11-1-2020

The Cycle Structure of Unicritical Polynomials

Andrew Bridy

Derek Garton
Portland State University, gartondw@pdx.edu

Citation Details

Bridy, A., & Garton, D. (2020). The Cycle Structure of Unicritical Polynomials. *International Mathematics Research Notices*, *2020*(23), 9120–9147. https://doi.org/10.1093/imrn/rny232

THE CYCLE STRUCTURE OF UNICRITICAL POLYNOMIALS

ANDREW BRIDY AND DEREK GARTON

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 $\mathbb{F}_p$. The questions of whether and in what sense these families are random have been studied extensively, spurred in part by Pollard's famous "rho" algorithm for integer factorization (the heuristic justification of which is the randomness of one such family). However, the cycle structure of these families *cannot* be random, since in any such family, the number of cycles of a fixed length in any dynamical system in the family is bounded. In this paper, we show that the cycle statistics of many of these families are *as random as possible*. As a corollary, we show that most members of these families have many cycles, addressing a conjecture of Mans et. al.

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 $n \in \mathbb{Z}_{>0}$, we let $f^n = \overbrace{f \circ \cdots \circ f}^{n \text{ times}}$; furthermore, we set $f^0 = \mathrm{id}_S$. We will denote the set of rational primes by $\mathcal{P}$. For $f \in \mathbb{Z}[x]$ and $p \in \mathcal{P}$, write $[f]_p$ for the polynomial in $\mathbb{F}_p[x]$ obtained by reducing the coefficients of f mod p. Similarly, let $[f]_{\mathcal{P}}$ be the family of dynamical systems $\{(\mathbb{F}_p, [f]_p) \mid p \in \mathcal{P}\}$. Spurred in part by Pollard's rho algorithm [Pol75], the following question presents itself: for $f \in \mathbb{Z}[x]$, in what sense does the family $[f]_{\mathcal{P}}$ behave randomly? Of course, the answer to this question depends upon

- the choice of $f \in \mathbb{Z}[x]$ and
- what "behave randomly" means.

In this paper, we restrict our attention to

- monic binomial unicritical polynomials (that is, polynomials of the form $x^k + a$ for $k \in \mathbb{Z}_{\geq 2}$ and $a \in \mathbb{Z}$) and
- the cycle structure of dynamical systems.

Recall that if (S, f) is a dynamical system, and $s \in S$ 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, and if s happens to be a point of period n, we call $\{f^i(s) \mid i \in \mathbb{Z}_{\geq 0}\}$ an *n-cycle*. In [Gon44] (see also the translation [Gon62]), Gončarov discovered the cycle structure of random dynamical systems, which we now recall. To ease notation, for any sets S and T, let S^T denote the set of functions from T to S, and for any $X \in \mathbb{Z}_{\geq 1}$, let

Date: January 26, 2018.
2010 *Mathematics Subject Classification.* Primary 37P05; Secondary 37P25, 11R32, 20B35.
Key words and phrases. Arithmetic Dynamics, Finite Fields, Galois Theory, Wreath Products.

$[X] = \{1, \dots, X\}$. Gončarov proved that for any $n \in \mathbb{Z}_{\geq 1}$, the function

$$\begin{aligned} \mu_n \colon \mathbb{Z}_{\geq 0} &\to \mathbb{R}_{\geq 0} \\ j &\mapsto \lim_{X \to \infty} \frac{|\{f \in [X]^{[X]} \mid ([X], f) \text{ has precisely } j \text{ } n\text{-cycles}\}|}{|[X]^{[X]}|} \end{aligned}$$

is the Poisson distribution with mean $\frac{1}{n}$. As the Poisson distribution will play an important role in this paper, we pause here to introduce some notation: for any $\lambda \in \mathbb{R}_{>0}$, we let $\rho_\lambda \colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ be the Poisson distribution of mean λ. With this notation in hand, we can rephrase Gončarov's result: if $n \in \mathbb{Z}_{\geq 1}$, then $\mu_n = \rho_{1/n}$.

Since Gončarov was kind enough to compute the cycle statistics of random dynamical systems, we now turn to quantifing the cycle statistics of the families $[f]_{\mathcal{P}}$ for $f \in \mathbb{Z}[x]$; we do this by using the natural density on $\mathcal{P}$—which we will denote by δ. Specifically, for any subset $P \subseteq \mathcal{P}$, let

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

Similarly, let

$$\overline{\delta}(P) := \limsup_{X \to \infty} \frac{|\{p \in \mathcal{P} \mid p \leq X \text{ and } p \in P\}|}{|\{p \in \mathcal{P} \mid p \leq X\}|}.$$

Remark 1.1. We must begin by remarking that it is *a priori* impossible for the cycle statistics of $[f]_{\mathcal{P}}$ to match those of random dynamical systems. As shown by Gončarov, if $n \in \mathbb{Z}_{\geq 1}$ then for any $j \in \mathbb{Z}_{\geq 0}$, there is a positive proportion of dynamical systems with precisely j n-cycles (that is, $\mu_n(j) > 0$ for all $j \in \mathbb{Z}_{\geq 0}$). On the other hand, if $f \in \mathbb{Z}[x]$, $p \in \mathcal{P}$, and $\alpha \in \mathbb{F}_p$ is a point of period n of $(\mathbb{F}_p, [f]_p)$, then α is a root of $[f^n(x) - x]_p$; thus, there are no more than $n^{-1} \cdot \deg(f^n)$ n-cycles in $(\mathbb{F}_p, [f]_p)$. (In fact, something more is true: all points of period n in $(\mathbb{F}_p, [f]_p)$ are roots of the nth dynatomic polynomial of $[f]_p$; we review the theory of dynatomic polynomials in Section 2.2.)

In Theorem 4.4 we compute the cycle statistics of the family $[x^k + a]_{\mathcal{P}}$ for any $k \in \mathbb{Z}_{\geq 2}$ and most $a \in \mathbb{Z}$. In particular, we obtain the following corollary, which relates these statistics to those discovered by Gončarov.

Corollary 1.2. *For any $k \in \mathbb{Z}_{\geq 2}$ and $n \in \mathbb{Z}_{\geq 1}$, there is a probability distribution ${}_k\omega_n \colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ and a thin set*[1] *$\mathcal{A}_{k,n} \subseteq \mathbb{Z}$ such that for all $a \in \mathbb{Z} \smallsetminus \mathcal{A}_{k,n}$,*

- *for all $j \in \mathbb{Z}_{\geq 0}$,*

$$ {}_k\omega_n(j) = \delta\left(\left\{p \in \mathcal{P} \,\middle|\, \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } j \text{ } n\text{-cycles}\right\}\right)$$

  and
- *there is an explicit constant $r_k(n) \in \mathbb{Z}_{\geq 1}$ such that for all $m \in \mathbb{Z}_{\geq 0}$,*
  - *if $m \leq r_k(n)$, the mth moment of the distributions ${}_k\omega_n$ and μ_n are the same and*
  - *if $m > r_k(n)$, the mth moment of ${}_k\omega_n$ is less than the mth moment of μ_n.*

For any $a \in \mathbb{Z}$, the integer $nr_k(n)$ is the degree of the nth dynatomic polynomial of f, so $r_k(n)$ is the maximum possible number of cycles of length n in $\left(\mathbb{F}_p, \left[x^k + a\right]_p\right)$. See Definition 2.1 for more details. In particular, we have the inequality $n^{-1}k^{n-1} < r_k(n) < n^{-1}k^n$.

[1] See Remark 4.2 for a discussion of thin sets and their sizes.

Remark 1.3. As pointed out in Remark 1.1, for any $k \in \mathbb{Z}_{\geq 2}$ and $n \in \mathbb{Z}_{\geq 1}$, we know that ${}_k\omega_n(j) = 0$ for all $j > r_k(n)$. Since the matrix $(i^j)_{1\leq i,j\leq r_k(n)}$ is invertible, we know that there is at most one distribution $\omega\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}$ with the property that for all $m \in \{0, 1, \ldots, r_k(n)\}$, the mth moments of ω and μ_n are the same. In other words, Corollary 1.2 is the statement that for most $a \in \mathbb{Z}$, the cycle distribution of $[x^k + a]_{\mathcal{P}}$ is *as random as possible*.

The organization of this paper is as follows: we begin with some background in Section 2; in particular, we recall Pollard's algorithm and introduce the theory of dynatomic polynomials. Afterwards, in in Section 3, we define and study a family of distributions $\{\omega_{n,r}\}_{n,r\in\mathbb{Z}_{\geq 1}}$ containing the distributions mentioned in Corollary 1.2 as a subfamily. In Theorem 3.3, we compute all their moments. Then, in Theorem 3.6, we prove precise estimates for them; this theorem generalizes Theorem 3.5 of [BG17], which estimates only $\omega_{n,r}(0)$. In Section 4.1 we prove the aforementioned Theorem 4.4, obtaining Corollary 1.2 as an immediate consequence. Next, in Section 4.2 we apply our results to prove a version of Conjecture 2.2 of [MSSS], which concerns the statistics of $\bigcup_{a\in\mathbb{Z}} [x^2 + a]_{\mathcal{P}}$. This conjecture asserts in particular that

$$\left|\left\{a \in [p] \,\middle|\, \left(\mathbb{F}_p, \left[x^2 + a\right]_p\right) \text{ has precisely one cycle}\right\}\right| = O\left(\sqrt{p}\right).$$

Our result is Theorem 4.7, which we prove in Section 4.2.

Theorem 4.7. If $k \in \mathbb{Z}_{\geq 2}$ and $J \in \mathbb{Z}_{\geq 1}$, then for any $\epsilon \in \mathbb{R}_{>0}$, there exists a thin set $\mathcal{A}_{k,J,\epsilon} \subseteq \mathbb{Z}$ such that for all $a \in \mathbb{Z} \smallsetminus \mathcal{A}_{k,J,\epsilon}$,

$$\overline{\delta}\left(\left\{p \in \mathcal{P} \mid \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has } J \text{ or fewer cycles}\right\}\right) < \epsilon.$$

Note that Theorem 4.7 addresses the presence of arbitrarily many cycles, for fixed unicritical polynomials of arbitrarily large degree.

Additionally, in Section 4 we introduce a family of cycle densities on the set of *all* monic binomial unicritical polynomials in $\mathbb{Z}[x]$. In Theorem 4.5 and Corollary 4.9, we prove in particular that

- for all $k \in \mathbb{Z}_{\geq 2}$ and $n \in \mathbb{Z}_{\geq 1}$

$$\lim_{X\to\infty} \frac{1}{2X+1} \sum_{a=-X}^{X} \delta\left(\left\{p \in \mathcal{P} \,\middle|\, \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } j \text{ } n\text{-cycles}\right\}\right) = {}_k\omega_n(j),$$

  and
- for all $k \in \mathbb{Z}_{\geq 2}$, $J \in \mathbb{Z}_{\geq 1}$, and $\epsilon \in \mathbb{R}_{>0}$, there exists $N \in \mathbb{Z}_{\geq 1}$ such that for all $n \in \mathbb{Z}_{\geq N}$,

$$\lim_{X\to\infty} \frac{1}{2X+1} \sum_{a=-X}^{X} \delta\left(\left\{p \in \mathcal{P} \,\middle|\, \substack{\left(\mathbb{F}_p, \left[x^k+a\right]_p\right) \text{ has } J \text{ or fewer cycles} \\ \text{of length at most } n}\right\}\right) < \epsilon.$$

The latter fact implies that there is an increasing function $\gamma\colon \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ such that

$$\lim_{J\to\infty} \frac{1}{2\gamma(J)+1} \sum_{a=-\gamma(J)}^{\gamma(J)} \delta\left(\left\{p \in \mathcal{P} \,\middle|\, \substack{\left(\mathbb{F}_p, \left[x^k+a\right]_p\right) \text{ has } J \text{ or fewer cycles} \\ \text{of length at most } \gamma(J)}\right\}\right) = 0.$$

We conclude the paper with a conjecture on the growth rate of γ.

2. Background

2.1. **Pollard's rho algorithm and randomness.** In [Pol75], Pollard presented his famous "rho algorithm" for integer factorization, which was the first algorithm to factor the Fermat number $2^{256}+1$, see [BP81]. A conjectural termination time of this algorithm relies upon an aspect of the supposed "randomness" of $[x^2+1]_{\mathcal{P}}$. To better state this conjecture, we introduce a bit more notation. For any dynamical system (S,f) and $s \in S$, we let

$$\mathbf{O}_{(S,f)}(s) = \left|\{f^n(s) \mid n \in \mathbb{Z}_{\geq 0}\}\right|.$$

(If $\{f^n(s) \mid n \in \mathbb{Z}_{\geq 0}\}$ is infinite, we write $\mathbf{O}_{(S,f)}(s) = \infty$.) Now, letting $g = x^2+1$, then the conjecture that

$$\mathbf{O}_{(\mathbb{F}_p,[g]_p)}(0) = O\left(\sqrt{p}\right)$$

implies that there is some $C \in \mathbb{R}_{>0}$ such that Pollard's algorithm, applied to any positive composite integer m, terminates in at most

$$C\sqrt{\min\left(\{p \in \mathcal{P} \mid p \text{ divides } m\}\right)}$$

steps. This conjecture formalizes the hope that for all $p \in \mathcal{P}$, the "time to first repeat" of $[g]_p$ (acting on $0 \in \mathbb{F}_p$) is the same as that of a random self-map on a set of size p, which is well-known and classical; indeed,

$$\frac{1}{\left|[X]^{[X]}\right|} \sum_{f \in [X]^{[X]}} \mathbf{O}_{([X],f)}(0) = O\left(\sqrt{X}\right).$$

This conjecture provides motivation for the question mentioned in Section 1: what properties do families of polynomials share with random maps? See [BGH+13, Sil08] for further analysis of the "random map" model in arithmetic dynamics and its limitations, and [FO90] for an extensive presentation of the statistics of random mappings (also [Har60, Ste69, AB82]).

There has been quite a bit of recent work on this question, both for the families

$$[f]_{\mathcal{P}}, \quad \text{for } f \in \mathbb{Z}[x],$$

and the families

$$\bigcup_{\substack{f \in \mathbb{Z}[x] \\ \deg f = k}} [f]_{\mathcal{P}}, \quad \text{for } k \in \mathbb{Z}_{\geq 2}.$$

For the latter case, see [FG14], [BS17], [BGTW18], and in particular [Bac91], who proved that for any $N \in \mathbb{Z}_{\geq 1}$, there is a constant $C_N \in \mathbb{R}_{>0}$ with the property that for all $p \in \mathcal{P}$,

$$\frac{1}{p^2} \sum_{\alpha \in \mathbb{F}_p} \left|\left\{\beta \in \mathbb{F}_p \mid \mathbf{O}_{(\mathbb{F}_p, x^2+\alpha)}(\beta) \leq N\right\}\right| > \frac{1}{p}\binom{N}{2} + C_N p^{-\frac{3}{2}}.$$

In the former case, Juul, Kurlberg, Madhu, and Tucker prove in [JKMT16] that if $f = x^k + a$, with $k \in \mathbb{Z}_{\geq 2}$ and $a \in \mathbb{Z}$, and f is not conjugate to the Chebyshev polynomial $x^2 - 2$, then

$$\liminf_{p \to \infty} \left(\frac{1}{p} \cdot \left|\{\alpha \in \mathbb{F}_p \mid \alpha \text{ periodic in } (\mathbb{F}_p, [f]_p)\}\right|\right) = 0.$$

In [HB17], Heath-Brown computed explicit bounds on periodic points of a family of dynamical systems; indeed, for any $a, c \in \mathbb{Z}_{\geq 1}$, he showed that

$$\left|\left\{\alpha \in \mathbb{F}_p \mid \alpha \text{ periodic in } \left(\mathbb{F}_p, [ax^2 + c]_p\right)\right\}\right| = O_{a,c}\left(\frac{p}{\log\log p}\right).$$

Both Bach and Heath-Brown obtain their results by using classical point-counting techniques (such as Weil's "Riemann Hypothesis" and Bezout's Theorem) to study the curves $([f]_p)^n(x) = ([f]_p)^n(y)$, for $f \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}_{\geq 1}$. On the other hand, Juul et. al. use the "arboreal Galois theory" pioneered by Odoni [Odo85], and elaborated upon by Boston, Jones, and many others [BJ07]. This theory analyzes Galois groups of polynomials of the form $f^n(x) - a$ for $f \in \mathbb{Q}[x]$ and $a \in \mathbb{Q}$.

To analyze the cycle structure of periodic points of dynamical system, we use the Galois theory of dynatomic polynomials, which we now recall.

2.2. **Dynatomic polynomials.** As we intend to study the cycle structure of dynamical systems induced by polynomials, we will make use of the theory of dynatomic polynomials (and their Galois groups). See [MP94], [Mor96] (and the correction in [Mor11]), [Mor98], and [Sil07, Chapter 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 $d \in \mathbb{Z}_{\geq 1}$ and $d \mid n$, then this polynomial vanishes on points of period d as well (for example, if $\alpha \in K$ is a fixed point of (K, f), i.e. $f(\alpha) = \alpha$, then $f^n(\alpha) = \alpha$ for all $n \in \mathbb{Z}_{\geq 1}$). In an attempt to sieve out the points of lower period, one defines the nth *dynatomic polynomial of* f for any $n \in \mathbb{Z}_{\geq 1}$:

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

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

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

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. (It turns out that $\Phi_{f,n}$ may occasionally vanish on points of period d for $d < n$: see [Sil07, Example 4.2]. Luckily, Proposition 4.1 addresses this inconvenience.) We should mention that it is not *a priori* obvious that $\Phi_{f,n}$ is a polynomial. See [MP94, 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 $n \in \mathbb{Z}_{\geq 1}$ and $k \in \mathbb{Z}_{\geq 2}$, define $r_k(n)$ to be the positive integer such that $n \cdot r_k(n)$ is the degree (in x) of the nth dynatomic polynomial of $x^k + c \in \mathbb{Q}(c)[x]$; that is,

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

Remark 2.2. For any $n \in \mathbb{Z}_{\geq 1}$ and $k \in \mathbb{Z}_{\geq 2}$, the quantity $r_k(n)$ is quite large compared to n; indeed, for all such n and k,

$$\frac{k^{n-1}}{n} < r_k(n) < \frac{k^n}{n}.$$

Our proofs of Theorem 4.7 and Theorem 4.4 rely in part on the knowledge of the structure of the Galois groups of $\Phi_{f,n}$, where $n \in \mathbb{Z}_{\geq 1}$ and $f(x) = x^k + a \in \mathbb{Z}[x]$ for $k \in \mathbb{Z}_{\geq 2}$ and $a \in \mathbb{Z}$. 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 [Mor98]—the Galois groups of $\Phi_{f,n}$ for $f(x) = x^k + c \in \mathbb{Q}(c)[x]$ are known. To state Morton's Theorem, we introduce a bit more notation. If $f = f(x) = x^k + c \in \mathbb{Q}(c)[x]$ and $n \in \mathbb{Z}_{\geq 1}$, let

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

Note that $K_{f,n}$ is the compositum of the fields in $\{\Sigma_{f,d} \mid d \in \mathbb{Z}_{\geq 1} \text{ and } d \mid n\}$.

We now have most of the notation to state Morton's Theorem. We postpone the discussion of wreath products (which appear in Morton's Theorem as $C_d \wr S_{r_k(d)}$) and their natural action (on the sets $B(n, r_k(n))$) until Section 3, which immediately follows the statement of the theorem; there, we will introduce wreath products and their actions, then discuss them in detail. The following theorem combines results from [Mor98].

Morton's Theorem. *Let $k \in \mathbb{Z}_{\geq 2}$, $n \in \mathbb{Z}_{\geq 1}$, and $f = f(x) = x^k + c \in \mathbb{Q}(c)[x]$. Next, set $\mathcal{S} = \{\Sigma_{f,d} \mid d \in \mathbb{Z}_{\geq 1} \text{ and } d \mid n\}$. Then $f^n(x) - x$ has no repeated roots, and if $\Sigma_{f,d} \in \mathcal{S}$, then*

- *the field $\Sigma_{f,d}$ is linearly disjoint from the compositum of the fields in $\mathcal{S} \smallsetminus \{\Sigma_{f,d}\}$,*
- *the roots of $\Phi_{f,d}$ are precisely the points of period d in the dynamical system $(\Sigma_{f,d}, f)$,*
- *$\mathrm{Gal}(\Sigma_{f,d}/\mathbb{Q}(c)) \simeq C_d \wr S_{r_k(d)}$, and*
- *the action of $\mathrm{Gal}(\Sigma_{f,d}/\mathbb{Q}(c))$ on the points of period d in the dynamical system $(\Sigma_{f,d}, f)$ matches the action of $C_d \wr S_{r_k(d)}$ on $B(d, r_k(d))$.*

3. Fixed points in wreath product actions

In this section, we study the statistics of fixed-point proportions in a family of wreath products. This family includes the groups that appear as Galois groups of dynatomic polynomials, so these statistics are a vital component of our proofs of Theorem 4.4 and Theorem 4.7. We begin with some definitions.

Suppose that $r \in \mathbb{Z}_{\geq 1}$. For any group G, we write $G \wr S_r$ to mean the wreath product $G \wr_{\{1,\dots,r\}} S_r$. 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 [Isa08, Chapter 3A] for background on wreath products. For any $n \in \mathbb{Z}_{\geq 1}$, we let C_n denote the cyclic group of size n; we then write $B(n, r)$ for the set $C_n \times \{1, \dots, r\}$. The group $C_n \wr S_r$ acts naturally on $B(n, r)$; concretely, for any $\sigma = ((\zeta_1, \dots, \zeta_r), \pi) \in C_n \wr S_r$, this action is given by

$$\begin{aligned} \sigma \colon B(n,r) &\to B(n,r) \\ (\zeta, i) &\mapsto (\zeta_i \cdot \zeta, \pi(i)). \end{aligned}$$

For any $\sigma \in C_n \wr S_r$, define

$$\mathrm{Fix}\,\sigma = \left\{(\zeta, i) \in B(n,r) \;\middle|\; \sigma(\zeta, i) = (\zeta, i)\right\}.$$

Observe that n divides $|\mathrm{Fix}\,\sigma|$—this follows from the fact that if σ fixes any $(\zeta_0, i) \in B(n, r)$, then it must fix each (ζ, i) for all $\zeta \in C_n$. With this fact in mind, we now define the random variable $\mathbf{W}_{n,r}$ on $C_n \wr S_r$ by

$$\begin{aligned} \mathbf{W}_{n,r} \colon C_n \wr S_r &\to \mathbb{Z}_{\geq 0} \\ \sigma &\mapsto \frac{1}{n} \cdot |\mathrm{Fix}\,\sigma|. \end{aligned}$$

Note that the random variable $n \cdot \mathbf{W}_{n,r}$ is the permutation character of the action of $C_n \wr S_r$ on $B(n,r)$. We will denote the probability distribution associated to $\mathbf{W}_{n,r}$ by $\omega_{n,r}$; concretely,

$$\begin{aligned} \omega_{n,r} \colon \mathbb{Z}_{\geq 0} &\to \mathbb{R}_{\geq 0} \\ j &\mapsto \frac{\left|\left\{\sigma \in C_n \wr S_r \,\middle|\, |\operatorname{Fix}\sigma| = jn\right\}\right|}{|C_n \wr S_r|}. \end{aligned}$$

Section 3.1 is devoted to computing the moments of $\mathbf{W}_{n,r}$. Then, Section 3.2 computes useful bounds on $\omega_{n,r}$. These bounds generalize Theorem 3.5 of [BG17]; in Section 4.2 we apply these bounds to prove Theorem 4.7.

3.1. **Moments of permutation characters.** In this section, we compute the moments of the distributions $\omega_{n,r}$. Recall that if ω is a discrete probability distribution on $\mathbb{Z}_{\geq 0}$, the *mth moment* of ω is

$$\sum_{j=0}^{\infty} j^m \omega(j);$$

we denote the mth moment of a probability distribution ω by $\mathbb{M}_m(\omega)$. If $\mathbf{X}$ is a random variable with codomain $\mathbb{Z}_{\geq 0}$, we will write $\mathbb{M}_m(\mathbf{X})$ for the moment of the probability distribution associated to $\mathbf{X}$. The moments of the Poisson distribution are well known; they are expressed in terms of Stirling numbers of the second kind. For any $m, i \in \mathbb{Z}_{\geq 0}$, the *Stirling number of the second kind* is the number of ways of partitioning a set of m elements into i distinct nonempty subsets; we denote this number by $\left\{ {m \atop i} \right\}$. By convention we take

$$\left\{ {m \atop 0} \right\} = \begin{cases} 1 & \text{if } m = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Fact 3.1. For all $\lambda \in \mathbb{R}_{>0}$ and $m \in \mathbb{Z}_{\geq 0}$,

$$\mathbb{M}_m(\rho_\lambda) = \sum_{i=0}^{m} \left\{ {m \atop i} \right\} \lambda^i.$$

We now turn to computing the moments of $n \cdot \mathbf{W}_{n,r}$ for any $n, r \in \mathbb{Z}_{\geq 0}$; before proceeding, we prove a combinatorial identity involving Stirling numbers.

Lemma 3.2. *If $m \in \mathbb{Z}_{\geq 1}$ and $i \in \mathbb{Z}_{\geq 0}$, then*

$$\sum_{\ell=i}^{m-1} \binom{m-1}{\ell} \left\{ {\ell \atop i} \right\} = \left\{ {m \atop i+1} \right\}.$$

Proof. For any $\ell \in \{1, \ldots, m-1\}$, the number of ways to choose a subset of $\{1, \ldots, m-1\}$ of size ℓ and partition it into i nonempty subsets is $\binom{m-1}{\ell} \left\{ {\ell \atop i} \right\}$. These choices are in bijection with partitions of $\{1, \ldots, m\}$ into $i+1$ nonempty subsets with the condition that the subset containing m is of size $m - \ell$. Summing over ℓ yields the result. □

We now have the tools to use character theory to compute the moments of $n \cdot \mathbf{W}_{n,r}$; the moments of $\mathbf{W}_{n,r}$ will follow as an immediate corollary.

Theorem 3.3. *Let $m \in \mathbb{Z}_{\geq 0}$. For all $n, r \in \mathbb{Z}_{\geq 1}$,*

$$\mathbb{M}_m(n \cdot \mathbf{W}_{n,r}) = \sum_{i=0}^{\min(\{m,r\})} \left\{ {m \atop i} \right\} n^{m-i}$$

Proof. We induct on m. The $m = 0$ case is trivial and the $m = 1$ case follows immediately from Burnside's Lemma: indeed, $C_n \wr S_r$ acts transitively on $B(n,r)$, so

$$\frac{1}{|C_n \wr S_r|} \cdot \sum_{\sigma \in C_n \wr S_r} n \cdot \mathbf{W}_{n,r}(\sigma) = 1 = \left\{ {1 \atop 1} \right\} n^0.$$

Now assume that $m \geq 2$ and that the statement of the theorem is true for every $\ell \in \{0, \ldots, m-1\}$. Choose any $n, r \in \mathbb{Z}_{\geq 1}$ and any $\alpha \in B(n,r)$. To ease notation, let

- $W = C_n \wr S_r$,
- $\chi = n \cdot \mathbf{W}_{n,r}$,
- $W_\alpha = \{\sigma \in W \mid \alpha \in \operatorname{Fix} \sigma\}$, the isotropy subgroup of α,
- χ_α be the restriction of χ to W_α, and
- $\mathbb{1}_\alpha$ be the principal character of W_α.

Additionally, let $\langle \cdot, \cdot \rangle$ be the usual inner product of class functions. Since χ is the permutation character of the action of W on $B(n,r)$, we know that χ is induced from $\mathbb{1}_\alpha$; see [Isa06, Lemma 5.14]. That is, $\chi = (\mathbb{1}_\alpha)^W$. By Frobenius reciprocity, we compute

$$\mathbb{M}_m(n \cdot \mathbf{W}_{n,r}) = \frac{1}{|W|} \sum_{\sigma \in W} \chi^m(\sigma) = \left\langle \chi^{m-1}, \chi \right\rangle = \left\langle \chi^{m-1}, (\mathbb{1}_\alpha)^W \right\rangle = \left\langle (\chi_\alpha)^{m-1}, \mathbb{1}_\alpha \right\rangle.$$

Observe that if $\alpha = (\zeta, i)$, then W_α acts trivially on the n elements of $C_n \times \{i\}$ and acts transitively on the remaining elements in $B(n,r)$, if there are any. There are two cases.

- If $r \geq 2$, the preceding observation implies both that we can restrict the action of W_α to an action on $B(n,r) \setminus (C_n \times \{i\})$ as well as that $W_\alpha \simeq C_n \wr S_{r-1}$. If we let ψ be the permutation character of this restricted action, then the induction hypothesis implies that for all $\ell \in \{0, \ldots, m-1\}$,

$$\frac{1}{|W_\alpha|} \sum_{\sigma \in W_\alpha} \psi^\ell(\sigma) = \mathbb{M}_\ell(n \cdot \mathbf{W}_{n,r-1}) = \sum_{i=0}^{\min(\{r-1,\ell\})} \left\{ {\ell \atop i} \right\} n^{\ell - i}.$$

- On the other hand, if we are in the case where $r = 1$, then W_α is the trivial group. In this case, we let ψ be the trivial class function of W_α—that is, ψ evaluates to zero on the single element of W_α. We adopt the convention that $\psi^0 = \mathbb{1}_\alpha$, so that for all $\ell \in \{0, \ldots, m-1\}$,

$$\frac{1}{|W_\alpha|} \sum_{\sigma \in W_\alpha} \psi^\ell(\sigma) = \sum_{i=0}^{\min(\{r-1,\ell\})} \left\{ {\ell \atop i} \right\} n^{\ell - i},$$

as in the previous case.

In either case, note that $\chi_\alpha = n\mathbb{1}_\alpha + \psi$. Thus,

$$\begin{aligned}
\left\langle (\chi_\alpha)^{m-1}, \mathbb{1}_\alpha \right\rangle &= \left\langle (n\mathbb{1}_\alpha + \psi)^{m-1}, \mathbb{1}_\alpha \right\rangle \\
&= \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} n^{m-1-\ell} \left\langle \mathbb{1}_\alpha, \psi^\ell \right\rangle && \text{since } \psi^0 = \mathbb{1}_\alpha \\
&= \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} n^{m-1-\ell} \left(\frac{1}{|W_\alpha|} \sum_{\sigma \in W_\alpha} \psi^\ell(\sigma) \right) && \text{by definition of } \langle \cdot, \cdot \rangle \\
&= \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} n^{m-1-\ell} \sum_{i=0}^{\min(\{r-1,\ell\})} \left\{ \begin{matrix} \ell \\ i \end{matrix} \right\} n^{\ell-i} && \text{by the induction hypothesis} \\
&= \sum_{i=0}^{\min(\{r-1,m-1\})} n^{m-1-i} \sum_{\ell=i}^{m-1} \binom{m-1}{\ell} \left\{ \begin{matrix} \ell \\ i \end{matrix} \right\} \\
&= \sum_{i=0}^{\min(\{r-1,m-1\})} n^{m-1-i} \left\{ \begin{matrix} m \\ i+1 \end{matrix} \right\} && \text{by Lemma 3.2} \\
&= \sum_{i=0}^{\min(\{r,m\})} \left\{ \begin{matrix} m \\ i \end{matrix} \right\} n^{m-i},
\end{aligned}$$

completing the proof. □

Corollary 3.4. *If $n, r \in \mathbb{Z}_{\geq 1}$, then for all $m \in \mathbb{Z}_{\geq 0}$,*

$$\mathbb{M}_m(\mathbf{W}_{n,r}) = \sum_{i=0}^{\min(\{m,r\})} \left\{ \begin{matrix} m \\ i \end{matrix} \right\} n^{-i}.$$

In particular, if $m \leq r$, then

$$\mathbb{M}_m(\omega_{n,r}) = \mathbb{M}_m\left(\rho_{1/n}\right).$$

Proof. Immediate from Theorem 3.3 and Fact 3.1. □

Remark 3.5. In [CM12], the authors also studied the moments of the distributions $\omega_{n,r}$ in the context of an application of their main results on moment generating functions. However, their computation of the moments of $\omega_{n,r}$ contains an error: they state that $\mathbb{M}_m(\omega_{n,r}) = \mathbb{M}_m(n \cdot \mathbf{W}_{n,r}) = \sum_{i=0}^{r} \left\{ \begin{matrix} m \\ i \end{matrix} \right\} n^{m-i}$, but this equality only holds when $m \leq r$. Our methods are entirely different, relying instead on character theory.

3.2. **Bounds on fixed point probabilities in wreath products.** Having computed the moments of $\omega_{n,r}$ for all $n, r \in \mathbb{Z}_{\geq 1}$, we now bound $\omega_{n,r}(j)$ for any $j \in \mathbb{Z}_{\geq 0}$. Before proceeding, we introduce a bit of notation. For any $r \in \mathbb{Z}_{\geq 1}$ and $i \in \{0, \ldots, r\}$, let $D_{r,i}$ be the (r,i)th rencontres number; i.e. the number of permutations in S_r with exactly i fixed points. For convenience, we set $D_{0,0} = 1$. Note that $D_{r,0}$ is the number of derangements in S_r.

Theorem 3.6. *Let $k \in \mathbb{Z}_{\geq 2}$ and $r, n \in \mathbb{Z}_{\geq 1}$. For any $j \in \mathbb{Z}_{\geq 0}$, if $j \leq r$, then*

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

If $j > r$, then $\omega_{n,r}(j) = 0$.

Proof. If $j > r$, the result is trivial, so suppose that $j \leq r$. Choose $\sigma = ((\zeta_1, \ldots, \zeta_r), \pi) \in C_n \wr S_r$. Note that if $|\operatorname{Fix} \sigma| = nj$, then π—acting on $\{1, \ldots, r\}$—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 $\zeta_{i'} = 1$.

Using this fact, and enumerating permutations π by their number of fixed points, we conclude that

$$|\{\sigma \in C_n \wr S_r \mid |\mathrm{Fix}\,\sigma| = nj\}| = \sum_{i=0}^{r} \binom{i}{j} D_{r,i}(n-1)^{i-j} n^{r-i}.$$

Now, for any $i \in \mathbb{Z}_{\geq 0}$ it is simple to show $D_{r,i} = \binom{r}{i} D_{r-i,0}$ (see [BG17, Lemma 3.4]), so we see

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

Next, recall the well-known fact that for any $i \in \mathbb{Z}_{\geq 0}$, the $(i,0)$th rencontres number $D_{i,0}$ satisfies $\frac{i!}{e} - 1 < D_{i,0} < \frac{i!}{e} + 1$. Thus,

$$\left| \omega_{n,r}(j) - \frac{1}{r! n^j e} \sum_{i=j}^{r} \binom{i}{j} \binom{r}{i} (r-i)! \left(\frac{n-1}{n}\right)^{i-j} \right| < \frac{1}{r! n^j} \sum_{i=j}^{r} \binom{i}{j} \binom{r}{i} \left(\frac{n-1}{n}\right)^{i-j}.$$

We will address the approximation and error terms in turn.

- Approximating the Taylor series remainder of the approximation, we see that

$$\begin{aligned} \frac{1}{r! n^j e} \sum_{i=j}^{r} \binom{i}{j} \binom{r}{i} (r-i)! \left(\frac{n-1}{n}\right)^{i-j} &= \frac{1}{j! n^j e} \sum_{i=j}^{r} \frac{1}{(i-j)!} \left(\frac{n-1}{n}\right)^{i-j} \\ &= \frac{1}{j! n^j e} \sum_{i=0}^{r-j} \frac{1}{i!} \left(\frac{n-1}{n}\right)^{i} \\ &< \frac{e^{-1/n}}{j! n^j} + \frac{1}{j! n^j e \cdot (r-j+1)!}. \end{aligned}$$

- As for the error term, we certainly know that

$$\left(1 + \frac{n-1}{n}\right)^{r-j} < 2^{r-j},$$

so the binomial theorem implies

$$\begin{aligned} \frac{1}{r! n^j} \sum_{i=j}^{r} \binom{i}{j} \binom{r}{i} \left(\frac{n-1}{n}\right)^{i-j} &= \frac{1}{j! n^j} \sum_{i=j}^{r} \frac{1}{(i-j)!(r-i)!} \left(\frac{n-1}{n}\right)^{i-j} \\ &= \frac{1}{j! n^j (r-j)!} \sum_{i=0}^{r-j} \binom{r-j}{i} \left(\frac{n-1}{n}\right)^{i} \\ &< \frac{2^{r-j}}{j! n^j (r-j)!}. \end{aligned}$$

Thus, the theorem is true. □

For our applications, we must estimate those wreath products occurring as Galois groups of dynatomic polynomials, so we introduce the following notation.

Definition 3.7. For any $k \in \mathbb{Z}_{\geq 2}$ and $n \in \mathbb{Z}_{\geq 1}$, let ${}_k\omega_n := \omega_{n,r_k(n)}$. (Recall that $nr_k(n)$ is the degree of the nth dynatomic polynomial of $x^k + c \in \mathbb{Q}(c)[x]$, see Definition 2.1.)

For any $k \in \mathbb{Z}_{\geq 2}$ and $j \in \mathbb{Z}_{\geq 0}$, the sequence $\{{}_k\omega_n(j)\}_{n \in \mathbb{Z}_{\geq 1}}$ has particularly stable behavior as $n \to \infty$; we now record this behavior for use in the proof of Theorem 4.7 in Section 4.2.

Corollary 3.8. *If $k \in \mathbb{Z}_{\geq 2}$ and $j \in \mathbb{Z}_{\geq 0}$, then*

$$ {}_k\omega_n(j) = \frac{e^{-1/n}}{j!n^j} + O\left(\frac{2^{r_k(n)-j}}{(r_k(n)-j)!}\right). $$

In particular,

$$ {}_k\omega_n(j) = \frac{1}{j!n^j}\left(1 - \frac{1}{n}\right) + O\left(\frac{1}{n^{j+2}}\right). $$

Proof. This follows immediately from Theorem 3.6, Remark 2.2, and Taylor's Theorem. □

4. The cycle structure of unicritical polynomials

Before proving Theorem 4.4 and Theorem 4.7, we recall three important results, in the forms which will be most useful for the remainder of the paper. In this section, for any polynomial $f = f(c,x) \in \mathbb{Q}[c][x]$ and any $a \in \mathbb{Q}$, we will write f_a for the specialization of f at $c = a$; that is, $f_a = f_a(x) = f(a,x) \in \mathbb{Q}[x]$.

The first result addresses the following inconvenience: for any $f \in \mathbb{Z}[x]$, $n \in \mathbb{Z}_{\geq 1}$, and $p \in \mathcal{P}$, the polynomial $[\Phi_{f,n}]_p$ certainly vanishes on the period n points of $(\mathbb{F}_p, [f]_p)$, but, as discussed in [BG17], it occasionally vanishes at points of lower period as well (indeed this can happen even in characteristic 0—see [Sil07, Example 4.2]). Luckily, as long as $f^n(x) - x$ has distinct roots, this pathology can only occur for finitely many $p \in \mathcal{P}$. We record this fact as Proposition 4.1.

Proposition 4.1. *Let $f \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}_{\geq 1}$, and suppose that $f^n(x) - x$ has no repeated roots. If $j \in \mathbb{Z}_{\geq 0}$, then for all but finitely many $p \in \mathcal{P}$,*

$$ (\mathbb{F}_p, [f]_p) \text{ has precisely } j \text{ } n\text{-cycles} \quad \text{if and only if} \quad [\Phi_{f,n}]_p \text{ has precisely } jn \text{ roots in } \mathbb{F}_p. $$

Proof. This is a trivial generalization of [BG17, Corollary 4.3], which follows from [Sil07, Theorem 4.5]. □

Next, we state the forms of the Hilbert Irreducibility Theorem and Frobenius Density Theorem which will be most useful to us in the following sections.

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" $\mathcal{A} \subset \mathbb{Z}$ such that for all $a \in \mathbb{Z} \smallsetminus \mathcal{A}$,*

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

Remark 4.2. For details on the connection between the Hilbert Irreducibility Theorem and Galois theory, see, for example, [Coh81], [Lan83, Chapter VIII], and [Völ96, Chapter 1].

As for the size of "thin" sets, for any thin set $\mathcal{A}$ there is some constant $C_{\mathcal{A}} \in \mathbb{R}_{>0}$ such that for all $X \in \mathbb{Z}_{\geq 0}$,

$$ |\{a \in \mathcal{A} \mid -X \leq a \leq X\}| \leq C_{\mathcal{A}}\sqrt{X}. $$

(See [Ser97], Section 9.7, for more details).

Frobenius Density Theorem. *Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic polynomial with no repeated roots, and fix any $j \in \mathbb{Z}_{\geq 0}$. Let $G = \mathrm{Gal}(f/\mathbb{Q})$ and $P \subseteq \mathcal{P}$ be the set of primes p such that $[f]_p$ has exactly j roots in $\mathbb{F}_p$. Then*

$$ \delta(P) = \frac{1}{|G|} \cdot |\{\sigma \in G \mid \sigma \text{ fixes exactly } j \text{ roots of } f\}|. $$

(See [SL96] for more details on this theorem.)

Remark 4.3. We will use this theorem in the following form. Fix any finite sets $\mathcal{M},\mathcal{N}$ such that $\mathcal{N}\subseteq\mathcal{M}\subseteq\mathbb{Z}_{\geq 1}$. Suppose that for all $m\in\mathcal{M}$ there exist monic polynomials $f_m\in\mathbb{Z}[x]$, with splitting fields K_m and Galois groups $G_m=\mathrm{Gal}(K_d/\mathbb{Q})$. Suppose that $\prod_{m\in\mathcal{M}} f_m$ has no repeated roots and for any $m\in\mathcal{M}$, the field K_m is linearly disjoint from the compositum of $\{K_{m'}\mid m'\in\mathcal{M}\smallsetminus\{m\}\}$. Then for any function $\varphi\colon\mathcal{N}\to\mathbb{Z}_{\geq 0}$,

$$\delta\left(\bigcap_{i\in\mathcal{N}}\left\{p\in\mathcal{P}\mid [f_i]_p \text{ has precisely } \varphi(i) \text{ roots in } \mathbb{F}_p\right\}\right) = \prod_{i\in\mathcal{N}}\frac{1}{|G_i|}\cdot\left|\{\sigma\in G_i\mid \sigma \text{ fixes exactly } \varphi(i) \text{ roots of } f_i\}\right|.$$

4.1. **How random is the cycle structure of unicritical polynomials?** We now prove our main theorem about the distribution of cycles in $[x^k+a]_{\mathcal{P}}$, for $k\in\mathbb{Z}_{\geq 2}$ and most $a\in\mathbb{Z}$. Afterwards, we deduce a density result that encompasses *all* integers $a\in\mathbb{Z}$.

Theorem 4.4. *If $k\in\mathbb{Z}_{\geq 2}$ and $\mathcal{N}$ is a finite subset of $\mathbb{Z}_{\geq 1}$, then there is a thin set $\mathcal{A}_{k,\mathcal{N}}$ with the property that for any $a\in\mathbb{Z}\smallsetminus\mathcal{A}_{k,\mathcal{N}}$ and any function $\varphi\colon\mathcal{N}\to\mathbb{Z}_{\geq 0}$,*

$$\delta\left(\left\{p\in\mathcal{P}\mid \text{for all } i\in\mathcal{N},\ \left(\mathbb{F}_p,\left[x^k+a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right)=\prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i)).$$

In particular, if $a\in\mathbb{Z}\smallsetminus\mathcal{A}_{k,\mathcal{N}}$ and $i\in\mathcal{N}$, then for all $j\in\mathbb{Z}_{\geq 0}$,

$$\delta\left(\left\{p\in\mathcal{P}\mid \left(\mathbb{F}_p,\left[x^k+a\right]_p\right) \text{ has precisely } j\ i\text{-cycles}\right\}\right)={}_k\omega_i(j).$$

Proof. Choose any $N_0>\max(\mathcal{N})$, let $N=N_0!$, and let let $\mathcal{N}_0$ be the set of positive integer divisors of N, so that $\mathcal{N}\subseteq\mathcal{N}_0$. Set $f=x^k+c\in\mathbb{Q}(c)[x]$, so that if $a\in\mathbb{Z}$, then $f_a=x^k+a\in\mathbb{Z}[x]$. Next, for any such a, let

$$\mathcal{F}(a)=\{\Sigma_{f_a,d}\mid d\in\mathcal{N}_0\}.$$

By Morton's Theorem and the Hilbert Irreducibility Theorem, there exists a thin set of integers $\mathcal{A}_{k,\mathcal{N}}$ such that for all $a\in\mathbb{Z}\smallsetminus\mathcal{A}_{k,\mathcal{N}}$,

(1) $(f_a)^N(x)-x$ has no repeated roots,
(2) any field in $\mathcal{F}(a)$ is linearly disjoint from the compositum of the others,
(3) if $\Sigma_{f_a,d}\in\mathcal{F}(a)$, then $\mathrm{Gal}(\Sigma_{f_a,d}/\mathbb{Q})\simeq C_d\wr S_{r_k(d)}$, and
(4) if $\Sigma_{f_a,d}\in\mathcal{F}(a)$, then the action of $\mathrm{Gal}(\Sigma_{f_a,d}/\mathbb{Q})$ on the points of period d of $(\Sigma_{f_a,d},f)$ matches the action of $C_d\wr S_{r_k(d)}$ on $B(d,r_k(d))$.

Fix any $a\in\mathbb{Z}\smallsetminus\mathcal{A}_{k,\mathcal{N}}$. To ease notation, for any $i\in\mathcal{N}$, we will write Φ_i for $\Phi_{f_a,i}$. By Proposition 4.1 and (1), note that

$$\begin{aligned}\delta\left(\left\{p\in\mathcal{P}\mid \text{for all } i\in\mathcal{N},\ \left(\mathbb{F}_p,\left[x^k+a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right)&\\ =\delta\left(\bigcap_{i\in\mathcal{N}}\left\{p\in\mathcal{P}\mid \left(\mathbb{F}_p,\left[x^k+a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right)&\\ =\delta\left(\bigcap_{i\in\mathcal{N}}\left\{p\in\mathcal{P}\mid [\Phi_i]_p \text{ has precisely } i\cdot\varphi(i) \text{ roots in } \mathbb{F}_p\right\}\right).&\end{aligned}$$

Since $\mathcal{N} \subseteq \mathcal{N}_0$ by construction, properties (1)–(4) allow us to apply the Frobenius Density Theorem (see Remark 4.3) to conclude that

$$\delta\left(\bigcap_{i\in\mathcal{N}} \left\{p \in \mathcal{P} \mid [\Phi_i]_p \text{ has precisely } i\cdot\varphi(i) \text{ roots in } \mathbb{F}_p\right\}\right) = \prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i)).$$

□

At this point, Corollary 1.2 is immediate from Theorem 4.4 and Corollary 3.4.

To analyze the cycle structure of *all* monic binomial unicritical integral polynomials of a fixed degree k, we now introduce an asymptotic density on the set of such polynomials. Let $k \in \mathbb{Z}_{\geq 2}$, let $\mathcal{N}$ be a finite subset of $\mathbb{Z}_{\geq 1}$, and choose any $\varphi:\mathcal{N} \to \mathbb{Z}_{\geq 0}$. Define the *truncated cycle density* on $\{x^k + a \mid a \in \mathbb{Z}\}$ to be the function ${}_k\delta_{\mathcal{N},\varphi}:\mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by

$${}_k\delta_{\mathcal{N},\varphi}(X) = \frac{1}{2X+1} \sum_{a=-X}^{X} \delta\left(\left\{p \in \mathcal{P} \mid \text{for all } i \in \mathcal{N}, \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right).$$

Next, define the *cycle density* on $\{x^k + a \mid a \in \mathbb{Z}\}$ to be the function ${}_k\delta_{\mathcal{N}}:{\mathbb{Z}_{\geq 0}}^{\mathcal{N}} \to \mathbb{R}_{\geq 0}$ given by

$${}_k\delta_{\mathcal{N}}(\varphi) = \lim_{X\to\infty} {}_k\delta_{\mathcal{N},\varphi}(X)$$

(we will show in Theorem 4.5 that these limit exists).

Theorem 4.5. *Let $k \in \mathbb{Z}_{\geq 2}$, let $\mathcal{N}$ be a finite subset of $\mathbb{Z}_{\geq 1}$, and choose any $\varphi \in {\mathbb{Z}_{\geq 0}}^{\mathcal{N}}$. Then*

$$\left|\prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i)) - {}_k\delta_{\mathcal{N},\varphi}(X)\right| = O_{k,\mathcal{N}}\left(\frac{1}{\sqrt{X}}\right).$$

In particular,

- *the implied constants do not depend on φ and*
- ${}_k\delta_{\mathcal{N}}(\varphi) = \prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i))$.

Proof. By Theorem 4.4, there exists a thin set $\mathcal{A}_{k,\mathcal{N}}$ with the property that for any $a \in \mathbb{Z} \setminus \mathcal{A}_{k,\mathcal{N}}$,

$$\delta\left(\left\{p \in \mathcal{P} \mid \text{for all } i \in \mathcal{N}, \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right) = \prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i)).$$

Now, by Remark 4.2 we know that

$$|\{a \in \mathcal{A}_{k,\mathcal{N}} \mid -X \leq a \leq X\}| = O\left(\sqrt{X}\right);$$

thus,

$$\begin{aligned}
&\left|\prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i)) - {}_k\delta_{\mathcal{N},\varphi}(X)\right| \\
&\quad\le \left|\prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i)) - \frac{|\{a\in\mathbb{Z}\smallsetminus\mathcal{A}_{k,\mathcal{N}} \mid -X\le a\le X\}|\cdot\prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i))}{2X+1}\right| + \sum_{\substack{a\in\mathcal{A}_{k,\mathcal{N}}\\ -X\le a\le X}} \frac{1}{2X+1} \\
&\quad= \prod_{i\in\mathcal{N}} {}_k\omega_i(\varphi(i))\cdot\frac{2X+1-|\{a\in\mathbb{Z}\smallsetminus\mathcal{A}_{k,\mathcal{N}} \mid -X\le a\le X\}|}{2X+1} + \sum_{\substack{a\in\mathcal{A}_{k,\mathcal{N}}\\ -X\le a\le X}} \frac{1}{2X+1} \\
&\quad= O_{k,\mathcal{N}}\left(\frac{1}{\sqrt{X}}\right),
\end{aligned}$$

as desired. □

4.2. **Most unicritical polynomials have many cycles.** We now prove Lemma 4.6, which computes asymptotics for a certain family of recursively defined sequences; it will be useful for proving Theorem 4.7.

Lemma 4.6. *For all $j\in\mathbb{Z}_{\ge0}$, let $(t_{j,n})_{n\in\mathbb{Z}_{\ge1}}$ be a sequence of nonnegative real numbers. For all such j, let $(s_{j,n})_{n\in\mathbb{Z}_{\ge1}}$ be the sequence defined recursively by*

$$s_{j,n} = \begin{cases} t_{j,1} & \text{if } n=1,\\ \sum_{i=0}^{j} s_{i,n-1}t_{j-i,n} & \text{otherwise.}\end{cases}$$

If

$$\text{for all } j\in\mathbb{Z}_{\ge0},\quad t_{j,n} = \frac{1}{j!n^j}\left(1-\frac{1}{n}\right)+O\left(\frac{1}{n^{j+2}}\right),$$

then

$$\text{for all } j\in\mathbb{Z}_{\ge0},\quad s_{j,n} = O\left(n^{-\frac{1}{j+1}}\right).$$

Proof. We will induct on j. For the $j=0$ case, we begin by noting that $s_{0,n}=\prod_{i=1}^{n} t_{0,i}$ for all $n\in\mathbb{Z}_{\ge1}$. Choose any $R\in\mathbb{R}_{>0}$ such that for all $n\in\mathbb{Z}_{\ge1}$,

$$t_{0,n} < 1-\frac{1}{n}+\frac{R}{n^2}.$$

Then for all such n,

$$0\le ns_{0,n} < n\prod_{i=1}^{n}\left(1-\frac{1}{i}+\frac{R}{i^2}\right) = R\prod_{i=2}^{n}\left(\frac{i-1+\frac{R}{i}}{i-1}\right) = R\prod_{i=2}^{n}\left(1+\frac{R}{i(i-1)}\right).$$

Since $\prod_{i=2}^{\infty}\left(1+\frac{R}{i(i-1)}\right)$ converges, we see $s_{0,n}=O\left(\frac{1}{n}\right)$, as desired.

For the induction step, suppose that $j\in\mathbb{Z}_{\ge1}$ and

$$s_{j',n} = O\left(n^{-\frac{1}{j'+1}}\right)\quad\text{for all } j'\in\{0,\dots,j-1\}.$$

By the induction hypothesis, we see that

$$\sum_{i=0}^{j-1} s_{i,n-1}t_{j-i,n} = O\left(n^{-1-\frac{1}{j}}\right).$$

Choose any $R\in\mathbb{R}_{>0}$ such that

- $\sum_{i=0}^{j-1} s_{i,n-1}t_{j-i,n} < Rn^{-1-\frac{1}{j}}$ for all $n \in \mathbb{Z}_{\geq 1}$ and
- $t_{0,n} < 1 - \frac{1}{n} + \frac{R}{n^2}$ for all $n \in \mathbb{Z}_{\geq 1}$.

Note that since

$$\left((n-1)n^{\frac{1}{j+1}} + 1\right)^{j+1} = n^{j+2} - (j+1)n^{j+1} + O\left(n^{j+\frac{j}{j+1}}\right),$$

there is some $M \in \mathbb{Z}_{\geq 1}$ such that

$$(n-1)n^{\frac{1}{j+1}} + 1 < n(n-1)^{\frac{1}{j+1}}$$

for all $n \in \mathbb{Z}_{\geq M}$. Now choose any $N \in \mathbb{Z}_{\geq 1}$ such that $N > \max\left(\left\{R^{\frac{j+1}{j}}, M\right\}\right)$, and note that for any $n \in \mathbb{Z}_{\geq N}$,

$$\begin{aligned}
n^{\frac{1}{j+1}} s_{j,n} &< \frac{R}{n^{1+\frac{1}{j}-\frac{1}{j+1}}} + s_{j,n-1}\left(\frac{n-1}{n^{1-\frac{1}{j+1}}} + \frac{R}{n^{2-\frac{1}{j+1}}}\right) && \text{by choice of } R \\
&< \frac{R}{n^{1+\frac{1}{j(j+1)}}} + (n-1)^{\frac{1}{j+1}} s_{j,n-1}\left(\left(\frac{n-1}{n}\right)^{1-\frac{1}{j+1}} + \frac{1}{n(n-1)^{\frac{1}{j+1}}}\right) && \text{since } n > R^{\frac{j+1}{j}} \\
&< \frac{R}{n^{1+\frac{1}{j(j+1)}}} + (n-1)^{\frac{1}{j+1}} s_{j,n-1} && \text{since } n > M.
\end{aligned}$$

Finally, since $\sum_{n=1}^{\infty} n^{-1-\frac{1}{j(j+1)}} < \infty$, we see that $n^{\frac{1}{j+1}} s_{j,n}$ is bounded, as desired. □

Before continuing, we pause to introduce a bit of notation. For any dynamical system (S, f) and positive integer n, let $\mathbf{C}_n(S, f) = |\{n\text{-cycles in } (S, f)\}|$. We now use Theorem 4.4, along with Lemma 4.6 and the bounds computed in Section 3.2 (in particular, Corollary 3.8) to prove Theorem 4.7.

Theorem 4.7. *If $k \in \mathbb{Z}_{\geq 2}$ and $J \in \mathbb{Z}_{\geq 1}$, then for any $\epsilon \in \mathbb{R}_{>0}$ there exists a thin set $\mathcal{A}_{k,J,\epsilon} \subseteq \mathbb{Z}$ such that for all $a \in \mathbb{Z} \setminus \mathcal{A}_{k,J,\epsilon}$,*

$$\overline{\delta}\left(\left\{p \in \mathcal{P} \mid \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has } J \text{ or fewer cycles}\right\}\right) < \epsilon.$$

Proof. For any $j \in \mathbb{Z}_{\geq 0}$ and $n \in \mathbb{Z}_{\geq 1}$, let

- $\mathcal{J}_{j,n} = \left\{\varphi \in {\mathbb{Z}_{\geq 0}}^{[n]} \mid \sum_{i=1}^{n} \varphi(i) = j\right\}$,
- $t_{j,n} = {}_k\omega_n(j)$, and
- $s_{j,n} = \sum_{\varphi \in \mathcal{J}_{j,n}} \prod_{i \in [n]} {}_k\omega_i(\varphi(i))$.

To see how these quantities are interrelated, first note that for all $j \in \mathbb{Z}_{\geq 0}$, they imply that $s_{j,1} = t_{j,1}$; moreover, if $n \in \mathbb{Z}_{\geq 2}$, then

$$s_{j,n} = \sum_{\varphi \in \mathcal{J}_{j,n}} \prod_{i \in [n]} {}_k\omega_i(\varphi(i)) = \sum_{m=0}^{j} \sum_{\varphi \in \mathcal{J}_{m,n-1}} \left({}_k\omega_n(j-m) \prod_{i \in [n-1]} {}_k\omega_i(\varphi(i))\right) = \sum_{m=0}^{j} s_{m,n-1}t_{j-m,n}.$$

Now, by Corollary 3.8, we know that for $j \in \mathbb{Z}_{\geq 0}$,

$$t_{j,n} = \frac{1}{j!n^j}\left(1 - \frac{1}{n}\right) + O\left(\frac{1}{n^{j+2}}\right).$$

Thus, by Lemma 4.6, there exists N in $\mathbb{Z}_{\geq 1}$ such that $\sum_{j=0}^{J} s_{j,N} < \epsilon$. Set $\mathcal{N} = [N]$; then by Theorem 4.4, there is a thin set $\mathcal{A} = \mathcal{A}_{k,J,\epsilon} \subseteq \mathbb{Z}$ such that for all $a \in \mathbb{Z} \setminus \mathcal{A}$ and any function

$\varphi: \mathcal{N} \to \mathbb{Z}_{\geq 0}$,

$$\delta\left(\left\{p \in \mathcal{P} \mid \text{for all } i \in \mathcal{N},\ \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right) = \prod_{i \in \mathcal{N}} {}_k\omega_i(\varphi(i)).$$

For any such a, note that

$$\begin{aligned}
&\overline{\delta}\left(\left\{p \in \mathcal{P} \,\middle|\, \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has } J \text{ or fewer cycles}\right\}\right) \\
&\quad = \overline{\delta}\left(\left\{p \in \mathcal{P} \,\middle|\, \sum_{n=1}^{\infty} \mathbf{C}_n\left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \leq J\right\}\right) \\
&\quad \leq \overline{\delta}\left(\left\{p \in \mathcal{P} \,\middle|\, \sum_{n=1}^{N} \mathbf{C}_n\left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \leq J\right\}\right) \\
&\quad = \sum_{j=0}^{J} \delta\left(\left\{p \in \mathcal{P} \,\middle|\, \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } j \text{ cycles of length at most } N\right\}\right) \\
&\quad = \sum_{j=0}^{J} \delta\left(\bigcup_{\varphi \in \mathcal{J}_{j,N}} \left\{p \in \mathcal{P} \,\middle|\, \text{for all } i \in \mathcal{N},\ \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right) \\
&\quad = \sum_{j=0}^{J} \sum_{\varphi \in \mathcal{J}_{j,N}} \delta\left(\left\{p \in \mathcal{P} \,\middle|\, \text{for all } i \in \mathcal{N},\ \left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \text{ has precisely } \varphi(i)\ i\text{-cycles}\right\}\right) \\
&\quad = \sum_{j=0}^{J} \sum_{\varphi \in \mathcal{J}_{j,N}} \prod_{i \in \mathcal{N}} {}_k\omega_i\left(\varphi(i)\right),
\end{aligned}$$

so we are done by our choice of N. □

As in Section 4.1, we can show that *all* monic binomial unicritical polynomials of a fixed degree k have few cycles, on average, once we introduce the appropriate density functions. For $k \in \mathbb{Z}_{\geq 2}$, $n \in \mathbb{Z}_{\geq 1}$, and $J, X \in \mathbb{Z}_{\geq 0}$, define

$${}_k\delta_{n,J}(X) = \frac{1}{2X+1} \sum_{a=-X}^{X} \delta\left(\left\{p \in \mathcal{P} \,\middle|\, \sum_{i=1}^{n} \mathbf{C}_i\left(\mathbb{F}_p, \left[x^k + a\right]_p\right) \leq J\right\}\right).$$

Remark 4.8. Note that for any such k, n, J, X,

$${}_k\delta_{n,J}(X) = \sum_{\substack{\varphi \in (\mathbb{Z}_{\geq 0})^{[n]} \\ \varphi(1)+\cdots+\varphi(n) \leq J}} {}_k\delta_{[n],\varphi}(X).$$

As in Section 4.1, let

$${}_k\delta_n(J) = \lim_{X \to \infty} {}_k\delta_{n,J}(X)$$

(this limit exists by Theorem 4.5.)

Corollary 4.9. *If $k \in \mathbb{Z}_{\geq 2}$ and $J \in \mathbb{Z}_{\geq 1}$, then for any $\epsilon \in \mathbb{R}_{>0}$, there exist $C \in \mathbb{R}_{>0}$ and $N \in \mathbb{Z}_{\geq 1}$ such that for all $n \in \mathbb{Z}_{\geq N}$ and $X \in \mathbb{Z}_{\geq 1}$,*

$${}_k\delta_{n,J}(X) < \epsilon + \frac{C}{\sqrt{X}}.$$

In particular, for all such n,

$${}_k\delta_n(J) \leq \epsilon.$$

Proof. Adopting the notation of Theorem 4.7, we see by Lemma 4.6 that there is some $N \in \mathbb{Z}_{>0}$ such that $\sum_{j=1}^{J} s_{j,n} < \epsilon$ for all $n \geq N$. Thus, we apply Theorem 4.5 and Remark 4.8 to note that for all such n,

$$ {}_k\delta_{n,J}(X) = \sum_{j=1}^{J} s_{j,n} + O\left(\frac{1}{\sqrt{X}}\right). $$

□

Corollary 4.10. *Suppose that $k \in \mathbb{Z}_{\geq 2}$. There is an increasing function $\gamma\colon \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ such that*

$$ \lim_{J\to\infty} {}_k\delta_{\gamma(J),J}\left(\gamma(J)\right) = 0. $$

Proof. Set $\gamma(1) = 1$ and for any $J \in \mathbb{Z}_{\geq 2}$, apply Corollary 4.9 to choose $\gamma(J) \in \mathbb{Z}_{\geq 1}$ such that

- $\gamma(J) > \gamma(J-1)$ and
- ${}_k\delta_{\gamma(J),J}\left(\gamma(J)\right) < \dfrac{1}{J}$.

□

It is a classical fact that the average number of cycles of a random discrete dynamical system grows logarithmically; indeed Kruskal [Kru54] proved that

$$ \frac{1}{|[X]^{[X]}|} \cdot \sum_{f\in[X]^{[X]}} |\{\text{cycles in } (S,f)\}| = \frac{1}{2}\log X + \left(\frac{\log 2 + E}{2}\right) + o(1), $$

where $E = .5772\ldots$ is Euler's constant. This fact leads us to make the following conjecture about the nature of the function γ introduced in Corollary 4.10.

Conjecture 4.11. *Suppose that $k \in \mathbb{Z}_{\geq 2}$ and $\gamma \in \left(\mathbb{Z}_{\geq 0}\right)^{\mathbb{Z}_{\geq 0}}$.*

- *If $J = o\left(\log \gamma(J)\right)$, then there exists an increasing function $\alpha\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ such that*

$$ \lim_{J\to\infty} {}_k\delta_{\gamma(J),J}\left(\alpha(J)\right) = 0. $$

- *If there is some $\epsilon \in (-\infty, 1)$ such that $\log \gamma(J) = O\left(J^{\epsilon}\right)$, then there exists an increasing function $\alpha\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ such that*

$$ \lim_{J\to\infty} {}_k\delta_{\gamma(J),J}\left(\alpha(J)\right) = 1. $$

Acknowledgements

The authors would like to thank Rafe Jones for many useful discussions and for directing us to pertinent background literature. We also thank Roger Heath-Brown for posing a version of the problem studied in this paper, as well as for helpful conversations on this topic. Finally, we thank Igor Shparlinski for his comments on an early draft of this paper.

References

[AB82] James Arney and Edward A. Bender, *Random mappings with constraints on coalescence and number of origins*, Pacific J. Math. **103** (1982), no. 2, 269–294. MR 705228

[Bac91] Eric Bach, *Toward a theory of Pollard's rho method*, Inform. and Comput. **90** (1991), no. 2, 139–155. MR 1094034

[BG17] Andrew Bridy and Derek Garton, *Dynamically distinguishing polynomials*, Res. Math. Sci. **4** (2017), no. 4, 1–17. MR 3669394

[BGH+13] Robert L. Benedetto, Dragos Ghioca, Benjamin Hutz, Pär Kurlberg, Thomas Scanlon, and Thomas J. Tucker, *Periods of rational maps modulo primes*, Math. Ann. **355** (2013), no. 2, 637–660. MR 3010142

[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

[BJ07] Nigel Boston and Rafe Jones, *Arboreal Galois representations*, Geom. Dedicata **124** (2007), 27–35.

[BP81] Richard P. Brent and John M. Pollard, *Factorization of the eighth Fermat number*, Math. Comp. **36** (1981), no. 154, 627–630. MR 606520

[BS17] Charles Burnette and Eric Schmutz, *Periods of iterated rational functions*, Int. J. Number Theory **13** (2017), no. 5, 1301–1315. MR 3639698

[CM12] Chak-On Chow and Toufik Mansour, *Asymptotic probability distributions of some permutation statistics for the wreath product $C_r \wr S_n$*, Online J. Anal. Comb. (2012), no. 7, 14. MR 3016122

[Coh81] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. (3) **43** (1981), no. 2, 227–250. MR 628276

[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

[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

[Gon44] V. Gontcharoff, *Du domaine de l'analyse combinatoire*, Bull. Acad. Sci. URSS Sér. Math. [Izvestia Akad. Nauk SSSR] **8** (1944), 3–48. MR 0010922

[Gon62] V. Gončarov, *On the field of combinatory analysis*, Amer. Math. Soc. Transl. (2) **19** (1962), 1–46. MR 0131369

[Har60] Bernard Harris, *Probability distributions related to random mappings*, Ann. Math. Statist. **31** (1960), 1045–1062. MR 0119227

[HB17] D. R. Heath-Brown, *Iteration of Quadratic Polynomials Over Finite Fields*, Mathematika **63** (2017), no. 3, 1041–1059. MR 3731313

[Isa06] I. Martin Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006, Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. MR 2270898

[Isa08] ———, *Finite group theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008. MR 2426855

[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

[Kru54] Martin D. Kruskal, *The expected number of components under a random mapping function*, Amer. Math. Monthly **61** (1954), 392–397. MR 0062973 (16,52b)

[Lan83] Serge Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983. MR 715605

[Mor96] Patrick Morton, *On certain algebraic curves related to polynomial maps*, Compositio Math. **103** (1996), no. 3, 319–350. MR 1414593 (97m:14030)

[Mor98] ———, *Galois groups of periodic points*, J. Algebra **201** (1998), no. 2, 401–428. MR 1612390

[Mor11] ———, *Corrigendum: 'On certain algebraic curves related to polynomial maps, Compositio Math. 103 (1996), 319–350'*, Compos. Math. **147** (2011), no. 1, 332–334. MR 2771135

[MP94] Patrick Morton and Pratiksha Patel, *The Galois theory of periodic points of polynomial maps*, Proc. London Math. Soc. (3) **68** (1994), no. 2, 225–263. MR 1253503

[MSSS] B. Mans, M. Sha, I. E. Shparlinski, and D. Sutantyo, *On Functional Graphs of Quadratic Polynomials*, to appear in Exp. Math.

[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.

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

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., 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. MR 1757192

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

[Sil08] ———, *Variation of periods modulo p in arithmetic dynamics*, New York J. Math. **14** (2008), 601–616. MR 2448661

[SL96] P. Stevenhagen and H. W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37. MR 1395088

[Ste69] V. E. Stepanov, *Limit distributions of certain characteristics of random mappings*, Teor. Verojatnost. i Primenen. **14** (1969), 639–653. MR 0278350

[Völ96] Helmut Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996, An introduction. MR 1405612

Department of Mathematics, Texas A&M University
E-mail address: andrewbridy@math.tamu.edu

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