

Proportion of periodic points in reduction of polynomials

by

SANTIAGO RADI

Abstract. In 2014, Juul, Kurlberg, Madhu and Tucker asked the following: given K a number field and f a rational function with coefficients in K , if $f_{\mathfrak{p}}$ denotes the reduction of f modulo a prime ideal $\mathfrak{p}$ in the ring of integers of K , what is the limit inferior of the proportion of periodic points of $f_{\mathfrak{p}}$ when the norm of $\mathfrak{p}$ goes to infinity?

Recent results of Fariña-Asategui and the author show that when f is a polynomial of degree $d \geq 2$ that is not linearly conjugate over $\mathbb{C}$ to a Chebyshev polynomial then the limit inferior is zero.

In this article, we address the remaining cases to give a complete classification of the problem in the case of polynomials.

1. Introduction. Let K be a number field, $\mathcal{O}_K$ its ring of integers and f a polynomial with coefficients in K . For all but finitely many prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$, we can consider the reduction map $f_{\mathfrak{p}}$ acting on the residue field $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$.

As $\mathbb{F}_{\mathfrak{p}}$ is a finite field, a point $x \in \mathbb{F}_{\mathfrak{p}}$ is either periodic or strictly preperiodic for $f_{\mathfrak{p}}$. How does the proportion of periodic points vary as the norm of the prime $\mathfrak{p}$ goes to infinity?

The first problem in this direction was formulated by Schur in 1923, who asked for a classification of all polynomials with coefficients in $\mathbb{Q}$ whose reduction is a bijection for infinitely many primes [20] (note that if the reduction is a bijection, every point must be periodic and consequently the proportion of periodic points is 1). The question was answered in 1970 by Fried over any number field K , showing that a polynomial whose reduction is a bijection for infinitely many primes must be a composition of linear polynomials with coefficients in K and Dickson polynomials, where Dickson polynomials are defined by $f(x + a/x) = x^n + a^n/x^n$ with $a \in K$; see [8]. In 2002, Gural-

2020 *Mathematics Subject Classification*: Primary 37C25; Secondary 37P25, 13A35, 11R45, 37F10.

Key words and phrases: arithmetic dynamics, algebraic number theory, proportion of periodic points, reduction of maps in number fields.

Received 30 March 2026; revised 14 July 2026.

Published online 10 October 2026.

nick, Müller and Saxl generalized Fried's result to rational functions over any number field, using the theory of arithmetic and geometric iterated Galois groups [10]. These maps are referred to in [10] as *arithmetically exceptional*.

Although we find infinitely many primes where the proportion of periodic points is 1 for arithmetically exceptional maps, the proportion of periodic points for the other primes might be arbitrarily small. In fact, this is what we expect to happen in a random map. In [7], Flajolet and Odlyzko proved that if $f : S \rightarrow S$ is a random map, where S is finite, then the number of periodic points is asymptotically

$$\sqrt{\frac{\pi \cdot \#S}{2}}$$

when $\#S \rightarrow +\infty$. Therefore, based on this heuristic, we would expect to find prime ideals $\mathfrak{p}$ where the reduction $f_{\mathfrak{p}}$ has a proportion of periodic points arbitrarily small. Unfortunately, the assumption that the reductions of a polynomial behave randomly is far from being true. This leads to the following question:

QUESTION 1.1 ([15, Question 1.4]). *Given a number field K and $f \in K[x]$, denote*

$$\text{Per}(f, \mathbb{F}_{\mathfrak{p}}) := \{\alpha \in \mathbb{F}_{\mathfrak{p}} : \alpha \text{ is periodic for } f_{\mathfrak{p}}\}.$$

What is the value of

$$\text{Per}_{\inf}(f, K) := \liminf_{N(\mathfrak{p}) \rightarrow +\infty} \frac{\#\text{Per}(f, \mathbb{F}_{\mathfrak{p}})}{N(\mathfrak{p})}?$$

Question 1.1 was firstly formulated in 2014 by Juul, Kurlberg, Madhu and Tucker [15], who asked for a classification of the values of $\text{Per}_{\inf}(f, K)$ for every number field K and any rational function $f \in K(x)$ [15, Question 1.4].

In [15], the authors proved that

$$\text{Per}_{\inf}(x^d + c, K) = 0$$

for any $d \geq 2$ and $c \in K$ such that 0 is not preperiodic, allowing them to give a complete classification of the problem in the case of quadratic polynomials over $\mathbb{Q}$ [15, Theorem 1.5]. In [15, Theorem 1.3], they also proved that if f has two critical points whose forward orbits do not intersect, then $\text{Per}_{\inf}(f, K) = 0$.

It is expected that in general $\text{Per}_{\inf}(f, K) = 0$ and this has been confirmed in most of the examples known. In accordance with this, in [15, Theorem 1.2] the authors showed that given a number field K and numbers $\epsilon > 0$ and $d \geq 2$, there is an open Zariski dense set $U_{d,\epsilon}$ in the moduli space of rational functions such that

$$\text{Per}_{\inf}(f, K) \leq \epsilon$$

for all $f \in U_{d,\epsilon}$.

The only cases known where $\text{Per}_{\text{inf}}(f, K) > 0$ correspond to the Chebyshev polynomials. Recall that the Chebyshev polynomial of degree d , denoted T_d , is defined as the unique polynomial with coefficients in $\mathbb{Z}$ satisfying

$$(1) \quad T_d\left(x + \frac{1}{x}\right) = x^d + \frac{1}{x^d}.$$

In [15, Example 7.2] it is proved that if $d \geq 2$ then

$$(2) \quad \text{Per}_{\text{inf}}(T_d, \mathbb{Q}) = \begin{cases} 1/2 & \text{if } d \text{ is an odd prime power,} \\ 1/4 & \text{if } d \text{ is an even prime power,} \\ 0 & \text{otherwise.} \end{cases}$$

In this article, we give a complete answer to Question 1.1. The cases where f is a polynomial of degree $d = 0$ or 1 are straightforward and will be solved in Lemma 3.1. When $d \geq 2$, we rely on the tools of arboreal representations, particularly, the results related to iterated Galois groups and fixed-point proportion. In 1985, Odoni initiated the study of iterated Galois groups and fixed-point proportion to solve problems in number theory [17]. In his pioneering article, he developed these tools to prove that the Dirichlet density of prime numbers dividing at least one term in the Sylvester sequence (defined recursively as $w_0 = 2$ and $w_{n+1} = 1 + w_1 \dots w_n$) is zero. His idea was then generalized to other problems in number theory. Specifically, in 2014 Juul, Kurlberg, Madhu and Tucker proved that

$$(3) \quad \text{Per}_{\text{inf}}(f, K) \leq \text{FPP}(G_{\infty}(\mathbb{C}, f, t)),$$

where FPP is the fixed-point proportion, $G_{\infty}(\mathbb{C}, f, t)$ is the iterated Galois group of f over $\mathbb{C}$ and t is transcendental over $\mathbb{C}$ (see Section 3 for the unexplained terms here and [13] for a survey about the topic).

The recent breakthrough of Fariña-Asategui and the author completely classifies the fixed-point proportion for geometric iterated Galois groups of polynomials [6, Theorem 2]. As $\mathbb{C}$ is algebraically closed, the result applies to this case, implying that $\text{FPP}(G_{\infty}(\mathbb{C}, f, t)) = 0$ if f is not linearly conjugate over $\mathbb{C}$ to $\pm T_d$. Therefore

$$\text{Per}_{\text{inf}}(f, K) = 0$$

if f is not linearly conjugate over $\mathbb{C}$ to $\pm T_d$.

In the case where f is linearly conjugate over $\mathbb{C}$ to $\pm T_d$, the fixed-point proportion of $G_{\infty}(\mathbb{C}, f, t)$ is positive and therefore the upper bound in equation (3) is not enough to calculate $\text{Per}_{\text{inf}}(f, K)$. For these cases, we will work out $\text{Per}_{\text{inf}}(f, K)$ directly. We will prove that if f is linearly conjugate over $\mathbb{C}$ to $\pm T_d$ then

$$(4) \quad \text{Per}_{\text{inf}}(f, K) = \text{Per}_{\text{inf}}(T_d, K).$$

Although this step can look obvious, it is not obvious if the conjugation does not have coefficients in K . We shall see in Section 5 that when the conjugation is not in K , it lies in a field extension K'/K of degree 2. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ that is inert in $\mathcal{O}_{K'}$, then the periodic points of f in $\mathbb{F}_{\mathfrak{p}}$ are in bijection with the periodic points of T_d . But if $\mathfrak{p}$ is split in $\mathcal{O}_{K'}$, then the periodic points of f are in bijection with the periodic points of T_d in a degree-2 extension of $\mathbb{F}_{\mathfrak{p}}$ and some work needs to be done to prove that $\text{Per}_{\inf}(f, K)$ does not change when we restrict to the periodic points of f in $\mathbb{F}_{\mathfrak{p}}$ (see Proposition 5.2 for a proof of this fact).

Once we know equation (4), we reduce the problem to find $\text{Per}_{\inf}(T_d, K)$. The calculation is based on the ideas used by the authors in [15, Example 7.2] for the case of $K = \mathbb{Q}$, implying that

$$\text{Per}_{\inf}(T_d, K) = \frac{1}{2} \liminf_{N(\mathfrak{p}) \rightarrow +\infty} \frac{r(N(\mathfrak{p}) - 1, d) + r(N(\mathfrak{p}) + 1, d)}{N(\mathfrak{p})},$$

where $r(a, b)$ is defined as the largest divisor of a coprime to b .

So, in order to calculate $\text{Per}_{\inf}(T_d, K)$ we need to find infinitely many prime ideals in $\mathcal{O}_K$ such that $N(\mathfrak{p}) - 1$ and $N(\mathfrak{p}) + 1$ have large divisors that are not coprime to d , since this will make $r(N(\mathfrak{p}) - 1, d)$ and $r(N(\mathfrak{p}) + 1, d)$ relatively small compared to $N(\mathfrak{p})$. The main tool to find such prime ideals will be Chebotarev's theorem. However, the existence of roots of unity in K will impose restrictions on the prime factors dividing $N(\mathfrak{p}) - 1$ for all but finitely many prime ideals. Concretely, if m_K is the maximal positive number such that K contains an m_K th root of unity, then for all but finitely many prime ideals, m_K divides $N(\mathfrak{p}) - 1$. The relation between the prime factors of m_K and d will allow us to reduce $r(N(\mathfrak{p}) - 1, d)$ and $r(N(\mathfrak{p}) + 1, d)$ more or less, leading to cases where $\text{Per}_{\inf}(T_d, K)$ is zero and others where $\text{Per}_{\inf}(T_d, K)$ is positive.

In order to state the main theorem, recall that the radical of a number d , denoted $\text{rad}(d)$, is the product of the prime divisors of d . Therefore, note that when we say that $\text{rad}(d) \mid \text{rad}(m)$, this means that all prime divisors of d also divide m . Contrarily, when we say $\text{rad}(d) \nmid \text{rad}(m)$, this means that there exists a prime p such that $p \mid d$ and $p \nmid m$. Given a prime p , the valuation of m at p will be denoted $v_p(m)$.

THEOREM 1. *Let K be a number field and let m_K denote the greatest positive number such that K contains an m_K th primitive root of unity. Let f be a polynomial with coefficients in K and degree d .*

(1) *If $d = 0$ then*

$$\text{Per}_{\inf}(f, K) = 0.$$

(2) *If $d = 1$ then*

$$\text{Per}_{\inf}(f, K) = 1.$$

(3) If $d \geq 2$ and f is not linearly conjugate over $\mathbb{C}$ to $\pm T_d$, then

$$\text{Per}_{\inf}(f, K) = 0.$$

(4) If $d \geq 2$ and f is linearly conjugate over $\mathbb{C}$ to $\pm T_d$, then

$$\text{Per}_{\inf}(f, K) = \text{Per}_{\inf}(T_d, K).$$

(5) If d has at least two prime factors and $\text{rad}(d) \nmid \text{rad}(m_K)$, then

$$\text{Per}_{\inf}(T_d, K) = 0.$$

(6) If d is odd, has at least two prime factors and $\text{rad}(d) \mid \text{rad}(m_K)$, then

$$\text{Per}_{\inf}(T_d, K) = 1/2.$$

(7) If d is even, has at least two prime factors, $\text{rad}(d) \mid \text{rad}(m_K)$ and $v_2(m_K) \geq 2$, then

$$\text{Per}_{\inf}(T_d, K) = 1/4.$$

(8) If d is even, has at least two prime factors, $\text{rad}(d) \mid \text{rad}(m_K)$ and $v_2(m_K) = 1$, then

$$\text{Per}_{\inf}(T_d, K) = 0.$$

(9) If d is an odd prime power, then

$$\text{Per}_{\inf}(T_d, K) = 1/2.$$

(10) If d is an even prime power, then

$$\text{Per}_{\inf}(T_d, K) = 1/4.$$

In the case that $K = \mathbb{Q}$ we have $m_K = 2$ and only the cases (1), (2), (3), (4), (5), (9) and (10) apply. Moreover, the results obtained in Theorem 1 for the case $K = \mathbb{Q}$ are consistent with equation (2).

COROLLARY 2. *If f is a polynomial with coefficients in $\mathbb{Q}$ and degree $d \geq 1$, then*

$$\text{Per}_{\inf}(f, \mathbb{Q})$$

$$= \begin{cases} 1 & \text{if } d=1, \\ 1/2 & \text{if } d \text{ is an odd prime power and } f \text{ is conjugate over } \mathbb{C} \text{ to } \pm T_d, \\ 1/4 & \text{if } d \text{ is an even prime power and } f \text{ is conjugate over } \mathbb{C} \text{ to } \pm T_d, \\ 0 & \text{otherwise.} \end{cases}$$

Although equation (3) also holds in the case of rational functions, there is not a complete classification of the fixed-point proportion of $G_{\infty}(\mathbb{C}, f, t)$ in the case of rational maps. In [6], the authors proved that $\text{FPP}(G_{\infty}(\mathbb{C}, f, t)) = 0$ for rational maps whose critically exceptional set does not have more than one element (see [6, Theorem 6]) and conjectured that the cases of positive fixed-point proportion should come from rational maps with Euclidean

orbifold of type different from (∞, ∞) (see [6, Conjecture 7]). This latter family includes Lattès maps L , although the value of $\text{FPP}(G_\infty(\mathbb{C}, L, t))$ is not known for any of them. Regarding $\text{Per}_{\inf}(L, K)$, the authors in [15, Example 7.3] proved that in many cases, Lattès maps L induced by multiplication by a prime ℓ in an elliptic curve defined over $\mathbb{Q}$ must have $\text{Per}_{\inf}(L, K) = 0$. In contrast to Chebyshev polynomials, there are not known cases of Lattès maps such that $\text{Per}_{\inf}(L, K) > 0$. Therefore, there still remains open a whole classification in the case of rational functions:

QUESTION 1.2. *What are the values of $\text{Per}_{\inf}(f, K)$ for every number field K and every rational function $f \in K(x)$?*

2. Preliminaries

2.1. Iteration of maps and local degree. Given a set S and a function $f : S \rightarrow S$, we use the notation f^n to refer to the n th composition of f with itself. By convention, f^0 equals the identity map in S .

Given $\alpha \in S$, we say that α is *preperiodic* if there exist $m > n \geq 0$ such that $f^n(\alpha) = f^m(\alpha)$. By the pigeonhole principle, if S is finite every point is preperiodic. We say that α is *periodic* if n can be taken zero in the definition of preperiodic. We denote

$$\text{Per}(f, S) := \{\alpha \in S : \alpha \text{ is periodic for } f\}.$$

We say that a point α is *strictly preperiodic* if it is preperiodic but not periodic.

DEFINITION 2.1. Let F be a field, $\overline{F}$ an algebraic closure of F and $f, g \in \overline{F}(x)$. We say that f and g are *linearly conjugate* over F if there exists $L \in F(x)$ of degree 1 such that $g = L^{-1} \circ f \circ L$.

Given $\alpha \in \mathbb{P}^1(F)$ and $f \in F(x)$, the *local degree* of α at f is

$$e_f(\alpha) := \min \{k \geq 1 : f^{(k)}(\alpha) \neq 0\}$$

where $f^{(k)}$ is the k th derivative of f . We say that α is a *critical point* for f if $e_f(\alpha) > 1$. We say that α is *totally ramified* for f if $e_f(\alpha) = \deg(f)$. If f is a polynomial, then ∞ is a totally ramified point.

LEMMA 2.2. *If F is a field and $f, g \in F[x]$ are linearly conjugate over $\overline{F}$ by a function L , and f has only ∞ as a totally ramified point, then L is a polynomial.*

Proof. Write $g = L^{-1} \circ f \circ L$ and suppose that L is not a polynomial. Then $L(\infty) \neq \infty$. By multiplicativity of the local degree and the fact that $e_L(\alpha) = 1$ for every $\alpha \in \mathbb{P}^1(F)$, we have

$$\deg(f) = e_g(\infty) = e_{L^{-1}}(f(L(\infty))) \cdot e_f(L(\infty)) \cdot e_L(\infty) = e_f(L(\infty)),$$

which implies that $L(\infty)$ is totally ramified for f , giving a contradiction. ■

2.2. Algebraic number theory. In this subsection we summarize some results from algebraic number theory that we will use in the article. Choose an embedding ι of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ and given $n \geq 1$, define ξ_n in $\overline{\mathbb{Q}}$ by

$$\iota(\xi_n) = e^{2\pi i/n}.$$

By a slight abuse of notation, we will write $\xi_n = e^{2\pi i/n}$ with no emphasis on the embedding ι .

LEMMA 2.3. *Let K be a number field, $n, m \geq 1$ and suppose that K contains primitive roots of unity of order m and n . Then K contains $\xi_{\text{lcm}(m,n)}$.*

Proof. Taking powers if necessary, we may assume that ξ_m and ξ_n are in K .

By Bézout's theorem there exist $a, b \in \mathbb{Z}$ such that $am + bn = \gcd(m, n)$. Then

$$\xi_m^b \xi_n^a = e^{2\pi i(\frac{b}{m} + \frac{a}{n})} = e^{2\pi i(\frac{am+bn}{mn})} = e^{2\pi i(\frac{\gcd(m,n)}{mn})} = e^{2\pi i(\frac{1}{\text{lcm}(m,n)})}. \blacksquare$$

As K is a number field, it is a finite extension of $\mathbb{Q}$ and therefore Lemma 2.3 justifies the existence of a maximal number $m_K \geq 1$ such that K contains ξ_{m_K} .

LEMMA 2.4. *Let $n \geq 1$ and K a number field. Then*

$$\text{Gal}(K(\xi_n)/K) \cong \{r \in (\mathbb{Z}/\text{lcm}(n, m_K)\mathbb{Z})^\times : r \equiv 1 \pmod{m_K}\}.$$

Proof. By Lemma 2.3, $K(\xi_n) = K(\xi_{\text{lcm}(m_K, n)})$. If $\sigma \in \text{Gal}(K(\xi_n)/K)$ then

$$\sigma(\xi_{\text{lcm}(m_K, n)}) = (\xi_{\text{lcm}(m_K, n)})^{\varphi(\sigma)}$$

for some $\varphi(\sigma) \in (\mathbb{Z}/\text{lcm}(n, m_K)\mathbb{Z})^\times$. Moreover, if $\text{lcm}(m_K, n)/c = m_K$ then

$$\sigma(\xi_{m_K}) = \sigma((\xi_{\text{lcm}(m_K, n)})^c) = (\xi_{\text{lcm}(m_K, n)})^{\varphi(\sigma)c} = (\xi_{m_K})^{\varphi(\sigma)}.$$

But σ must fix ξ_{m_K} so $\varphi(\sigma) \equiv 1 \pmod{m_K}$. By maximality of m_K , we obtain the bijection. $\blacksquare$

The following result will be crucial in Section 6 and is based on Chebotarev's theorem:

PROPOSITION 2.5. *Let K be a number field. Let $\{n_i\}_{i=1}^k$ be a set of positive numbers and $\{a_i\}_{i=1}^k$ another set of numbers such that $a_i \in (\mathbb{Z}/n_i\mathbb{Z})^\times$. If the system of congruences*

$$\begin{cases} x \equiv 1 \pmod{m_K}, \\ x \equiv a_1 \pmod{n_1}, \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has a solution in $\mathbb{Z}$, then for infinitely many prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ we have

$$n_i \mid (N(\mathfrak{p}) - a_i) \quad \text{for all } i = 1, \dots, k.$$

Proof. Let r be a solution and write $n = \text{lcm}(n_1, \dots, n_k)$. By the Chinese remainder theorem we have $r \in (\mathbb{Z}/\text{lcm}(m_K, n)\mathbb{Z})^\times$. By Lemma 2.4, we have that r corresponds to an element $\sigma \in \text{Gal}(K(\xi_n)/K)$. Then, by Chebotarev's theorem, there exist infinitely many prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ such that

$$\text{Frob}_{\mathfrak{p}}(\xi_{\text{lcm}(m_K, n)}) = (\xi_{\text{lcm}(m_K, n)})^r.$$

Write $n_i = \text{lcm}(m_K, n)/c_i$. Then

$$\text{Frob}_{\mathfrak{p}}(\xi_{n_i}) = \text{Frob}_{\mathfrak{p}}((\xi_{\text{lcm}(m_K, n)})^{c_i}) = (\xi_{\text{lcm}(m_K, n)})^{r \cdot c_i} = (\xi_{n_i})^r = (\xi_{n_i})^{a_i}.$$

On the other hand,

$$\text{Frob}_{\mathfrak{p}}(\xi_{n_i}) = (\xi_{n_i})^{N(\mathfrak{p})},$$

so combining both equations we obtain

$$N(\mathfrak{p}) \equiv a_i \pmod{n_i},$$

which implies that $n_i \mid (N(\mathfrak{p}) - a_i)$. ■

2.3. Chebyshev polynomials. Given $d \geq 0$, a field F and $\zeta \in \overline{F}$ we define the *twisted Chebyshev polynomial* of degree d with parameter ζ by

$$T_{d, \zeta}\left(x + \frac{\zeta}{x}\right) := x^d + \frac{\zeta}{x^d}.$$

Note that when $\zeta = 1$, this corresponds to the standard Chebyshev polynomial defined in equation (1).

When $d \geq 1$, then ζ must be a $(d-1)$ th root of unity. Indeed, replacing x by $1/x$ we have

$$\frac{1}{x^d} + \zeta x^d = f\left(\frac{1}{x} + \zeta x\right) = f\left(\frac{\zeta}{\zeta x} + \zeta x\right) = (\zeta x)^d + \frac{\zeta}{(\zeta x)^d} = \zeta^d x^d + \frac{1}{\zeta^{d-1} x^d},$$

which yields $\zeta^{d-1} = 1$.

In [1], Adams considered twisted Chebyshev polynomials as another family of polynomials having iterated Galois groups with bad properties. However, these polynomials are just linearly conjugate to the standard Chebyshev polynomials:

LEMMA 2.6. *Let F be a field, F_p its prime field and $d \geq 1$. Then the twisted Chebyshev polynomial $T_{d, \zeta}$ is linearly conjugate over $F_p(\sqrt{\zeta})$ to $\pm T_d$. Moreover, if d is even then T_d and $-T_d$ are linearly conjugate over F_p .*

Proof. Let ξ_{d-1} be a $(d-1)$ th primitive root of unity. Then $\zeta = \xi_{d-1}^s$ for some $s \in \{0, \dots, d-2\}$. Consider a such that $a^2 = \zeta$. If d is even, then $a = \xi_{d-1}^t$ for some $t \in \{0, \dots, d-2\}$. This is because if $a^2 = \zeta$ then we need

to solve $2t \equiv s \pmod{d-1}$ which has a solution since 2 is invertible modulo $d-1$. In particular, $a^{d-1} = 1$. On the other hand, if d is odd, then

$$a^{d-1} = ((\xi_{d-1})^{\frac{d-1}{2}})^s = (-1)^s.$$

Consider $L(x) = ax$. Then

$$\begin{aligned} L^{-1} \circ T_{d,\zeta} \circ L \left(x + \frac{1}{x} \right) &= L^{-1} \circ T_{d,\zeta} \left(ax + \frac{a^2}{ax} \right) = L^{-1} \left(a^d x^d + \frac{\zeta}{a^d x^d} \right) \\ &= a^{d-1} x^d + \frac{1}{a^{d-1} x^d}. \end{aligned}$$

If d is even, we obtain $L^{-1} \circ T_{d,\zeta} \circ L = T_d$. If d is odd, then $L^{-1} \circ T_{d,\zeta} \circ L = (-1)^s T_d$.

Finally, observe that when d is even, the maps $-T_d$ and T_d are linearly conjugate by $L(x) = -x$. ■

3. Polynomials not linearly conjugate over $\mathbb{C}$ to $\pm T_d$. We start with the points (1) and (2) in Theorem 1. Although it is not of our interest in this article, note that the following proof also applies if f is an invertible rational function of degree 1.

LEMMA 3.1. *Let K be a number field and $f \in K[x]$ a polynomial.*

(1) *If f has degree 0, then*

$$\text{Per}_{\inf}(f, K) = 0.$$

(2) *If f has degree 1, then*

$$\text{Per}_{\inf}(f, K) = 1.$$

Proof. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ of good reduction for f . If f has degree zero then $f_{\mathfrak{p}}(\alpha) = \alpha$ at only one point, so

$$\text{Per}_{\inf}(f, K) = 0.$$

If f is a polynomial of degree 1, then $f_{\mathfrak{p}}$ is invertible. Therefore, if x_0 is a strictly preperiodic point, there exist minimal numbers $n > m \geq 1$ such that $f_{\mathfrak{p}}^n(x_0) = f_{\mathfrak{p}}^m(x_0)$. But then, as m and n are minimal, this implies that $f_{\mathfrak{p}}^m(x_0)$ has two different preimages, $f_{\mathfrak{p}}^{m-1}(x_0)$ and $f_{\mathfrak{p}}^{n-1}(x_0)$, contradicting that $f_{\mathfrak{p}}$ is invertible.

Therefore, every point is periodic and $\text{Per}_{\inf}(f, K) = 1$. ■

The next step is to prove point (3) in Theorem 1, i.e., that $\text{Per}_{\inf}(f, K) = 0$ for every polynomial f that is not linearly conjugate over $\mathbb{C}$ to $\pm T_d$. As mentioned in the introduction, the proof is a simple corollary from the theory of iterated Galois groups and fixed-point proportion that we explain in the following.

Let F be a field, t transcendental over F and fix $F(t)^{\text{sep}}$, a separable closure of $F(t)$. If $f \in F(x)$ is a separable rational function with degree

$d \geq 2$, we denote by $f^{-n}(t)$ the set of preimages of t under f^n . Let

$$F_\infty(f, t) := F\left(\bigcup_{n \geq 0} f^{-n}(t)\right)$$

be the field extension of $F(t)$ obtained by adding all the preimages of t . It can be proved that $F_\infty(f, t)/F(t)$ is a Galois extension. Its Galois group, called the *iterated Galois group* of f over F , is

$$G_\infty(F, f, t) := \text{Gal}(F_\infty(f, t)/F(t)).$$

The Galois group $G_\infty(F, f, t)$ is profinite and acts transitively on $f^{-n}(t)$ for every $n \geq 1$; see [13, 19]. Given $n \geq 1$ and $g \in G_\infty(F, f, t)$, let us denote

$$X_n(g) := \#\{z \in f^{-n}(t) : g(z) = z\}.$$

As $G_\infty(F, f, t)$ is profinite, we can consider μ , its unique Haar probability measure. The *fixed-point proportion* of $G_\infty(F, f, t)$ is defined by

$$\text{FPP}(G_\infty(F, f, t)) := \mu(\{g \in G_\infty(F, f, t) : \#X_n(g) > 0 \text{ for all } n \geq 1\}).$$

It has been known since the eighties that this number has several applications to problems in arithmetic dynamics [14, 16, 17, 18] and for this reason is one of the areas strongly studied currently; see [1, 2, 5, 9, 11, 12] and [3, Section 5].

One of the applications of the fixed-point proportion concerns $\text{Per}_{\text{inf}}(f, K)$.

PROPOSITION 3.2 ([15, proof of Theorem 6.5] or [4, Theorem 3.11]). *Let K be a number field and $f \in K(x)$ a rational function with degree at least 2. Then*

$$\text{Per}_{\text{inf}}(f, K) \leq \text{FPP}(G_\infty(\mathbb{C}, f, t))$$

where t is transcendental over $\mathbb{C}$.

A recent result of Fariña-Asategui and the author classifies the values of the fixed-point proportion for iterated Galois groups over algebraically closed fields:

THEOREM 3.3 ([6, Theorem 2]). *Let F be a field and $f \in F[x]$ a polynomial of degree $d \geq 2$ such that either $\text{char}(F) = 0$ or $\text{char}(F)$ does not divide the local degree of any critical point of f . Then, for t transcendental over F , either*

(i) *f has a Euclidean orbifold of type $(2, 2, \infty)$ and*

$$\text{FPP}(G_\infty(\overline{F}, f, t)) = \begin{cases} 1/2 & \text{if } d \text{ is odd,} \\ 1/4 & \text{if } d \text{ is even,} \end{cases}$$

or

(ii) $\text{FPP}(G_\infty(\overline{F}, f, t)) = 0$.

As proved in [6, Proposition 6.6], polynomials with Euclidean orbifold $(2, 2, \infty)$ are linearly conjugate over $\overline{F}$ to $\pm T_{d,\zeta}$ for some $d \geq 2$ and $\zeta \in \overline{F}$. By Lemma 2.6, we know that in fact the maps $T_{d,\xi}$ are linearly conjugate over $\overline{F}$ to $\pm T_d$.

All this together allows us to conclude point (3) in Theorem 1:

THEOREM 3.4. *Let K be a number field and $f \in K[x]$ a polynomial with degree $d \geq 2$ such that f is not linearly conjugate over $\mathbb{C}$ to $\pm T_d$. Then*

$$\text{Per}_{\inf}(f, K) = 0.$$

Proof. Combine Proposition 3.2 and Theorem 3.3. ■

4. Proportion of periodic points in Chebyshev polynomials. The goal of this section is to calculate $\text{Per}(\pm T_d, F)$ for any field F and any $d \geq 2$, and count its number of elements when F is a finite field. The strategy will follow the idea exposed in [15, Example 7.2], and for this reason we keep much of the notation used there.

Let F be any field of $\text{char}(F) \neq 2$ and $\overline{F}$ its algebraic closure. Given $d \geq 2$, define $\pi(x) := x + x^{-1}$ and $g(x) := x^d$. Then equation (1) can be read as the following commutative diagram:

$$(5) \quad \begin{array}{ccc} \mathbb{P}^1(F) & \xrightarrow{g} & \mathbb{P}^1(F) \\ \downarrow \pi & & \downarrow \pi \\ \mathbb{P}^1(F) & \xrightarrow{T_d} & \mathbb{P}^1(F) \end{array}$$

LEMMA 4.1. *Let F be any field of $\text{char}(F) \neq 2$.*

- (1) *The map $\pi : \mathbb{P}^1(\overline{F}) \rightarrow \mathbb{P}^1(\overline{F})$ is surjective.*
- (2) *We have $\pi(x) = \pi(y)$ if and only if $y = x$ or $y = x^{-1}$.*
- (3) *The only critical points of π are ± 1 with local degree 2.*

Proof. Let $w \in \mathbb{P}^1(F)$. If $w = \infty$, then $\pi(0) = \pi(\infty) = \infty$. If $w \in F$, then $\pi(x) = w$ if and only if

$$x^2 - wx + 1 = 0.$$

This has a solution since we are working over $\overline{F}$. Moreover, since it is a quadratic polynomial it has at most two solutions. As $\pi(x) = \pi(x^{-1})$, this implies that $\pi(x) = \pi(y)$ if and only if $y = x$ or $y = x^{-1}$.

Finally, the derivative of π is

$$\pi'(x) = 1 - x^{-2},$$

so the critical points are ± 1 . As $\pi''(\pm 1) = \pm 2$, we conclude that $e_\pi(\pm 1) = 2$. ■

We summarize well-known properties of the Chebyshev polynomials in the following proposition:

PROPOSITION 4.2. *Let $d \geq 1$ and F a field of characteristic zero.*

(1) $T_0(x) = 2$, $T_1(x) = x$ and we have the recursion

$$T_{d+1}(x) = xT_d(x) - T_{d-1}(x).$$

(2) If $T_d(x) = \sum_{i=0}^d a_{i,d}x^i$, then $a_{i,d} \in \mathbb{Z}$ and $a_{i,d} = 0$ if and only if $i \equiv d \pmod{2}$.

(3) If $\alpha \in \overline{F}$ then $e_{\pm T_d}(\alpha)$ is either 1 or 2. In particular, if $d \geq 3$ then $\pm T_d$ is only totally ramified at ∞ .

Proof. For (1), the first cases are obvious from equation (1). Then

$$\begin{aligned} \left(x + \frac{1}{x}\right)T_d\left(x + \frac{1}{x}\right) &= \left(x + \frac{1}{x}\right)\left(x^d + \frac{1}{x^d}\right) \\ &= T_{d+1}\left(x + \frac{1}{x}\right) + T_{d-1}\left(x + \frac{1}{x}\right). \end{aligned}$$

For (2), using the previous point we have the relation

$$a_{d+1-j,d+1} = a_{d-j,d} - a_{d+1-j,d-1}.$$

Then by induction it follows that

$$\begin{cases} a_{d-j,d} > 0 & \text{if } j \equiv 0 \pmod{4}, \\ a_{d-j,d} = 0 & \text{if } j \equiv 1 \pmod{2}, \\ a_{d-j,d} < 0 & \text{if } j \equiv 2 \pmod{4}. \end{cases}$$

Finally for (3), using equation (1) we obtain

$$T'_d(\pi(x)) = \frac{d}{x^{d-1}} \frac{(x^2)^d - 1}{x^2 - 1}.$$

So, if $\pi(x) \neq \infty$ and we let ξ_{2d} be a primitive $(2d)$ th root of unity, then $T'_d(\pi(x)) = 0$ at the points

$$x_k = (\xi_{2d})^k$$

with $k \notin d\mathbb{Z}$. By multiplicativity of the local degree and diagram (5) we have

$$e_{T_d}(\pi(x_k)) \cdot e_\pi(x_k) = e_\pi(g(x_k)) \cdot e_g(x_k).$$

Then $g(x_k) = \pm 1$ and $e_g(x_k) = 1$. Moreover, by Lemma 4.1, $e_\pi(x_k) = 1$ and $e_\pi(g(x_k)) = 2$, so $e_{T_d}(\pi(x_k)) = 2$. The critical points of $-T_d$ and its corresponding local degrees are the same. ■

In principle we need to find the periodic points of $\pm T_d$. However, the following lemma shows us that we only need to worry about the periodic points of the positive case:

LEMMA 4.3. *Given $d \geq 2$ and a field F , we have*

$$\text{Per}(-T_d, F) = (-1)^{d+1} \text{Per}(T_d, F).$$

Proof. If d is even, by Lemma 2.6 we find that T_d and $-T_d$ are linearly conjugate over F by $L(x) = -x$, so

$$\text{Per}(-T_d, F) = -\text{Per}(T_d, F) := \{-\alpha : \alpha \in \text{Per}(T_d, F)\}.$$

If d is odd, using equation (1) it is not hard to see that

$$(-T_d)^2 = (T_d)^2.$$

Thus if $\alpha \in \text{Per}(-T_d, F)$, there exists $m \geq 1$ such that $(-T_d)^m(\alpha) = \alpha$ and so

$$\alpha = (-T_d)^{2m}(\alpha) = (T_d)^{2m}(\alpha)$$

proving that α is also periodic for T_d . The same argument applies starting from T_d so $\text{Per}(-T_d, F) = \text{Per}(T_d, F)$. ■

The next lemma shows that the periodic points of T_d are obtained from the periodic points of g .

LEMMA 4.4. *Let $d \geq 1$ and F a field. Let $\alpha \in F$ and $\beta \in \overline{F}$ be such that $\pi(\beta) = \alpha$. Then $\alpha \in \text{Per}(T_d, F)$ if and only if $\beta \in \text{Per}(g, \overline{F})$.*

Proof. If $\alpha \in \text{Per}(T_d, F)$, there exists $m \geq 1$ such that $(T_d)^m(\alpha) = \alpha$. Then by diagram (5),

$$\pi(\beta) = \alpha = (T_d)^m(\alpha) = (T_d)^m(\pi(\beta)) = \pi(g^m(\beta)).$$

By Lemma 4.1 this means that $g^m(\beta) \in \{\beta, \beta^{-1}\}$. In the first case β is periodic for g . If $g^m(\beta) = \beta^{-1}$ then

$$g^{2m}(\beta) = g^m(\beta^{-1}) = (g^m(\beta))^{-1} = \beta.$$

Conversely, if $\beta \in \text{Per}(g, \overline{F})$, there exists $m \geq 1$ such that $g^m(\beta) = \beta$. Again by diagram (5),

$$\alpha = \pi(\beta) = \pi(g^m(\beta)) = (T_d)^m(\pi(\beta)) = (T_d)^m(\alpha). \quad \blacksquare$$

From now on, assume that F is a finite field with $\text{char}(F) \neq 2$ and let F_2 be the extension of degree 2 of F . By Lemma 4.1 $\pi(F_2^\times)$ contains $F^\times$ and it is 2-to-1 except at ± 1 . Consider the subgroup

$$H_2 := \{\beta \in F_2^\times : \beta^{|F|+1} = 1\}$$

and $U_2 := H_2 \setminus \{\pm 1\}$.

LEMMA 4.5. *Let F be a finite field with $\text{char}(F) \neq 2$. Then the set*

$$\{\beta \in F_2^\times : \pi(\beta) \in F\} = F^\times \cup U_2.$$

Moreover, the union is disjoint.

Proof. If $\beta \in F^\times$ clearly $\pi(\beta) \in F$. Now $\beta \in F_2^\times \setminus F^\times$ if and only if the action of the Frobenius map is non-trivial. As the Frobenius map must send β to the other solution of $\pi(x) = \pi(\beta)$, by Lemma 4.1 this implies that

$$(6) \quad \beta \in F_2^\times \setminus F^\times \iff \beta^{|F|} = \beta^{-1} \text{ and } \beta \neq \pm 1.$$

Similarly, we have $\pi(\beta) \in F$ if and only if the action of the Frobenius map is trivial, namely,

$$(7) \quad \pi(\beta) \in F \iff \beta + \beta^{-1} = \beta^{|F|} + \beta^{-|F|}.$$

Combining equations (6) and (7) we obtain

$$\beta \in F_2^\times \setminus F^\times \text{ and } \pi(\beta) \in F \iff \beta^{|F|+1} = 1 \text{ and } \beta \neq \pm 1.$$

To prove that the union is disjoint observe that if $\beta \in F^\times \cap U_2$ then $\beta^{|F|} = \beta$ and $\beta^{|F|+1} = 1$, which implies that $\beta^2 = 1$ and consequently $\beta = \pm 1$. However, by definition $\pm 1 \notin U_2$. ■

Combining Lemmas 4.4 and 4.5, we can give a description of the periodic points of T_d in F :

LEMMA 4.6. *Let $d \geq 2$, F a finite field with $\text{char}(F) \neq 2$, F_2 the extension of degree 2 of F and let $|\cdot|$ denote the order of an element in the group $F_2^\times$. Then*

$$\text{Per}(T_d, F) = \bigcup_{\gamma \in \{-1, 1\}} \{\pi(\beta) \in F : \gcd(|\beta|, d) = 1 \text{ and } |\beta| \mid (|F| + \gamma)\}$$

and the sets involved in the union intersect at 1 if d is even or at ± 1 if d is odd.

Proof. We have the following chain of equivalences:

$$\begin{aligned} \beta \in \text{Per}(g, F_2^\times) &\iff g^m(\beta) = \beta^{d^m} = \beta \text{ for some } m \geq 1, \\ &\iff |\beta| \mid (d^m - 1) \text{ for some } m \geq 1, \\ &\iff d^m \equiv 1 \pmod{|\beta|} \text{ for some } m \geq 1, \\ &\iff \gcd(|\beta|, d) = 1. \end{aligned}$$

Among the elements in the set $\text{Per}(g, F_2^\times)$, we are only interested in those where $\pi(\beta) \in F$. By Lemma 4.5, we have two disjoint cases. If $\beta \in F^\times$, then $|\beta|$ must divide $|F| - 1$. If $\beta \in U_2$ then $|\beta|$ must divide $|F| + 1$. ■

Our next goal in this section is to calculate the number of periodic points of $\pm T_d$ in F .

DEFINITION 4.7. Given $a, b \geq 1$, define

$$r(a, b) := \text{largest divisor of } a \text{ coprime to } b.$$

LEMMA 4.8. *Let G be a cyclic finite group of order n . Let $m \geq 1$ be such that $m \mid n$ and let $b \geq 1$. Define*

$$H := \{g \in G : g^m = 1\}.$$

Then

$$\#\{h \in H : \gcd(|h|, b) = 1\} = r(m, b).$$

Proof. As G is cyclic, H is a cyclic subgroup of G . Moreover, since $m \mid n$, we have $|H| = m$. Finally,

$$\begin{aligned} \#\{h \in H : \gcd(|h|, b) = 1\} &= \sum_{u \mid r(m, b)} \#\{h \in H : |h| = u\} \\ &= \sum_{u \mid r(m, b)} \varphi(u) = r(m, b), \end{aligned}$$

which completes the proof. ■

So the number of periodic points for $\pm T_d$ in a finite field F is the following:

LEMMA 4.9. *Let $d \geq 2$ and F a finite field with $\text{char}(F) \neq 2$. Then*

$$\#\text{Per}(\pm T_d, F) = \frac{r(|F| - 1, d) + r(|F| + 1, d)}{2}.$$

Proof. By Lemma 4.3 we only need to worry about the periodic points of T_d . As before, let F_2 be the extension of F of degree 2.

Consider

$$H_1 = \{\beta \in F_2^\times : \beta^{|F|-1} = 1\}.$$

As $F_2^\times$ is a cyclic subgroup, by Lemma 4.8 we have

$$\#\{\beta \in F_2^\times : \gcd(|\beta|, d) = 1 \text{ and } |\beta| \mid (|F| - 1)\} = r(|F| - 1, d).$$

The same argument works for H_2 so

$$\#\{\beta \in F_2^\times : \gcd(|\beta|, d) = 1 \text{ and } |\beta| \mid (|F| + 1)\} = r(|F| + 1, d).$$

To calculate $\#\text{Per}(T_d, F)$, observe that $\alpha = \pi(\beta) = \pi(\beta^{-1})$, so every element with $\beta \neq \pm 1$ is counted twice. Then $\beta = 1$ gives $\gcd(|\beta|, d) = 1$, while $\beta = -1$ gives $\gcd(|\beta|, d) = 1$ if and only if d is odd. If we define $\chi(d) = 1$ if d is even and $\chi(d) = 2$ if d is odd, then $\chi(d)$ indicates if we need to isolate 1 or 2 elements depending on the parity of d , to avoid an overcount. Therefore,

$$\#\text{Per}(T_d, F) = \frac{r(|F| - 1, d) - \chi(d)}{2} + \frac{r(|F| + 1, d) - \chi(d)}{2} + \chi(d). \quad \blacksquare$$

REMARK 4.10. If K is a number field and $d \geq 2$, then by Lemma 4.9 we obtain

$$\text{Per}_{\inf}(\pm T_d, K) = \frac{1}{2} \liminf_{N(\mathfrak{p}) \rightarrow +\infty} \frac{r(N(\mathfrak{p}) - 1, d) + r(N(\mathfrak{p}) + 1, d)}{N(\mathfrak{p})}.$$

5. Polynomials linearly conjugate over $\mathbb{C}$ to $\pm T_d$. In this section we prove point (4) in Theorem 1:

LEMMA 5.1. *Let K be a number field and $f, g \in K[x]$ be linearly conjugate over K . Then*

$$\text{Per}_{\inf}(f, K) = \text{Per}_{\inf}(g, K).$$

In particular, if f is linearly conjugate over K to $\pm T_d$, then

$$\text{Per}_{\inf}(f, K) = \text{Per}_{\inf}(T_d, K).$$

Proof. Let L be a linear conjugation over K between f and g . Then, if $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ of good reduction for f , g and L , then L induces a bijection between $\text{Per}(f_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}})$ and $\text{Per}(g_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}})$. As $\text{Per}_{\inf}(-T_d, K) = (-1)^{d+1} \text{Per}_{\inf}(T_d, K)$ by Lemma 4.3, the second part follows. ■

Let f be a polynomial with coefficients in a number field K and degree d . First of all, observe that we may assume that the $(d-1)$ th coefficient of f is zero. Indeed, conjugate f by a map of the form $L(x) = x + b$. If $f(x) = \sum_{i=0}^d b_i x^i$, then

$$L^{-1} \circ f \circ L(x) = b_d x^d + (d \cdot b \cdot b_d + b_{d-1}) x^{d-1} + \dots$$

So, we can take

$$b = -\frac{b_{d-1}}{d \cdot b_d}.$$

Suppose f is linearly conjugate over $\mathbb{C}$ to $\pm T_d$ by a linear map L . If $d = 2$ and L is not a polynomial, then L must exchange 0 and ∞ as those are the totally ramified critical points of $\pm T_2$. Thus $L(x) = a/x$ and

$$L^{-1} \circ (\pm T_2) \circ L(x) = \pm \frac{ax^2}{a^2 - 2x^2},$$

which is not a polynomial. If $d \geq 3$, then by Proposition 4.2, $\pm T_d$ is only totally ramified at ∞ and therefore L is a polynomial by Lemma 2.2. Write $L(x) = ax + b$ and $\pm T_d = \sum_{i=0}^d a_i x^i$. Recall that by Proposition 4.2 we have $a_{d-1} = 0$. Then

$$f(x) = L^{-1} \circ (\pm T_d) \circ L(x) = a^{d-1} \cdot a_d \cdot x^d + a^{d-2} \cdot a_d \cdot d \cdot b \cdot x^{d-1} + \dots,$$

which implies that $b = 0$ as we are assuming that the $(d-1)$ th coefficient of f is zero. Then

$$f(x) = L^{-1} \circ (\pm T_d) \circ L(x) = \sum_{i=0}^d a^{i-1} \cdot a_i \cdot x^i.$$

If d is even, then $a \cdot a_2 \in K$ and as $a_2 \neq 0$ by Proposition 4.2, we have $a \in K$. By Remark 4.10 and Lemma 5.1 we conclude that

$$(8) \quad \text{Per}_{\inf}(f, K) = \frac{1}{2} \liminf_{N(\mathfrak{p}) \rightarrow +\infty} \frac{r(N(\mathfrak{p}) - 1, d) + r(N(\mathfrak{p}) + 1, d)}{N(\mathfrak{p})}.$$

If d is odd, then $a_2 = 0$ but $a_3 \neq 0$, so we conclude that $a^2 \cdot a_3 \in K$ and thus $a^2 \in K$. If $a \in K$ then $\text{Per}_{\inf}(f, K)$ is calculated as in equation (8), so let us assume that $a \notin K$.

PROPOSITION 5.2. *Let K be a number field, $d \geq 2$ an odd number and $f = L^{-1} \circ (\pm T_d) \circ L \in K[x]$ with $L(x) = ax$ and $a \notin K$. Then*

$$\text{Per}_{\inf}(f, K) = \frac{1}{2} \liminf_{N(\mathfrak{p}) \rightarrow +\infty} \frac{r(N(\mathfrak{p}) - 1, d) + r(N(\mathfrak{p}) + 1, d)}{N(\mathfrak{p})}.$$

Proof. Set $K' = K(a)$. By hypothesis K'/K is an extension of degree 2. Let $\mathfrak{p}$ be a prime ideal such that $\text{char}(\mathbb{F}_{\mathfrak{p}}) \neq 2$ and $\mathfrak{p}$ does not ramify at K' . Notice that we are excluding only finitely many prime ideals. Let $\mathfrak{p}'$ be a prime ideal in $\mathcal{O}_{K'}$ such that $\mathfrak{p}' | \mathfrak{p}$.

As f and $\pm T_d$ are linearly conjugate over K' , we see that L induces a bijection

$$(9) \quad \text{Per}(f_{\mathfrak{p}'}, \mathbb{F}_{\mathfrak{p}'}) \rightarrow \text{Per}((\pm T_d)_{\mathfrak{p}'}, \mathbb{F}_{\mathfrak{p}'}), \quad \alpha \mapsto a\alpha.$$

Moreover, since d is odd, by Lemma 4.3 we have

$$\text{Per}((\pm T_d)_{\mathfrak{p}'}, \mathbb{F}_{\mathfrak{p}'}) = \text{Per}((T_d)_{\mathfrak{p}'}, \mathbb{F}_{\mathfrak{p}'}).$$

We have two cases for $\mathfrak{p}$. If $\mathfrak{p}$ is split, then $\mathbb{F}_{\mathfrak{p}'} = \mathbb{F}_{\mathfrak{p}}$ and therefore by Lemma 4.9,

$$(10) \quad \# \text{Per}(f_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}}) = \frac{r(N(\mathfrak{p}) - 1, d) + r(N(\mathfrak{p}) + 1, d)}{2}.$$

If $\mathfrak{p}$ is inert, then $\mathbb{F}_{\mathfrak{p}'}/\mathbb{F}_{\mathfrak{p}}$ is an extension of degree 2 and consequently the Frobenius map sends a to $-a$ in $\mathbb{F}_{\mathfrak{p}'}$.

Recall the trace is (in this case) the surjective additive group homomorphism

$$\text{tr} : \mathbb{F}_{\mathfrak{p}'} \rightarrow \mathbb{F}_{\mathfrak{p}}, \quad y \mapsto y + \text{Frob}_{\mathfrak{p}}(y).$$

As it is surjective we have

$$\# \ker(\text{tr}) = N(\mathfrak{p}).$$

We claim that

$$a\mathbb{F}_{\mathfrak{p}} = \ker(\text{tr}).$$

Indeed, if $y \in a\mathbb{F}_{\mathfrak{p}}$ then $y = ax$ for some $x \in \mathbb{F}_{\mathfrak{p}}$. Therefore

$$\text{tr}(y) = ax - ax^{N(\mathfrak{p})} = 0$$

as $x \in \mathbb{F}_{\mathfrak{p}}$. This proves that $a\mathbb{F}_{\mathfrak{p}} \subseteq \ker(\text{tr})$, but since they have the same cardinality, it follows that $a\mathbb{F}_{\mathfrak{p}} = \ker(\text{tr})$.

Let F_2 be the extension of degree 2 of $\mathbb{F}_{\mathfrak{p}'}$ and recall the map $\pi : \mathbb{P}^1(F_2) \rightarrow \mathbb{P}^1(F_2)$. Then, if $\beta \in F_2^\times$,

$$\text{tr}(\pi(\beta)) = \beta + \beta^{-1} + \beta^{N(\mathfrak{p})} + \beta^{-N(\mathfrak{p})} = \frac{(\beta^{N(\mathfrak{p})-1} + 1)(\beta^{N(\mathfrak{p})+1} + 1)}{\beta^{N(\mathfrak{p})}}.$$

We are interested in calculating $\# \text{Per}(f_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}})$. Using the bijection in equation (9), we obtain

$$\# \text{Per}(f_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}}) = \#(a\mathbb{F}_{\mathfrak{p}} \cap \text{Per}((T_d)_{\mathfrak{p}'}, \mathbb{F}_{\mathfrak{p}'})).$$

Using Lemma 4.6, we reduce the previous problem to calculating the number of elements of

$$V_{\gamma} := \{\pi(\beta) \in \mathbb{F}_{\mathfrak{p}'} : \text{tr}(\pi(\beta)) = 0, \gcd(|\beta|, d) = 1 \text{ and } |\beta| \mid (N(\mathfrak{p})^2 + \gamma)\}$$

for $\gamma \in \{-1, 1\}$.

Start with $\gamma = 1$. We claim that

$$\{\beta \in F_2^{\times} : \text{tr}(\pi(\beta)) = 0 \text{ and } |\beta| \mid (N(\mathfrak{p})^2 + 1)\} = \emptyset,$$

which in particular implies that $V_1 = \emptyset$. Indeed, if $\text{tr}(\pi(\beta)) = 0$ then $\beta^{N(\mathfrak{p}) \pm 1} = -1$ for either $+$ or $-$ in the exponent. Therefore

$$|\beta| \mid 2(N(\mathfrak{p}) \pm 1).$$

Notice that as $N(\mathfrak{p})$ is odd, the previous formula implies that

$$|\beta| \mid (N(\mathfrak{p})^2 - 1).$$

On the other hand, if $|\beta| \mid (N(\mathfrak{p})^2 + 1)$, subtracting we conclude that $|\beta| \mid 2$ and therefore $\beta = \pm 1$. However, $\text{tr}(\pi(\pm 1)) \neq 0$.

If $\gamma = -1$ consider

$$H_{-1} := \{\beta \in F_2^{\times} : \text{tr}(\pi(\beta)) = 0 \text{ and } |\beta| \mid (N(\mathfrak{p})^2 - 1)\}.$$

By the calculation done before if $\text{tr}(\pi(\beta)) = 0$ then $|\beta| \mid (N(\mathfrak{p})^2 - 1)$, so

$$H_{-1} = \{\beta \in F_2^{\times} : \text{tr}(\pi(\beta)) = 0\}.$$

Let

$$G_c := \{\beta \in F_2^{\times} : \beta^c = 1\}.$$

Then

$$H_{-1} = \bigcup_{\gamma \in \{-1, 1\}} (G_{2(N(\mathfrak{p})+\gamma)} \setminus G_{N(\mathfrak{p})+\gamma})$$

as $\text{tr}(\pi(\beta)) = 0$ if and only if $\beta^{N(\mathfrak{p})+\gamma} = -1$ for either $\gamma = 1$ or $\gamma = -1$.

Moreover,

$$\beta \in \bigcap_{\gamma \in \{-1, 1\}} (G_{2(N(\mathfrak{p})+\gamma)} \setminus G_{N(\mathfrak{p})+\gamma})$$

if and only if $|\beta| = 4$.

Notice that as $\pm 1 \notin H_{-1}$, if $\pi(\beta) \in V_{-1}$ then $\pi(\beta)$ has two different preimages in H_{-1} . Using this observation and Lemma 4.8 we obtain

$$\#V_{-1} = \frac{1}{2} \left(\sum_{\gamma \in \{-1, 1\}} (r(2(N(\mathfrak{p}) + \gamma), d) - r(N(\mathfrak{p}) + \gamma, d)) \right) - \frac{\#\{\beta \in F_2^\times : |\beta| = 4\}}{2}.$$

As d is odd then $r(2(N(\mathfrak{p}) + \gamma), d) = 2r(N(\mathfrak{p}) + \gamma, d)$ and therefore

$$\#V_{-1} = \frac{1}{2} \left(\sum_{\gamma \in \{-1, 1\}} r(N(\mathfrak{p}) + \gamma, d) \right) - \frac{\#\{\beta \in F_2^\times : |\beta| = 4\}}{2}.$$

As V_1 was empty, then $\# \text{Per}(f_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}}) = \#V_{-1}$ allowing us to conclude

$$(11) \quad \# \text{Per}(f_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}}) = \frac{1}{2} \left(\sum_{\gamma \in \{-1, 1\}} r(N(\mathfrak{p}) + \gamma, d) \right) - \frac{\#\{\beta \in F_2^\times : |\beta| = 4\}}{2}.$$

Dividing equation (10) and equation (11) by $N(\mathfrak{p})$ and taking limit, we obtain

$$\text{Per}_{\inf}(f, K) = \frac{1}{2} \liminf_{N(\mathfrak{p}) \rightarrow +\infty} \frac{r(N(\mathfrak{p}) - 1, d) + r(N(\mathfrak{p}) + 1, d)}{N(\mathfrak{p})}$$

as desired. ■

6. Analysis of $\text{Per}_{\inf}(T_d, K)$. In this last section, we prove the points from (5) to (10) in Theorem 1, completing the classification.

Fix a number field K and recall m_K is the greatest positive number such that K contains an m_K th primitive root of unity. By Remark 4.10 and Proposition 5.2, if f is linearly conjugate to $\pm T_d$ over $\mathbb{C}$ then

$$\text{Per}_{\inf}(f, K) = \frac{1}{2} \liminf_{N(\mathfrak{p}) \rightarrow +\infty} \frac{r(N(\mathfrak{p}) - 1, d) + r(N(\mathfrak{p}) + 1, d)}{N(\mathfrak{p})},$$

so we just need to analyze the possible values of this limit in the different cases considered in Theorem 1. For this task, we will use Proposition 2.5 many times.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Since we are taking a limit, we may assume the norm of $\mathfrak{p}$ is coprime m_K . Notice that in particular $N(\mathfrak{p})$ is coprime to 2 as $2 \mid m_K$ since $-1 \in \mathbb{Q}$. Under this assumption, the polynomial

$$x^{m_K} - 1$$

is separable in $\mathbb{F}_{\mathfrak{p}}$ and therefore all the m_K th roots of unity are different in $\mathbb{F}_{\mathfrak{p}}$. As $\xi_{m_K} \in \mathcal{O}_K$ this implies that

$$(12) \quad m_K \mid (N(\mathfrak{p}) - 1).$$

6.1. d has at least two prime factors and $\text{rad}(d) \nmid \text{rad}(m_K)$. Let p_1 and p_2 be two different prime factors of d such that $p_2 \nmid m_K$. Let $m_1 \geq v_{p_1}(m_K)$ and $m_2 \geq 1$. Consider the system of congruences

$$\begin{cases} x \equiv 1 \pmod{m_K}, \\ x \equiv 1 \pmod{p_1^{m_1}}, \\ x \equiv -1 \pmod{p_2^{m_2}}. \end{cases}$$

As $p_2 \nmid m_K$, the system has a solution. By Proposition 2.5 there are infinitely many primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that

$$p_1^{m_1} \mid (N(\mathfrak{p}) - 1) \quad \text{and} \quad p_2^{m_2} \mid (N(\mathfrak{p}) + 1).$$

As p_1 and p_2 are factors of d , we have

$$r(N(\mathfrak{p}) - 1, d) \leq \frac{N(\mathfrak{p}) - 1}{p_1^{m_1}} \quad \text{and} \quad r(N(\mathfrak{p}) + 1, d) \leq \frac{N(\mathfrak{p}) + 1}{p_2^{m_2}}.$$

Therefore

$$\text{Per}_{\inf}(f, K) \leq \frac{1}{2} \left(\frac{1}{p_1^{m_1}} + \frac{1}{p_2^{m_2}} \right).$$

As m_1 and m_2 are arbitrary, it follows that

$$\text{Per}_{\inf}(f, K) = 0.$$

6.2. d is odd and $\text{rad}(d) \mid \text{rad}(m_K)$. We claim that

$$r(N(\mathfrak{p}) + 1, d) = N(\mathfrak{p}) + 1.$$

Indeed, suppose that $r(N(\mathfrak{p}) + 1, d) < N(\mathfrak{p}) + 1$. Then there exists p prime such that

$$p \mid (N(\mathfrak{p}) + 1) \quad \text{and} \quad p \mid d.$$

As d is odd, so is p .

On the other hand, if p divides d , then p also divides m_K by hypothesis, so by equation (12),

$$p \mid (N(\mathfrak{p}) - 1).$$

Therefore $p \mid 2$, leading to a contradiction since p is odd.

Let p be any prime divisor of d . For any $m \geq 1$, consider the system of congruences

$$\begin{cases} x \equiv 1 \pmod{m_K}, \\ x \equiv 1 \pmod{p^m}. \end{cases}$$

As the system has a solution, by Proposition 2.5 there are infinitely many primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that

$$p^m \mid (N(\mathfrak{p}) - 1)$$

and consequently

$$r(N(\mathfrak{p}) - 1, d) \leq \frac{N(\mathfrak{p}) - 1}{p^m}$$

for any $m \geq 1$. In conclusion,

$$\text{Per}_{\inf}(f, K) = 1/2.$$

6.3. d is even, $\text{rad}(d) \mid \text{rad}(m_K)$ and $v_2(m_K) \geq 2$. We claim that

$$r(N(\mathfrak{p}) + 1, d) = \frac{N(\mathfrak{p}) + 1}{2}.$$

If not there exists p prime such that

$$p \mid \frac{N(\mathfrak{p}) + 1}{2} \quad \text{and} \quad p \mid d.$$

Since p divides d , as in the previous case we obtain

$$p \mid (N(\mathfrak{p}) - 1)$$

and so $p = 2$. But now if $p = 2$ then

$$4 \mid (N(\mathfrak{p}) + 1)$$

and since $4 \mid m_K$ by hypothesis, it follows that

$$4 \mid (N(\mathfrak{p}) - 1),$$

leading to a contradiction.

Now taking p a prime divisor of d , considering the same system of congruences as in the previous case and arguing the same way we obtain

$$\text{Per}_{\inf}(f, K) = 1/4.$$

6.4. d is even, has at least two prime factors, $\text{rad}(d) \mid \text{rad}(m_K)$ and $v_2(m_K) = 1$. Let p be an odd prime dividing d . Let $m_1 \geq v_p(m_K)$ and $m_2 \geq v_2(m_K)$. Consider the system of congruences

$$\begin{cases} x \equiv 1 \pmod{m_K}, \\ x \equiv 1 \pmod{p^{m_1}}, \\ x \equiv -1 \pmod{2^{m_2}}. \end{cases}$$

As $\gcd(m_K, 2^{m_2}) = 2$, the system has a solution and so by Proposition 2.5 there are infinitely many primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that

$$p^{m_1} \mid (N(\mathfrak{p}) - 1) \quad \text{and} \quad 2^{m_2} \mid (N(\mathfrak{p}) + 1).$$

Proceeding as in the first case we obtain

$$\text{Per}_{\inf}(f, K) = 0.$$

6.5. d is an odd prime power. Let p be the prime dividing d . Observe that either $r(N(\mathfrak{p}) - 1, d) = N(\mathfrak{p}) - 1$ or $r(N(\mathfrak{p}) + 1, d) = N(\mathfrak{p}) + 1$. Indeed, if not then

$$p \mid (N(\mathfrak{p}) - 1) \quad \text{and} \quad p \mid (N(\mathfrak{p}) + 1),$$

which contradicts that p is odd. Then, arguing as in the second case we obtain

$$\text{Per}_{\inf}(T_d, K) = 1/2.$$

6.6. d is an even prime power. As before, we have either

$$r(N(\mathfrak{p}) - 1, d) = \frac{N(\mathfrak{p}) - 1}{2} \quad \text{or} \quad r(N(\mathfrak{p}) + 1, d) = \frac{N(\mathfrak{p}) + 1}{2}.$$

If not, then 4 divides $N(\mathfrak{p}) - 1$ and $N(\mathfrak{p}) + 1$, which leads to a contradiction.

Finally, taking $m \geq v_2(m_K)$ and considering the system of congruences

$$\begin{cases} x \equiv 1 \pmod{m_K}, \\ x \equiv 1 \pmod{2^m}, \end{cases}$$

we conclude that

$$\text{Per}_{\inf}(T_d, K) = 1/4.$$

Acknowledgements. The author would like to thank Rostislav Grigorchuk and Thomas Tucker for their support and feedback, as well as Jorge Fariña-Asategui for useful suggestions.

Funding. The author is supported by Grigorchuk's Simons Foundation Grant MP-TSM-00002045 and the Department of Mathematics of Texas A&M University.

References

- [1] O. Adams, *Semiconjugacy and self-similar subgroups of pfIMGs*, arXiv:2508.12122v1 (2025).
- [2] O. Adams and T. Hyde, *Profinite iterated monodromy groups of unicritical polynomials*, arXiv:2504.13028v1 (2025).
- [3] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. Silverman and T. Tucker, *Current trends and open problems in arithmetic dynamics*, Bull. Amer. Math. Soc. (N.S.) 56 (2019), 611–685.
- [4] A. Bridy, J. Doyle, D. Ghioca, L.-C. Hsia and T. Tucker, *Finite index theorems for iterated Galois groups of unicritical polynomials*, Trans. Amer. Math. Soc. 374 (2021), 733–752.
- [5] J. Fariña-Asategui, *Arboreal Galois representations of rational functions: fixed-point proportion and the extension problem*, arXiv:2601.19414v1 (2026).
- [6] J. Fariña-Asategui and S. Radi, *Fixed-point proportion of geometric iterated Galois groups*, arXiv:2601.16173v1 (2026).
- [7] P. Flajolet and A. Odlyzko, *Random mapping statistics*, in: Advances in Cryptology–EUROCRYPT'89, Lecture Notes in Computer Sci. 434, Springer, Berlin, 1990, 329–354.

- [8] M. Fried, *On a conjecture of Schur*, Michigan Math. J. 17 (1970), 41–55.
- [9] C. Gratton, K. Nguyen and T. Tucker, *ABC implies primitive prime divisors in arithmetic dynamics*, Bull. London Math. Soc. 45 (2013), 1194–1208.
- [10] R. Guralnick, P. Müller and J. Saxl, *The rational function analogue of a question of Schur and exceptionality of permutation representations*, Mem. Amer. Math. Soc. 162 (2003), no. 773, viii+79 pp.
- [11] R. Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. London Math. Soc. 78 (2008), 523–544.
- [12] R. Jones, *Fixed-point-free elements of iterated monodromy groups*, Trans. Amer. Math. Soc. 367 (2015), 2023–2049.
- [13] R. Jones, *Galois representations from pre-image trees: an arboreal survey*, Publ. Math. Besançon Algèbre Théor. Nombres 2013, 107–136.
- [14] R. Jones and M. Manes, *Galois theory of quadratic rational functions*, Comment. Math. Helv. 89 (2014), 173–213.
- [15] J. Juul, P. Kurlberg, K. Madhu and T. Tucker, *Wreath products and proportions of periodic points*, Int. Math. Res. Notices 2016, 3944–3969.
- [16] M. Manes and B. Thompson, *Periodic points in towers of finite fields for polynomials associated to algebraic groups*, Rocky Mountain J. Math. 49 (2019), 171–197.
- [17] R. Odoni, *On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \dots w_n$* , J. London Math. Soc. 32 (1985), 1–11.
- [18] R. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. 51 (1985), 385–414.
- [19] S. Radi, *Branch iterated Galois groups with positive fixed-point proportion and positive Hausdorff dimension*, Int. Math. Res. Notices 2026, no. 12, art. rnag119, 30 pp.
- [20] I. Schur, *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*, S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl. 1923, 123–134.

Santiago Radi
 Texas A&M University
 College Station, TX 77843, USA
 E-mail: santiradi@tamu.edu