6-25-2024

Preperiodic Points of Polynomial Dynamical Systems over Finite Fields

Aaron Andersen
Portland State University

Derek Garton
Portland State University, gartondw@pdx.edu

Citation Details

Published as: Andersen, A., & Garton, D. (2024). Preperiodic points of polynomial dynamical systems over finite fields. International Journal of Number Theory, 1–10. https://doi.org/10.1142/s1793042124501124

PREPERIODIC POINTS OF POLYNOMIAL DYNAMICAL SYSTEMS OVER FINITE FIELDS

AARON ANDERSEN AND DEREK GARTON

ABSTRACT. For a prime p, positive integers r, n, and a polynomial f with coefficients in $\mathbb{F}_{p^r}$, let $W_{p,r,n}(f) = f^n(\mathbb{F}_{p^r}) \setminus f^{n+1}(\mathbb{F}_{p^r})$. As n varies, the $W_{p,r,n}(f)$ partition the set of strictly preperiodic points of the dynamical system induced by the action of f on $\mathbb{F}_{p^r}$. In this paper we compute statistics of strictly preperiodic points of dynamical systems induced by unicritical polynomials over finite fields by obtaining effective upper bounds for the proportion of $\mathbb{F}_{p^r}$ lying in a given $W_{p,r,n}(f)$. Moreover, when we generalize our definition of $W_{p,r,n}(f)$, we obtain both upper and lower bounds for the resulting averages.

CONTENTS

1. INTRODUCTION

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

When S is a finite field, say $S = \mathbb{F}_q$ for some prime power q, and f is a polynomial with coefficients in $\mathbb{F}_q$, a question arises: for $n \in \mathbb{Z}_{\geq 0}$, what is the size of $f^n(\mathbb{F}_q)$? This question has been studied, for example, in [JKMT16, HB17, Juu19, Juu21, Gar22, Gar23]. In each of these papers, the authors use the answers they find to address the related question: what is the size of $\mathrm{Per}(\mathbb{F}_q, f)$? This is due to the fact that for any $n \in \mathbb{Z}_{\geq 0}$, the set $f^n(\mathbb{F}_q)$ contains $\mathrm{Per}(\mathbb{F}_q, f)$—see [JKMT16, Lemma 5.2]. Specifically, upper bounds on the size of $f^n(\mathbb{F}_q)$ yield upper bounds on the size of $\mathrm{Per}(\mathbb{F}_q, f)$.

In this paper, we turn to the study of strictly preperiodic points. If (S, f) is a dynamical system and $s \in S$, we say that s is *strictly preperiodic* (for f) if s is not periodic and there is

Date: May 2, 2024.
2020 *Mathematics Subject Classification.* Primary 37P05; Secondary 37P25, 37P35, 11T06, 13B05.
Key words and phrases. Arithmetic Dynamics, Periodic Points, Finite Fields, Galois Theory.

some positive integer n such that $f^n(s)$ is periodic. Of course, when S is finite, the strictly preperiodic points are precisely $S \setminus \mathrm{Per}(S, f)$. In the finite case, we partition the strictly preperiodic points as follows: for a nonnegative integer n, let

$$W_n(S, f) = f^n(S) \setminus f^{n+1}(S).$$

We prove in Lemma 1.5 that the nonempty $W_n(S, f)$ do indeed partition the strictly preperiodic points of (S, f); see Fig. 1 for an illustration of this phenomenon. The purpose of this paper is to average the proportion of S in these $W_n(S, f)$, as f varies; so when S is finite, let

$$w_n(S, f) = \frac{|W_n(S, f)|}{|S|}.$$

There is a natural generalization of this classification of strictly preperiodic points: for a dynamical system (S, f) and integers m, n with $n > m \geq 0$, we define

$$W_{m,n}(S, f) = f^m(S) \setminus f^n(S).$$

As above, when S is finite, we write $w_{m,n}(S, f) = |W_{m,n}(S, f)| \cdot |S|^{-1}$. Of course, it is clear from these definitions that $W_n(S, f) = W_{n,n+1}(S, f)$.

Before stating our results, we introduce one more bit of notation. If q is a prime power, $d \in \mathbb{Z}_{\geq 2}$, and $\alpha \in \mathbb{F}_q$, we will write $f_{d,\alpha} = f_{d,\alpha}(x) = x^d + \alpha \in \mathbb{F}_q[x]$. As these polynomials have only one critical point, they are examples of *unicritical polynomials*; our main results hold for dynamical systems induced by such polynomials. In Section 3, we prove Corollary 1.1, which is the $d = 2$ case of the more-general Proposition 3.1.

Corollary 1.1. *Suppose $p > 3$ is prime. Choose positive integers r, n with $n > 2$ and $\alpha \in \mathbb{F}_{p^r}$ with $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$. If $r > 2^{2n+3}$, then*

$$w_n(\mathbb{F}_{p^r}, f_{2,\alpha}) < 15\left(\frac{\log n}{n^2}\right) + \frac{32}{p^{r/2}}.$$

Unlike previous work, we also obtain *lower* bounds. The work on periodic proportions previously mentioned uses only upper bounds on image size; Corollary 1.2 follows from using both upper and lower bounds on image size (which we record in Proposition 2.3).

Corollary 1.2. *Let $d \in \mathbb{Z}_{\geq 2}$, and suppose p is a prime satisfying $p > (d!)^2$ and $p \equiv 1 \pmod{d}$. Choose $r, m, n \in \mathbb{Z}_{\geq 1}$ with $5 < m < n$, and $\alpha \in \mathbb{F}_{p^r}$ with $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$. If $r > 2d^{2n}$, then*

$$\frac{7}{8(d-1)}\left(\frac{1}{m} - \frac{1}{n} - \frac{4\log m}{mn}\right) - \frac{16d}{p^{r/2}} < w_{m,n}(\mathbb{F}_{p^r}, f_{d,\alpha}) < \frac{2}{d-1}\left(\frac{1}{m} - \frac{1}{n} + \frac{4\log n}{mn}\right) + \frac{16d}{p^{r/2}}.$$

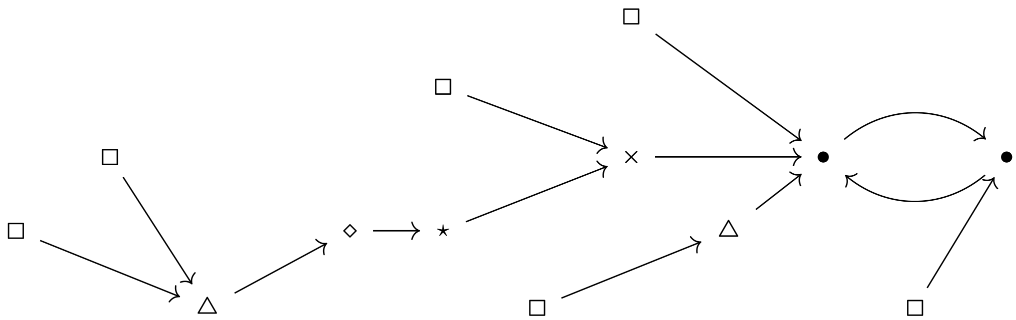
In Section 5, we compute upper bounds on the statistics of strictly preperiodic points, averaging over all quadratic polynomials. To do so, we use that fact that any quadratic polynomial (in odd characteristic) is conjugate to a unicritical polynomial.

Theorem 1.3. *Suppose $p > 3$ is prime. Let $n, r \in \mathbb{Z}_{\geq 1}$. If $n > 133$ and $r > 2^{2n+3}$, then*

$$\frac{1}{|\{f \in \mathbb{F}_{p^r}[x] \mid \deg f = 2\}|} \cdot \sum_{\substack{f \in \mathbb{F}_{p^r}[x] \\ \deg f = 2}} w_n(\mathbb{F}_{p^r}, f) < \frac{1}{n^{3/2}} + \frac{34}{p^{r/2}}.$$

Moreover, as in Corollary 1.2, we can obtain both lower and upper bounds for statistics of strictly preperiodic points by the using lower bounds on image sizes given in Proposition 2.3.

FIGURE 1. A partition of the strictly preperiodic points of a dynamical system (S, f)



$\square$ $W_0(S,f)$ $\triangle$ $W_1(S,f)$ $\diamond$ $W_2(S,f)$ $\star$ $W_3(S,f)$ $\times$ $W_4(S,f)$

Corollary 1.4. *Suppose $p > 3$ is prime. Let $r, m, n \in \mathbb{Z}_{\geq 1}$ with $5 < m < n$. If $r > 2^{2n+1}$, then*

$$\frac{7}{8}\left(\frac{1}{m} - \frac{1}{n}\right) - 4\left(\frac{\log m}{mn}\right) < \frac{1}{|\{f \in \mathbb{F}_{p^r}[x] \mid \deg f = 2\}|} \cdot \sum_{\substack{f \in \mathbb{F}_{p^r}[x] \\ \deg f = 2}} w_{m,n}(\mathbb{F}_{p^r}, f)$$
$$< 2\left(\frac{1}{m} - \frac{1}{n}\right) + 9\left(\frac{\log n}{mn}\right).$$

The organization of this paper is as follows. In Section 2, we prove basic facts about our partition of strictly preperiodic points, as well as the main technical tool needed for our applications, Proposition 2.3, which gives an effective estimate of image sizes of polynomial dynamical systems. In Section 3 and Section 4, we use Proposition 2.3 to prove the upper and lower bounds in Corollary 1.2, respectively. Finally, in Section 5, we compute averages over all quadratic polynomials.

Before proceeding to Section 2, we prove Lemma 1.5.

Lemma 1.5. *If (S, f) is a dynamical system and S is finite, then*

$$\{W_n(S,f) \mid n \in \mathbb{Z}_{\geq 0} \text{ and } W_n(S,f) \neq \varnothing\}$$

is a partition of the strictly preperiodic points of (S, f).

Proof. We begin by showing that the the sets $W_n(S,f)$ contain all strictly preperiodic points of (S, f). To this end, choose any strictly preperiodic point $s_0 \in S$ and set

$$P_{s_0} = \{s \in S \mid \text{there exists } n \in \mathbb{Z}_{\geq 0} \text{ such that } f^n(s) = s_0\}.$$

We claim that for any $s \in P_{s_0}$, there is a *unique* $n \in \mathbb{Z}_{>0}$ such that $f^n(s) = s_0$. Indeed, this follows from the fact that s is not periodic. For any $s \in P_{s_0}$, let n_s be this positive integer. Since S is finite, we may set $n_0 = \max(\{n_s \mid s \in P_{s_0}\})$. Then $s_0 \in W_{n_0}(S, f)$.

To see that the $W_n(S,f)$ are pairwise disjoint, choose any $m, n \in \mathbb{Z}_{\geq 0}$ with $n > m$. Since $f^n(S) \subseteq f^m(S)$ and $f^{n+1}(S) \subseteq f^{m+1}(S)$, we see that

$$W_m(S,f) \cap W_n(S,f) = f^n(S) \smallsetminus f^{m+1}(S) = \varnothing.$$

$\square$

2. Preliminaries

We begin this section by noting that for certain parameters, we need only elementary tools to compute statistics of strictly preperiodic points. For example, the fact that for any odd prime power q, the number of squares in $\mathbb{F}_q$ is $\frac{1}{2}(q+1)$ yields Remark 2.1.

Remark 2.1. Suppose q is an odd prime power and $\alpha \in \mathbb{F}_q$. Then

$$w_0(\mathbb{F}_q, f_{2,\alpha}) = \frac{1}{2}\left(1 - \frac{1}{q}\right).$$

Of course, Remark 2.1 immediately generalizes to Proposition 2.2.

Proposition 2.2. *Let q be a prime power and $\alpha \in \mathbb{F}_q$. Then for any $d \in \mathbb{Z}_{\geq 1}$,*

$$w_0(\mathbb{F}_q, f_{d,\alpha}) = \left(1 - \frac{1}{\gcd(q-1, d)}\right)\left(1 - \frac{1}{q}\right).$$

Proof. Indeed, consider the bijection

$$\begin{aligned}(\mathbb{F}_q)^d &\mapsto f_{d,\alpha}(\mathbb{F}_q)\\ \beta &\mapsto \beta + \alpha,\end{aligned}$$

then use the fact that $(\mathbb{F}_q)^d$ has size $1 + \frac{q-1}{\gcd(q-1,d)}$. □

The main technical tool we will use in proving our main results is Proposition 2.3.

Proposition 2.3. *Let $d \in \mathbb{Z}_{\geq 2}$, and suppose p is a prime that satisfies $p > (d!)^2$ and $p \equiv 1 \pmod{d}$. Choose $r, n \in \mathbb{Z}_{\geq 1}$. If $r > 2d^{2n}$, then for all $\alpha \in \mathbb{F}_{p^r}$ with $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$,*

$$\frac{2}{(d-1)(n+4+\log n)} - \frac{8d}{p^{r/2}} < \frac{\left|f_{d,\alpha}^n(\mathbb{F}_{p^r})\right|}{p^r} < \frac{2}{(d-1)(n+1)} + \frac{8d}{p^{r/2}}.$$

Proof. Let $R = \mathbb{F}_p[s]$ and $\phi(x) = x^d + s \in R[x]$. We will apply [Gar22, Corollary 5.7] to the dynamical system (R, ϕ). To do so, we set $f(x) = \phi(x) - t \in R[t, x]$ and $K = \mathrm{Frac}(R[t])$, then write L for the splitting field of $f(x)$ over K, write B for the integral closure of $R[t]$ in L, write G for $\mathrm{Gal}(L/K)$, and write ρ for the action of G on the roots of $f(x)$ in B. Let $\pi(s) \in R$ be the minimal polynomial for α over $\mathbb{F}_p$, so that $\deg(\pi(s)) = r$ by hypothesis. Since $p \equiv 1 \pmod{d}$, we see that $\mathrm{Frac}(B/\pi(s)B)/\mathrm{Frac}(R[t]/\pi(s)R[t])$ is Galois with

$$\mathrm{Gal}(\mathrm{Frac}(B/\pi(s)B)/\mathrm{Frac}(R[t]/\pi(s)R[t])) \simeq G \simeq \mathbb{Z}/d\mathbb{Z}.$$

Moreover, as in the proof of [Gar22, Theorem 1.2], we know that $R/\pi(s)R$ is algebraically closed in $\mathrm{Frac}(B/\pi(s)B)$.

Let's write S for the set of roots of $f(x)$ in B. Let $[\rho]^n$ be the nth iterated wreath product of the action ρ; this is an action of the nth iterated wreath product of the group G (denoted by $[G]^n$) on the set S^n (see [Gar22, Section 5] for more details). Using this notation, let $\mathrm{f}_n(\rho)$ be the proportion of $[G]^n$ with a fixed point under the action of $[\rho]^n$. We are now in a position to apply [Gar22, Corollary 5.7]. Since ϕ is unicritical with critical point 0, [Gar22, Corollary 5.7] holds for n at most

$$\left\lfloor \frac{\log(\log(p^r)) - \log(\log(p^2))}{2\log d} \right\rfloor;$$

this constraint follows by computing the height bound given in [Gar22, Definition 4.2], applied to the valuation on $\mathrm{Frac}(R)$ given by $\pi(s)$. Since $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$, our hypothesis on $r = \deg(\pi(s))$ ensures that n satisfies this bound. Therefore, noting that the specialization of ϕ at $\pi(s)R \in \mathrm{Spec}(R)$ is $f_{d,\alpha}$, we may apply [Gar22, Corollary 5.7]. However, since [Gar22, Corollary 5.7] applies to $f_{d,\alpha}$ acting on $\mathbb{P}^1(\mathbb{F}_{p^r})$, we must slightly adjust the constants appearing in the statement of that Corollary; using the inefficient estimate $1 < dp^{r/d}(p^r+1)$, this adjustment yields

$$\mathrm{f}_n(\rho) - \frac{8d}{p^{r/2}} < \frac{\left|f_{d,\alpha}^n(\mathbb{F}_{p^r})\right|}{p^r} < \mathrm{f}_n(\rho) + \frac{8d}{p^{r/2}}.$$

The result now follows by applying Juul's estimates on fixed point proportions in wreath products [Juu21, Proposition 4.2]. ☐

3. Effective upper bounds

With Proposition 2.3 in hand, we proceed to proving the upper bounds on strictly preperiodic points mentioned in Section 1. Indeed, Proposition 2.3 immediately implies Proposition 3.1.

Proposition 3.1. *Let $d \in \mathbb{Z}_{\geq 2}$, and suppose p is a prime that satisfies $p > (d!)^2$ and $p \equiv 1 \pmod d$. Choose $r, n \in \mathbb{Z}_{\geq 1}$ and $\alpha \in \mathbb{F}_{p^r}$ with $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$. If $r > 2d^{2n+2}$, then*

$$w_n(\mathbb{F}_{p^r}, f_{d,\alpha}) < \frac{2\log(n+1)+8}{(d-1)(n+1)(n+5+\log(n+1))} + \frac{16d}{p^{r/2}}.$$

Proof. Proposition 2.3 tells us that

$$\frac{\left|f_{d,\alpha}^n(\mathbb{F}_{p^r})\right|}{p^r} < \frac{2}{(d-1)(n+1)} + \frac{8d}{p^{r/2}} \quad \text{and} \quad \frac{\left|f_{d,\alpha}^{n+1}(\mathbb{F}_{p^r})\right|}{p^r} > \frac{2}{(d-1)(n+5+\log(n+1))} - \frac{8d}{p^{r/2}}.$$

☐

We are now in a position to prove Corollary 1.1, which we mentioned in Section 1. It is a simplification of the quadratic case of Proposition 3.1. (In Corollary 5.1, we present an even cruder simplification, which we will apply in our proof of Theorem 1.3.)

Proof of Corollary 1.1. Since $2 \leq n$, we know that $8 < 8\log(n+1)$, so that

$$\frac{2\log(n+1)+8}{(n+1)(n+5+\log(n+1))} < 10\left(\frac{\log(n+1)}{n^2}\right).$$

Moreover, the fact that $3 \leq n$ implies $n+1 < n^{3/2}$, which tells us that

$$10\left(\frac{\log(n+1)}{n^2}\right) + \frac{32}{p^{r/2}} < 10\left(\frac{\log(n^{3/2})}{n^2}\right) + \frac{32}{p^{r/2}} = 15\left(\frac{\log n}{n^2}\right) + \frac{32}{p^{r/2}}.$$

☐

Proposition 2.3 enables us to find upper bounds not just on sets of the form $W_n(\mathbb{F}_{p^r}, f_{2,\alpha})$, but also for the generalized sets $W_{m,n}(\mathbb{F}_{p^r}, f_{d,\alpha})$ for $d \in \mathbb{Z}_{\geq 2}$.

Theorem 3.2. *Let $d \in \mathbb{Z}_{\geq 2}$, and suppose p is a prime that satisfies $p > (d!)^2$ and $p \equiv 1 \pmod{d}$. Choose $r, m, n \in \mathbb{Z}_{\geq 1}$ with $1 < m < n$, and $\alpha \in \mathbb{F}_{p^r}$ with $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$. If $r > 2d^{2n}$, then*

$$w_{m,n}(\mathbb{F}_{p^r}, f_{d,\alpha}) < \frac{2}{d-1}\left(\frac{1}{m} - \frac{1}{n} + \frac{4\log n}{mn}\right) + \frac{16d}{p^{r/2}}.$$

Proof. Using Proposition 2.3 as in Proposition 3.1, we see that

$$\begin{aligned}
&w_{m,n}(\mathbb{F}_{p^r}, f_{d,\alpha}) \\
&\quad< \left(\frac{2}{(d-1)(m+1)} + \frac{8d}{p^{r/2}}\right) - \left(\frac{2}{(d-1)(n+4+\log n)} - \frac{8d}{p^{r/2}}\right) \\
&\quad= \frac{2n-2m+2\log n+6}{(d-1)(m+1)(n+4+\log n)} + \frac{16d}{p^{r/2}} \\
&\quad< \frac{2n-2m+8\log n}{(d-1)mn} + \frac{16d}{p^{r}} && \text{(since } 6 < 6\log n) \\
&\quad= \frac{2}{d-1}\left(\frac{1}{m} - \frac{1}{n} + \frac{4\log n}{mn}\right) + \frac{16d}{p^{r/2}}.
\end{aligned}$$

□

We remark that Theorem 3.2 establishes one half of Corollary 1.2.

4. Effective lower bounds

We proceed to proving the lower bound of Corollary 1.2.

Proposition 4.1. *Let $d \in \mathbb{Z}_{\geq 2}$, and suppose p is a prime that satisfies $p > (d!)^2$ and $p \equiv 1 \pmod{d}$. Choose $r, m, n \in \mathbb{Z}_{\geq 1}$ with $5 < m < n$, and $\alpha \in \mathbb{F}_{p^r}$ with $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$. If $r > 2d^{2n}$, then*

$$w_{m,n}(\mathbb{F}_{p^r}, f_{d,\alpha}) > \frac{7}{8(d-1)}\left(\frac{1}{m} - \frac{1}{n} - \frac{4\log m}{mn}\right) - \frac{16d}{p^{r/2}}.$$

Proof. Apply Proposition 2.3 to see that

$$\begin{aligned}
&w_{m,n}(\mathbb{F}_{p^r}, f_{d,\alpha}) \\
&\quad> \left(\frac{2}{(d-1)(m+4+\log m)} - \frac{8d}{p^{r/2}}\right) - \left(\frac{2}{(d-1)(n+1)} + \frac{8d}{p^{r/2}}\right) \\
&\quad= \frac{2n-2m-2\log m-6}{(d-1)(n+1)(m+4+\log m)} - \frac{16d}{p^{r/2}} \\
&\quad> \frac{2n-2m-8\log m}{(d-1)(n+1)(m+4+\log m)} - \frac{16d}{p^{r}} && \text{(since } 6 < 6\log m).
\end{aligned}$$

Since $5 < m < n$, we observe

$$\frac{mn}{(n+1)(m+4+\log m)} > \frac{mn}{(n+1)(2m)} \geq \frac{7}{16}.$$

Thus, we see that

$$\frac{2n-2m-8\log m}{(d-1)(n+1)(m+4+\log m)} - \frac{16d}{p^{r/2}} > \frac{7}{16(d-1)}\left(\frac{2n-2m-8\log m}{mn}\right) - \frac{16d}{p^{r/2}}.$$

□

Corollary 1.2 now follows immediately from Theorem 3.2 and Proposition 4.1.

5. Averaging over polynomials

We now compute statistics of our strictly preperiodic partitions over all quadratic polynomials. We first prove Corollary 5.1, which is a simplification of Proposition 3.1. We use this simplification only to aid our proof of Theorem 1.3.

Corollary 5.1. *Keep the hypotheses of Proposition 3.1. If $n > 133$, then*

$$w_n\left(\mathbb{F}_{p^r}, f_{d,\alpha}\right) < \frac{1}{n^{3/2}} + \frac{16d}{p^{r/2}}.$$

Proof. Indeed, for all such n,

$$\frac{2\log(n+1)+8}{(d-1)(n+1)(n+5+\log(n+1))} < \frac{1}{n^{3/2}}.$$

The result now follows from Proposition 3.1. □

Corollary 5.1 in hand, we now prove Theorem 1.3.

Proof of Theorem 1.3. We begin by counting the number of quadratic polynomials that are conjugate to a given unicritical polynomial. To this end, let's write

$$\mathcal{Q} = \{f \in \mathbb{F}_{p^r}[x] \mid \deg(f) = 2\} \qquad \text{and} \qquad \mathcal{U} = \left\{x^2 + \delta \mid \delta \in \mathbb{F}_{p^r}\right\}.$$

Since p is odd, for any $\alpha \in \mathbb{F}_{q^r} \smallsetminus \{0\}$ and $\beta \in \mathbb{F}_{q^r}$ we may define the following coordinate change on $\mathbb{F}_{p^r}$:

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

Next, we set

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

Then μ is surjective and $p^r(p^r-1)$-to-one. Moreover, for any $f \in \mathcal{Q}$, say with $f(X) = \alpha X^2 + \beta X + \gamma$, we see that

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

thus,

$$\left|W_n\left(\mathbb{F}_{p^r}, f\right)\right| = \left|W_n\left(\mathbb{F}_{p^r}, \mu(f)\right)\right|.$$

Let's write $(\mathbb{F}_{p^r})^{\text{prim}}$ for the set of $\alpha \in \mathbb{F}_{p^r}$ with $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^r}$, and recall $\left|\mathbb{F}_{p^r} \setminus (\mathbb{F}_{p^r})^{\text{prim}}\right| < 2p^{r/2}$. Then by the first paragraph of this proof, we see

$$\begin{aligned}
&\frac{1}{|\mathcal{Q}|}\sum_{f\in\mathcal{Q}} w_n(\mathbb{F}_{p^r}, f)\\
&\qquad = \frac{p^r(p^r-1)}{p^{3r}-p^{2r}}\sum_{f\in\mathcal{U}} w_n(\mathbb{F}_{p^r}, f)\\
&\qquad < \frac{1}{p^r}\left(\sum_{\delta\in(\mathbb{F}_{p^r})^{\text{prim}}} w_n\left(\mathbb{F}_{p^r}, x^2+\delta\right) + \sum_{\delta\in\mathbb{F}_{p^r}\setminus(\mathbb{F}_{p^r})^{\text{prim}}} w_n\left(\mathbb{F}_{p^r}, x^2+\delta\right)\right)\\
&\qquad < \frac{1}{p^r}\left(p^r\left(\frac{1}{n^{3/2}}+\frac{32}{p^{r/2}}\right)+2p^{r/2}\right) \qquad \text{(by Corollary 5.1)}\\
&\qquad = \frac{1}{n^{3/2}}+\frac{34}{p^{r/2}}.
\end{aligned}$$

□

Theorem 1.3 applies when $n > 133$. If we are willing to accept a higher threshold for n, we achieve Theorem 5.2, a stronger bound.

Theorem 5.2. *Suppose $p > 3$ is prime. Let $\epsilon \in \mathbb{R}_{>0}$ and $n, r \in \mathbb{Z}_{\geq 1}$. Then there exists $N_\epsilon \in \mathbb{Z}_{>0}$ such that if $n > N_\epsilon$ and $r > 2^{2n+3}$, then*

$$\frac{1}{|\{f\in\mathbb{F}_{p^r}[x] \mid \deg f = 2\}|}\cdot\sum_{\substack{f\in\mathbb{F}_{p^r}[x]\\ \deg f=2}} w_n(\mathbb{F}_{p^r}, f) < \frac{1}{n^{2-\epsilon}}+\frac{34}{p^{r/2}}.$$

Proof. Choose N_ϵ so that for any $n > N_\epsilon$

$$\frac{2\log(n+1)+8}{(n+1)(n+5+\log(n+1))} < \frac{1}{n^{2-\epsilon}}.$$

The remainder of the proof is similar to that of Theorem 1.3. □

Using Theorem 3.2 instead of Corollary 5.1, we prove Proposition 5.3.

Proposition 5.3. *Suppose $p > 3$ is prime. Let $r, m, n \in \mathbb{Z}_{\geq 1}$ with $1 < m < n$. If $r > 2^{2n+1}$, then*

$$\frac{1}{|\{f\in\mathbb{F}_{p^r}[x] \mid \deg f = 2\}|}\cdot\sum_{\substack{f\in\mathbb{F}_{p^r}[x]\\ \deg f=2}} w_{m,n}(\mathbb{F}_{p^r}, f) < 2\left(\frac{1}{m}-\frac{1}{n}\right)+9\left(\frac{\log n}{mn}\right).$$

Proof. Keeping the same notation as the proof of Theorem 1.3, note that

$$\begin{aligned}
&\frac{1}{|\mathcal{Q}|}\sum_{f\in\mathcal{Q}} w_{m,n}(\mathbb{F}_{p^r}, f)\\
&\quad < \frac{p^r(p^r-1)}{p^{3r}-p^{2r}}\left(\sum_{\alpha\in(\mathbb{F}_{p^r})^{\text{prim}}} w_{m,n}\left(\mathbb{F}_{p^r}, x^2+\alpha\right) + \sum_{\alpha\in\mathbb{F}_{p^r}\setminus(\mathbb{F}_{p^r})^{\text{prim}}} w_{m,n}\left(\mathbb{F}_{p^r}, x^2+\alpha\right)\right)\\
&\quad < \frac{1}{p^r}\left(p^r\left(\frac{2}{m}-\frac{2}{n}+\frac{8\log n}{mn}+\frac{32}{p^{r/2}}\right)+2p^{r/2}\right) \qquad \text{(by Theorem 3.2)}\\
&\quad = \frac{2}{m}-\frac{2}{n}+\frac{8\log n}{mn}+\frac{34}{p^{r/2}}.
\end{aligned}$$

And since $r > 2^{2n+1}$, we conclude by noting that

$$\frac{34}{p^{r/2}} < \frac{\log n}{mn}.$$

□

Finally, we prove Proposition 5.4, completing the proof of Corollary 1.4.

Proposition 5.4. *Keep the hypotheses of Proposition 5.3, but assume* $5 < m$. *Then*

$$\frac{1}{|\{f \in \mathbb{F}_{p^r}[x] \mid \deg f = 2\}|} \cdot \sum_{\substack{f \in \mathbb{F}_{p^r}[x] \\ \deg f = 2}} w_{m,n}(\mathbb{F}_{p^r}, f) > \frac{7}{8}\left(\frac{1}{m} - \frac{1}{n}\right) - 4\left(\frac{\log m}{mn}\right).$$

Proof. This follows by a similar argument to Proposition 5.3, using Proposition 4.1 instead of Theorem 3.2. □

Acknowledgements

We would very much like to thank John Caughman, who asked the question that led to this paper. We would also like to thank the anonymous reviewer for many useful comments.

References

[Gar22] Derek Garton, *Periodic points of polynomials over finite fields*, Trans. Amer. Math. Soc. **375** (2022), no. 7, 4849–4871. MR 4439493

[Gar23] Derek Garton, *Periodic points of rational functions of large degree over finite fields*, 2023, (Submitted for publication).

[HB17] D. R. Heath-Brown, *Iteration of quadratic polynomials over finite fields*, Mathematika **63** (2017), no. 3, 1041–1059. MR 3731313

[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

[Juu19] Jamie Juul, *Iterates of generic polynomials and generic rational functions*, Trans. Amer. Math. Soc. **371** (2019), no. 2, 809–831. MR 3885162

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

Fariborz Maseeh Department of Mathematics and Statistics, Portland State University
Email address: aaander2@pdx.edu, gartondw@pdx.edu