ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 49, Number 1, 2019

PERIODIC POINTS IN TOWERS OF FINITE FIELDS FOR POLYNOMIALS ASSOCIATED TO ALGEBRAIC GROUPS

MICHELLE MANES AND BIANCA THOMPSON

ABSTRACT. We find the limiting proportion of periodic points in towers of finite fields for polynomial maps associated to algebraic groups, namely, pure power maps $\phi(z) = z^d$ and Chebyshev polynomials.

1. Introduction. Let K be a field. We fix the following notation: $\phi(z)$ is a polynomial in $K[z]$, $\phi^n(z)$ is the nth iterate of ϕ under composition; we take $\phi^0(z) = z$. $\mathcal{O}_\phi(\alpha)$ is the (forward) orbit of a point α under ϕ, i.e., $\{\phi^n(z) \mid n \geq 0\}$; and $\mathrm{Per}(\phi, K)$ is the set of periodic points for ϕ in the field K, i.e., $\{\alpha \in K \mid \phi^n(\alpha) = \alpha \text{ for some } n > 0\}$.

When iterating a polynomial function ϕ over a finite field, the orbit of any point $\alpha \in \mathbb{F}_{p^n}$ is a finite set, that is, all points are preperiodic, meaning the orbit eventually enters a cycle. However, many natural questions about the structure of orbits over finite fields remain:

(1) Fix a finite field $\mathbb{F}_{p^n}$ and look over all polynomials of fixed degree d: on average, are there "many" periodic points with relatively small tails leading into the cycles? Or, do we expect few periodic points with long tails? (See Figures 1 and 2.)

(2) Fix a polynomial defined over $\mathbb{Q}$: what is the proportion of periodic points for the reduced map over $\mathbb{F}_p$ as $p \to \infty$?

(3) Again, fix a polynomial: how does the proportion of periodic points in $\mathbb{F}_{p^n}$ vary as $n \to \infty$?

2010 AMS *Mathematics subject classification.* Primary 37P25, Secondary 11T06, 37P05.

Keywords and phrases. Finite fields, polynomial dynamics, periodic points.

The work of both authors was partially supported by NSF-DMS 1102858. The first author was supported by a Simons grant, No. 359721.

Received by the editors on February 3, 2018, and in revised form on July 3, 2018.

DOI:10.1216/RMJ-2019-49-1-171

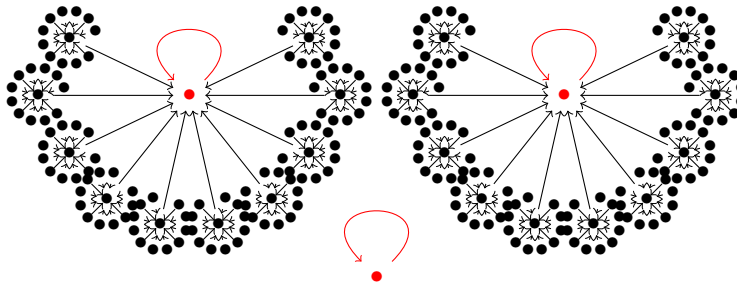

FIGURE 1. Few periodic points: $\phi(z) = z^{11}$ on $\mathbb{F}_{35}$ has 3 fixed points and 240 strictly preperiodic points.

Work by Flynn and Garton [**2**] addresses the first question. Using combinatorial arguments, they bound the average number of periodic points over all polynomials of degree d. For d large, that is, $d \geq \sqrt{p^n}$, their bound of $(5/6)\sqrt{p^n}$ agrees with earlier heuristic arguments.

In her thesis [**5**], Madhu tackles the second question for polynomials $\phi(z) = z^m + c$ over $\mathbb{F}_p$, using Galois-theoretic methods. With some restrictions on c, she shows that, for primes congruent to 1 modulo m, the proportion of points in $\mathbb{F}_p$ that are periodic points for ϕ goes to 0 as $p \to \infty$. Her work was later generalized for rational functions by Juul, et al. [**4**]. There, they show that, for many rational functions, the proportion of periodic points should be small. In [**6,** Section 3], Hu and Sha fix an n and look at power maps over $\mathbb{F}_{p^n}$. Exploiting the underlying group structure of such functions allows them to find the number of periodic points for such functions over $\mathbb{F}_{p^n}$ and to compute the asymptotic mean number of periodic points as $p \to \infty$.

In the current work, we focus on the third question in the special case that the polynomial map $\phi(z)$ can be viewed as an endomorphism of an underlying algebraic group. This restriction makes the structure of the periodic points particularly simple and is, therefore, a natural place to begin a more complete investigation of the question.

In this paper, we consider the limiting proportions of strictly periodic points and quickly see that, in fact, the naïve limit

$$\lim_{n\to\infty} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n}$$

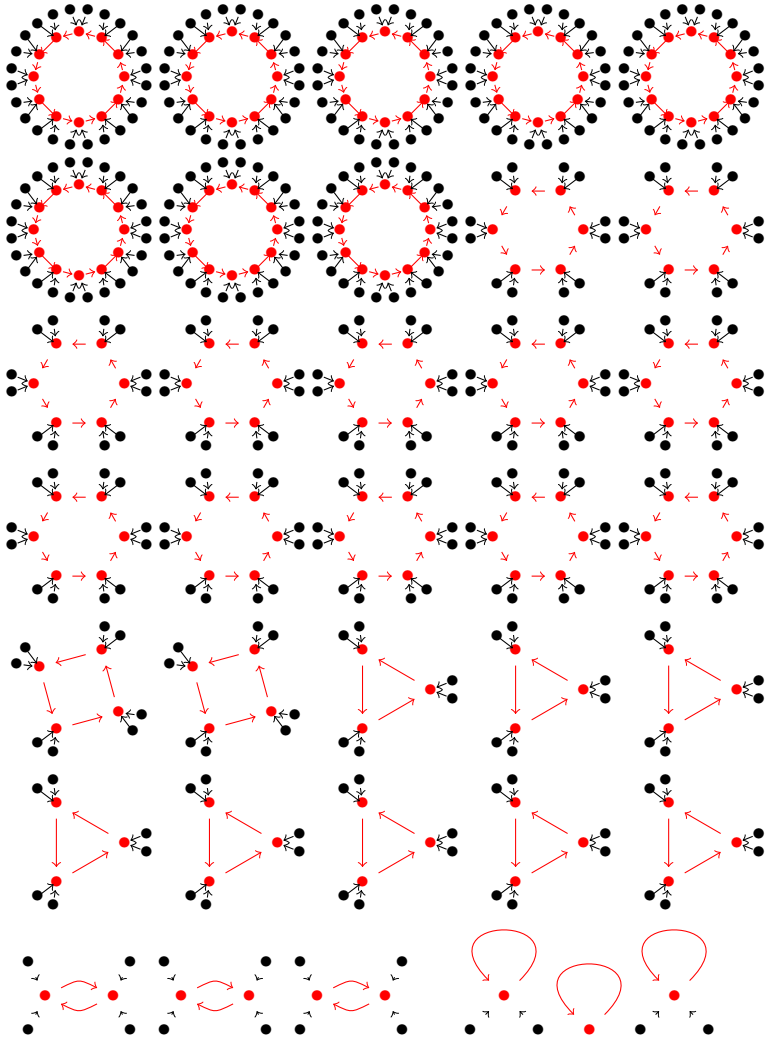

FIGURE 2. Many periodic points: $\phi(z) = z^3$ on $\mathbb{F}_{5^4}$ has 209 periodic points and 416 strictly preperiodic points.

does not exist in general, since the map ϕ acts as a permutation polynomial whenever n is relatively prime to the multiplicative order of p modulo the degree of ϕ.

However, we are able to find limiting proportions along towers of finite fields $\mathbb{F}_{p^n}$ with suitable divisibility conditions on n. For example, we have the following two results for q an odd prime. Similar results hold in the case $q = 2$ and for maps of composite degree. This work includes a proof of the composite degree case and prime $p \geq 3$ case.

Theorem 1.1 (Theorems 4.7 and 5.7)**.** *Fix a prime p, and let q be a different odd prime. Define δ to be the multiplicative order of p modulo q and $\mu = v_q\,(p^\delta - 1) \geq 1$. Let $\phi(z) = z^q$, and let $T_q(z)$ be the qth Chebyshev polynomial. Then, we have the following*:

$$\lim_{\substack{n\to\infty \\ \delta|n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \frac{1}{q^{\mu+\nu}},$$

and

$$\lim_{\substack{n\to\infty \\ \delta|2n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(T_q, \mathbb{F}_{p^n})}{p^n} = \frac{q^{\mu+\nu}+1}{2q^{\mu+\nu}}.$$

This first result is related to, but different from, the results in **[6,** Section 4], in which Hu and Sha examine the asymptotic mean number of fixed points for a power map ϕ over $\mathbb{F}_{p^n}$ as $n \to \infty$. They find that, under strict conditions on m, the asymptotic mean number of fixed points for $\phi(x) = x^m$ does not exist, and they provide heuristic arguments that, in general, these mean numbers will be difficult to compute.

Next is the outline of the paper and a survey of the techniques used. Section 2 is a brief overview of the two families of polynomials considered here: pure power maps and Chebyshev polynomials. Section 3 provides useful lemmas concerning q-adic valuations. Sections 4 and 5 give our main results for pure power maps and Chebyshev polynomials, respectively.

2. Polynomials associated to endomorphisms of algebraic groups. We first consider the multiplicative group $\mathbb{G}_m$ where, for a field K, the K-valued points are $\mathbb{G}_m(K) = K^*$. The endomorphism ring of $\mathbb{G}_m$ is $\mathbb{Z}$:

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathrm{End}(\mathbb{G}_m) \\ d &\longmapsto z^d. \end{aligned}$$

Hence, these pure power maps can be viewed as endomorphisms of an underlying group. Iteration of pure power maps is particularly easy to understand, as

$$\phi(z) = z^d$$

means

$$\phi^n(z) = z^{d^n}.$$

Similarly, we consider the additive group $\mathbb{G}_a$, whose underlying scheme is the affine line $\mathbb{A}^1$, which may be viewed as a quotient of $\mathbb{G}_m$:

$$\begin{aligned} \mathbb{G}_m/\{z = z^{-1}\} &\longrightarrow \mathbb{A}^1 \\ z &\longmapsto z + z^{-1}. \end{aligned}$$

Since the automorphism $z \mapsto z^{-1}$ commutes with the power map $\phi(z) = z^d$, the polynomial ϕ descends to an endomorphism of $\mathbb{A}^1$, which we denote T_d, the dth Chebyshev polynomial.

$$\begin{array}{ccc} \mathbb{G}_m & \xrightarrow{z\mapsto z^d} & \mathbb{G}_m \\ \downarrow & & \downarrow \\ \mathbb{G}_m/z \sim z^{-1} & \xrightarrow{z\mapsto z^d} & \mathbb{G}_m/z \sim z^{-1} \\ \downarrow{\scriptstyle z\mapsto z+z^{-1}} & & \downarrow{\scriptstyle z\mapsto z+z^{-1}} \\ \mathbb{A}^1 & \xrightarrow{\omega\mapsto T_d(\omega)} & \mathbb{A}^1. \end{array}$$

Taking as a definition the fact that $T_d(w) \in \mathbb{Z}[w]$ satisfies

$$T_d(z + z^{-1}) = z^d + z^{-d}, \tag{2.1}$$

we may prove existence and uniqueness of the Chebyshev polynomials along with a simple recursion

$$T_d(w) = \begin{cases} 2 & d = 0 \\ w & d = 1 \\ wT_{d-1}(w) - T_{d-2}(w) & d \geq 2. \end{cases} \tag{2.2}$$

A pleasant rule for composition of Chebyshev polynomials arises directly from the definition in (2.1):

$$T_d \circ T_e(w) = T_{de}(w) = T_e \circ T_d(w),$$

which, in turn, gives a simple form of iteration

$$T_d^n(w) = T_{d^n}(w). \tag{2.3}$$

We refer the interested reader to [**7,** Chapter 6] for more on the dynamics of pure power maps, Chebyshev polynomials and other rational maps arising from algebraic groups, including proofs of some of the statements above.

3. Preliminaries. This section contains a few facts regarding valuations and periodic points over finite fields which will be useful in the sequel. Throughout this section, p and q represent distinct primes, n is a positive integer, and we use the following, additional, notation: $v_q(n)$ is the q-adic valuation, i.e., if $n = q^\nu d$ with $q \nmid d$, then $v_q(n) = \nu$. δ is the multiplicative order of p modulo q, i.e., the smallest positive integer such that $q \mid (p^\delta - 1)$.

Since our goal is ultimately to classify periodic points in finite fields, we need to be able to recognize which points are periodic as opposed to strictly preperiodic. Our first result states that any finite set which is *forward invariant under* ϕ contains only periodic points.

Lemma 3.1. *Let $\phi(z) \in K[z]$ be a polynomial, and let $S \subseteq K$ be finite. If*

$$\phi(S) = S,$$

then $S \subseteq \mathrm{Per}(\phi, K)$.

Proof. Fix $\alpha \in S$. For every $n > 0$, we have $\phi^n(S) = S$. Hence, for every n, we can find $\beta_n \in S$ such that $\phi^n(\beta_n) = \alpha$.

Since S is finite, for some $n > m > 0$, we must have $\beta_n = \beta_m$. However, this means we have $\beta \in S$ such that

$$\phi^m(\beta) = \alpha \quad \text{and} \quad \phi^n(\beta) = \alpha, \text{ so } \phi^{n-m}(\alpha) = \alpha,$$

and α is periodic. □

The next three lemmas give us the tools to calculate the q-adic valuation of $p^{nd} - 1$ based on the valuations of $p^d - 1$ and n. These will be used to create the towers of finite fields for which we can calculate limiting proportions of periodic points. The results are different enough for $q = 2$ compared to odd primes that the cases are broken up along those lines.

Lemma 3.2. *Let p and q be distinct primes. Suppose that $v_q(p^d-1) = \mu \geq 1$ and $v_q(n) = 0$. Then, $v_q(p^{nd} - 1) = \mu$.*

Proof.

$$\begin{aligned} v_q(p^{nd} - 1) &= v_q(p^d - 1) + v_q(\underbrace{p^{(n-1)d} + p^{(n-2)d} + \cdots + p^d + 1}_{n \text{ terms, all } 1 \bmod q}) \\ &= \mu + 0 = \mu. \end{aligned}$$

□

Lemma 3.3. *Let p be an odd prime with $\max\{v_2(p-1), v_2(p+1)\} = \mu$. Let $v_2(n) = \nu \geq 1$. Then, $v_2(p^n - 1) = \mu + \nu$.*

Proof. We proceed by induction on $v_2(n)$. For every odd d, exactly one of $p^d - 1$, $p^d + 1$ is divisible by 4. (In particular, $\mu \geq 2$.) Similarly to the proof of Lemma 3.2, we have

$$\begin{aligned} v_2(p^{2d} - 1) &= v_2(p^d - 1) + v_2(p^d + 1) \\ &= v_2(p - 1) + v_2 \text{ (odd number)} \\ &\quad + v_2(p + 1) + v_2 \text{ (odd number)} \\ &= \mu + 1. \end{aligned}$$

Assume, for all n with $v_2(n) = \nu > 1$, that we have $v_2(p^n - 1) = \mu + \nu > 1$, in which case $v_2(p^n + 1) = 1$. Consider some n with $v_2(n) = \nu + 1$, and choose d odd such that $n = 2^{\nu+1}d$.

$$\begin{aligned} v_2(p^n - 1) &= v_2(p^{2^{\nu+1}d} - 1) \\ &= v_2(p^{2^\nu d} - 1) + v_2(p^{2^\nu d} + 1) \\ &= \mu + \nu + 1. \end{aligned}$$

□

Lemma 3.4. *Let q be an odd prime. Suppose that $v_q(p^d - 1) = \mu \geq 1$ and $v_q(n) = \nu$. Then, $v_q(p^{nd} - 1) = \mu + \nu$.*

Proof. The result for $\nu = 0$ is exactly Lemma 3.2. Choose k so that $p^d = 1 + kq^\mu$ (in particular, $q \nmid k$). Since $q \geq 3$ and $\mu \geq 1$, we have $q\mu \geq \mu + 2$. Hence,

$$p^{qd} = (1 + kq^\mu)^q \equiv 1 + kq^{\mu+1} \pmod{q^{\mu+2}}.$$

The result then follows by straightforward induction. □

Our main results in Sections 4 and 5 will be stated for maps of prime degree q. The following lemma shows that, in fact, the proportion of periodic points is identical for the maps of degree q and degree q^e. We focus on the prime degree case for ease of exposition.

Lemma 3.5. *Let $\phi(z) = z^q$ and $\psi(z) = z^{q^e}$. Then*:

$$\mathrm{Per}(\phi, \mathbb{F}_{p^n}) = \mathrm{Per}(\psi, \mathbb{F}_{p^n}) \quad \textit{for every } n.$$

Similarly, $\mathrm{Per}(T_q, \mathbb{F}_{p^n}) = \mathrm{Per}(T_{q^e}, \mathbb{F}_{p^n})$.

Proof. Note that $\phi^m(z) = z^{q^m}$ and $\psi^m(z) = z^{q^{em}}$. Thus, if $\phi^m(\alpha) = \alpha$, then, likewise, $\psi^m(\alpha) = \alpha$. On the other hand, if $\psi^m(\alpha) = \alpha$, then $\phi^{em}(\alpha) = \alpha$. Applying the iteration for Chebyshev polynomials in (2.3) gives the result in that case as well. □

4. Power maps. Throughout this section, we fix the polynomial

$$\phi(z) = z^q,$$

for q prime. We also take p to be any prime different from q. Our interest is in understanding the proportion of periodic points in $\mathbb{F}_{p^n}$ as n grows. In particular, we consider the following limits.

Definition 4.1. We define the following proportions for integers $\nu \geq 0$. Recall that δ is the multiplicative order of p modulo q.

$$P_\nu(\phi) = \lim_{\substack{n \to \infty \\ \delta | n \\ v_q(n) = \nu}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n}.$$

Since δ is the multiplicative order of p modulo q, we know that $\delta < q$. Thus, if n satisfies

$$\delta \mid n \quad \text{and} \quad v_q(n) = \nu,$$

then there is an n' such that

$$n = \delta n' \quad \text{and} \quad v_q(n') = \nu.$$

We will implicitly use this fact later when applying Lemma 3.4.

We begin by explicitly classifying the periodic points of ϕ in $\mathbb{F}_{p^n}$.

Lemma 4.2. *Let $p^n - 1 = q^e d$ with $q \nmid d$. Then*:

$$\operatorname{Per}(\phi, \mathbb{F}_{p^n}) = \{0\} \cup \{\alpha \in \mathbb{F}_{p^n} : \alpha^d = 1\}.$$

Proof. This was more generally proven in [**1,** Theorem 1]; we include a proof using our own notation for the convenience of the reader. The defining equation for $\mathbb{F}_{p^n}$ is

$$z^{p^n} - z = z(z^d - 1)Q(z), \tag{4.1}$$

for some monic $Q(z) \in \mathbb{Z}[z]$. Clearly, 0 is fixed by ϕ. Since $q \nmid d$, the roots of $z^d - 1$ form a group of order prime to q. Hence, $\phi(z) = z^q$ is a permutation of the group elements, and these roots are forward invariant under ϕ. Hence, we have

$$\{0\} \cup \{\alpha \in \mathbb{F}_{p^n} : \alpha^d = 1\} \subseteq \operatorname{Per}(\phi, \mathbb{F}_{p^n}).$$

Now, let α be a root of $Q(z)$; thus, in particular, $\alpha^{q^e d} = 1$, but $\alpha^d \neq 1$. Hence, for some $1 \leq i \leq e$ and some $d' \mid d$, we have $\alpha^{q^i d'} = 1$. In other words, α^{q^i} has order dividing d and is, therefore, a root of $z^d - 1$. Since roots of $z^d - 1$ are forward invariant under ϕ, α is not periodic for ϕ. □

Remark 4.3. We applied Lemma 4.2 to create the examples in Figures 1 and 2. Finding a value of $p^n - 1$ where, in the notation of the lemma, q^e is much smaller than d, gives "many periodic points." Similarly, an example where q^e is relatively large compared with d gives few periodic points.

Remark 4.4. Let q be prime, and define d_n by $p^n - 1 = q^e d_n$ where $q \nmid d_n$. It follows from Lemma 4.2 that the periodic points of z^q are 0 and roots of $z^{d_n} - 1$; thus, $\#\operatorname{Per}(z^q, \mathbb{F}_{p^n}) = d_n + 1$, see [**6,** Propostion 2.9].

The following proposition justifies our choice of limit in Definition 4.1 since the only interesting proportions of periodic points are those where $\delta \mid n$.

Proposition 4.5. *If $\delta \nmid n$, all points of $\mathbb{F}_{p^n}$ are periodic under ϕ.*

Proof. Since $\delta \nmid n$, $q \nmid p^n - 1$. The result follows immediately from Lemma 4.2. □

We now prove our main results for pure power maps. The statement is slightly different, depending upon whether $q = 2$ or q is an odd prime. The difference exactly parallels the difference between the valuation calculations in Lemmas 3.3 and 3.4.

Theorem 4.6. *Let $v_2(p-1) = \lambda$ and $\max\{v_2(p-1), v_2(p+1)\} = \mu$. Then, for $\phi(z) = z^2$, we have*

$$P_0(\phi) = \frac{1}{2^\lambda},$$

and

$$P_\nu(\phi) = \frac{1}{2^{\mu+\nu}} \quad \text{for } \nu \geq 1.$$

Proof. First, consider n odd. By Lemma 3.2, we may choose d_n odd so that $p^n - 1 = 2^\lambda d_n$. By Remark 4.4, there are $d_n + 1$ points in

$\mathrm{Per}(\phi, \mathbb{F}_{p^n})$. Then,

$$P_0(\phi) = \lim_{\substack{n\to\infty \\ n \text{ odd}}} \frac{\#\,\mathrm{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \lim_{d_n\to\infty} \frac{d_n+1}{2^\lambda d_n+1}$$
$$= \lim_{\substack{d_n\to\infty \\ d_n \text{ odd}}} \frac{d_n+1}{2^\lambda d_n+1} = \frac{1}{2^\lambda}.$$

Now, let $v_2(n) = \nu \geq 1$. By Lemma 3.3, $p^n - 1 = 2^{\mu+\nu} d_n$ with d_n odd. Again, the number of periodic points for ϕ in $\mathbb{F}_{p^n}$ is $d_n + 1$. Hence,

$$P_\nu(\phi) = \lim_{\substack{n\to\infty \\ v_2(n)=\nu}} \frac{\#\,\mathrm{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \lim_{\substack{d_n\to\infty \\ d_n \text{ odd}}} \frac{d_n+1}{2^{\mu+\nu} d_n+1} = \frac{1}{2^{\mu+\nu}}. \quad \square$$

In Tables 1 and 2, we illustrate Theorem 4.6. The data were calculated using `Sage` [**8**].

TABLE 1. $\#\,\mathrm{Per}(z^2, \mathbb{F}_{p^n})/p^n$ with n odd.

p	3	5	41	17
$\lambda = v_2(p-1)$	1	2	3	4
$\dfrac{\#\,\mathrm{Per}(z^2, \mathbb{F}_p)}{p}$	0.666666667	0.400000000	0.146341463	0.117647059
$\dfrac{\#\,\mathrm{Per}(z^2, \mathbb{F}_{p^3})}{p^3}$	0.518518518	0.256000000	0.125012696	0.0626908203
$\dfrac{\#\,\mathrm{Per}(z^2, \mathbb{F}_{p^5})}{p^5}$	0.502057613	0.250240000	0.125000008	0.0625006603
$\dfrac{\#\,\mathrm{Per}(z^2, \mathbb{F}_{p^7})}{p^7}$	0.500228624	0.250009600	0.125000000	0.0625000023
$\dfrac{1}{2^\lambda}$	0.5	0.25	0.125	0.0625

TABLE 2. $\#\operatorname{Per}(z^2, \mathbb{F}_{p^n})/p^n$ with $v_2(n) = 1$.

p	3	7	17
$\mu = \max\{v_2(p-1), v_2(p+1)\}$	2	3	4
$\frac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^2})}{p^2}$	0.222222222	0.0816326530	0.0346020761
$\frac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^6})}{p^6}$	0.126200274	0.0625079686	0.0312500401
$\frac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^{10}})}{p^{10}}$	0.125014818	0.0625000033	0.0312500000
$\frac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^{14}})}{p^{14}}$	0.125000183	0.0625000000	0.0312500000
$\frac{1}{2^{\mu+1}}$	0.125	0.0625	0.03125

Theorem 4.7. *Let q be an odd prime. We continue with the earlier notation: δ is the multiplicative order of p* modulo *q and $v_q(p^\delta - 1) = \mu \geq 1$. For $\phi(z) = z^q$, we have*

$$P_\nu(\phi) = \frac{1}{q^{\mu+\nu}}.$$

Proof. Recall that the limit for $P_\nu(\phi)$ is taken over n such that $\delta \mid n$ and $v_q(n) = \nu$. By Lemma 3.4, for such n, we have $p^n - 1 = q^{\mu+\nu} d_n$ with $q \nmid d_n$, and, by Remark 4.4, there are $d_n + 1$ points in $\operatorname{Per}(\phi, \mathbb{F}_{p^n})$. Thus,

$$\begin{aligned} P_\nu(\phi) &= \lim_{\substack{n\to\infty \\ \delta\mid n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \lim_{\substack{n\to\infty \\ \delta\mid n \\ v_q(n)=\nu}} \frac{d_n + 1}{q^{\mu+\nu} d_n + 1} \\ &= \lim_{\substack{d_n\to\infty \\ q\nmid d_n}} \frac{d_n + 1}{q^{\mu+\nu} d_n + 1} = \frac{1}{q^{\mu+\nu}}. \end{aligned}$$

□

Tables 3 and 4 illustrate Theorem 4.7 for the map $\phi(z) = z^3$. Again, the data were calculated using `Sage` [**8**].

TABLE 3. $\#\operatorname{Per}(z^3, \mathbb{F}_{p^n})/p^n$ with $v_3(n) = 0$.

p	5	19	53
δ	2	1	2
$\mu = v_3(p^\delta - 1)$	1	2	3
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^\delta})}{p^\delta}$	0.360000000	0.157894737	0.0373798505
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{2\delta}})}{p^{2\delta}}$	0.334400000	0.113573407	0.0370371591
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{4\delta}})}{p^{4\delta}}$	0.333335040	0.111117932	0.0370370371
$\dfrac{1}{3^\mu}$	0.333333333	0.111111111	0.0370370370

TABLE 4. $\#\operatorname{Per}(z^3, \mathbb{F}_{p^n})/p^n$ with $v_3(n) = 1$.

p	5	19	53
δ	2	1	2
$\mu = v_3(p^\delta - 1)$	1	2	3
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{3\delta}})}{p^{3\delta}}$	0.111168000	0.0371774311	0.0123456791
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{6\delta}})}{p^{6\delta}}$	0.111111115	0.0370370575	0.0123456790
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{12\delta}})}{p^{12\delta}}$	0.111111111	0.0370370370	0.0123456790
$\dfrac{1}{3^{\mu+1}}$	0.111111111	0.0370370370	0.0123456790

We wish to extend our results to polynomials with composite degree. Lemma 3.5 takes care of the prime power degree; thus, we are left to consider the case $\phi(z) = z^t$ for $t = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ and $r \geq 2$. For each $1 \leq i \leq r$, let

$$\delta_i \text{ be the multiplicative order of } p \text{ modulo } q_i$$

and

$$\mu_i = v_{q_i}(p^{\delta_i} - 1).$$

We also define

$$\Delta = \operatorname{lcm}\{\delta_i\}_{1 \leq i \leq r}.$$

An argument identical to the argument in Proposition 4.5 shows that, if $\gcd(\Delta, n) = 1$, then all points of $\mathbb{F}_{p^n}$ will be periodic. Unlike the case of the prime degree, however, we need not require $\Delta \mid n$ to have a nontrivial ratio of periodic points.

In order to define the appropriate towers of fields, we need a bit more notation. For each nonempty subset $I \subseteq \{1, 2, \ldots, r\}$, let

$$\delta_I = \operatorname{lcm}\{\delta_i\}_{i \in I}.$$

If $\delta_I = \delta_{I'}$, then $\delta_{I \cup I'} = \delta_I$ as well. Hence, to a fixed value of δ, we will associate the *maximal* subset $J \subseteq \{1, 2, \ldots, r\}$ such that $\delta_J \mid \delta$. Finally, given an integer n, we define an r-tuple of valuations

$$v(n) = \langle v_{q_i}(n) \rangle_{1 \leq i \leq r}.$$

We now have the tools to define limiting proportions of periodic points along appropriate towers of finite fields. Define

$$P_{\delta,\nu}(\phi) = \lim_{\substack{n \to \infty \\ \gcd(\Delta, n) = \delta \\ v(n) = \langle \nu_i \rangle}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n}.$$

Proposition 4.8. *Let $\phi(z) = z^t$ where $t = q_1^{f_1} q_2^{f_2} \ldots q_r^{f_r}$, with q_i distinct odd primes for $1 \leq i \leq r$. Then, for $J \subseteq \{1, 2, \ldots, r\}$ maximal with $\delta_J \mid \delta$,*

$$P_{\delta,\nu}(\phi) = \prod_{j \in J} \frac{1}{q_j^{\mu_j + \nu_j}}.$$

Remark 4.9. If no $\delta_i \mid \delta$, then the maximal set J is empty, and we recover the fact that all points in $\mathbb{F}_{p^n}$ are periodic in this case. This theorem also recovers our result in Theorem 4.7 when applied to the case $t = q$ for q an odd prime.

Proof of Proposition 4.8. Since J is maximal such that $\delta_J \mid \gcd(\Delta, n)$, we have

$$p^n - 1 = d_n \prod_{j \in J} q_j^{e_j} \quad \text{with} \quad \gcd(t, d_n) = 1.$$

Lemma 3.4 shows that $e_j = v_{q_j}(p^n - 1) = \mu_j + \nu_j$ for each $j \in J$.

The proof of Lemma 4.2 extends easily to this case, and we have

$$\operatorname{Per}(\phi, \mathbb{F}_{p^n}) = \{0\} \cup \{\alpha \in \mathbb{F}_{p^n} : \alpha^{d_n} = 1\}.$$

Hence,

$$\begin{aligned} P_{\delta,\nu}(\phi) &= \lim_{\substack{n \to \infty \\ \gcd(\Delta, n) = \delta \\ v(n) = \langle \nu_i \rangle}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n}. \\ &= \lim_{\substack{d_n \to \infty \\ \gcd(t, d_n) = 1}} \frac{d_n + 1}{d_n \prod_{j \in J} q_j^{\mu_j + \nu_j} + 1} \\ &= \prod_{j \in J} \frac{1}{q_j^{\mu_j + \nu_j}}. \end{aligned}$$

□

In Tables 5 and 6, we use data from `Sage` [**8**] to illustrate Proposition 4.8 for the map $\phi(z) = z^{15}$ over fields $\mathbb{F}_{2^n}$. In the notation of the theorem, we have the following:

$$\begin{array}{lll} q_1 = 3 & q_2 = 5 & p = 2 \\ \delta_1 = 2 & \delta_2 = 4 & \Delta = 4 \\ \mu_1 = v_3(2^2 - 1) = 1 & \mu_2 = v_5(2^4 - 1) = 1. & \end{array}$$

The table contains values of n with $\gcd(4, n) = \delta$.

Remark 4.10. A statement similar to Proposition 4.8 holds when t is even, although the bookkeeping is somewhat messier. One must apply the results in Lemma 3.3, with the exponent for 2 depending

TABLE 5. $\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^n})/2^n$ with $\nu = (v_3(n), v_5(n)) = (0, 0)$.

δ	1	2	4
$\frac{\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^\delta})}{2^\delta}$	1.00000000	0.500000000	0.125000000
$\frac{\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^{7\delta}})}{2^{7\delta}}$	1.00000000	0.333374023	0.0666666701
$\frac{\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^{11\delta}})}{2^{11\delta}}$	1.00000000	0.333333492	0.0666666667
$\{q_j : j \in J\}$	$\emptyset$	$\{3\}$	$\{3, 5\}$
$\prod_{j \in J} \frac{1}{q_j^{\mu_j}}$	1	0.333333333	0.0666666666

TABLE 6. $\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^n})/2^n$ with $\nu = (v_3(n), v_5(n)) = (1, 0)$.

δ	1	2	4
$\frac{\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^{3\delta}})}{2^{3\delta}}$	1.00000000	0.125000000	0.0224609375
$\frac{\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^{21\delta}})}{2^{21\delta}}$	1.00000000	0.111111111	0.0222222222
$\frac{\#\operatorname{Per}(z^{15}, \mathbb{F}_{2^{33\delta}})}{2^{33\delta}}$	1.00000000	0.111111111	0.0222222222
$\{q_j : j \in J\}$	$\emptyset$	$\{3\}$	$\{3, 5\}$
$\prod_{j \in J} \frac{1}{q_j^{\mu_j + \nu_j}}$	1	0.111111111	0.0222222222

on $\max\{v_2(p-1), v_2(p+1)\}$ and $v_2(n)$. We leave the details to the interested reader.

5. Chebyshev polynomials. Throughout this section, we consider $T_q(z)$, the Chebyshev polynomial of prime degree q. We take p to be any prime different from q. The proportions of interest in this case run over slightly different towers of finite fields than in the power map case.

Definition 5.1. We define the following proportions for integers $\nu \geq 0$. Recall that δ is the multiplicative order of p modulo q.

$$R_\nu(T_q) = \lim_{\substack{n\to\infty \\ \delta|2n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(T_q, \mathbb{F}_{p^n})}{p^n}.$$

We begin with an explicit classification of the periodic points of T_q in $\overline{\mathbb{F}_p}$. For any $\omega \in \overline{\mathbb{F}_p}$, we may solve a quadratic to find a nonzero $\zeta \in \overline{\mathbb{F}_p}$ such that $\omega = \zeta + \zeta^{-1}$.

Lemma 5.2. *Consider some nonzero $\zeta \in \overline{\mathbb{F}_p}$ and an integer $d \geq 0$. Then*:

$$\zeta + \zeta^{-1} = \zeta^d + \zeta^{-d}$$

if and only if

$$\zeta = \zeta^d \quad \text{or} \quad \zeta = \zeta^{-d}.$$

Proof.

$$\zeta + \zeta^{-1} = \zeta^d + \zeta^{-d}$$

$$\zeta^{2d} - \zeta^{d+1} - \zeta^{d-1} + 1 = 0$$
$$(\zeta^{d-1} - 1)(\zeta^{d+1} - 1) = 0.$$

Since $\zeta \neq 0$, the first factor vanishes if and only if $\zeta^d = \zeta$, and the second vanishes if and only if $\zeta^d = 1/\zeta$. □

Lemma 5.3. *Let $\omega \in \overline{\mathbb{F}_p}$. Then, $\omega \in \operatorname{Per}(T_q, \overline{\mathbb{F}_p})$ if and only if $\omega = \zeta + \zeta^{-1}$, where $\zeta^d = 1$ for some d relatively prime to q.*

Proof. Suppose that $\omega \in \overline{\mathbb{F}_p}$ is periodic for T_q, and choose ζ so that $\omega = \zeta + \zeta^{-1}$. Then,

$$T_q^n(\omega) = \omega,$$

that is,

$$T_{q^n}(\zeta + \zeta^{-1}) = \zeta^{q^n} + \zeta^{-q^n} = \zeta + \zeta^{-1}.$$

Thus, by Lemma 5.2, $\zeta^{q^n-1} = 1$ or $\zeta^{q^n+1} = 1$.

Conversely, suppose that there is a d prime to q such that $\zeta^d = 1$, and let φ be the Euler totient function. Since $d \mid (q^{\varphi(d)} - 1)$,

$$\zeta^{q^{\varphi(d)}-1} = 1,$$

that is,

$$\zeta^{q^{\varphi(d)}} = \zeta.$$

Hence, $\omega = \zeta + \zeta^{-1}$ is fixed by $T_q^{\varphi(d)}$. □

We see that counting the periodic points for $T_q(z)$ in $\mathbb{F}_{p^n}$ is reduced to counting $\zeta \in \mathbb{F}_{p^n}$ such that $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$ and $\zeta^d = 1$ for some d prime to q.

Lemma 5.4. *Let $\zeta \in \overline{\mathbb{F}_p}$. Then, $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$ if and only if $0 \neq \zeta \in \mathbb{F}_{p^n}$ or $\zeta^{p^n+1} = 1$.*

Proof. We have $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$ if and only if it satisfies

$$(\zeta + \zeta^{-1})^{p^n} = \zeta + \zeta^{-1}$$
$$\zeta^{p^n} + \zeta^{-p^n} = \zeta + \zeta^{-1}.$$

Thus, by Lemma 5.2, either $\zeta = \zeta^{p^n}$, i.e., $\zeta \in \mathbb{F}_{p^n}$, or $1/\zeta = \zeta^{p^n}$. □

Once again, the classification of periodic points explains our choice of the limit in Definition 5.1.

Proposition 5.5. *If $\delta \nmid 2n$, then all points of $\mathbb{F}_{p^n}$ are periodic under T_q.*

Proof. Given that

$$q \nmid p^{2n} - 1,$$

we conclude that

$$q \nmid p^n + 1 \quad \text{and} \quad q \nmid p^n - 1.$$

By Lemma 5.4, every $\omega \in \mathbb{F}_{p^n}$ can be written as $\zeta + \zeta^{-1}$ for some ζ with either $\zeta^{p^n-1} = 1$ or $\zeta^{p^n+1} = 1$. Since $p^n - 1$ and $p^n + 1$ are both prime to q, the result follows from Lemma 5.3. □

We now prove our main results for the Chebyshev polynomials. As in the case of pure power maps, the statements are slightly different in the case $q = 2$ versus q odd.

Theorem 5.6. *Let* $\mu = \max\{v_2(p-1), v_2(p+1)\}$. *Then*:

$$R_\nu(T_2) = \frac{2^{\mu+\nu-1} + 1}{2^{\mu+\nu+1}}.$$

Proof. Assume that $\omega \in \mathbb{F}_{p^n}$ is periodic for T_2. Then, by Lemma 5.3, $\omega = \zeta + \zeta^{-1}$, where $\zeta^d = 1$ for some odd d. Since $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$, we apply Lemma 5.4 to conclude that $\zeta^{p^n+1} = 1$ or $\zeta^{p^n-1} = 1$.

First, suppose $v_2(n) = 0$; thus, by Lemma 3.2, $v_2(p-1) = v_2(p^n-1)$. Then,

$$p^n - 1 = 2^\mu d_1, \qquad p^n + 1 = 2d_2; \tag{5.1}$$

or

$$p^n - 1 = 2d_2, \qquad p^n + 1 = 2^\mu d_1,$$

where d_1 and d_2 are odd. Note that d_1 and d_2 are relatively prime since $d_1 \mid (p^n + 1)$ and $d_2 \mid (p^n - 1)$ or vice versa, with both odd.

Similarly, if $v_2(n) = \nu \geq 1$, Lemma 3.3 shows that $v_2(p^n-1) = \mu+\nu$; thus, we have

$$p^n - 1 = 2^{\mu+\nu} d_1 \quad \text{and} \quad p^n + 1 = 2d_2,$$

where d_1 and d_2 are odd and relatively prime.

In either case, $\zeta + \zeta^{-1}$ is periodic if and only if $\zeta^{d_1} = 1$ or $\zeta^{d_2} = 1$. Each such pair (ζ, ζ^{-1}), including the pair $(1, 1)$, corresponds to a

periodic point for T_2. Therefore, we have $(d_1 + d_2)/2$ periodic points for T_2 in $\mathbb{F}_{p^n}$.

Asymptotically, $p^n + 1 \sim p^n - 1$, that is,

$$2^{\mu+\nu} d_1 \sim 2d_2,$$

thus,

$$2^{\mu+\nu-1} d_1 \sim d_2.$$

Hence,

$$\begin{aligned} R_\nu(T_2) &= \lim_{\substack{n\to\infty \\ v_2(n)=\nu}} \frac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^n})}{p^n} \\ &= \lim_{\substack{d_1\to\infty \\ d_1 \text{ odd}}} \frac{(d_1 + 2^{\mu+\nu-1} d_1)/2}{2^\mu d_1 + 1} = \frac{2^{\mu+\nu-1} + 1}{2(2^{\mu+\nu})}. \end{aligned}$$ □

Theorem 5.7. *Let q be an odd prime. Let $v_q(p^\delta - 1) = \mu \geq 1$. Then*:

$$R_\nu(T_q) = \frac{q^{\mu+\nu} + 1}{2q^{\mu+\nu}}.$$

In Tables 7 and 8, we illustrate Theorem 5.6 using data from `Sage` [**8**].

Proof. Assume $\omega \in \mathbb{F}_{p^n}$ is periodic for T_q. Then, by Lemma 5.3, $\omega = \zeta + \zeta^{-1}$, where $\zeta^d = 1$ for some d prime to q. Since $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$, we apply Lemma 5.4 to conclude that $\zeta^{p^n+1} = 1$ or $\zeta^{p^n-1} = 1$.

Since $v_q(p^\delta - 1) = \mu \geq 1$ and $v_q(n) = \nu$, by Lemma 3.4, $v_q(p^{2n} - 1) = \mu + \nu \geq 1$. Thus, $q \mid p^{2n} - 1$, which means that

$$q \mid p^n - 1 \quad \text{or} \quad q \mid p^n + 1$$

but not both. Therefore,

$$p^n - 1 = q^{\mu+\nu} d_1, \qquad p^n + 1 = d_2; \tag{5.2}$$

TABLE 7. $\#\operatorname{Per}(T_2, \mathbb{F}_{p^n})/p^n$ with n odd.

p	3	7	17
$\mu = \max\{v_2(p-1), v_2(p+1)\}$	2	3	4
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_p)}{p}$	0.333333333	0.285714286	0.294117647
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^3})}{p^3}$	0.370370370	0.311953353	0.281294525
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^5})}{p^5}$	0.374485597	0.312488844	0.281250154
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^7})}{p^7}$	0.374942844	0.312499772	0.281250001
$\dfrac{2^{\mu-1}+1}{2^{\mu+1}}$	0.375	0.3125	0.28125

TABLE 8. $\#\operatorname{Per}(T_2, \mathbb{F}_{p^n})/p^n$ with $v_2(n) = 1$.

p	3	7	17
$\mu = \max\{v_2(p-1), v_2(p+1)\}$	2	3	4
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^2})}{p^2}$	0.333333333	0.285714286	0.266435986
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^6})}{p^6}$	0.312757202	0.281251859	0.265625010
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^{10}})}{p^{10}}$	0.312503175	0.281250001	0.265625000
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^{14}})}{p^{14}}$	0.312500039	0.281250000	0.265625000
$\dfrac{2^{\mu}+1}{2^{\mu+2}}$	0.3125	0.28125	0.265625

or

$$p^n - 1 = d_2, \qquad p^n + 1 = q^{\mu+\nu} d_1,$$

where $q \nmid d_1 d_2$.

Now, $\zeta + \zeta^{-1}$ is periodic if and only if $\zeta^{d_1} = 1$ or $\zeta^{d_2} = 1$. Each such pair (ζ, ζ^{-1}), including the pairs $(1,1)$ and $(-1,-1)$ for p odd, corresponds to a periodic point for T_q. Thus, we have $(d_1 + d_2)/2$ periodic points for T_q in $\mathbb{F}_{p^n}$.

Again, $p^n + 1 \sim p^n - 1$, meaning

$$q^{\mu+\nu} d_1 \sim d_2.$$

Hence,

$$\begin{aligned} R_\nu(T_q) &= \lim_{\substack{n\to\infty \\ \delta \mid 2n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(T_q, \mathbb{F}_{p^n})}{p^n} \\ &= \lim_{\substack{d_1\to\infty \\ q\nmid d_1}} \frac{(d_1 + q^{\mu+\nu} d_1)/2}{q^{\mu+\nu} d_1 + 1} = \frac{q^{\mu+\nu}+1}{2q^{\mu+\nu}}. \end{aligned}$$

□

Remark 5.8. Theorem 5.6 states that the proportion of periodic points in the appropriate towers for T_2 is something slightly more than $1/4$, where the difference depends upon the tower. Similarly, Theorem 5.7 states that, for q an odd prime, the proportion is slightly greater than $1/2$. We can understand these results a bit more intuitively in the following way.

Consider roots of the polynomials $z^{p^n+1} - 1$ and $z^{p^n-1} - 1$ over the field $\overline{\mathbb{F}_p}$. Equation (5.2) shows that, for one of the two equations, all roots ζ yield a periodic point $\zeta + \zeta^{-1}$ for T_q. Thus, we are guaranteed something close to $p^n/2$ periodic points from roots of one of the polynomials, and we pick up a few more from roots of the other polynomial. A similar explanation for T_2 can be derived from equation (5.1).

In Table 9, we illustrate Theorem 5.7 for $T_3(z)$ over various finite fields. Note that, for the choices of primes in the table, $\delta \mid 2n$ for all integers n.

TABLE 9. $\#\operatorname{Per}(T_3, \mathbb{F}_{p^n})/p^n$ with $v_3(n) = 0$.

p	5	19	53
δ	2	1	2
$\mu = v_3(p^\delta - 1)$	1	2	3
$\dfrac{\#\operatorname{Per}(T_3, \mathbb{F}_p)}{p}$	0.600000000	0.578947368	0.509433962
$\dfrac{\#\operatorname{Per}(T_3, \mathbb{F}_{p^2})}{p^2}$	0.680000000	0.556786704	0.518689925
$\dfrac{\#\operatorname{Per}(T_3, \mathbb{F}_{p^4})}{p^4}$	0.667200000	0.555558966	0.518518579
$\dfrac{3^\mu + 1}{2 \cdot 3^\mu}$	0.666666667	0.555555556	0.518518519

Once again, we wish to extend our results to polynomials with composite degree. Lemma 3.5 takes care of prime power degree; thus, we are left to consider the case of the tth Chebyshev polynomial $T_t(z)$ for $t = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ and $r \geq 2$. We continue with the notation introduced at the end of Section 4: for each $1 \leq i \leq r$, let δ_i be the multiplicative order of p modulo q_i and $\mu_i = v_{q_i}(p^{\delta_i} - 1)$. We also define

$$\Delta = \operatorname{lcm}\{\delta_i\}_{1 \leq i \leq r}.$$

The argument in Proposition 5.5 can be modified to show that, if $\gcd(\Delta, 2n) = 1$, then all points of $\mathbb{F}_{p^n}$ will be periodic. However, as in Section 4, we need not require $\Delta \mid 2n$ to have a nontrivial ratio of periodic points.

As before, for each $n \in \mathbb{Z}$, we define an r-tuple of valuations

$$v(n) = \langle v_{q_i}(n) \rangle_{1 \leq i \leq r}.$$

We then define the ratios of interest:

$$R_{\delta,\nu}(T_t) = \lim_{\substack{n \to \infty \\ \gcd(\Delta, n) = \delta \\ v(n) = \langle \nu_i \rangle}} \frac{\#\operatorname{Per}(T_t, \mathbb{F}_{p^n})}{p^n}.$$

Theorem 5.9. *Let $t = q_1^{f_1} q_2^{f_2} \dots q_r^{f_r}$, with q_i distinct odd primes for $1 \le i \le r$. Then, there are disjoint subsets $I, J \subseteq \{1, 2, \dots, r\}$ such that*

$$R_{\delta,\nu}(T_t) = \frac{Q_I + Q_J}{2Q_I Q_J},$$

where

$$Q_I = \prod_{i \in I} q_i^{\mu_i + \nu_i} \quad \text{and} \quad Q_J = \prod_{j \in J} q_j^{\mu_j + \nu_j}.$$

Proof. Take J maximal with $\delta_J \mid \delta$; then, we know that $q_j \mid p^\delta - 1$ if and only if $j \in J$. Now, define

$$I = \{1 \le i \le r \colon q_i \mid p^\delta + 1\}.$$

Since the primes dividing t are distinct odd primes, no q_i divides both $p^\delta - 1$ and $p^\delta + 1$. Hence, $I \cap J = \emptyset$.

Now, consider any n with $\gcd(\Delta, n) = \delta$. Clearly, $q_j \mid p^n - 1$ if and only if $j \in J$. For any $i \in I$, we have

$$q_i \mid p^\delta + 1 \Longrightarrow q_i \mid p^{2\delta} - 1 \Longrightarrow q_i \mid p^{2n} - 1.$$

Since $i \notin J$, $q_i \nmid p^n - 1$. Therefore, $q_i \mid p^n + 1$. Furthermore, since $\gcd(\Delta, 2n) \mid 2\delta$, we have

$$q_i \mid p^{2n} - 1 \Longleftrightarrow q_i \mid p^{2\delta} - 1 \Longleftrightarrow i \in I \cup J,$$

that is, $q_i \mid p^n + 1$ if and only if $i \in I$. Therefore,

$$p^n - 1 = d_1 \prod_{j \in J} q_j^{e_j}, \qquad p^n + 1 = d_2 \prod_{i \in I} q_i^{e_i},$$

with $\gcd(t, d_1) = \gcd(t, d_2) = 1$. Lemma 3.4, applied to n and $2n$, respectively, shows that $e_j = \mu_j + \nu_j$ for $j \in J$ and $e_i = \mu_i + \nu_i$ for $i \in I$.

Lemma 5.3 easily extends to the case of composite degree, and we conclude that $\omega \in \mathbb{F}_{p^n}$ is periodic for T_t if and only if $\omega = \zeta + \zeta^{-1}$ with $\zeta^{d_1} = 1$ or $\zeta^{d_2} = 1$. As before, we have $(d_1 + d_2)/2$ periodic points for T_t in $\mathbb{F}_{p^n}$.

Since $p^n + 1 \sim p^n - 1$, we have

$$d_1 \prod_{j \in J} q_j^{\mu_j + \nu_j} \sim d_2 \prod_{i \in I} q_i^{\mu_i + \nu_i},$$

meaning

$$d_2 \sim d_1 \frac{Q_J}{Q_I}.$$

We can now calculate the limit:

$$\begin{aligned} R_{\delta,\nu}(T_t) &= \lim_{\substack{n \to \infty \\ \gcd(\Delta, n) = \delta \\ v(n) = \langle \nu_i \rangle}} \frac{\#\operatorname{Per}(T_t, \mathbb{F}_{p^n})}{p^n} \\ &= \lim_{\substack{d \to \infty \\ \gcd(t,d)=1}} \frac{(d_1 + d_1(Q_J/Q_I))/2}{Q_J d_1 + 1} \\ &= \frac{Q_I + Q_J}{2 Q_I Q_J}. \end{aligned}$$

□

TABLE 10. $\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^n})/2^n$ with $\nu = (v_3(n), v_5(n)) = (0, 0)$.

δ	1	2	4
$2^\delta - 1$	1	3	$3 \cdot 5$
$2^\delta + 1$	3	5	17
$\dfrac{\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^\delta})}{2^\delta}$	0.500000000	0.266662598	0.562500000
$\dfrac{\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^{7\delta}})}{2^{7\delta}}$	0.656250000	0.266666651	0.506667137
$\dfrac{\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^{11\delta}})}{2^{11\delta}}$	0.664062500	0.266666667	0.533333335
$\{q_i : i \in I\}$	$\{3\}$	$\{5\}$	$\emptyset$
$\{q_j : j \in J\}$	$\emptyset$	$\{3\}$	$\{3, 5\}$
$\dfrac{Q_I + Q_J}{2 Q_I Q_J}$	0.666666667	0.266666667	0.533333333

In Table 10, we use data from `Sage` [**8**] to illustrate Theorem 5.9 for the fifteenth Chebyshev polynomial over fields $\mathbb{F}_{2^n}$. In the notation of the theorem, we have:

$$\begin{aligned} &q_1 = 3 && q_2 = 5 && p = 2 \\ &\delta_1 = 2 && \delta_2 = 4 && \Delta = 4 \\ &\mu_1 = v_3(2^2 - 1) = 1 && \mu_2 = v_5(2^4 - 1) = 1. \end{aligned}$$

Note that, in the table, we restrict to values of n with $\gcd(4, n) = \delta$.

Acknowledgments. The three questions in the introduction grew out of Joseph Silverman's lectures and problems at the 2010 Arizona Winter School, which the authors were both lucky to attend. The authors are very grateful for the opportunity to attend Sage Days 42, where this work was begun in earnest. Thanks especially to our working group for helpful conversations and computations: Alina Bucur, Anna Haensch, Adriana Salerno, Lola Thompson and Stephanie Treneer. Thank you to Tom Tucker and Kalyani Madhu for help with the pictures. We would also like to thank Joseph Silverman for helpful comments on earlier drafts. Thanks to Igor Shparlinski and Rafe Jones for their helpful comments and numerous references to the literature. Also, thank you to the referee for helpful comments and edits.

REFERENCES

1. W.S. Chou and I.E. Shparlinski, *On the cycle structure of repeated exponentiation modulo a prime*, J. Num. Th. **107** (2004), 345–356.

2. R. Flynn and D. Garton, *Graph components and dynamics over finite fields*, Int. J. Num. Th. **10** (2014), 779–792.

3. S. Hamblen, R. Jones and K. Madhu, *The density of primes in orbits of* $zd + c$, Int. Math. Res. Not. (2015), 1924–1958.

4. J. Juul, P. Kurlberg, K. Madhu and T.J. Tucker, *Wreath products and proportions of periodic points*, Int. Math. Res. Not. (2016), 3944–3969.

5. K. Madhu, *Galois theory and polynomial orbits*, Ph.D. dissertation, University of Rochester, Rochester, NY, 2011.

6. M. Sha and S. Hu, *Monomial dynamical systems of dimension one over finite fields*, Acta Arith. **148** (2011), 309–331.

7. J.H. Silverman, *The arithmetic of dynamical systems*, Grad. Texts Math. **241** (2007).

8. The Sage Developers, *SageMath, The Sage mathematics software* (Version 4.7.2), 2011, `https://www.sagemath.org`.

University of Hawaii, Department of Mathematics, 2565 McCarthy Mall, Honolulu, HI 96822
Email address: **mmanes@math.hawaii.edu**

Westminster College, Department of Mathematics, 1840 S 1300 E, Salt Lake City, UT 84105
Email address: **bthompson@westminstercollege.edu**