e_\phi(z) \in \{1, 3\}$ for all $z \in \phi^{-1}(\alpha_i)$, the latter by Lemma 3.6. This gives p-ramification structure (4). If $p = 2$, then $n(d-1)(p-1)/p = (n/2)(d-1)$, and

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

(4.2) contradicts Riemann–Hurwitz unless $n \le 4$. The case $n = 3$ gives p-ramification structure (3). If $n = 4$, then the first inequality in (4.2) must be an equality, and hence we have equality in Lemma 3.6 with $T = \{\alpha_i\}$. The latter happens if and only if $e_\phi(z) \in \{1, 2\}$ for all $z \in \phi^{-1}(\alpha_i)$, which gives p-ramification structure (5). ■

We now move to the more complicated case where $p \mid d$. The following lemma is of central importance both in this section and in subsequent sections.

Lemma 4.4 *Let $\phi \in \mathbb{C}(x)$ have degree $d \ge 2$. If $p > 3$ is prime, then ϕ has at most two p-branch abundant points in $\mathbb{P}^1(\mathbb{C})$. Moreover, ϕ has at most three 3-branch abundant points in $\mathbb{P}^1(\mathbb{C})$, and at most four 2-branch abundant points in $\mathbb{P}^1(\mathbb{C})$. If ϕ possesses a set V of three 3-branch abundant points (resp. four 2-branch abundant points), then all ramification points of ϕ lie in $\phi^{-1}(V)$, and $e_\phi(z) \in \{1, 3\}$ (resp. $e_\phi(z) \in \{1, 2\}$) for all $z \in \mathbb{P}^1(\mathbb{C})$.*

Proof Let p be prime, and let $V = V_0 = \{\alpha_1, \dots, \alpha_k\} \subset \mathbb{P}^1(\mathbb{C})$ be a set of distinct p-branch abundant points for ϕ. For $i \ge 1$, put $V_i = \{z \in \phi^{-1}(V_{i-1}) : p \nmid e_\phi(z)\}$. Observe that V_i consists of all $z \in \phi^{-i}(V_0)$ with $p \nmid e_{\phi^i}(z)$, and in particular, $\#V_i = \sum_{n=1}^{k} \rho_i(\alpha_n)$ (notation as in Definition 2.1). By the p-branch abundance of the α_i, we have that $(\#V_i)_{i \ge 0}$ is bounded. Hence, the sequence cannot be strictly increasing, and so there is $j \ge 1$ with $\#V_j \le \#V_{j-1}$. Assume that j is minimal with this property. Because $\#V_0 = k$, the minimality of j ensures that $\#V_{j-1} \ge k$. Apply Lemma 3.6 with $T = V_{j-1}$ to get

$$\begin{aligned}(4.3)\qquad \sum_{z \in \phi^{-1}(V_{j-1})} \big(e_\phi(z) - 1\big) &\ge \big((\#V_{j-1})d - \#V_j\big)\frac{p-1}{p} \\ &\ge (\#V_{j-1})(d-1)\frac{p-1}{p} \ge k(d-1)\frac{p-1}{p}.\end{aligned}$$

If $p > 3$, then Riemann–Hurwitz implies $k \le 2$. If $p = 3$ (resp. $p = 2$), then Riemann–Hurwitz implies $k \le 3$ (resp. $k \le 4$). If $p = k = 3$ or $p = 2, k = 4$, then by Riemann-Hurwitz again we have equality throughout (4.3). In particular, we have $\#V_{j-1} = k$, and the minimality of j then gives $j = 1$. Equality in (4.3) also implies equality in Lemma 3.6 with $T = V_{j-1} = V$, and thus $e_\phi(z) \in \{1, p\}$ for all $z \in \phi^{-1}(V)$. Finally, (4.3) gives $\sum_{z \in \phi^{-1}(V)} (e_\phi(z) - 1) = 2d - 2$, implying that all ramification points for ϕ lie in $\phi^{-1}(V)$, and hence $e_\phi(z) \in \{1, p\}$ for all $z \in \mathbb{P}^1(\mathbb{C})$. ■

Theorem 4.5 *Let $\phi \in \mathbb{C}(x)$ have degree $d \ge 2$, let p be a prime with $p \mid d$, and suppose that $\alpha \in \mathbb{P}^1(\mathbb{C})$ is p-branch abundant for ϕ. Then the p-ramification structure for $O_\phi^-(\alpha)$ is one of those in Figure 2, where points named with distinct letters within a given diagram are distinct.*

Proof For any $z \in \mathbb{P}^1(\mathbb{C})$, we define

$$u(z) = \#\big\{\beta \in \phi^{-1}(z) : p \nmid e_\phi(\beta)\big\},$$
$$u_0(z) = \#\big\{\beta \in \phi^{-1}(z) \smallsetminus \{z\} : p \nmid e_\phi(\beta)\big\}.$$

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

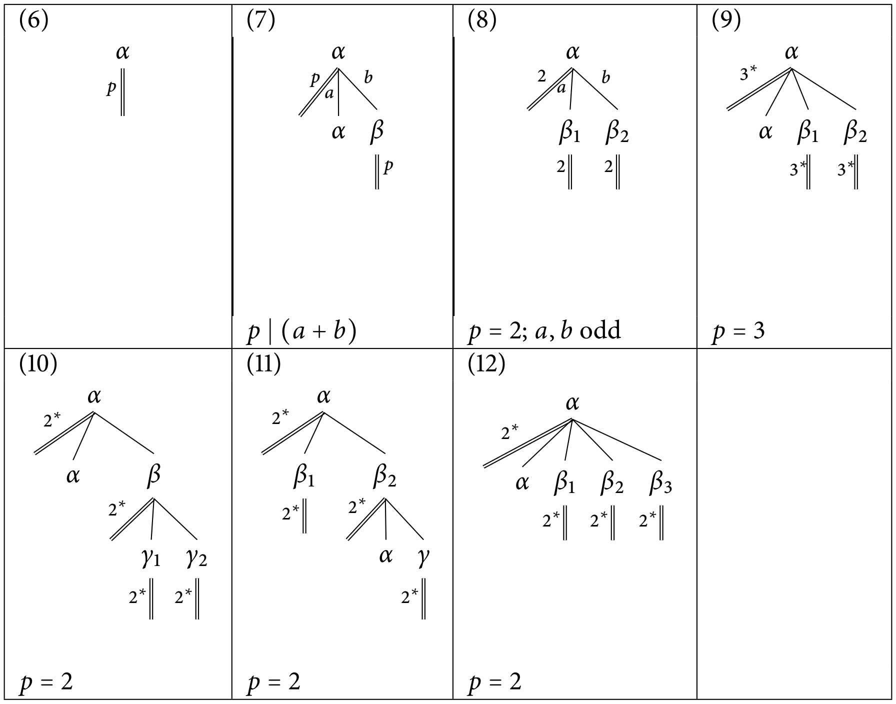


Figure 2

Note that $u(z) = u_0(z)$ or $u(z) = u_0(z) + 1$, with the latter holding if and only if $\phi(z) = z$ and $p \nmid e_\phi(z)$. We frequently use the observation that $p \mid d$ implies $u(z) \neq 1$ for all $z \in \mathbb{P}^1(\mathbb{C})$. For example, if $u_0(\alpha) = 0$, then $u(\alpha) \leq 1$, and so because $p \mid d$, we have $u(\alpha) = 0$, which gives p-ramification structure (6).

Case 1a: Let $p \geq 3$ and $u_0(\alpha) \geq 2$. Because α is p-branch abundant, Lemma 3.3 yields the same conclusion for $\beta \in \phi^{-1}(\alpha) \smallsetminus \{\alpha\}$ with $p \nmid e_\phi(\beta)$. If $u_0(\alpha) \geq 3$, we thus have a set of four distinct p-branch abundant points for ϕ, contradicting Lemma 4.4. Thus $u_0(\alpha) = 2$, and we let β_1, β_2 be the two elements of $\phi^{-1}(\alpha) \smallsetminus \{\alpha\}$ with ramification index not divisible by p. Then $V = \{\alpha, \beta_1, \beta_2\}$ is a set of three p-branch abundant points for ϕ, and by Lemma 4.4 this implies $p = 3$ and $e_\phi(z) \in \{1, 3\}$ for all $z \in \phi^{-1}(V)$. In particular, we have $e_\phi(\beta_1) = e_\phi(\beta_2) = 1$. Because $3 \mid d$, we must have $\alpha \in \phi^{-1}(\alpha)$ and $3 \nmid e_\phi(\alpha)$, whence $e_\phi(\alpha) = 1$. Now from Lemma 4.4, V contains all 3-branch abundant points for ϕ, and it follows from Lemma 3.3 that $e_\phi(z) = 3$ for all $z \in \phi^{-1}(V) \smallsetminus V$. But $V \cap \phi^{-1}(\{\beta_1, \beta_2\}) = \varnothing$, for otherwise applying ϕ gives $\alpha \in \{\beta_1, \beta_2\}$. Hence $e_\phi(z) = 3$ for all $z \in \phi^{-1}(\{\beta_1, \beta_2\})$, giving 3-ramification structure (9).

Case 1b: Let $p \geq 3$ and $u_0(\alpha) = 1$. Let β be the unique element of $\phi^{-1}(\alpha) \smallsetminus \{\alpha\}$ with $p \nmid e_\phi(\beta)$. Because $p \mid d$ we have $u(\alpha) = 2$, whence $\phi(\alpha) = \alpha$. From Lemma 3.3 we have that β is p-branch abundant for ϕ. By our work in Case 1a, $u_0(\beta) = 2$ implies

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

that $\phi(\beta) = \beta$, contradicting $\alpha \neq \beta$. If $u_0(\beta) = 1$, then because $p \mid d$, we have $u(\beta) = 2 > u_0(\beta)$, and so $\phi(\beta) = \beta$, again a contradiction. Thus we have $u_0(\beta) = 0$, and therefore $u(\beta) = 0$, giving p-ramification structure (7).

Case 2a: Let $p = 2$ and $u_0(\alpha) \geq 3$. Arguing similarly to Case 1a, we must have $u_0(\alpha) = 3$. Let $\beta_1, \beta_2, \beta_3$ be the three elements of $\phi^{-1}(\alpha) \setminus \{\alpha\}$ with odd ramification index. Then $V = \{\alpha, \beta_1, \beta_2, \beta_3\}$ is a set of four 2-branch abundant points for ϕ, and by Lemma 4.4 this implies $e_\phi(z) \in \{1, 2\}$ for all $z \in \phi^{-1}(V)$. Because d is even, we must have $\alpha \in \phi^{-1}(\alpha)$ and $2 \nmid e_\phi(\alpha)$, whence $e_\phi(\alpha) = 1$. Lemma 4.4 shows that V contains all 2-branch abundant points for ϕ, and it follows from Lemma 3.3 that $e_\phi(z) = 2$ for all $z \in \phi^{-1}(V) \setminus V$. But $V \cap \phi^{-1}(\{\beta_1, \beta_2, \beta_3\}) = \varnothing$, for otherwise applying ϕ gives $\alpha \in \{\beta_1, \beta_2, \beta_3\}$. Hence, $e_\phi(z) = 2$ for all $z \in \phi^{-1}(\{\beta_1, \beta_2, \beta_3\})$, giving 2-ramification structure (12).

Case 2b: Let $p = 2$ and $u_0(\alpha) = 2$. The latter implies $u(\alpha) \in \{2, 3\}$, but $u(\alpha)$ must be even because d is, giving $u(\alpha) = 2$ and hence $\alpha \notin \phi^{-1}(\alpha)$. Let β_1, β_2 be the two elements of $\phi^{-1}(\alpha) \setminus \{\alpha\}$ with odd ramification index. Note that β_1 and β_2 are both 2-branch abundant by Lemma 3.3, and so Lemma 4.4 implies $u_0(\beta_i) \leq 3$ for $i = 1, 2$. Moreover, neither of the β_i can have $u_0(\beta_i) = 3$, because then $\phi(\beta_i) = \beta_i$ by Case 2a, giving a contradiction.

Suppose that $u_0(\beta_i) = 2$ for some i (say without loss of generality $i = 2$), and let z_1, z_2 be the elements of $\phi^{-1}(\beta_2) \setminus \{\beta_2\}$ with odd ramification index. Then $V = \{\alpha, \beta_1, \beta_2, z_1, z_2\}$ is a set of 2-branch abundant points for ϕ, and Lemma 4.4 gives $\#V \leq 4$. But $\#\{\beta_1, \beta_2, z_1, z_2\} = 4$ and $\alpha \notin \{\beta_1, \beta_2\}$ by construction, whence $\alpha \in \{z_1, z_2\}$. Without loss of generality say $\alpha = z_1$. Because $\#V = 4$, Lemma 4.4 shows that $e_\phi(z) \in \{1, 2\}$ for all $z \in \phi^{-1}(V)$. Lemma 4.4 also shows that V contains all 2-branch abundant points for ϕ, and it follows from Lemma 3.3 that $e_\phi(z) = 2$ for all $z \in \phi^{-1}(V) \setminus V$. Note that $\phi(V) = \{\alpha, \beta_2\}$, and so if $V \cap \phi^{-1}(\{\beta_1, z_2\}) \neq \varnothing$, then applying ϕ gives $\{\beta_1, z_2\} \cap \{\alpha, \beta_2\} \neq \varnothing$, which is impossible. Hence, $e_\phi(z) = 2$ for all $z \in \phi^{-1}(\{\beta_1, z_2\})$, which gives 2-ramification structure (11).

Suppose that $u_0(\beta_i) \leq 1$ for $i = 1, 2$. Because $\beta_i \neq \alpha$, we have $\phi(\beta_i) \neq \beta_i$, and thus $u(\beta_i) = u_0(\beta_i)$ for $i = 1, 2$. Because $2 \mid d$, we cannot have $u(\beta_i) = 1$, which proves that $u(\beta_1) = u(\beta_2) = 0$. This gives 2-ramification structure (8).

Case 2c: Let $p = 2$ and $u_0(\alpha) = 1$. Then there exists a unique $\beta \in \phi^{-1}(\alpha) \setminus \{\alpha\}$ with $e_\phi(\beta)$ odd. Because $u(\alpha) \neq 1$, we must have $u(\alpha) > u_0(\alpha)$, implying that $\phi(\alpha) = \alpha$ and $e_\phi(\alpha)$ is odd. Note that $u_0(\beta) \leq 3$ by Lemma 4.4. If $u_0(\beta) = 3$, then by Case 2a we have $\phi(\beta) = \beta$, contradicting $\beta \neq \alpha$. We also cannot have $u_0(\beta) = 1$, for then $u(\beta) = 2$, and so again $\phi(\beta) = \beta$. If $u_0(\beta) = 0$, we have 2-ramification structure (7).

Suppose then that $u_0(\beta) = 2$, and let γ_1, γ_2 be the two elements of $\phi^{-1}(\beta) \setminus \{\beta\}$ with odd ramification index. Note that $\alpha \notin \{\gamma_1, \gamma_2\}$, for otherwise $\phi(\alpha) = \alpha$ gives the contradiction $\beta = \alpha$. Thus, $V = \{\alpha, \beta, \gamma_1, \gamma_2\}$ is a set of four 2-branch abundant points for ϕ, and Lemma 4.4 shows that $e_\phi(z) \in \{1, 2\}$ for all $z \in \phi^{-1}(V)$. Lemma 4.4 also shows that V contains all 2-branch abundant points for ϕ, and it follows from Lemma 3.3 that $e_\phi(z) = 2$ for all $z \in \phi^{-1}(V) \setminus V$. Note that $\phi(V) = \{\alpha, \beta\}$, and so if $V \cap \phi^{-1}(\{\gamma_1, \gamma_2\}) \neq \varnothing$, then applying ϕ gives $\{\gamma_1, \gamma_2\} \cap \{\alpha, \beta\} \neq \varnothing$, which is impossible. Hence, $e_\phi(z) = 2$ for all $z \in \phi^{-1}(\{\gamma_1, \gamma_2\})$, which gives 2-ramification structure (10). ∎

If $\alpha \in \mathbb{P}^1(\mathbb{C})$ is p-branch abundant for $\phi \in \mathbb{C}(x)$, define

$$Ab(\alpha) = \bigcup_{n \geq 1} \{z \in \phi^{-n}(\alpha) : p \nmid e_{\phi^n}(z)\},$$

and note that by Lemma 3.3, $Ab(\alpha)$ consists of p-branch abundant points for ϕ. In the notation of Theorems 4.3 and 4.5, the named points in each p-ramification structure comprise $Ab(\alpha)$. Note that it follows from Lemma 3.3 that if α_1 and α_2 are p-branch abundant points for ϕ and $\alpha_2 \in Ab(\alpha_1)$, then $Ab(\alpha_2) \subseteq Ab(\alpha_1)$. If $\alpha_1, \dots, \alpha_n$ are p-branch abundant points for ϕ, we write $Ab(\alpha_1, \dots, \alpha_n)$ for $\bigcup_{i=1}^n Ab(\alpha_i)$.

Theorem 4.6 *Let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, and assume that $A = \{\alpha_1, \alpha_2\} \subset \mathbb{P}^1(\mathbb{C})$ is a set of distinct 3-branch abundant points for ϕ. Suppose that ϕ is not 3-trivial with respect to A, and let μ be a Möbius transformation exchanging α_1 and α_2. Then for either ϕ or $\mu \circ \phi \circ \mu^{-1}$, one of the following holds.*

(3A) *$O^-_\phi(\alpha_1)$ has 3-ramification structure (4), $\alpha_2 \in Ab(\alpha_1)$, and $\phi(\alpha_2) = \alpha_1$;*

(3B) *$O^-_\phi(\alpha_1)$ (resp. $O^-_\phi(\alpha_2)$) has 3-ramification structure (2) (resp. (1)), and $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$;*

(3C) *$O^-_\phi(\alpha_1)$ has 3-ramification structure (9), $\alpha_2 \in Ab(\alpha_1)$, and $\phi(\alpha_2) = \alpha_1$.*

Moreover, in all cases we have

$$\text{(4.4)} \quad \textit{all ramification points of } \phi \textit{ lie in } \phi^{-1}(Ab(\alpha_1, \alpha_2)), \quad \textit{and } e_\phi(z) \in \{1, 3\} \textit{ for all } z \in \mathbb{P}^1(\mathbb{C}).$$

Remark The conditions in (4.4) are invariant under Möbius conjugation, and thus hold for both ϕ and $\mu \circ \phi \circ \mu^{-1}$.

Proof Let $O^-_\phi(\alpha_1)$ have 3-ramification structure (a) and $O^-_\phi(\alpha_1)$ have 3-ramification structure (b), where we use the numbering of Theorems 4.3 and 4.5. Replacing ϕ with $\mu \circ \phi \circ \mu^{-1}$ if necessary, we assume that $a \geq b$. In the case where $a = b$, clearly it is not necessary to replace ϕ by $\mu \circ \phi \circ \mu^{-1}$ in order to obtain $a \geq b$, and so we are free to make this replacement for other purposes. Because ϕ is assumed to be non-3-trivial with respect to A, we must have $a \notin \{1, 6\}$.

Suppose first that $3 \nmid \deg \phi$. If $a = 4$, then $Ab(\alpha_1)$ contains three 3-branch abundant points for ϕ, and hence by Lemma 4.4 we have that $\alpha_2 \in Ab(\alpha_1)$ and (4.4) holds. Because $Ab(\alpha_1)$ consists of a 3-cycle, we can replace ϕ with $\mu \circ \phi \circ \mu^{-1}$ if necessary to obtain $\phi(\alpha_2) = \alpha_1$. This gives (3A). Suppose that $a = b = 2$, and note that $Ab(\alpha_i)$ is invariant under ϕ for $i = 1, 2$. It follows that either $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$ or $Ab(\alpha_1) = Ab(\alpha_2)$. The former contradicts Lemma 4.4, while the latter implies that ϕ is 3-trivial with respect to A. This leaves us with $a = 2$ and $b = 1$. In this case $\phi(\alpha_2) = \alpha_2$, and so $Ab(\alpha_2) \cap Ab(\alpha_1) = \varnothing$, which is (3B). Lemma 4.4 then gives that (4.4) holds.

Suppose now that $3 \mid \deg \phi$. If $a = 9$, then $Ab(\alpha_1)$ contains three 3-branch abundant points for ϕ, and hence by Lemma 4.4 we have $\alpha_2 \in Ab(\alpha_1)$ and (4.4) holds. Replacing ϕ by $\mu \circ \phi \circ \mu^{-1}$ if necessary, we have $\phi(\alpha_2) = \alpha_1$, giving (3C). If $a = b = 7$, then both α_1 and α_2 are fixed points of ϕ, and thus $Ab(\alpha_1)$ and $Ab(\alpha_2)$ are disjoint, contradicting Lemma 4.4. If $a = 7, b = 6$, and $\alpha_2 \notin Ab(\alpha_1)$, then Lemma 4.4 gives

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

$e_\phi(z) \in \{1,3\}$ for all $z \in \mathbb{P}^1(\mathbb{C})$, and in particular, $d = \sum_{z\in\phi^{-1}(\alpha_1)} e_\phi(z) \equiv 2 \bmod 3$, contrary to supposition. Hence, $\alpha_2 \in Ab(\alpha_1)$, implying that ϕ is 3-trivial with respect to A. ∎

Theorem 4.7 *Let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, and assume that $A = \{\alpha_1, \alpha_2\} \subset \mathbb{P}^1(\mathbb{C})$ is a set of distinct 2-branch abundant points for ϕ. Suppose that ϕ is not 2-trivial with respect to A, and let μ be a Möbius transformation exchanging α_1 and α_2. Then for either ϕ or $\mu \circ \phi \circ \mu^{-1}$, one of the following holds:*

(2A) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (5), *$\alpha_2 \in Ab(\alpha_1)$, and $\phi(\alpha_2) = \alpha_1$;*

(2B) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (5), *$\alpha_2 \in Ab(\alpha_1)$, $\phi(\alpha_2) \neq \alpha_1$, and $\phi^2(\alpha_2) = \alpha_1$;*

(2C) *$O^-_\phi(\alpha_1)$ (resp. $O^-_\phi(\alpha_2)$) has 2-ramification structure* (3) *(resp.* (1)*), and $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$;*

(2D) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (3), *$\alpha_2 \in Ab(\alpha_1)$, and $\phi(\alpha_2) = \alpha_1$;*

(2E) *$O^-_\phi(\alpha_1)$ and $O^-_\phi(\alpha_1)$ have*

(2F) *$O^-_\phi(\alpha_1)$ (resp. $O^-_\phi(\alpha_2)$) has 2-ramification structure* (2) *(resp.* (1)*), and $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$;*

(2G) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (12), *$\alpha_2 \in Ab(\alpha_1)$, and $\phi(\alpha_2) = \alpha_1$;*

(2H) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (11), *$\alpha_2 \in Ab(\alpha_1)$, $\phi(\alpha_2) = \alpha_1$, and $\phi(\alpha_1) = \alpha_2$;*

(2I) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (11), *$\alpha_2 \in Ab(\alpha_1)$, $\phi(\alpha_2) = \alpha_1$, and $\phi(\alpha_1) \neq \alpha_2$;*

(2J) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (11), *$\alpha_2 \in Ab(\alpha_1)$, $\phi(\alpha_2) \neq \alpha_1$, and $\phi^2(\alpha_2) = \alpha_1$;*

(2K) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (10), *$\alpha_2 \in Ab(\alpha_1)$, and $\phi(\alpha_2) = \alpha_1$;*

(2L) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (10), *$\alpha_2 \in Ab(\alpha_1)$, $\phi(\alpha_2) \neq \alpha_1$, and $\phi^2(\alpha_2) = \alpha_1$;*

(2M) *$O^-_\phi(\alpha_1)$ has 2-ramification structure* (8), *$\alpha_2 \in Ab(\alpha_1)$, and $\phi(\alpha_2) = \alpha_1$;*

(2N) *$O^-_\phi(\alpha_1)$ and $O^-_\phi(\alpha_1)$ have 2-ramification structure* (7), *and $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$;*

(2O) *$O^-_\phi(\alpha_1)$ (resp. $O^-_\phi(\alpha_2)$) has 2-ramification structure* (7) *(resp.* (6)*), and $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$.*

Moreover, in all cases except (2D), (2F), (2M), *and* (2O), *we have*

$$\text{(4.5)} \quad \textit{all ramification points of } \phi \textit{ lie in } \phi^{-1}(Ab(\alpha_1, \alpha_2)), \\ \textit{and } e_\phi(z) \in \{1,2\} \textit{ for all } z \in \mathbb{P}^1(\mathbb{C}).$$

Proof Similarly to the proof of Theorem 4.6, we let $O^-_\phi(\alpha_1)$ have 2-ramification structure (1) and $O^-_\phi(\alpha_1)$ have 2-ramification structure (2), and we assume that $a \geq b$. Because ϕ is assumed to be non-2-trivial with respect to A, we must have $a \notin \{1,6\}$.

Suppose that $2 \nmid \deg \phi$. If $a = 5$, then $Ab(\alpha_1)$ contains four 2-branch abundant points for ϕ, and hence by Lemma 4.4, we have that $\alpha_2 \in Ab(\alpha_1)$ and (4.4) holds. Replacing ϕ with $\mu \circ \phi \circ \mu^{-1}$ if necessary, we have either $\phi(\alpha_2) = \alpha_1$ or $\phi(\alpha_2) \neq \alpha_1$ and $\phi^2(\alpha_2) = \alpha_1$, giving (2A) and (2B), respectively.

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

If $a = 3$, then observe that $b \in \{1,2,3\}$, and it follows that both $Ab(\alpha_1)$ and $Ab(\alpha_2)$ are invariant under ϕ. If $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$, then from Lemma 4.4 we must have that $b = 1$ and (4.5) holds. This gives (2C). If $Ab(\alpha_1) \cap Ab(\alpha_2) \neq \varnothing$, then the invariance of $Ab(\alpha_1)$ and $Ab(\alpha_2)$ under ϕ implies $\alpha_2 \in Ab(\alpha_1)$, and hence $b = 3$. Replacing ϕ by $\mu \circ \phi \circ \mu^{-1}$ if necessary, we have $\phi(\alpha_2) = \alpha_1$. This is (2D).

If $a = b = 2$, then as in the previous paragraph, we have that $Ab(\alpha_i)$ is invariant under ϕ for $i = 1,2$. It follows that either $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$ or $Ab(\alpha_1) = Ab(\alpha_2)$. In the former case, Lemma 4.4 shows that (4.5) holds, giving (2E). In the latter case, ϕ is 2-trivial with respect to A. This leaves us with $a = 2$ and $b = 1$. In this case $\phi(\alpha_2) = \alpha_2$, and so $Ab(\alpha_2) \cap Ab(\alpha_1) = \varnothing$, which is (2F).

Suppose now that $2 \mid \deg \phi$. If $a \in \{10, 11, 12\}$, then $Ab(\alpha_1)$ contains four 2-branch abundant points for ϕ, and hence by Lemma 4.4 we have $\alpha_2 \in Ab(\alpha_1)$ and (4.4) holds. If $a = 12$, then because $\alpha_1 \neq \alpha_2$, we must have $\phi(\alpha_2) = \alpha_1$, and so (2G) holds. If $a = 11$ and $\phi(\alpha_2) = \alpha_1$, then either both α_1 and α_2 lie in the 2-cycle that is part of 2-ramification structure (11), or only α_1 lies in said 2-cycle. These give (2H) and (2I), respectively. If $a = 11$ and $\phi(\alpha_2) \neq \alpha_1$, then α_1 and $\phi(\alpha_2)$ must lie in the 2-cycle that is part of 2-ramification structure (11), and thus $\phi^2(\alpha_2) = \alpha_1$, giving (2J). If $a = 10$, then we clearly have either (2K) or (2L).

If $a = 8$ and $Ab(\alpha_1) \cap Ab(\alpha_2) = \varnothing$, then from Lemma 4.4 we have $b = 6$. Then applying Lemma 3.6 with $T = Ab(\alpha_1) \cup Ab(\alpha_2)$ gives

$$\sum_{z \in \phi^{-1}(T)} (e_\phi(z) - 1) \geq \frac{4d-2}{2} > 2d - 2.$$

Hence, $\alpha_2 \in Ab(\alpha_1)$, and necessarily $\phi(\alpha_2) = \alpha_1$, giving (2M).

If $a = b = 7$, then both α_1 and α_2 are fixed points of ϕ, and thus $Ab(\alpha_1)$ and $Ab(\alpha_2)$ are disjoint. By Lemma 4.4, we have that (4.5) holds, giving (2N). If $a = 7, b = 6$, and $Ab(\alpha_2) \cap Ab(\alpha_1) \neq \varnothing$, then $\alpha_2 \in Ab(\alpha_1)$, implying that ϕ is 2-trivial with respect to A. If $Ab(\alpha_2) \cap Ab(\alpha_1) \neq \varnothing$, we have (2O). ■

5 Maps with Two m-branch Abundant Points, $m = 4$

In this section we study rational functions with two 4-branch abundant points α_1 and α_2. In Theorem 5.3, we show that either such a map is 4-trivial with respect to $\{\alpha_1, \alpha_2\}$ (see Definition 3.1), or the 4-ramification structure of $O_\phi^-(\alpha_1)$ has a very restricted form, and in particular $\alpha_2 \in Ab(\alpha_1)$ with $\phi(\alpha_2) = \alpha_1$. This is done in Theorem 5.3.

Theorem 5.1 *Suppose $\phi \in \mathbb{C}(x)$ has degree d with d odd, and let $\alpha_1, \alpha_2 \in \mathbb{P}^1(\mathbb{C})$ be distinct 4-branch abundant points for ϕ. Then ϕ is 4-trivial with respect to $\{\alpha_1, \alpha_2\}$.*

Proof Any point α that is 4-branch abundant for ϕ is also 2-branch abundant for ϕ, and by the classification of 2-branch abundant points (Theorem 4.3), α must be periodic with its orbit consisting only of points with odd ramification index. If $w \in \phi^{-1}(\alpha)$ has ramification index divisible by 2 but not by 4, then by Lemma 3.3 we have that w is 2-branch abundant, and hence by Theorem 4.3, w must be periodic. But then $w \in O_\phi^+(\alpha)$, and the evenness of $e_\phi(w)$ gives a contradiction. Furthermore, again by Theorem 4.3, $\phi^{-1}(\alpha)$ must have a unique element with odd ramification index.

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

Thus, there is $x_\alpha \in \phi^{-1}(\alpha)$ with odd ramification index such that every member of $\phi^{-1}(\alpha) \smallsetminus \{x_\alpha\}$ has ramification index divisible by 4.

Suppose now that α_1, α_2, and α_3 are distinct 4-branch abundant points for ϕ. By Lemma 3.6, we have

$$\sum_{c \in \phi^{-1}(\{\alpha_1,\alpha_2,\alpha_3\})} \big(e_\phi(c) - 1\big) \geq 3\big((d-1)(3/4)\big) = \frac{9}{8}(2d-2) > 2d-2,$$

contradicting Riemann–Hurwitz. Hence, if α_1 and α_2 are distinct 4-branch abundant for ϕ, they are the only such points. Now x_{α_1} and x_{α_2} are also 4-branch abundant, and hence $\{x_{\alpha_1}, x_{\alpha_2}\} = \{\alpha_1, \alpha_2\}$. Therefore, $\phi^{-1}(\{\alpha_1,\alpha_2\}) \smallsetminus \{\alpha_1,\alpha_2\}$ is empty, as desired. ■

Lemma 5.2 *Let $\phi \in \mathbb{C}(x)$ have even degree $d \geq 2$. If ϕ has two 4-branch abundant points in $\mathbb{P}^1(\mathbb{C})$, then ϕ has at most three 2-branch abundant points in $\mathbb{P}^1(\mathbb{C})$.*

Proof Let $A = \{\alpha_1, \alpha_2\} \subset \mathbb{P}^1(\mathbb{C})$ be a set of two 4-branch abundant points for ϕ, and suppose that $V \subset \mathbb{P}^1(\mathbb{C})$ is a set of four 2-branch abundant points for ϕ. Because α_1 and α_2 are 2-branch abundant, we have $A \subseteq V$, and we take $V = \{\alpha_1, \alpha_2, v_1, v_2\}$. By Lemma 4.4, V is the complete set of 2-branch abundant points, and $e_\phi(z) \in \{1,2\}$ for each $z \in \phi^{-1}(V)$. It then follows from Lemma 3.3 that every element of $\phi^{-1}(A)$ is 2-branch abundant for ϕ, and so $\phi^{-1}(A) \subseteq V$. Hence,

$$2d = \sum_{z \in \phi^{-1}(A)} e_\phi(z) \leq \sum_{z \in V} e_\phi(z) \leq 8, \tag{5.1}$$

and it follows that $d \in \{2,4\}$. If $d = 4$, then we have equality in (5.1), implying that $\phi^{-1}(A) = V$ and $e_\phi(z) = 2$ for all $z \in V$. Because $\phi^{-1}(A) = V$, we must have $\phi^{-1}(\{v_1,v_2\}) \cap V = \varnothing$, for, otherwise, applying ϕ gives the impossible $\{v_1,v_2\} \cap A \neq \varnothing$. If $e_\phi(u) = 2$ for all $u \in \phi^{-1}(\{v_1,v_2\})$, then $\#\phi^{-1}(\{v_1,v_2\}) = 2d/2 = 4$, and together with $e_\phi(z) = 2$ for $z \in V$, we have a contradiction to Riemann–Hurwitz (recall $d = 4$ here). Hence, $e_\phi(u) = 1$ for some $u \in \phi^{-1}(\{v_1,v_2\})$. But then u is 2-branch abundant and $u \notin V$, contradicting Lemma 4.4.

Finally, suppose $d = 2$. Let $U = \{z \in \phi^{-1}(\{v_1,v_2\}) : e_\phi(z) = 1\}$, and note that the set $\phi^{-1}(A) \cup U$ consists of 2-branch abundant points for ϕ, and so is a subset of V, and hence has at most four elements. Let r_1 (resp. r_2) be the number of ramification points of ϕ in $\phi^{-1}(A)$ (resp. $\phi^{-1}(\{v_1,v_2\})$), and note that $\#\phi^{-1}(A) = 4 - r_1$ and $\#U = 4 - 2r_2$. Thus, $4 - r_1 + 4 - 2r_2 \leq 4$, implying $4 \leq r_1 + 2r_2$. Because $d = 2$ and $\phi^{-1}(A) \cap \phi^{-1}(\{v_1,v_2\} = \varnothing$ (otherwise $A \cap \{v_1,v_2\} \neq \varnothing$), we have $r_1 + r_2 \leq 2$. It follows that $r_2 = 2$ and $r_1 = 0$. Now $r_1 = 0$ implies $e_\phi(z) = 1$ for all $z \in V$. In addition, $r_1 = 0$ and $\phi^{-1}(A) \subseteq V$ give $\phi^{-1}(A) = V$, and hence v_1 and v_2 are 4-branch abundant by Lemma 3.3. Therefore $\phi^{-1}(\{v_1,v_2\})$ consists of 2-branch abundant points, again by Lemma 3.3. But $r_2 = 2$ and $e_\phi(z) = 1$ for all $z \in V$ imply $\phi^{-1}(\{v_1,v_2\}) \cap V = \varnothing$, contradicting Lemma 4.4. ■

Theorem 5.3 *Let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, and assume that $A = \{\alpha_1, \alpha_2\} \subset \mathbb{P}^1(\mathbb{C})$ is a set of distinct 4-branch abundant points for ϕ. Suppose that ϕ is not 4-trivial with respect to A, and let μ be a Möbius transformation exchanging α_1 and α_2. Then for either*

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

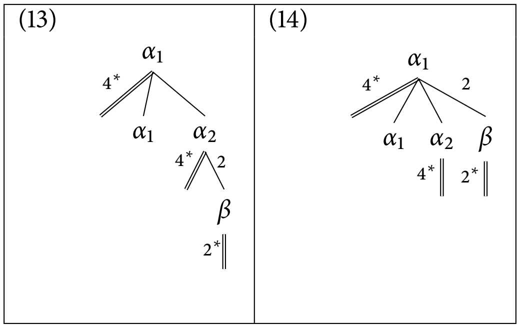


Figure 3

ϕ or $\mu \circ \phi \circ \mu^{-1}$, the 4*-ramification structure for $O_\phi^-(\alpha_1)$ is one of those in Figure* 3*, where points named with distinct letters within a given diagram are distinct.*

Proof Because ϕ is not 4-trivial with respect to A, Theorem 5.1 shows that d is even. Let

$$B = \{ z \in \phi^{-1}(A) \smallsetminus A : 4 \nmid e_\phi(z) \},$$

and observe that by Lemma 3.3, B consists of 2-branch abundant points for ϕ. It follows from Lemma 5.2 that $\#B \le 1$. If B is empty, then ϕ is 4-trivial with respect to A, which gives a contradiction. Hence $\#B = 1$, and we take $B = \{\beta\}$. Observe that $4 \nmid e_\phi(\beta)$ and $4 \mid e_\phi(z)$ for each $z \in \phi^{-1}(A) \smallsetminus A$ with $z \ne \beta$. But also, $\sum_{z \in \phi^{-1}(A)} e_\phi(z) = 2d$ is divisible by 4 (since d is even), whence we must have $\phi^{-1}(A) \cap A \ne \varnothing$, which implies

$$A \cap \phi(A) \ne \varnothing. \tag{5.2}$$

If $2 \nmid e_\phi(\beta)$, then Lemma 3.3 gives that β is 4-branch abundant for ϕ, and so $W = \{\alpha_1, \alpha_2, \beta\}$ is a set of three 4-branch abundant points for ϕ. Then $U = \#\{\phi^{-1}(W) \smallsetminus W : 4 \nmid e_\phi(z)\}$ consists of 2-branch abundant points for ϕ, and Lemma 5.2 implies that U is empty. Applying Lemma 3.6 with $T = W$ gives the contradiction

$$\sum_{z \in \phi^{-1}(W)} \big(e_\phi(z) - 1 \big) \ge (3d - 3) \cdot (3/4) > 2d - 2.$$

Therefore, $e_\phi(\beta) \equiv 2 \bmod 4$. Suppose now that there is $v \in \phi^{-1}(\beta)$ with $e_\phi(v)$ odd. Because d is even, there must also be $v' \in \phi^{-1}(\beta)$ with $e_\phi(v')$ odd and $v' \ne v$. By Lemma 3.3, β, v, and v' are all 2-branch abundant, and so by Lemma 5.2 we have $\#\{\alpha_1, \alpha_2, \beta, v, v'\} = 3$. But $\beta \notin \{v, v'\}$, for otherwise applying ϕ gives the impossible $A \ni \beta$. Hence, $\{v, v'\} = A$, and thus $\{\beta\} = \phi(A)$, contradicting (5.2).

Thus, all elements of $\phi^{-1}(\beta)$ have even ramification index. Let

$$R = \{ z \in \phi^{-1}(A) : 4 \mid e_\phi(z) \},$$

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

and observe that $\phi^{-1}(A) \subseteq A \cup \{\beta\} \cup R$, with equality if and only if $A \subseteq \phi^{-1}(A)$. We claim that

$$\#\phi^{-1}(A) \le 3 + \frac{2d-2-e_\phi(\beta)}{4}, \qquad \text{with equality holding if and only if} \tag{5.3}$$

$$e_\phi(z) = 4 \text{ for all } z \in R, \quad A \subseteq \phi^{-1}(A), \quad \text{and } e_\phi(\alpha_1) = e_\phi(\alpha_2) = 1. \tag{5.4}$$

To see why, let $a = \#(A \cap \phi^{-1}(A))$, and write $e_\phi(z) = 4r_z$ for each $z \in R$. Then $\#\phi^{-1}(A) = a + 1 + \#R$. To compute $\#R$, observe that

$$2d = \sum_{\phi^{-1}(A)} e_\phi(z) = \Big(\sum_{z \in (A \cap \phi^{-1}(A))} e_\phi(z) \Big) + e_\phi(\beta) + 4\Big(\sum_{z \in R} (r_z - 1) + \#R \Big),$$

from which it follows that

$$\begin{aligned} \#\phi^{-1}(A) &= a + 1 + \frac{1}{4}\Big(2d - e_\phi(\beta) - \sum_{z \in (A \cap \phi^{-1}(A))} e_\phi(z) \Big) - \sum_{z \in R} (r_z - 1) \\ &\le a + 1 + \frac{1}{4}\big(2d - e_\phi(\beta) - a \big), \end{aligned}$$

with equality holding if and only if $e_\phi(z) = 1$ for all $z \in (A \cap \phi^{-1}(A))$ and $e_\phi(z) = 4$ for all $z \in R$. But $a \in \{1, 2\}$, and from this, one has $a + 1 + (2d - e_\phi(\beta) - a)/4 \le 3 + (2d - 2 - e_\phi(\beta))/4$, with equality holding if and only if $a = 2$. This proves the statements in (5.3) and (5.4). Recall that all elements of $\phi^{-1}(\beta)$ have even ramification index, and apply this together with (5.3) to get

$$\begin{aligned} \sum_{z \in \phi^{-1}(A \cup \{\beta\})} (e_\phi(z) - 1) &= 2d - \#(\phi^{-1}(A)) + \sum_{z \in \phi^{-1}(\beta)} (e_\phi(z) - 1) \\ &\ge 2d - \Big(3 + \frac{2d - 2 - e_\phi(\beta)}{4} \Big) + \frac{d}{2} \\ &= 2d - 3 + \frac{2 + e_\phi(\beta)}{4} \ge 2d - 2, \end{aligned} \tag{5.5}$$

with equality holding if and only if the conditions in (5.4) hold, and also $e_\phi(\beta) = 2$ and $e_\phi(z) = 2$ for all $z \in \phi^{-1}(\beta)$. Because d is even, we must have $A \subseteq \phi^{-1}(\alpha_1)$ or $A \subseteq \phi^{-1}(\alpha_2)$; replacing ϕ by $\mu \circ \phi \circ \mu^{-1}$ if necessary, we assume the former. If $d \equiv 2 \pmod 4$, we obtain 4-ramification structure (13) for $O_\phi^-(\alpha_1)$, and if $d \equiv 0 \pmod 4$ we obtain 4-ramification structure (14) for $O_\phi^-(\alpha_1)$. ■

6 Field of Definition of ϕ and its Components

Many of our main results require showing that if ϕ is defined over a subfield K of $\mathbb{C}$, then certain irreducible factors of the numerator and denominator of iterates of ϕ can also be defined over K. In view of potential future applications, and because it entails no additional work, we state the results of this section for arbitrary fields of characteristic zero.

Lemma 6.1 *Let F be a field of characteristic zero and let $\overline{F}$ be an algebraic closure of F. Given $h \in \overline{F}[x]$ and $m \ge 2$, let $g \in \overline{F}[x]$ be the monic polynomial of maximal degree*

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

such that $h(x) = f(x)(g(x))^m$ for some $f \in \overline{F}[x]$. If h has coefficients in F, then so do both f and g.

Remark The assumption that F have characteristic zero is necessary, as illustrated by the case where ℓ is prime, $F = \mathbb{F}_\ell(t)$, $f(x) = x$, $g(x) = (x - \sqrt[\ell]{t})$, and $m = \ell$.

Proof Let

$$\begin{aligned} R_1 &= \{\text{roots of } f \text{ that are not roots of } g\},\\ R_2 &= \{\text{roots of } g \text{ that are not roots of } f\},\\ \operatorname{Crit}(\phi)R_3 &= \{\text{roots of both } f \text{ and } g\}. \end{aligned}$$

These are pairwise disjoint subsets of $\overline{F}$. The maximality of the degree of g implies that $e_h(\alpha) < m$ for each $\alpha \in R_1$, $m \mid e_h(\alpha)$ for each $\alpha \in R_2$, and each $\alpha \in R_3$ satisfies $m > e_h(\alpha)$ and $m \nmid e_h(\alpha)$. Because the set of roots of h is $R_1 \cup R_2 \cup R_3$ and $h \in F[x]$, each $\sigma \in G_F := \operatorname{Gal}(\overline{F}/F)$ permutes $R_1 \cup R_2 \cup R_3$. We also have $e_h(\alpha) = e_h(\sigma(\alpha))$, and it follows that $\sigma(R_i) = R_i$ for $i = 1,2,3$. Now the set of roots of f is $R_1 \cup R_3$, and the set of roots of g is $R_2 \cup R_3$. Let c_f be the leading coefficient of f, and observe that each of f/c_f and g are monic polynomials whose set of roots is preserved by the action of G_F. Because F has characteristic zero, $\overline{F}/F$ is Galois, and thus the fixed field of G_F is F, implying that f/c_f and g are both in $F[x]$. But c_f is the leading coefficient of h, and thus is in F. Hence, $f \in F[x]$. ■

We remark here that by definition a rational function ϕ is defined over F (written $\phi \in F(x)$) if there are relatively prime $p, q \in F[x]$ with $\phi = p/q$. If $\phi \in F(x)$ and $f, g \in \overline{F}[x]$ with $\phi = f/g$ and $\gcd(f,g) = 1$, then we have $pg = fq$, whence $cf = p$ and $cg = q$ for some $c \in \overline{F}$. If f and g are monic, then c equals the leading coefficient of p (or q), and hence $c \in F$, giving that $f, g \in F[x]$.

Theorem 6.2 *Let F be a field of characteristic zero, $\overline{F}$ an algebraic closure of F, and $\phi \in \overline{F}(x)$. Let $\operatorname{Crit}(\phi)$ be the set of all $\alpha \in \mathbb{P}^1(\overline{F})$ with $e_\phi(\alpha) > 1$. For each $\alpha \in \operatorname{Crit}(\phi)$, write $e_\phi(\alpha) = q_\alpha m + r_\alpha$, with $0 < r_\alpha < m$. Let*

$$\psi(x) = \prod_{\alpha \in \operatorname{Crit}(\phi)} (x - \alpha)^{q_\alpha}.$$

If $\phi \in F(x)$, then $\psi(x)$ and $\phi(x)/(\psi(x))^m$ are both in $F(x)$.

Proof Assume that $\phi \in F(x)$. Write $\psi = g_1/g_2$, where each $g_i \in \overline{F}[x]$ is monic and $\gcd(g_1, g_2) = 1$, and write $\phi(x)/(\psi(x))^m = f_1/f_2$, where each $f_i \in \overline{F}[x]$ and $\gcd(f_1, f_2) = 1$. Because $\phi \in F[x]$, there is $c \in \overline{F}$ with $cf_i(x)(g_i(x))^m \in F[x]$ for $i = 1,2$. By Lemma 6.1, we have $g_i \in F[x]$ and $cf_i \in F[x]$. Hence, $\psi \in F(x)$ and $\phi(x)/(\psi(x))^m \in F(x)$, the latter since $\phi(x)/(\psi(x))^m = (cf_1)/(cf_2)$. ■

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

7 Proof of Theorem 1.2

To prove Theorem 1.2, we must relate the ramification structure of backward orbits of m-branch abundant points to global properties of ϕ. When these ramification structures have certain properties, ϕ must descend from an endomorphism of an algebraic group – either $\mathbb{G}_m$ or an elliptic curve. For this we cite some results from the invaluable paper of Milnor [15]. We call $z \in \mathbb{P}^1(\mathbb{C})$ *exceptional* for ϕ if the backwards orbit $\bigcup_{n=1}^{\infty} \phi^{-n}(z)$ is finite, and we denote by $\mathcal{E}_\phi$ the collection of all exceptional points for ϕ. Recall that we denote the postcritical set of ϕ by $\operatorname{Postcrit}(\phi)$ (see the paragraph before Theorem 1.2 for the definition). A rational function $\phi \in \mathbb{C}(x)$ of degree at least two is a *finite quotient of an affine map* if there is a flat surface $\mathbb{C}/\Lambda$ (where $\Lambda \subset \mathbb{C}$ is a lattice), an affine self-map of $\mathbb{C}/\Lambda$ given by $L(t) = at + b$, and a finite-to-one holomorphic map $\Theta\colon \mathbb{C}/\Lambda \to \mathbb{P}^1(\mathbb{C}) \smallsetminus \mathcal{E}_\phi$ satisfying $\phi \circ \Theta = \Theta \circ L$. As stated prior to Theorem 1.2, we call ϕ a Lattès map when Λ has rank two, and hence $\mathbb{C}/\Lambda$ is a torus. Milnor states a useful ramification-based characterization of Lattès maps, which we make heavy use of in the proof of Theorem 1.2.

Theorem 7.1 (Milnor [15, Theorem 4.1]) *Let $\phi \in \mathbb{C}(x)$ be a rational function and $\mathcal{E}_\phi$ its set of exceptional points. Then ϕ is a finite quotient of an affine map if and only if there exists an integer-valued function $r(z)$ on $\mathbb{P}^1(\mathbb{C}) \smallsetminus \mathcal{E}_\phi$ that satisfies $r(\phi(z)) = e_\phi(z) r(z)$ and takes the value* 1 *outside of* $\operatorname{Postcrit}(\phi)$.

We can extend r to a function from $\mathbb{P}^1(\mathbb{C})$ to $\mathbb{Z} \cup \{\infty\}$ by taking $r(z) = \infty$ if $z \in \mathcal{E}_\phi$. When ϕ is a finite quotient of an affine map, its *signature* is the sequence of values r takes on $\operatorname{Postcrit}(\phi)$. It is true, though not obvious, that the existence of the map r as in Theorem 7.1 implies the finiteness of the post-critical set of ϕ (see the proof of [15, Theorem 4.1]). In [15, Theorem 4.5 and Remark 4.7], Milnor shows that there are only six possible signatures. They are $(2,2,\infty)$ and (∞,∞), which give maps conjugate to Chebyshev polynomials and power maps, respectively; and $(2,2,2,2)$, $(3,3,3)$, $(2,4,4)$, and $(2,3,6)$, which give Lattès maps. We summarize this as follows.

Theorem 7.2 (Milnor [15]) *Let $\phi \in \mathbb{C}(x)$ be a rational function. Then ϕ is a Lattès map if and only if there exists a function $r\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{Z}$ satisfying $r(\phi(z)) = e_\phi(z) r(z)$ and taking the value* 1 *outside of* $\operatorname{Postcrit}(\phi)$. *In this case, the signature of ϕ is one of* $(2,2,2,2)$, $(3,3,3)$, $(2,4,4)$, *or* $(2,3,6)$.

We immediately obtain a corollary that will be useful in the proof of Theorem 1.2.

Corollary 7.3 *Let $m \in \mathbb{Z}$ with $m \geq 2$, let $\phi \in \mathbb{C}(x)$ have degree $d \geq 2$, and assume that $A = \{\alpha_1, \alpha_2\} \subset \mathbb{P}^1(\mathbb{C})$ is a set of distinct m-branch abundant points for ϕ. Suppose that ϕ is not m-trivial with respect to A, and let μ be a Möbius transformation exchanging α_1 and α_2. Then $m \leq 4$. If $m = 4$ (resp. 3), then ϕ is a Lattès map of signature* $(2,4,4)$ *(resp.* $(3,3,3)$*) with $r(\alpha_1) = r(\alpha_2) = m$. If $m = 2$, then unless ϕ or $\mu \circ \phi \circ \mu^{-1}$ satisfies* (2D), (2F), (2M), *or* (2O) *of Theorem 4.7, ϕ is a Lattès map of signature* $(2,2,2,2)$ *with* $r(\alpha_1) = r(\alpha_2) = 2$.

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

Proof It is well known that the collection of Lattès maps is invariant under Möbius conjugation; hence for this corollary it suffices to show that either ϕ or $\mu \circ \phi \circ \mu^{-1}$ is Lattès. Because ϕ is not m-trivial with respect to A, Theorem 3.8 shows $m \le 4$. If $m = 4$, then for either ϕ or $\mu \circ \phi \circ \mu^{-1}$, $O_\phi^+(\alpha_1)$ has 4-ramification structure (13) or (14) in Theorem 5.3, and we let β be as in those 4-ramification structures. Observe that (5.5) implies that $e_\phi(z) = 1$ for $z \notin \phi^{-1}(\{\alpha_1, \alpha_2, \beta\}$, and so taking $r(\alpha_1) = r(\alpha_2) = 4$ and $r(\beta) = 2$ and applying Theorem 7.2 shows that ϕ is Lattès of signature (2,4,4). If $m = 3$, then it follows from Theorem 4.6 that we can take $r(z) = 3$ for $z \in Ab(\alpha_1, \alpha_2)$ and $r(z) = 1$ otherwise and apply Theorem 7.2 to show that ϕ is Lattès of signature (3,3,3). If $m = 2$ and neither ϕ nor $\mu \circ \phi \circ \mu^{-1}$ satisfies (2D), (2F), (2M), or (2O) of Theorem 4.7, then it follows from Theorem 4.6 that we can take $r(z) = 2$ for $z \in Ab(\alpha_1, \alpha_2)$ and $r(z) = 1$ otherwise and apply Theorem 7.2 to show that ϕ is Lattès of signature (2,2,2,2). ■

Proof of Theorem 1.2 Fix $m \ge 2$, let K be a subfield of $\mathbb{C}$, let $\phi \in K(x)$ have degree $d \ge 2$, and let g_n be defined as in the discussion before Theorem 1.1.

Suppose that g_n is bounded as $n \to \infty$. By Corollary 2.5 we have that 0 and ∞ are m-branch abundant points for ϕ. If ϕ is m-trivial with respect to $\{0, \infty\}$, then Proposition 3.2 shows that $\phi(x) = cx^j(\psi(x))^m$ with $\psi \in \mathbb{C}(x)$, $0 \le j \le m-1$, and $c \in \mathbb{C}^*$. We can apply Theorem 6.2 to conclude that $\psi \in K(x)$ and $c \in K^*$.

Assume that ϕ is not m-trivial with respect to $\{0, \infty\}$. We apply Corollary 7.3 with $\mu(x) = 1/x$. If $m = 4$ (resp. $m = 3$), then Corollary 7.3 shows that we are in case (2) (resp. (3)) of the present theorem. If $m = 2$ and neither ϕ nor $\mu \circ \phi \circ \mu^{-1}$ satisfies (2D), (2F), (2M), or (2O) of Theorem 4.7, then we are in case (4) of the present theorem.

If $m = 2$ and one of ϕ or $\mu \circ \phi \circ \mu^{-1}$ satisfies (2D) in Theorem 4.7, then we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, giving a 3-cycle $C \mapsto \infty \mapsto 0 \mapsto C$ ($C \in \mathbb{C}^*$) in 2-ramification structure (3) from Theorem 4.3. Observe that $\phi(x) = B\prod_{r \in R}(x-r)\prod_{p \in P}(x-p)^{-1}$, where $B \in \mathbb{C}^*$ and R (resp. P) is the set of roots (resp. poles) of ϕ, with multiplicity. From 2-ramification structure (3), we have that all roots of ϕ except ∞, and all poles of ϕ except C, occur to even multiplicity. Hence,

$$\phi(x) = B\frac{f(x)^2}{(x-C)g(x)^2}, \tag{7.1}$$

for $f, g \in \mathbb{C}[x]$ monic with $\deg g \ge \deg f$ and $\gcd(f(x), (x-C)g(x)) = 1$. From Theorem 6.2, we have $B(x-C) \in K[x]$ and $f/g \in K(x)$, and hence $B, C \in K^*$, and by the remark before Theorem 6.2, we have $f, g \in K[x]$.

Subtracting C from both sides of (7.1) and doing some algebra yields

$$\phi(x) - C = \frac{B}{(x-C)g(x)^2}\big(f(x)^2 - (C/B)(x-C)g(x)^2\big).$$

Because 0 is the only preimage of C under ϕ with odd ramification index, we must have

$$f(x)^2 - (C/B)(x-C)g(x)^2 = bxh(x)^2, \quad b \in \mathbb{C}^*. \tag{7.2}$$

Because the left-hand side of (7.2) is in $K[x]$, $bxh(x)^2$ must be as well. By Theorem 6.2 we have $b \in K$ and $h \in K[x]$. Putting $x = 0$ in (7.2) gives $-B \in K^2$ (note that $f(0), g(0) \ne 0$ since $\phi(0) \notin \{0, \infty\}$), and putting $x = C$ then gives $b \in CK^2$ ($f(C) \ne 0$

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

by assumption, whence $h(C) \neq 0$). Letting $D, E \in K$ satisfy $D^2 = -B$ and $b = CE^2$, we take $f_1(x) = Df(x) \in K[x]$ and $h_1(x) = DEh(x)$ to obtain

$$\phi(x) = -\frac{f_1(x)^2}{(x-C)g(x)^2}$$

with $f_1(x)^2/D^2 - (C/B)(x-C)g(x)^2 = bxh_1(x)^2/(DE)^2$, *i.e.*, $f_1(x)^2 + C(x-C)g(x)^2 = Cxh_1(x)^2$. Writing f for f_1 and h for h_1, we have obtained the form in Theorem 1.2(5a). Note that $Cxh(x)^2$ has odd degree, and so we must have $\deg g \geq \deg f$, and hence we do not need to make this stipulation separately.

If $m = 2$ and one of ϕ or $\mu\circ\phi\circ\mu^{-1}$ satisfies (2F) in Theorem 4.7, then we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, giving a 2-cycle $C \mapsto 0 \mapsto C$ ($C \in \mathbb{C}^*$) in 2-ramification structure (2) from Theorem 4.3. If one of ϕ or $\mu\circ\phi\circ\mu^{-1}$ satisfies (2M) in Theorem 4.7, then we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, so that ∞ and C are the preimages of 0 having odd multiplicity. If one of ϕ or $\mu\circ\phi\circ\mu^{-1}$ satisfies (2O) in Theorem 4.7, then we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, so that 0 is a fixed point in 2-ramification structure (7) of Theorem 4.5 with unique non-zero preimage C of odd multiplicity. In each case, we argue as in case (2D) above to show that ϕ has form (5b), (5c), or (5d), respectively, and that (1.4) holds. We leave the details to the reader.

We now prove the 'only if' part of the theorem. Suppose that ϕ satisfies one of conditions (1)–(5). We show that 0 and ∞ are m-branch abundant for ϕ, which by Corollary 2.5 shows that g_n is bounded as $n \to \infty$. If ϕ satisfies condition (1), the desired conclusion follows from Proposition 3.2. If ϕ satisfies conditions (2)–(4), then ϕ is Lattès with $r(0) = r(\infty) = m$, where r is the function in Theorem 7.2. It follows from the definition of r that for each $n \geq 1$, we have

$$e_\phi(z) = m \text{ for all } z \in \phi^{-n}(0) \smallsetminus \operatorname{Postcrit}(\phi).$$

By Theorem 7.2, $\operatorname{Postcrit}(\phi)$ has at most four elements, and thus in the notation of Definition 2.1, we have that $\rho_n(0) \leq 4$ for all n. Hence, 0 is m-branch abundant for ϕ, and an identical argument shows the same conclusion for ∞. If ϕ satisfies one conditions (5a)–(5d), then by construction 0 and ∞ are 2-branch abundant points for ϕ. ■

We now discuss the parameterizations of maps in cases (5a)–(5d) in Theorem 1.2 mentioned in the introduction. We begin with a detailed analysis of the case (5a).

Proposition 7.4 *Let $f, g \in \mathbb{C}[x]$ and $C \in \mathbb{C} \smallsetminus \{0\}$. The following are equivalent:*

(i) $\gcd(f, g) = 1$, $f(C) \neq 0$, *and* $f(x)^2 + C(x-C)g(x)^2 = Cxh(x)^2$ *for some* $h(x) \in \mathbb{C}[x]$.

(ii) *There exist* $P, Q \in \mathbb{C}[x]$ *satisfying* $\gcd(P, Q) = 1$, $Q(C) \neq 0$, $CP(0) \neq Q(0)$,

$$f(x) = C^2P(x)^2(x-C) - 2CP(x)Q(x)(x-C) - CQ(x)^2,$$
$$g(x) = -CP(x)^2(x-C) - 2CP(x)Q(x) + Q(x)^2.$$

Proof Given P and Q as in (ii), one checks that $f(x)^2 + C(x-C)g(x)^2 = Cxh(x)^2$ for $h(x) = Q(x)^2 + CP(x)^2(x-C)$. The assumption that $Q(C) \neq 0$ implies that $f(C) \neq 0$. Moreover, $f(x) + Cg(x) = -2CxP(x)Q(x)$, and so if $r \in \mathbb{C}$ is a common root of f and g, then $r = 0$, $P(r) = 0$, or $Q(r) = 0$. Observe that $f(0) = -C(CP(0) -$

$Q(0))^2$, and the assumption that $CP(0) \neq Q(0)$ forces $f(0) \neq 0$. Hence, $r \neq 0$. If $P(r) = 0$, then $0 = f(r) = -CQ(r)^2$, contradicting $\gcd(P, Q) = 1$. If $Q(r) = 0$, then $r \neq C$ by assumption, and so $0 = f(r) = C^2 P(r)(r-C)$ also contradicts $\gcd(P, Q) = 1$. It follows that $\gcd(f, g) = 1$.

Given f, g as in (i), observe that $f(x)^2 + C(x-C)g(x)^2 = Cxh(x)^2$ is equivalent to $(f(x)/h(x))^2 + C(x-C)(g(x)/h(x))^2 = Cx$. We thus look for solutions $\alpha, \beta \in \mathbb{C}(x)$ to the equation $\alpha(x)^2 + C(x-C)\beta(x)^2 = Cx$. Clearly, $\alpha(x) = C$ and $\beta(x) = 1$ is one such solution, and because our equation is a conic, we use projection to find all other solutions. Letting s and t be variables and γ an undetermined constant in $\mathbb{C}(x)$, the line $s = \gamma t + (1 - C\gamma)$ passes through $(C, 1)$. Substituting $\beta = \gamma\alpha + (1 - C\gamma)$ into our conic and dividing through by $\alpha - C$ gives the solution

$$\alpha = \frac{C^2\gamma^2(x-C) - 2C\gamma(x-C) - C}{1 + C\gamma^2(x-C)}.$$

We then use $\beta = \gamma\alpha + (1 - C\gamma)$ to obtain

$$\beta = \frac{-C\gamma^2(x-C) - 2C\gamma + 1}{1 + C\gamma^2(x-C)}.$$

Writing $\gamma(x) = P(x)/Q(x)$ with $\gcd(P, Q) = 1$ and clearing denominators gives the expressions for f and g in the Proposition 7.4(ii). Because $f(C) \neq 0$, we must have $Q(C) \neq 0$. We must also have $CP(0) \neq Q(0)$, for otherwise $f(0) = g(0) = 0$, contradicting $\gcd(f, g) = 1$. ■

For maps of the form (5b), a similar analysis gives the parameterization

$$f(x) = CP(x)^2 - 2CP(x)Q(x) - (x-C)Q(x)^2,$$
$$g(x) = -CP(x)^2 - 2(x-C)P(x)Q(x) + (x-C)Q(x)^2.$$

Taking $C = -4$, $Q(x) = 2$, and $P(x) = 1$ gives $f(x) = -4(x+1)$ and $g(x) = 4$, leading to $\phi(x) = -(x+4)(x+1)^2$, which is $-(T_3(x+2)) + 2$, one of the maps mentioned in the paragraph following Theorem 1.2.

As for maps of the form (5c), note that $B(x-C)f(x)^2 - Cg(x)^2 = -Ch(x)^2$ is equivalent to $(B/C)(x-C)f(x)^2 = (g(x)+h(x))(g(x)-h(x))$. From $\gcd(f, g) = 1$ it follows that $\gcd(g, h) = 1$, and so $\gcd(g+h, g-h) = 1$. Thus one of $g+h, g-h$ is a square in $\mathbb{C}[x]$ while the other is $(x-C)$ times a square, and the squares multiply to $f(x)$. It follows that

$$g(x) = a(x-C)P(x)^2 + bQ(x)^2,$$
$$f(x) = P(x)Q(x)$$

for some $P, Q \in \mathbb{C}[x]$ with $ab = B/4C$ and $\gcd((x-C)P(x), Q(x)) = 1$. Clearly, any such P, Q give a solution to $B(x-C)f(x)^2 - Cg(x)^2 = -Ch(x)^2$.

Maps of the form (5d) can be handled with a similar analysis, though there are two cases: when one of $g+h, g-h$ is a square in $\mathbb{C}[x]$ and the other is $x(x-C)$ times a square; and when one is x times a square and the other is $(x-C)$ times a square.

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

8 Proof of Theorem 1.1

As a stepping stone to proving Theorem 1.1, we give a useful result on m-trivial maps. We require some notation. For an integer $n \geq 1$, let P_n be the (possibly empty) set of primes dividing n. Fix an integer $j \geq 1$, and let $n \geq 1$ satisfy $P_n \subseteq P_j$. Define $w_j(n)$ to be the smallest nonnegative exponent ℓ such that $n \mid j^\ell$. More explicitly, if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, and $f_i = v_{p_i}(j)$ for $i = 1, \dots, k$, where v_{p_i} denotes the p_i-adic valuation, then $w_j(n) = \max_i \lceil (e_i/f_i) \rceil$. For relatively prime integers $a, b \geq 1$, we denote the order of a in $(\mathbb{Z}/b\mathbb{Z})^*$ by $\operatorname{ord}(a \bmod b)$.

Lemma 8.1 *Let $m \geq 2$, let K be a subfield of $\mathbb{C}$, let $\phi \in K(x)$ have degree $d \geq 2$, and assume that ϕ is m-trivial with respect to $\{0, \infty\}$. Let $\phi(x) = cx^j(\psi_0(x))^m$ as in Proposition 3.2, and let g_n be as in the discussion preceding Theorem 1.1. Then $g_n = 0$ for all $n \geq 1$ and there exist integers $r > s \geq 0$ such that*

$$\phi^r(x) = \phi^s(x)(\psi(x))^m \text{ for some } \psi \in K(x). \tag{8.1}$$

When $j = 0$, (8.1) holds if and only if $s \geq 1$. When $j > 0$, let t be the minimal positive integer with $c^t \in K^m$, and let m' (resp. t') be the maximal divisor of m (resp. t) relatively prime to j. Then (8.1) holds if and only if

$$\begin{cases} s \geq w_j(m/m'), \\ t' \mid (r - s) \text{ if } j = 1, \\ \operatorname{lcm}[\operatorname{ord}(j \bmod m'), \operatorname{ord}(j \bmod t'(j-1))] \mid (r - s) \text{ if } j > 1. \end{cases} \tag{8.2}$$

In all cases there exists $r \leq m$ such that (8.1) holds.

Proof Because $\phi \in K(x)$, we can apply Theorem 6.2 to conclude that $\psi_0 \in K(x)$ and $c \in K^*$. We describe the image of ϕ^n in $K(x)^*/K(x)^{*m}$ for all $n \geq 1$. Because $\phi(x) \equiv cx^j \pmod{K(x)^{*m}}$, we have

$$\phi^n(x) \equiv c^{1+j+\cdots+j^{n-1}} x^{j^n} \pmod{K(x)^{*m}} \tag{8.3}$$

for $n \geq 1$. It follows immediately from Proposition 2.3 that $g_n = 0$ for all $n \geq 1$. Note that if $j = 0$, then (8.3) gives $\phi^r(x) \equiv \phi(x)$ for all $r \geq 1$, and we can take $r = 2 \leq m$.

Assume for the rest of the proof that $j \geq 1$. We now show that (8.1) holds if and only if (8.2) does. It follows from (8.3) that $\phi^r(x) \equiv \phi^s(x) \pmod{K(x)^{*m}}$ for $r > s \geq 0$ is equivalent to $x^{j^r} \equiv x^{j^s} \pmod{K(x)^{*m}}$ and $c^{1+j+\cdots+j^{r-1}} \in K^{*m}$ (if $s = 0$) or $c^{1+j+\cdots+j^{r-1}} \equiv c^{1+j+\cdots+j^{s-1}} \pmod{K^{*m}}$ (if $s \geq 1$). This in turn is equivalent to:

$$j^r \equiv j^s \pmod{m} \quad \text{and} \tag{8.4}$$

$$j^s + \cdots + j^{r-1} \equiv 0 \pmod{t}. \tag{8.5}$$

Now (8.4) holds if and only if $m \mid j^s(j^{r-s} - 1)$. Observe that $\gcd(m', j) = 1$ implies that $\gcd(m', j^s) = 1$, and hence $m' \mid (j^{r-s} - 1)$. This holds if and only if $\operatorname{ord}(j \bmod m') \mid r - s$. Moreover, every prime dividing m/m' also divides j, and so we have that m/m' and $(j^{r-s} - 1)$ are relatively prime, whence $(m/m') \mid j^s$. By the definition of w_j, this holds if and only if $s \geq w_j(m/m')$. Similarly, (8.5) holds if and only if $t \mid j^s(1 + \cdots + j^{r-s-1})$, and as above this is equivalent to $t' \mid (1 + \cdots + j^{r-s-1})$ and $(t/t') \mid j^s$. The former is

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

equivalent to $t' \mid r-s$ (if $j=1$) and $t'(j-1) \mid (j^{r-s}-1)$, *i.e.*, $\operatorname{ord}(j \bmod t'(j-1)) \mid r-s$ (if $j>1$). Note that the minimality of t implies that $t \mid m$, and so $t' \mid m'$ and $(t/t') \mid (m/m')$. Hence, $(t/t') \mid j^s$ is implied by $(m/m') \mid j^s$.

It remains to show that there exists $r \leq m$ such that (8.1) holds. From (8.2), if we set

$$s = w_j(m/m'),$$
$$r = \begin{cases} s + t' & \text{if } j = 1 \\ s + \operatorname{lcm}[\operatorname{ord}(j \bmod m'), \operatorname{ord}(j \bmod t'(j-1))] & \text{if } j > 1 \end{cases}$$

then (8.1) is satisfied, and so it is enough to show that

$$w_j(m/m') + \operatorname{lcm}\big[\operatorname{ord}(j \bmod m'), \operatorname{ord}(j \bmod t'(j-1))\big] \leq m$$

and

$$w_j(m/m') + t' \leq m.$$

Because $t' \mid m'$, we have that both $\operatorname{ord}(j \bmod t'(j-1))$ and $\operatorname{ord}(j \bmod m')$ divide $\operatorname{ord}(j \bmod m'(j-1))$. But j belongs to the subgroup

$$\big\{ g \in (\mathbb{Z}/m'(j-1)\mathbb{Z})^* : g \equiv 1 \pmod{(j-1)} \big\},$$

which has at most m' elements, whence $\operatorname{ord}(j \bmod m'(j-1)) \leq m'$, and so

$$\operatorname{lcm}\big[\operatorname{ord}(j \bmod m'), \operatorname{ord}(j \bmod t'(j-1))\big] \leq m'.$$

Hence, it suffices in both the $j>1$ and $j=1$ cases to show that $w_j(m/m') + m' \leq m$. If $m = m'$, then $w_j(m/m') = 0$, and we are done. If $m \neq m'$, then write $m/m' = p_1^{e_1} \cdots p_k^{e_k}$, with $k \geq 1$. Let $e_\ell = \max_i e_i$, write $e = e_\ell$ and $p = p_\ell$, and note that $m' \leq m/p^e$. Hence we must show $e + (m/p^e) \leq m$. But $p^e \mid m$ and $e \geq 1$, and so $1 + e \leq p^e \leq m$. Using $e/(p^e-1) \leq 1$ gives $e/(p^e-1) + e \leq m$, and dividing by e and combining terms gives $p^e/(p^e-1) \leq m/e$. Taking reciprocals gives $1 - (1/p^e) \geq e/m$, which gives $m \geq e + (m/p^e)$, as desired. ∎

Before proving Theorem 1.1, we give one more preliminary result that will aid in our analysis.

Lemma 8.2 *Let K be a subfield of $\mathbb{C}$, let $\phi \in K(x)$ be a Lattès map satisfying $\phi(\infty) = \infty$, and write $\phi(x) = Mf(x)/g(x)$ with $f, g \in K(x)$ monic. If ϕ has signature (2,4,4) and $r(\infty) = 4$, where r is the function in Theorem 7.2, then $M^2 \in K^4$. If ϕ has signature (3,3,3) and $r(\infty) = 3$, then $M \in K^3$.*

Proof By definition, $r(\phi(z)) = e_\phi(z) r(z)$ for all $z \in \mathbb{P}^1(\mathbb{C})$. By assumption, $\phi(\infty) = \infty$ and $r(\infty) \neq 0$, and hence we must have $e_\phi(\infty) = 1$. Therefore, $\deg f = 1 + \deg g$. Now the multiplier $\lambda_\infty(\phi)$ of ϕ at ∞ is defined to be $(1/\phi(1/x))'$ evaluated at $x = 0$ (see [22, Exercise 1.13]). Because $\deg f = 1 + \deg g$, one easily deduces that $\lambda_\infty(\phi) = 1/M$. Put $n_\phi = 3$ if ϕ has signature (3,3,3), and $n_\phi = 4$ if ϕ has signature (2,4,4), and recall from Theorems 7.1 and 7.2 that ϕ is a finite quotient of a linear map $L\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice. By [15, Corollary 3.9], the multiplier at any fixed point z_0 of ϕ has the form $(\omega a)^{r(z_0)}$, where $\omega^{n_\phi} = 1$. Hence, M is of the form a^{n_ϕ}.

From [15, Theorem 5.1], we have $a\Lambda \subset \Lambda$ and $\zeta_{n_\phi}\Lambda = \Lambda$, where ζ_{n_ϕ} is a primitive (n_ϕ)-th root of unity. It follows that $a \in \Lambda$ and $\Lambda = \mathbb{Z}[i]$ if $n_\phi = 4$ and $\Lambda = \mathbb{Z}[e^{2\pi i/3}]$ if $n_\phi = 3$. Therefore $[K(a):K] \le 2$, and hence $[K(M^{1/n_\phi}):K] \le 2$. Because $n_\phi \ge 3$, this implies $x^{n_\phi} - M$ is reducible over K, and by a well-known theorem (*e.g.,* [13, Theorem 8.1.6]), it follows that either $n_\phi = 3$ and $M \in K^3$ or $n_\phi = 4$ and one of $M \in K^2$ or $M \in -4K^4$ holds. In either of the cases for $n_\phi = 4$ we have $M^2 \in K^4$, which proves the lemma. ∎

Proof of Theorem 1.1 Fix $m \ge 2$, let K be a subfield of $\mathbb{C}$, let $\phi \in K(x)$ have degree $d \ge 2$, and let g_n be defined as in the discussion before Theorem 1.1. By Corollary 2.5 it suffices to show that 0 and ∞ are m-branch abundant points for ϕ if and only if $\phi^r(x) = \phi^s(x)$ in $K(x)^*/K(x)^{*m}$ for $r > s \ge 0$ with $r \le m$ if $m \ge 3$ and $r \le 6$ if $m = 2$. One direction is easy: if there are r and s satisfying the requisite properties, then for all $n \ge r$, we have $\phi^n(x) = \phi^j(x)$ in $K(x)^*/K(x)^{*m}$ for some $j \in \{0, \dots, r-1\}$, and hence all $z \in \phi^{-n}(0)$ with $m \nmid e_{\phi^n}(z)$ lie in the set $\bigcup_{j=0}^{r-1} \phi^{-j}(0)$, which is independent of n. Hence, 0 is m-branch abundant for ϕ. Observe that

$$\phi^r(x) = \phi^s(x)(\psi(x))^m \text{ implies } \phi_1^r(x) = \phi_1^s(x)(\psi_1(x))^m, \tag{8.6}$$

where $\phi_1(x) = 1/\phi(1/x)$ and $\psi_1(x) = 1/\psi(1/x)$; note in particular that if $\psi \in K(x)$, then $\psi_1 \in K(x)$. Because $\phi_1^{-n}(0) = \phi^{-n}(\infty)$, we have that ∞ is also m-branch abundant for ϕ.

Assume henceforth that 0 and ∞ are m-branch abundant; we will show that there exist r and s as described in the previous paragraph. From (8.6) and the remark following, it suffices to show that for all ϕ, the desired conclusion holds for either ϕ or $\mu \circ \phi \circ \mu^{-1}$, where $\mu(x) = 1/x$.

If ϕ is m-trivial with respect to $\{0, \infty\}$, then the desired conclusion follows from Lemma 8.1. If ϕ is not m-trivial with respect to $\{0, \infty\}$, then $m \le 4$ by Theorem 3.8, and $O_\phi^-(0)$ and $O_\phi^-(\infty)$ are described in one of Theorems 4.7, 4.6, or 5.3, according to whether $m = 2, 3$, or 4. We consider each of these cases separately.

Case 1: $\boldsymbol{m = 4}$. If $O_\phi^-(\alpha_1)$ has 4-ramification structure (13) for either $\phi(x)$ or $1/\phi(1/x)$), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let β be the unique preimage of 0 with ramification index 2. Then

$$\phi(x) = M\frac{(x-\beta)^2 f(x)^4}{xg(x)^4}$$

where the numerator and denominator are relatively prime, f and g are monic, and $M \in \mathbb{C}^*$. As with the function in (7.1), we use Theorem 6.2 to conclude that $M \in K$ and f, g, and $(x-\beta)^2$ are all in $K[x]$. Therefore, $\phi(x) \equiv M(x-\beta)^2/x \pmod{K(x)^{*4}}$, and hence

$$\phi^2(x) \equiv M\big(\phi(x) - \beta\big)^2/\phi(x) \pmod{K(x)^{*4}}. \tag{8.7}$$

Note that $(x-\beta)^2 \in K[x]$ implies $2\beta \in K$, and so $\beta \in K$. Now,

$$\phi(x) - \beta = \frac{1}{xg(x)^4}\big[M(x-\beta)^2 f(x)^4 - \beta x g(x)^4\big].$$

Let $u(x) = M(x-\beta)^2 f(x)^4 - \beta x g(x)^4$. The roots (with multiplicity) of u are the preimages (with multiplicity) of β under ϕ, and hence $u(x) = bh(x)^2$, with $h \in \mathbb{C}[x]$

monic and $b \in \mathbb{C}\setminus\{0\}$. Applying Theorem 6.2 again, we have $b \in K$ and $h \in K[x]$. This shows that $\phi(x) - \beta \in \frac{b}{x}K(x)^{*2} = bxK(x)^{*2}$, and so $(\phi(x)-\beta)^2 \in b^2x^2K(x)^{*4}$. Now $bh(\beta)^2 = u(\beta) = -\beta^2 g(\beta)^4$, and because $g(\beta) \neq 0$ (otherwise $\phi(\beta) \neq 0$, contrary to supposition), we have $-b \in K^2$, and squaring gives $b^2 \in K^4$. Therefore, $(\phi(x) - \beta)^2 \in x^2K(x)^{*4}$. Similarly, putting $x = 0$ in $u(x)$ yields $Mb \in K^2$, and hence $M^2 \in K^4$ (one could also use Lemma 8.2 to derive this latter fact). Returning to (8.7) now gives

$$\phi^2(x) \equiv M\frac{(\phi(x)-\beta)^2}{\phi(x)} \equiv x^2 \cdot \frac{x}{(x-\beta)^2} \equiv x^3(x-\beta)^2 \pmod{K(x)^{*4}}.$$

Thus, modulo $K(x)^{*4}$, we have $\phi^3(x) \equiv (\phi(x))^3(\phi(x)-\beta)^2 \equiv M^3(x-\beta)^2/x \equiv \phi(x)$, where the last equivalence follows, because $M^2 \in K^4$. Hence, (1.1) holds with $r = 3$ and $s = 1$, and from Proposition 2.3 we have $g_n = 1$ for all $n \geq 1$.

If $O_\phi^-(\alpha_1)$ has 4-ramification structure (14) for either $\phi(x)$ or $1/\phi(1/x)$), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let β be the unique preimage of ∞ with ramification index 2. Then

$$\phi(x) = \frac{Mf(x)^4}{(x(x-\beta)^2 g(x)^4)} \qquad \text{and} \qquad \phi(x) - \beta = \frac{u(x)}{(x(x-\beta)^2 g(x)^4)},$$

with

$$u(x) := Mf(x)^4 - \beta x(x-\beta)^2 g(x)^4 = bh(x)^2. \tag{8.8}$$

Taking $x = \beta$ or $x = 0$ in (8.8) yields $b/M \in K^2$, and thus $b^2M^2 \in K^4$, but no further information. However, by Corollary 7.3 we have that ϕ is Lattès of signature (2,4,4) with $r(\infty) = 4$, and so from Lemma 8.2 we get $M^2 \in K^4$, whence $b^2 \in K^4$. One now obtains $\phi^2(x) \equiv x^3(x-\beta)^2 \pmod{K(x)^{*4}}$ and $\phi^3(x) \equiv \phi(x) \pmod{K(x)^{*4}}$ using an argument virtually identical to the previous case. The same conclusions about r, s, and g_n hold.

Remark The same general template as in the $m = 4$ case is applied to further cases below, and we omit certain details. For example, Theorem 6.2 is frequently applied in subsequent cases to show that relevant polynomials and constants are defined over K. Hence, from now on we assume that f and g are monic relatively prime polynomials with coefficients in K, and that $b, b_1, b_2 \in K$ and $h, h_1, h_2 \in K[x]$ are monic.

Case 2: $m = 3$. We invoke Theorem 4.6 with $\mu(x) = 1/x$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (3A), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and let γ be the unique preimage of 0 with ramification index 1. Hence,

$$\phi(x) = \gamma\frac{(x-\gamma)f(x)^3}{xg(x)^3}, \quad \phi(x) - \gamma = \frac{u(x)}{xg(x)^3},$$

where $u(x) := \gamma(x-\gamma)f(x)^3 - \gamma x g(x)^3 = bh(x)^3$ and the initial γ in ϕ is because $\phi(\infty) = \gamma$. Putting $x = 0$ in $u(x)$ gives $-b/\gamma^2 \in K^3$, and so $b\gamma \in K^3$, implying that $\phi(x) - \gamma \in \gamma^2x^2K(x)^{*3}$. It is then straightforward to check that $\phi^2(x) \equiv \gamma^2(x-\gamma)^2 \pmod{K(x)^{*3}}$, and $\phi^3(x) \equiv x \pmod{K(x)^{*3}}$. Hence, (1.1) holds with $r = 3$ and $s = 0$, and from Proposition 2.3 we have $g_n = 0$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (3B), then we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, and let γ be the unique preimage of 0 with ramification index 1. Writing

$$\phi(x) = M(x-\beta)f(x)^3/g(x)^3$$

and arguing as in the previous case, one obtains $\phi^2(x) \in xK(x)^{*3}$. Thus, (1.1) holds with $r = 2$ and $s = 0$, and $g_n = 0$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (3C), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and let β be the unique element of $\phi^{-1}(\infty) \setminus \{0,\infty\}$ with ramification index 1. Then $\phi(x) = Mf(x)^3/(x(x-\beta)g(x)^3)$ and $\phi(x)-\beta = u(x)/(x(x-\beta)g(x)^3)$ with $u(x) := Mf(x)^3 - \beta x(x-\beta)g(x)^3 = bh(x)^3$. Putting $x = 0$ or $x = \beta$ gives $b^2M \in K^3$ but no further information. However, by Corollary 7.3 we have that ϕ is Lattès of signature (3,3,3) with $r(\infty) = 3$, and so from Lemma 8.2 we get $M \in K^3$, whence $b \in K^3$. One now easily calculates $\phi^2(x) \equiv x^2(x-\beta)^2 \equiv \phi(x) \pmod{K(x)^{*3}}$. Thus, (1.1) holds with $r = 2$ and $s = 1$, and from Proposition 2.3, we have $g_n = 1$ for all $n \geq 1$.

Case 3: $\boldsymbol{m}$ = 2. We invoke Theorem 4.7 with $\mu(x) = 1/x$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2A), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and let γ be the unique preimage of 0 with multiplicity 1, and δ be the unique preimage of γ with multiplicity 1. Thus,

$$\phi(x) = \delta\frac{(x-\gamma)f(x)^2}{xg(x)^2}, \quad \phi(x)-\gamma = \frac{u_1(x)}{xg(x)^2}, \quad \phi(x)-\delta = \frac{u_2(x)}{xg(x)^2},$$

where

$$\begin{aligned} u_1(x) &:= \delta(x-\gamma)f(x)^2 - \gamma xg(x)^2 = b_1(x-\delta)h_1(x)^2, \\ u_2(x) &:= \delta(x-\gamma)f(x)^2 - \delta xg(x)^2 = b_2h_2(x)^2. \end{aligned}$$

Taking $x = 0$ in $u_1(x)$ yields $b_1 \in \gamma K^2$, and taking $x = 0$ in $u_2(x)$ gives $b_2 \in -\delta\gamma K^2$. Then one calculates $\phi^2(x) \equiv \gamma(x-\gamma)(x-\delta) \pmod{K(x)^{*2}}$, $\phi^3(x) \equiv -\gamma\delta(x-\delta) \pmod{K(x)^{*2}}$, and $\phi^4(x) \equiv x \pmod{K(x)^{*2}}$, so that (1.1) holds with $r = 4$ and $s = 0$, and $g_n = 0$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2B), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and let γ be the unique preimage of ∞ with multiplicity 1, and δ be the unique preimage of 0 with multiplicity 1. Arguing as in (2A) gives

$$\begin{aligned} \phi(x) &\equiv \delta(x-\gamma)(x-\delta) \pmod{K(x)^{*2}}, \\ \phi^2(x) &\equiv \gamma\delta x \pmod{K(x)^{*2}}, \phi^3(x) \equiv \gamma(x-\gamma)(x-\delta) \pmod{K(x)^{*2}}, \end{aligned}$$

and $\phi^4(x) \equiv x \pmod{K(x)^{*2}}$. Hence, (1.1) holds with $r = 4$ and $s = 0$, and $g_n = 0$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2C), then we take $\alpha_1 = 0$ and $\alpha_2 = \infty$, and let β be the unique preimage of 0 with odd multiplicity, and γ be the unique preimage of β with odd multiplicity. Thus,

$$\phi(x) = \frac{M(x-\beta)f(x)^2}{g(x)^2}, \quad \phi(x)-\beta = \frac{u_1(x)}{g(x)^2}, \quad \phi(x)-\gamma = \frac{u_2(x)}{g(x)^2},$$

where

$$u_1(x) := M(x-\beta)f(x)^2 - \beta g(x)^2 = b_1(x-\gamma)h_1(x)^2,$$
$$u_2(x) := M(x-\beta)f(x)^2 - \gamma g(x)^2 = b_2 x h_2(x)^2.$$

Substituting $x=\gamma$ and $x=\beta$ into $u_1(x)$ gives $\beta M(\gamma-\beta)\in K^2$ and $b_1\beta M(\gamma-\beta)\in K^2$, respectively. Hence, $b_1\in K^2$. Similar reasoning using u_2 gives $b_2\in K^2$. We now have the following equivalencies modulo $K(x)^{*2}$:

$$\phi(x)\equiv M(x-\beta),\qquad \phi^2(x)\equiv M(x-\gamma),\qquad \phi^3(x)\equiv Mx,$$
$$\phi^4(x)\equiv (x-\beta),\qquad \phi^5(x)\equiv (x-\gamma),\qquad \phi^6(x)\equiv x,$$

showing that (1.1) holds with $r=6$ and $s=0$, and $g_n=0$ for all $n\ge 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2D), then we take $\alpha_1=0$ and $\alpha_2=\infty$ and let C be the unique preimage of ∞ with odd multiplicity. Then (7.1) and (7.2) give $\phi^2(x)\equiv Cx(x-C) \pmod{K(x)^{*2}}$, and $\phi^3(x)\equiv Cbx\equiv x \pmod{K(x)^{*2}}$, showing that (1.1) holds with $r=3$ and $s=0$, and $g_n=0$ for all $n\ge 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2E), then we take $\alpha_1=\infty$, $\alpha_2=0$, β_1 to be the unique preimage of ∞ with odd ramification index, and β_2 to be the unique preimage of 0 with odd ramification index. This gives

$$\phi(x)=\beta_1\frac{(x-\beta_2)f(x)^2}{(x-\beta_1)g(x)^2},\quad \phi(x)-\beta_1=\frac{u_1(x)}{(x-\beta_1)g(x)^2},$$
$$\phi(x)-\beta_2=\frac{u_2(x)}{(x-\beta_1)g(x)^2},$$

where

$$u_1(x) := \beta_1(x-\beta_2)f(x)^2-\beta_1(x-\beta_1)g(x)^2=b_1h_1(x)^2,$$
$$u_2(x) := \beta_1(x-\beta_2)f(x)^2-\beta_2(x-\beta_1)g(x)^2=b_2xh_2(x)^2.$$

Taking $x=\beta_1$ in $u_1(x)$ and $u_2(x)$ gives $b_1\beta_1(\beta_1-\beta_2)\in K^2$ and $b_2\beta_1(\beta_1-\beta_2)\in K^2$, which together imply $b_1b_2\in K^2$. It is now straightforward to check that $\phi^2(x)\equiv b_1b_2x\equiv x \pmod{K(x)^{*2}}$, whence (1.1) holds with $r=2$ and $s=0$, and $g_n=0$ for all $n\ge 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2F), then we take $\alpha_1=\infty$ and $\alpha_2=0$, and we let C be the unique preimage of 0 with odd ramification index. Then $\phi(x)=B(x-C)f(x)^2/g(x)^2$ and $\phi(x)-C=u(x)/g(x)^2$ with $B,C\in K^*$ and $u(x):=B(x-C)f(x)^2-Cg(x)^2=bxh(x)^2$. Putting $x=0$ in $u(x)$ gives $-B\in K^2$, and putting $x=C$ then gives $b\in K^2$. It easily follows that $\phi^2(x)\equiv x \pmod{K(x)^{*2}}$. Hence, (1.1) holds with $r=2$ and $s=0$, and $g_n=0$ for all $n\ge 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2G), then we take $\alpha_1=\infty$ and $\alpha_2=0$, and we let β_1,β_2 be the elements of $\phi^{-1}(\infty)\smallsetminus\{0,\infty\}$ with ramification index 1. Then for $i=1,2$, we have

$$\phi(x)=M\frac{f(x)^2}{x(x-\beta_1)(x-\beta_2)g(x)^2},\quad \phi(x)-\beta_i=\frac{u_i(x)}{x(x-\beta_1)(x-\beta_2)g(x)^2},$$

where

$$u_i(x) := Mf(x)^2-\beta_ix(x-\beta_1)(x-\beta_2)g(x)^2=b_ih_i(x)^2.$$

Putting $x = 0$ in $u_i(x)$ gives $Mb_i \in K^2$ for $i = 1,2$ and multiplying yields $b_1b_2 \in K^2$. One now calculates

$$\phi^2(x) \equiv x(x-\beta_1)(x-\beta_2) \pmod{K(x)^{*2}},$$
$$\phi^3(x) \equiv Mx(x-\beta_1)(x-\beta_2) \equiv \phi(x) \pmod{K(x)^{*2}}.$$

Hence, (1.1) holds with $r = 3$ and $s = 1$, and $g_n = 1$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2H), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, we let β be the unique element of $\phi^{-1}(\infty) \smallsetminus \{0\}$ with ramification index 1, and we let γ be the unique element of $\phi^{-1}(0) \smallsetminus \{\infty\}$ with ramification index 1. Then

$$\phi(x) = C\frac{(x-\gamma)f(x)^2}{x(x-\beta)g(x)^2}, \quad \phi(x) - \gamma = \frac{u_1(x)}{x(x-\beta)g(x)^2},$$
$$\phi(x) - \beta = \frac{u_2(x)}{x(x-\beta)g(x)^2},$$

where

$$u_1(x) := C(x-\gamma)f(x)^2 - \gamma x(x-\beta)g(x)^2 = b_1h_1(x)^2,$$
$$u_2(x) := C(x-\gamma)f(x)^2 - \beta x(x-\beta)g(x)^2 = b_2h_2(x)^2.$$

Putting $x = 0$ in $u_1(x)$ gives $-C\gamma b_1 \in K^2$, putting $x = \gamma$ in $u_1(x)$ gives $(\beta-\gamma)b_1 \in K^2$, and putting $x = \beta$ in $u_1(x)$ gives $C(\beta-\gamma)b_1 \in K^2$. In particular, $C \in K^2$. Putting $x = 0$ in $u_2(x)$ yields $-C-\gamma b_2 \in K^2$, and thus $b_1b_2 \in K^2$. Now we obtain $\phi^2(x) \equiv b_1b_2x(x-\beta)(x-\gamma) \equiv \phi(x) \pmod{K(x)^{*2}}$. Hence, (1.1) holds with $r = 2$ and $s = 1$, and $g_n = 1$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2I), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let $\beta = \phi(\infty)$, and γ the unique element of $\phi^{-1}(\beta) \smallsetminus \{\infty\}$ with ramification index 1. An argument similar to that of case (2H) shows that we have the following equivalences modulo $K(x)^{*2}$: $\phi^2(x) \equiv -\beta\gamma(x-\gamma), \phi^3(x) \equiv -\gamma x(x-\beta), \phi^4(x) \equiv (x-\gamma)$, and $\phi^5(x) \equiv \beta x(x-\beta) \equiv \phi(x)$. Thus, (1.1) holds with $r = 5$ and $s = 1$, and $g_n = 0$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2J), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let $\beta = \phi(0)$, and let γ be the unique element of $\phi^{-1}(\infty) \smallsetminus \{\beta\}$ with ramification index 1. Arguing as in case (2H), we obtain $\phi^2(x) \equiv x \pmod{K(x)^{*2}}$, and thus (1.1) holds with $r = 2$ and $s = 1$, and we have $g_n = 0$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2K), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let γ_1 and γ_2 be the two preimages of 0 with ramification index 1. Thus,

$$\phi(x) = \frac{M(x-\gamma_1)(x-\gamma_2)f(x)^2}{(xg(x)^2)}, \quad \phi(x) - \gamma_1 = \frac{u_1(x)}{(xg(x)^2)}, \quad \phi(x) - \gamma_2 = \frac{u_2(x)}{(xg(x)^2)},$$

where $u_i(x) := M(x-\gamma_1)(x-\gamma_2)f(x)^2 - \gamma_i xg(x)^2 = b_ih_i(x)^2$ for $i = 1,2$. Putting $x = 0$ in $u_i(x)$ yields $Mb_i\gamma_1\gamma_2 \in K^2$, whence $b_1b_2 \in K^2$, and it follows that $(\phi(x) - \gamma_1)(\phi(x) - \gamma_2) \in K(x)^{*2}$. One now calculates

$$\phi^2(x) \equiv x(x-\gamma_1)(x-\gamma_2) \pmod{K(x)^{*2}},$$
$$\phi^3(x) \equiv Mx(x-\gamma_1)(x-\gamma_2) \equiv \phi(x) \pmod{K(x)^{*2}}.$$

Hence, (1.1) holds with $r = 3$ and $s = 1$, and $g_n = 1$ for all $n \geq 1$.

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2L), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let $\beta = \phi(0)$ and γ be the non-zero preimage of β with ramification index 1. Writing $\phi(x) = Mf(x)^2/((x-\beta)g(x)^2)$ and arguing as in case (2K), we obtain $\phi(x) \in M(x-\beta)K(x)^{*2}$, $\phi(x) - \beta \in Mx(x-\beta)(x-\gamma)K(x)^{*2}$, and $\phi(x) - \gamma \in M(x-\beta)K(x)^{*2}$. It follows that $\phi^2(x) \equiv x(x-\beta)(x-\gamma) \pmod{K(x)^{*2}}$, $\phi^3(x) \equiv Mx(x-\beta)(x-\gamma) \pmod{K(x)^{*2}}$, and $\phi^4(x) \equiv \phi^2(x) \pmod{K(x)^{*2}}$. Thus, (1.1) holds with $r = 4$ and $s = 2$, and we have $g_1 = 0$ and $g_n = 1$ for all $n \geq 2$. This is the only case where g_n is non-constant.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2M), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let C be the unique non-zero preimage of ∞ with odd ramification index. Writing $\phi(x) = B(x-C)f(x)^2/g(x)^2$ with $B \in K^*$, we obtain $\phi(x) - C \in -CK(x)^{*2}$, and hence $\phi^n(x) \equiv -BC \pmod{K(x)^{*2}}$ for all $n \geq 2$. Thus, (1.1) holds with $r = 3$ and $s = 2$, and $g_n = 0$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2N), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let β_1 (resp. β_2) be the unique preimage of ∞ (resp. 0) with ramification index 1. We have

$$\phi(x) = M\frac{x(x-\beta_2)f(x)^2}{(x-\beta_1)g(x)^2}, \quad \phi(x) - \beta_1 = \frac{u_1(x)}{(x-\beta_1)g(x)^2},$$
$$\phi(x) - \beta_2 = \frac{u_2(x)}{(x-\beta_1)g(x)^2},$$

where $u_i(x) := Mx(x-\beta_2)f(x)^2 - \beta_i(x-\beta_1)g(x)^2 = b_i h_i(x)^2$ for $i = 1, 2$. Putting $x = 0$ in $u_1(x)$ yields $b_1 \in K^2$. Putting $x = \beta_2$ in $u_i(x)$ yields $\beta_i(\beta_1 - \beta_2)b_i \in K^2$, and putting $x = \beta_1$ in $u_i(x)$ yields $M\beta_1(\beta_1 - \beta_2)b_i \in K^2$. The latter immediately implies $b_1 b_2 \in K^2$, so $b_2 \in K^2$. Using $\beta_1(\beta_1 - \beta_2)b_1 \in K^2$ and $M\beta_1(\beta_1 - \beta_2)b_1 \in K^2$ implies $M \in K^2$, and it quickly follows that $\phi^2(x) \equiv x(x-\beta_1)(x-\beta_2) \equiv \phi(x) \pmod{K(x)^2}$. Hence (1.1) holds with $r = 2$ and $s = 1$, and $g_n = 1$ for all $n \geq 1$.

If either $\phi(x)$ or $1/\phi(1/x)$ satisfies (2O), then we take $\alpha_1 = \infty$ and $\alpha_2 = 0$, and we let C be the unique non-zero preimage of 0 with odd ramification index. Writing $\phi(x) = Bx(x-C)f(x)^2/g(x)^2$ with $B \in K^*$, we obtain $\phi(x) - C \in -CK(x)^{*2}$, whence $\phi^2(x) \equiv -Cx(x-C) \pmod{K(x)^{*2}}$ and $\phi^3(x) \equiv \phi(x) \pmod{K(x)^{*2}}$. Thus (1.1) holds with $r = 3$ and $s = 1$, and $g_n = 0$ for all $n \geq 1$. ■

9 Proofs of Remaining Results

Proof of Corollary 1.3 Let K be a finitely generated field of characteristic zero, fix $m \geq 2$, let $\phi \in K(x)$ have degree at least two, and assume there exists $a \in \mathbb{P}^1(K)$ such that $O_\phi^+(a) \cap \mathbb{P}^1(K)^m$ is infinite. Let C_n be the curve given by $\phi^n(x) = y^m$; in the notation of the discussion following Conjecture 1.6, we then have $X = \mathbb{P}^1$, $Y = \mathbb{P}^1$, $\lambda(x) = x^m$, and $Z_n = C_n$. Then (1.8) implies that $C_n(K)$ is infinite for all $n \geq 1$, and it follows from Faltings' Theorem that $g_n \leq 1$ for all $n \geq 1$. Hence, ϕ falls into one of the cases in Theorem 1.2 and satisfies (1.3) and (1.4), and ϕ also satisfies (1.1) with $\psi \in K(x)$. ■

Proof of Theorem 1.5 Let K be a finitely generated field of characteristic zero, let $\phi, \lambda \in K(x)$ have degree at least two, and suppose that λ is Möbius-conjugate (over

K) to a power map. From equation (1.7) in the introduction, it suffices to show that the set $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ satisfies the conclusions of the theorem for any $\phi \in K(x)$ and $a \in \mathbb{P}^1(K)$. Take $a \in \mathbb{P}^1(K)$, and note that the theorem holds when $O_\phi(a) \cap \mathbb{P}^1(K)^m$ is finite, by the discussion following the statement of Theorem 1.5. Suppose for the rest of the proof that $O_\phi^+(a) \cap \mathbb{P}^1(K)^m$ is infinite. We will show that $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a union of at most three arithmetic progressions with modulus at most m (or 6 if $m = 2$). As in the proof of Corollary 1.3, we use Faltings' Theorem to derive $g_n \le 1$ for all $n \ge 1$, and hence Corollary 2.5 gives that 0 and ∞ are m-branch abundant points for ϕ.

By Theorem 1.1, there are $r > s \ge 0$ with $\phi^r(x) \equiv \phi^s(x) \pmod{K(x)^{*m}}$. The sequence $(\phi^n(x))_{n\ge0}$ in the group $K(x)^*/K(x)^{*m}$ therefore has the form

$$x, \phi(x), \dots, \phi^s(x), \dots, \phi^{r-1}(x), \phi^s(x), \dots, \phi^{r-1}(x), \phi^s(x), \dots .$$

Observe that if $\psi \in K(x)$, $b \in K$, and $\psi(b) \notin \{0, \infty\}$, then $\psi(b) \in K^m$ if and only if $\widetilde{\psi}(b) \in K^m$ for every $\widetilde{\psi} \in K(x)$ with $\psi(x) \equiv \widetilde{\psi}(x) \pmod{K(x)^{*m}}$. Let $J = \{s \le n \le r-1 : \phi^n(a) \in K^m\}$. If $O_\phi^+(a) \cap \{0,\infty\} = \varnothing$, then it follows that

$$\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\} = I \cup F$$

with

$$I = \bigcup_{j\in J} (j + (r-s)\mathbb{N}) \quad \text{and} \quad F = \{0 \le n < s : \phi^n(a) \in K^m\}. \tag{9.1}$$

Suppose first that ϕ is m-trivial with respect to $\{0,\infty\}$, and write $\phi(x) = cx^j(\psi_0(x))^m$ as in Proposition 3.2. Let t be the minimal positive integer such that $c^t \in K^m$. If $j = 0$ and $t > 1$, then we have $c \notin K^m$, and hence $\phi(b) \notin K^m$ for all $b \in \mathbb{P}^1(K)$ with $\phi(b) \notin \{0,\infty\}$. This forces $O_\phi^+(a) \cap \mathbb{P}^1(K)^m$ to be finite, a contradiction. If $j = 0$ and $t = 1$, then $c \in K^m$, whence $\phi(b) \in K^m$ for all $b \in \mathbb{P}^1(K)$, implying that $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\} = \ell + M\mathbb{N}_0$ with $M = 1$ and $\ell = 0$ (if $a \in K^m$) or $\ell = 1$ (otherwise).

If $j > 0$, then because $0 < j < m$ and the order of any zero or pole of ψ^m is divisible by m, we must have $\phi(0) \in \{0,\infty\}$ and $\phi(\infty) \in \{0,\infty\}$. The infinitude of $O_\phi^+(a)$ then implies that $O_\phi^+(a) \cap \{0,\infty\} = \varnothing$. We could now use (9.1) to show that $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a union of finitely many arithmetic progressions, but we wish to prove the stronger statement that it is a single arithmetic progression. Let ℓ be the minimal non-negative integer with $\phi^\ell(a) \in \mathbb{P}^1(K)^m$, and because $\phi^\ell(a) \ne \infty$, we can write $\phi^\ell(a) = b^m$ for some $b \in K$. From (8.3) and the fact that $O_\phi^+(a) \cap \{0,\infty\} = \varnothing$, for all $u \ge 1$ we have $\phi^{\ell+u}(a) \in K^m$ if and only if $c^{1+j+\cdots+j^{u-1}} \in K^m$. This in turn is equivalent to

$$1 + j + \cdots + j^{u-1} \equiv 0 \bmod t. \tag{9.2}$$

If $\gcd(t,j) \ne 1$, then (9.2) cannot hold for any $u \ge 1$, giving the contradiction $O_\phi^+(a) \cap \mathbb{P}^1(K)^m = \{\phi^\ell(a)\}$. Therefore, $\gcd(t,j) = 1$. If $j = 1$, then (9.2) holds if and only if u is a multiple of t, and we have $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\} = \ell + t\mathbb{N}_0$. If $j > 1$, then note that j is relatively prime to both $j-1$ and t, and let M be the order of j in $(\mathbb{Z}/t(j-1)\mathbb{Z})^*$. Then (9.2) is equivalent to $j^u - 1 \equiv 0 \bmod t(j-1)$, which holds if and only if u is a multiple of M. Hence, $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\} = \ell + M\mathbb{N}_0$.

Suppose that ϕ is not m-trivial with respect to $\{0,\infty\}$. Then $m \le 4$ by Theorem 3.8, and so either $\phi(x)$ or $\phi_1(x) := 1/\phi(1/x)$ is described by one of Theorems 4.6, 4.7, or 5.3. Note that if $O_\phi^+(0)$ and $O_\phi^+(\infty)$ are both finite, then $O_{\phi_1}(0)$ and $O_{\phi_1}(\infty)$ are also finite. Hence, if either ϕ or ϕ_1 satisfies any of the conclusions of Theorems 4.6, 4.7, or 5.3 except for (2M) and (2O) in Theorem 4.7, we have that $O_\phi^+(0)$ and $O_\phi^+(\infty)$ are both finite, whence the infinitude of $O_\phi^+(a)$ implies that $O_\phi^+(a) \cap \{0,\infty\} = \varnothing$. We can then use (9.1) to conclude that $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ consists of at most s arithmetic progressions of modulus 0 (*i.e.*, singletons) plus at most k infinite arithmetic progressions of modulus dividing $r-s$, where $k=(r-s)/2$ if $r-s$ is even and $k=s-1$ if $r-s$ is odd. From the proof of Theorem 1.1 we have in each case that $s+k \le 3$, $r-s \le m$ for $m \ge 3$, and $r-s \le 6$ for $m=2$.

Finally, suppose that either ϕ or ϕ_1 satisfies (2M) or (2O) of Theorem 4.7. Because $O_\phi^+(a)$ is infinite, each of 0 and ∞ can appear at most once in the sequence $(\phi^n(a))_{n\ge 0}$. In case (2M) we have $\phi^n(x) \equiv \phi^2(x) \pmod{K}(x)^{*2}$ for all $n \ge 2$, and the infinitude of $O_\phi^+(a) \cap \mathbb{P}^1(K)^m$ implies that $\phi^n(a) \in \mathbb{P}^1(K)^m$ for all $n \ge 2$. It follows that $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a union of at most two arithmetic progressions. In case (2O), observe that precisely one of $0,\infty$ has infinite forward orbit, and hence at most one of them can appear in $O_\phi^+(a)$; without loss of generality, say this is ∞. From the last paragraph of the proof of Theorem 1.1, we can take $r=3$ and $s=1$ in (1.1), and the infinitude of $O_\phi^+(a) \cap \mathbb{P}^1(K)^m$ implies that one of the following holds: $\phi^n(a) \in \mathbb{P}^1(K)^m$ for all $n \ge 1$; $\phi^{2n}(a) \in \mathbb{P}^1(K)^m$ for all $n \ge 1$ and $\phi^{2n-1}(a) \notin \mathbb{P}^1(K)^m$ for all $n \ge 1$ except at most one value of n with $\phi^{2n-1}(a)=\infty$; or $\phi^{2n-1}(a) \in \mathbb{P}^1(K)^m$ for all $n \ge 1$ and $\phi^{2n}(a) \notin \mathbb{P}^1(K)^m$ for all $n \ge 1$ except at most one value of n with $\phi^{2n}(a)=\infty$. In each of these cases, $\{n \ge 1 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a union of at most two arithmetic progressions, and thus $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(K)^m\}$ is a union of at most three arithmetic progressions. ■

Finally, we prove Corollaries 1.8 and 1.9. The following lemma aids in the proof of Corollary 1.8.

Lemma 9.1 ([20, Lemma 6, p. 26]) *Let F be a field of characteristic* $\ne 2$, *and suppose that*

$$\big(Q(x)-q_1\big)\big(Q(x)-q_2\big) = (x-\xi_1)(x-\xi_2)\big(R(x)\big)^2,$$

for $Q,R \in F[x]$, $q_1,q_2,\xi_1,\xi_2 \in F$, $q_1 \ne q_2$, $\xi_1 \ne \xi_2$. *Then* $Q = L \circ T_{\deg Q} \circ M^{-1}$, *where*

$$L(x) = \frac{q_1-q_2}{4}x + \frac{q_1+q_2}{2} \quad \textit{and} \quad M(x) = \frac{\xi_1-\xi_2}{4}x + \frac{\xi_1+\xi_2}{2}.$$

Proof of Corollary 1.8 Let K be a finitely generated field of characteristic zero, fix $m \ge 2$, let $\phi \in K[x]$ have degree $d \ge 2$, and assume there exists $a \in \mathbb{P}^1(K)$ such that $O_\phi^+(a) \cap \mathbb{P}^1(K)^m$ is infinite. As in the proof of Corollary 1.3, we use Faltings' Theorem to derive $g_n \le 1$ for all $n \ge 1$; indeed, in this case we can use Siegel's theorem to show $g_n = 0$ for all $n \ge 1$, though we do not need this stronger conclusion. Corollary 2.5 then gives that 0 and ∞ are m-branch abundant points for ϕ. If ϕ is m-trivial with respect to $\{0,\infty\}$, then Proposition 3.2 and Lemma 6.1 imply Corollary 1.8(i).

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

Suppose that ϕ is not m-trivial with respect to $\{0,\infty\}$. Then $m \le 4$ by Theorem 3.8, and so either $\phi(x)$ or $\phi_1(x) := 1/\phi(1/x)$ is described by one of Theorems 4.6, 4.7, or 5.3. Minor modifications to the proof of Lemma 4.4 show that ϕ has at most one 3-branch abundant point in $\mathbb{C}$, and at most two 2-branch abundant points in $\mathbb{C}$. Indeed, in the proof of Lemma 4.4, let $V = \{\alpha_1, \dots, \alpha_k\} \subset \mathbb{C}$ be a set of p-branch abundant points for ϕ. Because $\sum_{z\in\mathbb{C}}(e_\phi(z) - 1) = d - 1$, the bound in (4.3) implies that $k = 1$ if $p = 3$ and $k \le 2$ if $p = 2$, as desired. Hence, ϕ has at most three 2-branch abundant points in $\mathbb{P}^1(\mathbb{C})$, and at most two 3-branch abundant points in $\mathbb{P}^1(\mathbb{C})$, and in both cases one of these is a fixed point whose only preimage is itself. The same statements hold for $\phi_1(x)$. This rules out all cases of Theorems 4.6, 4.7, and 5.3, except for (2F) (where d is odd) and (2O) (where d is even) in Theorem 4.7. In both of those cases, let $\{\infty, 0, \beta\}$ be the 2-branch abundant points for ϕ, and note that ∞ must be the fixed point. It follows that the conditions of Lemma 9.1 are satisfied with $\{q_1, q_2\} = \{\xi_1, \xi_2\} = \{0, \beta\}$, and thus $L(x) = -(\beta/4)(\epsilon_L x - 2)$ and $M(x) = -(\beta/4)(\epsilon_M x - 2)$, with $\epsilon_L, \epsilon_M \in \{1, -1\}$. Setting $c = -4/\beta$, we then have

$$c\phi(x/c) = \epsilon_L\big(T_d(\epsilon_M(x+2))\big) - 2. \tag{9.3}$$

If d is odd, then T_d is an odd function, T_d fixes both 2 and -2, and $\phi(0) \ne 0$ from 2-ramification structure (2F). Putting $x = 0$ in (9.3) gives $\epsilon_L\epsilon_M = -1$. Because d is odd, T_d is an odd function, and so in both cases $\epsilon_L = 1, \epsilon_M = -1$ and $\epsilon_L = -1, \epsilon_M = 1$, we have $c\phi(x/c) = -(T_d(x+2)) - 2$. If d is even, then T_d is an even function, $T_d(\pm 2) = 2$, and $\phi(0) = 0$ from 2-ramification structure (2O). Putting $x = 0$ in (9.3) then gives $\epsilon_L = -1$, implying $c\phi(x/c) = T_d(\pm(x+2)) - 2 = T_d(x+2) - 2$.

It remains only to show that $c \in K$. But $\phi \in K[x]$ by assumption, and $\phi(x) \in (x-\beta)\mathbb{C}[x]^{*2}$ if d is odd and $\phi(x) \in x(x-\beta)\mathbb{C}[x]^{*2}$ if d is even. From Theorem 6.2 we have $\beta \in K$, whence $c \in K$. ■

Proof of Corollary 1.9 Let $\phi \in \mathbb{Q}[x]$ have degree 2, and suppose that ϕ has a rational orbit containing infinitely many distinct squares. Then Corollary 1.8 implies that either (1) $\phi(x) = c(g(x))^2$ for some $g \in \mathbb{Q}(x)$ or (2) $c\phi(x/c) = T_2(x+2) - 2 = x^2 + 4x$ with $c \in \mathbb{Q}^*$. In case (1), we must have $c \in \mathbb{Q}^{*2}$, for otherwise ϕ has no rational orbits with infinitely many distinct squares; hence ϕ satisfies (i) of the present corollary. In case (2), putting $x = cX$ gives $\phi(X) = (c^2X^2 + 4cX)/c = cX^2 + 4X$, and so ϕ satisfies (ii) of the present corollary.

Assume now that ϕ satisfies (i) or (ii) of the present corollary. For maps satisfying (i), all infinite orbits contain infinitely many distinct squares. For maps satisfying (ii), a simple calculation shows that $\phi^2(x) = \phi(x)(g_2(x))^2$ for some $g_2 \in \mathbb{Q}[x]$, and it immediately follows that $\phi^2(x) = \phi(x)(g_n(x))^2$ for some $g_n \in \mathbb{Q}[x]$ for each $n \ge 1$. Hence for $a \in \mathbb{Q}$, $O_\phi^+(a)$ contains infinitely many squares if and only if a is the x-coordinate of a rational point on the curve $C : y^2 = cx^2 + 4x$. But C has genus zero and the rational point $(0, 0)$, and thus $C(\mathbb{Q})$ is infinite. By Northcott's theorem [16], ϕ has only finitely many rational points with finite orbits, and hence there must be a rational orbit of ϕ containing infinitely many distinct squares. ■

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

10 An Example

In this section we present an example of a rational function $\phi \in \mathbb{Q}(x)$ of degree 2 and $a \in \mathbb{Q}$ such that $O_\phi^+(a) \cap \mathbb{P}^1(\mathbb{Q})^2$ is infinite and $\{n \in \mathbb{N}_0 : \phi^n(a) \in \mathbb{P}^1(\mathbb{Q})^2\}$ cannot be written as union of fewer than three arithmetic progressions. By the proof of Theorem 1.5, such an example cannot be 2-trivial with respect to $\{0,\infty\}$, and hence satisfies one of the conditions of Theorem 4.7. Our example satisfies (2O) of this theorem, and hence has the form (5d) in Theorem 1.2. In the notation of that theorem, set $f(x) = 1$ and $g(x) = x - s$. The discriminant of $(Bx(x-C) - C(x-s)^2)/(-C)$ is $BC(BC - 4Cs + 4s^2)$, and to make this discriminant zero we take $B = 4s(C-s)/C$. We wish for s to have a rational preimage under ϕ, and so we find that the discriminant of the numerator of $\phi(x) - s$ is $16s^2(C-s)^3/C$. We wish for this to be a square, and hence we take $(C-s)/C = d^2$, *i.e.*, $s = C(1-d^2)$. Doing so gives

$$\phi^{-1}(s) = \Big\{ \frac{C(d+1)^2}{2d+1}, -\frac{C(d-1)^2}{2d-1} \Big\}.$$

Letting $v = C(d+1)^2/(2d+1)$, we have the orbit $v \mapsto s \mapsto \infty \mapsto B \mapsto \phi(B) \mapsto \cdots$. From the last paragraph of the proof of Theorem 1.1, we have the following equivalences modulo $\mathbb{Q}(x)^{*2}$:

$$\text{(10.1)}\quad \phi(x) \equiv Bx(x-C),\ \ \phi^2(x) \equiv -Cx(x-C),\ \text{ and } \phi^n(x) \equiv \phi^{n-2}(x) \text{ for all } n \geq 3.$$

We wish to have $\{n \in \mathbb{N}_0 : \phi^n(v) \in \mathbb{P}^1(\mathbb{Q})^2\} = \{0,2\} \cup \{2n+1 : n \geq 0\}$, which cannot be written as a union of fewer than three arithmetic progressions. Assume for a moment that $O_\phi^+(v)$ is infinite, and in particular, $\phi^n(v) \in \mathbb{Q}$ for all $n \neq 2$; we will justify this later. From (10.1), it is sufficient for v and s to be in $\mathbb{Q}^2$ and $\phi(B) \notin \mathbb{Q}^2$. Clearly, $v \equiv C(2d+1) \bmod \mathbb{Q}^2$ and $s \equiv C(1-d^2) \bmod \mathbb{Q}^2$, and one calculates $\phi(B) \equiv -C \bmod \mathbb{Q}^2$. If $d \in \mathbb{Q}$ satisfies $C(2d+1) \in \mathbb{Q}^2$, $C(1-d^2) \in \mathbb{Q}^2$, and $-C \notin \mathbb{Q}^2$, then the elliptic curve

$$E : y^2 = (2x+1)(1-x^2)$$

has a point in $E(\mathbb{Q})$ with x-coordinate d. This curve has conductor 24 and is isomorphic to curve 24a1 in Cremona's table [7]. It has rank zero over $\mathbb{Q}$ and $\mathbb{Q}$-torsion subgroup $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/4\mathbb{Z}$. Among the seven finite torsion points are five with $x \in \{0, \pm 1, -1/2\}$, and if d takes any of these values, then either $v = 0$, $s = 0$, or $s = C$, which are impossible in our setting. The other two points are $(x,y) = (-2, \pm 3)$, and so we must have $d = -2$. With this choice, we can take $C = -3t^2$ for any $t \in \mathbb{Q} \smallsetminus \{0\}$, giving $s = 9t^2$ and $v = t^2$. Hence,

$$\phi(x) = \frac{144t^2x(x+3t^2)}{(x-9t^2)^2} \qquad t \in \mathbb{Q} \smallsetminus \{0\},$$

is the unique family in $\mathbb{Q}(x)$ satisfying our conditions. It remains to show that the orbit

$$\text{(10.2)}\quad O_\phi^+(t^2) = \Big\{ t^2, 9t^2, \infty, 144t^2, 3\Big(\frac{112t}{5}\Big)^2, \Big(\frac{151872t}{11869}\Big)^2, 3\Big(\frac{17917453568t}{807305405}\Big)^2, \dots \Big\}$$

is infinite. Observe that if (10.2) is infinite for $t = 1$, then the same holds for all $t \in \mathbb{Q} \smallsetminus \{0\}$. When $t = 1$ we obtain the map $\phi_1(x) = 144x(x+3)/(x-9)^2$, which has

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

good reduction at the primes 5 and 7. Writing $\mathbb{F}_p$ for the finite field with p elements, one checks that in $\mathbb{P}^1(\mathbb{F}_5)$, ϕ_1 has a fixed point and a two-cycle and no other periodic points, while in $\mathbb{P}^1(\mathbb{F}_7)$, ϕ_1 has a fixed point and no other periodic points. It follows from [22, Theorem 2.21] that all periodic points of ϕ_1 in $\mathbb{Q}$ have period one or two. A simple calculation shows that the numerator of $\phi_1^2(x) - x$ is irreducible, and so ϕ_1 has no two-cycles in $\mathbb{Q}$. Hence, the only periodic point for ϕ_1 in $\mathbb{Q}$ is the fixed point 0. Thus, $O_{\phi_1}(1)$ is infinite, as desired.

Acknowledgments We thank Tommy Occhipinti, Bjorn Poonen, Joseph Silverman, Thomas Tucker, and Fedor Pakovich, for helpful comments and references. We extend special thanks to Michael Zieve for extensive and illuminating discussions of the literature surrounding this paper. We are also grateful to the anonymous referees, who furnished numerous suggestions for improving the paper's exposition, including the proof of Proposition 7.4.

References

[1] T. T. H. An and N. T. N. Diep, *Genus one factors of curves defined by separated variable polynomials.* J. Number Theory **133**(2013), no. 8, 2616–2634. http://dx.doi.org/10.1016/j.jnt.2012.12.017

[2] R. M. Avanzi and U. M. Zannier, *Genus one curves defined by separated variable polynomials and a polynomial Pell equation.* Acta Arith. **99**(2001), 227–256. http://dx.doi.org/10.4064/aa99-3-2

[3] ———, *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$.* Compositio Math. **139**(2003), no. 3, 263–295. http://dx.doi.org/10.1023/B:COMP.0000018136.23898.65

[4] A. F. Beardon, *Iteration of rational functions. Complex analytic dynamical systems.* Graduate Texts in Mathematics, 132, Springer-Verlag, New York, 1991. http://dx.doi.org/10.1007/978-1-4612-4422-6

[5] J. P. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell-Lang conjecture*. Mathematical Surveys and Monographs, 210, American Mathematical Society, Providence, RI, 2016.

[6] Y. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$.* Acta Arith. **95**(2000), no. 3, 261–288. http://dx.doi.org/10.4064/aa-95-3-261-288

[7] J. Cremona, *The elliptic curve database for conductors to 130000.* In: Algorithmic number theory, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006, pp. 11–29. http://dx.doi.org/10.1007/11792086_2

[8] M. D. Fried, *Arithmetical properties of function fields. II. The generalized Schur problem.* Acta Arith. **25**(1973/74), 225–258. http://dx.doi.org/10.4064/aa-25-3-225-258

[9] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Intersections of polynomials orbits, and a dynamical Mordell-Lang conjecture.* Invent. Math. **171**(2008), 463–483. http://dx.doi.org/10.1007/s00222-007-0087-5

[10] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Linear relations between polynomial orbits.* Duke Math. J. **161**(2012), no. 7, 1379–1410. http://dx.doi.org/10.1215/00127094-1598098

[11] C. Gratton, K. Nguyen, and T. J. Tucker, *ABC implies primitive prime divisors in arithmetic dynamics.* Bull. Lond. Math. Soc. **45**(2013), 1194–1208. http://dx.doi.org/10.1112/blms/bdt049

[12] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*. Graduate Texts in Mathematics, 201, Springer-Verlag, New York, 2000. http://dx.doi.org/10.1007/978-1-4612-1210-2

[13] G. Karpilovsky, *Topics in field theory*. North-Holland Mathematics Studies, 155, Notas de Matemática [Mathematical Notes], 124, North-Holland Publishing Co., Amsterdam, 1989.

[14] S. Lang, *Number theory. III. Diophantine geometry.* Encyclopaedia of Mathematical Sciences, 60, Springer-Verlag, Berlin, 1991.

[15] J. Milnor, *On Lattès maps.* In: Dynamics on the Riemann sphere, Eur. Math. Soc., Zürich, 2006, pp. 9–43. http://dx.doi.org/10.4171/011-1/1

[16] D. G. Northcott, *Periodic points on an algebraic variety.* Ann. of Math. (2) **51**(1950), 167–177. http://dx.doi.org/10.2307/1969504

[17] F. Pakovich, *Algebraic curves $A^{\circ l}(x) - U(y) = 0$ and arithmetic of orbits of rational functions.* 2018. arxiv:1801.01985

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press

[18] F. Pakovich, *Algebraic curves $P(x) - Q(y) = 0$ and functional equations.* Complex Var. Elliptic Equ. **56**(2011), no. 1–4, 199–213. http://dx.doi.org/10.1080/17476930903394838

[19] J. F. Ritt, *Prime and composite polynomials.* Trans. Amer. Math. Soc. **23**(1922), no. 1, 51–66. http://dx.doi.org/10.2307/1988911

[20] A. Schinzel, *Selected topics on polynomials*. University of Michigan Press, Ann Arbor, Mich., 1982.

[21] J. H. Silverman, *Integer points, Diophantine approximation, and iteration of rational maps.* Duke Math. J. **71**(1993), no. 3, 793–829. http://dx.doi.org/10.1215/S0012-7094-93-07129-3

[22] ———, *The arithmetic of dynamical systems*. Graduate Texts in Mathematics, 241, Springer, New York, 2007. http://dx.doi.org/10.1007/978-0-387-69904-2

[23] H. Stichtenoth, *Algebraic function fields and codes*. Second ed., Graduate Texts in Mathematics, 254, Springer-Verlag, Berlin, 2009.

Department of Mathematics and Statistics, Carleton College, One North College Street, Northfield, MN 55057, USA

Email: jordan.f.cahn@gmail.com rfjones@carleton.edu spearjm77@gmail.com

https://doi.org/10.4153/CJM-2018-026-x Published online by Cambridge University Press