2022

Periodic Points of Polynomials over Finite Fields

Derek Garton
Portland State University, gartondw@pdx.edu

Citation Details

Published as: Garton, D. (2022). Periodic points of polynomials over finite fields. Transactions of the American Mathematical Society.

PERIODIC POINTS OF POLYNOMIALS OVER FINITE FIELDS

DEREK GARTON

Abstract. Fix an odd prime p. If r is a positive integer and f a polynomial with coefficients in $\mathbb{F}_{p^r}$, let $P_{p,r}(f)$ be the proportion of $\mathbb{P}^1(\mathbb{F}_{p^r})$ that is periodic with respect to f. We show that as r increases, the expected value of $P_{p,r}(f)$, as f ranges over quadratic polynomials, is less than $22/(\log\log p^r)$. This result follows from a uniformity theorem on specializations of dynamical systems of rational functions over residually finite Dedekind domains. The specialization theorem generalizes previous work by Juul et al. that holds for rings of integers of number fields. Moreover, under stronger hypotheses, we effectivize this uniformity theorem by using the machinery of heights over general global fields; this version of the theorem generalizes previous work of Juul on polynomial dynamical systems over rings of integers of number fields. From these theorems we derive effective bounds on image sizes and periodic point proportions of families of rational functions over finite fields.

1. Introduction

A (*discrete*) *dynamical system* is a pair (S, f) consisting of a set S and a function $f\colon S \to S$. For notational convenience, for any positive integer n, we let $f^n = \overbrace{f \circ \cdots \circ f}^{n \text{ times}}$; furthermore, we set $f^0 = \mathrm{id}_S$. For any $\alpha \in S$, if there is some positive integer n such that $f^n(\alpha) = \alpha$, we say that α is *periodic* (for f). Let $\mathrm{Per}(S, f) = \{\alpha \in S \mid \alpha \text{ is periodic for } f\}$. One of the results of this paper is the following application of Theorem 1.3.

Corollary 1.1. *Suppose p is an odd prime and r is a positive integer. If $r > 6\log p$, then*

$$\frac{1}{|\{f \in \mathbb{F}_{p^r}[X] \mid \deg f = 2\}|} \cdot \sum_{\substack{f \in \mathbb{F}_{p^r}[X] \\ \deg f = 2}} \frac{|\mathrm{Per}(\mathbb{P}^1(\mathbb{F}_{p^r}), f)|}{|\mathbb{P}^1(\mathbb{F}_{p^r})|} < \frac{22}{\log\log p^r}.$$

This corollary addresses Question 18.2 in *Current trends and open problems in arithmetic dynamics*, "To what extent do polynomial maps behave like random set maps?" [BIJ+19]. Indeed, the corresponding statistic for random set maps on $\mathbb{P}^1(\mathbb{F}_{p^r})$ is: if p is prime, then

$$\frac{1}{|\mathrm{Aut}_{\mathsf{Set}}(\mathbb{P}^1(\mathbb{F}_{p^r}))|} \cdot \sum_{f \in \mathrm{Aut}_{\mathsf{Set}}(\mathbb{P}^1(\mathbb{F}_{p^r}))} \frac{|\mathrm{Per}(\mathbb{P}^1(\mathbb{F}_{p^r}), f)|}{|\mathbb{P}^1(\mathbb{F}_{p^r})|} = O\left(p^{-\frac{r}{2}}\right)$$

(see [FO90, Theorem 2]). That is, Corollary 1.1 shows that for any odd prime p: as $r \to \infty$, the expected value of $|\mathrm{Per}(\mathbb{P}^1(\mathbb{F}_{p^r}), f)| \cdot |\mathbb{P}^1(\mathbb{F}_{p^r})|^{-1}$ approaches 0, whether f ranges over the $p^{3r} - p^{2r}$ quadratic polynomials in $\mathbb{F}_{p^r}[X]$ or the $(p^r+1)^{p^r+1}$ set maps in $\mathrm{Aut}_{\mathsf{Set}}(\mathbb{P}^1(\mathbb{F}_{p^r}))$.

For numerical data and conjectures on the statistics of the periodic points of dynamical systems of polynomials of a fixed degree over finite fields (and other statistics), see [KLM+16]. In [FG14], the authors bound from below the number of periodic points and number of cycles

Date: January 4, 2022.

2020 *Mathematics Subject Classification.* Primary 37P05; Secondary 37P25, 37P35, 11T06, 13B05.

Key words and phrases. Arithmetic Dynamics, Periodic Points, Finite Fields, Galois Theory.

of these dynamical systems, if the degree of the polynomials grows with the size of the finite field of coefficients; moreover, this bound is consistent with the statistics of random maps. For fixed-degree polynomials, the authors of [BGTW18] prove that a "noncorrelation" heuristic implies that the statistics of the numbers of cycles in these dynamical systems match those of random set maps, providing a heuristic justification for Question 18.2 of [BIJ+19], mentioned above.

We now mention a different approach to studying the randomness of dynamical systems associated to polynomials over finite fields. Suppose that R is a commutative ring and $f \in R[X]$. For any $\mathfrak{p} \in \operatorname{Spec}(R)$, write $[R]_{\mathfrak{p}}$ for $\operatorname{Frac}(R/\mathfrak{p})$ and $[f]_{\mathfrak{p}}$ for the image of f under the R-algebra morphism

$$R[X] \twoheadrightarrow (R/\mathfrak{p})[X] \hookrightarrow [R]_{\mathfrak{p}}[X].$$

With this notation, we see that $\operatorname{Spec}(R)$ parameterizes a family of dynamical systems: indeed, to $\mathfrak{p} \in \operatorname{Spec}(R)$ we associate the dynamical system $(\mathbb{P}^1([R]_{\mathfrak{p}}), [f]_{\mathfrak{p}})$. Of course, if R is residually finite, then (for nonzero primes) this family consists of polynomials acting on a finite set, so we may once again ask: how random are its statistics? As an example of the utility of this approach, we recall that Pollard's famous "rho" method of factorization [Pol75] relies on an aspect of the purported randomness of the family of dynamical systems associated to $R = \mathbb{Z}$ and $f = X^2 + 1$. For recent work on this approach to studying randomness, see [JKMT16, BG17, BG20, Juu21]. To ease notation, for any commutative ring R, we write $\mathcal{P}_R$ for the nonzero prime ideals of R; moreover, if R is residually finite, then for any $\mathfrak{p} \in \mathcal{P}_R$, we write $\mathrm{N}(\mathfrak{p})$ for $|[R]_{\mathfrak{p}}|$. We mention in particular a consequence of [JKMT16, Proposition 6.4]: if R is the ring of integers of a number field and if there exists $\alpha \in R \smallsetminus \{-2\}$ with $f = X^2 + \alpha$, then

$$\lim_{\substack{\mathfrak{p} \in \mathcal{P}_R \\ \mathrm{N}(\mathfrak{p}) \to \infty}} \frac{\left|\operatorname{Per}\left(\mathbb{P}^1([R]_{\mathfrak{p}}), [f]_{\mathfrak{p}}\right)\right|}{\left|\mathbb{P}^1([R]_{\mathfrak{p}})\right|} = 0.$$

Moreover, an effective version of this result follows from [Juu21, Theorem 1.5 (b)]. In this paper, we generalize this work of [JKMT16] and [Juu21] to address the case where R is a residually finite Dedekind domain. One benefit of this generalization is it allows us to bring to bear the techniques of [JKMT16, Juu21] on the study of the statistics of the dynamical systems associated to the set of polynomials of fixed degree over a fixed finite field. For example, if we set $R = \mathbb{F}_p[s]$ and $f = X^2 + s \in R[X]$, then for any $r \in \mathbb{Z}_{\geq 1}$, the family

$$\left\{\left(\mathbb{P}^1([R]_{\mathfrak{p}}), [f]_{\mathfrak{p}}\right) \mid \mathfrak{p} \in \mathcal{P}_R \text{ and } \mathrm{N}(\mathfrak{p}) = p^r\right\}$$

parameterizes nearly all (Galois orbits of) dynamical systems in the family

$$\left\{\left(\mathbb{P}^1(\mathbb{F}_{p^r}), X^2 + \alpha\right) \mid \alpha \in \mathbb{F}_{p^r}\right\}.$$

We now describe the methods, results, and organization of this paper. In Section 2, we address the issue of preservation of Galois actions under specialization. Specifically, if we let

- R be a Noetherian integral domain,
- A be a finitely-generated R-algebra that is an integrally closed Noetherian integral domain, and
- L be a finite Galois extension of $\operatorname{Frac}(A)$,

and we write K for $\operatorname{Frac}(A)$ and B for the integral closure of A in L, then Theorem 2.3 provides criteria than ensure the existence of a nonempty open subset $\mathcal{P}_{A,L}$ of $\operatorname{Spec}(R)$ such that for all $\mathfrak{p} \in \mathcal{P}_{A,L}$, the ideals $\mathfrak{p}A$ and $\mathfrak{p}B$ are prime, the extension $[B]_{\mathfrak{p}B}/[A]_{\mathfrak{p}A}$ is Galois,

and the $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}([B]_{\mathfrak{p}B}/[A]_{\mathfrak{p}A})$. Theorem 2.3 is a generalization of Proposition 4.1 of [JKMT16], which holds when $\mathrm{char}(R) = 0$. As one might expect, the proof of Theorem 2.3 must address issues of separability.

As our general results hold for rational functions in addition to polynomials, we pause to introduce some notation. If k is a field and $\phi \in k(X)$, by the *splitting field of ϕ over k* we mean the splitting field of any polynomial $f \in k[X]$ with the property that there exists $g \in k[X]$ such that $\phi = f/g$ and $\gcd(f, g) = 1$. If R is an integral domain with $k = \mathrm{Frac}(R)$, then for any rational function $\phi \in k(X)$, prime $\mathfrak{p} \in \mathrm{Spec}(R)$, and polynomials $f, g \in R[X]$ with $\phi = f/g$ and $[g]_{\mathfrak{p}} \neq 0$, we write $[\phi]_{\mathfrak{p}}$ for $[f]_{\mathfrak{p}}/[g]_{\mathfrak{p}}$. In Section 3, we apply Theorem 2.3 to the study of the periodic points of dynamical systems of rational functions with coefficients in (the fraction field of) a residually finite integral domain. To do this, we recall an Effective Image Size Theorem [Juu21, Theorem 2.1], which states that if a rational function over a finite field satisfies certain Galois constraints, then there are effective bounds on the image size of (iterates of) that function. Using this result along with Theorem 2.3, we prove in Theorem 3.4 that for any

- residually finite Dedekind domain R with field of fractions k,
- rational function $\phi \in k(X)$, and
- positive integer n,

certain Galois hypotheses on the splitting field of $\phi^n(X) - t$ over $k(t)$ imply that for all but finitely many $\mathfrak{p} \in \mathcal{P}_R$, the quantity $\left|[\phi]_{\mathfrak{p}}^n([R]_{\mathfrak{p}})\right|$ is effectively bounded in terms of $\mathrm{N}(\mathfrak{p})$. This result is a generalization of [JKMT16, Proposition 5.3], which holds in characteristic zero. As a consequence, we obtain Corollary 3.5, which states that if these hypotheses are satisfied for all $n \in \mathbb{Z}_{\geq 1}$, then

$$\lim_{\substack{\mathfrak{p} \in \mathcal{P}_R \\ \mathrm{N}(\mathfrak{p}) \to \infty}} \frac{\left|\mathrm{Per}\left(\mathbb{P}^1([R]_{\mathfrak{p}}), [\phi]_{\mathfrak{p}}\right)\right|}{\left|\mathbb{P}^1([R]_{\mathfrak{p}})\right|} = 0;$$

this is a generalization of [JKMT16, Corollary 5.4], which holds when R is the ring of integers of a number field.

In Section 5, we prove Theorem 5.6, an effective version of Theorem 3.4 and Corollary 3.5, under the hypothesis that the critical points of $\phi \in k(X)$ lie in $\mathbb{P}^1(k)$ and do not collide under iterations of ϕ. This hypothesis ensures that for all $n \in \mathbb{Z}_{\geq 1}$, the Galois groups of splitting fields of $\phi^n(X) - t$ over $k(t)$ are certain wreath products (see the Wreath Product Theorem, due to [Odo85, JKMT16], in Section 5). Our work in Section 4—specifically, Proposition 4.7—guarantees that the critical points of specializations (at primes of large enough norm) of ϕ retain this property; to prove it, we introduce the machinery of heights on global fields. A version of these results has appeared in [Juu21, Section 7], in the special case where ϕ is a polynomial and k is a number field.

Finally, in Section 6, we apply known statistics of wreath products due to [Juu21] to deduce our main results. Indeed, Theorem 6.2 provides an effective bound on periodic points of rational functions over global fields in the case where the Galois group of the function field extension generated by generic preimages is of the form studied in [Juu21]. Turning to more specific applications, we also prove the following theorem.

Theorem 1.2. *Suppose that q is a prime power, that $r, m \in \mathbb{Z}_{\geq 1}$, that $d \in \mathbb{Z}_{\geq 2}$, and that $\alpha \in \mathbb{F}_{q^r}$. If $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$, $q \equiv 1 \pmod{d}$, and $r > \max\left(\left\{2md^2, 4d\log_q(d!)\right\}\right)$, then*

$$\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right), X^d + \alpha^m\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|} < \frac{4\log d}{(d-1)\left(\log\left(\log q^r - \log 2\right) - \log\max\left(\left\{\log q^{2m}, \log\left(d!\right)^4\right\}\right)\right)} + \frac{7d}{q^{\frac{r}{2}}}.$$

Moreover, in Theorem 6.3 we prove a version of Corollary 1.1 that holds for unicritical polynomials of arbitrarily large degree. Section 6 also contains a proof of the following more precise version of Corollary 1.1.

Theorem 1.3. *Suppose q is a power of an odd prime and $r \in \mathbb{Z}_{\geq 1}$. If $r > 8$, then*

$$\frac{1}{\left|\left\{f \in \mathbb{F}_{q^r}[X] \mid \deg f = 2\right\}\right|} \cdot \sum_{\substack{f \in \mathbb{F}_{q^r}[X] \\ \deg f = 2}} \frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right), f\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|}$$
$$< \frac{q^r+1}{q^r-1}\left(\frac{\log 16}{\log\left(\log q^r - \log 2\right) - \log\max\left(\left\{\log q^2, \log 16\right\}\right)} + \frac{16}{q^{\frac{r}{2}}}\right).$$

2. Stability of Galois groups under specialization

We start this section with some notation. For any commutative ring R, prime $\mathfrak{p} \in \mathcal{P}_R$, and element $\alpha \in R$, we write $[\alpha]_{\mathfrak{p}}$ for the image of $\alpha + \mathfrak{p}$ under the canonical injection $R/\mathfrak{p} \hookrightarrow [R]_{\mathfrak{p}}$. Next, suppose that A is an integrally closed domain and L is a Galois extension of $\mathrm{Frac}\, A$, and write B for the integral closure of A in L. If $\mathfrak{q}$ a prime ideal of A and $\mathfrak{Q}$ a prime ideal of B lying over $\mathfrak{q}$, let

$$D_{L,A}\left(\mathfrak{Q}|\mathfrak{q}\right)$$

be the decomposition group of $\mathfrak{Q}$ over $\mathfrak{q}$ and

$$\rho_{\mathfrak{Q}|\mathfrak{q}} \colon D_{L,A}\left(\mathfrak{Q}|\mathfrak{q}\right) \to \mathrm{Aut}_{[A]_{\mathfrak{q}}}\left([B]_{\mathfrak{Q}}/[A]_{\mathfrak{q}}\right)$$

be the associated surjective homomorphism of groups. We are now in the position to recall a fact from algebraic number theory. The first, second, and fourth bullets below are immediate, and for the third bullet see, for example, [Lan02, Proposition VII.2.8].

Fact 2.1. *Suppose that A is an integrally closed domain with field of fractions K, that L/K is a finite Galois extension, and that $\mathfrak{q}$ is a prime ideal of A. Write B for the integral closure of A in L and $\mathfrak{J}$ for $\mathfrak{q}B$. Let $f \in A[X]$ be the minimal polynomial of an integral primitive element of the extension L/K. If $\mathfrak{J}$ is prime and $[f]_{\mathfrak{q}}$ is separable, then*

- *$[B]_{\mathfrak{J}}/[A]_{\mathfrak{q}}$ is a Galois extension,*
- *$D_{L,A}(\mathfrak{J}|\mathfrak{q}) = \mathrm{Gal}\left(L/K\right)$,*
- *$\rho_{\mathfrak{J}|\mathfrak{q}}$ is an isomorphism of groups, and*
- *for any $\alpha \in B$ and $\sigma \in \mathrm{Gal}\left(L/K\right)$,*

$$\rho_{\mathfrak{J}|\mathfrak{q}}\left(\sigma\right)\left([\alpha]_{\mathfrak{J}}\right) = [\sigma(\alpha)]_{\mathfrak{J}}.$$

We now recall two definitions from topology, which we will use only in the following remark and in the proof of Theorem 2.3. If $\mathbf{X}$ is a Noetherian topological space, we say a subset of $\mathbf{X}$ is *locally closed* if it an intersection of an open set and a closed set. We say that a subset of $\mathbf{X}$ is *constructible* if it is a finite union of locally closed sets. The following remark is immediate; we will use it in the proof of Theorem 2.3.

Remark 2.2. Suppose R is a Noetherian integral domain and E is a constructible subset of $\operatorname{Spec}(R)$. If $\{0\} \in E$, then E contains a nonempty open subset of $\operatorname{Spec}(R)$.

Theorem 2.3. *Suppose that R is a Noetherian integral domain and that A is a finitely-generated R-algebra that is an integrally closed integral domain. Write k, K for the fraction fields of R, A, respectively, and suppose that L/K is a finite Galois extension. Let B be the integral closure of A in L and let $f \in A[X]$ be the minimal polynomial of an integral primitive element of the extension L/K. If*

- *k is algebraically closed in L and*
- *K is separable over k,*

then

$$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p}B \text{ is prime and } [R]_{\mathfrak{p}} \text{ is algebraically closed in } [B]_{\mathfrak{p}B}\}$$

and

$$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid [f]_{\mathfrak{p}A} \text{ is irreducible and separable}\}$$

both contain nonempty open subsets of $\operatorname{Spec}(R)$.

Proof. We begin by showing the first statement. Let $\mathbf{X} = \operatorname{Spec}(B)$ and for all $\mathfrak{p} \in \operatorname{Spec}(R)$, let $\mathbf{X}_{\mathfrak{p}} = \operatorname{Spec}(B \otimes_R [R]_{\mathfrak{p}})$. Then let

$$E_1 = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathbf{X}_{\mathfrak{p}} \text{ is a geometrically integral } [R]_{\mathfrak{p}}\text{-scheme}\}.$$

Since A is an is integrally closed Noetherian domain and f is separable, we know that B is a finitely-generated A-algebra (see, for example, Proposition I.6 of [Lan94]), hence a finitely-generated R-algebra. Thus, we apply Theorem 9.7.7 of [Gro66] to conclude that E_1 is a constructible set. Now, for any $\mathfrak{p} \in E_1$,

- $\mathfrak{p}B$ is prime, since $B \otimes_R [R]_{\mathfrak{p}} \simeq B/\mathfrak{p}B$, and
- $[R]_{\mathfrak{p}}$ is algebraically closed in $[B]_{\mathfrak{p}B}$, by Proposition 5.51 of [GW10], for example.

Hence, by Remark 2.2, to show the first statement we need only show that $\mathbf{X}_{\{0\}}$ is geometrically integral.

To see that $\mathbf{X}_{\{0\}}$ is integral, let $S = R \setminus \{0\}$ and note that

$$B \otimes_R k = B \otimes_R \left(S^{-1}R\right) \simeq S^{-1}B$$

is a subring of the field L, so it is in particular an integral domain. Thus, as the function field of $\mathbf{X}_{\{0\}}$ is L, the geometric integrality of $\mathbf{X}_{\{0\}}$ will follow if both the following conditions hold:

- k is algebraically closed in L and
- L is separable over k

(see, for example, Proposition 5.51 of [GW10]). But these conditions follow immediately from our hypotheses.

The proof of the second statement is similar. Let $\mathbf{Y} = \operatorname{Spec}(A[X]/f)$ and for all $\mathfrak{p} \in \operatorname{Spec}(R)$, let $\mathbf{Y}_{\mathfrak{p}} = \operatorname{Spec}((A[X]/f) \otimes_R [R]_{\mathfrak{p}})$. Then let

$$E_2 = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathbf{Y}_{\mathfrak{p}} \text{ is a geometrically integral } [R]_{\mathfrak{p}}\text{-scheme}\}.$$

Since f is the minimal polynomial of an integral element of the extension L/K, we know $A[X]/f$ is a finitely-generated A-algebra, hence a finitely-generated R-algebra. Thus, we apply Theorem 9.9.7 of [Gro66] a second time to conclude that E_2 is a constructible set. Now, for $\mathfrak{p} \in \operatorname{Spec}(R)$, we know

$$(A[X]/f) \otimes_R [R]_{\mathfrak{p}} \simeq (A/\mathfrak{p}A)[X]/[f]_{\mathfrak{p}A},$$

so if $\mathfrak{p} \in E_2$, then $[f]_{\mathfrak{p}A}$ is irreducible and separable. Once again, by Remark 2.2, the second statement will now follow from the geometric integrality of $\mathbf{Y}_{\{0\}}$.

As above, the ring $(A[X]/f) \otimes_R k$ is isomorphic to a subring of B, so it is an integral domain. And the function field of $\mathbf{Y}_{\{0\}}$ is L, so the result follows from our hypotheses and [GW10, Proposition 5.51]. □

3. Image size of specialized rational functions

Before applying Theorem 2.3 to dynamical systems, we recall two facts about the dynamics of rational functions. And before stating these facts, we mention some notation. For any field k, if $\phi \in k(X)$ and $d \in \mathbb{Z}_{\geq 0}$, we will write $\deg \phi = d$ if there exist $f, g \in k[X]$ such that

- $\phi = f/g$,
- $\gcd(f, g) = 1$, and
- $d = \max(\{\deg f, \deg g\})$.

We extend the definition of "separable" by saying that ϕ is *separable over* k if there exist $f, g \in k[X]$ such that $\phi = f/g$ and f is separable over k. If R is an integral domain with $k = \operatorname{Frac}(R)$, then for any $\phi \in k(X)$ and $\mathfrak{p} \in \operatorname{Spec}(R)$, we say that ϕ has *good reduction at* $\mathfrak{p}$ if $\deg [\phi]_{\mathfrak{p}} = \deg \phi$.

Fact 3.1. *Suppose that R is an integral domain with field of fractions k and that $\phi \in k(X)$. If we write*

$$\mathcal{R} = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \phi \text{ has good reduction at } \mathfrak{p}\},$$

then $\mathcal{R}$ contains a nonempty open subset of $\operatorname{Spec}(R)$.

Proof. This fact follows from [Sil07, Section 2.4]: for any $f, g \in R[X]$ such that $\phi = f/g$ and f, g have no common factors in $k[X]$, if we let $\alpha \in R \smallsetminus \{0\}$ be the resultant of f and g, then any $\mathfrak{p} \in \mathcal{P}_R \smallsetminus \mathcal{R}$ must contain α. □

The following fact was noted in the first paragraph of [JKMT16, Section 3].

Fact 3.2. *Suppose that k is a field and $\phi \in k(X)$. If $\phi'(X) \neq 0$, then for all $n \in \mathbb{Z}_{\geq 1}$, the rational function $\phi^n(X) - t$ is separable over $k(t)$.*

With these facts in hand, we prove the following corollary of Theorem 2.3.

Corollary 3.3. *Suppose that R is a Noetherian integral domain with field of fractions k, that $\phi \in k(X)$, and that $n \in \mathbb{Z}_{\geq 1}$. Let*

- *$A = R[t]$,*
- *$K = \operatorname{Frac} A = k(t)$,*
- *L be the splitting field of $\phi^n(X) - t$ over K, and*
- *B be the integral closure of A in L.*

If

(1) *$\phi'(X) \neq 0$ and*
(2) *k is algebraically closed in L,*

then the subset of $\operatorname{Spec}(R)$ *consisting of those primes $\mathfrak{p}$ such that*

- *$\mathfrak{p}B$ is prime,*
- *$[B]_{\mathfrak{p}B}/[A]_{\mathfrak{p}A}$ is Galois,*
- *$\rho_{\mathfrak{p}B|\mathfrak{p}A}$ is an isomorphism, and*
- *$[R]_{\mathfrak{p}}$ is algebraically closed in $[B]_{\mathfrak{p}B}$*

contains a nonempty open subset of $\operatorname{Spec}(R)$.

Proof. Thanks to Fact 3.2, hypothesis (1) implies that rational function $\phi^n(X)-t$ is separable over K, so we see that L is separable (hence Galois) over K. Let $f \in A[X]$ be a minimal polynomial of a primitive integral element of the extension L/K. Since K is separable over k by construction, hypothesis (2) ensures that the hypotheses of Theorem 2.3 are satisfied, so

$$\{\mathfrak{p} \in \mathcal{P}_R \mid \mathfrak{p}B \text{ is prime, } [f]_{\mathfrak{p}A} \text{ is separable, and } [R]_{\mathfrak{p}} \text{ is algebraically closed in } [B]_{\mathfrak{p}B}\}$$

contains a nonempty open subset of $\operatorname{Spec}(R)$. The result now follows from Fact 2.1. □

Before stating the next theorem, we introduce some notation for group actions. If ρ is an action of a finite group G on a set S, we will write

- $\mathrm{F}(\rho) := \{\sigma \in G \mid \text{there exists } s \in S \text{ such that } \rho(\sigma)(s) = s\}$ and
- $\mathrm{f}(\rho) := |\mathrm{F}(\rho)|/|G|$.

To extend this notation to Galois actions, for any field K and separable $\psi \in K(X)$, let L be a splitting field of ψ over K and ρ be the action of $\operatorname{Gal}(L/K)$ on the roots of ψ in L; we will write $\mathrm{f}_K(\psi)$ for $\mathrm{f}(\rho)$, since this quantity depends only on K and ψ.

Versions of the following result have appeared many times, see the proof of Proposition 5.3 in [JKMT16], the proof of Proposition 3.3 in [Juu18], and [Juu21, Theorem 2.1]. The theorem below is a special case of [Juu21, Theorem 2.1] and is based on effective version of the Chebotarev Density Theorem; namely, Proposition 6.4.8 of [FJ08].

Effective Image Size Theorem. *Suppose that q is a prime power, that $\phi \in \mathbb{F}_q(X)$, and that $n \in \mathbb{Z}_{\geq 1}$. Suppose that $\phi'(X) \neq 0$ and let*

- *$d = \deg \phi$,*
- *L be a splitting field of $\phi^n(X) - t$ over $\mathbb{F}_q(t)$, and*
- *$G = \operatorname{Gal}(L/\mathbb{F}_q(t))$.*

If

- *$L/\mathbb{F}_q(t)$ is tamely ramified, and*
- *$\mathbb{F}_q$ is algebraically closed in L,*

then

$$\left| \frac{|\phi^n(\mathbb{P}^1(\mathbb{F}_q))|}{\mathrm{f}_{\mathbb{F}_q(t)}(\phi^n(X)-t)} - |\mathbb{P}^1(\mathbb{F}_q)| \right| < \frac{7nd|G|}{q^{1/2}}.$$

To apply the Effective Image Size Theorem to the the specializations considered in Theorem 2.3, we must ensure that these specializations are finite fields—that is, we turn our considerations to residually finite Dedekind domains. The following theorem generalizes [JKMT16, Proposition 5.3] both in its effectivity and in that it holds in positive characteristic.

Theorem 3.4. *Suppose that R is a residually finite Dedekind domain with field of fractions k, that $\phi \in k(X)$, and that $n \in \mathbb{Z}_{\geq 1}$. Write*

- *A for $R[t]$,*
- *K for $\operatorname{Frac} A = k(t)$, and*
- *d for $\deg \phi$.*

Suppose that

(1) $\phi'(X) \neq 0$,

so that $\phi^n(X)-t$ is separable over K by Fact 3.2, and let

- *L be the splitting field of $\phi^n(X)-t$ over K and*
- *G be the Galois group of L/K.*

If

(2) *k is algebraically closed in L, and*
(3) *either $\operatorname{char}(k)=0$ or $\gcd(\operatorname{char}(k),|G|)=1$,*

then there exists $N_{R,\phi,n}\in\mathbb{Z}_{\geq 1}$ such that for all $\mathfrak{p}\in\mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p})>N_{R,\phi,n}$,

$$\left|\frac{\left|[\phi]_{\mathfrak{p}}^n\left(\mathbb{P}^1([R]_{\mathfrak{p}})\right)\right|}{\left|\mathbb{P}^1([R]_{\mathfrak{p}})\right|}-\mathrm{f}_K\left(\phi^n(X)-t\right)\right|<\frac{7nd|G|}{\mathrm{N}(\mathfrak{p})^{3/2}}\cdot\mathrm{f}_K\left(\phi^n(X)-t\right).$$

Proof. Write B for the integral closure of A in L. Thanks to hypotheses (1) and (2), the hypotheses of Corollary 3.3 satisfied. Thus, since R is a Dedekind domain, Corollary 3.3 and Fact 3.1 imply that there exists $N_0\in\mathbb{Z}_{\geq 1}$ such that for all $\mathfrak{p}\in\mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p})>N_0$,

- $\mathfrak{p}B$ is prime, the extension $[B]_{\mathfrak{p}B}/[A]_{\mathfrak{p}A}$ is Galois, and $\rho_{\mathfrak{p}B|\mathfrak{p}A}$ is an isomorphism,
- $[R]_{\mathfrak{p}}$ is algebraically closed in $[L]_{\mathfrak{p}B}$, and
- ϕ has good reduction at $\mathfrak{p}$.

For any such prime $\mathfrak{p}$, since $[B]_{\mathfrak{p}B}/[A]_{\mathfrak{p}A}$ is the Galois splitting field of the irreducible polynomial $[\phi]_{\mathfrak{p}A}^n(X)-[t]_{\mathfrak{p}A}$, we know $[\phi]_{\mathfrak{p}A}^n(X)-[t]_{\mathfrak{p}A}$ is separable. As $\mathfrak{p}B$ is prime, we know $D_{L,A}(\mathfrak{p}B|\mathfrak{p}A)=\mathrm{Gal}(L/K)$, so the fact that $\rho_{\mathfrak{p}B|\mathfrak{p}A}$ is an isomorphism implies that the action of $\mathrm{Gal}(L/K)$ on the roots of $\phi^n(X)-t$ is isomorphic to the action of $\mathrm{Gal}([B]_{\mathfrak{p}B}/[A]_{\mathfrak{p}A})$ on the roots of $[\phi]_{\mathfrak{p}A}^n(X)-[t]_{\mathfrak{p}A}$. In particular, for all such primes $\mathfrak{p}$,

$$\mathrm{f}_K\left(\phi^n(X)-t\right)=\mathrm{f}_{[A]_{\mathfrak{p}A}}\left([\phi]_{\mathfrak{p}A}^n(X)-[t]_{\mathfrak{p}A}\right).$$

Now, if $\operatorname{char}(k)=0$, the fact that R is a Dedekind domain ensures only finitely many $\mathfrak{p}\in\mathcal{P}_R$ contain any divisor of $|G|$; thus, we may choose an integer $N\geq N_0$ such that if $\mathfrak{p}\in\mathcal{P}_R$ and $\mathrm{N}(\mathfrak{p})>N$, then $\gcd(\operatorname{char}([R]_{\mathfrak{p}}),|G|)=1$. If, on the other hand, we are in the case $\operatorname{char}(k)>0$, we set $N=N_0$. In either case, we know that for all $\mathfrak{p}\in\mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p})>N$, the extension $[B]_{\mathfrak{p}B}/[A]_{\mathfrak{p}A}$ is tamely ramified (by choice of N if $\operatorname{char}(k)=0$ and by hypothesis (3) if $\operatorname{char}(k)>0$). For all such $\mathfrak{p}$, we know $d=\deg([\phi]_{\mathfrak{p}})$ since ϕ has good reduction at $\mathfrak{p}$; the conclusion now follows from the Effective Image Size Theorem. □

Thanks to Theorem 3.4, we obtain Corollary 3.5 below, showing the scarcity of periodic points in specializations of dynamical systems of rational functions over residually finite Dedekind domains. (The characteristic zero case of Corollary 3.5 is Corollary 5.4 of [JKMT16].)

Corollary 3.5. *Suppose that R is a residually finite Dedekind domain with field of fractions k and that $\phi\in k(X)$. Write*

- *A for $R[t]$ and*
- *K for $\operatorname{Frac}A=k(t)$.*

Suppose that

(1) *$\phi'(X)\neq 0$,*

and for every $m\in\mathbb{Z}_{\geq 1}$, let

- *L_m be the splitting field of $\phi^m(X)-t$ over K and*
- *G_m be the Galois group of L_m/K.*

If

(2) *for all* $m \in \mathbb{Z}_{\geq 1}$, *the field* k *is algebraically closed in* L_m,
(3) *either* $\operatorname{char}(k) = 0$ *or for all* $m \in \mathbb{Z}_{\geq 1}$, *the integers* $\operatorname{char}(k)$ *and* $|G_m|$ *are coprime, and*
(4) $\lim_{m\to\infty} \mathrm{f}_K(\phi^m(X) - t) = 0$,

then

$$\lim_{\substack{\mathfrak{p}\in\mathcal{P}_R \\ \mathrm{N}(\mathfrak{p})\to\infty}} \frac{|\mathrm{Per}(\mathbb{P}^1([R]_\mathfrak{p}), [\phi]_\mathfrak{p})|}{|\mathbb{P}^1([R]_\mathfrak{p})|} = 0.$$

Proof. Let $\epsilon > 0$. By hypothesis (4), there exists $n \in \mathbb{Z}_{\geq 0}$ such that

$$\mathrm{f}_K(\phi^n(X) - t) < \epsilon/2.$$

Hypotheses (1), (2), and (3) allow us to apply Theorem 3.4 to find an integer $N_0 \in \mathbb{Z}_{\geq 1}$ with the property that for all $\mathfrak{p} \in \mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p}) > N_0$,

$$\frac{\left|[\phi]_\mathfrak{p}^n(\mathbb{P}^1([R]_\mathfrak{p}))\right|}{|\mathbb{P}^1([R]_\mathfrak{p})|} < \mathrm{f}_K(\phi^n(X) - t) + \frac{7nd|G_n|}{\mathrm{N}(\mathfrak{p})^{3/2}} \cdot \mathrm{f}_K(\phi^n(X) - t).$$

The result follows by setting $N = \max\left(\left\{N_0, \left(\frac{14nd|G_n|}{\epsilon}\right)^{\frac{2}{3}}\right\}\right)$ and noting

$$\mathrm{Per}\left(\mathbb{P}^1([R]_\mathfrak{p}), [\phi]_\mathfrak{p}\right) \subseteq [\phi]_\mathfrak{p}^n\left(\mathbb{P}^1([R]_\mathfrak{p})\right).$$

□

4. Global fields and heights

In Section 5, we make Theorem 2.3 more effective in the special case where the critical points of the specified rational function do not collide. As the proof of Theorem 5.6 relies on the theory of heights, we begin this section by recalling basic facts on global fields, following [AW45].

If k is a field, we will write $\mathcal{M}_k$ for the set of places of k and we say k *satisfies the product formula* if for every $\mathfrak{v} \in \mathcal{M}_k$ there exists an absolute value $|\cdot|_\mathfrak{v} \in \mathfrak{v}$ such that for every $\alpha \in k \smallsetminus \{0\}$,

- $|\{\mathfrak{v} \in \mathcal{M}_k \mid 1 \neq |\alpha|_\mathfrak{v}\}| < \infty$ and
- $\prod_{\mathfrak{v}\in\mathcal{M}_k} |\alpha|_\mathfrak{v} = 1$.

A field k is a *global field* if

- k satisfies the product formula and
- for all $\mathfrak{v} \in \mathcal{M}_k$, either
  - $\mathfrak{v}$ is archimedean or
  - $\mathfrak{v}$ is nonarchimedean and discrete, with a finite residue field.

For any global field k, we will write $\mathcal{P}_k$ for the nonarchimedean places of k. Additionally, if $\mathfrak{v} \in \mathcal{P}_k$, then we will write

- $[k]_\mathfrak{v}$ for the residue field of k at $\mathfrak{v}$,
- $\mathrm{N}(\mathfrak{v})$ for $|[k]_\mathfrak{v}|$, and
- $v_\mathfrak{v} \colon k^\times \to \mathbb{Z}$ for the associated normalized valuation on k.

For such a place $\mathfrak{v}$, we define the function

$$\begin{aligned} \|\cdot\|_{\mathfrak{v}} : k &\to \mathbb{R}_{\geq 0} \\ \alpha &\mapsto \begin{cases} \mathrm{N}(\mathfrak{v})^{-v_{\mathfrak{v}}(\alpha)} & \text{if } \alpha \neq 0 \\ 0 & \text{if } \alpha = 0. \end{cases} \end{aligned}$$

Moreover, if $\alpha \in k$ and $\|\alpha\|_{\mathfrak{v}} \leq 1$, we will write $[\alpha]_{\mathfrak{v}}$ for the image of α in $[k]_{\mathfrak{v}}$; if $[\alpha : \beta] \in \mathbb{P}^1(k)$, we will write

$$[\alpha : \beta]_{\mathfrak{v}} := \begin{cases} [[\alpha/\beta]_{\mathfrak{v}} : 1] & \text{if } \beta \neq 0 \text{ and } \|\alpha/\beta\|_{\mathfrak{v}} \leq 1 \\ [1 : [\beta/\alpha]_{\mathfrak{v}}] & \text{if } \alpha \neq 0 \text{ and } \|\beta/\alpha\|_{\mathfrak{v}} \leq 1. \end{cases}$$

On the other hand, If $\mathfrak{v}$ is an archimedean place of a global field k, then we know by by [Ost16] that the completion of k with respect to $\mathfrak{v}$ is isometric to either $\mathbb{R}$ or $\mathbb{C}$; in the former situation, we say that $\mathfrak{v}$ is a real place and write $\|\cdot\|_{\mathfrak{v}} : k \to \mathbb{R}_{\geq 0}$ for the restriction of the Euclidean absolute value on $\mathbb{R}$ to k and in the latter, we say $\mathfrak{v}$ is a complex place and write $\|\cdot\|_{\mathfrak{v}} : k \to \mathbb{R}_{\geq 0}$ for the restriction of the square of the Euclidean absolute value on $\mathbb{C}$ to k. The number of archimedean places of a global field is finite (see, for example, [AW45, page 473]); if there are r real places and s imaginary places, we define $\mathrm{arch}(k) := r + 2s$.

Fact 4.1 (See Theorem 3 of [AW45])**.** *If k is a global field, then for all $\alpha \in k \smallsetminus \{0\}$,*

$$\prod_{\mathfrak{v} \in \mathcal{M}_k} \|\alpha\|_{\mathfrak{v}} = 1.$$

Turning to heights, for any global field k, we define a height function H_k on k by setting

$$\begin{aligned} H_k : k &\to \mathbb{R}_{\geq 1} \\ \alpha &\mapsto \prod_{\mathfrak{v} \in \mathcal{M}_k} \max\{1, \|\alpha\|_{\mathfrak{v}}\}. \end{aligned}$$

We extend this definition to projective space by defining

$$\begin{aligned} H_k : \mathbb{P}^1(k) &\to \mathbb{R}_{\geq 1} \\ [\alpha : \beta] &\mapsto \begin{cases} H_k(\alpha/\beta) & \text{if } \beta \neq 0 \\ H_k(\beta/\alpha) & \text{if } \alpha \neq 0. \end{cases} \end{aligned}$$

We now introduce the quantities needed to make Theorem 5.6 explicit.

Definition 4.2. Suppose that k is a global field. If $f \in k[X]$, say with $f(X) = \alpha_n X^n + \cdots + \alpha_0$ for some $\alpha_n, \ldots, \alpha_0 \in k$, then for any $\mathfrak{v} \in \mathcal{M}_k$ we will write

$$\|f\|_{\mathfrak{v}} := \max\left(\{\|a_n\|_{\mathfrak{v}}, \ldots, \|a_0\|_{\mathfrak{v}}\}\right).$$

If $g \in k[X]$ as well, we write

$$\|f, g\|_{\mathfrak{v}} := \max\left(\{\|f\|_{\mathfrak{v}}, \|g\|_{\mathfrak{v}}\}\right)$$

and

$$H_k(f, g) := \prod_{\mathfrak{v} \in \mathcal{M}_k} \|f, g\|_{\mathfrak{v}}.$$

If $g \neq 0$, we write

$$b_{k,f,g} := \max\left(\left\{2, (\deg(f/g) + 1)^{\mathrm{arch}(k)} H_k(f, g)\right\}\right).$$

Furthermore, if C is a finite subset of $\mathbb{P}^1(k)$, we write

$$c_{k,f,g,C} := b_{k,f,g} \cdot \max\left(\{H_k(\gamma) \mid \gamma \in C\}\right).$$

Finally, for any $\epsilon \in \mathbb{R}_{>0}$, define the function

$$n_{k,f,g,C,\epsilon} \colon \left\{ \mathfrak{v} \in \mathcal{P}_k \mid \mathrm{N}(\mathfrak{v}) > 2^{\mathrm{arch}(k)} \right\} \to \mathbb{Z}$$

by setting

$$n_{k,f,g,C,\epsilon}(\mathfrak{v}) := \left\lfloor \frac{\log\left(\log\left(\mathrm{N}(\mathfrak{v})\right) - \mathrm{arch}(k)\log 2\right) - \log\max\left(\left\{2\log\left(c_{k,f,g,C}\right), \frac{4\log(d!)}{\epsilon}\right\}\right)}{2\log\left(\deg(f/g)\right)} \right\rfloor.$$

With these quantities in hand, we now recall two facts on heights that we will need to prove Theorem 5.6.

Fact 4.3. *If k is a global field and $\alpha, \beta \in k$, then*

$$H_k(\alpha+\beta) \le 2^{\mathrm{arch}(k)} H_k(\alpha) H_k(\beta).$$

Remark 4.4. See [BG06, Proposition 1.5.15] for a proof of this fact for absolute heights on number fields (which are a power of the heights we have defined). The proof of Fact 4.3 is similar, and easier, in the case $\mathrm{char}(k) > 0$.

Heights and Iterates Theorem. *Suppose that k is a global field and $\phi \in k(X)$, say with $\phi = f/g$ for $f, g \in k[X]$. For all $\gamma \in \mathbb{P}^1(k)$,*

$$H_k(\phi(\gamma)) \le b_{k,f,g} H_k(\gamma)^{\deg(\phi(X))}.$$

Remark 4.5. See [Sil07, Theorem 3.11]. As in Remark 4.4, we mention that Theorem 3.11 of [Sil07] addresses heights on number fields. As above, the case when $\mathrm{char}(k) > 0$ is similar and easier.

The following lemma is a version of the Heights and Iterates Theorem that holds for iterates of finite subsets of projective space.

Lemma 4.6. *Suppose that k is a global field, that $\phi \in k(X)$, and that C is a finite subset of $\mathbb{P}^1(k)$. Suppose further that $f, g \in k[X]$ and $\phi = f/g$. Write $d = \deg\phi$ and $c = c_{k,f,g,C}$. If $d \ge 2$, then for all $\gamma \in C$, $n \in \mathbb{Z}_{\ge 0}$, and $m \in \{0, 1, \ldots, n\}$,*

$$H_k(\phi^m(\gamma)) < c^{d^n}.$$

Proof. Write b for $b_{k,f,g}$. Since $b \ge 2$, the lemma is certainly true if $m = 0$ or $n = 0$, so suppose that m and n are positive. Then for all $\gamma \in C$,

$$\begin{aligned}
H_k\left(\phi^m(\gamma)\right) &\le b^{1+d+\cdots+d^{m-1}} H_k(\gamma)^{d^m} && \text{(apply the Heights and Iterates Theorem } m \text{ times)} \\
&\le b^{1+d+\cdots+d^{n-1}} H_k(\gamma)^{d^n} && \text{(since } b \ge 1\text{)} \\
&< \left(bH_k(\gamma)\right)^{d^n} && \text{(since } d \ge 2 \text{ and } b \ge 2\text{)} \\
&\le c^{d^n} && \text{(by definition of } c_{k,f,g,C}\text{)}.
\end{aligned}$$

□

For any global field k, rational function $\phi \in k(X)$, finite subset $C \subseteq \mathbb{P}^1(k)$, and nonarchimedean place $\mathfrak{v} \in \mathcal{P}_k$, it is quite possible that size of the image of C in $\mathbb{P}^1\left([k]_{\mathfrak{v}}\right)$ is smaller than $|C|$. The following theorem gives a bound ensuring that for nonarchimedean places of large enough norm, this possibility does not arise. It is a generalization of [Juu21, Lemma 7.2], which addresses the case where k is a number field, the rational function ϕ is a polynomial, and $C \subseteq \mathbb{A}^1(k)$.

Proposition 4.7. *Suppose that k is a global field, that $\phi \in k(X)$, that C is a finite subset of $\mathbb{P}^1(k)$, that $\mathfrak{v} \in \mathcal{P}_k$, and that $n \in \mathbb{Z}_{\geq 0}$. Suppose further that $f, g \in k[X]$ and $\phi = f/g$. Write $d = \deg \phi$ and $c = c_{k,f,g,C}$. If*

- $d \geq 2$,
- $\gamma_1, \gamma_2 \in C$,
- $m_1, m_2 \in \{0, \dots, n\}$,
- $\phi^{m_1}(\gamma_1) \neq \phi^{m_2}(\gamma_2)$, *and*
- $[\phi^{m_1}(\gamma_1)]_{\mathfrak{v}} = [\phi^{m_2}(\gamma_2)]_{\mathfrak{v}}$,

then $\mathrm{N}(\mathfrak{v}) < 2^{\operatorname{arch}(k)} c^{2d^n}$.

Proof. We proceed by analyzing two cases.

- Suppose that $[\phi^{m_1}(\gamma_1)]_{\mathfrak{v}} = [\phi^{m_2}(\gamma_2)]_{\mathfrak{v}} = [1:0]_{\mathfrak{v}}$. Since $\phi^{m_1}(\gamma_1) \neq \phi^{m_2}(\gamma_1)$, either $\phi^{m_1}(\gamma_1) \neq [1:0]$ or $\phi^{m_2}(\gamma_2) \neq [1:0]$; without loss of generality, suppose the former is true. Then there exists $\alpha \in k$ such that $\phi^{m_1}(\gamma_1) = [1:\alpha]$ and $\|\alpha\|_{\mathfrak{v}} < 1$. Thus, we use Fact 4.1 to see that

$$\mathrm{N}(\mathfrak{v}) \leq \mathrm{N}(\mathfrak{v})^{v_{\mathfrak{v}}(\alpha)} = \|\alpha\|_{\mathfrak{v}}^{-1} = \prod_{\substack{\mathfrak{w} \in \mathcal{M}_k \\ \mathfrak{w} \neq \mathfrak{v}}} \|\alpha\|_{\mathfrak{w}} \leq H_k(\alpha) \leq 2^{\operatorname{arch}(k)} H_k(\phi^{m_1}(\gamma_1)) H_k(\phi^{m_2}(\gamma_2)).$$

- On the other hand, suppose there are $\alpha, \beta \in k$ such that $\phi^{m_1}(\gamma_1) = [\alpha : 1]$ and $\phi^{m_2}(\gamma_2) = [\beta : 1]$. Then $\|\alpha - \beta\|_{\mathfrak{v}} < 1$, and we use Fact 4.1 and Fact 4.3 to see that

$$\mathrm{N}(\mathfrak{v}) \leq \mathrm{N}(\mathfrak{v})^{v_{\mathfrak{v}}(\alpha-\beta)} = \|\alpha - \beta\|_{\mathfrak{v}}^{-1} \leq H_k(\alpha - \beta) \leq 2^{\operatorname{arch}(k)} H_k(\alpha) H_k(\beta).$$

The result now follows from Lemma 4.6. □

5. Effective image size of specialized rational functions

Before proceeding, we recall some basic facts about wreath products. Suppose that G, H are finite groups and T is a finite set. If $\tau : H \to \mathrm{Aut}_{\mathsf{Set}}(T)$ is an action of H on T, then we use the coordinate permutation action of H on $G^{|T|}$ to construct the group $G^{|T|} \rtimes H$; we denote this group by $G \wr_\tau H$. Now, if S is a another finite set and σ is an action of G on S, then $G \wr_\tau H$ acts on $S \times T$ via

$$((g_i)_{i \in T}, h) : (s, t) \mapsto (\sigma(g_t)(s), \tau(h)(t));$$

we denote this action by $\sigma \wr \tau$.

We may also define an iterated wreath product: if G is a finite group and σ is an action of G on a finite set S,

- write $[G]^1$ for G and $[\sigma]^1$ for σ, and
- for any $n \in \mathbb{Z}_{\geq 2}$, write $[G]^n$ for $[G]^{n-1} \wr_\sigma G$ and $[\sigma]^n$ for $[\sigma]^{n-1} \wr \sigma$.

Thus, for all $n \in \mathbb{Z}_{\geq 1}$, we see that $[\sigma]^n$ is an action of $[G]^n$ on S^n; in this situation, we will write $\mathrm{F}_n(\sigma)$ and $\mathrm{f}_n(\sigma)$ for $\mathrm{F}([\sigma]^n)$ and $\mathrm{f}([\sigma]^n)$, respectively. The following remark follows immediately from the definitions.

Fact 5.1. *If ρ is an action of a finite group G on a finite set S, then for every $n \in \mathbb{Z}_{\geq 1}$,*

$$|[G]^n| = |G|^{1+|S|+\cdots+|S|^{n-1}}.$$

It turns out that the Galois groups of the extensions studied in Theorem 3.4 and Corollary 3.5 are always subgroups of certain wreath products; we record this fact formally in the Wreath Product Theorem, below. The Wreath Product Theorem also includes a criterion ensuring maximality of Galois groups as well as consequences that follow from maximality. Wreath Product Theorem (1) follows from [JKMT16, Lemma 2.5], Wreath Product Theorem (2) follows from Theorem 3.1 and Remark 3.2 of [JKMT16], and Wreath Product Theorem (3b) follows from [JKMT16, Proposition 3.6]. Finally, Wreath Product Theorem (3a) follows from [Odo85, Lemma 4.1]. To state the theorem, we introduce the following terminology. If k is a field and $\phi \in k(X)$, let

$$\mathrm{Crit}\,(k,\phi) = \left\{\gamma \in \mathbb{P}^1(k) \mid \gamma \text{ is a critical point of } \phi\right\}.$$

We will say that the critical points of ϕ are *defined over* k if for every field extension $\widehat{k}$ of k,

$$\mathrm{Crit}\left(\widehat{k},\phi\right) = \mathrm{Crit}\,(k,\phi).$$

If $C \subseteq \mathbb{P}^1(k)$ and $n \in \mathbb{Z}_{\geq 1}$, we say that C is *ϕ-disjoint for n* if for all $\gamma_1, \gamma_2 \in C$ and $m_1, m_2 \in \{0,\dots,n\}$,

$$\text{if } \phi^{m_1}(\gamma_1) = \phi^{m_2}(\gamma_2), \text{ then } \gamma_1 = \gamma_2 \text{ and } m_1 = m_2.$$

If C is ϕ-disjoint for every positive integer, we will simply say that C is *ϕ-disjoint*.

Wreath Product Theorem. *Suppose that k is a field, that $\phi \in k(X)$, and that $n \in \mathbb{Z}_{\geq 2}$. Write $K = k(t)$, and for every $m \in \mathbb{Z}_{\geq 1}$, let L_m be the splitting field of $\phi^m(X) - t$ over K. Suppose that $\phi'(X) \neq 0$, so that for all $m \in \mathbb{Z}_{\geq 1}$, the field extension L_m/K is Galois by Fact 3.2. Let $G = \mathrm{Gal}\,(L_1/K)$ and let ρ be the action of G on the roots of $\phi(X) - t$ in L_1.*

(1) *Then $\mathrm{Gal}\,(L_n/K)$ is isomorphic to a subgroup of $[G]^n$.*
(2) *Suppose that $C \subseteq \mathrm{Crit}\,(k,\phi)$. If*
   - *k is algebraically closed in L_1,*
   - *the critical points of ϕ are defined over k,*
   - *C is ϕ-disjoint for n, and*
   - *$|\mathrm{Crit}\,(k,\phi) \smallsetminus C| \leq 1$,*

   then $\mathrm{Gal}\,(L_n/K) \simeq [G]^n$.
(3) *If $\mathrm{Gal}\,(L_n/K) \simeq [G]^n$, then*
   (a) *$\mathrm{f}_K(\phi^n(X) - t) = \mathrm{f}_n(\rho)$ and*
   (b) *if $m \in \{1,\dots,n-1\}$ and $m \mid n$, then k is algebraically closed in L_m.*

Remark 5.2. A priori, the discussion in [JKMT16, Remark 3.2] implies Wreath Product Theorem (2) only in the case where $C = \mathrm{Crit}\,(k,\phi) \smallsetminus \{\infty\}$. However, the version we state above follows easily from their argument. Indeed, if $\gamma \in \mathbb{P}^1(k)$ and $C = \mathrm{Crit}\,(k,\phi) \smallsetminus \{\gamma\}$, choose any coordinate change $\mu \in \mathrm{PGL}\,(k)$ with $\mu(\infty) = \gamma$, let $\phi^\mu = \mu^{-1} \circ \phi \circ \mu$, then apply their remark to ϕ^μ and $\mathrm{Crit}\,(k,\phi^\mu) \smallsetminus \{\infty\}$, noting that L_n is a splitting field for $(\phi^\mu)^n(X) - \mu^{-1}(t)$ over $k\left(\mu^{-1}(t)\right) = k(t) = K$ and

$$\mathrm{Crit}\,(k,\phi^\mu) \smallsetminus \{\infty\} = \left\{\mu^{-1}(\delta) \mid \delta \in \mathrm{Crit}\,(k,\phi)\right\} \smallsetminus \left\{\mu^{-1}(\gamma)\right\} = \left\{\mu^{-1}(\delta) \mid \delta \in C\right\}.$$

Remark 5.3. Similarly, the statement of [JKMT16, Proposition 3.6] is only the $m = 1$ case of Wreath Product Theorem (3b). To deduce the more general statement, we apply this case to the rational function ϕ^m.

Before proving Theorem 5.6, we pause to introduce terminology connecting our previous work on residually finite Dedekind domains in Section 3 to our current setting of global

fields. Suppose that k is a global field and R is a subring of k. If R is a Dedekind domain with $\mathrm{Frac}(R) = k$, then R is necessarily residually finite, so for every $\mathfrak{p} \in \mathcal{P}_R$, we may write $\mathfrak{v}_\mathfrak{p}$ for the associated (nonarchimedean) place of k. If it is also the case that the function

$$\begin{aligned} \mathcal{P}_R &\to \mathcal{P}_k \\ \mathfrak{p} &\mapsto \mathfrak{v}_\mathfrak{p} \end{aligned}$$

is cofinite, we will say that R is an *Artin-Whaples subring of k*.

Fact 5.4 (See Theorem 3 of [AW45])**.** *If k is a global field, then k has an Artin-Whaples subring.*

Recall that if (S, ϕ) and (S', ϕ') are dynamical systems, we say a function $\sigma : S \to S'$ is an *isomorphism of dynamical systems* if σ is bijective and $\sigma \circ \phi = \phi' \circ \sigma$. Of course, if (S, ϕ) and (S', ϕ') are isomorphic, then $\sigma(\mathrm{Per}(S, \phi)) = \mathrm{Per}(S', \phi')$. The following remark is immediate.

Remark 5.5. Suppose that k is a global field, that $\phi \in k(X)$, and that R is an Artin-Whaples subring of k. For all $\mathfrak{p} \in \mathrm{Spec}(R)$, then dynamical systems $(\mathbb{P}^1([R]_\mathfrak{p}), [\phi]_\mathfrak{p})$ and $\left(\mathbb{P}^1\left([k]_{\mathfrak{v}_\mathfrak{p}}\right), [\phi]_{\mathfrak{v}_\mathfrak{p}}\right)$ are isomorphic via the natural isomorphism of fields $[R]_\mathfrak{p} \to [k]_{\mathfrak{v}_\mathfrak{p}}$.

We may now use the height results of Section 4 to apply Wreath Product Theorem and Corollary 3.3 to deduce an effective version of Corollary 3.5. As Theorem 5.6 holds for rational functions over arbitrary global fields, it is a generalization of [Juu21, Theorem 1.5], which holds for polynomials over number fields.

Theorem 5.6. *Suppose that k is a global field, that $\phi \in k(X)$, that $C \subseteq \mathrm{Crit}(k, \phi)$, and that $\epsilon > 0$. Suppose further that $f, g \in k[X]$ and $\phi = f/g$. Write*

- *d for $\deg \phi$, and*
- *K for $k(t)$.*

Suppose that

(1) *$\phi'(X) \neq 0$,*

and for every $m \in \mathbb{Z}_{\geq 1}$, let

- *L_m be the splitting field of $\phi^m(X) - t$ over K, which is Galois by Fact 3.2, and*
- *G_m be $\mathrm{Gal}(L_m/K)$.*

Finally, write G for G_1 and let ρ be the action of G on the roots of $\phi(X) - t$ in L_1. If

(2) *$\deg \phi \geq 2$,*
(3) *k is algebraically closed in L_1,*
(4) *either $\mathrm{char}(k) = 0$ or $\gcd(\mathrm{char}(k), |G|) = 1$,*
(5) *the critical points of ϕ are defined over k,*
(6) *C is ϕ-disjoint, and*
(7) *$|\mathrm{Crit}(k, \phi) \smallsetminus C| \leq 1$,*

then there exists $N \in \mathbb{Z}_{\geq 1}$ such that for all $\mathfrak{v} \in \mathcal{P}_k$ with $\mathrm{N}(\mathfrak{v}) > N$,

- *$n_{k,f,g,C,\epsilon}(\mathfrak{v}) \geq 1$ and*
- *for all $n \in \{1, \ldots, n_{k,f,g,C,\epsilon}(\mathfrak{v})\}$,*

$$\left| \frac{|[\phi]_\mathfrak{v}^n([k]_\mathfrak{v})|}{|\mathbb{P}^1([k]_\mathfrak{v})|} - \mathrm{f}_n(\rho) \right| < \frac{7d}{\mathrm{N}(\mathfrak{v})^{\frac{3}{2}-\epsilon}}.$$

In particular, for all such $\mathfrak{v}$ *and* n,

$$\frac{|\mathrm{Per}\left(\mathbb{P}^1\left([k]_{\mathfrak{v}}\right),[\phi]_{\mathfrak{v}}\right)|}{|\mathbb{P}^1\left([k]_{\mathfrak{v}}\right)|} < \mathrm{f}_n(\rho) + \frac{7d}{\mathrm{N}(\mathfrak{v})^{\frac{3}{2}-\epsilon}}.$$

Proof. Use Fact 5.4 to choose an Artin-Whaples subring of k, and call it R. Let $A = R[t]$ and for every $m \in \mathbb{Z}_{\geq 1}$, let B_m be the integral closure of A in L_m.

Thanks to hypotheses (1), (3), (5), (6), and (7), we may apply Wreath Product Theorem (2) and (3b) to deduce that for all $m \in \mathbb{Z}_{\geq 0}$,

- $G_m \simeq [G]^m$ and
- k is algebraically closed in L_m.

We may now apply the definition of Artin-Whaples subring, Fact 3.1, and Corollary 3.3 (thanks to hypotheses (1) and (3)) to produce an $N_1 \in \mathbb{Z}_{\geq 1}$ such that

- for all $\mathfrak{v} \in \mathcal{P}_k$ with $\mathrm{N}(\mathfrak{v}) > N_1$, there exists $\mathfrak{p} \in \mathcal{P}_R$ with $\mathfrak{v}_{\mathfrak{p}} = \mathfrak{v}$ and
- for all $\mathfrak{p} \in \mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p}) > N_1$,
  - ϕ has good reduction at $\mathfrak{p}$,
  - $\mathfrak{p}B_1$ is prime,
  - $[B_1]_{\mathfrak{p}B_1}$ is a Galois (in particular separable) extension of $[A]_{\mathfrak{p}A}$,
  - $\rho_{\mathfrak{p}B_1|\mathfrak{p}A}$ is an isomorphism, and
  - $[R]_{\mathfrak{p}}$ is algebraically closed in $[B_1]_{\mathfrak{p}B_1}$.

Now,

- choose any $N_2 \in \mathbb{Z}_{\geq 1}$ such that for all $q \in \mathbb{Z}$ with $q > N_2$,
$$\log\log q < q^{\frac{\epsilon}{2}},$$
- let $N_3 = 2^{\mathrm{arch}(k)} c_{k,f,g,C}^{(2d^2)}$,
- let N_4 be any integer greater than $2^{\mathrm{arch}(k)}(d!)^{4d/\epsilon}$, and
-
  - if $\mathrm{char}(k) > 0$, let $N_5 = 1$ and
  - if $\mathrm{char}(k) = 0$, use the fact that R is a Dedekind domain to choose any positive integer N_5 with the property that for all $\mathfrak{p} \in \mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p}) > N_5$,
$$\gcd\left(\mathrm{char}\left([R]_{\mathfrak{p}}\right), |G|\right) = 1.$$

Finally, set $N = \max\left(\{N_1, N_2, N_3, N_4, N_5\}\right)$.

Choose any $\mathfrak{p} \in \mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p}) > N$. For any $\gamma \in \mathbb{P}^1(k)$, we will write $[\gamma]_{\mathfrak{p}}$ for $[\gamma]_{\mathfrak{v}_{\mathfrak{p}}}$. Similarly, we write $[C]_{\mathfrak{p}}$ for $\{[\gamma]_{\mathfrak{p}} \mid \gamma \in C\}$. Set

$$n_{\mathfrak{p}} = n_{k,f,g,C,\epsilon}\left(\mathfrak{v}_{\mathfrak{p}}\right),$$

which is defined since $\mathrm{N}\left(\mathfrak{v}_{\mathfrak{p}}\right) = \mathrm{N}(\mathfrak{p}) > N_3 > 2^{\mathrm{arch}(k)}$. Note that

- by definition of N_3 and N_4, it follows that $n_{\mathfrak{p}} \geq 1$ and
- by definition of $n_{\mathfrak{p}}$, we know $\mathrm{N}(\mathfrak{p}) = \mathrm{N}\left(\mathfrak{v}_{\mathfrak{p}}\right) \geq 2^{\mathrm{arch}(k)} c_{k,f,g,C}^{\left(2d^{2n_{\mathfrak{p}}}\right)}$.

Thus, by hypotheses (2) and (6), and Proposition 4.7, we see that $[C]_{\mathfrak{p}}$ is $[\phi]_{\mathfrak{p}}$-disjoint for $2n_{\mathfrak{p}}$. Now fix any $n \in \{1, \ldots, n_{\mathfrak{p}}\}$. As the definition of N_1 ensures that $[R]_{\mathfrak{p}}$ is algebraically closed in $[B_1]_{\mathfrak{p}B_1}$ and $\mathrm{Gal}\left([B_1]_{\mathfrak{p}B_1}/[A]_{\mathfrak{p}A}\right) \simeq G$, we use hypotheses (5) and (7) to note that the critical points of $[\phi]_{\mathfrak{p}}$ are defined over $[R]_{\mathfrak{p}}$ and $|\mathrm{Crit}\left([R]_{\mathfrak{p}}, [\phi]_p\right) \smallsetminus [C]_{\mathfrak{p}}| \leq 1$. Thus, we may apply Wreath Product Theorem (2) and (3b) to deduce that

- $\mathrm{Gal}\left([B_{2n}]_{\mathfrak{p}B_{2n}}/[A]_{\mathfrak{p}A}\right) \simeq [G]^{2n}$,
- $[R]_{\mathfrak{p}}$ algebraically closed in $[B_n]_{\mathfrak{p}B_n}$, and

- $\mathrm{Gal}\left([B_n]_{\mathfrak{p}B_n}/[A]_{\mathfrak{p}A}\right) \simeq [G]^n$.

To see that the extension $[B_n]_{\mathfrak{p}B_n}/[A]_{\mathfrak{p}A}$ is tamely ramified, note that

- if $\mathrm{char}\,(k) > 0$, then Fact 5.1 and hypothesis (4) imply that
$$\gcd\left(\mathrm{char}\left([A]_{\mathfrak{p}A}\right), |[G]^n|\right) = \gcd\left(\mathrm{char}\,(k), |G|\right) = 1,$$
and
- if $\mathrm{char}\,(k) = 0$, then Fact 5.1 and the definition of N_5 imply that
$$\gcd\left(\mathrm{char}\left([A]_{\mathfrak{p}A}\right), |[G]^n|\right) = \gcd\left(\mathrm{char}\left([R]_{\mathfrak{p}}\right), |G|\right) = 1.$$

Thus, we apply the Effective Image Size Theorem and Wreath Product Theorem (3a) to deduce that
$$\left|\frac{\left|[\phi]_{\mathfrak{p}}^n\left([R]_{\mathfrak{p}}\right)\right|}{\left|\mathbb{P}^1\left([R]_{\mathfrak{p}}\right)\right|} - \mathrm{f}_n(\rho)\right| < \frac{7nd\,|[G]^n|}{\mathrm{N}(\mathfrak{p})^{3/2}} \cdot \mathrm{f}_n(\rho).$$

Finally, note that
$$\begin{aligned}
|[G]^n| &= |G|^{1+\cdots+d^{(n-1)}} && \text{(by Fact 5.1)}\\
&< |G|^{2d^{(n_{\mathfrak{p}}-1)}} && \text{(since } d \geq 2\text{)}\\
&\leq (d!)^{2d^{(n_{\mathfrak{p}}-1)}} && \text{(by definition of } G\text{)}\\
&< (d!)^{\frac{\epsilon \log \mathrm{N}(\mathfrak{p})}{2\log(d!)}} && \text{(by definition of } n_{\mathfrak{p}}\text{)}\\
&= \mathrm{N}(\mathfrak{p})^{\frac{\epsilon}{2}}.
\end{aligned}$$

Since $\mathrm{f}_n(\rho) \leq 1$ and $n \leq n_{\mathfrak{p}} \leq \log(\log \mathrm{N}(\mathfrak{p}))$, the theorem follows by the definition of N_2 and Remark 5.5.

□

We now take a moment to remark that the construction of the constant N in the proof of Theorem 5.6 is almost entirely explicit, especially in positive characteristic; taking advantage of this explicitness leads to the following porism.

Porism 5.7. *Keep the notation and hypotheses of Theorem 5.6, and suppose further that $N_1 \in \mathbb{Z}_{\geq 1}$ and R is an Artin-Whaples subring of K such that for all $\mathfrak{v} \in \mathcal{P}_k$ with $\mathrm{N}(\mathfrak{v}) > N_1$, there exists $\mathfrak{p} \in \mathcal{P}_R$ such that $\mathfrak{v} = \mathfrak{v}_{\mathfrak{p}}$. Write A for $R[t]$ and B_1 for the integral closure of A in L_1. Suppose that $\mathrm{char}\,(k) > 0$ and for all $\mathfrak{p} \in \mathcal{P}_R$ with $\mathrm{N}(\mathfrak{p}) > N_1$,*

- *ϕ has good reduction at $\mathfrak{p}$,*
- *$\mathfrak{p}B_1$ is prime,*
- *$[B_1]_{\mathfrak{p}B_1}$ is a Galois extension of $[A]_{\mathfrak{p}A}$,*
- *$\rho_{\mathfrak{p}B_1|\mathfrak{p}A}$ is an isomorphism, and*
- *$[R]_{\mathfrak{p}}$ is algebraically closed in $[B_1]_{\mathfrak{p}B_1}$.*

Then for all $\mathfrak{v} \in \mathcal{P}_k$ with $\mathrm{N}(\mathfrak{v}) > \max\left(\left\{N_1, c_{k,f,g,C}^{2d^2}, (d!)^{4d}\right\}\right)$,

- *$n_{k,f,g,C,1}(\mathfrak{v}) \geq 1$ and*
- *for all $n \in \{1, \ldots, n_{k,f,g,C,1}(\mathfrak{v})\}$,*
$$\left|\frac{\left|[\phi]_{\mathfrak{v}}^n\left([k]_{\mathfrak{v}}\right)\right|}{\left|\mathbb{P}^1\left([k]_{\mathfrak{v}}\right)\right|} - \mathrm{f}_n(\rho)\right| < \frac{7d}{\mathrm{N}(\mathfrak{v})^{\frac{1}{2}}}.$$

In particular, for all such $\mathfrak{v}$ *and* n,

$$\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left([k]_{\mathfrak{v}}\right)[\phi]_{\mathfrak{v}}\right)\right|}{\left|\mathbb{P}^1\left([k]_{\mathfrak{v}}\right)\right|} < \mathrm{f}_n(\rho) + \frac{7d}{\mathrm{N}(\mathfrak{v})^{\frac{1}{2}}}.$$

Proof. This follows immediately from the proof of Theorem 5.6: set $\epsilon = 1$ and compute N_2, N_3, N_4, N_5 while keeping in mind that $\mathrm{arch}(k) = 0$. □

6. Applications

We now apply Theorem 5.6 and Porism 5.7 to deduce the results mentioned in the introduction, taking advantage of the fact that for many group actions ρ and integers $n \in \mathbb{Z}_{\geq 1}$, Juul [Juu21] has computed effective bounds for $\mathrm{f}_n(\rho)$.

Definition 6.1. For any $d \in \mathbb{Z}_{\geq 1}$, let $\rho_{S,d}$, $\rho_{A,d}$, $\rho_{D,d}$, $\rho_{C,d}$ denote the usual actions of S_d, A_d, D_d, $\mathbb{Z}/d\mathbb{Z}$ on $\{1, \ldots, d\}$.

The following result records the upper bounds proved in Proposition 4.2, Proposition 4.5, Proposition 4.8, and Proposition 4.10 of [Juu21].

Juul's Wreath Bounds. *Suppose* $d \in \mathbb{Z}_{\geq 2}$. *For all* $n \in \mathbb{Z}_{\geq 1}$,

(1)
$$\mathrm{f}_n(\rho_{S,d}) \leq \frac{2}{n+2},$$

(2) *if* $d \geq 5$, *then*
$$\mathrm{f}_n(\rho_{A,d}) \leq \frac{2}{n+2},$$
and
$$\mathrm{f}_n(\rho_{A,4}) \leq \frac{2}{n+1-\log n},$$

(3) *if* $d \geq 3$, *then*
$$\mathrm{f}_n(\rho_{D,d}) \leq \frac{2}{n+2},$$
and

(4)
$$\mathrm{f}_n(\rho_{C,d}) \leq \frac{2}{(d-1)(n+1)}.$$

The combination of Theorem 5.6 and Juul's Wreath Bounds immediately implies the following theorem.

Theorem 6.2. *Keep the notation and hypotheses of Theorem 5.6, and assume that* ρ *is isomorphic to* $\rho_{S,d}$, $\rho_{A,d}$, $\rho_{D,d}$, *or* $\rho_{S,d}$. *Then there exists* $N \in \mathbb{Z}_{\geq 1}$ *such that for all* $\mathfrak{v} \in \mathcal{P}_k$ *with* $\mathrm{N}(\mathfrak{v}) > N$,

$$\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left([k]_{\mathfrak{v}}\right),[\phi]_{\mathfrak{v}}\right)\right|}{\left|\mathbb{P}^1\left([k]_{\mathfrak{v}}\right)\right|} < \begin{cases} \frac{4\log d}{\log\log \mathrm{N}(\mathfrak{v})} + \frac{7d}{\mathrm{N}(\mathfrak{v})^{\frac{3}{2}-\epsilon}} & \text{if } \rho \ncong \rho_{A,4}, \\ \frac{1+4\log d}{\log\log \mathrm{N}(\mathfrak{v})} + \frac{7d}{\mathrm{N}(\mathfrak{v})^{\frac{3}{2}-\epsilon}} & \text{if } \rho \simeq \rho_{A,4}. \end{cases}$$

Proof. This follows immediately from Theorem 5.6, Juul's Wreath Bounds, and Definition 4.2. □

To apply Porism 5.7, we now turn to the special case where q is an odd prime and $k = \mathbb{F}_q(s)$.

Proof of Theorem 1.2. Set

- $R = \mathbb{F}_q[s]$,
- $k = \mathbb{F}_q(s)$,
- $A = \mathbb{F}_q[s,t]$, and
- $K = \mathbb{F}_q(s,t)$.

For any monic irreducible $\pi \in R$, we write $\mathfrak{p}_\pi$ for the prime ideal πR and $\mathfrak{v}_\pi$ for the associated $\mathfrak{p}_\pi$-adic place of k in $\mathcal{P}_k$. Let $\phi(X) = X^d + s^m$, let $f(X) = \phi(X) - t$, let L_1 be the splitting field of f over K, let B_1 the integral closure of A in L_1, let u be any root of f lying in L_1, let $G = \mathrm{Gal}(L_1/K)$, and let ρ be the action of G on the roots of f in L. Since $q \equiv 1 \pmod{d}$, we know K contains a primitive dth root of unity, so that $L_1 = K(u) = \mathbb{F}_q(s,u)$ and $G \simeq \mathbb{Z}/d\mathbb{Z}$. Moreover, as $\mathbb{F}_q[s,u]$ is integrally closed in $\mathbb{F}_q(s,u)$, we see that $B_1 = \mathbb{F}_q[s,u]$.

Now, for any monic irreducible polynomial $\pi \in R$, we know

$$B_1/\mathfrak{p}_\pi B_1 = \mathbb{F}_q[s,u]/\pi(s)\mathbb{F}_q[s,u] \simeq (R/\mathfrak{p}_\pi)[u],$$

so we see

- $\mathfrak{p}_\pi B_1$ is prime and
- $[R]_{\mathfrak{p}_\pi} = R/\mathfrak{p}_\pi$ is algebraically closed in $[B_1]_{\mathfrak{p}_\pi B_1}$.

Moreover, since $\gcd(q,d) = 1$ by hypothesis, we know $[f]_{\mathfrak{p}_\pi A}$ is separable. And since u is a primitive element for the extension L_1/K, Fact 2.1 implies that $[B_1]_{\mathfrak{p}_\pi B_1}/[A]_{\mathfrak{p}_\pi A}$ is a Galois extension and $\rho_{\mathfrak{p}_\pi B_1|\mathfrak{p}_\pi A}$ is an isomorphism. Thus, we set $N_1 = q$, compute $c_{k,\phi,1,\{0\}} = q^m$, and apply Porism 5.7: for any monic irreducible polynomial $\pi \in R$ with $\deg(\pi) > \max\left(\left\{2md^2, 4d\log_q(d!)\right\}\right)$,

$$\frac{\left|\mathrm{Per}\left(\mathbb{P}^1([R]_{\mathfrak{p}_\pi}), [\phi]_{\mathfrak{p}_\pi}\right)\right|}{\left|\mathbb{P}^1([R]_{\mathfrak{p}_\pi})\right|} = \frac{\left|\mathrm{Per}\left(\mathbb{P}^1([k]_{\mathfrak{v}_\pi})[\phi]_{\mathfrak{v}_\pi}\right)\right|}{\left|\mathbb{P}^1([k]_{\mathfrak{v}_\pi})\right|} < \mathrm{f}_{n_{k,\phi,1,\{0\},1}(\mathfrak{v}_\pi)}(\rho) + \frac{7d}{\mathrm{N}(\mathfrak{v}_\pi)^{\frac{1}{2}}}.$$

Let $\pi_\alpha \in R$ be the minimal polynomial of α over $\mathbb{F}_q$, so that

$$\frac{\left|\mathrm{Per}\left(\mathbb{P}^1(\mathbb{F}_{q^r}), X^d + \alpha^m\right)\right|}{\left|\mathbb{P}^1(\mathbb{F}_{q^r})\right|} = \frac{\left|\mathrm{Per}\left(\mathbb{P}^1(\mathbb{F}_q(\alpha)), X^d + \alpha^m\right)\right|}{\left|\mathbb{P}^1(\mathbb{F}_q(\alpha))\right|} = \frac{\left|\mathrm{Per}\left(\mathbb{P}^1([R]_{\mathfrak{p}_\alpha}), [\phi]_{\mathfrak{p}_\alpha}\right)\right|}{\left|\mathbb{P}^1([R]_{\mathfrak{p}_\alpha})\right|}.$$

Since $\deg(\pi_\alpha) > \max\left(\left\{2md^2, 4d\log_q(d!)\right\}\right)$ by hypothesis, the result follows by Juul's Wreath Bounds and Definition 4.2. □

Of course, for prime powers q and positive integers r, most elements $\alpha \in \mathbb{F}_{q^r}$ have the property that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$; we use this fact to deduce the following theorem on averages of periodic points. For ease of notation, for the rest of the paper, we will write $\mathbb{F}_{q^r}^{\mathrm{prim}}$ for the set $\{\beta \in \mathbb{F}_{q^r} \mid \mathbb{F}_q(\beta) = \mathbb{F}_{q^r}\}$.

Theorem 6.3. *Suppose that q is a prime power, that $r, m \in \mathbb{Z}_{\geq 1}$, and that $d \in \mathbb{Z}_{\geq 2}$. If $q \equiv 1 \pmod{d}$ and $r > \max\left(\left\{2md^2, 4d\log_q(d!)\right\}\right)$, then*

$$\frac{1}{\left|(\mathbb{F}_{q^r})^m\right|} \cdot \sum_{\beta \in (\mathbb{F}_{q^r})^m} \frac{\left|\mathrm{Per}\left(\mathbb{P}^1(\mathbb{F}_{q^r}), X^d + \beta\right)\right|}{\left|\mathbb{P}^1(\mathbb{F}_{q^r})\right|}$$
$$< \frac{4\log(d)\gcd(q^r - 1, m)}{(d-1)\left(\log\left(\log q^r - \log 2\right) - \log\max\left(\left\{\log q^{2m}, \log(d!)^4\right\}\right)\right)} + \frac{(7d+2)\gcd(q^r-1,m)}{q^{\frac{r}{2}}}.$$

In particular,

$$\frac{1}{\left|\left(\mathbb{F}_{q^r}\right)^m\right|}\cdot\sum_{\beta\in\left(\mathbb{F}_{q^r}\right)^m}\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right),X^d+\beta\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|}=O_{q,m,d}\left(\frac{1}{\log\log q^r}\right).$$

Proof. We begin by setting

$$\kappa_{q,d,m}(r)=\frac{4\log d}{(d-1)\left(\log\left(\log q^r-\log 2\right)-\log\max\left(\left\{\log q^{2m},\log\left(d!\right)^4\right\}\right)\right)}+\frac{7d}{q^{\frac{r}{2}}}.$$

Write $\mathcal{P}_q(r)$ for the set of monic irreducible polynomials in $\mathbb{F}_q[s]$ of degree r and for any such polynomial π, write $S_q(\pi)$ for its roots in $\mathbb{F}_{q^r}$. If we let $\phi(X)=X^d+s^m\in\mathbb{F}_q[s][X]$, then we see that

$$\begin{aligned}\sum_{\beta\in\left(\mathbb{F}_{q^r}^{\mathrm{prim}}\right)^m}\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right),X^d+\beta\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|}&\le\sum_{\pi\in\mathcal{P}_q(r)}\sum_{\alpha\in S_q(\pi)}\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right),X^2+\alpha^m\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|}\\&=\sum_{\pi\in\mathcal{P}_q(r)}r\cdot\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_q[s]/\pi\mathbb{F}_q[s]\right),[\phi]_\pi\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|}\\&<r\left|\mathcal{P}_q(r)\right|\kappa_{q,d,m}(r)&&\text{(by Theorem 1.2)}\\&\le q^r\kappa_{q,d,m}(r)&&\text{(since }\left|\mathcal{P}_q(r)\right|\le r^{-1}q^r\text{).}\end{aligned}$$

Next, we recall that there are at most $2q^{r/2}$ elements of $\mathbb{F}_{q^r}$ whose minimal polynomial is of degree less than r. Thus,

$$\sum_{\beta\in\left(\mathbb{F}_{q^r}\smallsetminus\mathbb{F}_{q^r}^{\mathrm{prim}}\right)^m}\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right),X^2+\beta\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|}\le\sum_{\beta\in\left(\mathbb{F}_{q^r}\smallsetminus\mathbb{F}_{q^r}^{\mathrm{prim}}\right)^m}1\le 2q^{\frac{r}{2}},$$

so that

$$\frac{1}{1+\frac{q^r}{\gcd\left(q^r-1,m\right)}}\left(q^r\kappa_{q,d,m}(r)+2q^{\frac{r}{2}}\right)<\gcd\left(q^r-1,m\right)\left(\kappa_{q,d,m}(r)+\frac{2}{q^{\frac{r}{2}}}\right),$$

as desired. □

Finally, we address the specific case of quadratic polynomials.

Proof of Theorem 1.3. Let $Q=\{f\in\mathbb{F}_{q^r}[X]\mid\deg f=2\}$ and $U=\{X^2+\delta\mid\delta\in\mathbb{F}_{q^r}\}$. Since $\mathrm{char}\left(\mathbb{F}_q\right)\neq 2$, for any $\alpha\in\mathbb{F}_{q^r}\smallsetminus\{0\}$ and $\beta\in\mathbb{F}_{q^r}$ we may define the following coordinate change on $\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)$:

$$\mu_{\alpha,\beta}:x\mapsto\alpha x+\frac{\beta}{2}.$$

Next, we set

$$\begin{aligned}\mu:\qquad Q&\to U\\\alpha X^2+\beta X+\gamma&\mapsto X^2-\frac{\beta^2-4\alpha\gamma-2\beta}{4}.\end{aligned}$$

This map is clearly surjective. Moreover, if $\delta\in\mathbb{F}_{q^r}$, then

$$\left|\mu^{-1}\left(X^2+\delta\right)\right|=\begin{cases}q^{2r}-q^r & \text{if } 1-4\delta \text{ is not a square in } \mathbb{F}_{q^r}\\ q^{2r}+q^r & \text{if } 1-4\delta \text{ is a nonzero square in } \mathbb{F}_{q^r}\\ q^{2r} & \text{if } 1-4\delta=0.\end{cases}$$

Note that for any $f \in Q$, if $f(X) = \alpha X^2 + \beta X + \gamma$, then

$$\mu(f) = \mu_{\alpha,\beta} \circ f \circ \mu_{\alpha,\beta}^{-1},$$

so that

$$\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right), f\right)\right| = \left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right), \mu(f)\right)\right|.$$

Setting

$$\kappa_q(r) = \frac{\log 16}{\log\left(\log q^r - \log 2\right) - \log\max\left(\{\log q^2, \log 16\}\right)} + \frac{14}{q^{\frac{r}{2}}},$$

we apply Theorem 1.2 to see that

$$\begin{aligned}
&\frac{1}{|Q|}\sum_{f\in Q}\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right), f\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|} \\
&\qquad < \frac{q^{2r}+q^r}{|Q|}\left(\sum_{\beta\in\mathbb{F}_{q^r}^{\mathrm{prim}}}\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right), X^2+\beta\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|} + \sum_{\beta\in\mathbb{F}_{q^r}\setminus\mathbb{F}_{q^r}^{\mathrm{prim}}}\frac{\left|\mathrm{Per}\left(\mathbb{P}^1\left(\mathbb{F}_{q^r}\right), X^2+\beta\right)\right|}{\left|\mathbb{P}^1\left(\mathbb{F}_{q^r}\right)\right|}\right) \\
&\qquad < \frac{q^{2r}+q^r}{|Q|}\left(q^r\kappa_q(r) + 2q^{\frac{r}{2}}\right) \\
&\qquad = \frac{q^r+1}{q^r-1}\left(\kappa_q(r) + \frac{2}{q^{\frac{r}{2}}}\right).
\end{aligned}$$

□

We now need only apply elementary estimates to Theorem 1.3 to prove Corollary 1.1.

Proof of Corollary 1.1. Suppose that $p \geq 5$ and set $x = \log p^r - \log 2$. Since $r > 6\log p$, we see that

$$x > 5\left(\log p\right)^2 > \frac{\left(\log p^2\right)^2 + \sqrt{\left(\log p^2\right)^4 + 4\left(\log p^2\right)^2\log 2}}{2},$$

so that

$$x^2 - \left(\log p^2\right)^2 x - \left(\log p^2\right)^2\log 2 > 0.$$

This implies that

$$\frac{x}{\log p^2} > \left(x + \log 2\right)^{\frac{1}{2}} > \left(x+\log 2\right)^{\frac{\log 16}{6}}$$

so

$$\frac{6}{\log\left(x+\log 2\right)} > \frac{\log 16}{\log x - \log\log p^2}.$$

Since

$$\frac{5}{\log\log p^r} > \frac{16}{p^{\frac{r}{2}}},$$

the result follows from Theorem 1.3. When $p = 3$, the proof is similar. □

Acknowledgements

I would like to thank Andrew Bridy and Jamie Juul for useful correspondence. I also owe Tom Tucker my gratitude for taking the time to discuss the finer points of [JKMT16]. Finally, I thank the anonymous reviewer for many helpful comments.

References

[AW45] Emil Artin and George Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. **51** (1945), 469–492. MR 13145

[BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR 2216774

[BG17] Andrew Bridy and Derek Garton, *Dynamically distinguishing polynomials*, Res. Math. Sci. **4** (2017), Paper No. 13, 17. MR 3669394

[BG20] ———, *The cycle structure of unicritical polynomials*, Int. Math. Res. Not. IMRN (2020), no. 23, 9120–9147. MR 4182792

[BGTW18] Elisa Bellah, Derek Garton, Erin Tannenbaum, and Noah Walton, *A probabilistic heuristic for counting components of functional graphs of polynomials over finite fields*, Involve **11** (2018), no. 1, 169–179. MR 3681355

[BIJ+19] Robert Benedetto, Patrick Ingram, Rafe Jones, Michelle Manes, Joseph H. Silverman, and Thomas J. Tucker, *Current trends and open problems in arithmetic dynamics*, Bull. Amer. Math. Soc. (N.S.) **56** (2019), no. 4, 611–685. MR 4007163

[FG14] Ryan Flynn and Derek Garton, *Graph components and dynamics over finite fields*, Int. J. Number Theory **10** (2014), no. 3, 779–792. MR 3190008

[FJ08] Michael D. Fried and Moshe Jarden, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden. MR 2445111

[FO90] Philippe Flajolet and Andrew M. Odlyzko, *Random mapping statistics*, Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989), Lecture Notes in Comput. Sci., vol. 434, Springer, Berlin, 1990, pp. 329–354. MR 1083961

[Gro66] Alexander Grothendieck, *Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas, Troisième partie*, Inst. Hautes Études Sci. Publ. Math. **28** (1966), 5–255 (fr). MR 217086

[GW10] Ulrich Görtz and Torsten Wedhorn, *Algebraic Geometry I. Schemes with examples and exercises*, Advanced Lectures in Mathematics, Vieweg + Teubner, Wiesbaden, 2010. MR 2675155

[JKMT16] Jamie Juul, Pär Kurlberg, Kalyani Madhu, and Tom J. Tucker, *Wreath products and proportions of periodic points*, Int. Math. Res. Not. IMRN (2016), no. 13, 3944–3969. MR 3544625

[Juu18] Jamie Juul, *Fixed point proportions for Galois groups of non-geometric iterated extensions*, Acta Arith. **183** (2018), no. 4, 301–315. MR 3820058

[Juu21] ———, *The image size of iterated rational maps over finite fields*, Int. Math. Res. Not. IMRN (2021), no. 5, 3362–3388. MR 4227574

[KLM+16] Sergei V. Konyagin, Florian Luca, Bernard Mans, Luke Mathieson, Min Sha, and Igor E. Shparlinski, *Functional graphs of polynomials over finite fields*, J. Combin. Theory Ser. B **116** (2016), 87–122. MR 3425238

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR 1282723

[Lan02] ———, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

[Odo85] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414. MR 805714

[Ost16] Alexander Ostrowski, *Über einige lösungen der funktionalgleichung $\psi(x) \cdot \psi(x) = \psi(xy)$*, Acta Math. **41** (1916), no. 1, 271–284. MR 1555153

[Pol75] J. M. Pollard, *A Monte Carlo method for factorization*, Nordisk Tidskr. Informationsbehandling (BIT) **15** (1975), no. 3, 331–334. MR 0392798

[Sil07] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007. MR 2316407

Fariborz Maseeh Department of Mathematics and Statistics, Portland State University
Email address: gartondw@pdx.edu