Forum of Mathematics, Sigma (2024), **Vol. 12**:e45 1–20
doi:10.1017/fms.2023.112

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Lower Bounds for the Canonical Height of a Unicritical Polynomial and Capacity

P. Habegger[1] and H. Schmidt[2]

[1]Department of Mathematics and Computer Science, University of Basel, Spiegelgasse 1, 4051 Basel, Switzerland;
E-mail: philipp.habegger@unibas.ch (corresponding author).
[2]Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, UK;
E-mail: harry.schmidt@warwick.ac.uk.

Received: 1 December 2021; **Revised:** 13 June 2023; **Accepted:** 4 September 2023

2020 Mathematics Subject Classification: *Primary* – 11G50; *Secondary* – 14G40, 30C85, 37P15

Abstract
In a recent breakthrough, Dimitrov [Dim] solved the Schinzel–Zassenhaus conjecture. We follow his approach and adapt it to certain dynamical systems arising from polynomials of the form $T^p + c$, where p is a prime number and where the orbit of 0 is finite. For example, if $p = 2$ and 0 is periodic under $T^2 + c$ with $c \in \mathbb{R}$, we prove a lower bound for the local canonical height of a wandering algebraic integer that is inversely proportional to the field degree. From this, we are able to deduce a lower bound for the canonical height of a wandering point that decays like the inverse square of the field degree. For these f, our method has application to the irreducibility of polynomials. Indeed, say y is preperiodic under f but not periodic. Then any iteration of f minus y is irreducible in $\mathbb{Q}(y)[T]$.

1. Introduction

Let K be a field, and suppose $f \in K[T]$ has degree $\deg f \geq 2$. For $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$, we write $f^{(n)} \in K[T]$ for the n-fold iterate of f and define $f^{(0)} = T$. Let $x \in K$. We call x an *f-periodic point* if there exists $n \in \mathbb{N}$ with $f^{(n)}(x) = x$. We call x an *f-preperiodic point* if there exists an integer $m \geq 0$ such that $f^{(m)}(x)$ is f-periodic. Suppose x is f-preperiodic. The *preperiod length* of x is

$$\mathrm{preper}(x) = \min\{m \geq 0 : f^{(m)}(x) \text{ is } f\text{-periodic}\} \geq 0$$

and the *minimum period* of x is

$$\mathrm{per}(x) = \min\{n \geq 1 : f^{(n+\mathrm{preper}(x))}(x) = f^{(\mathrm{preper}(x))}(x)\} \geq 1.$$

An element of K is called an *f-wandering point* if it is not f-preperiodic. Equivalently, $x \in K$ is an f-wandering point if and only if $\{f^{(n)}(x) : n \in \mathbb{N}\}$ is infinite.

Suppose for the moment that K is a subfield of $\mathbb{C}$. We call f *post-critically finite* if its *post-critical set*

$$\mathrm{PCO}^+(f) = \{f^{(m)}(x) : m \in \mathbb{N}, x \in \mathbb{C}, \text{ and } f'(x) = 0\}$$

is finite. For example, $T^2 - 1$ is post-critically finite as its post-critical set equals $\{-1, 0\}$.

Let $M_{\mathbb{Q}}$ denote the set consisting of the v-adic absolute value on $\mathbb{Q}$ for all prime numbers v together with the Archimedean absolute value. For each prime number v, let $\mathbb{C}_v$ denote a completion of an algebraic closure of the valued field of v-adic numbers. We also set $\mathbb{C}_v = \mathbb{C}$ if v is Archimedean.

For a real number $t \geq 0$, we set $\log^+ t = \log\max\{1, t\}$. Let $v \in M_{\mathbb{Q}}$, and suppose $f \in \mathbb{C}_v[T]$ has degree $d \geq 2$. For all $x \in \mathbb{C}_v$, the limit

$$\lambda_{f,v}(x) = \lim_{n\to\infty} \frac{\log^+ |f^{(n)}(x)|_v}{d^n} \tag{1.1}$$

exists and satisfies $\lambda_{f,v}(f(x)) = d\lambda_{f,v}(x)$; see Chapter 3 and in particular Theorem 3.27 or Exercise 3.24 [Sil07] for details. For example, $\lambda_{T^2,v}(x) = \log^+ |x|_v$.

If v is Archimedean, we often abbreviate $\lambda_{f,v} = \lambda_f$. The local canonical height differs from $z \mapsto \log^+ |z|$ by a bounded function on $\mathbb{C}$. We define

$$\mathsf{C}(f) = \max\left\{1, \sup_{z\in\mathbb{C}} \frac{\max\{1, |z|\}}{e^{\lambda_f(z)}}\right\} < \infty. \tag{1.2}$$

Thus, the filled Julia set attached to f is contained in the closed disk of radius $\mathsf{C}(f)$ centered at 0.

Next, we define the canonical height of an algebraic number with respect to f. Let K be a number field and $f \in K[T]$ be of degree ≥ 2. Suppose x lies in a finite extension F of K. Let $v \in M_{\mathbb{Q}}$, and for a ring homomorphism $\sigma \in \mathrm{Hom}(F, \mathbb{C}_v)$ we let $\sigma(f)$ be the polynomial obtained by applying σ to each coefficient of f. The *canonical* or *Call–Silverman* height of x (with respect to f) is

$$\hat{h}_f(x) = \frac{1}{[F:\mathbb{Q}]} \sum_{v\in M_{\mathbb{Q}}} \sum_{\sigma\in\mathrm{Hom}(F,\mathbb{C}_v)} \lambda_{\sigma(f),v}(\sigma(x)). \tag{1.3}$$

This value does not depend on the number field $F \supseteq K$ containing x. Let $\overline{K}$ denote an algebraic closure of K, we obtain a well-defined map $\hat{h}_f : \overline{K} \to [0, \infty)$. For $x \in F$, we define

$$\lambda_f^{\max}(x) = \max\bigl\{\lambda_{\sigma(f)}(\sigma(x)) : \sigma \in \mathrm{Hom}(F, \mathbb{C})\bigr\}.$$

To formulate our results, we require Dimitrov's notion of a hedgehog. A *quill* is a line segment $[0, 1]z = \{tz : t \in [0, 1]\} \subseteq \mathbb{C}$, where $z \in \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. A *hedgehog* with at most q quills is a finite union of quills

$$\mathcal{H}(z_1, \ldots, z_q) = \bigcup_{i=1}^{q} [0, 1]z_i,$$

where $z_1, \ldots, z_q \in \mathbb{C}^\times$; we also define $\mathcal{H}() = \{0\}$ to be the quill-less hedgehog. A hedgehog is a compact, path connected, topological tree.

We will also use Dubinin's theorem [Dub84] which states

$$\mathrm{cap}(\mathcal{H}(z_1, \ldots, z_q)) \leq 4^{-1/q} \max\{|z_1|, \ldots, |z_q|\}$$

if $q \geq 1$, where $\mathrm{cap}(\mathcal{K})$ is the capacity, or equivalently the transfinite diameter, of a compact subset $\mathcal{K} \subseteq \mathbb{C}$. We refer to Section 3 for basic properties of the capacity.

Quill Hypothesis. Let K be a number field, and let $f \in K[T]$ have degree ≥ 2. We say that f satisfies the *quill hypothesis* if there exist $\sigma_0 \in \mathrm{Hom}(K, \mathbb{C})$ and an integer $q \geq 0$ such that the post-critical set $\mathrm{PCO}^+(\sigma_0(f))$ is contained in a hedgehog with at most q quills and

$$q \log \mathsf{C}(\sigma_0(f)) < \log 4. \tag{1.4}$$

This hypothesis will be only be relevant for polynomials $f = T^p + c$ with p a prime number.

The condition and the constant 4 are artefacts of Dubinin's theorem. Our main results require f to satisfy the quill hypothesis, which should be unnecessary conjecturally.

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

Say $f = T^2 - 1$. Then $\mathrm{PCO}^+(f)$ is contained in the single quill $[-1, 0]$. We will see in Lemma 3.6 that $\mathsf{C}(T^2 - 1) \leq (\sqrt{5} + 1)/2 < 4$. So $f = T^2 - 1$ satisfies the quill hypothesis.

We are now ready to state our results.

Theorem 1.1. *Let p be a prime number, let K be a number field and let $f = T^p + c \in K[T]$. Suppose that 0 is an f-periodic point and that f satisfies the quill hypothesis. Then there exists $\kappa = \kappa(f) > 0$ with the following properties.*

(i) *If $x \in \overline{K}$ is an algebraic integer and also an f-wandering point, then $\lambda_f^{\max}(x) \geq \kappa/[K(x) : K]$.*

(ii) *If $x \in \overline{K}$ is an f-wandering point, then $\hat{h}_f(x) \geq \kappa/[K(x) : K]^2$.*

Let us explain why (i) can be seen as a dynamical Schinzel–Zassenhaus property for *f*. Indeed, let *x* be an algebraic integer with $\mathbb{Q}$-minimal polynomial $(X - x_1) \cdots (X - x_d)$, where $x_1, \ldots, x_d \in \mathbb{C}$. The house $\boxed{x}$ of *x* is $\max_{1 \leq i \leq d} |x_i|$. We have $\boxed{x} \geq 1$ if $x \neq 0$. Kronecker's theorem states that $\log \boxed{x}$ vanishes if and only if *x* is 0 or a root of unity. Dimitrov [Dim] proved $\log \boxed{x} \geq \frac{\log 2}{4[\mathbb{Q}(x):\mathbb{Q}]}$ for all remaining algebraic integers *x*. This is sometimes called the Schinzel–Zassenhaus conjecture [SZ65]. Observe that if $x \neq 0$, then $\log \boxed{x} = \lambda_{T^2}^{\max}(x)$. Moreover, *x* is T^2-preperiodic if and only if it is 0 or a root of unity.

Part (ii) of the theorem is conjectured to hold for all rational functions $f \in K(T)$ of degree ≥ 2 with $[K(x) : K]^2$ replaced by $[K(x) : K]$. This is called the dynamical Lehmer conjecture; see Conjecture 3.25 [Sil07] or Conjecture 16.2 [BIJ+19] for a higher-dimensional version. The dynamical Lehmer conjecture is already open in the classical case $f = T^2$. In this case, $\hat{h}_{T^2}$ is the absolute logarithmic Weil height. Suppose *x* is a nonzero algebraic number that is not a root of unity. Dobrowolski's theorem [Dob79] implies $\hat{h}_{T^2}(x) \geq \frac{c}{d}\left(\frac{\log \log d}{\log d}\right)^3$ with $d = [\mathbb{Q}(x) : \mathbb{Q}]$ and for an absolute constant $c > 0$.

In the dynamical setting, little is known. However, we mention that M. Baker obtained a lower bound for the canonical height for general rational maps, up to an exceptional set. For a polynomial *f* as above, his Theorem 1.14 [Bak06] states the following. There exist constants $c_1 > 0$ and $c_2 > 0$ that depend on *K* and *f* with the following property. Let F/K be a finite extension. Then $\hat{h}_f(x) > \frac{c_1}{[F:\mathbb{Q}]}$ for all $x \in F$ with at most $c_2[F : \mathbb{Q}] \log(2[F : \mathbb{Q}])$ exceptions.

Next, we exhibit some cases where the quill hypothesis is satisfied.

Lemma 1.2. *Let p be a prime number, let K be a number field and let $f = T^p + c \in K[T]$. Suppose that $f \neq T^2 - 2$. Then f satisfies the quill hypothesis in both of the following cases.*

(i) *There exists a field embedding $\sigma_0 \colon K \longrightarrow \mathbb{R}$ with image in the real numbers such that* $\mathrm{PCO}^+(\sigma_0(f))$ *is bounded.*

(ii) *There exists a field embedding $\sigma_0 \colon K \longrightarrow \mathbb{C}$ such that* $\#\mathrm{PCO}^+(\sigma_0(f)) \leq 2p - 2$.

Let $n \in \mathbb{N}$, and let G_n denote the monic polynomial whose roots are precisely those $c \in \mathbb{C}$ for which 0 is $(T^2 + c)$-periodic with exact period *n*. Then $G_n \in \mathbb{Z}[X]$ and work of Lutzky [Lut93] implies that G_n has at least one real root. In particular, by Lemma 1.2(i) the quill hypothesis is met for infinitely many quadratic polynomials $T^2 + c \in \overline{\mathbb{Q}}[T]$ with periodic critical point. It is a folklore conjecture that G_n is irreducible for all $n \in \mathbb{N}$. Conditional on this conjecture, any $f = T^2 + c$ with $c \neq -2$ for which 0 is *f*-periodic satisfies the quill hypothesis.

Let us briefly address $f = T^2 - 2$. Then $\lambda_f(w + w^{-1}) = \big|\log |w|\big|$ for all $w \in \mathbb{C}^\times$. Moreover, $\hat{h}_f(w + w^{-1}) = 2h(w)$ for all nonzero algebraic *w*; here, $h = h_{T^2}$ is the absolute logarithmic Weil height. For $f = T^2 - 2$, Theorem 1.1 follows from Dimitrov's Theorem 1 [Dim]. Moreover, part (ii) with a better exponent in $[K(x) : K]$ follows from Dobrowolski's Theorem 1 [Dob79].

If 0 is periodic of minimal period larger than 1, then $f = T^p + c$ is not conjugate to a Chebyshev polynomial or T^p. Using the lemma above, we find for each prime *p* an *f* not of this form that satisfies the quill hypothesis.

The main technical results of this paper are in Section 4. For example, we also cover some cases where 0 is an *f*-preperiodic point. In Theorem 4.4 below, we prove a more general version of Theorem 1.1.

We now draw several corollaries.

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

Corollary 1.3. *Let p be a prime number, let K be a number field and let $f = T^p + c \in K[T]$. Suppose that 0 is an f-periodic point and that f satisfies the quill hypothesis. Suppose $y \in K$.*

(i) *Suppose $K/\mathbb{Q}$ is unramified above p. Let y be an f-periodic point. Let $x \in \overline{K}$ satisfy $f^{(n)}(x) = y$ with $n \geq 0$ minimal. Then $[K(x) : K] \geq p^{n-\mathrm{per}(y)}$.*
(ii) *Suppose $K/\mathbb{Q}$ is unramified above p. Let y be an f-preperiodic point and not f-periodic. Then $f^{(n)} - y \in K[T]$ is irreducible for all $n \in \mathbb{N}$.*
(iii) *Let y be an f-wandering point. Then there exists $\kappa = \kappa(f, y) > 0$ such that, for all $n \in \mathbb{N}$, each irreducible factor of $f^{(n)} - y \in K[T]$ has degree at least κp^n.*

By Lemma 4.1, the extension $\mathbb{Q}(c)/\mathbb{Q}$ is unramified above p if 0 is f-preperiodic.

For example, if $f = T^2 - 1$, then $f^{(n)} - 1$ is irreducible in $\mathbb{Q}[T]$ for all $n \in \mathbb{N}$. Stoll [Sto92] showed that iterates of certain quadratic polynomials are irreducible over $\mathbb{Q}$. Part (iii) of Corollary 1.3 was proved in more general form by Jones and Levy [JL17] using different methods.

The method presented here is effective in that it can produce explicit lower bounds for heights. In the next two corollaries, we take a closer look at the quadratic polynomial $f = T^2 - 1$.

Corollary 1.4. *Let $f = T^2 - 1$.*

(i) *Let $x \in \overline{\mathbb{Q}}$ be an algebraic integer and an f-wandering point. Then*

$$\lambda_f^{\max}(x) \geq \frac{\log(4^{11/10}/(\sqrt{5}+1))}{48} \frac{1}{[\mathbb{Q}(x) : \mathbb{Q}]} > \frac{0.007}{[\mathbb{Q}(x) : \mathbb{Q}]}.$$

(ii) *Let $x \in \overline{\mathbb{Q}}$ be an f-wandering point. Then*

$$\hat{h}_f(x) \geq \frac{\log(4^{11/10}/(\sqrt{5}+1))}{48} \frac{1}{[\mathbb{Q}(x) : \mathbb{Q}]^2} > \frac{0.007}{[\mathbb{Q}(x) : \mathbb{Q}]^2}.$$

Corollary 1.5. *Let $f = T^2 - 1 \in \mathbb{Q}[T]$, and let $x \in \overline{\mathbb{Q}}$ be an f-preperiodic point. Then*

$$[\mathbb{Q}(x) : \mathbb{Q}] \geq \frac{1}{2} \max\{2^{\mathrm{preper}(x)}, \mathrm{per}(x)\}.$$

We now discuss the method of proof. It is an adaptation of Dimitrov's proof of the Schinzel–Zassenhaus conjecture [Dim].

Suppose we are given f as in Theorem 1.1 and an algebraic integer x such that $\lambda_f^{\max}(x)$ is sufficiently small. For simplicity, say $f = T^p + c \in \mathbb{Q}[T]$ has rational coefficients.

The $\mathbb{Q}$-minimal polynomial $A \in \mathbb{Q}[X]$ of x factors as $(X - x_1) \cdots (X - x_D)$ with $x_1, \ldots, x_D \in \mathbb{C}$. For an integer $k \geq 1$, we set $A_k = (X - f^{(k)}(x_1)) \cdots (X - f^{(k)}(x_D))$. The basic idea is to consider a p-th root ϕ of the rational function $(A_l/A_k)^{p-1} = 1 + O(1/X)$ for certain integers $1 \leq k < l$. *A priori*, we may consider ϕ as a formal power series in $\mathbb{Q}[[1/X]]$. However, an appropriate choice of k and l will imply $\phi \in \mathbb{Z}[[1/X]]$. This formal power series is constructed in Section 2 where we also analyze integrality properties via congruence conditions. This step requires that the degree of $T^p + c$ is a prime number. The power series ϕ represents a holomorphic function on the complement of a large enough disk. This step is similar as in Dimitrov's proof.

Our next step will be to construct a sufficiently nice connected domain $U \subseteq \mathbb{C}$ on which ϕ represents a holomorphic function. Our choice U will have bounded complement in $\mathbb{C}$. This construction is done in Section 3, and it is the main new aspect of this paper. Let $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ denote the extended complex plane. The construction of U depends on a parameter $n \in \mathbb{N}$. It takes as an input a hedgehog I_0 that contains the post-critical set of f (or at least part of it). The critical values of $f^{(n)}$ are contained in the preimage $(f^{(n)})^{-1}(I_0)$, which one should think of as a finite topological tree. Thus, $f^{(n)}$ has no critical points on $\mathbb{C} \setminus (f^{(n)})^{-1}(I_0)$. Moreover, adding the point at infinity will make $\mathbb{C} \setminus (f^{(n)})^{-1}(I_0)$ simply connected.

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

However, this complement is not yet the desired U. We need to ensure that U does not contain the $f^{(k)}(x_i)$ and $f^{(l)}(x_j)$ so that A_l/A_k has neither poles nor zeros on U. This can be done by augmenting $(f^{(n)})^{-1}(I_0)$ to a larger finite topological tree while retaining the property that $U \cup \{\infty\}$ is simply connected. By monodromy, the p-th root ϕ extends to a holomorphic function on U.

Dubinin's theorem is our tool to bound from above the capacity of a suitable hedgehog. We will be able to relate the capacity of $\mathbb{C} \setminus U$ to the capacity of a hedgehog using transformation properties of the capacity under certain holomorphic mappings.

Finally, in Section 4 we prove the results stated in the introduction. As did Dimitrov, we use the Pólya–Bertrandias theorem. It implies that ϕ is a rational function if $\mathrm{cap}(\mathbb{C} \setminus U) < 1$. The quill hypothesis, the post-critically finite hypothesis on f, and the fact that $\lambda_f^{\max}(x)$ is small is used to ensure the capacity inequality. Here, we also choose the parameter n that controls the tree and ultimately U. If ϕ, whose p-th power is $(A_l/A_k)^{p-1}$, is a rational function, then we are in one of two cases. The first case is when A_k and A_l have a common root that cancels out in A_l/A_k. Thus, $f^{(k)}(x_i) = f^{(l)}(x_j)$ for some i, j. A standard argument involving the canonical height and $k < l$ shows that x is f-preperiodic. In the second case, A_k has a multiple root, say $f^{(k)}(x_i) = f^{(k)}(x_j)$ for distinct i, j. This collision of Galois conjugates implies that $\mathbb{Q}(f^{(k)}(x))$ is a proper subfield of $\mathbb{Q}(x)$. We can then proceed by an induction on the field degree. This case study is laid out in detail in Proposition 4.3 which then quickly leads to the results mentioned in the introduction.

2. Constructing the power series

In this section, we construct an auxiliary power series. Our approach largely follows the approach laid out in Section 2 [Dim] and in particular Proposition 2.2 and Lemma 2.5 *loc.cit.* We adapt it to the dynamical setting. Dimitrov's crucial observation is that $\sqrt{1+4X}$ is a formal power series in X with integral coefficients.

Throughout this section, let R denote an integrally closed domain of characteristic 0. Let p be a prime number.

For $D \in \mathbb{N}$ and $j \in \{0, \dots, D\}$, let $e_j \in \mathbb{Z}[X_1, \dots, X_D]$ denote the elementary symmetric polynomial of degree j. We set

$$\Psi_{p,j} = \frac{1}{p}\left(e_j(X_1, \dots, X_D)^p - e_j(X_1^p, \dots, X_D^p)\right).$$

So $\Psi_{p,j} \in \mathbb{Z}[X_1, \dots, X_D]$ by Fermat's little theorem and

$$e_j(X_1, \dots, X_D)^p = e_j(X_1^p, \dots, X_D^p) + p\Psi_{p,j}. \tag{2.1}$$

If R is subring of a ring S and $a, b \in S$, we write $a \equiv b \pmod{p}$ or $a \equiv b \pmod{pS}$ to signify $a - b \in pS$.

Lemma 2.1. *For all $k \in \mathbb{N}$ and all $j \in \{0, \dots, D\}$, we have*

$$e_j(X_1, \dots, X_D)^{p^k} \equiv e_j(X_1^{p^k}, \dots, X_D^{p^k}) + p\Psi_{p,j}^{p^{k-1}} \pmod{p^2}. \tag{2.2}$$

Proof. By Equation (2.1) our claim (2.2) holds for $k = 1$.

We assume that Equation (2.2) holds for $k \geq 1$ and will deduce it for $k+1$. So

$$\begin{aligned} e_j(X_1, \dots, X_D)^{p^{k+1}} &\equiv \left(e_j(X_1^{p^k}, \dots, X_D^{p^k}) + p\Psi_{p,j}^{p^{k-1}}\right)^p \pmod{p^2} \\ &\equiv e_j(X_1^{p^k}, \dots, X_D^{p^k})^p \pmod{p^2} \end{aligned} \tag{2.3}$$

as $(x+py)^p \equiv x^p \pmod{p^2}$.

We evaluate $\Psi_{p,j}$ at $(X_1^{p^k}, \ldots, X_D^{p^k})$ and use Equation (2.1) to find

$$e_j(X_1^{p^k}, \ldots, X_D^{p^k})^p = e_j(X_1^{p^{k+1}}, \ldots, X_D^{p^{k+1}}) + p\Psi_{p,j}(X_1^{p^k}, \ldots, X_D^{p^k}). \tag{2.4}$$

Finally, $\Psi_{p,j}(X_1^{p^k}, \ldots, X_D^{p^k}) \in \Psi_{p,j}^{p^k} + p\mathbb{Z}[X_1, \ldots, X_D]$ and hence $e_j(X_1^{p^k}, \ldots, X_D^{p^k})^p \equiv e_j(X_1^{p^{k+1}}, \ldots, X_D^{p^{k+1}}) + p\Psi_{p,j}^{p^k} \pmod{p^2}$ from Equation (2.4). Thus, Equation (2.2) for $k+1$ follows from Equation (2.3). □

Lemma 2.2. *Let S be a ring of which R is a subring and suppose $x_1, \ldots, x_D \in S$ such that $(X - x_1)\cdots(X - x_D) \in R[X]$. Let p be a prime number.*

(i) *The value of a symmetric polynomial in $R[X_1, \ldots, X_D]$ evaluated at $(x_1, \ldots, x_D)$ lies in R.*
(ii) *Let $k, l \in \mathbb{N}$ with $a^{p^{k-1}} \equiv a^{p^{l-1}} \pmod{pR}$ for all $a \in R$. For all $j \in \{0, \ldots, D\}$, we have*

$$e_j(x_1^{p^k}, \ldots, x_D^{p^k}) \equiv e_j(x_1^{p^l}, \ldots, x_D^{p^l}) \pmod{p^2R}.$$

Proof. An elementary symmetric polynomial in $R[X_1, \ldots, X_D]$ lies in $R[e_1, \ldots, e_D]$. We conclude (i) as $e_1(x_1, \ldots, x_D), \ldots, e_D(x_1, \ldots, x_D) \in R$ by hypothesis.

For (ii), observe that $\Psi_{p,j}$ is symmetric so $\Psi_{p,j}(x_1, \ldots, x_D) \in R$ by part (i). For the same reason, $e_j(x_1^{p^k}, \ldots, x_D^{p^k}) \in R$ and $e_j(x_1^{p^l}, \ldots, x_D^{p^l}) \in R$.

By the hypothesis in (ii), we conclude $\Psi_{p,j}(x_1, \ldots, x_D)^{p^{k-1}} \equiv \Psi_{p,j}(x_1, \ldots, x_D)^{p^{l-1}} \pmod{pR}$. Lemma 2.1 implies

$$e_j(x_1, \ldots, x_D)^{p^k} - e_j(x_1^{p^k}, \ldots, x_D^{p^k}) \equiv e_j(x_1, \ldots, x_D)^{p^l} - e_j(x_1^{p^l}, \ldots, x_D^{p^l}) \pmod{p^2R}. \tag{2.5}$$

Raising $a^{p^{k-1}} \equiv a^{p^{l-1}} \pmod{pR}$ to the p-th power gives $a^{p^k} \equiv a^{p^l} \pmod{p^2R}$ for all $a \in R$. In particular, $e_j(x_1, \ldots, x_D)^{p^k}$ and $e_j(x_1, \ldots, x_D)^{p^l}$ are equivalent modulo p^2. Part (ii) now follows from Equation (2.5).□ □

Lemma 2.3. *Let $f = T^p + c \in R[T]$. We have*

$$f^{(k)} \equiv \left(T^{p^{k-1}} + f^{(k-1)}(0)\right)^p + c \pmod{p^2R[T]}$$

for all $k \in \mathbb{N}$.

Proof. As $f^{(0)}(0) = 0$, the claim holds for $k = 1$. Say $k \geq 2$. By induction on k, we have $f^{(k-1)} \equiv T^{p^{k-1}} + pg + f^{(k-2)}(0)^p + c \pmod{p^2R[T]}$ for some $g \in R[T]$. So

$$\begin{aligned} f^{(k)} &\equiv \left(T^{p^{k-1}} + pg + f^{(k-2)}(0)^p + c\right)^p + c \pmod{p^2R[T]} \\ &\equiv \left(T^{p^{k-1}} + f^{(k-2)}(0)^p + c\right)^p + c \pmod{p^2R[T]} \end{aligned}$$

and the lemma follows from $f^{(k-1)}(0) = f^{(k-2)}(0)^p + c$. □

Let $f \in R[T]$ and $A = \prod_{j=1}^D (X - x_j) \in R[X]$, where $x_1, \ldots, x_D$ are in a splitting field of A. For all integers $k \geq 0$, we set

$$A_k = \prod_{j=1}^D (X - f^{(k)}(x_j)).$$

Then $A_k \in R[X]$ by Lemma 2.2(i).

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

Lemma 2.4. *Let $f = T^p + c \in R[T]$. Suppose that $k, l \in \mathbb{N}$ satisfy $k \le l$ and $f^{(k-1)}(0) = f^{(l-1)}(0)$. Set*

$$\delta = \begin{cases} 0 : \text{if } k = 1, \\ 1 : \text{if } k \ge 2. \end{cases} \tag{2.6}$$

We assume that

$$a^{p^{k-\delta-1}} \equiv a^{p^{l-\delta-1}} \pmod p \quad \text{for all } a \in R. \tag{2.7}$$

Then $A_k \equiv A_l \pmod{p^2 R[X]}$ for all monic $A \in R[X]$.

Proof. If $k = 1$, then $0 = f^{(k-1)}(0) = f^{(l-1)}(0)$. In this case, Lemma 2.3 implies $f^{(l)} \equiv g(T^{p^l}) \pmod{p^2 R[T]}$ with $g = T + c$. Observe that $f^{(k)} = f = g(T^p) = g(T^{p^k})$.

If $k \ge 2$, Lemma 2.3 implies $f^{(k)} \equiv g(T^{p^{k-1}}) \pmod{p^2 R[T]}$ and $f^{(l)} \equiv g(T^{p^{l-1}}) \pmod{p^2 R[T]}$, where $g = (T + f^{(k-1)}(0))^p + c$.

We can summarize both cases by $f^{(k)} \equiv g(T^{p^{k-\delta}}) \pmod{p^2}$ and $f^{(l)} \equiv g(T^{p^{l-\delta}}) \pmod{p^2}$; we sometimes drop the reference to base ring in $\pmod{p^2}$ below.

Let $j \in \{0, \dots, D\}$; the polynomial $e_j(g(X_1), \dots, g(X_D))$ is symmetric. So

$$e_j(g(X_1), \dots, g(X_D)) = P_j(e_1, \dots, e_D)$$

for some $P_j \in R[X_1, \dots, X_D]$. Next, we replace X_i by $X_i^{p^{k-\delta}}$ to get

$$e_j(g(X_1^{p^{k-\delta}}), \dots, g(X_D^{p^{k-\delta}})) = P_j(e_1(X_1^{p^{k-\delta}}, \dots, X_D^{p^{k-\delta}}), \dots, e_D(X_1^{p^{k-\delta}}, \dots, X_D^{p^{k-\delta}})).$$

Hence,

$$e_j(f^{(k)}(X_1), \dots, f^{(k)}(X_1)) \equiv P_j(e_1(X_1^{p^{k-\delta}}, \dots, X_D^{p^{k-\delta}}), \dots, e_D(X_1^{p^{k-\delta}}, \dots, X_D^{p^{k-\delta}})) \pmod{p^2}. \tag{2.8}$$

The same argument for l yields

$$e_j(f^{(l)}(X_1), \dots, f^{(l)}(X_D)) \equiv P_j(e_1(X_1^{p^{l-\delta}}, \dots, X_D^{p^{l-\delta}}), \dots, e_D(X_1^{p^{l-\delta}}, \dots, X_D^{p^{l-\delta}})) \pmod{p^2}. \tag{2.9}$$

We factor $A = (X - x_1) \cdots (X - x_D)$ with $x_1, \dots, x_D$ inside a fixed splitting field of A. We specialize $(x_1, \dots, x_D)$ in Equation (2.8) to get

$$e_j\left(f^{(k)}(x_1), \dots, f^{(k)}(x_D)\right) \in P_j\left(e_1(x_1^{p^{k-\delta}}, \dots, x_D^{p^{k-\delta}}), \dots, e_D(x_1^{p^{k-\delta}}, \dots, x_D^{p^{k-\delta}})\right) + p^2 R[x_1, \dots, x_D];$$

both elements lie in R by Lemma 2.2(i). As any element in $R[x_1, \dots, x_D]$ is integral over R and since R is integrally closed, we conclude

$$e_j(f^{(k)}(x_1), \dots, f^{(k)}(x_D)) \equiv P_j\left(e_1(x_1^{p^{k-\delta}}, \dots, x_D^{p^{k-\delta}}), \dots, e_D(x_1^{p^{k-\delta}}, \dots, x_D^{p^{k-\delta}})\right) \pmod{p^2 R}.$$

The same statement holds with k replaced by l by using Equation (2.9).

By hypothesis (2.7) and by Lemma 2.2(ii) applied to $k - \delta, l - \delta$, we have

$$e_j(x_1^{p^{k-\delta}}, \dots, x_D^{p^{k-\delta}}) \equiv e_j(x_1^{p^{l-\delta}}, \dots, x_D^{p^{l-\delta}}) \pmod{p^2 R}$$

and hence

$$e_j(f^{(k)}(x_1), \dots, f^{(k)}(x_D)) \equiv e_j(f^{(l)}(x_1), \dots, f^{(l)}(x_D)) \pmod{p^2 R}.$$

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

This holds for all j and so $A_k \equiv A_l \pmod{p^2}$, as desired. $\square$

Let

$$\Phi_p = \sum_{k=0}^{\infty} \binom{1/p}{k} U^k \in \mathbb{Q}[[U]]; \tag{2.10}$$

it satisfies $\Phi_p^p = 1 + U$. If $k \geq 0$ is an integer, then

$$\binom{1/p}{k} p^k = \frac{1}{k!}\frac{1}{p}\left(\frac{1}{p} - 1\right)\cdots\left(\frac{1}{p} - k + 1\right)p^k \in \frac{1}{k!}\mathbb{Z}.$$

The exponent of the prime p in $k!$ equals the finite sum $\sum_{e=1}^{\infty}[k/p^e]$ which is at most $k\sum_{e=1}^{\infty} p^{-e} = k/(p-1) \leq k$. So p does not appear in the denominator of $\binom{1/p}{k}p^{2k} \in \mathbb{Q}$ for all $k \geq 0$. Moreover, if ℓ is a prime distinct from p, then ℓ does not appear in the denominator of $\binom{1/p}{k}$. Therefore,

$$\Phi_p(p^2 U) \in \mathbb{Z}[[U]]. \tag{2.11}$$

Let $R[[1/X]]$ be the ring of formal power series in X. We write ord_∞ for the natural valuation on $R[[1/X]]$, that is, $\mathrm{ord}_\infty(1/X) = 1$. A nonconstant polynomial in $R[X]$ does not lie in $R[[1/X]]$, rather it lies in the ring of formal Laurent series $R((1/X))$ to which we extend ord_∞ in the unique fashion. So we will consider $R[X] \subseteq R((1/X))$. For example, any monic polynomial in $R[X]$ is a unit in $R((1/X))$.

Proposition 2.5. *Let p be a prime number, and let $f = T^p + c \in R[T]$. Suppose that $k, l \in \mathbb{N}$ satisfy $k \leq l$ and $f^{(k-1)}(0) = f^{(l-1)}(0)$. Let $\delta \in \{0, 1\}$ be as in Lemma 2.4, and suppose $a^{p^{k-\delta-1}} \equiv a^{p^{l-\delta-1}} \pmod{p}$ for all $a \in R$. If $A \in R[T]$ is monic, there exists $B \in R[X]$ such that* $\deg B \leq \deg A_k^p - 1$, $\Phi_p(p^2 B/A_k^p) \in R[[1/X]]$ *and* $\Phi_p(p^2 B/A_k^p)^p = (A_l/A_k)^{p-1}$.

Proof. Lemma 2.4 implies $A_k A_l^{p-1} = A_k^p + p^2 B$ for some $B \in R[X]$. As A_k and A_l are both monic of degree $D = \deg A$, leading terms cancel and we find $\deg B \leq pD - 1$. Then,

$$A_k A_l^{p-1} = \left(1 + p^2 C\right) A_k^p$$

with $C = B/A_k^p$. Since A_k is monic, we have $C \in R((1/X))$. So $\mathrm{ord}_\infty(C) = -\deg B + pD \geq 1$. Therefore, C is a formal power series in $1/X$ and even lies in the ideal $(1/X)R[[1/X]]$.

Recall that $\Phi_p(p^2 U) \in \mathbb{Z}[[U]]$ by Equation (2.11). Therefore, $\Phi_p(p^2 C) \in R[[1/X]]$ and

$$A_k A_l^{p-1} = \left(\Phi_p(p^2 C) A_k\right)^p$$

by the functional equation $\Phi_p^p = 1 + U$; this is an identity in $R((1/X))$. We conclude the proof by dividing by A_k^p. $\square$

3. Constructing simply connected domains

Recall that $\widehat{\mathbb{C}}$ denotes the extended complex plane $\mathbb{C} \cup \{\infty\}$, that is, the Riemann sphere. This section concerns the construction of a domain $U \subseteq \widehat{\mathbb{C}}$ containing ∞ that is related to the discussion in the introduction. It depends on a polynomial $f = T^p + c$ and ultimately on an algebraic integer of small canonical height. The complement $\widehat{\mathbb{C}} \setminus U$ will be a compact subset of $\mathbb{C}$ of capacity strictly less than 1. The relevant properties are stated in Proposition 3.4. Later on, we will construct a holomorphic function on U using the power series introduced in Section 2.

We begin with a topological lemma which is most likely well-known. We provide a proof as we could not find a proper reference.

Lemma 3.1. *Let $f \in \mathbb{C}[T] \setminus \mathbb{C}$. Let $B \subseteq \mathbb{C}$ be compact such that $\mathbb{C} \setminus B$ is connected with cyclic fundamental group. Suppose B contains all critical values of f. Then $\mathbb{C} \setminus f^{-1}(B)$ is connected and $\widehat{\mathbb{C}} \setminus f^{-1}(B)$ is simply connected.*

Proof. Let us denote the restriction $f|_{f^{-1}(\mathbb{C}\setminus B)} \colon f^{-1}(\mathbb{C} \setminus B) = \mathbb{C} \setminus f^{-1}(B) \to \mathbb{C} \setminus B$ by ψ. Then ψ is a surjective continuous map. As a nonconstant polynomial induces a proper map, we see that ψ is proper and thus closed. By hypothesis, $f^{-1}(\mathbb{C} \setminus B)$ does not contain any critical point of f. So ψ is a local homeomorphism and thus open. As ψ is closed and open, the image of a connected component of $\mathbb{C} \setminus f^{-1}(B)$ under ψ is all of $\mathbb{C} \setminus B$. As ψ is the restriction of a polynomial, we conclude that all connected components of $\mathbb{C} \setminus f^{-1}(B)$ are unbounded. The preimage $f^{-1}(B)$ is compact, and so $\mathbb{C} \setminus f^{-1}(B)$ has a only one unbounded connected component. Therefore, $\mathbb{C} \setminus f^{-1}(B)$ is connected and so is $\widehat{\mathbb{C}} \setminus f^{-1}(B)$.

We fix a base point $z_0 \in \mathbb{C} \setminus f^{-1}(B)$. The proper, surjective, local homeomorphism ψ is a topological covering by Lemma 2 [Ho75]. Then $\pi_1(\mathbb{C} \setminus f^{-1}(B), z_0)$ is isomorphic to a subgroup of $\pi_1(\mathbb{C} \setminus B, p(z_0))$ of finite index and thus cyclic.

Let U_∞ be the complement in $\mathbb{C}$ of a closed disk centered at 0 containing the compact set $f^{-1}(B)$. We suppose $z_0 \in U_\infty$. Adding the point at infinity gives us a simply connected domain $U_\infty \cup \{\infty\} \subseteq \widehat{\mathbb{C}}$ and we have $\widehat{\mathbb{C}} \setminus f^{-1}(B) = (U_\infty \cup \{\infty\}) \cup (\mathbb{C} \setminus f^{-1}(B))$. The theorem of Seifert and van Kampen tells us that the inclusion induces a short exact sequence

$$1 \to \pi_1(U_\infty, z_0) \to \pi_1(\mathbb{C} \setminus f^{-1}(B), z_0) \to \pi_1(\widehat{\mathbb{C}} \setminus f^{-1}(B), z_0) \to 1. \tag{3.1}$$

We may assume $B \neq \emptyset$. Consider the loop $t \mapsto z_0 e^{2\pi\sqrt{-1}t}$, its image lies in U_∞. Fix any $w \in f^{-1}(B)$. It is well-known that such loop represents a generator of $\pi_1(\mathbb{C} \setminus \{w\}, z_0) \cong \mathbb{Z}$ and that the natural homomorphism $\pi_1(U_\infty, z_0) \to \pi_1(\mathbb{C} \setminus f^{-1}(B), z_0) \to \pi_1(\mathbb{C} \setminus \{w\}, z_0)$ is an isomorphism. So also the middle group is isomorphic to $\mathbb{Z}$ and the first arrow is a group isomorphism. Therefore, $\widehat{\mathbb{C}} \setminus f^{-1}(B)$ is simply connected by Equation (3.1). □

We recall the definition of the transfinite diameter of a nonempty compact subset $\mathcal{K}$ of $\mathbb{C}$; see Chapter 5.5 [Ran95] for details. For an integer $n \geq 2$, we define

$$d_n(\mathcal{K}) = \sup\left\{ \prod_{1\leq i<j\leq n} |z_i - z_j|^{2/(n(n-1))} : z_1, \ldots, z_n \in \mathcal{K} \right\}.$$

The sequence $\left(d_n(\mathcal{K})\right)_{n\geq 2}$ is nonincreasing, and the transfinite diameter of $\mathcal{K}$ is its limit. The transfinite diameter is known to equal the capacity $\mathrm{cap}(\mathcal{K})$ of $\mathcal{K}$ by the Fekete–Szegö theorem; see Theorem 5.5.2 [Ran95]. It is convenient to define $\mathrm{cap}(\emptyset) = 0$.

For $f \in \mathbb{C}[T]$ and for $n \in \mathbb{N}$, we introduce the truncated post-critical set

$$\mathrm{PCO}^+_n(f) = \left\{ f^{(m)}(x) : m \in \{1, \ldots, n\}, x \in \mathbb{C}, \text{ and } f'(x) = 0 \right\} \subseteq \mathrm{PCO}^+(f).$$

In the next proposition we will use Dubinin's theorem.

Proposition 3.2. *Let $f \in \mathbb{C}[T]$ be monic of degree $d \geq 2$ such that $f'(0) = 0$. Let $n \in \mathbb{N}$ such that there exist $q \geq 0$ and $\gamma_1, \ldots, \gamma_q \in \mathbb{C}^\times$ with $\mathrm{PCO}^+_n(f) \subseteq \mathcal{H}(\gamma_1, \ldots, \gamma_q)$. Let $m \geq 1$, and let $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ be arbitrary. There is a simply connected domain $U \subseteq \widehat{\mathbb{C}}$ containing ∞ with the following properties.*

(i) *We have $0, \alpha_1, \ldots, \alpha_m \notin U$ and $\widehat{\mathbb{C}} \setminus U$ is a compact subset of $\mathbb{C}$.*

(ii) *We have*

$$\mathrm{cap}(\widehat{\mathbb{C}} \setminus U) \leq 4^{-1/(qd^n+m)} \max\{|\gamma_1|, \ldots, |\gamma_q|, |f^{(n)}(\alpha_1)|, \ldots, |f^{(n)}(\alpha_m)|\}^{1/d^n}.$$

To prepare for the proof of Proposition 3.2, let $f \in \mathbb{C}[T]$ denote a monic polynomial of degree $d \geq 2$ with $f'(0) = 0$. Let $n \in \mathbb{N}$, and suppose $\gamma_1, \ldots, \gamma_q \in \mathbb{C}^\times$ are such that $I_0 = \mathcal{H}(\gamma_1, \ldots, \gamma_q)$ contains $\mathrm{PCO}^+_n(f)$.

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

We apply Lemma 3.1 to $f^{(n)}$ and $B = I_0$; the fundamental group of $\mathbb{C} \setminus I_0$ is cyclic and generated by a large enough loop. We set

$$H_f^{(n)} = (f^{(n)})^{-1}(I_0).$$

By Lemma 3.1, the complement $\mathbb{C} \setminus H_f^{(n)}$ is connected and $\widehat{\mathbb{C}} \setminus H_f^{(n)}$ is simply connected. Observe that $0 \in H_f^{(n)}$ because 0 is a critical point of f.

We will show that a branch of $z \mapsto f^{(n)}(z)^{1/d^n}$ admits a holomorphic continuation on $\mathbb{C} \setminus H_f^{(n)}$. Moreover, this continuation will be a biholomorphic map between $\mathbb{C} \setminus H_f^{(n)}$ and the complement of a hedgehog.

Let $z \in \mathbb{C}$ satisfy $f^{(n)}(z) = 0$. Then $z \in H_f^{(n)}$ as $0 \in I_0$. Therefore, $f^{(n)}$ has no roots in $\mathbb{C} \setminus H_f^{(n)}$. The association $w \mapsto f^{(n)}(w^{-1})$ is meromorphic on $\mathbb{C} \setminus \tilde{H}$ with $\tilde{H} = \{w \in \mathbb{C}^\times : w^{-1} \in H_f^{(n)}\}$ closed in $\mathbb{C}$. It never vanishes and has only one pole at $0 \in \mathbb{C} \setminus \tilde{H}$ the order of which is d^n. It follows that $\tilde{f}\colon w \mapsto w^{d^n} f^{(n)}(w^{-1})$ is holomorphic on $\mathbb{C} \setminus \tilde{H}$ without zeros. Moreover, $\tilde{f}(0) = 1$ as f is monic.

The complements $\widehat{\mathbb{C}} \setminus H_f^{(n)}$ and $\mathbb{C} \setminus \tilde{H}$ are homeomorphic via the Möbius transformation $z \mapsto z^{-1}$. In particular, the latter is simply connected. So there exists a holomorphic function $\tilde{g}_n\colon \mathbb{C} \setminus \tilde{H} \to \mathbb{C}$ with $\tilde{g}_n(w)^{d^n} = \tilde{f}(w)$ for all $w \in \mathbb{C} \setminus \tilde{H}$ and with $\tilde{g}_n(0) = 1$. We resubstitute $z = 1/w$ and define $g_n(z) = z\tilde{g}_n(z^{-1})$ to find

$$g_n(z)^{d^n} = f^{(n)}(z) \tag{3.2}$$

for all $z \in \mathbb{C} \setminus H_f^{(n)}$. Then g_n is holomorphic and $g_n(z) = z + O(1)$ as $z \to \infty$.

Let $z \in \mathbb{C} \setminus H_f^{(n)}$. Then $g_n(z) \in \mathbb{C} \setminus I_n$ with $I_n = \{z \in \mathbb{C} : z^{d^n} \in I_0\}$ by Equation (3.2). Now,

$$I_n = \mathcal{H}\big(e^{2\pi\sqrt{-1}j/d^n} w_i\big)_{\substack{1 \le i \le q \\ 1 \le j \le d^n}} \tag{3.3}$$

is a hedgehog with at most qd^n quills where the w_i satisfy $w_i^{d^n} = \gamma_i$.

Let us consider two examples.

First, suppose $f = T^2$. In this case, the post-critical set equals $\{0\}$. We may take $q = 0$ and $I_0 = \mathcal{H}() = \{0\}$. For all $n \in \mathbb{N}$, we have $H_f^{(n)} = I_n = \{0\}$. Moreover, $g_n(z) = z$ for all $z \in \mathbb{C}^\times$.

Second, say $f = T^2 - 2$. Its post-critical set is $\{-2, 2\}$. This time the hedgehog $I_0 = \mathcal{H}(-2, 2) = [-2, 0] \cup [0, 2]$ has $q = 2$ quills. As $f^{-1}([-2, 2]) = [-2, 2]$, we have $H_f^{(n)} = [-2, 2]$ for all $n \in \mathbb{N}$. In particular, $f^{(n)}(z) \neq 0$ for all $z \in \mathbb{C} \setminus [-2, 2]$. The polynomial mapping $w \mapsto w^{2^n} f^{(n)}(w^{-1})$ does not vanish on the simply connected domain $\mathbb{C} \setminus ((-\infty, -1/2] \cup [1/2, \infty))$ and attains 1 at $z = 0$. So it has a holomorphic 2^n-th root $\tilde{g}_n$ that maps 0 to 1. As above, we set $g_n(z) = z\tilde{g}_n(z^{-1})$ for all $z \in \mathbb{C} \setminus [-2, 2]$. Then g_n takes values in $\mathbb{C} \setminus I_n$. Here, I_n is a hedgehog with 2^{n+1} quills ending at $2^{1/2^n} e^{2\pi\sqrt{-1}(k+\delta)/2^n}$ for $k \in \mathbb{Z}$ and $\delta \in \{0, 1/2\}$.

We return to the general case. The map g_n is a key tool in constructing U from Proposition 3.2. Let us first show that it is injective and determine its image.

Lemma 3.3. *The holomorphic function g_n induces a bijection $\mathbb{C} \setminus H_f^{(n)} \to \mathbb{C} \setminus I_n$.*

Proof. Suppose $z \in \mathbb{C} \setminus H_f^{(n)}$ is a critical point of g_n. Taking the derivative of Equation (3.2) gives $d^n g_n(z)^{d^n-1} g_n'(z) = (f^{(n)})'(z)$ and hence $(f^{(n)})'(z) = 0$. The chain rule yields $f'(f^{(n-1)}(z)) \cdots f'(z) = 0$, so f' vanishes at $f^{(j)}(z)$ for some $j \in \{0, \ldots, n-1\}$. Hence, $f^{(n)}(z) \in \mathrm{PCO}_n^+(f)$. But $\mathrm{PCO}_n^+(f) \subseteq I_0$ by our standing hypothesis and so $z \in H_f^{(n)}$. This is a contradiction. We conclude that g_n has no critical points on its domain $\mathbb{C} \setminus H_f^{(n)}$ and that it is a local homeomorphism.

Let us verify that the map $\mathbb{C}\setminus H_f^{(n)} \to \mathbb{C}\setminus I_n$ is proper. Indeed, let $\mathcal{K}$ be compact with $\mathcal{K}\subseteq \mathbb{C}\setminus I_n$. We need to verify that $g_n^{-1}(\mathcal{K})$ is compact. To this end, let $(x_k)_{k\in\mathbb{N}}$ be a sequence in $g_n^{-1}(\mathcal{K})$. If the sequence is unbounded, then so is $(f^{(n)}(x_k))_{k\in\mathbb{N}}$. This is impossible as $f^{(n)}(x_k) = g_n(x_k)^{d^n}$ lies in the image of $\mathcal{K}$ in $\mathbb{C}$ under the d^n-th power map, itself a bounded set. So we may replace $(x_k)_{k\in\mathbb{N}}$ by a convergent subsequence with limit $x\in\mathbb{C}$. To verify our claim, it suffices to check $x\in g_n^{-1}(\mathcal{K})$. If $x\in\mathbb{C}\setminus H_f^{(n)}$, then $g_n(x) = \lim_{k\to\infty} g_n(x_k)\in\mathcal{K}$ and we are done. Let us assume $x\in H_f^{(n)}$. As $\mathcal{K}$ is compact, we may pass to a subsequence for which $(g_n(x_k))_{k\in\mathbb{N}}$ converges to $y\in\mathcal{K}$. Now, $y^{d^n} = \lim_{k\to\infty} f^{(n)}(x_k) = f^{(n)}(x)\in I_0$ using that $f^{(n)}$ is a polynomial. Hence, $y\in I_n$, but this contradicts $\mathcal{K}\subseteq\mathbb{C}\setminus I_n$.

The continuous map $\mathbb{C}\setminus H_f^{(n)} \to \mathbb{C}\setminus I_n$ is a proper local homeomorphism. So it is open and closed, hence surjective as both $\mathbb{C}\setminus H_f^{(n)}$ and $\mathbb{C}\setminus I_n$ are connected. We find that $\mathbb{C}\setminus H_f^{(n)} \to \mathbb{C}\setminus I_n$ is a topological covering using again Lemma 2 [Ho75].

Recall that I_0 contains all critical values of $z\mapsto z^{d^n}$ and $z\mapsto f^{(n)}(z)$. The fiber of either map above a point of $\mathbb{C}\setminus I_0$ contains $d^n = \deg f^{(n)}$ elements. So Equation (3.2) implies that g_n is injective. □

The inverse of a holomorphic bijection is again holomorphic. So the inverse

$$h_n\colon \mathbb{C}\setminus I_n \to \mathbb{C}\setminus H_f^{(n)}$$

of g_n is also holomorphic; the function h_n is a branch of $z\mapsto (f^{(n)})^{-1}(z^{d^n})$. We have

$$h_n(z) = z + O(1) \text{ for } z\to\infty$$

by the same property of g_n. Thus, h_n extends to a homeomorphism $\widehat{\mathbb{C}}\setminus I_n \to \widehat{\mathbb{C}}\setminus H_f^{(n)}$.

Proof of Proposition 3.2. If $\alpha_i\in\mathbb{C}\setminus H_f^{(n)}$, then the value $g_n(\alpha_i)$ is well-defined. We define a further hedgehog

$$I_n' = I_n \cup \mathcal{H}\big(g_n(\alpha_i)\big)_{\substack{1\le i\le m\\ \alpha_i\notin H_f^{(n)}}} \tag{3.4}$$

with at most $qd^n + m$ quills; see Equation (3.3).

The hedgehog complement $\widehat{\mathbb{C}}\setminus I_n'$ is connected and simply connected, and therefore so is its homeomorphic image

$$U = h_n(\widehat{\mathbb{C}}\setminus I_n'). \tag{3.5}$$

The image U lies open in $\widehat{\mathbb{C}}\setminus H_f^{(n)}$ and thus in $\widehat{\mathbb{C}}$. Because $\infty\in U$, we find that $\widehat{\mathbb{C}}\setminus U = \mathbb{C}\setminus U$ is compact; this yields part of the claim of (i).

Recall $0\in H_f^{(n)}$, so $0\notin U$. Suppose $\alpha_i\in U$ for some i. So $\alpha_i\notin H_f^{(n)}$ and thus $g_n(\alpha_i)\in I_n'$ by construction. But α_i also lies in the image of h_n, that is, $\alpha_i = h_n(\beta)$ for some $\beta\in\mathbb{C}\setminus I_n'$. We deduce $g_n(\alpha_i) = g_n(h_n(\beta)) = \beta$, which is a contradiction. So no α_i lies in U. This implies the rest of (i).

We apply Theorem 5.2.3 [Ran95] with $K_1 = I_n', K_2 = \widehat{\mathbb{C}}\setminus U, D_1 = \widehat{\mathbb{C}}\setminus I_n', D_2 = U$, and f as $h_n|_{D_1}\colon D_1\to D_2$ extended as above to send $\infty\mapsto\infty$. Hence,

$$\operatorname{cap}(\widehat{\mathbb{C}}\setminus U) \le \operatorname{cap}(I_n').$$

Recall that I_n' is a hedgehog with at most $qd^n + m$ quills and lengths given in Equations (3.3) and (3.4). Dubinin's theorem [Dub84] implies

$$\operatorname{cap}(I_n') \le 4^{-1/(qd^n+m)} \max\{|\gamma_1|^{1/d^n},\ldots,|\gamma_q|^{1/d^n}, |g_n(\alpha_i)| : \alpha_i\in\mathbb{C}\setminus H_f^{(n)}\}.$$

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

Combining these two estimates and using $|g_n(\alpha_i)| = |f^{(n)}(\alpha_i)|^{1/d^n}$ if $\alpha_i \in \mathbb{C} \setminus H_f^{(n)}$ yields

$$\mathrm{cap}(\widehat{\mathbb{C}} \setminus U) \leq 4^{-1/(qd^n+m)} \max\{|\gamma_1|, \ldots, |\gamma_q|, |f^{(n)}(\alpha_1)|, \ldots, |f^{(n)}(\alpha_m)|\}^{1/d^n}.$$

This completes the proof of (ii). □

We keep the notation of the previous proof and make a final expository remark. The complement of U as in Equation (3.5) is obtained by augmenting $H_f^{(n)}$. More precisely, we claim that

$$\mathbb{C} \setminus U = H_f^{(n)} \cup h_n(I_n' \setminus I_n). \tag{3.6}$$

Indeed, note that $U = h_n(\widehat{\mathbb{C}} \setminus I_n') \subseteq h_n(\widehat{\mathbb{C}} \setminus I_n) = \widehat{\mathbb{C}} \setminus H_f^{(n)}$ as $I_n \subseteq I_n'$. Taking the complement in $\mathbb{C}$ yields $H_f^{(n)} \subseteq \mathbb{C} \setminus U$. Suppose $z = h_n(w)$ with $w \in I_n' \setminus I_n$. If $z \in U$, then $z = h_n(w')$ for some $w \in \widehat{\mathbb{C}} \setminus I_n'$. But then $w = w'$ because h_n is injective; this is a contradiction. So the right-hand side of Equation (3.6) is contained in its left-hand side. To see the converse inclusion, we suppose $z \in \mathbb{C} \setminus U$ and $z \notin H_f^{(n)}$. As h_n maps onto $\widehat{\mathbb{C}} \setminus H_f^{(n)}$, there is $w \in \widehat{\mathbb{C}} \setminus I_n$ with $z = h_n(w)$. Because $z \notin U$, we must have $w \in I_n'$. Thus, $z \in h_n(I_n' \setminus I_n)$. This completes the proof of Equation (3.6).

Next, we make the estimate in Proposition 3.2 more explicit for polynomials of the shape $T^d + c$.

Proposition 3.4. *Let $d \geq 2$ be an integer, and let $f = T^d + c \in \mathbb{C}[T]$. Let $n \in \mathbb{N}$ such that $\mathrm{PCO}_n^+(f)$ is contained in a hedgehog with at most $q \geq 0$ quills. Let $m \geq 1$, and let $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$. There is a simply connected domain $U \subseteq \widehat{\mathbb{C}}$ with the following properties.*

(i) *We have $0, \alpha_1, \ldots, \alpha_m \notin U$ and $\widehat{\mathbb{C}} \setminus U$ is a compact subset of $\mathbb{C}$.*
(ii) *We have*

$$\mathrm{cap}(\widehat{\mathbb{C}} \setminus U) \leq 4^{-1/(qd^n+m)} \mathsf{C}(f)^{1/d^n} e^{\max\{\lambda_f(0), \lambda_f(\alpha_1), \ldots, \lambda_f(\alpha_m)\}}.$$

Proof. By hypothesis, there are $\gamma_1, \ldots, \gamma_q \in \mathbb{C}^\times$ with $\mathrm{PCO}_n^+(f) \subseteq \mathcal{H}(\gamma_1, \ldots, \gamma_q)$. By shortening and omitting quills, we may assume that each γ_i lies in $\mathrm{PCO}_n^+(f)$. In other words, for each i there is $n_i \in \{1, \ldots, n\}$ with $\gamma_i = f^{(n_i)}(0)$. By the definition (1.2) of $\mathsf{C}(f)$, we have $|\gamma_i| \leq \mathsf{C}(f) e^{\lambda_f(f^{(n_i)}(0))} \leq \mathsf{C}(f) e^{d^{n_i}\lambda_f(0)} \leq \mathsf{C}(f) e^{d^n \lambda_f(0)}$. The same definition also gives $|f^{(n)}(\alpha_i)| \leq \mathsf{C}(f) e^{d^n \lambda_f(\alpha_i)}$ for all i. The proof follows from Proposition 3.2. □

Our applications require $\lambda_f(0) = 0$ in Equation (3.4).

We conclude this section by deducing upper bounds for $\mathsf{C}(f)$ when $f = T^d + c \in \mathbb{C}[T]$. Ingram has related estimates; see Section 2 [Ing09].

Lemma 3.5. *Let $d \geq 2$ be an integer, and let $c \in \mathbb{C}$. The polynomial $T^d - T - |c|$ has a unique root r in $(0, \infty)$. Moreover, $r \geq 1$ and $\log^+ |z^d + c| \geq -(d-1) \log r + d \log^+ |z|$ for all $z \in \mathbb{C}$ with $|z| \geq r$.*

Proof. Both statements are invariant under rotating c. So we may assume $c \in [0, \infty)$.

The polynomial $T^d - T - c$ is a convex function on $(0, \infty)$, and it is negative for small positive arguments. So it has exact one root r in $(0, \infty)$. We must have $r \geq 1$ as $1^d - 1 - c \leq 0$.

Let $z \in \mathbb{C}$. We prove the lemma by showing

$$\frac{\max\{1, |z^d + c|\}}{\max\{1, |z|^d\}} \geq \frac{1}{r^{d-1}} \tag{3.7}$$

for all $z \in \mathbb{C}$ with $|z| \geq r$. Note that $|z| \geq r \geq 1$ gives $|z|^d - c \geq |z|$. The triangle inequality implies $|z^d + c| \geq \big||z^d| - c\big| \geq |z| \geq 1$. So the left-hand side of Equation (3.7) equals $|z^d + c|/|z^d| = |1 + c/z^d| > 0$. By the minimum modulus principle, we have $|1 + c/z^d| \geq 1$ for all z with $|z| \geq r$, or $|1 + c/z^d|$ attains a minimum < 1 on the boundary $|z| = r$. In the first case, Equation (3.7) holds true. Finally, if $|z| = r$ and $|1 + c/z^d|$ is minimal, then necessarily $z^d = -r^d$ by elementary geometry. In this case, $|1 + c/z^d| = |1 - c/r^d| = |(r^d - c)/r^d| = r^{1-d}$ and we recover Equation (3.7). $\square$

Lemma 3.6. *Let $d \geq 2$ be an integer, and let $c \in \mathbb{C}$. Let $r \geq 1$ be as in Lemma 3.5. Then $\mathsf{C}(T^d + c) \leq r$.*

Proof. Set $f = T^d + c$. Observe that by Lemma 3.5 we have $|f(z)| \geq r$ if $|z| \geq r$. By a simple induction, we find $\log^+ |f^{(n)}(z)| \geq -(d-1)\log r + d\log^+ |f^{(n-1)}(z)|$ for all $n \geq 1$ if $|z| \geq r$. Considering the telescoping sum, we get

$$\begin{aligned}\frac{\log^+ |f^{(n)}(z)|}{d^n} - \log^+ |z| &= \sum_{j=1}^{n} \frac{\log^+ |f^{(j)}(z)|}{d^j} - \frac{d\log^+ |f^{(j-1)}(z)|}{d^j} \\ &\geq \sum_{j=1}^{n} \frac{-(d-1)\log r}{d^j} \geq \sum_{j=1}^{\infty} \frac{-(d-1)\log r}{d^j} = -\log r.\end{aligned}$$

On taking the limit $n \to \infty$, the left-hand side becomes $\lambda_f(z) - \log^+ |z|$ by Equation (1.1). So we obtain $\log^+ |z| \leq \log r + \lambda_f(z)$ if $|z| \geq r$. Since λ_f is nonnegative, this bound also holds if $|z| < r$. We obtain $\log^+ |z| - \lambda_f(z) \leq \log r$ for all $z \in \mathbb{C}$. The lemma follows from the definition (1.2). $\square$

Lemma 3.7. *Let $d \geq 2$ be an integer, let $c \in \mathbb{C}$ and let $f = T^d + c$. Suppose $\mathrm{PCO}^+(f) = \{f^{(n)}(0) : n \in \mathbb{N}\}$ is a bounded set.*

(i) *We have $|c| \leq 2^{1/(d-1)}$ and $\mathsf{C}(f) \leq 2^{1/(d-1)}$.*
(ii) *Suppose $c^{d-1} \neq -2$. Then $\mathsf{C}(f) < 2^{1/(d-1)}$.*
(iii) *Suppose d is odd. Then $\mathsf{C}(f) < 2^{1/(d-1)}$.*

Proof. By hypothesis, we have $\lambda_f(c) = \lambda_f(f(0)) = 0$. Thus, $|c| \leq \mathsf{C}(f) \leq r$ by Lemma 3.6, where r is the unique positive real number with $r^d = r + |c|$. As $T^d - T - |c|$ has no roots on $(0, r)$ by Lemma 3.5 we find that it takes negative values on $(0, r)$. So $|c|^d \leq |c| + |c|$ and therefore $|c| \leq t$, where $t = 2^{1/(d-1)}$. We note $t^d - t - |c| \geq t^d - t - t = 0$ and hence $t \geq r$. We conclude $\mathsf{C}(f) \leq r \leq t = 2^{1/(d-1)}$. Part (i) follows.

For the proof of (ii), let us assume $\mathsf{C}(f) = 2^{1/(d-1)}$ and retain the notation from the proof of part (i). Then $r = t$ and hence $2^{1/(d-1)}$ is a root of $T^d - T - |c|$. This yields $|c| = 2^{1/(d-1)}$ after a short calculation.

Suppose $d = 2$. Then it is well-known that the Mandelbrot set meets the circle of radius 2 with center 0 in the single point -2. This implies (ii) for $d = 2$. Here is a direct verification that extends to all $d \geq 2$. It involves $c^d + c$, the second iterate of 0 under f. Indeed, its orbit under f is also bounded and so $|c||c^{d-1} + 1| = |c^d + c| \leq \mathsf{C}(f) = 2^{1/(d-1)}$. But $|c| = 2^{1/(d-1)}$ and thus $|c^{d-1} + 1| \leq 1$. The circle around 0 of radius 2 meets the closed disk around -1 of radius 1 in the single point -2. We conclude $c^{d-1} = -2$, and this implies (ii).

In (iii), we have that d is odd. We will prove $c^{d-1} \neq -2$ by contradiction; (iii) then follows from (ii). Indeed, if $c^{d-1} = -2$, then $f^{(2)}(0) = c^d + c = -c$. So $f^{(3)}(0) = -c^d + c$ has absolute value $|c||c^{d-1} - 1| = 3|c| > 2^{1/(d-1)} \geq \mathsf{C}(f)$. But then $\lambda_f(f^3(0)) > 0$ and this contradicts the hypothesis that the f-orbit of 0 is bounded. $\square$

We are now ready to prove Lemma 1.2 from the introduction.

Proof of Lemma 1.2. Let σ_0 be a complex embedding of K as in (i) or (ii). By hypothesis, $\sigma_0(f) \neq T^2 - 2$ and $d = p$ is a prime. Moreover, $\mathrm{PCO}^+(\sigma_0(f))$ is bounded in both (i) and (ii). So Lemma 3.7 yields $\mathsf{C}(\sigma_0(f)) < 2^{1/(p-1)} \leq 2$; if $p = 2$ we use part (ii), and if $p \geq 3$ we use (iii).

For case (i), the embedding σ_0 is real. The set $\mathrm{PCO}^+(\sigma_0(f)) = \{\sigma_0(f)(0), \sigma_0(f)^{(2)}(0), \ldots\}$ lies in $\mathbb{R}$. So it is contained in the union $[-\alpha, 0] \cup [0, \beta]$ of $q = 2$ quills. Thus, $q \log \mathsf{C}(\sigma_0(f)) < \log 4$ and Equation (1.4) is satisfied.

In case (ii), the set $\mathrm{PCO}^+(\sigma_0(f))$ is finite and can be covered by $q \leq 2p - 2$ quills. Now, we find $q \log \mathsf{C}(\sigma_0(f)) < 2(p-1)\log 2^{1/(p-1)} = \log 4$ and Equation (1.4) is again satisfied. $\square$

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

4. Proof of main results

The following lemma is well-known; the second claim goes back to Gleason. See Lemme 2, Exposé XIX [DH84] for $p = 2$, and to Epstein and Poonen [Eps12]. For the reader's convenience, we give a proof.

Lemma 4.1. *Let p be a prime number and $f = T^p + c \in \mathbb{C}[T]$.*

(i) *Suppose 0 is f-preperiodic. Then c is an algebraic integer.*
(ii) *Suppose 0 is f-periodic. Then $\mathbb{Q}(c)/\mathbb{Q}$ is unramified above p.*

Proof. We shall consider $P = T^p + X$ as polynomial in $\mathbb{Z}[T, X]$.

We set $P^{(0)} = T, P^{(1)} = P = T^p + X, P^{(2)} = P(P(T, X), X) = (T^p + X)^p + X, P^{(3)} = P(P^{(2)}(T, X), X) = ((T^p + X)^p + X)^p + X$, etc. A simple induction shows that $P^{(k)}$ is monic of degree p^{k-1} in X for all $k \in \mathbb{N}$.

Suppose $c \in \mathbb{C}$ such that 0 is f-preperiodic, where $f = T^p + c$. So there exist integers k, l with $0 \le k < l$ such that $P^{(k)}(0, c) = P^{(l)}(0, c)$. This produces a monic polynomial in integral coefficients of degree p^{l-1} that vanishes at c. Part (i) follows.

For part (ii), we observe that $P^{(k)} = (P^{(k-1)})^p + X$ for $k \in \mathbb{N}$. The derivative by X satisfies $\frac{\partial}{\partial X} P^{(k)} = pP^{(k-1)} \frac{\partial}{\partial X} P^{(k-1)} + 1 \in 1 + p\mathbb{Z}[T, X]$. We specialize T to 0 and get $\frac{\partial}{\partial X} P^{(k)}(0, X) \in 1 + p\mathbb{Z}[X]$.

The determinant of the Sylvester matrix of the pair $P^{(k)}(0, X), \frac{\partial}{\partial X} P^{(k)}(0, X)$ is up to sign the discriminant of $P^{(k)}(0, X)$. The reduction modulo p of this matrix has upper triangular form with diagonal entries $\equiv 1 \pmod{p}$. In particular, the discriminant is not divisible by p.

If 0 is f-periodic with $f = T^p + c$, then $f^{(k)}(0) = 0$ for some $k \in \mathbb{N}$. The $\mathbb{Q}$-minimal polynomial of c has integral coefficients by (i), and it divides $P^{(k)}(0, X)$. So its discriminant is not divisible by p either. This implies (ii). □

The following result is a special case of the Pólya–Bertrandias theorem; it is crucial for our application and is also at the core of Dimitrov's proof of the Schinzel–Zassenhaus conjecture.

Let K be a number field, and let $\mathcal{O}_K$ denote the ring of algebraic integers of K. For $\phi = \sum_{j \ge 0} \phi_j / X^j \in K[[1/X]]$ and $\sigma \in \mathrm{Hom}(K, \mathbb{C})$, we define $\sigma(\phi) = \sum_{j \ge 0} \sigma(\phi_j)/X^j \in \mathbb{C}[[1/X]]$. Recall that $\mathrm{cap}(\mathcal{K})$ is the transfinite diameter of a nonempty compact subset $\mathcal{K} \subseteq \mathbb{C}$.

Theorem 4.2 (Pólya–Bertrandias). *Let K be a number field and $\phi \in \mathcal{O}_K[[1/X]]$. Suppose that for each $\sigma \in \mathrm{Hom}(K, \mathbb{C})$ there exists a connected open subset $U_\sigma \subseteq \mathbb{C}$ with the following properties.*

(i) *The complement $\mathbb{C} \setminus U_\sigma$ is compact.*
(ii) *The formal power series $\sigma(\phi)$ converges at all $z \in \mathbb{C}$ with $|z|$ sufficiently large.*
(iii) *The holomorphic function induced by $\sigma(\phi)$ as in (ii) extends to a holomorphic function on U_σ.*

If $\prod_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \mathrm{cap}(\mathbb{C} \setminus U_\sigma) < 1$, then ϕ is a rational function.

Proof. This is a special case of Théorème 5.4.6 [Ami75]. Note that our power series has integral coefficients, so we can take $P_1(K) = \emptyset$ in the reference. Let $\overline{\sigma}$ denote σ composed with complex conjugation. Then we may take $U_{\overline{\sigma}}$ to be the complex conjugate of U_σ. □

We come to the main technical result of our paper.

Proposition 4.3. *Let p be a prime number, let K be a number field and let $f = T^p + c \in K[T]$. Suppose further that there are $k, l \in \mathbb{N}$ with $k < l$, $f^{(k-1)}(0) = f^{(l-1)}(0)$ and the following properties.*

(i) *Let δ be as in Equation (2.6), and assume $a^{p^{k-\delta-1}} \equiv a^{p^{l-\delta-1}} \pmod{p\mathcal{O}_K}$ for all $a \in \mathcal{O}_K$.*
(ii) *For all field embeddings $\sigma \in \mathrm{Hom}(K, \mathbb{C})$, we assume that there exists $n_\sigma \in \mathbb{N}$ such that $\mathrm{PCO}^+_{n_\sigma}(\sigma(f))$ is contained in a hedgehog with at most $q_\sigma \ge 0$ quills.*

Let $x \in \overline{K}$ be an algebraic integer. Then one of the following conclusions holds true:

(A) *We have*

$$\lambda_f^{\max}(x) \geq \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \frac{1}{p^{l+n_\sigma}} \left(\frac{\log 4}{q_\sigma + 2[K(x):K]p^{-n_\sigma}} - \log \mathsf{C}(\sigma(f)) \right). \tag{4.1}$$

(B) *We have* $[K(f^{(k)}(x)) : K] \leq [K(x) : K]/p$.

(C) *The point x is f-preperiodic,* $\mathrm{preper}(x) \leq k$, *and* $\mathrm{per}(x) \leq (l-k)[K(x) : K]$.

Proof. We begin by observing $c \in \mathcal{O}_K$ by Lemma 4.1(i). Let $A \in K[X]$ be the K-minimal polynomial of x. Then $A \in \mathcal{O}_K[X]$ has degree $D = [K(x) : K]$

We apply Proposition 2.5 to the ring $R = \mathcal{O}_K$. There exists $\phi \in \mathcal{O}_K[[1/X]]$ with

$$\phi^p = (A_l/A_k)^{p-1} \tag{4.2}$$

and

$$\phi = \Phi_p(p^2 B/A_k^p) \quad \text{where} \quad \deg B \leq \deg A_k^p - 1 = pD - 1; \tag{4.3}$$

we recall Equation (2.10). Then $\sigma(\phi)^p = \sigma(A_l/A_k)^{p-1}$ for all $\sigma \in \mathrm{Hom}(K,\mathbb{C})$.

We split $\sigma(A) = (X - x_{\sigma,1}) \cdots (X - x_{\sigma,D})$, where $x_{\sigma,1}, \ldots, x_{\sigma,D} \in \mathbb{C}$ are conjugates of $\sigma(x)$ over $\sigma(K) \subseteq \mathbb{C}$. Then

$$\sigma(\phi)^p = \prod_{j=1}^{D} \left(\frac{X - \sigma(f)^{(l)}(x_{\sigma,j})}{X - \sigma(f)^{(k)}(x_{\sigma,j})} \right)^{p-1}.$$

Recall the degree condition in Equation (4.3). The formal power series $\sigma(\phi) \in \mathbb{C}[[1/X]]$ converges for all $z \in \mathbb{C}$ for which $|z|$ is sufficiently large. For these z, we have

$$\sigma(\phi)(z)^p = \prod_{j=1}^{D} \left(\frac{1 - \sigma(f)^{(l)}(x_{\sigma,j})/z}{1 - \sigma(f)^{(k)}(x_{\sigma,j})/z} \right)^{p-1}. \tag{4.4}$$

We apply Proposition 3.4 to $\sigma(f) = T^p + \sigma(c)$ and n_σ. By hypothesis, $\mathrm{PCO}^+_{n_\sigma}(\sigma(f))$ is contained in a hedgehog with at most $q_\sigma \geq 0$ quills. We take $m = 2D$ and set

$$\alpha_1 = \sigma(f)^{(k)}(x_{\sigma,1}), \ldots, \alpha_D = \sigma(f)^{(k)}(x_{\sigma,D}), \alpha_{D+1} = \sigma(f)^{(l)}(x_{\sigma,1}), \ldots, \alpha_{2D} = \sigma(f)^{(l)}(x_{\sigma,D}). \tag{4.5}$$

We obtain a simply connected domain $U_\sigma \subseteq \widehat{\mathbb{C}}$ with the two stated properties.

The right-hand side of Equation (4.4) is well-defined and nonzero for all $z \in U_\sigma \setminus \{\infty\}$; indeed, none among 0 and the Equation (4.5) lie in U_σ by Proposition 3.4. So the right-hand side extends to a holomorphic function on U_σ that never vanishes; the extension maps ∞ to 1. By the monodromy theorem from complex analysis and since U_σ is simply connected, we conclude that $z \mapsto \sigma(\phi)(z)$, defined *a priori* only if $|z|$ is large, extends to a holomorphic map $\sigma(\phi) : U_\sigma \to \mathbb{C}$.

We split up into two cases.

Case 1. First, suppose that ϕ is not a rational function.

Theorem 4.2 implies

$$0 \leq \sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \log \mathrm{cap}(\widehat{\mathbb{C}} \setminus U_\sigma). \tag{4.6}$$

Recall that $\lambda_{\sigma(f)}(0) = 0$ as f is post-critically finite by hypothesis. This contribution can be omitted from the capacity bound from Proposition 3.4 since the local canonical height is nonnegative. So $k \leq l$

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

implies

$$\sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \log \operatorname{cap}(\widehat{\mathbb{C}}\setminus U_\sigma) \le \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} -\frac{\log 4}{q_\sigma p^{n_\sigma}+2D} + \frac{\log \mathsf{C}(\sigma(f))}{p^{n_\sigma}} + p^l \max_{1\le i\le D} \lambda_{\sigma(f)}(x_{\sigma,i}). \tag{4.7}$$

We compare Equations (4.6) and (4.7) and rearrange to find

$$\sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \max_{1\le i\le D} \lambda_{\sigma(f)}(x_{\sigma,i}) \ge \frac{1}{p^l} \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \left(\frac{\log 4}{q_\sigma p^{n_\sigma}+2D} - \frac{\log \mathsf{C}(\sigma(f))}{p^{n_\sigma}}\right).$$

The left-hand side is at most $[K:\mathbb{Q}]\lambda_f^{\max}(x)$. So conclusion (A) holds.

Case 2. Second, suppose that ϕ is a rational function.

In particular, ϕ is meromorphic on $\mathbb{C}$. It follows from Equation (4.2) that any root of A_l/A_k has vanishing order divisible by p. Let F be a splitting field of A. Then $\{f^{(k)}(\tau(x)) : \tau \in \mathrm{Gal}(F/K)\}$ are the roots of A_k and $\{f^{(l)}(\tau(x)) : \tau \in \mathrm{Gal}(F/K)\}$ are the roots of A_l.

We split up into two subcases.

Subcase 2a. Suppose $\#\{f^{(k)}(\tau(x)) : \tau \in \mathrm{Gal}(F/K)\} \le D/p$. This means $[K(f^{(k)}(x)) : K] \le D/p$, and we are in conclusion (B) because $D = [K(x):K]$.

Subcase 2b. Suppose $\#\{f^{(k)}(\tau(x)) : \tau \in \mathrm{Gal}(F/K)\} > D/p$. Recall $D = \deg A_k$. Then there exists τ such that the vanishing order of A_k at $f^{(k)}(\tau(x))$ is positive and strictly less than p. But then it must also be a zero of A_l. After replacing τ, we may assume $f^{(k)}(\tau(x)) = f^{(l)}(x)$. Recall $k < l$. A simple induction shows $\tau^e(f^{(k)}(x)) = f^{((l-k)e+k)}(x)$ for all $e \in \mathbb{N}$. Indeed, for $e \ge 2$ we have

$$\tau^e(f^{(k)}(x)) = \tau(\tau^{e-1}(f^{(k)}(x))) = \tau(f^{((l-k)(e-1)+k)}(x)) = f^{((l-k)(e-1)+k)}(\tau(x)) = f^{((l-k)e+k)}(x) \tag{4.8}$$

as $f \in K[T]$.

Take e to be $\#\mathrm{Gal}(F/K)$. So $\tau^e(f^{(k)}(x)) = f^{(k)}(x)$ and thus

$$f^{(k)}(x) = f^{((l-k)e+k)}(x).$$

In particular, x is f-preperiodic and $f^{(k)}(x)$ is f-periodic. In other words, $\mathrm{preper}(x) \le k$. So the first two statements in conclusion (C) hold.

By the pigeonhole principle, there are integers e and e' with $0 \le e < e' \le [K(x):K]$ with $\tau^e(f^{(k)}(x)) = \tau^{e'}(f^{(k)}(x))$. So $f^{((l-k)e+k)}(x) = f^{((l-k)e'+k)}(x)$ by Equation (4.8). Hence, x has minimal period at most $(l-k)(e'-e) \le (l-k)[K(x):K]$. Therefore, the final statement in conclusion (C) holds. □

Theorem 4.4. *Let p be a prime number, let K be a number field and let $f = T^p + c \in K[T]$. Suppose further that there are $k, l \in \mathbb{N}$ with $k < l$, $f^{(k-1)}(0) = f^{(l-1)}(0)$, and the following properties.*

(i) *Let δ be as in Equation (2.6), and assume $a^{p^{k-\delta-1}} \equiv a^{p^{l-\delta-1}} \pmod{p\mathcal{O}_K}$ for all $a \in \mathcal{O}_K$.*
(ii) *We suppose hat f satisfies the quill hypothesis.*

Then there exists a constant $\kappa > 0$ depending on the data above with the following properties.

(i) *Let $x \in \overline{K}$ be an algebraic integer and f-wandering. Then $\lambda_f^{\max}(x) \ge \kappa/[K(x):K]^k$.*
(ii) *Let $x \in \overline{K}$ be f-wandering. Then $\hat{h}_f(x) \ge \kappa/[K(x):K]^{k+1}$.*

Proof. We remark that $c \in \mathcal{O}_K$ by Lemma 4.1(i). Let $x \in \overline{K}$ be f-wandering.

Our proof of (i) is by induction on $[K(x):K]$. Here, x is an algebraic integer. We will apply Proposition 4.3. Observe that an f-wandering point cannot lead to conclusion (C).

https://doi.org/10.1017/fms.2023.112 Published online by Cambridge University Press

Let $\sigma_0 \in \mathrm{Hom}(K,\mathbb{C})$ and $q \geq 0$ be as in the quill hypothesis. We introduce two parameters, $\epsilon_0, \epsilon \in (0,1)$ both are sufficiently small and fixed in terms of f and the other given data such as q and $\sigma_0(f)$, but independent of x. We will fix ϵ in function of ϵ_0.

Let $n_{\sigma_0} \geq 1$ be the unique integer with $p^{n_{\sigma_0}} \geq [K(x):K]/\epsilon_0 > p^{n_{\sigma_0}-1}$. For all $\sigma \in \mathrm{Hom}(K,\mathbb{C})$ with $\sigma \neq \sigma_0$, we fix the unique $n_\sigma \in \mathbb{N}$ with $p^{n_\sigma} \geq [K(x):K]/\epsilon > p^{n_\sigma - 1}$.

For any σ, we set $q_\sigma = \#\mathrm{PCO}^+(\sigma(f)) < \infty$. Then $\mathrm{PCO}^+(\sigma(f))$ is contained in a hedgehog with at most q_σ quills and therefore so is $\mathrm{PCO}^+_{n_\sigma}(\sigma(f)) \subseteq \mathrm{PCO}^+(\sigma(f))$.

We have

$$\begin{aligned} Y &= \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \frac{1}{p^{n_\sigma}}\left(\frac{\log 4}{q_\sigma + 2[K(x):K]p^{-n_\sigma}} - \log \mathsf{C}(\sigma(f))\right) \\ &\geq \frac{1}{p^{n_{\sigma_0}}}\left(\frac{\log 4}{q + 2[K(x):K]p^{-n_{\sigma_0}}} - \log \mathsf{C}(\sigma_0(f))\right) - \sum_{\sigma\neq\sigma_0} \frac{\log \mathsf{C}(\sigma(f))}{p^{n_\sigma}} \\ &\geq \frac{1}{p^{n_{\sigma_0}}}\left(\frac{\log 4}{q + 2\epsilon_0} - \log \mathsf{C}(\sigma_0(f))\right) - \frac{\epsilon}{[K(x):K]} \sum_{\sigma\neq\sigma_0} \log \mathsf{C}(\sigma(f)). \end{aligned} \tag{4.9}$$

For ϵ_0 small enough and fixed in function of f, the quill hypothesis (1.4) implies $(\log 4)/(q+2\epsilon_0) - \log \mathsf{C}(\sigma_0(f)) \geq \kappa_1$ where $\kappa_1 = \kappa_1(f) > 0$ depends only on f. So

$$Y \geq \frac{\kappa_1}{p^{n_{\sigma_0}}} - \frac{\epsilon}{[K(x):K]} \sum_{\sigma\neq\sigma_0} \log \mathsf{C}(\sigma(f)) \geq \frac{1}{[K(x):K]}\left(\frac{\kappa_1\epsilon_0}{p} - \epsilon \sum_{\sigma\neq\sigma_0} \log \mathsf{C}(\sigma(f))\right).$$

Now, we fix ϵ small in terms of ϵ_0 and f to achieve $\kappa_1\epsilon_0/(2p) \geq \epsilon \sum_{\sigma\neq\sigma_0} \log \mathsf{C}(\sigma(f))$. So

$$Y \geq \frac{\kappa_2}{[K(x):K]} \quad \text{with} \quad \kappa_2 = \frac{\kappa_1\epsilon_0}{2p}. \tag{4.10}$$

Suppose we are in conclusion (A) of Proposition 4.3. Then $\lambda_f^{\max}(x) \geq Y[K:\mathbb{Q}]^{-1}p^{-l} \geq \kappa_2 p^{-l}/[K(x):\mathbb{Q}]$. This is stronger than the claim as we may assume $\kappa \leq \kappa_2[K:\mathbb{Q}]^{-1}p^{-l}$.

Suppose we are in conclusion (B). Then we have $[K(f^{(k)}(x)):K] \leq [K(x):K]/p < [K(x):K]$. In particular, this rules out $x \in K$, so the base case of the induction was handled by conclusion (A) above. Now, $\lambda_f^{\max}(f^{(k)}(x)) = p^k\lambda_f^{\max}(x)$. Induction on $[K(x):K]$ yields $p^k\lambda_f^{\max}(x) \geq \kappa/[K(f^{(k)}(x)):K]^k \geq \kappa p^k/[K(x):K]^k$. This completes the proof of (i) as conclusion (C) is impossible in the wandering case.

For (ii), we observe that $\hat{h}_f(x)$ is a normalized sum of local canonical heights as in Equation (1.3). Moreover, every local canonical height takes nonnegative values. In particular, $\hat{h}_f(x) \geq \lambda_f^{\max}(x)/[\mathbb{Q}(x):\mathbb{Q}]$. If x is an algebraic integer, then part (i) implies the desired lower bound for $\hat{h}_f(x)$ after adjusting κ. So assume that x is not an algebraic integer. Let F be a number field containing x. There is a non-Archimedean $v \in M_\mathbb{Q}$, which we may identify with a prime number, and a field embedding $\sigma \in \mathrm{Hom}(F,\mathbb{C}_v)$ with $|\sigma(x)|_v > 1$. By anticipating ramification, we find $|\sigma(x)|_v \geq v^{1/[\mathbb{Q}(x):\mathbb{Q}]}$. Thus, $|\sigma(x^p+c)|_v = |\sigma(x)|_v^p > 1$ by the ultrametric triangle inequality and since $c \in \mathcal{O}_K$. Furthermore, $|\sigma(f^{(n)}(x))|_v = |\sigma(x)|_v^{p^n}$ for all $n \in \mathbb{N}$. Therefore, $\lambda_{\sigma(f),v}(\sigma(x)) = \log^+|\sigma(x)|_v \geq (\log v)/[\mathbb{Q}(x):\mathbb{Q}] \geq (\log 2)/[\mathbb{Q}(x):\mathbb{Q}]$. Again, we use that local canonical heights are nonnegative and conclude $\hat{h}_f(x) \geq (\log 2)/[\mathbb{Q}(x):\mathbb{Q}]^2 \geq (\log 2)/[K(x):\mathbb{Q}]^2 = [K:\mathbb{Q}]^{-2}(\log 2)/[K(x):K]^2$. Thetheorem follows as we may assume $\kappa \leq [K:\mathbb{Q}]^{-2}\log 2$. □

We consider an example before moving on. Let $c = -1.543689\ldots$ be the real root of T^3+2T^2+2T+2. Then $[K:\mathbb{Q}] = 3$, where $K = \mathbb{Q}(c)$. Moreover, $f^{(3)}(0) = f^{(4)}(0)$ for $f = T^2+c$ and $\mathrm{PCO}^+(f) \subseteq \mathbb{R}$ is contained in a union of 2 quills. Let $\wp$ be a prime ideal of $\mathcal{O}_K$ containing 2. Then $\wp^3 = 2\mathcal{O}_K$ follows from a pari/gp computation. We claim that $a^4 \equiv a^8 \pmod{2\mathcal{O}_K}$ for all $a \in \mathcal{O}_K$. Indeed, $a^4(a^4-1) \in 2\mathcal{O}_K$

if $a \in \wp$. If $a \notin \wp$, then a is a unit modulo $2\mathcal{O}_K$. So $a^4 - 1 \in 2\mathcal{O}_K$ as the unit group $(\mathcal{O}_K/2\mathcal{O}_K)^\times$ has order 4. So hypothesis (i) in Theorem 4.4 is satisfied with $(k,l) = (4,5)$; note $\delta = 1$. The quill hypothesis is met since $\mathsf{C}(f) < 2$ by Lemma 3.7(ii).

Theorem 4.5. *Let p be a prime number, let K be a number field and let $f = T^p + c \in K[T]$. Suppose k and l are as in Theorem 4.4. Suppose furthermore that f satisfies the quill hypothesis. Let $x \in \overline{K}$ be f-preperiodic. Then*

$$[K(x) : K] \geq p^{\mathrm{preper}(x)/k-1} \tag{4.11}$$

and

$$[K(x) : K] \geq [K(f^{(\mathrm{preper}(x))}(x)) : K] \geq \frac{\mathrm{per}(x)}{l-k}. \tag{4.12}$$

Proof. By hypothesis, the f-orbit of 0 is finite and so is $\mathrm{PCO}^+(f)$. By Lemma 4.1(i), we see that c is an algebraic integer. So x, an f-preperiodic point, is also an algebraic integer. Moreover, $\lambda_f^{\max}(x) = 0$.

Let $\sigma_0 \in \mathrm{Hom}(K,\mathbb{C})$ and $q \geq 0$ be as in the quill hypothesis. Let $\epsilon_0, \epsilon \in (0,1), n_\sigma \in \mathbb{N}$, and $q_\sigma \in \mathbb{N}$, for $\sigma \in \mathrm{Hom}(K,\mathbb{C})$, be as in the proof of Theorem 4.4. Recall that ϵ, ϵ_0 depend on f, q, and $\sigma_0(f)$, but they are independent of x. Moreover, ϵ is small in terms of ϵ_0. Arguing as in the said proof up to Equation (4.10), we find $Y > 0$ with Y as in Equation (4.9). So the right-hand side of Equation (4.1) is strictly positive. Therefore, we can rule out conclusion (A) of Proposition 4.3.

So we are either in conclusion (B) where $[K(f^{(k)}(x)) : K] \leq [K(x) : K]/p$ or conclusion (C) where $\mathrm{preper}(x) \leq k$ and $\mathrm{per}(x) \leq (l-k)[K(x) : K]$.

Observe that we have $\mathrm{preper}(f(x)) = \max\{0, \mathrm{preper}(x) - 1\}$. Iterating gives $\mathrm{preper}(f^{(m)}(x)) = \max\{0, \mathrm{preper}(x) - m\}$ for all integers $m \geq 0$.

We prove Equation (4.11) by induction on $\mathrm{preper}(x)$. The claim is trivial if $\mathrm{preper}(x) \leq k$. So let us assume $\mathrm{preper}(x) > k$. Then we are in conclusion (B) of Proposition 4.3. Hence, $[K(f^{(k)}(x)) : K] \leq [K(x) : K]/p$ and $\mathrm{preper}(f^{(k)}(x)) = \mathrm{preper}(x) - k < \mathrm{preper}(x)$. By induction,

$$[K(x) : K] \geq p[K(f^{(k)}(x)) : K] \geq p^{\mathrm{preper}(f^{(k)}(x))/k} = p^{\mathrm{preper}(x)/k-1},$$

as desired.

The first inequality in Equation (4.12) is immediate. We prove the second inequality in the case where x is f-periodic first. Indeed, then $K(f(x)) = K(x)$ and so we are again in conclusion (C). Hence, $[K(x) : K] \geq \mathrm{per}(x)/(l-k)$, as desired. If x is f-preperiodic, then Equation (4.12) is applicable to the f-periodic $f^{(\mathrm{preper}(x))}(x)$. We find $[K(f^{(\mathrm{preper}(x))}(x)) : K] \geq \mathrm{per}(f^{(\mathrm{preper}(x))}(x))/(l-k)$. The theorem follows as $\mathrm{per}(f^{(m)}(x)) = \mathrm{per}(x)$ for all integers $m \geq 0$. □

Proof of Theorem 1.1. We suppose $f^{(l-1)}(0) = 0$ with $l \geq 2$. We want to apply Theorem 4.4 to $\mathbb{Q}(c)$. Indeed, it suffices to verify that hypothesis (i) holds true for $k = 1$ after possibly adjusting l.

By Lemma 4.1, the parameter c is an algebraic integer and $K/\mathbb{Q}$ is unramified above p.

We write m for the least common multiple of $l-1$ and all residue degrees of all prime ideals of $\mathcal{O}_K$ containing p. So $a \equiv a^{p^m} \pmod{p\mathcal{O}_K}$ for all $a \in \mathcal{O}_K$. Moreover, $f^{(l-1)}(0) = 0$ implies $f^{(m)}(0) = 0$. Note that $[\mathbb{Q}(c,x) : \mathbb{Q}(c)] \leq [K(x) : K][K : \mathbb{Q}]$. Theorem 1.1 follows from Theorem 4.4 applied to $(k,l) = (1, m+1)$; note $\delta = 0$. □

Proof of Corollary 1.3. In cases (i) and (ii), the extension $K/\mathbb{Q}$ is unramified above p. As in the proof of Theorem 1.1, there exists $l \geq 2$ such that the pair $(1,l)$ satisfies the hypothesis of Theorem 4.4.

To prove (i), we assume that y is f-periodic. Let $x \in \overline{K}$, and suppose $n \geq 0$ is minimal with $f^{(n)}(x) = y$. We may assume $n \geq m = \mathrm{per}(y)$. If $\mathrm{preper}(x) \leq n - m$, then $f^{(n-m)}(x)$ is f-periodic and one among $f^{(n-m)}(x), \ldots, f^{(n-1)}(x)$ must equal y. But this contradicts the minimality of n and so $\mathrm{preper}(x) \geq n - m + 1$. Theorem 4.5 implies $[K(x) : K] \geq p^{\mathrm{preper}(x)-1} \geq p^{n-m}$. We conclude (i).

The proof of part (ii) is very similar. Let $n \in \mathbb{N}$, and suppose $x \in \overline{K}$ satisfies $f^{(n)}(x) = y$. We use $1 \le \mathrm{preper}(y) = \mathrm{preper}(f^{(n)}(x)) = \max\{0, \mathrm{preper}(x) - n\}$ to infer $\mathrm{preper}(x) = n + \mathrm{preper}(y) \ge n + 1$. Theorem 4.5 implies $[K(x) : K] \ge p^{\mathrm{preper}(x)-1} \ge p^n$. But $[K(x) : K] \le \deg(f^{(n)} - y) = p^n$, so part (ii) follows.

For part (iii), we no longer restrict the ramification of $K/\mathbb{Q}$. But we assume that y is f-wandering. Note that c is an algebraic integer by Lemma 4.1(i). Let again $f^{(n)}(x) = y$.

We first suppose that y is an algebraic integer. Then x is also an algebraic integer. Then $\lambda_f^{\max}(x) \ge \kappa_1/[K(x) : K]$ by Theorem 1.1(i). The functional equation of the local canonical height implies $\lambda_f^{\max}(x) = \lambda_f^{\max}(y)/p^n$. We combine and rearrange to find $[K(x) : K]\lambda_f^{\max}(y) \ge \kappa_1 p^n$. So $\lambda_f^{\max}(y) > 0$ and $[K(x) : K] \ge \kappa p^n$ with $\kappa = \kappa_1/\lambda_f^{\max}(y)$.

Second, suppose that y is not an algebraic integer. Then there exists a prime number v and a field embedding $\sigma \in \mathrm{Hom}(K, \mathbb{C}_v)$ with $|\sigma(y)|_v > 1$. The ultrametric triangle inequality implies $|\sigma(x)|_v > 1$ and $|\sigma(y)|_v = |\sigma(f^{(n)}(x))|_v = |\sigma(x)|_v^{p^n}$. So the ramification index of $K(x)/K$ at some prime ideal above v grows like a positive multiple of p^n. In particular, $[K(x) : K] \ge \kappa p^n$ for all $n \in \mathbb{N}$, where $\kappa > 0$ is independent of n. □

Proof of Corollary 1.4. We will apply Proposition 4.3 to $p = 2, K = \mathbb{Q}$, and $f = T^2 - 1$.

Observe that $0 = f^{(2)}(0)$. As $a \equiv a^4 \pmod 2$ for all $a \in \mathbb{Z}$, we see that $(k, l) = (1, 3)$ satisfies hypothesis (i) of Proposition 4.3; here, $\delta = 0$. Note that $\mathrm{PCO}^+(f) = \{-1, 0\}$. The single quill $[-1, 0]$ suffices to cover $\mathrm{PCO}_n^+(f)$ for all $n \in \mathbb{N}$. Moreover, the root r from Lemma 3.5 applied to $d = 2$ and $c = -1$ is the golden ratio $(1 + \sqrt{5})/2$. So $\mathsf{C}(T^2 - 1) \le (1 + \sqrt{5})/2$ by Lemma 3.6.

Let x be as in (i). The proof of part (i) is by induction on $[\mathbb{Q}(x) : \mathbb{Q}]$. We fix $n \in \mathbb{N}$ to be minimal with $2^n \ge 3[\mathbb{Q}(x) : \mathbb{Q}]$, so $2^{n-1} < 3[\mathbb{Q}(x) : \mathbb{Q}]$.

Observe that the f-wandering point x is in conclusion (A) or (B) of Proposition 4.3. If $x \in \mathbb{Q}$, then we must be in conclusion (A).

Conclusion (A) implies

$$\begin{aligned}\lambda_f^{\max}(x) &\ge \frac{1}{2^{3+n}}\left(\frac{\log 4}{1 + 2[\mathbb{Q}(x) : \mathbb{Q}]2^{-n}} - \log\frac{\sqrt{5}+1}{2}\right) \ge \frac{1}{2^{3+n}}\log\left(\frac{4^{3/5}\cdot 2}{\sqrt{5}+1}\right)\\ &\ge \frac{1}{48}\log\left(\frac{4^{3/5}\cdot 2}{\sqrt{5}+1}\right)\frac{1}{[\mathbb{Q}(x) : \mathbb{Q}]}.\end{aligned}$$

Part (i) follows in this case and in particular if $x \in \mathbb{Q}$; which is the base case.

In conclusion (B), we have $[\mathbb{Q}(f(x)) : \mathbb{Q}] \le [\mathbb{Q}(x) : \mathbb{Q}]/2$. Part (i) follows by induction on $[\mathbb{Q}(x) : \mathbb{Q}]$ and since $\lambda_f^{\max}(f(x)) = 2\lambda_f^{\max}(x)$.

The estimate in part (ii) follows from part (i) in the integral case. In the nonintegral case, we use the same argument as in the proof of Theorem 4.4(ii) and conclude using $\log 2 > \log(4^{11/10}/(\sqrt{5} + 1))/48$. □

Proof of Corollary 1.5. As in the proof of Corollary 1.4, we set $K = \mathbb{Q}$ and $(k, l) = (1, 3)$. The single quill $[-1, 0]$ covers $\mathrm{PCO}^+(T^2 - 1)$ and we have $\mathsf{C}(T^2 - 1) \le (1 + \sqrt{5})/2$. The numerical condition in the quill hypothesis follows as $(1 + \sqrt{5})/2 < 4$. The corollary follows from Theorem 4.5. □

Acknowledgements. We thank Vesselin Dimitrov for suggesting to the second-named author to investigate the dynamical Schinzel–Zassenhaus for $f = T^2 - 1$. The authors thank Holly Krieger for comments on a draft of this text and Tom Tucker for pointing out a mistake in an earlier version of Corollary 1.3.

Competing interest. The authors have no competing interest to declare.

Financial support. The first-named author received funding from the Swiss National Science Foundation project n° 200020_184623.

References

[Ami75] Y. Amice. *Les nombres p-adiques*, Collection SUP: 'Le Mathématicien' vol. 14 (Presses Universitaires de France, Paris, 1975). *Préface de Ch*. Pisot.

[Bak06] M. Baker, 'A lower bound for average values of dynamical Green's functions', *Math. Res. Lett.* **13**(2–3) (2006), 245–257.

[BIJ+19] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman and T. J. Tucker, 'Current trends and open problems in arithmetic dynamics', *Bull. Amer. Math. Soc. (N.S.)* **56**(4) (2019), 611–685.

[DH84] A. Douady and J. H. Hubbard, *Étude dynamique des polynômes complexes. Partie I*, Publications Mathématiques d'Orsay [Mathematical Publications of Orsay], vol. 84 (Université de Paris-Sud, Département de Mathématiques, Orsay, 1984).

[Dim] V. Dimitrov, 'A proof of the Schinzel–Zassenhaus conjecture on polynomials', Preprint arXiv:1912.12545.

[Dob79] E. Dobrowolski, 'On a question of Lehmer and the number of irreducible factors of a polynomial', *Acta Arith.* **34**(4) (1979), 391–401.

[Dub84] V. N. Dubinin, 'Change of harmonic measure in symmetrization', *Mat. Sb. (N.S.)* **124**(166)(2) (1984), 272–279.

[Eps12] A. Epstein, 'Integrality and rigidity for postcritically finite polynomials', *Bull. Lond. Math. Soc.* **44**(1) (2012), 39–46. With an appendix by Epstein and Bjorn Poonen.

[Ho75] C.-W. Ho, 'A note on proper maps', *Proc. Amer. Math. Soc.* **51** (1975), 237–241.

[Ing09] P. Ingram, 'Lower bounds on the canonical height associated to the morphism $\phi(z) = z^d + c$', *Monatsh. Math.* **157**(1) (2009), 69–89.

[JL17] R. Jones and A. Levy, 'Eventually stable rational functions', *Int. J. Number Theory* **13**(9) (2017), 2299–2318.

[Lut93] M. Lutzky, 'Counting hyperbolic components of the Mandelbrot set', *Phys. Lett. A* **177**(4–5) (1993), 338–340.

[Ran95] T. Ransford, *Potential Theory in the Complex Plane*, London Mathematical Society Student Texts, vol. 28 (Cambridge University Press, Cambridge, 1995).

[Sil07] J. H. Silverman, *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, vol. 241 (Springer, New York, 2007).

[Sto92] M. Stoll, 'Galois groups over Q of some iterated polynomials', *Arch. Math. (Basel)* **59**(3) (1992), 239–244.

[SZ65] A. Schinzel and H. Zassenhaus, 'A refinement of two theorems of Kronecker', *Michigan Math. J.* **12** (1965), 81–85.