Bridy and Garton *Res Math Sci(2017)4:13*
DOI 10.1186/s40687-017-0103-3

Research in the Mathematical Sciences

RESEARCH Open Access

Dynamically distinguishing polynomials

Andrew Bridy[1*] and Derek Garton[2]

*Correspondence: andrewbridy@math.tamu.edu
[1]Department of Mathematics, Texas A&M University, College Station, TX, USA
Full list of author information is available at the end of the article

Abstract

A polynomial with integer coefficients yields a family of dynamical systems indexed by primes as follows: For any prime p, reduce its coefficients mod p and consider its action on the field $\mathbb{F}_p$. We say a subset of $\mathbb{Z}[x]$ is dynamically distinguishable mod p if the associated mod p dynamical systems are pairwise non-isomorphic. For any $k, M \in \mathbb{Z}_{>1}$, we prove that there are infinitely many sets of integers $\mathcal{M}$ of size M such that $\{x^k + m \mid m \in \mathcal{M}\}$ is dynamically distinguishable mod p for most p (in the sense of natural density). Our proof uses the Galois theory of dynatomic polynomials largely developed by Morton, who proved that the Galois groups of these polynomials are often isomorphic to a particular family of wreath products. In the course of proving our result, we generalize Morton's work and compute statistics of these wreath products.

Keywords: Arithmetic dynamics, Finite fields, Galois theory, Wreath products

Mathematics Subject Classification: Primary 37P05; Secondary 37P25, 11R32, 20B35

1 Introduction

A (*discrete*) *dynamical system* is a pair (S, f) consisting of a set S and a function $f : S \to S$. The *functional graph* of (S, f), which we will denote by $\Gamma(S, f)$, is the directed graph whose set of vertices is S and whose edges are given by the relation $s \to t$ if and only if $f(s) = t$.

Recently there has been interest in the following problem: Given a set S and a family $\mathcal{F}$ of self-maps of S, describe or enumerate the set $M(S, \mathcal{F}) := \{\Gamma(S, f) \mid f \in \mathcal{F}\}/\simeq$, where for two directed graphs Γ and Δ, we write $\Gamma \simeq \Delta$ if they are isomorphic as directed graphs. For example, for any $n \in \mathbb{Z}_{>0}$ and prime power q, Bach and Bridy [2] bound the size of $M(S, \mathcal{F})$, where $S = (\mathbb{F}_q)^n$ and $\mathcal{F}$ is the set of affine-linear transformations from S to itself. Konyagin et al. [14] give non-trivial upper and lower bounds on $M\left(\mathbb{F}_q, \{f \in \mathbb{F}_q[x] \mid \deg(f) = d\}\right)$. Similarly, Ostafe and Sha [22] give bounds on $M\left(\mathbb{F}_q, \mathcal{F}\right)$ for certain families $\mathcal{F}$ of rational functions and "sparse" polynomials. A special case of Theorem 2.8 of [14] proves that

$$\left|M\left(\mathbb{F}_q, \{x^2 + \alpha \mid \alpha \in \mathbb{F}_q\}\right)\right| > q^{\frac{1}{4}+o(1)}$$

as q increases amongst odd prime powers. Moreover, the authors suggest that it is "most likely" that for any rational prime p with $p \notin \{2, 17\}$,

$$\left|M\left(\mathbb{F}_p, \{x^2 + \alpha \mid \alpha \in \mathbb{F}_p\}\right)\right| = p.$$

However, they also state that "proving [this suggestion] may be difficult... as there is no intrinsic reason for this to be true."

Springer Open

In this paper, we study the suggestion of Konyagin et al. [14] "in reverse"; that is, we fix (integer polynomial) maps and then vary the set upon which they act by reducing these polynomials modulo rational primes. Before stating our results, we introduce a bit of notation. Denote the set of rational primes by $\mathcal{P}$. For $f \in \mathbb{Z}[x]$ and $p \in \mathcal{P}$, write

- $\left[f\right]_p$ for the polynomial in $\mathbb{F}_p[x]$ obtained by reducing the coefficients of f mod p and
- $\Gamma_{f,p}$ for $\Gamma\left(\mathbb{F}_p, [f]_p\right)$.

We say that a set $\mathcal{F} \subseteq \mathbb{Z}[x]$ is *dynamically distinguishable* mod p if $\Gamma_{f,p} \not\simeq \Gamma_{g,p}$ for all $f, g \in \mathcal{F}$ with $f \neq g$. Let μ be the natural density on $\mathcal{P}$; that is, for any subset $P \subseteq \mathcal{P}$,

$$\mu(P) := \lim_{X\to\infty} \frac{|\{p \in \mathcal{P} \mid p \leq X \text{ and } p \in P\}|}{|\{p \in \mathcal{P} \mid p \leq X\}|} \quad \text{(if this limit exists).}$$

In Sect. 4, we prove the following theorem.

Theorem 1.1 *Let $k \geq 2$ be an integer. For any $\epsilon > 0$ and any $M \in \mathbb{Z}_{>0}$, there exist infinitely many sets of integers $\mathcal{M}$ of size M such that*

$$\mu\left(\left\{p \in \mathcal{P} \mid \left\{x^k + m \mid m \in \mathcal{M}\right\} \text{ is dynamically distinguishable mod } p\right\}\right) > 1 - \epsilon.$$

Establishing the truth of the suggestion of Konyagin et al. [14] mentioned above would immediately produce the $k = 2$ case of Theorem 1.1 as a weaker corollary.

For any $f, g \in \mathbb{Z}[x]$ and $p \in \mathcal{P}$, the dynamical systems $\left([f]_p, \mathbb{F}_p\right)$ and $\left([g]_p, \mathbb{F}_p\right)$ are isomorphic in the category of dynamical systems on the set $\mathbb{F}_p$ if and only if f and g are dynamically indistinguishable mod p. In more generality, for any set S and set maps $f, g : S \to S$, note that $\Gamma(S, f) \simeq \Gamma(S, g)$ if and only if there exists a bijective set map $\varphi : S \to S$ such that $\varphi \circ f = g \circ \varphi$. In many settings, researchers study subcategories of the category of dynamical systems on the set S by insisting that the maps f, g, and φ belong to the set of morphisms in an appropriate category containing S as an object. For example, suppose K is a field, $S = \mathbb{P}^1(K)$, and $f, g : S \to S$ are rational functions. Then in the subcategory of dynamical systems of $\mathbb{P}^1(K)$, with the self-maps of $\mathbb{P}^1(K)$ restricted to rational maps, the dynamical systems $(\mathbb{P}^1(K), f)$ and $(\mathbb{P}^1(K), g)$ are isomorphic if and only if there exists a Möbius transformation φ such that $\varphi \circ f = g \circ \varphi$. Fixing an integer $d \in \mathbb{Z}_{>1}$, setting $\mathcal{F}$ to be rational functions of degree d, and studying $M\left(\mathbb{P}^1(K), \mathcal{F}\right)$ lead to an interesting moduli space problem, one studied by Silverman [26] using geometric invariant theory. See [3,8,17] for further work on this problem and extensions of it.

To prove Theorem 1.1, we will distinguish dynamical systems by their periodic points. If (S, f) is a dynamical system, let $f^n = (\overbrace{f \circ \cdots \circ f}^{n \text{ times}})$ for any $n \in \mathbb{Z}_{>0}$. If $s \in S$ has the property that there is some $n \in \mathbb{Z}_{>0}$ with $f^n(s) = s$, we say that s is *periodic* or a *periodic point* of (S, f). The smallest such n is the *period* of s. As is standard, we will also refer to points of period one as *fixed points*. Points of period n are precisely those that lie in cycles of length n in the graph $\Gamma(S, f)$. Periodic points are a classical object of study in discrete dynamical systems over $\mathbb{C}$, going back at least to work of Fatou [9,10] and Julia [13] in the early twentieth century. Recently there has been much work on statistics of periodic points in families of dynamical systems over finite fields, partially motivated by an attempt started by Bach [1] to make rigorous the heuristic assumptions in Pollard's "rho method" for integer factorization [23]. For example, in [11], Flynn and Garton prove that for the family of polynomials in $\mathbb{F}_q[x]$ of a fixed degree d, the average number of cycles in their

associated functional graphs is at least $\frac{1}{2}\log q - 4$, as long as $d \geq \sqrt{q}$. More recently, Bellah et al. [4] develop a heuristic that implies that this average is $\frac{1}{2}\log q + O(1)$ for any d. Burnette and Schmutz [6] prove, for this same family of polynomials, that if $d = o\left(\sqrt{q}\right)$ as $d, q \to \infty$, then the average "ultimate period" of the associated functional graphs is at least $\frac{d}{2}(1 + o(1))$.

Our proof of Theorem 1.1 relies on the trivial observation that for any $n \in \mathbb{Z}_{>0}$, if one directed graph has a cycle of length n and another does not, then the graphs are not isomorphic. As an illustration of our approach, consider the following example.

Example 1.2 Let $f = x^2 + 1$ and $g = x^2 + 2$. If $p \in \mathcal{P}$, then $\Gamma_{f,p}$ has a point of period one if and only if there exists $\alpha \in \mathbb{F}_p$ such that

$$0 = [f]_p(\alpha) - \alpha = \alpha^2 + 1 - \alpha.$$

Now, such an α exists if and only if the prime ideal $(p) \subseteq \mathbb{Z}$ splits (or ramifies) in the splitting field of $f(x) - x = x^2 - x + 1$ (over $\mathbb{Q}$). Similarly, $\Gamma_{g,p}$ has a fixed point if and only if (p) splits (or ramifies) in the splitting field of $g(x) - x$. Let K_f and K_g be the splitting fields of $f(x) - x$ and $g(x) - x$, respectively. The Frobenius Density Theorem implies that the natural density of primes that split in K_f and K_g is the proportion of their Galois groups that fix a root of the polynomials whose roots we adjoin (that is, a root of $f(x) - x$ and $g(x) - x$, respectively). Since $\mathrm{Gal}\left(K_f/\mathbb{Q}\right) \simeq \mathrm{Gal}\left(K_g/\mathbb{Q}\right) \simeq \mathbb{Z}/2\mathbb{Z}$, the natural density of primes that split in these fields is $\frac{1}{2}$. Moreover, since K_f and K_g are linearly disjoint, we know that $\mathrm{Gal}\left(K_f K_g/\mathbb{Q}\right) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; thus, when we apply the theorem to the polynomial $(f(x) - x)(g(x) - x)$, we see that the splitting behavior of prime ideals in these two fields is independent.

That is,

$$\begin{aligned}
&\mu(p \in \mathcal{P} \mid \{f, g\} \text{ is dynamically distinguishable mod } p) \\
&\quad = \mu\left(p \in \mathcal{P} \mid \Gamma_{f,p} \not\simeq \Gamma_{g,p}\right) \\
&\quad \geq \mu\left(p \in \mathcal{P} \mid \Gamma_{f,p} \text{ has a fixed point and } \Gamma_{g,p} \text{ does not}\right) \\
&\qquad + \mu\left(p \in \mathcal{P} \mid \Gamma_{f,p} \text{ does not have a fixed point and } \Gamma_{g,p} \text{ does}\right) \\
&\quad = \frac{1}{2}\left(1 - \frac{1}{2}\right) + \left(1 - \frac{1}{2}\right)\frac{1}{2} \\
&\quad = \frac{1}{2}.
\end{aligned}$$

The goal of this paper is to generalize this argument to points of period greater than one. However, to produce polynomials in $\mathbb{Z}[x]$ and apply the Frobenius density theorem, as in Example 1.2, we must prove several theorems to overcome various obstacles. Before describing them, we introduce the notational conventions we will use throughout the rest of the paper. If F is a field and $f \in F[x]$, we will write $\mathrm{Gal}(f/F)$ to denote the Galois group of the splitting field of f over F. Additionally, if $\mathcal{F}$ is a finite subset of $F[x]$, say with splitting fields $\{K_f\}_{f \in \mathcal{F}}$, then we will write $\prod_{f \in \mathcal{F}} K_f$ for the splitting field of $\prod_{f \in \mathcal{F}} f$. (Of course, if we choose an algebraic closure of F, then $\prod_{f \in \mathcal{F}} K_f$ is isomorphic to the compositum of the images of the embeddings of the K_fs in that algebraic closure.) Similarly, for any family of groups $\mathcal{G}$, we will write $\prod_{G \in \mathcal{G}} G$ for their direct product. (If $\mathcal{G} = \{G_1, \ldots, G_n\}$ for a positive integer n, we will write $G_1 \times \cdots \times G_n$ for this group, and if there is some group G

such that $G_i = G$ for all $i \in \{1, \ldots, n\}$, we will write G^n.) The following fact, which we will use often, relates these conventions: If F is a field and $\mathcal{F}$ is finite subset of $F[x]$, say with splitting fields $\{K_f\}_{f\in\mathcal{F}}$, then the members of $\{K_f\}_{f\in\mathcal{F}}$ are pairwise F-linearly disjoint if and only if

$$\mathrm{Gal}\left(\left(\prod_{f\in\mathcal{F}} K_f\right)\Big/F\right) \simeq \prod_{f\in\mathcal{F}} \mathrm{Gal}\,(f/F).$$

Now, if G is a group and S_r is the symmetric group on r letters, we write $G \wr S_r$ to mean the wreath product $G \wr_{\{1,\ldots,r\}} S_r$. That is, $G \wr S_r = G^r \rtimes S_r$, where S_r acts on G^r by permuting coordinates. In particular, we note that $|G \wr S_r| = r!|G|^r$. See [12, Chap. 3A] for background on the wreath product. (In Sect. 3, we introduce and analyze the aspects of the wreath product that we require for this paper.)

With these notations in hand, we can now describe the path to generalizing Example 1.2.

- If K is a field and $f \in K[x]$, then $\alpha \in K$ is a fixed point in (K,f) if and only if α is a root of $f(x) - x$. To generalize the argument of Example 1.2, we review the famous "dynatomic polynomials of f" in Sect. 2, which we will denote by $\Phi_{f,n}$ for any $n \in \mathbb{Z}_{>0}$. These polynomials have the property that for any $n \in \mathbb{Z}_{>0}$, every point of period n in (K,f) is a root of $\Phi_{f,n}$ (in particular, $\Phi_{f,1} = f(x) - x$). When K is the rational function field $\mathbb{Q}(c)$, Morton [19, Theorem D] proved that if $f(x) = x^k + c$ for some $k \in \mathbb{Z}_{>1}$, then for any $n, n' \in \mathbb{Z}_{>0}$ with $n \neq n'$, the splitting fields of $\Phi_{f,n}$ and $\Phi_{f,n'}$ are linearly disjoint. In Theorem 2.3, we generalize Morton's theorem to prove that for any $k, M, N \in \mathbb{Z}_{>1}$, there exist infinitely many sets of integers $\mathcal{M}$ of size M such that for any $f, g \in \{x^k + (c+m) \mid m \in \mathcal{M}\} \subseteq \mathbb{Q}(c)[x]$ and n, n' with $n, n' \leq N$, the splitting fields of $\Phi_{f,n}$ and $\Phi_{g,n'}$ are linearly disjoint. We point out that this includes the case where $n = n'$, which is quite important for our applications.
- In Example 1.2, we set $f(x) = x^2 + 1$ and applied the Frobenius density theorem to $\mathrm{Gal}\left(\Phi_{f,1}/\mathbb{Q}\right) \simeq \mathbb{Z}/2\mathbb{Z}$. In general, the Galois groups of dynatomic polynomials are quite often wreath products of the form $\mathbb{Z}/n\mathbb{Z} \wr S_r$ for $n, r \in \mathbb{Z}_{>0}$. To apply the Frobenius density theorem, we must study the action of these wreath products on the roots of dynatomic polynomials. In Theorem 3.5, we prove that for any $n, r \in \mathbb{Z}_{>0}$, the proportion of the group $\mathbb{Z}/n\mathbb{Z} \wr S_r$ (considered with its natural action on $\mathbb{Z}/n\mathbb{Z} \times \{1, \ldots, r\}$) that acts with a fixed point is approximately $1 - e^{-\frac{1}{n}}$.
- In Example 1.2, with $f(x) = x^2 + 1$, we used the fact that for any $p \in \mathcal{P}$, the polynomial $\left[f(x) - x\right]_p$ has a root if and only if $\left(\mathbb{F}_p, [f]_p\right)$ has a fixed point. Unfortunately, the picture is not quite so clear for points of period greater than one. For example, if we let $g(x) = x^2 + 3$, then $\left[\Phi_{g,2}\right]_5$ has exactly one root (with multiplicity two), which happens to have period one in $(\mathbb{F}_5, [g]_5)$. In Corollary 4.3, we provide a sufficient condition on $f \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}_{>0}$ that ensures that $\left[\Phi_{f,n}\right]_p$ has a root in $\mathbb{F}_p$ if and only if $\left(\mathbb{F}_p, [f]_p\right)$ has a point of period n for all but finitely many primes p.
- Finally, in Sect. 4, we apply the Hilbert irreducibility theorem to the polynomials produced in Theorem 2.3 to prove Theorem 1.1.

2 Galois groups of dynatomic polynomials

As we intend to distinguish dynamical systems by analyzing their periodic points, we will make use of the theory of dynatomic polynomials (and their Galois groups). See [18,19,21]

(and the correction in [20]), and [27, Chap. 4.1] for background in this area. We sketch an introduction, focusing on the aspects of the theory we will use in our results.

Let K be a field, $f \in K[x]$, and $n \in \mathbb{Z}_{>0}$. The points of period n of the dynamical system (K, f) are certainly roots of the polynomial $f^n(x) - x$. However, if $d \in \mathbb{Z}_{>0}$ and $d \mid n$, then this polynomial vanishes on points of period d as well (e.g., if $\alpha \in K$ is a fixed point of (K, f), i.e., $f(\alpha) = \alpha$, then $f^n(\alpha) = \alpha$ for all $n \in \mathbb{Z}_{>0}$). In an attempt to sieve out the points of lower period, one defines the nth *dynatomic polynomial of* f for any $n \in \mathbb{Z}_{>0}$:

$$\Phi_{f,n}(x) := \prod_{d|n} \left(f^d(x) - x\right)^{\mu(n/d)},$$

where $\mu : \mathbb{Z}_{\geq 0} \to \{-1, 0, 1\}$ is the usual Möbius function. The fact that

$$\prod_{d|n} \Phi_{f,n}(x) = f^n(x) - x$$

follows quickly by applying the Möbius inversion formula. As usual, we omit "K" from the notation "$\Phi_{f,n}$"; we will always specify the set of coefficients of f, so that the field K will be clear from context. As indicated by its name, the nth dynatomic polynomial is analogous to the nth cyclotomic polynomial, which vanishes precisely on primitive nth roots of unity. (As mentioned in the discussion following Example 1.2, it turns out that $\Phi_{f,n}$ may occasionally vanish on points of period d for $d < n$: see [27, Example 4.2]. In Corollary 4.3, we address this inconvenience.) We should mention that it is not *a priori* obvious that $\Phi_{f,n}$ is a polynomial. See [21, Theorem 2.5] for a proof that $\Phi_{f,n} \in K[x]$. (In particular, if $f \in \mathbb{Z}[x]$ and f is monic, then $\Phi_{f,n} \in \mathbb{Z}[x]$ by Gauss's Lemma.)

The degrees of certain dynatomic polynomials will be important quantities in many computations that follow, so we introduce the following notation.

Definition 2.1 For any $n \in \mathbb{Z}_{>0}$ and $k \in \mathbb{Z}_{>1}$, let

$$r_k(n) = \frac{1}{n} \cdot \sum_{d|n} k^d \mu\left(\frac{n}{d}\right).$$

Note that $nr_k(n)$ is the degree (in x) of the nth dynatomic polynomial of $x^k + c \in \mathbb{Q}(c)[x]$.

As mentioned in Example 1.2, our proof of Theorem 1.1 relies in part on the knowledge of the structure of the Galois groups of $\Phi_{f,n}$, where $n \in \mathbb{Z}_{>0}$ and $f(x) = x^k + m \in \mathbb{Z}[x]$ for $k \in \mathbb{Z}_{>1}$ and $m \in \mathbb{Z}$. Moreover, we must find arbitrarily large finite sets of polynomials of this form that have the property that the splitting fields of their dynatomic polynomials are linearly disjoint. For a specific polynomial $f \in \mathbb{Z}[x]$ of this form and any large n, it is difficult to compute the Galois group of $\Phi_{f,n}$, since the degree of $\Phi_{f,n}$ is so large, but—thanks to work of Morton [19, Theorem D]—the Galois groups of $\Phi_{f,n}$ for $f(x) = x^k + c \in \mathbb{Q}(c)[x]$ are known. The remainder of this section addresses the question of linear disjointness in the function field setting.

We will need the following elementary lemma of field theory.

Lemma 2.2 *Let K be a field and let $\sigma \in \mathrm{Aut}(K)$. Let $f \in K[x]$ be an irreducible polynomial, and let f^σ be the polynomial in $K[x]$ obtained by applying σ to each of the coefficients of f. Let L, L^σ be the splitting fields of f, f^σ, respectively. Then L and L^σ are isomorphic as fields. In particular,*

(1) $\mathrm{Gal}(f/K) \simeq \mathrm{Gal}(f^\sigma/K)$, *and*
(2) *if K is the fraction field of a Dedekind domain and $\mathfrak{p}$ is a prime of K, then*

$\mathfrak{p}$ *ramifies in L if and only if $\sigma(\mathfrak{p})$ ramifies in L^σ.*

Proof Let $\overline{K}$ be an algebraic closure of K containing both L and L^σ. Then we can extend $\sigma \in \mathrm{Aut}(K)$ to some automorphism $\widehat{\sigma} \in \mathrm{Aut}(\overline{K})$ [16, Theorem V.2.2.8]. It is easy to see that $\widehat{\sigma}$ furnishes a one-to-one correspondence between the roots of f and the roots of f^σ; thus $\widehat{\sigma}|_L : L \to L^\sigma$ is an isomorphism. Statement (1) follows immediately, and the map from $\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(L^\sigma/K)$ is given by

$$\tau \mapsto \widehat{\sigma}^{-1} \circ \tau \circ \widehat{\sigma}.$$

For (2), if the prime $\mathfrak{p}$ of K ramifies in L, there is a prime $\mathfrak{q}$ of L with $e(\mathfrak{q}/\mathfrak{p}) > 1$, and

$$e(\widehat{\sigma}(\mathfrak{q})/\sigma(\mathfrak{p})) = e(\widehat{\sigma}(\mathfrak{q})/\widehat{\sigma}(\mathfrak{p})) = e(\mathfrak{q}/\mathfrak{p}) > 1,$$

so $\sigma(\mathfrak{p})$ ramifies in L^σ. Replacing $\widehat{\sigma}$ by its inverse shows that the converse holds as well. □

For the rest of this section, we will work with polynomials $f(x) \in \mathbb{Q}(c)[x]$. For any $n \in \mathbb{Z}_{>0}$, let

- $\Sigma_{f,n}$ denote the splitting field of $\Phi_{f,n}$, and
- $K_{f,n}$ denote the splitting field of $f^n(x) - x$.

These splitting fields will be defined over $\mathbb{Q}(c)$ or $\overline{\mathbb{Q}}(c)$, depending on context. There should be no ambiguity about which definition is intended. Note that in either case, $K_{f,n}$ is the compositum of the fields $\Sigma_{f,d}$ for all positive integers d dividing n.

The next theorem generalizes the first part of Theorem D in [19].

Theorem 2.3 *Let $k \geq 2$ be an integer and $f = f(x) = x^k + c \in \mathbb{Q}(c)[x]$. Suppose that $M, N \in \mathbb{Z}_{>0}$. Then there exist infinitely many M-tuples of integers $(m_1, \ldots m_M) \in \mathbb{Z}^M$ such that*

$$\mathrm{Gal}\left(\left(\prod_{i=1}^{M} K_{f+m_i,N}\right) \Big/ \overline{\mathbb{Q}}(c)\right) \simeq \prod_{i=1}^{M} \mathrm{Gal}\left(K_{f+m_i,N}/\overline{\mathbb{Q}}(c)\right).$$

Proof Following the proof of Theorem 10 in [19], for any $n \in \mathbb{Z}_{>0}$, there exists a polynomial $\delta_n(x) \in \mathbb{Z}[x]$ such that the finite primes in $\overline{\mathbb{Q}}(c)$ that ramify in $\Sigma_{f,n}$ have the form $c-b$, where $b \in \overline{\mathbb{Q}}$ satisfies $\delta_n(b) = 0$. The roots of $\delta_n(x)$ are the roots of the hyperbolic components of the degree-k Multibrot set, which is the famous Mandelbrot set when $k = 2$. It is a consequence of the structure of the Multibrot set that $\delta_n(x)$ and $\delta_d(x)$ have no roots in common if $d \neq n$. (Closures of hyperbolic components of different periods may only intersect at a root of the component of higher period, see [5,24].) For any $m \in \mathbb{Z}$, consider the unique $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}(c)/\overline{\mathbb{Q}})$ defined by $\sigma(c) = c + m$. Then $f + m = f^\sigma$ in the notation of Lemma 2.2, so the primes that ramify in $\Sigma_{f+m,n}$ have the form $c - (b - m)$, where $b \in \overline{\mathbb{Q}}$ satisfies $\delta_n(b) = 0$.

With the above facts in mind, let R be the (finite) set

$$\left\{b \in \overline{\mathbb{Q}} \mid \text{there exists } d \in \mathbb{Z}_{>0} \text{ such that } d \mid N \text{ and } \delta_d(b) = 0\right\},$$

then choose $(m_1, \ldots, m_M) \in \mathbb{Z}^M$ such that the sets $\{R - m_i\}$ are pairwise disjoint. As R is a finite set, there are infinitely many such choices. For any $i \in \{1, \ldots, M\}$, let

$$\mathcal{F} = \left\{ \Sigma_{f+m_i,d} \;\middle|\; d \in \mathbb{Z}_{>0} \text{ with } d \mid N \right\} \quad \text{and} \quad \mathcal{G} = \left\{ \Sigma_{f+m_j,d} \;\middle|\; \begin{smallmatrix} j\in\{1,\ldots,M\} \text{ with } j\neq i \\ d\in\mathbb{Z}_{>0} \text{ with } d\mid N \end{smallmatrix} \right\}.$$

Recall that for any $m \in \mathbb{Q}$ and $n \in \mathbb{Z}_{>0}$, we have $K_{f+m,n} = \prod_{d|n} \Sigma_{f+m,d}$. Thus

$$\prod_{F\in\mathcal{F}} F = K_{f+m_i,N} \quad \text{and} \quad \prod_{F\in\mathcal{G}} F = \prod_{\substack{j=1 \\ j\neq i}}^{M} K_{f+m_j,N}.$$

By our choice of the m_is, these two fields have no finite ramified primes in common, so they are linearly disjoint over $\overline{\mathbb{Q}}(c)$. Therefore the fields $K_{f+m_1,N}, \ldots, K_{f+m_M,N}$ are linearly disjoint over $\overline{\mathbb{Q}}(c)$. The result now follows by elementary Galois theory. □

The corollary below follows immediately from Theorem 2.3 and by work of Morton. It will be crucial in the proof of Theorem 1.1.

Corollary 2.4 *Keep the same hypotheses as Theorem 2.3, and for any* $\mathbf{m} = (m_1, \ldots, m_M) \in \mathbb{Z}^M$, *let*

$$\mathcal{F}(\mathbf{m}) = \left\{ \Sigma_{f+m_i,d} \mid i \in \{1,\ldots,M\} \text{ and } d \in \mathbb{Z}_{>0} \text{ such that } d \mid N \right\}.$$

Then there exist infinitely many $\mathbf{m} \in \mathbb{Z}^M$ *such that*

- *any field in* $\mathcal{F}(\mathbf{m})$ *is linearly disjoint from the compositum of the others,*
- *if* $\Sigma_{f+m_i,d} \in \mathcal{F}(\mathbf{m})$, *then* $\mathrm{Gal}\left(\Sigma_{f+m_i,d}/\mathbb{Q}(c)\right) \simeq \mathrm{Gal}\left(\Sigma_{f+m_i,d}/\overline{\mathbb{Q}}(c)\right) \simeq \left(\mathbb{Z}/d\mathbb{Z} \wr S_{r_k(d)}\right)$, *and*
- $\mathrm{Gal}\left(\left(\prod_{i=1}^{M} K_{f+m_i,N}\right)\Big/\mathbb{Q}(c)\right) \simeq \prod_{i=1}^{N} \prod_{d|N} \left(\mathbb{Z}/d\mathbb{Z} \wr S_{r_k(d)}\right)$.

(Recall that $dr_k(d)$ *is the degree of the* d*th dynatomic polynomial of* $f(x)$, *see Definition 2.1.)*

Proof Theorem 9 in [19] shows that $f(x) = x^k + c \in \mathbb{Q}(c)[x]$ satisfies the assumptions of Theorem B in the same paper, which proves that for any $n \in \mathbb{Z}_{>0}$, both $\mathrm{Gal}(\Phi_{f,n}/\mathbb{Q}(c))$ and $\mathrm{Gal}(\Phi_{f,n}/\overline{\mathbb{Q}}(c))$ are isomorphic to $\mathbb{Z}/d\mathbb{Z} \wr S_{r_k(d)}$. Applying Lemma 2.2, with $\sigma : c \mapsto c + m$, we see that the same is true of the Galois group of $\Phi_{f+m,n}$ for any $m \in \mathbb{Q}$.

Let $\mathbf{m} = (m_1, \ldots, m_M)$ be any of the (infinitely many) M-tuples that satisfy the conclusion of Theorem 2.3. From the proof of Theorem 2.3, we know that if i, j are distinct integers in $\{1, \ldots, M\}$ and d is a positive integer divisor of N, then $\Sigma_{f+m_i,d}$ and $\Sigma_{f+m_j,d}$ are linearly disjoint over $\overline{\mathbb{Q}}(c)$. Thus

$$\begin{aligned} \mathrm{Gal}\left(\left(\prod_{i=1}^{M} K_{f+m_i,N}\right)\Big/\overline{\mathbb{Q}}(c)\right) &\simeq \prod_{i=1}^{M} \mathrm{Gal}\left(K_{f+m_i,N}/\overline{\mathbb{Q}}(c)\right) \\ &\simeq \prod_{i=1}^{M} \prod_{d|N} \mathrm{Gal}\left(\Sigma_{f+m_i,d}/\overline{\mathbb{Q}}(c)\right) \\ &\simeq \prod_{i=1}^{M} \prod_{d|N} \left(\mathbb{Z}/d\mathbb{Z} \wr S_{r_k(d)}\right). \end{aligned}$$

Let $G = \mathrm{Gal}\left(\left(\prod_{i=1}^{M} K_{f+m_i,N}\right)\Big/\mathbb{Q}(c)\right)$. By Theorem B from [19] again, we know G is isomorphic to a subgroup of $\prod_{i=1}^{M} \prod_{d|N} \left(\mathbb{Z}/d\mathbb{Z} \wr S_{r_k(d)}\right)$. Conversely, since $\overline{\mathbb{Q}}(c)$ contains $\mathbb{Q}(c)$, we see that $\prod_{i=1}^{M} \prod_{d|N} \left(\mathbb{Z}/d\mathbb{Z} \wr S_{r_k(d)}\right)$ is isomorphic to a subgroup of G, so the proof is complete. □

3 Fixed-point proportions in wreath products

In this section, we analyze some statistics of a certain family of wreath products. As these groups appear as Galois groups of dynatomic polynomials, these statistics are a vital component of our proof of Theorem 1.1. We begin with some definitions.

Suppose that $n, r \in \mathbb{Z}_{>0}$. Recall the definition of $\mathbb{Z}/n\mathbb{Z} \wr S_r$ from the end of Sect. 1. Let $B(n, r)$ denote $\mathbb{Z}/n\mathbb{Z} \times \{1, \dots, r\}$. The group $\mathbb{Z}/n\mathbb{Z} \wr S_r$ acts on the set $B(n, r)$; concretely, for any $\sigma = ((\overline{a_1}, \dots, \overline{a_r}), \pi) \in \mathbb{Z}/n\mathbb{Z} \wr S_r$, this action is

$$\begin{aligned} \sigma : B(n,r) &\to B(n,r) \\ \left(\overline{b}, i\right) &\mapsto \left(\overline{b + a_i}, \pi(i)\right). \end{aligned}$$

For any $\sigma \in \mathbb{Z}/n\mathbb{Z} \wr S_r$, define

$$\operatorname{Fix}\sigma = \left\{\left(\overline{b}, i\right) \in B(n,r) \mid \sigma\left(\overline{b}, i\right) = \left(\overline{b}, i\right)\right\};$$

then we set

$$P_{r,n} = \frac{|\{\sigma \in \mathbb{Z}/n\mathbb{Z} \wr S_r \mid \operatorname{Fix}\sigma \neq \emptyset\}|}{|\mathbb{Z}/n\mathbb{Z} \wr S_r|}.$$

In many cases, this action matches the action of the Galois groups of dynatomic polynomials on the roots of those polynomials, so we make the following definition.

Definition 3.1 For any $k \in \mathbb{Z}_{>1}$ and $n \in \mathbb{Z}_{>0}$, let

$$P_k(n) = P_{r_k(n),n},$$

where $r_k(n) = \sum_{d|n} k^d \mu\left(\frac{n}{d}\right)$ as in Definition 2.1.

Remark 3.2 When we apply the results of this section in the proof of Theorem 1.1, the groups $\mathbb{Z}/n\mathbb{Z} \wr S_{r_k(n)}$ will be isomorphic to the groups $\operatorname{Gal}(\Phi_{f,n}/\mathbb{Q})$ in a setting where $f \in \mathbb{Z}[x]$ and the roots of $\Phi_{f,n}$ are exactly the $nr_k(n)$ points of period n in $\left(\overline{\mathbb{Q}}, f\right)$. In this setting, we can identify $B(n, r_k(n))$ with the union of the $r_k(n)$ cycles of length n in $(\overline{\mathbb{Q}}, f)$ in such a way that the permutation action of $\operatorname{Gal}\left(\Phi_{f,n}/\mathbb{Q}\right)$ on the roots of $\Phi_{f,n}$ is precisely the action of $\mathbb{Z}/n\mathbb{Z} \wr S_{r_k(n)}$ on $B(n, r)$ described above (see Sect. 4 of [21] for details).

In particular, in the proof of Theorem 1.1, we will exploit the fact that

$$P_k(n) = \frac{\left|\sigma \in \operatorname{Gal}(\Phi_{f,n}/\mathbb{Q}) \mid \sigma \text{fixes a root of } \Phi_{f,n}\right|}{\left|\operatorname{Gal}(\Phi_{f,n}/\mathbb{Q})\right|}$$

for the polynomials $f \in \mathbb{Z}[x]$ and integers $n \in \mathbb{Z}_{>0}$ under consideration.

Now, the Galois groups in the conclusion of Corollary 2.4 are isomorphic to direct sums of the wreath products defined above. With this in mind, we need a bit more notation before proceeding—notation whose purpose will become clear in the proof of Theorem 1.1.

If G, H are groups acting on sets B, C, say with actions $\odot_G, \odot_H$, respectively, define the *product action* of $G \times H$ on $B \times C$ to be the action

$$\begin{aligned} (G \times H) \times (B \times C) &\to B \times C \\ ((g,h),(b,c)) &\mapsto (g,h) \odot_{G\times H} (b,c) := (g \odot_G b, h \odot_H c). \end{aligned}$$

Suppose $k \in \mathbb{Z}_{>1}$ and let $A = (b_i)_{i\in\mathbb{Z}_{>0}}$ be any increasing arithmetic progression of positive integers. For any $i \in \mathbb{Z}_{>0}$, define

$$W_{A,i} = \mathbb{Z}/b_i\mathbb{Z} \wr S_{r_k(b_i)} \times \mathbb{Z}/b_i\mathbb{Z} \wr S_{r_k(b_i)} \quad \text{and} \quad B_{A,i} = B\left(b_i, r_k\left(b_i\right)\right) \times B\left(b_i, r_k\left(b_i\right)\right),$$

so that $W_{A,i}$ acts on $B_{A,i}$ with the product action defined above. Next, for any $n \in \mathbb{Z}_{>0}$, let

$$W_A(n) = W_{A,1} \times \cdots \times W_{A,n} \quad \text{and} \quad B_A(n) = B_1 \times \cdots \times B_n;$$

once again, $W_A(n)$ acts on $B_A(n)$ with the product action induced from the action of the $W_{A,i}$s on the $B_{A,i}$s. In the proof of Theorem 1.1, we require knowledge of the proportion of these groups that act with a fixed point. To begin specifying the quantity we need, we first set, for any $i \in \{1, \ldots, n\}$,

$$C_{A,i}(n) = \left\{((\sigma_1, \tau_1), \ldots, (\sigma_n, \tau_n)) \in W_A(n) \mid \text{exactly one of } \operatorname{Fix}\sigma_i, \operatorname{Fix}\tau_i \text{ is empty}\right\}.$$

Let $s_{A,0} = 0$. Define

$$s_{A,n} = \frac{\left|\bigcup_{i=1}^{n} C_{A,i}(n)\right|}{|W_A(n)|}.$$

The main technical result of this section is Corollary 3.3, which exhibits a recurrence relation on the terms of sequences of the form $s_{A,n}$ and computes the limit of this sequence; the recurrence relation uses the quantities $P_k(b)$, for $b \in A$—these quantities were defined in Definition 3.1. We defer the proof until the end of the section, after establishing some estimates on fixed-point proportions in wreath products.

Corollary 3.3 *If $k \in \mathbb{Z}_{>1}$ and $A = (b_i)_{i\in\mathbb{Z}_{>0}}$ is any increasing arithmetic progression of positive integers, then for any $n \in \mathbb{Z}_{>0}$,*

$$s_{A,n} = s_{A,n-1} + (1 - s_{A,n-1})\, 2P_k(b_n)\left(1 - P_k(b_n)\right).$$

Moreover, $\lim_{n\to\infty} s_{A,n} = 1$.

We turn to computing $P_{r,k}$ for general $r \in \mathbb{Z}_{>0}$ and $k \in \mathbb{Z}_{>1}$. To do so, we recall the *rencontres numbers* from combinatorics. For any $r \in \mathbb{Z}_{>0}$ and $i \in \{0, \ldots, r\}$, we will denote the (r, i)th *rencontres number* by $D_{r,i}$; that is, $D_{r,i}$ is the number of permutations of $\{1, \ldots, r\}$ with exactly i fixed points. In particular, the number of derangements of $\{1, \ldots, r\}$ is $D_{r,0}$. For convenience, we set $D_{0,0} = 1$. We now record some basic identities involving rencontres numbers, which we will use in the proof of Theorem 3.5.

Lemma 3.4 *For all $i, r \in \mathbb{Z}_{\geq 0}$,*

(1) $D_{r,i} = \binom{r}{i} D_{r-i,0}$ *and*
(2) $\sum_{i=1}^{r} \binom{r}{i} D_{r-i,0} = r! - D_{r,0}$.

Proof For (1), note that a permutation of $\{1, \ldots, r\}$ with precisely i fixed points is completely determined by choosing its i fixed points and specifying its action on the $r - i$ remaining non-fixed points. For (2), observe that $\sum_{i=0}^{r} D_{r,i} = |S_r| = r!$, as each permutation in S_r contributes to exactly one term in the sum, then apply (1). □

We now prove an important estimate on $P_{r,n}$ for all wreath products defined above (that is, a larger class of wreath products than those which arise as Galois groups of dynatomic polynomials).

Theorem 3.5 *Suppose that $n, r \in \mathbb{Z}_{>0}$. Then*

$$\left|P_{r,n} - \left(1 - e^{-\frac{1}{n}}\right)\right| < \frac{1+2^r}{r!}.$$

Proof We begin by noting that if $\sigma \in \mathbb{Z}/n\mathbb{Z} \wr S_r$, then $|\mathrm{Fix}\,\sigma|$ is a multiple of n. This follows from the fact that if σ fixes any $\left(\overline{b}, i\right) \in B(n,r)$, then it must fix each $(\overline{c}, i)$ for all $\overline{c} \in \mathbb{Z}/n\mathbb{Z}$. Now, if $j \in \{1,\dots,r\}$, $\sigma = ((\overline{a_i}), \pi)$, and $|\mathrm{Fix}\,\sigma| = nj$, then π, acting on $\{1,\dots,r\}$, has at least j fixed points. Moreover, there is a subset R of the fixed points of π such that

- $|R| = j$ and
- if $i' \in \{1,\dots,r\}$ is a fixed point of π, then $i' \in R$ if and only if $\overline{a_{i'}} = 0$.

In other words, if $\pi \in S_r$, $\mathrm{Fix}\,\pi = T$, and $(\overline{a_i}) \in (\mathbb{Z}/n\mathbb{Z})^r$, then $|\mathrm{Fix}\,((\overline{a_i}), \pi)| = nj$ if and only if there exists $R \subseteq T$ with $|R| = j$ and for all $i' \in T$, $a_{i'} = \overline{0}$ if and only if $i' \in R$. Using this fact, and enumerating permutations π by their number of fixed points, note that

$$\left|\left\{\sigma \in \mathbb{Z}/n\mathbb{Z} \wr S_r \mid |\mathrm{Fix}\,\sigma| = nj\right\}\right| = \sum_{i=1}^{r} \binom{i}{j} D_{r,i}(n-1)^{i-j} n^{r-i}.$$

Using Lemma 3.4, we see that

$$\begin{aligned}
|\{\sigma \in \mathbb{Z}/n\mathbb{Z} \wr S_r \mid \mathrm{Fix}\,\sigma \neq \emptyset\}| &= \sum_{j=1}^{r}\sum_{i=1}^{r} \binom{i}{j} D_{r,i}(n-1)^{i-j} n^{r-i} \\
&= \sum_{j=1}^{r}\sum_{i=1}^{r} \binom{i}{j}\binom{r}{i} D_{r-i,0}(n-1)^{i-j} n^{r-i} \\
&= \sum_{i=1}^{r} \binom{r}{i} D_{r-i,0} n^{r-i} \sum_{j=1}^{r} \binom{i}{j} (n-1)^{i-j} \\
&= \sum_{i=1}^{r} \binom{r}{i} D_{r-i,0} n^{r-i} \left(n^i - (n-1)^i\right) \\
&= \sum_{i=1}^{r} \binom{r}{i} D_{r-i,0} n^r - \sum_{i=1}^{r} \binom{r}{i} D_{r-i,0} n^{r-i}(n-1)^i \\
&= r!n^r - D_{r,0}n^r - \sum_{i=1}^{r} \binom{r}{i} D_{r-i,0} n^{r-i}(n-1)^i \\
&= r!n^r - \sum_{i=0}^{r} \binom{r}{i} D_{i,0} n^i (n-1)^{r-i}.
\end{aligned}$$

Thus,

$$P_{r,n} = \frac{1}{r!n^r}\left(r!n^r - \sum_{i=0}^{r} \binom{r}{i} D_{i,0} n^i (n-1)^{r-i}\right) = 1 - \sum_{i=0}^{r} \frac{D_{i,0}}{i!(r-i)!}\left(\frac{n-1}{n}\right)^{r-i}.$$

Using the Taylor expansion of e^x evaluated at $x = 1 - \frac{1}{n}$, we see that

$$\left|P_{r,n} - \left(1 - e^{-\frac{1}{n}}\right)\right| = \left|\frac{1}{e}\sum_{i=0}^{\infty} \frac{1}{i!}\left(\frac{n-1}{n}\right)^i - \sum_{i=0}^{r} \frac{D_{i,0}}{i!(r-i)!}\left(\frac{n-1}{n}\right)^{r-i}\right|.$$

Finally, we use the well-known fact that $\frac{i!}{e} - 1 < D_{i,0} < \frac{i!}{e} + 1$ to conclude

$$\begin{aligned}\left|P_{r,n} - \left(1 - e^{-\frac{1}{n}}\right)\right| &< \frac{1}{e}\sum_{i=0}^{\infty}\frac{1}{i!}\left(\frac{n-1}{n}\right)^i - \frac{1}{e}\sum_{i=0}^{r}\frac{i!}{i!(r-i)!}\left(\frac{n-1}{n}\right)^{r-i} \\ &\quad + \sum_{i=0}^{r}\frac{1}{i!(r-i)!}\left(\frac{n-1}{n}\right)^{n-i} \\ &\leq \frac{1}{(r+1)!}\left(\frac{n-1}{n}\right)^{r+1} + \frac{1}{r!}\left(1 + \frac{n-1}{n}\right)^r \\ &< \frac{1+2^r}{r!}.\end{aligned}$$

□

We record a simple bound we will use in our study of fixed-point proportions. The goal is to prove that $P_k(n)(1 - P_k(n))$ is close enough to $\frac{1}{n}$ to satisfy the hypotheses of Lemma 3.7, so the exact error bound does not matter much.

Theorem 3.6 *Suppose that $k \in \mathbb{Z}_{>0}$. If $n \in \mathbb{Z}_{>0}$, then*

$$\left|P_k(n)\,(1 - P_k(n)) - \frac{1}{n}\right| < \frac{121}{n^2}.$$

Proof Using Theorem 3.5, we see that

$$\begin{aligned}&\left|P_k(n)\,(1 - P_k(n)) - e^{-\frac{1}{n}}\left(1 - e^{-\frac{1}{n}}\right)\right| \\ &= \left|P_k(n) - \left(1 - e^{-\frac{1}{n}}\right) + \left(1 - e^{-\frac{1}{n}}\right)^2 - P_n(k)^2\right| \\ &\leq \left|P_k(n) - \left(1 - e^{-\frac{1}{n}}\right)\right| \cdot \left(1 + \left|\left(1 - e^{-\frac{1}{n}}\right) + P_k(n)\right|\right) \\ &< \frac{1+2^{r_k(n)}}{r_k(n)!} \cdot 3.\end{aligned}$$

Writing the Taylor series of $e^x\,(1 - e^x)$ shows

$$\left|e^{-\frac{1}{n}}\left(1 - e^{-\frac{1}{n}}\right) - \frac{1}{n}\right| < \frac{3}{2n^2},$$

so by the triangle inequality,

$$\left|P_k(n)\,(1 - P_k(n)) - \frac{1}{n}\right| < 3 \cdot \frac{1+2^{r_k(n)}}{r_k(n)!} + \frac{3}{2n^2}.$$

Since $0 < P_k(n)\,(1 - P_k(n)) < \frac{1}{4}$, we know that $\left|P_k(n)\,(1 - P_k(n)) - \frac{1}{n}\right| < 1$ for all n; in particular, the statement is true for all $n \leq 11$. Thus, we may assume that $n \geq 12$. This implies immediately that $r_k(n) > \frac{k^{n-1}}{n} > 7$ and $k^{n-1} > n^3$. Next, we note that

$$3 \cdot \frac{1+2^x}{(x-1)!} < 1 \quad \text{for all } x \geq 7.$$

Putting these estimates together, we obtain

$$3 \cdot \frac{1+2^{r_k(n)}}{(r_k(n))!} < \frac{1}{r_k(n)} < \frac{n}{k^{n-1}} < \frac{1}{n^2} \quad \text{when} \quad n \geq 12.$$

So for all such n, we conclude that

$$\left|P_k(n)\,(1-P_k(n))-\frac{1}{n}\right|<\frac{1}{n^2}+\frac{3}{2n^2}=\frac{5}{2n^2}.$$

□

Before proving the corollary we will use in the proof of Theorem 1.1, we prove a short lemma about a certain class of recurrence relations.

Lemma 3.7 *Suppose $(a_n)_{n\in\mathbb{Z}_{>0}}$ is a sequence of real numbers that satisfies*

$$\sum_{n=1}^{\infty}a_n=\infty,\quad \lim_{n\to\infty}a_n=0,\ \textit{and}\ a_n\in[0,1]\quad \textit{for all}\ n\in\mathbb{Z}_{>0}.$$

Suppose $t_0\in[0,1]$, and define

$$t_n=t_{n-1}+a_n\,(1-t_{n-1})\quad \textit{for all}\ n\in\mathbb{Z}_{>0}.$$

Then $\lim_{n\to\infty}t_n=1$.

Proof A short induction argument shows that (t_n) is non-decreasing and bounded above by 1. So (t_n) converges; suppose for a contradiction that it converges to $L\in[0,1)$. Note that

$$t_n-t_{n-1}=a_n\,(1-t_{n-1})\geq a_n(1-L).$$

Summing both sides of this inequality over all $n\in\mathbb{Z}_{\geq 0}$ yields the contradiction

$$\lim_{n\to\infty}(t_n-t_0)=\infty.$$

□

Putting together the results in this section, we can now prove Corollary 3.3.

Proof of Corollary 3.3 Recall that $W_A(n)=W_{A,1}\times\cdots\times W_{A,n}$, that

$$C_{A,i}\,(n)=\left\{((\sigma_1,\tau_1),\ldots,(\sigma_n,\tau_n))\in W_A\,(n)\mid \text{exactly one of Fix}\,\sigma_i,\,\text{Fix}\,\tau_i\,\text{is empty}\right\},$$

and that $s_{A,n}$ is defined by $s_{A,0}=0$ and

$$s_{A,n}=\frac{\left|\bigcup_{i=1}^{n}C_{A,i}\,(n)\right|}{|W_A\,(n)|}$$

for $n>0$. Observe that $\left|W_A(n)\right|=\left|W_A(n-1)\right|\left|W_{A,n}\right|$ and $\left|C_{A,i}(n)\right|=\left|C_{A,i}(n-1)\right|\left|W_{A,n}\right|$ for $1\leq i\leq n-1$. Thus, the sequence $s_{A,n}$ satisfies the recurrence relation

$$\begin{aligned}s_{A,n}&=s_{A,n-1}\frac{\left|W_{A,n}\right|}{\left|W_{A,n}\right|}\\&\quad+(1-s_{A,n-1})\,\frac{\left|\left\{(\sigma,\tau)\in W_{A,n}\mid \text{exactly one of Fix}\,\sigma,\ \text{Fix}\,\tau\ \text{is empty}\right\}\right|}{\left|W_{A,n}\right|}\\&=s_{A,n-1}+(1-s_{A,n-1})\,2P_k\,(b_n)\,(1-P_k\,(b_n)).\end{aligned}$$

Since $0<P_k\,(b_n)<1$ for all n, we note that $0<2P_k\,(b_n)\,(1-P_k\,(b_n))<1$ for all n as well. Setting $a_n=2P_k\,(b_n)\,(1-P_k\,(b_n))$, Theorem 3.6 implies that (a_n) satisfies the hypotheses of Lemma 3.7, which we apply to conclude the proof. □

4 Applying the Hilbert Irreducibility and the Frobenius Density Theorems

In this section, for any polynomial $f(c,x) \in \mathbb{Q}[c][x]$ and any $a \in \mathbb{Q}$, we will write f_a for the specialization of f at $c = a$; that is, $f_a = f_a(x) = f(a,x) \in \mathbb{Q}[x]$. Below is a version of the Hilbert irreducibility theorem, one which we will apply in the proof of Theorem 1.1.

Hilbert irreducibility theorem. *Let $f(c,x) \in \mathbb{Z}[c][x]$, let K be the splitting field of $f(c,x)$ over $\mathbb{Q}(c)$, and for any $a \in \mathbb{Z}$, let K_a be the splitting field of f_a over $\mathbb{Q}$. Suppose that $f(c,x)$ has no repeated roots (in $\overline{\mathbb{Q}(c)}$). Then there exists a "thin set" $A \subset \mathbb{Z}$ such that for all $a \in \mathbb{Z} \setminus A$,*

$$f_a \text{ has no repeated roots} \quad \text{and} \quad \mathrm{Gal}(K_a/\mathbb{Q}) \simeq \mathrm{Gal}(K/\mathbb{Q}(c)).$$

Remark 4.1 The Hilbert irreducibility theorem is normally stated for irreducible polynomials (as in [25]). To obtain the version stated above, let $g(c,x)$ be the minimal polynomial of a primitive element of $K/\mathbb{Q}(c)$, which is irreducible over $\mathbb{Q}(c)$. Then specialize $g(c,x)$ instead of $f(c,x)$. Moreover, if $f(c,x)$ has no repeated roots in $\overline{\mathbb{Q}(c)}$, then there are only finitely many $a \in \mathbb{Q}$ for which $f_a(x)$ has a repeated root in $\overline{\mathbb{Q}}$ (these are precisely the a for which the discriminant $\mathrm{Disc} f(c,x)$ vanishes under the specialization at $c = a$). For more on the connection between the Hilbert irreducibility theorem and Galois theory, see, for example, [7], [15, Chap. VIII], and [30, Chap. 1].

As for the size of the "thin set" A, we know there is some constant C such that for all $X \in \mathbb{Z}_{>0}$,

$$|\{a \in A \mid a \le X\}| \le C\sqrt{X}$$

(See [25, Sect. 9.7], for more details). In particular, there are infinitely many integers for which the conclusion of the theorem is true.

Next, we recall a case of the Frobenius density theorem (See [28] for more details).

Frobenius Density Theorem. *Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic polynomial with no repeated roots. Let $G = \mathrm{Gal}(f/\mathbb{Q})$ and $P \subseteq \mathcal{P}$ be the set of primes p such that $[f]_p$ has a root in $\mathbb{F}_p$. Then*

$$\mu(P) = \frac{1}{|G|} \cdot \left|\left\{\sigma \in G \mid \sigma \text{ fixes a root of } f\right\}\right|.$$

Remark 4.2 If $f, g \in \mathbb{Z}[x]$ satisfy the hypotheses of the Frobenius Density Theorem, the sets

$$P_f = \{p \in \mathcal{P} \mid [f]_p \text{ has a root in } \mathbb{F}_p\} \quad \text{and} \quad P_g = \{p \in \mathcal{P} \mid [g]_p \text{ has a root in } \mathbb{F}_p\}$$

are probabilistically independent (in the sense that $\mu\left(P_f \cap P_g\right) = \mu\left(P_f\right) \cdot \mu\left(P_g\right)$) if and only if the splitting fields of f and g are linearly disjoint over $\mathbb{Q}$. This follows immediately from the fact that the Galois group of a compositum of fields is the direct product of the Galois groups if and only if the fields are linearly disjoint.

In light of the Frobenius density theorem, one might hope that given $f \in \mathbb{Z}[x]$ and $p \in \mathcal{P}$, the roots of $\left[\Phi_{f,n}\right]_p$ are precisely the points of $\left(\mathbb{F}_p, [f]_p\right)$ of period n, but—as mentioned in Sect. 1—this hope would be in vain. Indeed, even before reducing mod p, if $\alpha \in \overline{\mathbb{Q}}$ is a point of period n in $\left(\overline{\mathbb{Q}}, f\right)$, then $\Phi_{f,n}(\alpha) = 0$, but the converse is not always true—that is, there are examples of (K, f), n, α, and d, where $d < n$, α is a point of period d, but $\Phi_{f,n}(\alpha) = 0$, see [27, Example 4.2]. In general, if $\alpha \in \overline{\mathbb{Q}}$ and $\Phi_{f,n}(\alpha) = 0$, then α is of

period d for some $d \leq n$, and $d < n$ is possible only if the polynomial derivative of f^d evaluated at α is a root of unity; this quantity is known as the *multiplier of* α. The way in which the period depends on the multiplier is the content of the following theorem [27, Theorem 4.5].

Roots and multipliers theorem. *Suppose that K is a field, $f \in K[x]$, $n \in \mathbb{Z}_{>0}$, and $\alpha \in \overline{K}$ satisfies $\Phi_{f,n}(\alpha) = 0$. Let $\lambda = (f^m)'(\alpha)$ where m is the (least) period of α. Then either*

(1) $n = m$,
(2) $n = mj$, *when λ is a primitive j*th *root of unity, or*
(3) $n = mjp^e$, *with $e \in \mathbb{Z}_{>0}$, when λ is a primitive j*th *root of unity and* $\operatorname{char} K = p > 0$.

Conversely, if $\alpha \in \overline{K}$ has period n in $(K(\alpha), f)$, then $\Phi_{f,n}(\alpha) = 0$.

Luckily, given $f \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}_{>0}$, the following corollary provides a sufficient condition that ensures that for all but finitely many primes $p \in \mathcal{P}$, the dynamical system $\left(\mathbb{F}_p, [f]_p\right)$ has a point of period n if and only if $\left[\Phi_{f,n}\right]_p$ has a root. In the proof of Theorem 1.1, we will use the work in Sect. 2 to ensure that the polynomials obtained by applying the Hilbert irreducibility theorem satisfy this sufficient condition.

Corollary 4.3 *Let $f \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}_{>0}$, and suppose that $f^n(x) - x$ has no repeated roots. Then for all but finitely many $p \in \mathcal{P}$,*

$$\left[\Phi_{f,n}\right]_p \text{ has a root in } \mathbb{F}_p \text{ if and only if } \left(\mathbb{F}_p, [f]_p\right) \text{ has a point of period } n.$$

Proof As pointed out in Sect. 2 of [29], for example, if $f^n(x) - x$ has no repeated roots, then for all $\alpha \in \overline{\mathbb{Q}}$,

$$\Phi_{f,n}(\alpha) = 0 \text{ if and only if } \alpha \text{ is a point of period } n \text{ in } (\mathbb{Q}(\alpha), f).$$

As usual, for any $\alpha \in \overline{\mathbb{Q}}$ and $p \in \mathcal{P}$, we say p divides α if there exists a number field K containing α and a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $\mathfrak{p} \mid (p)$ and $\operatorname{ord}_{\mathfrak{p}}(\alpha) > 0$.

Let $p \in \mathcal{P}$, and suppose that $\left[\Phi_{f,n}\right]_p$ has a root. Let K be the splitting field of $\Phi_{f,n}$, choose any prime $\mathfrak{p}$ lying over p, and denote by $\bar{\cdot}$ the reduction $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$. Since $\mathcal{O}_K/\mathfrak{p}$ is an extension of $\mathbb{F}_p$ and $\left[\Phi_{f,n}\right]_p$ has a root, there exists $a \in \mathbb{Z} \subseteq \mathcal{O}_K$ such that $\left[\Phi_{f,n}\right]_p(\overline{a}) = 0$. Since $\Phi_{f,n}$ splits in K, we know that $\left[\Phi_{f,n}\right]_p$ splits in $\mathcal{O}_K/\mathfrak{p}$ and the roots of $\Phi_{f,n}$ map onto the roots of $\left[\Phi_{f,n}\right]_p$ under $\bar{\cdot}$; choose any $\alpha \in K$ such that $\Phi_{f,n}(\alpha) = 0$ and $\overline{\alpha} = \overline{a}$.

Now, by the roots and multipliers theorem, we know that $\overline{a}$ is a periodic point of $\left(\mathbb{F}_p, [f]_p\right)$ of period at most n; let us suppose its period is strictly less than n (so in particular, $n > 1$). This implies that there exists $j \in \{1, \ldots, n-1\}$ such that

$$\overline{f^j(\alpha) - \alpha} = \left([f]_p\right)^j(\overline{a}) - \overline{a} = 0;$$

that is, $\mathfrak{p}$ divides $f^j(\alpha) - \alpha$. We know that α has period n in (K, f), so the points $\alpha, f(\alpha), f^2(\alpha), \ldots, f^{n-1}(\alpha)$ are pairwise distinct; thus, there are only finitely many prime ideals of $\mathcal{O}_K$ dividing their differences, as desired.

Now suppose that $[f]_p$ has a point of period n in $\left(\mathbb{F}_p, [f]_p\right)$. It is easy to see that $[f^n]_p = \left([f]_p\right)^n$, so $\left[\Phi_{f,n}\right]_p = \Phi_{[f]_p,n}$. By the roots and multipliers theorem, with $K = \mathbb{F}_p$, we know that $\left[\Phi_{f,n}\right]_p$ has a root in $\mathbb{F}_p$. □

Finally, we can apply Corollaries 2.4, 3.3, and the results mentioned above to prove Theorem 1.1.

Proof of Theorem 1.1 Let $\mathcal{T} = \left\{J \subseteq \{1, \ldots, M\} \;\middle|\; |J| = 2\right\}$, set $t = |\mathcal{T}| = \binom{M}{2}$, and choose any bijection $\beta : \mathcal{T} \to \{1, \ldots, t\}$. For any $J \in \mathcal{T}$, let A_J denote the arithmetic progression $(\beta(J), \beta(J) + t, \beta(J) + 2t, \ldots)$. Define $s_{A_J,0} = 0$ and

$$s_{A_J,i} = s_{A_J,i-1} + 2\left(1 - s_{A_J,i-1}\right) P_k(\beta(J) + t(i-1))\left(1 - P_k(\beta(J) + t(i-1))\right)$$
$$\text{for all} \quad i \in \mathbb{Z}_{>0}.$$

By Corollary 3.3, for each choice of J we know $s_{A_J,i} \to 1$ as $i \to \infty$. Thus, there exists $N_0 \in \mathbb{Z}_{>0}$ such that $s_{A_J,N_0} > 1 - \frac{\epsilon}{t}$ for all $J \in \mathcal{T}$. Let $N = (tN_0)!$ and set $f = x^k + c \in \mathbb{Q}(c)[x]$, so that for any $a \in \mathbb{Z}$, $f_a = x^k + a \in \mathbb{Z}[x]$. Next, let

$$\mathcal{F}(a) = \left\{\Sigma_{f_a,d} \mid d \in \mathbb{Z}_{>0} \text{ and } d \mid N\right\},$$

where $\Sigma_{f_a,d}$ is the splitting field of $\Phi_{f_a,d}$ over $\mathbb{Q}$. By Theorem D of [19], we know that $f^N(x) - x$ has no repeated roots in $\overline{\mathbb{Q}(c)}$, so by Lemma 2.2, for any $m \in \mathbb{Z}$, we see that $(f + m)^N(x) - x$ has no repeated roots either. Thus, by Corollary 2.4 and the Hilbert irreducibility theorem, there exist infinitely many M-tuples $(m_1, \ldots, m_M) \in \mathbb{Z}^M$ such that

- any field in $\bigcup_{j=1}^{M} \mathcal{F}(m_j)$ is linearly disjoint from the compositum of the others,
- if $\Sigma_{f_{m_j},d} \in \bigcup_{j=1}^{M} \mathcal{F}(m_j)$, then $\mathrm{Gal}\left(\Sigma_{f_{m_j},d}/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/d\mathbb{Z} \wr S_{r_k(d)}\right)$, and
- for any $j \in \{1, \ldots, M\}$, we know $\left(f_{m_j}\right)^N(x) - x$ has no repeated roots.

We will prove that for any such $(m_1, \ldots, m_M)$,

$$\mu\left(\left\{p \in \mathcal{P} \;\middle|\; \left\{x^k + m_1, \ldots, x^k + m_M\right\} \text{ is dynamically distinguishable mod } p\right\}\right)$$
$$> 1 - \epsilon.$$

To begin, fix such an M-tuple $(m_1, \ldots, m_M)$. We introduce a bit of simplifying notation. For any $J = \{j, j'\} \in \mathcal{T}$, we will compare those $\Phi_{x^k+m_j,i}$, $\Phi_{x^k+m_{j'},i}$ for i in the truncated arithmetic progression $(\beta(J) + t(i-1) \mid i \in \{1, \ldots, N_0\})$. To make this analysis more convenient, for any $J \in \mathcal{T}$ and $j \in J$, write

$$\Phi_{J,j,i} = \Phi_{x^k+m_j,\beta(J)+t(i-1)}.$$

Using this notation, we can define for any $J \in \mathcal{T}$:

$$\Phi_J = \prod_{j \in J} \prod_{i=1}^{N_0} \Phi_{J,j,i} \quad \text{and} \quad G_J = \mathrm{Gal}\left(\Phi_J/\mathbb{Q}\right).$$

Now set

$$\Phi = \prod_{J \in \mathcal{T}} \Phi_J \quad \text{and} \quad G = \mathrm{Gal}\left(\Phi/\mathbb{Q}\right).$$

Note that

$$\Phi \text{ divides } \prod_{j=1}^{M} \left(\left(f_{m_j}\right)^N(x) - x\right) \text{ in } \mathbb{Q}[x]$$

by the definition of the dynatomic polynomials, so

$$\Phi \text{ has distinct roots in } \overline{\mathbb{Q}} \quad \text{and} \quad G \simeq \prod_{J \in \mathcal{T}} G_J$$

by our choice of $(m_1, \ldots, m_M) \in \mathbb{Z}^M$.

Next, we introduce the sets of primes whose natural densities we will compute; namely, for any $J \in \mathcal{T}$ and $i \in \{1, \ldots, N_0\}$, define

$$P^{\Gamma}_{J,i} = \{p \in \mathcal{P} \mid \text{exactly one of } \{\Gamma_{x^k+m_j,p} \mid j \in J\} \text{ has a } (\beta(J) + t(i-1))\text{-cycle}\},$$
$$P^{\Phi}_{J,i} = \{p \in \mathcal{P} \mid \text{exactly one of } \{[\Phi_{J,j,i}]_p \mid j \in J\} \text{ has a root in } \mathbb{F}_p\}.$$

As we will compare these sets to proportions of Galois groups, we define for any $J \in \mathcal{T}$,

$$C_J = \left\{\sigma \in G_J \mid \text{for some } i \in \{1, \ldots, N_0\}, \sigma \text{ fixes a root of exactly one of } \left\{\Phi_{J,j,i} \mid j \in J\right\}\right\}.$$

Now, set $P^{\Phi}_J = \bigcup_{i=1}^{N_0} P^{\Phi}_{J,i}$ and apply the Frobenius density theorem to Φ_J to see that

$$\mu\left(P^{\Phi}_J\right) = \frac{|C_J|}{|G_J|}.$$

Next, recall that Corollary 4.3 implies that for any $J \in \mathcal{T}$ and $i \in \{1, \ldots, N_0\}$, the symmetric difference of $P^{\Gamma}_{J,i}$ and $P^{\Phi}_{J,i}$ is finite. Thus,

$$\begin{aligned}
&\mu\left(\left\{p \in \mathcal{P} \mid \left\{x^k + m_1, \ldots, x^k + m_M\right\} \text{ is dynamically distinguishable mod } p\right\}\right) \\
&= \mu\left(\bigcap_{J\in\mathcal{T}} \left\{p \in \mathcal{P} \mid \left\{x^k + m_j \mid j \in J\right\} \text{ is dynamically distinguishable mod } p\right\}\right) \\
&\geq \mu\left(\bigcap_{J\in\mathcal{T}} \left(\bigcup_{i=1}^{N_0} P^{\Gamma}_{J,i}\right)\right) \\
&= \mu\left(\bigcap_{J\in\mathcal{T}} \left(\bigcup_{i=1}^{N_0} P^{\Phi}_{J,i}\right)\right) \\
&= \mu\left(\bigcap_{J\in\mathcal{T}} P^{\Phi}_J\right) \\
&= \prod_{J\in\mathcal{T}} \frac{|C_J|}{|G_J|},
\end{aligned}$$

where the last step follows from Remark 4.2.

We will conclude the proof by showing that if $J \in \mathcal{T}$, then $\frac{|C_J|}{|G_J|} > 1 - \frac{\epsilon}{t}$, whence

$$\prod_{J\in\mathcal{T}} \frac{|C_J|}{|G_J|} > \left(1 - \frac{\epsilon}{t}\right)^t > 1 - \epsilon.$$

By Remark 3.2, Corollary 3.3, and our choice of $(m_1, \ldots, m_M)$, we know that

$$\frac{|C_J|}{|G_J|} = s_{A_J,N_0},$$

so we are done by our original choice of N_0. □

Author details
[1] Department of Mathematics, Texas A&M University, College Station, TX, USA, [2] Fariborz Maseeh Department of Mathematics and Statistics, Portland State University, Portland, OR, USA.

Acknowledgements
We would like to thank the referee for a careful reading of the paper and very helpful comments on the presentation. We also thank Patrick Morton for helpful comments about the proofs in his series of papers on dynatomic polynomials, Rafe Jones for pointing us to Morton's work, and Robert Lemke Oliver for many constructive conversations regarding the topics in this paper.

Received: 13 October 2016 Accepted: 9 March 2017
Published online: 10 July 2017

References

1. Bach, E.: Toward a theory of Pollard's rho method. Inf. Comput. **90**(2), 139–155 (1991)
2. Bach, E., Bridy, A.: On the number of distinct functional graphs of affine-linear transformations over finite fields. Linear Algebra Appl. **439**(5), 1312–1320 (2013)
3. Blanc, J., Canci, J.K., Elkies, N.D.: Moduli spaces of quadratic rational maps with a marked periodic point of small order. Int. Math. Res. Not. **23**, 12459–12489 (2015)
4. Bellah, E., Garton, D., Tannenbaum, E., Walton, N.: A probabilistic heuristic for counting components of functional graphs of polynomials over finite fields. Involve, ArXiv e-prints (2016) (to appear)
5. Branner, B.: The mandelbrot set, chaos and fractals (Providence, RI, 1988). In: Proceedings of Symposium on Applied Mathematics, vol. 39, pp. 75–105. American Mathematical Society, Providence (1989)
6. Burnette, C., Schmutz, E.: Periods of iterated rational functions over a finite field. Int. J. Number Theory, ArXiv e-prints (2015) (to appear)
7. Cohen, S.D.: The distribution of Galois groups and Hilbert's irreducibility theorem. Proc. Lond. Math. Soc. **43**(2), 227–250 (1981)
8. DeMarco, L.: The moduli space of quadratic rational maps. J. Am. Math. Soc. **20**(2), 321–355 (2007)
9. Fatou, P.: Sur les équations fonctionnelles. Bull. Soc. Math. Fr. **47**, 161–271 (1919)
10. Fatou, P.: Sur les équations fonctionnelles. Bull. Soc. Math. Fr. **48**, 208–314 (1920)
11. Flynn, R., Garton, D.: Graph components and dynamics over finite fields. Int. J. Number Theory **10**(3), 779–792 (2014)
12. Isaacs, I.: Martin: Finite Group Theory, Graduate Studies in Mathematics, vol. 92. American Mathematical Society, Providence (2008)
13. Julia, G.: Mémoire sur literation des fonctions rationnelles. J. Math. Pure Appl. **8**, 47–245 (1918)
14. Konyagin, S.V., Luca, F., Mans, B., Mathieson, L., Sha, M., Shparlinski, I.E.: Functional graphs of polynomials over finite fields. J. Comb. Theory Ser. B **116**, 87–122 (2016)
15. Lang, S.: Fundamentals of Diophantine Geometry. Springer, New York (1983)
16. Lang, S.: Algebra. Graduate Texts in Mathematics, vol. 211, 3rd edn. Springer, New York (2002)
17. Levy, A.: The space of morphisms on projective space. Acta Arith. **146**(1), 13–31 (2011)
18. Morton, P.: On certain algebraic curves related to polynomial maps. Compos. Math. **103**(3), 319–350 (1996)
19. Morton, P.: Galois groups of periodic points. J. Algebra **201**(2), 401–428 (1998)
20. Morton, P.: Corrigendum: On certain algebraic curves related to polynomial maps. Compos. Math. 103 (1996), 319–350. Compos. Math. **147**(1), 332–334 (2011)
21. Morton, P., Patel, P.: The Galois theory of periodic points of polynomial maps. Proc. Lond. Math. Soc. **68**(2), 225–263 (1994)
22. Ostafe, A., Sha, M.: Counting Dynamical Systems Over Finite Fields. Dynamics and Numbers, Contemporary Mathematics, vol. 669, pp. 187–204. American Mathematical Society, Providence (2016)
23. Pollard, J.M.: A Monte Carlo method for factorization. Nord. Tidskr. Informationsbehandl. (BIT) **15**(3), 331–334 (1975)
24. Schleicher, D.: Internal Addresses in the Mandelbrot Set and Irreducibility of Polynomials. ProQuest LLC, Ann Arbor, MI, Thesis (Ph.D.), Cornell University (1994)
25. Serre, J.-P.: Lectures on the Mordell–Weil Theorem, 3rd edn., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig (1997) (Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre)
26. Silverman, J.H.: The space of rational maps on P^1. Duke Math. J. **94**(1), 41–77 (1998)
27. Silverman, J.H.: The Arithmetic of Dynamical Systems, Graduate Texts in Mathematics, vol. 241. Springer, New York (2007)
28. Stevenhagen, P., Lenstra Jr., H.W.: Chebotarëv and his density theorem. Math. Intell. **18**(2), 26–37 (1996)
29. Vivaldi, F., Hatjispyros, S.: Galois theory of periodic orbits of rational maps. Nonlinearity **5**(4), 961–978 (1992)
30. Völklein, H.: Groups as Galois Groups. An introduction. Cambridge Studies in Advanced Mathematics, vol. 53. Cambridge University Press, Cambridge (1996)