PRIMITIVE PRIME DIVISORS IN THE CRITICAL ORBIT OF POLYNOMIAL DYNAMICAL SYSTEMS

by
MOHAMED WAFIK MAHMOUD HASSAN ELSHEIKH

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Master of Science

Sabancı University
July 2022

ABSTRACT

PRIMITIVE PRIME DIVISORS IN THE CRITICAL ORBIT OF POLYNOMIAL DYNAMICAL SYSTEMS

MOHAMED WAFIK MAHMOUD HASSAN ELSHEIKH

Mathematics, Master Thesis, JULY 2022

Thesis Supervisor: Assoc. Prof. Mohammad Sadek

Keywords: dynamical systems, periodic point, p-adic dynamics, primitive prime divisors, critical orbit

Let $f_{d,c}(x) = x^d + c \in \mathbb{Q}[x]$, $d \geq 2$. We write $f_{d,c}^n$ for $\underbrace{f_{d,c} \circ f_{d,c} \circ \cdots \circ f_{d,c}}_{\text{n times}}$. The critical orbit of $f_{d,c}(x)$ is the set $\mathcal{O}_{f_{d,c}}(0) := \{f_{d,c}^n(0) : n \geq 0\}$.

For a sequence $\{a_n : n \geq 0\}$, a primitive prime divisor for a_n is a prime dividing a_n but not a_k for any $1 \leq k < n$. A result of H. Krieger asserts that if the critical orbit $\mathcal{O}_{f_{d,c}}(0)$ is infinite, then each element in $\mathcal{O}_{f_{d,c}}(0)$ has at least one primitive prime divisor, except possibly for 23 elements. In addition, under certain conditions, R. Jones proved that the density of primitive prime divisors appearing in any orbit of $f_{d,c}(x)$ is always 0.

Inspired by the previous results, we display an upper bound on the count of primitive prime divisors of a fixed iteration $f_{d,c}^n(0)$. We also investigate primitive prime divisors in the critical orbit of $f_{d,c}(x) \in K[x]$, where K is a number field. We develop links between the existence of a primitive prime divisor in the critical orbit and the periodicity of the critical orbit of the reduction of $f_{d,c}$ in the residue field of K modulo the primitive prime divisor. Consequently, under certain assumptions, we calculate the density of primes that can appear as primitive prime divisors of $f_{2,c}^n(0)$ for some $c \in \mathbb{Q}$. Furthermore, we show that there is no uniform upper bound on the count of primitive prime divisors of $f_{d,c}^n(0)$ that does not depend on c. In particular, given $N > 0$, there is $c \in \mathbb{Q}$ such that $f_{d,c}^n(0)$ has at least N primitive prime divisors.

ÖZET

POLİNOM DİNAMİK SİSTEMLERİN KRİTİK YÖRÜNGESİNDEKİ İLKEL ASAL BÖLENLER

MOHAMED WAFIK MAHMOUD HASSAN ELSHEIKH

Matimatik, Yüksek Lisans Tezi, TEMMUZ 2022

Tez Danışmanı: Doç. Dr. Mohammad Sadek

Anahtar Kelimeler: dinamik sistemler, periyodik nokta, p-adic dinamik, ilkel asal bölenler, kritik yörünge

$f_{d,c}(x)=x^d+c \in \mathbb{Q}[x]$ ve $d \geq 2$ olsun. $\underbrace{f_{d,c} \circ f_{d,c} \circ \cdots \circ f_{d,c}}_{\text{n kez}}$ için $f_{d,c}^n$ yazalım. $f_{d,c}(x)$ fonksiyonunun kritik yörüngesi $\mathcal{O}_{f_{d,c}}(0) := \{f_{d,c}^n(0) : n \geq 0\}$ kümesidir. $\{a_n : n \geq 0\}$ dizisi için, a_n'in ilkel bir asal böleni a_n'i bölen, ancak $1 \leq k < n$ için herhangi bir a_k'yı bölmeyen bir asal bölendir. H. Krieger'in bir sonucu, eğer $\mathcal{O}_{f_{d,c}}(0)$ kritik yörüngesi sonsuzsa, $\mathcal{O}_{f_{d,c}}(0)$ içindeki her elemanın, muhtemelen 23 eleman hariç, en az bir ilkel asal bölene sahip olduğunu iddia eder. Ek olarak, belirli koşullar altında, R. Jones, $f_{d,c}(x)$ herhangi bir yörüngede görünen ilkel asal bölenlerin yoğunluğunun her zaman 0 olduğunu kanıtladı.

Önceki sonuçlardan esinlenerek, sabit bir $f_{d,c}^n(0)$ yinelemesinin ilkel asal bölenlerinin sayısı üzerinde bir üst sınır gösteriyoruz. Ayrıca $f_{d,c}(x) \in K[x]$ kritik yörüngesindeki ilkel asal bölenleri araştırıyoruz, burada K bir sayı cismidir. Kritik yörüngede ilkel bir asal bölenin varlığı ile ilkel asal bölen K modülünün kalıntı alanındaki $f_{d,c}$ azalmasının kritik yörüngesinin periyodikliği arasında bağlantılar geliştiriyoruz. Sonuç olarak, belirli varsayımlar altında, bazı $c \in \mathbb{Q}$ için $f_{2,c}^n(0)$'ın ilkel asal bölenleri olarak görünebilen asal sayıların yoğunluğunu hesaplıyoruz. Ayrıca, $f_{d,c}^n(0)$'ın c'ye bağlı olmayan ilkel asal bölenlerinin sayısında tek tip bir üst sınır olmadığını gösteriyoruz. Özellikle, $N > 0$ verildiğinde, öyle bir $c \in \mathbb{Q}$ vardır ki, $f_{d,c}^n(0)$ en az N ilkel asal bölene sahiptir.

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Assoc. Prof. Dr. Mohammad Sadek for his great help and motivation during my studies. His dedication and constant support at all times encouraged me to do my best. No matter how busy his schedule was, he was always available to advise and help me and all his students with great insight, great passion, and great patience.

I also would like to thank the jury members, Assoc. Prof. Dr. Kağan Kurşungöz and Assoc. Prof. Dr. Omran Ahmadi, for their review of my thesis.

I also want to thank Dr. Mohammad Sadek again and Dr. Nermine El Sissi. This time as my unofficial family. They have motivated me to move forward in my academic life as in well as everything else. They helped me settle in Turkey and gave me the opportunity to move forward. They inspired and motivated me to become a better person. I am extremely grateful that I met them during my journey.

I would also like to thank my wife, Tuğba Yesin, for her support and motivation through everything, for her understanding and help whenever she can, and for being here through the ups and downs. Her presence in my life made this journey easier and enjoyable. I am extremely lucky to have her by my side.

Many thanks to my friend and my brother, Mohamed Darwish, for his constant encouragement, and for the great companionship he gave me through the years. He was one of the reasons I got back on track when I was drifting away from my goals. He was a great support in both Egypt and Turkey.

I would also like to take this opportunity to thank my friends in the mathematics program at Sabancı University, Antigona Pajaziti and Ali Ahmed for their invaluable friendship.

I also want to thank my whole family, in Egypt and in Turkey, for their support and their prayers which got me to this point.

Last but not least, I gratefully acknowledge the support provided by TÜBİTAK 1001 programme, project number 120F308.

To my family

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

Let K be a field, and let $f_{d,c}(x) = x^d + c \in K[x]$. We denote the n^{th} iterate of $f_{d,c}$ by $f^n_{d,c}(x)$ for $n \geq 0$, where $f^0_{d,c}(x) = x$ and $f^n_{d,c}(x) = f_{d,c}(f^{n-1}_{d,c}(x))$. We also denote the orbit of $a_0 \in K$ by $\mathcal{O}(a_0)$, where $\mathcal{O}(a_0) := \{f^n_{d,c}(a_0) : n \geq 0\}$. The orbit of 0 is called the critical orbit of $f_{d,c}(x)$. We now assume that K is a number field with a ring of integers R. Let $\mathfrak{p}$ be a prime ideal in R with the corresponding discrete valuation $\nu_{\mathfrak{p}}$, then $\mathfrak{p}$ is called a primitive prime divisor of $f^n_{d,c}(a_0)$ if $f^n_{d,c}(a_0) \neq 0$, $\nu_{\mathfrak{p}}(f^n_{d,c}(a_0)) > 0$, and $\nu_{\mathfrak{p}}(f^t_{d,c}(a_0)) = 0$ for all $1 \leq t < n$.

The primitive prime divisors of the critical orbit of polynomials of the form $f_{d,c}(x)$ have been extensively studied in the literature. The critical orbit of $f_{d,c}(x) \in \mathbb{Z}[x]$ was investigated in [10]. If the orbit is finite, we only need to check finitely many iterates to fully study the primitive prime divisors. In [10, Lemma 8], it was proven that the critical orbit is infinite for all $f_{d,c}(x) \in \mathbb{Z}[x]$ except for three cases, $c = 0$; $c = -1$ and d is even; or $c = -2$ and $d = 2$. In [10, Theorem 3], it was shown that when the critical orbit is infinite, then there is at least one primitive prime divisor of $f^n_{d,c}(0)$ for all $n \geq 2$ when $c = \pm 1$ and for all $n \geq 1$ otherwise.

These results were later generalized by H. Krieger in [19], to $f_{d,c}(x) \in \mathbb{Q}[x]$. For the critical orbit, it was observed that when $c = \frac{a}{b} \in \mathbb{Q}$, where $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ and $b \geq 2$, then $f^n_{d,c}(0) = \frac{a_n}{b^{d^{n-1}}}$, where $a_n \in \mathbb{Z}$ and $\gcd(a_n, b) = 1$. This means that when $c \notin \mathbb{Z}$, the critical orbit is always infinite. Therefore, it was shown in [19, Theorem 1.1] that for all $n \geq 1$, there is at least one primitive prime divisor of $f^n_{d,c}(0)$ except possibly for 23 values of n. Moreover, it was proved in [19, Theorem 1.3] that, unless d is even and $c \in (-2^{\frac{1}{d-1}}, -1)$, for all $n > 2$, $f^n_{d,c}(0)$ has at least one primitive prime divisor.

These results give an insight into the lower bound of the number of primitive prime divisors of $f^n_{d,c}(0)$. For the upper bound, we used some of the results in [19] to give an elementary upper bound in Theorem 4.23. Although the bound is an elementary bound, it raises the question if a uniform bound that does not depend on the value of c might exist or not. However, we show that the answer is negative. This is due to the following result, which can be found as Corollary 5.10 in Chapter 5.

Theorem 1.1. *Let d be a positive integer and $U = \{(n_i, t_i)\}_{i=1}^{m}$ be a finite set of pairs of positive integers. Then there exists an integer c such that $f_{d,c}^{n_i}(0)$ has at least t_i primitive prime divisors for each $1 \leq i \leq m$.*

This implies that fixing the degree $d \geq 2$ and the iteration $n \geq 1$, there is a polynomial of the form $f_{d,c}(x)$ for some $c \in \mathbb{Q}$ such that $f_{d,c}^{n}(0)$ has arbitrarily many primitive prime divisors. This means that the upper bound on the count of primitive prime divisors must depend on the value of c. Corollary 5.10 along with [17, Theorem 3.3] also give rise to Corollary 5.12 which gives a method to construct polynomials $f_{d,c}(x) \in \mathbb{Z}[x]$ such that the Galois group of the splitting field of $f_{d,c}^{n}(x)$ is maximal.

Another direction of studies has been conducted to calculate the density of primes appearing as primitive prime divisors in an orbit. R. W. K. Odoni, in [23, Theorem 2], proved that for the polynomial $f(x) = x^2 - x + 1 \in \mathbb{Q}[x]$, and denoting the set of primes appearing as primitive prime divisors for $f^n(a_0)$ for some $n \geq 0$ and $a_0 \in \mathbb{Q}$ by $P(f, a_0)$, the density of the set $P(f, 2)$ in the set of all primes is 0. Furthermore, in [23, Section 8], it was observed that changing a_0 to any other value such that $\{0,1\} \cap \mathcal{O}(a_0) = \emptyset$, yields the same result.

Later, these results were generalized by R. Jones in [17]. He proved that for some families of polynomials, including $f(x) = x^2 - kx + k$ for $k \in \mathbb{Z}$ and $x^2 + k$ for $k \in \mathbb{Z} \setminus \{-1\}$, the density of primes in $P(f, a_0)$ for any $a_0 \in \mathbb{Z}$ is zero, see [17, Theorem 1.2]. Moreover, denoting the set of primes dividing some elements in the set $\{g \circ f^n(a_0)\}_{n \geq 0}$ by $P(g, f, a_0)$, in [17, Theorem 1.1], it was proven, under certain assumptions on $f, g \in \mathbb{Z}[x]$, that for any $a_0 \in \mathbb{Z}$, the density of $P(g, f, a_0)$ is 0.

In [13], the latter results were generalized, under certain condition on the field K and the polynomial $f_{d,c}(x) \in K[x]$. More precisely, the density of primitive prime divisors in the orbit of any $a_0 \in K$ under the iterates of $f_{d,c}(x) \in K[x]$ was proved to be zero, see [13, Theorem 1].

Inspired by these studies, we investigate the density of the set $\mathcal{P}$ of primes that can appear as primitive prime divisors for $f_{d,c}^{n}(0)$ for some $c \in \mathbb{Q}$. We also note that in [17, Theorem 3.3], the value of $\nu_p(f_{d,c}^{n}(0))$ was crucial for studying the structure of Galois groups attached to the splitting fields of the iterations of $f_{d,c}(x)$. This motivates studying the density of the set $\mathcal{P}_T$ of primes that can appear with certain powers T as primitive divisors of $f_{d,c}^{n}(0)$ for some $c \in \mathbb{Q}$. In fact, the difference $\mathcal{P} \setminus \mathcal{P}_T$ for any T is finite, according to Corollary 4.9. For the case $d = 2$, conditional results on the densities of $\mathcal{P}$ and $\mathcal{P}_T$ are given in Theorem 5.3. In general, we have a partial answer that gives rise to the following theorem that can be found as Theorem 5.7 in Chapter 5.

Theorem 1.2. *For all $d \geq 2$ and $n \geq 1$, there are infinitely many primes p such that, there is $c \in \mathbb{Q}$ such that p is a primitive prime divisor of $f_{d,c}^n(0)$.*

To prepare for the proofs of the mentioned results, in Chapter 2 we state the main definitions and concepts about arithmetic dynamical systems. We also introduce some tools to help us in their study. After that, we introduce the notation of primitive prime divisors in integer sequences with definitions and some previous results for different integer sequences. We then talk about some related studies on those divisors in dynamical systems. Lastly, we talk briefly about post-critically finite polynomials in order to later investigate them and link them to our work.

In Chapter 3, we consider dynamical systems over a non-archimedean local field K with a ring of integers R and discrete valuation ν. We also denote the residue field of R by k with the reduction of a point $r \in R$ denoted by $\widetilde{r}$, and similarly the reduction of a polynomial $f_{d,c}(x) \in R[x]$ denoted by $\widetilde{f_{d,c}}(x)$. With these notations, we study the relation between the orbit of a point $r \in R$ under the iterations of $f_{d,c}(x)$ and the corresponding orbit of $\widetilde{r} \in k$ under the iterations of $\widetilde{f_{d,c}}(x)$. For the case that $\widetilde{r}$ is strictly preperiodic for $\widetilde{f_{d,c}}(x)$, we relate the orbit type of r and $\widetilde{r}$, and for the case where $r = 0$ and 0 is periodic for $\widetilde{f_{d,c}}(x)$, we obtain similar relations.

In Chapter 4, we work over a number field K with a ring of integers R and a prime ideal $\mathfrak{p}$. The localization at $\mathfrak{p}$ of K and R are denoted by $K_\mathfrak{p}$ and $R_\mathfrak{p}$ with the residue field $k_\mathfrak{p}$. The reduction of a point $r \in R_\mathfrak{p}$ and a polynomial $f_{d,c} \in R_\mathfrak{p}[x]$ in $k_\mathfrak{p}$ are denoted by $\widetilde{r}$ and $\widetilde{f_{d,c}}$. Fixing $t \geq 1$, we show that, except for finitely many primes, if a prime p can appear as a primitive prime divisor for $f_{d,c}^n(0)$ for some $c \in \mathbb{Q}$, then p can appear as a primitive prime divisor for $f_{d,c}^n(0)$ with $\nu_p(f_{d,c'}^n(0)) = t$ for some $c' \in \mathbb{Q}$.

We then use the tools of Chapter 4 to obtain a conditional one-to-one correspondence between the polynomials of the form $f_{d,c}(x)$ in $\mathbb{Z}_p[x]$ with periodic critical orbit, and the polynomials of the form $f_{d,c}(x)$ in $\mathbb{F}_p[x]$ with periodic critical orbit. Lastly, we move to the field $\mathbb{Q}$ and use the results from [19] to give an elementary upper bound on the count of primitive prime divisors of $f_{d,c}^n(0)$.

In Chapter 5, we investigate the densities of the sets $\mathcal{P}$ and $\mathcal{P}_T$. We first simplify the problem of finding these densities in the first section by replacing these sets with sets of primes p such that a certain polynomial has a root in $\mathbb{F}_p$. After that, we use the previous results developed in Chapter 4 to give a conditional result on the aforementioned density, with a full description of that density, for $d = 2$ in Theorem 5.3. For the general case, we also give an unconditional partial answer in Lemma 5.6, that the density is never 0, which leads to Theorem 5.7 talking about the existence of infinitely many primes that can appear as primitive prime divisors of $f^n_{d,c}(0)$ for some $c \in \mathbb{Q}$. This leads to Theorem 5.8, which briefly describes a constructive method to choose c such that certain powers of arbitrarily many primes appear in certain iterations, and Corollary 5.10 implying that there is no uniform bound on the count of primitive prime divisors of $f^n_{d,c}(0)$ that does not depend on c. We conclude by merging the result from Corollary 5.10 with [17, Theorem 3.3] to find c such that $f^n_{d,c}(x)$ has the Galois group of maximal order, which is 2^{2^n-1}.

We would like to remark that all the computations in this thesis are done using Mathematica [15] and MAGMA [5].

Chapter 2

Preliminaries

In this chapter, we work to lay the ground for our work. We give a brief about dynamical systems over different fields and rings along with important results from the literature that will help explain the direction of our work and give insights into our setup. We also introduce the notion of primitive prime divisors with a small survey of earlier results relating to different integer sequences. After that, we show how this notion relates to dynamical systems with some known results. We also discuss post-critically finite polynomials in brief to later introduce a connection between those, and primitive prime divisors in critical orbits.

2.1 Dynamical systems

We start by defining a dynamical system. The following definitions can be found in [24, p. 1] with change of some notations for the purpose of unifying the notations in our work.

Definition 2.1. *[24, p. 1] A dynamical system is a set S together with a self map $f : S \to S$ that allows iterations. The n^{th}-iterate of f is*

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}.$$

By convention, f^0 is the identity map, i.e., $f^0(x) = x$.

Definition 2.2. *[24, p. 1] For a given point $x_0 \in S$, the (forward) orbit of x_0 under the map f is the set*

$$\mathcal{O}_f(x_0) = \mathcal{O}(x_0) \quad = \quad \{f^n(x_0) : n \geq 0\}.$$

Definition 2.3. *[24, p. 1] The point $x_0 \in S$ is called a periodic point under f, if there exists an integer $n > 0$ such that $f^n(x_0) = x_0$. The orbit of x_0 is called a periodic orbit.*

An integer n such that $f^n(x_0) = x_0$ is called a period of x_0. The smallest such integer n is called the exact period of x_0. We also say that the point x_0 has period type $(0,n)$.

Definition 2.4. *[24, p. 1] The point $x_0 \in S$ is called a preperiodic point under f, if there exists an integer $m \geq 0$ such that $f^m(x_0)$ is periodic, i.e., x_0 is preperiodic if $\mathcal{O}_f(x_0)$ is finite. The orbit of x_0 is called a preperiodic orbit. If $m \neq 0$, then the point x_0 is called a strictly preperiodic point.*

The least such integer m is the tail length of the orbit, whereas the exact period of $f^m(x_0)$ is the eventual period. If the orbit of x_0 has a tail length m and an eventual period n, then we say that s has a period type (m,n).

Definition 2.5. *[24, p. 1] The sets of periodic and preperiodic points of f in S are denoted by*

$$\begin{aligned} Per(f,S) &= \{x_0 \in S : f^n(x_0) = x_0 \text{ for some } n \geq 1\} \\ PrePer(f,S) &= \{x_0 \in S : f^{n+m}(x_0) = f^m(x_0) \text{ for some } n \geq 1, m > 0\} \\ &= \{x_0 \in S : \mathcal{O}_f(x_0) \text{ is finite}\}. \end{aligned}$$

We write $Per(f)$ and $PrePer(f)$ when the set S is fixed.

From now on, following the notations of [24], we identify the set S as a local field K, with a normalized discrete valuation ν, an algebraic closure $\overline{K}$, and a ring of integers R. The maximal ideal of R is denoted $\mathfrak{p}$ and the residue field $k := R/\mathfrak{p}$.

Working inside a field allows us to use the following definition, which will be useful in many calculations.

Definition 2.6. *[24, p. 19] Let $x_0 \in K$ be a periodic point of exact period n for f. Then the multiplier f at x_0 is defined by*

$$\lambda_{x_0}(f) := (f^n)'(x_0)$$

We note that this means

$$\lambda_{x_0}(f) := \prod_{0\leq i\leq n-1} f'(f^i(x_0))$$

We denote the reduction of $f(x)$ modulo the maximal ideal $\mathfrak{p}$ by $\widetilde{f}$. We write a rational function $f(x) = \frac{F(x)}{G(x)}$ with $F(x), G(x) \in R[x]$. We also take the lowest form such that $\gcd(F,G) = 1$ in $K[x]$, and at least one of the coefficients of $F(x)$ or $G(x)$ is a unit in R, that is, it has a valuation equal to 0.

We say that a rational map written as above has good reduction modulo $\mathfrak{p}$ if $\gcd(\widetilde{F},\widetilde{G}) = 1$ in $k[x]$.

Theorem 2.7. *[24, Theorem 2.21] Let $f : K \to K$ be a rational function with degree $d \geq 2$ defined over a local field K with a non-archimedean absolute value $|.|_\nu$. Assume that f has good reduction, let $P \in K$ be a periodic point of f. Define the following quantities:*

n	*The exact period of P for the map f.*
m	*The exact period of $\widetilde{P}$ for the map $\widetilde{f}$.*
s	*The order of $\lambda_{\widetilde{f}}(\widetilde{P})$ in k^*. (If $\lambda_{\widetilde{f}}(\widetilde{P})$ is not a unit, then $s = \infty$)*
p	*The characteristic of k.*

Then n has one of the following forms:

$$n = m, \qquad n = ms, \qquad n = msp^e$$

For our work, we will be especially interested in the polynomial maps of the form $f_{d,c}(x) = x^d + c$. We also note that for this family of polynomials, there is only one critical point, i.e., a point x_0 such that $f'_{d,c}(x_0) = 0$, that is, the point $x_0 = 0$. Throughout this thesis, we will give special attention to the orbit of 0 under $f_{d,c}(x)$.

For the family of polynomials $f_{d,c}(x)$, we can see that

$$\lambda_{x_0}(f_{d,c}) := d^n \prod_{0\leq i\leq n-1} (f^i_{d,c}(x_0))^{d-1}$$

If $x_0 = 0$, then $f^0_{d,c}(0) = 0$ and so, $\lambda_0(f_{d,c}) = 0$.

2.2 Dynatomic polynomials

While searching for periodic points of $f(x) \in K(x)$ of period n, we note that these are the zeros of the polynomial $f^n(x) - x$. However, if we want to only look for points with **exact** period n, we need to exclude the points of exact period dividing n.

The dynatomic polynomials are defined as follows [24, Section 4.1]

$$\phi_n(x) := \prod_{t|n} (f^t(x) - x)^{\mu(\frac{n}{t})}.$$

Where μ is the Möbius function defined by $\mu(1) = 1$ and

$$\mu(p_1^{e_1} \dots p_r^{e_r}) = \begin{cases} (-1)^r & if\ e_1 = \dots = e_r = 1 \\ 0 & otherwise \end{cases}$$

We note that the roots of the dynatomic polynomials are periodic points of period n, but not necessarily exact period n. For that, we denote the roots of the dynatomic polynomials to be points of formal period n.

Although from the definition of the polynomial, it might not be clear that it is actually a polynomial. However, we refer to the following theorem:

Theorem 2.8. *[24, Theorem 4.5] Let $f(x) \in K(x)$ be a rational function of degree $d \geq 2$. For each $P \in \overline{K}$, let*

$$a_P(n) := \mathrm{Ord}_P(f^n(x) - x) \qquad\qquad a_P^*(n) := \mathrm{Ord}_P(\phi_n(x))$$

Then

(a) $\phi_n(x) \in K[x]$, or equivalently,

$$a_P^*(n) \geq 0\ for\ all\ n \geq 1\ and\ P \in \overline{K}.$$

(b) Let P be a point with exact period m and multiplier $\lambda(P) = (f^m)'(P)$. Then P has a formal period n (i.e., $a_P^*(n) > 0$) if and only if one of the following happens:

(i) $n = m$.

(ii) $n = ms$ and $\lambda(P)$ is a primitive s^{th} root of unity.

(iii) $n = msp^e$, *$\lambda(P)$ is a primitive s^{th} root of unity, K has characteristic p, and $e \geq 1$*

Part (a) of the previous theorem tells us that the dynatomic polynomial is, in fact, a polynomial. The second part shows the connection between points of formal period n and exact period m. In fact, if $\lambda(P)$ is not a root of unity, then P has a formal period n if and only if P has an exact period n.

For the special family $f_{d,c}(x) = x^d + c$, we give a special notation for ϕ_n to be $\phi_{d,n}$. Also, since we have just one coefficient, we can take this coefficient into account of the dynatomic polynomial in order to study the family of polynomials $f_{d,c}(x)$ for a fixed $d \geq 2$. So we work with

$$\phi_{d,n}(x,c) := \prod_{t|n} (f_{d,c}^t(x) - x)^{\mu(\frac{n}{t})}$$

Since we are especially interested in the point $x_0 = 0$, we take the polynomial evaluated at $x = 0$ to be

$$G_{d,n}(c) = \phi_{d,n}(0,c) := \prod_{t|n} (f_{d,c}^t(0))^{\mu(\frac{n}{t})}$$

We note that by the Möbius inversion, we get that

$$f_{d,c}^n(0) = \prod_{t|n} G_{d,t}(c).$$

Remark 2.9. *As we saw in the previous section, if* 0 *is periodic, then* $\lambda_0(f_{d,c}) = 0$. *This means that* λ *is not a root of unity. This implies that* 0 *can have formal period* n *if and only if* 0 *has exact period* n.

The polynomial $G_{d,n}(c)$ is called the Gleason polynomial. However, the definition of the Gleason polynomial is not entirely consistent in the literature. For example, some works define this polynomial similarly but starting with dynamical systems attached to polynomials of the form $ax^d + 1$ [6] instead of $x^d + c$ [2]. We note that even the irreducibility of these polynomials has not been proven yet. In [7, Conjecture 1.4], it has been conjectured that for $d = 2$, $G_{2,n}(c)$ is irreducible over $\mathbb{Q}[c]$ for all $n \geq 1$. Although many studies have been carried out in this direction even before formalizing the conjecture in the mentioned article, this appears to be a long-standing question with no proofs yet, even for the simplest case with $d = 2$.

2.3 Primitive Prime Divisors

We now move on to another concept, which will be linked to the dynamical systems in our work. We start in the first subsection by definitions and previous work in different setups to get an understanding of this concept. After that, we consider results from literature on the primitive prime divisors of orbits of polynomial dynamical systems.

2.3.1 Definition and Previous Results

We start by defining a primitive prime divisor in an integer sequence as follows:

Definition 2.10. *For an integer sequence $\{a_1, a_2, \dots\}$, a prime p is said to be a primitive prime divisor of a_n, if*

a. $p | a_n$, and

b. $p \nmid a_k$ for all $1 \leq k < n$

First, we introduce an elementary example to illustrate what this definition means.

Example 2.11. *Let $\{a_n : n \geq 1\}$ be a sequence in which*

$$a_1 = 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_4 = 6.$$

2 is a primitive prime divisor for a_2,

3 is a primitive prime divisor for a_3.

However, a_4 does not have any primitive prime divisors.

With this example comes the definition of the Zsigmondy set.

Definition 2.12. *For an integer sequence $\{a_1, a_2, \dots\}$, the set*

$$Z(\{a_i\}) := \{n : a_n \textit{ has no primitive prime divisors}\}$$

is called the Zsigmondy set attached to the sequence $\{a_i\}$.

Example 2.13. *For the sequence in Example 2.11, one has $4 \in Z(\{n\})$.*

Primitive prime divisors have been studied extensively in literature. Two of the sequences that have been heavily investigated are the Lucas and Lehmer numbers defined as follows:

Definition 2.14. *[4] A **Lucas pair** is a pair (α,β) of algebraic integers such that $\alpha+\beta$ and $\alpha\beta$ are non-zero coprime rational integers with $\frac{\alpha}{\beta}$ not a root of unity. For a **Lucas pair**, one defines the corresponding **Lucas numbers** by*

$$u_n = u_n(\alpha,\beta) = \frac{\alpha^n-\beta^n}{\alpha-\beta}, \qquad n = 0,1,\ldots$$

Definition 2.15. *[4] A **Lehmer pair** is a pair (α,β) of algebraic integers such that, $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers with $\frac{\alpha}{\beta}$ not a root of unity. For a **Lehmer pair**, one defines the corresponding **Lehmer numbers** by*

$$\widetilde{u_n} = \widetilde{u_n}(\alpha,\beta) = \begin{cases} \frac{\alpha^n-\beta^n}{\alpha-\beta} & \textit{If } n \textit{ is odd} \\ \frac{\alpha^n-\beta^n}{\alpha^2-\beta^2} & \textit{If } n \textit{ is even} \end{cases}$$

A famous example of these numbers is the famous Fibonnaci sequence.

Example 2.16. *Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, then $\alpha+\beta = 1 \in \mathbb{Z}$ and $\alpha\beta = -1 \in \mathbb{Z}$ with $\gcd(\alpha+\beta,\alpha\beta) = 1$.*

So, (α,β) is a Lucas pair with a corresponding Lucas numbers

$$u_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

which is the famous Fibonnaci sequence.

Remark 2.17. *If we choose for example, $\alpha = \frac{\sqrt{5}+1}{2}$ and $\beta = \frac{\sqrt{5}-1}{2}$, then $\alpha+\beta = \sqrt{5} \notin \mathbb{Z}$. In this case, (α,β) is not a Lucas pair. However, one can check that (α,β) is a Lehmer pair.*

The primitive prime divisors of Lucas and Lehmer numbers have been intensively studied in literature.

Theorem 2.18. *[8] For $\alpha,\beta \in \mathbb{R}$, $u_n(\alpha,\beta)$ has at least one primitive prime divisor for $n > 12$.*

Theorem 2.19. *[25] For $\alpha^2,\beta^2 \in \mathbb{R}$, $\widetilde{u_n}(\alpha,\beta)$ has at least one primitive prime divisor for $n > 30$.*

Theorem 2.20. *[4] For $\alpha,\beta \in \mathbb{C}$, $u_n(\alpha,\beta)$ and $\widetilde{u_n}(\alpha,\beta)$ have at least one primitive* *prime divisor for $n > 30$.*

We will now shed some light on studies related to dynamical systems.

2.3.2 Primitive Prime Divisors in Orbits of Dynamical Systems

Given a dynamical system, one can ask about the primitive prime divisors in an orbit of a point.

Given a map $f(x) \in K(x)$ and a point $a_0 \in K$, the orbit of a_0 can be thought of as the sequence $\{a_n : n \geq 0\}$, where $a_n = f^n(a_0)$. Note that, for the search of primitive divisors, we have to ignore the zero elements of the sequence if they existed. From now on, the Zsigmondy set of $\mathcal{O}_f(a_0)$ is denoted by $Z(f, a_0)$.

To study primitive prime divisors, the sequence should be infinite. For the family of polynomials that are of special interest to us, $f_{d,c}(x) = x^d + c$, there is one critical point ($x_0 = 0$). The orbit of this critical point has been investigated in many studies. For example, taking $c \in \mathbb{Z}$, the following was proven in [10].

Lemma 2.21. *[10, Lemma 8] Let $f_{d,c}(x) = x^d + c \in \mathbb{Z}[x]$ be a polynomial with $d \geq 2$. Then 0 is a preperiodic point if and only if exactly one of the following cases is true:*

(1) $c = 0$.

(2) $c = -1$ and d is even.

(3) $c = -2$ and $d = 2$.

This means, that for the search of primitive prime divisors in the critical orbit of $f_{d,c}(x) \in \mathbb{Z}[x]$, these three cases can be excluded. The following theorem can be found in [10, Theorem 3].

Theorem 2.22. *Let $f_{d,c}(x) = x^d + c \in \mathbb{Z}[x]$ be a polynomial with $d \geq 2$. If 0 is not a preperioidc point (i.e. is a wandering point), then*

(1) If $c = \pm 1$, then $f_{d,c}^n(0)$ has a primitive prime divisor for all $n \geq 2$.

(2) If $c \neq \pm 1$, then $f_{d,c}^n(0)$ has a primitive prime divisor for all $n \geq 1$.

This study was focused on $f_{d,c}$ when $c \in \mathbb{Z}$. When $c \in \mathbb{Q}$, similar results were obtained in [19]. For $c = \frac{a}{b} \in \mathbb{Q}$ with $\gcd(a, b) = 1$, it can be easily shown that $f_{d,c}^n(0) = \frac{a_n}{b^{d^{n-1}}}$, for some $a_n \in \mathbb{Z}$ with $\gcd(a_n, b) = 1$. Consequently, one can see that if 0 is preperiodic for $f_{d,c}(x)$, then $b = \pm 1$, i.e., $c \in \mathbb{Z}$. This means that Lemma 2.21 lists all polynomials $f_{d,c}(x)$ with a preperiodic orbit of 0.

For the primitive prime divisors of the critical orbit of these functions, we can look at the sequence of integers $\{a_n\}$, where $f_{d,c}^n(0) = \frac{a_n}{b^{d^{n-1}}}$. For this sequence, as mentioned before, the Zsigmondy set is denoted by $Z(f_{d,c}, 0)$. In [19], this set was studied and the following result was proved.

Theorem 2.23. *[19, Theorem 1.1] Let $f_{d,c}(x) = x^d + c \in \mathbb{Q}[x]$ be such that the critical orbit is infinite. Then $\#Z(f_{d,c}, 0) \leq 23$.*

We can look at the previous theorem from a different angle. We can say that in the critical orbit of $f_{d,c}(x)$, excluding 23 elements, the lower bound on the count of primitive prime divisors in an iteration is 1. This gives rise to our first question:

Question 2.24. *Let $f_{d,c}(x) = x^d + c$ such that the critical orbit is infinite. Let $n \geq 2$ be an integer, Is there an upper bound on the count of primitive prime divisors of $f_{d,c}^n(0)$?*

We would like to make a few remarks about the results of [19]. The integer 1 lies in $Z(f_{d,c}, 0)$ if and only if $c = \pm 1$. This means that a prime divisor p was considered primitive for $f_{d,c}(0)$ when either $p|a$ or $p|b$. However, in [13], a prime ideal $\mathfrak{q}$ was considered to be a primitive prime divisor for $f_{d,c}^n(0)$ if $\nu_{\mathfrak{q}}(f_{d,c}^n(0)) > 0$. Since the denominator in this orbit is growing in power without additional divisors, this inconsistency in the definition is only affecting $n = 1$.

The bound 23 in Theorem 2.23 is not affected whether the prime divisors of b are considered to be primitive divisors or not. This is due to the following result, where $M(c)$ denotes an integer such that, for all $n > M(c)$, $n \notin Z(f_{d,c}, 0)$.

Theorem 2.25. *[19, Theorem 1.3] Let $f_{d,c}(x) = x^d + c$ with $d \geq 2$ and $c = \frac{a}{b} \in \mathbb{Q}$. If d is odd, or d is even, and $c \notin (-2^{\frac{1}{d-1}}, -1)$, then we can take $M(c) = 2$.*

This means that the maximal bound 23 can only be attained, if possible, when $c \in (-2^{\frac{1}{d-1}}, -1)$. For this range, one must have $|a| > |b|$. This means that $|a| \neq 1$. So, there is at least one prime p such that $p|a$.

Another question that was studied in literature is about the density of primes that appear in the orbit. One of these studies is introduced in [13]. First, we summarize some definitions from that study. Denoting a number field K with algebraic closure $\overline{K}$, and a ring of integers R, a prime ideal $\mathfrak{q} \subset R$ is said to divide $\mathcal{O}_{f_{d,c}}(a_0)$ where $a_0, c \in K$, if there is $n \geq 0$ such that $f_{d,c}^n(a_0) \neq 0$ and $\nu_q(f_{d,c}^n(a_0)) > 0$. The author defines the set $P_{f_{d,c}}(a_0) := \{\mathfrak{q} \subset R : \mathfrak{q} \text{ divides } \mathcal{O}_{f_{d,c}}(a_0)\}$. With this set, the density of the prime divisors of the orbit is defined by

$$D(P_{f_{d,c}}(a_0)) := \limsup_{x\to\infty} \frac{\#\{q \in P_{f_{d,c}}(a_0) : N(\mathfrak{q}) \leq x\}}{\#\{q \subset R : N(\mathfrak{q}) \leq x\}}$$

where $N(\mathfrak{q})$ denotes the norm of the ideal $\mathfrak{q}$. With these notations and with M_K denoting the set of places of K, the following was proved:

Theorem 2.26. *[13, Theorem 1] Let K be a global field that contains a primitive d^{th} root of unity, and let $f_{d,c}(x) = x^d + c$. Suppose $c \in K$, $\mathcal{O}_{f_{d,c}}(0)$ is infinite, and one of the following holds:*

(1) There exists a non-archimedean place $\nu \in M_K$ such that $|c|_\nu < 1$, and the residue characteristic of ν is prime to d; or

(2) d is prime and for $j \geq 0$, $f^j_{d,c}(z) = g_1(z)\dots g_t(z)$ with each g_i irreducible and none of $\pm g_i(f_{d,c}(0)), g_i(f^2_{d,c}(0)), g_i(f^3_{d,c}(0)),\dots$ is a d^{th} power in K.

Then $D(P_{f_{d,c}}(a_0)) = 0$ for any $a_0 \in K$.

To elaborate, if we study $f_{d,c}(x) \in \mathbb{Q}[x]$, we can take $K = \mathbb{Q}(\zeta)$ where ζ is a primitive d^{th} root of unity and $c \in \mathbb{Q} \setminus \{0,-1,-2\}$. Condition (1) in this case translates to: if there is a prime p such that $\nu_p(c) > 0$ and $p \nmid d$. In this case, $D(P_{f_{d,c}}(a_0)) = 0$ for any $a_0 \in \mathbb{Q}$ (in general, with $a_0 \in \mathbb{Q}(\zeta)$).

Fixing $d \geq 2$, under some technical conditions, the density of primitive prime divisors in an orbit $\mathcal{O}_{f_{d,c}}(a_0)$ is 0. This raises our second question.

Question 2.27. *Fixing $d \geq 2$, $n \geq 1$, $a_0 \in K$. What is the density of the primes in the set $\{\mathfrak{p} : \mathfrak{p}$ is a primitive prime divisor of $f^n_{d,c}(a_0)$ for some $c \in K\}$?*

Another study related to primitive prime divisors in orbits was done in [17]. Denoting $H_n(f,g) := \mathrm{Gal}(K_n/K_{n-1})$, where K_n is the splitting field of $g \circ f^n$. $H_n(f,g)$ is said to be maximal if $H_n(f,g) \cong (\mathbb{Z}/2\mathbb{Z})^{\deg(g\circ f^{n-1})}$. The following was proved:

Theorem 2.28. *[17, Theorem 3.3] Let $f,g \in R[x]$ with $f(x) = ax^2 + bx + c$, and let γ be the critical point of $f(x)$. Suppose that $g \circ f^n$ is irreducible for all $n \geq 1$. If $n \geq 2$ and there is a prime $\mathfrak{p} \subset R$ such that $\nu_\mathfrak{p}(g(f^n(\gamma)))$ is odd, $\nu_\mathfrak{p}(g(f^m(\gamma))) = 0$ for all $1 \leq m < n$ and $\nu_\mathfrak{p}(2a) = 0$, then $H_n(f,g)$ is maximal.*

In the above theorem, setting g as the identity map and $f(x) = f_{2,c}(x) = x^2 + c$ where $-c$ is not a square in $\mathbb{Q}$. It follows that $f^n_{2,c}(x)$ is irreducible for all $n \geq 1$, see [9, Corollary 5]. In this case, Theorem 2.28 asserts that finding an odd primitive prime divisor p for $f^n_{2,c}(0)$ for which $\nu_p(f^n_{2,c}(0))$ is odd implies that $H_n(f_{2,c},g) \cong (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}$. In particular, there is a link between the forward orbits of polynomials and the behaviour of the Galois group of the iterates.

The condition on the power of the primitive divisor gives rise to the following question.

Question 2.29. *Fixing $d \geq 2$, $n \geq 1$, $a_0 \in K$. What is the density of primes in the set*

$$\{\mathfrak{p} : \mathfrak{p} \text{ is a primitive prime divisor of } f^n_{d,c}(a_0), \text{ and } \nu_{\mathfrak{p}}(f^n_{d,c}(a_0)) \text{ is odd for some } c \in K\}?$$

Fixing an integer $t \geq 1$, How about the following set

$$\{\mathfrak{p} : \mathfrak{p} \text{ is a primitive prime divisor of } f^n_{d,c}(a_0), \text{ and } \nu_{\mathfrak{p}}(f^n_{d,c}(a_0)) = t \text{ for some } c \in K\}?$$

2.4 Post-Critically Finite Polynomials

In this section, we discuss Post-Critically Finite (PCF) polynomials. Previous results about those polynomials will be discussed in general settings, as well as in p-adic fields, which will be of great interest to us.

Definition 2.30. *[1, Definition 1.1] A polynomial f is post-critically finite (PCF) if the orbit of each critical point is finite.*

PCF polynomials are of interest to us in finite and p-adic fields. That is because of the definition of primitive prime divisors, we can see that for $f_{d,c}(x)$, p is a primitive prime divisor for $f^n_{d,c}(0)$ is equivalent to saying that 0 is periodic with exact period n for the reduction of the polynomial $f_{d,c}(x)$ in $\mathbb{F}_p$.

Some studies have shed light on PCF polynomials. In [20], there is a complete classification of all PCF quadratic polynomials defined over $\mathbb{Q}$. Similarly, in [1], there is a similar classification of PCF cubic polynomials. We say that two maps f, g are conjugates if there exists a linear map $h(x) = ax + b \in \overline{K}[x]$ such that, $g = h \circ f \circ h^{-1}$. With this, the conjugacy class of $f \in K(x)$ is the set of all maps $g \in K(x)$ such that, g, f are conjugates. The authors proved in [20, Theorem 1] that there are exactly 12 conjugacy classes of PCF quadratic polynomials defined over $\mathbb{Q}$. Similarly, in [1, section 1], it was shown that there are 15 conjugacy classes of PCF cubic polynomials defined over $\mathbb{Q}$.

A polynomial with one critical point is called a unicritical polynomial. For the unicritical polynomials with $d = 2$, $f_{2,c}(x) = x^2 + c$, the periodic and preperiodic critical orbits were studied separately in [21]. For the preperiodic case,

Theorem 2.31. *[21, Theorem 1.1] Let $p \geq 3$ and consider the critical orbit for $f_{2,c}(x) = x^2 + c$, $c \in \mathbb{Z}_p$. If for the reduction of $f_{2,c}(x)$ in $\mathbb{F}_p[x]$ $\left(\widetilde{f_{2,c}}(x)\right)$, 0 is strictly pre-periodic with orbit type (m,n), with $m > 0$, then for $f_{2,c}(x) = x^2 + c \in \mathbb{Z}_p[x]$ either 0 has orbit type (m,n) over $\mathbb{Z}_p$ or there exists some $k \geq 1$ and $r|(p-1)$ (or possibly $r = p$ if $p = 3$) in $\mathbb{Z}$ such that*

(1) 0 has orbit type (m,n) (mod p^i) for all $i \leq k$, and

(2) 0 has orbit type (m,rn) (mod p^j) for all $j > k$.

Otherwise, 0 has an infinite orbit in $\mathbb{Z}_p$, with orbit type (m,n_i) (mod p^i) for all $i \geq 1$, where n_i is the length of the cycle in which 0 lands when its orbit is calculated (mod p^i).

For the periodic case:

Proposition 2.32. *[21, Proposition 2.4] Let $p \geq 3$ and consider the critical orbit of $f_{2,c}(x) = x^2 + c$, $c \in \mathbb{Z}_p$. If for the reduction of $f_{2,c}(x)$ in $\mathbb{F}_p[x]$ $\left(\widetilde{f_{2,c}}(x)\right)$, 0 is periodic with exact period n, then for $f_{2,c}(x) = x^2 + c \in \mathbb{Z}_p[x]$ either 0 is periodic with exact period n or 0 has an infinite orbit in $\mathbb{Z}_p$ with orbit type (m_i,n) (mod p^i) for all $i \geq 1$.*

In the next chapter, we will study the results in the thesis [21] and give a generalization of the results mentioned.

Chapter 3

PCF Unicritical Polynomials over Local Fields

In this chapter, $f_{d,c}(x) = x^d + c \in R[x]$ for $d \geq 2$ with R being the ring of integers of a non-archimedean local field K with discrete valuation ν corresponding to the unique maximal ideal $\mathfrak{p}$. The algebraic closure of K is denoted by $\overline{K}$, and the residue field of R with respect to the unique maximal ideal $\mathfrak{p}$ is denoted by $k = R/\mathfrak{p}$ with characteristic p. We denote the reduction of a point $r \in R$ modulo $\mathfrak{p}$ by $\widetilde{r}$ and the reduction modulo $\mathfrak{p}^t$ by $r + \mathfrak{p}^t$. Similarly, the reduction of a polynomial $f(x) \in R[x]$ modulo $\mathfrak{p}[x]$ is denoted by $\widetilde{f}(x)$ and the reduction modulo $\mathfrak{p}^t[x]$ by $f(x) + \mathfrak{p}^t[x]$. The units of R are denoted by R^* with $k^* = R^*/\mathfrak{p}$, where a unit in R is a point r such that $\nu(r) = 0$.

With this notation, we study the connection between the orbit structure of a point $r \in R$ under the iterations of $f_{d,c}(x) \in R[x]$, and the orbit structure of $\widetilde{r} \in k$ under the iterations of $\widetilde{f_{d,c}}(x) \in k[x]$. Since k is a finite field, the orbit of $\widetilde{r}$ must be preperiodic. So, given the orbit type of $\widetilde{r}$, we investigate the orbit structure of r. We divide the study into two sections. First, we study the case where the orbit of $\widetilde{r}$ is strictly preperiodic, i.e, the tail length of the orbit of $\widetilde{r}$ under the iterations of $\widetilde{f_{d,c}}$ is not 0. After that, we limit our scope to the critical orbit, and we continue by investigating the case that $\widetilde{0}$ is periodic under $\widetilde{f_{d,c}}(x)$.

3.1 Unicritical Polynomials with a strictly preperiodic orbit

We fix $d \geq 2$, $c \in R$, and $r \in R$. Assuming that the orbit of $\widetilde{r}$ under $\widetilde{f_{d,c}}(x)$ is strictly preperiodic in k, we investigate the orbit of r under $f_{d,c}(x)$. In particular, we are interested in whether the orbit is infinite or finite. In the case where the orbit of r

under $f_{d,c}$ is finite, we show that there are finitely many possibilities for the orbit type of r.

First, we introduce the following lemma that will be used throughout the rest of this section.

Lemma 3.1. *Let $f_{d,c}(x) = x^d + c \in R[x]$ where $\nu(d) = 0$. Let $r \in R$ be such that $\widetilde{r}$ is a strictly preperiodic point of $\widetilde{f_{d,c}}(x)$ in the residue field k. Then, if (m_t, n_t) is the period type of $r + \mathfrak{p}^t$ in $R/(\mathfrak{p}^t)$ for $f_{d,c}(x) + \mathfrak{p}^t[x]$, then $f_{d,c}^{n_t}(x) + \mathfrak{p}^{t+1}[x]$ behaves as a linear function around $f_{d,c}^{m_t}(r) + \mathfrak{p}^{t+1}$ in $R/\mathfrak{p}^{t+1}$, i.e, for $y \in \mathfrak{p}^t$*

$$\left(f_{d,c}^{n_t}\left(f_{d,c}^{m_t}(r) + y\right) - f_{d,c}^{m_t}(r)\right) + \mathfrak{p}^{t+1} = \lambda y + b + \mathfrak{p}^{t+1}$$

where $b \in \mathfrak{p}^t$ and $\lambda = \frac{\partial f_{d,c}^{n_t}(x)}{\partial x}|_{x = f_{d,c}^{m_t}(r)}$.

Proof. Let (m_t, n_t) be the period type of $r + \mathfrak{p}^t$ in $R/(\mathfrak{p}^t)$. Let $l = f_{d,c}^{m_t}(r) \in R$.

Define $g : \mathfrak{p}^t/\mathfrak{p}^{t+1} \to R/(\mathfrak{p}^{t+1})$ where $g(y) = (f_{d,c}^{n_t}(l + y) - l) + \mathfrak{p}^{t+1}$. Write $f_{d,c}^{n_t}(x) = \sum_{i=0}^{d^n} a_i \cdot x^i$ With $a_{d^n} = 1$

Note that l is a fixed point for $f_{d,c}^{n_t}(x) + \mathfrak{p}^t[x]$ in $R/(\mathfrak{p}^t)$, i.e, $\sum_{i=0}^{d^n} a_i \cdot l^i = l + b$ for some $b \in \mathfrak{p}^t$. Let $\lambda = \frac{\partial f_{d,c}^{n_t}(x)}{\partial x}|_{x=l} = \sum_{i=1}^{d^n} a_i \cdot i \cdot l^{i-1}$. So working in $R/(\mathfrak{p}^{t+1})$ we get that,

$$(f_{d,c}^{n_t}(l + y) - l) + \mathfrak{p}^{t+1} = \sum_{i=0}^{d^n} a_i \cdot (l + y)^i - l + \mathfrak{p}^{t+1}$$

Since $k \geq 1$ then, $y^2 \in \mathfrak{p}^{2k} \subseteq \mathfrak{p}^{t+1}$. This means that $(l + y)^i + \mathfrak{p}^{t+1} = l^i + i \cdot l^{i-1} \cdot y + \mathfrak{p}^{t+1}$. Hence,

$$(f_{d,c}^{n_t}(l + y) - l) + \mathfrak{p}^{t+1} = \sum_{i=0}^{d^n} a_i \cdot (l^i + i \cdot l^{i-1} \cdot y) - l + \mathfrak{p}^{t+1}$$

$$= (\sum_{i=0}^{d^n} a_i \cdot l^i - l) + \sum_{i=1}^{d^n} a_i \cdot (i \cdot l^{i-1} \cdot y) + \mathfrak{p}^{t+1}$$

$$= b + y \cdot \sum_{i=1}^{d^n} a_i \cdot i \cdot l^{i-1} + \mathfrak{p}^{t+1}$$

So,

$$g(y) = (f_{d,c}^{n_t}(l + y) - l) + \mathfrak{p}^{t+1} = b + \lambda \cdot y + \mathfrak{p}^{t+1}$$

□

Remark 3.2. *With the notations of the previous lemma, if* $l = f_{d,c}^{m}(r)$*,* $f_{d,c}^{n_t}(l) = l+b$ *where* $b \in \mathfrak{p}^t$*, and* $g : \mathfrak{p}^t/\mathfrak{p}^{t+1} \to R/(\mathfrak{p}^{t+1})$ *where* $g(y) = (f_{d,c}^{n_t}(l+y)-l)+\mathfrak{p}^{t+1}$*, then* $\mathrm{Im}(g) \subseteq \mathfrak{p}^t/\mathfrak{p}^{t+1}$*. This means that the iterates of* $g(y)$ *are well defined.*

Proof. As shown in the previous lemma, $g(y) = \lambda y + b + \mathfrak{p}^{t+1}$. Since $y, b \in \mathfrak{p}^k$, then $\lambda y + b \in \mathfrak{p}^k$. □

Using the previous lemma, we can now show that, under certain conditions, if $\widetilde{r}$ is strictly preperiodic for $\widetilde{f_{d,c}}(x)$ in k with tail length $m > 0$, then $r + \mathfrak{p}^t$ is strictly preperiodic for $f_{d,c}(x) + \mathfrak{p}^t[x]$ in $R/\mathfrak{p}^t$ with tail length m for all integers $t \geq 1$.

Lemma 3.3. *Let* $f_{d,c}(x) = x^d + c \in R[x]$ *Where* $\nu(d) = 0$*. Let* $r \in R$ *be such that* $\widetilde{r}$ *is a strictly preperiodic point of* $\widetilde{f_{d,c}}(x)$ *in the residue field* k *with period type* (m,n)*. If* $\nu(\lambda) = 0$ *where* $\lambda = \frac{\partial f_{d,c}^{n}(x)}{\partial x}|_{x=f_{d,c}^{m}(r)}$ *is the multiplier of* $f_{d,c}^{m}(r)$*, then* $r + \mathfrak{p}^t$ *is strictly preperiodic with period type* (m, n_t) *for* $f_{d,c}(x) + \mathfrak{p}^t[x]$ *for all* $t \geq 1$ *and some* $n_t \geq 1$*.*

Proof. For $t = 1$, the period type is (m,n) by the hypothesis of the lemma.

Let $r + \mathfrak{p}^t$ be a strictly preperiodic point in $R/\mathfrak{p}^t$ with period type (m, n_t). It is clear that since $R/\mathfrak{p}^{t+1}$ is a finite field, r will remain preperiodic. We want to show that the tail length is $m_{t+1} = m$.

Since $m_{t+1} \geq m$, it suffices to show that $f_{d,c}^{m}(r) + \mathfrak{p}^{t+1}$ is periodic in $R/\mathfrak{p}^{t+1}$.

In same notations as last lemma, we can write

$l = f_{d,c}^{m}(r)$, $f_{d,c}^{n_t}(l) = l + b$ where $b \in \mathfrak{p}^t$, $g(y) = (f_{d,c}^{n_t}(l+y) - l) + \mathfrak{p}^{t+1} = \lambda y + b + \mathfrak{p}^{t+1}$.

Looking at the iterates of 0 in g, we get $\{0, b + \mathfrak{p}^{t+1}, b(1+\lambda) + \mathfrak{p}^{t+1}, b(1+\lambda+\lambda^2) + \mathfrak{p}^{t+1}, \dots\}$.

If $\lambda = 1$ then $(\underbrace{1+\lambda+\dots}_{p-times}) = p$ where p is the characteristic of k. This means that $(\underbrace{1+\lambda+\dots}_{p-times}) \in \mathfrak{p}$ and since $b \in \mathfrak{p}^t$, then $g^p(0) = 0 + \mathfrak{p}^{t+1}$

If $\lambda \in R^* \setminus \{1\}$, then there is a positive integer s such that $\lambda^s + \mathfrak{p} = 1 + \mathfrak{p}$. So, $g^{s-1}(0) = b(1+\lambda+\dots+\lambda^{s-1}) + \mathfrak{p}^{t+1} = b \cdot \frac{1-\lambda^s}{1-\lambda} + \mathfrak{p}^{t+1} = 0 + \mathfrak{p}^{t+1}$.

Claim: $g^{\alpha}(0) = (f_{d,c}^{\alpha \cdot n_t + m}(r) - f_{d,c}^{m}(r)) + \mathfrak{p}^{t+1}$ for any $\alpha \geq 1$.

The proof of the claim is by induction. For $\alpha = 1$, it's trivial. Assume that it is true up to $\alpha = \alpha_0$.

$$\begin{aligned}
g^{\alpha_0+1}(0) &= g(g^{\alpha_0}(0)) \\
&= g((f_{d,c}^{\alpha_0 \cdot n_t + m}(r) - f_{d,c}^{m}(r)) + \mathfrak{p}^{t+1}) \\
&= (f_{d,c}^{n_t}[f_{d,c}^{m}(r) + \{f_{d,c}^{\alpha_0 \cdot n_t + m}(r) - f_{d,c}^{m}(r)\}] - f_{d,c}^{m}(r)) + \mathfrak{p}^{t+1} \\
&= (f_{d,c}^{n_t}(f_{d,c}^{\alpha_0 \cdot n_t + m}(r)) - f_{d,c}^{m}(r)) + \mathfrak{p}^{t+1} \\
&= (f_{d,c}^{(\alpha_0+1) \cdot n_t + m}(r) - f_{d,c}^{m}(r)) + \mathfrak{p}^{t+1}.
\end{aligned}$$

So if α is the period of 0 under the iterates of g, then

$$(f_{d,c}^{(\alpha) \cdot n_t + m}(r) - f_{d,c}^{m}(r)) + \mathfrak{p}^{t+1} = \mathfrak{p}^{t+1}.$$

Reordering the equality,

$$f_{d,c}^{(\alpha) \cdot n_t}(f^{m}(r)) + \mathfrak{p}^{t+1} = f_{d,c}^{m}(r) + \mathfrak{p}^{t+1}.$$

Or in other words,

$$f_{d,c}^{m}(r) + \mathfrak{p}^{t+1} \text{ is periodic for } f_{d,c}(x) + \mathfrak{p}^{t+1} \text{ in } R/\mathfrak{p}^{t+1}.$$

□

Corollary 3.4. *Let $f_{d,c}(x) = x^d + c \in R[x]$ where $\nu(d) = 0$. If $\widetilde{0}$ is a strictly preperiodic point of $\widetilde{f_{d,c}}(x)$ in the residue field k with period type (m,n), then $0 + \mathfrak{p}^t$ is strictly preperiodic with period type (m, n_t) for $f_{d,c}(x) + \mathfrak{p}^t$ for all $t \geq 1$ and some $n_t \geq 1$.*

Furthermore, for any $r \in R$ such that $\widetilde{r}$ is a strictly preperiodic point of $\widetilde{f_{d,c}}(x)$ in the residue field k with period type (α, β), $r + \mathfrak{p}^t$ is a strictly preperiodic of $f_{d,c}(x) + \mathfrak{p}^t$ with period type (α, β_t) for all $t \geq 1$ and some $n_t \geq 1$.

This corollary is a direct consequence of the fact that $\lambda = d^{n_t} \prod_{i=0}^{n_t - 1} (f_{d,c}^{m+i}(r))^{d-1}$. If $\nu(\lambda) \neq 0$ then either $\nu(d) > 0$ contradicting the hypothesis of the statement or $\nu\left((f_{d,c}^{m+i}(r))\right) > 0$ for some $0 \leq i \leq n_t - 1$ which means $(f_{d,c}^{m+i}(r)) \in \mathfrak{p}$. But in this case, $\widetilde{f_{d,c}}^{m+i}(\widetilde{r}) = \widetilde{0}$ is a periodic point for $\widetilde{f_{d,c}}(x)$ again contradicting the hypothesis.

With the tail length not changing, we can now use [24, Theorem 2.21] to prove that there are finitely many possibilities for the period type of the lifted point.

Theorem 3.5. *Let $f_{d,c}(x) = x^d + c \in R[x]$, where $\nu(d) = 0$. Let $r \in R$ be such that $\widetilde{r}$*

is a strictly preperiodic point of $\widetilde{f_{d,c}}(x)$ in the residue field k with period type (m,n) and $\nu(\lambda)=0$ where $\lambda=\frac{\partial f^n_{d,c}(x)}{\partial x}|_{x=f^m_{d,c}(r)}$ is the multiplier of $f^m_{d,c}(r)$, then r has infinite orbit in R, or r has orbit type (m,l) where $l=n$, $l=ns$ or $l=nsp^e$ for $s=\mathrm{Ord}_{k^*}(\lambda)$ and $0\leq e\in\mathbb{Z}$

Proof. Let $\tilde{r}$ be preperiodic with period type (m,n) in k. As seen in Lemma 3.3, r cannot be periodic in R. If r doesn't have an infinite orbit, then it must be preperiodic with tail length m.

If the period type of r in R is (m,l), then $f^m_{d,c}(r)$ is a periodic point with period l in R and its reduction $\widetilde{f_{d,c}}^m(\tilde{r})$ is periodic with period n in k. By [24, Theorem 2.21], we have $l=n,\quad l=ns$, or $l=nsp^e$. □

The previous result is for a non-archimedean local field K. Taking $K=\mathbb{Q}_p$, we obtain the following corollary.

Corollary 3.6. *Let $f_{d,c}(x)=x^d+c\in\mathbb{Z}_p[x]$, where p be a prime such that $p\nmid 6d$. If $\tilde{r}$ is strictly preperiodic for the reduced function $\widetilde{f_{d,c}}(x)$ over the residue field $\mathbb{F}_p$ with period type (m,n) and multiplier $\lambda=\frac{\partial f^n_{d,c}(x)'}{\partial x}|_{x=f^m(r)}\in\mathbb{Z}_p^*$, then either r has infinite orbit in $\mathbb{Z}_p$ or r has orbit type (m,l) where $l=n$ or $l=ns$ for $s=\mathrm{Ord}_p(\lambda)|p-1$.*

Proof. In the case of $K=\mathbb{Q}$ and $p\nmid 6$, [24, Theorem 2.28] implies that $l=nsp^e$ cannot occur. This is because the ramification index for any prime in the rational field is 1. Therefore,

$$p^{e-1}\leq\frac{2}{p-1}<1$$

Where the second inequality is due to $p\nmid 6$, that is, $p>3$. □

This corollary directly implies the period-type result mentioned in [21, Theorem 1.1] about preperiodic orbits in the case $d=2$ and $r=0$ with the exception of $p=3$. The theorem by Mullen gives more information about the change of the eventual period. Namely, in the case that the eventual period is of the form ns, there is an integer α such that $0+\mathfrak{p}^t$ has the period type (m,n) for $t<\alpha$ and the period type (m,ns) for $t\geq\alpha$.

3.2 Unicritical Polynomials with a periodic critical orbit

In this section, we only consider the critical orbit of $f_{d,c}(x)$. Starting with a unicritical polynomial with a periodic critical orbit in k and a lift of the polynomial in R, we show that there are only two possibilities for the critical orbit in R.

To do this, we prove that for the tail length must be 0. This is done in two steps. First, limiting the possibilities for the tail length. Then, we show that none of these possibilities can occur.

Before that, we show in the following lemma that the eventual period must remain n where n is the exact period of 0.

Lemma 3.7. *Let $f_{d,c}(x) = x^d + c \in R[x]$, where $\nu(d) = 0$. If $\widetilde{0}$ is periodic for $\widetilde{f_{d,c}}(x)$ in k with exact period n then 0 in R has infinite orbit or period type (m,n) for some $m \in \mathbb{Z}_{\geq 0}$.*

Proof. If 0 is not a wandering point, then for some m, $f^m_{d,c}(0)$ is periodic. We want to show that the period of $f^m_{d,c}(0)$ is n. Assume $f^m_{d,c}(0)$ has exact period l Let $k \geq \frac{m}{n}$. Then, $f^{kn}_{d,c}(0)$ is also periodic with exact period l.

Since $\widetilde{0}$ is periodic in the residue field with period n, then the reduction $\widetilde{f_{d,c}}^{kn}(\widetilde{0})$ in k is $\widetilde{0}$ which has period n. By [24, Theorem 2.21], $l = n$, $l = ns$ or $l = nsp^e$, where $s = \mathrm{Ord}_{k^*}(\lambda)$. But $f^{kn}_{d,c}(0)|\frac{\partial f^l(x))}{\partial x}|_{x=f^{kn}(0)} = \lambda$. So, the multiplier is $\lambda \in \mathfrak{p}$. This means that $s = \mathrm{Ord}_{k^*}(\lambda) = \infty$. i.e. $l = n$ or $l = \infty$ contradicting the assumption that 0 is not a wandering point. □

With the eventual period, we prove that the valuation of the difference between $f^{l+n}_{d,c} - f^l_{d,c}$ does not change within one cycle.

Lemma 3.8. *Let $f_{d,c}(x) = x^d + c \in R[x]$, where $\nu(d) = 0$.*

If $\widetilde{0}$ is periodic for $\widetilde{f_{d,c}}(x)$ in k with exact period n then for all $m \geq 1$ and $0 < a \leq n$, we have

(1) $\nu\left(f^{mn+a}_{d,c}(0) - f^{(m-1)n+a}_{d,c}(0)\right) = \nu\left(f^{mn+1}_{d,c}(0) - f^{(m-1)n+1}_{d,c}(0)\right)$.

(2) $\left(f^{mn}_{d,c}(0) - f^{(m-1)n}_{d,c}(0)\right)$ *divides* $\left(f^{mn+1}_{d,c}(0) - f^{(m-1)n+1}_{d,c}(0)\right)$.

Proof. The proof of (1) is by induction on a. For the case $a = 1$, it is the hypothesis.

Assuming that (1) is true for some a, $0 < a < n$, we prove the statement for $a+1$. Since in k, $\widetilde{0}$ is periodic with period n, then set $\beta := (f^{mn+a}_{d,c}(0) - f^{(m-1)n+a}_{d,c}(0)) \in \mathfrak{p}$, i.e, $f^{mn+a}_{d,c}(0) = f^{(m-1)n+a}_{d,c}(0) + \beta$. Let $\alpha \geq 1$ be an integer such that $\beta \in \mathfrak{p}^\alpha$ and $\beta \notin \mathfrak{p}^{\alpha+1}$.

Also, since $n \nmid ((m-1)n+a)$ and $\widetilde{0}$ has exact period n in k then, $\widetilde{f_{d,c}}^{(m-1)n+a}(\widetilde{0}) \neq \widetilde{0}$, i.e, $f_{d,c}^{(m-1)n+a}(0) \notin \mathfrak{p}$.

Now, looking at the difference

$$\begin{aligned}
& f_{d,c}^{mn+a+1}(0) - f_{d,c}^{(m-1)n+a+1}(0) + \mathfrak{p}^{\alpha+1} \\
= \quad & \left[f_{d,c}^{mn+a}(0)\right]^d - \left[f_{d,c}^{(m-1)n+a}(0)\right]^d + \mathfrak{p}^{\alpha+1} \\
= \quad & \left[f_{d,c}^{(m-1)n+a}(0)\right]^d + \beta \cdot d \cdot \left[f_{d,c}^{(m-1)n+a}(0)\right]^{d-1} - \left[f_{d,c}^{(m-1)n+a}(0)\right]^d + \mathfrak{p}^{\alpha+1} \\
= \quad & \beta \cdot d \cdot \left[f_{d,c}^{(m-1)n+a}(0)\right]^{d-1} + \mathfrak{p}^{\alpha+1},
\end{aligned}$$

where the second identity is due to the fact that $\left[f_{d,c}^{mn+a}(0)\right]^d = \left[(f_{d,c}^{(m-1)n+a}(0) + \beta)\right]^d$, and that $\beta^2 \in \mathfrak{p}^{\alpha+1}$.

Since $df_{d,c}^{(m-1)n+a}(0)^{d-1} \notin \mathfrak{p}$. And $\beta \in \mathfrak{p}^{\alpha}$ but $\beta \notin \mathfrak{p}^{\alpha+1}$ then,

$$f_{d,c}^{mn+a+1}(0) - f_{d,c}^{(m-1)n+a+1}(0) \in \mathfrak{p}^{\alpha}$$

but

$$f_{d,c}^{mn+a+1}(0) - f_{d,c}^{(m-1)n+a+1}(0) \notin \mathfrak{p}^{\alpha+1},$$

which implies that

$$\nu\left(f_{d,c}^{mn+a+1}(0) - f_{d,c}^{(m-1)n+a+1}(0)\right) = \nu(\beta) = \nu\left(f_{d,c}^{mn+a}(0) - f_{d,c}^{(m-1)n+a}(0)\right).$$

For the second part of the statement, we write $f_{d,c}^{(m-1)n}(0) = t_1$ and $\left(f_{d,c}^{mn}(0) - f_{d,c}^{(m-1)n}(0)\right) = t_2$. So,

$$\begin{aligned}
f_{d,c}^{mn+1}(0) - f_{d,c}^{(m-1)n+1}(0) &= \left[f_{d,c}^{(m+1)n}(0))\right]^d - \left[f_{d,c}^{mn}(0)\right]^d \\
&= (t_1 + t_2)^d - t_1^d \\
&= \sum_{i=1}^{d} \binom{d}{i} t_2^i t_1^{d-i} \\
&= t_2 \cdot \sum_{i=1}^{d} \binom{d}{i} t_2^{i-1} t_1^{d-i}.
\end{aligned}$$

Concluding the proof.

□

Now, we show that if the orbit is strictly preperiodic, then the tail length must be of the form $mn+1$ for some integer $m \geq 1$.

Corollary 3.9. *Let $f_{d,c}(x) = x^d + c \in R[x]$, where $\nu(d) = 0$. If $\widetilde{0}$ is periodic for $\widetilde{f_{d,c}}(x)$ in k with exact period n then 0 in R has infinite orbit, periodic with period n or preperiodic with period type $(mn+1, n)$ for some integer $m \geq 1$.*

This will be used to prove Theorem 3.10 by only showing that a tail length of the form $mn+1$ is not possible.

Proof. Assume that 0 is strictly preperiodic with period type $(mn+a, n)$ for some $m \in \mathbb{Z}_{\geq 0}$ and a, $0 < a \leq n$. This means that $f_{d,c}^{(m+1)n+a}(0) - f_{d,c}^{mn+a}(0) = 0$, i.e., $\nu\left(f_{d,c}^{(m+1)n+a}(0) - f_{d,c}^{mn+a}(0)\right) = \infty$. By Lemma 3.8 part (1), we have

$$\nu\left(f_{d,c}^{(m+1)n+1}(0) - f_{d,c}^{mn+1}(0)\right) = \infty.$$

Hence, $f_{d,c}^{(m+1)n+1}(0) - f_{d,c}^{mn+1}(0) = 0$, implying that $f_{d,c}^{mn+1}(0)$ is periodic in R. If $a > 1$, we get a contradiction since $mn+1 < mn+a$ and $f_{d,c}^{mn+1}(0)$ is periodic. So, $a = 1$.

It remains to assume $m = 0$, that is, assume that the period type of 0 is $(1, n)$. This means that $f_{d,c}^{n+1}(0) = f_{d,c}(0) = c$, i.e., $\left(f_{d,c}^{n}(0)\right)^d + c = c$. This implies $f_{d,c}^{n}(0) = 0$, which contradicts the assumption that 0 is strictly preperiodic. Therefore, $m \geq 1$. □

The previous lemma allows us to limit the possibilities for the preperiodic tails that we will investigate in order to prove the following theorem.

Theorem 3.10. *Let $f_{d,c}(x) = x^d + c \in R[x]$, where $\nu(d) = 0$ and $p > d$ where $\mathrm{char}(k) = p$. If $\widetilde{0}$ is periodic for $\widetilde{f_{d,c}}(x)$ in k with exact period n then either 0 is periodic in R with exact period n or it has an infinite orbit.*

Proof. We want to show that the tail length $mn+1$ mentioned in previous lemma is not possible. Now we assume that the tail length is $mn+1$.

Similar to the proof of Lemma 3.8, let $f_{d,c}^{mn}(0) = t_1$ with $\nu(t_1) = \alpha_1$. Now $f_{d,c}^{(m+1)n}(0) - f_{d,c}^{mn}(0) = t_2$ with $\nu(t_2) = \alpha_2$.

Then

$$\begin{aligned}
\nu\left(f_{d,c}^{(m+1)n+1}(0)-f_{d,c}^{mn+1}(0)\right) &= \nu\left((f_{d,c}^{(m+1)n}(0))^d-f_{d,c}^{mn}(0)^d\right)\\
&= \nu\left((t_1+t_2)^d-t_1^d\right)\\
&= \nu\left(\sum_{i=1}^{d}\binom{d}{i}t_2^it_1^{d-i}\right).
\end{aligned}$$

Since $p>d$, we have $p\nmid\binom{d}{i}$ for any $1\leq i\leq d$. This means that, $\nu\left(\binom{d}{i}t_2^it_1^{d-i}\right)=i\alpha_2+(d-i)\alpha_1$. Assume $\alpha_1\neq\alpha_2$. If $\nu\left(\binom{d}{i}t_2^it_1^{d-i}\right)=\nu\left(\binom{d}{j}t_2^jt_1^{d-j}\right)$ then, $i\alpha_2+(d-i)\alpha_1=j\alpha_2+(d-j)\alpha_1$ implying that $i=j$.

With the non-archimedean valuation, we get,

$$\begin{aligned}
\nu\left(\sum_{i=1}^{d}\binom{d}{i}t_2^it_1^{d-i}\right) &= \min_{1\leq i\leq d}\left(\nu\left(\binom{d}{i}t_2^it_1^{d-i}\right)\right)\\
&= \min_{1\leq i\leq d}(i\alpha_2+(d-i)\alpha_1)\\
&\neq \infty.
\end{aligned}$$

So, $f_{d,c}^{(m+1)n+1}(0)-f_{d,c}^{mn+1}(0)\neq 0$. So, for the tail length to be $mn+1$, we must have that $\alpha_1=\alpha_2=:\alpha$. We have that $f_{d,c}^n(f_{d,c}^{mn}(0))=f_{d,c}^{(m+1)n}(0)$. In other words, $f^n(t_1)=t_1+t_2$. Write $f_{d,c}^n(x)=\sum_{i=0}^{d^{n-1}}a_i\cdot x^{di}$ with $a_0=f_{d,c}^n(0)$, so we get $f_{d,c}^n(t_1)=a_0+\sum_{i=1}^{d^{n-1}}a_i\cdot t_1^{di}$, i.e,

$$t_1+t_2-\sum_{i=1}^{d^{n-1}}a_i\cdot t_1^{di}=a_0.$$

By the non-archimedean properties, we get that $\nu(a_0)=\nu\left(f_{d,c}^n(0)\right)\geq\alpha$.

If $\nu\left(f_{d,c}^n(0)\right)=\infty$, then 0 is periodic. Since the assumption is that $mn+1$ is the tail length, then $\nu\left(f_{d,c}^n(0)\right)\neq\infty$. Checking the following difference,

$$\nu\left(f_{d,c}^{n+1}(0)-f_{d,c}(0)\right)=\nu\left(f_{d,c}^n(0)^d\right)=d\cdot\nu\left(f_{d,c}^n(0)\right)\geq d\alpha>\alpha.$$

As seen in Lemma 3.8, $\nu\left(f_{d,c}^{mn+n}(0)-f_{d,c}^{mn}(0)\right)=\nu\left(f_{d,c}^{mn+1}(0)-f_{d,c}^{(m-1)n+1}(0)\right)$. This means that $\nu\left(f_{d,c}^{2n}(0)-f_{d,c}^n(0)\right)=\nu\left(f_{d,c}^{n+1}(0)-f_{d,c}(0)\right)>\alpha$.

Also, as seen in the second part of Lemma 3.8, we have that

$$[f_{d,c}^{mn}(0) - f_{d,c}^{(m-1)n}(0)] \text{ divides } [f_{d,c}^{mn+1}(0) - f_{d,c}^{(m-1)n+1}(0)],$$

i.e,

$$\nu\left(f_{d,c}^{mn+1}(0) - f_{d,c}^{(m-1)n+1}(0)\right) \geq \nu\left(f_{d,c}^{mn}(0) - f_{d,c}^{(m-1)n}(0)\right).$$

This implies that

$$\nu\left(f_{d,c}^{(m+1)n}(0) - f_{d,c}^{mn}(0)\right) \geq \nu\left(f_{d,c}^{mn}(0) - f_{d,c}^{(m-1)n}(0)\right).$$

By induction, it follows that for all $m \geq 1$,

$$\nu\left(f_{d,c}^{(m+1)n}(0) - f_{d,c}^{mn}(0)\right) > \alpha.$$

This is a contradiction because α is defined by $\nu\left(f_{d,c}^{(m+1)n}(0) - f_{d,c}^{mn}(0)\right)$ for some $m \geq 1$. □

We remark that if $K = \mathbb{Q}_p$ and $d = 2$, then this was proved in [21, Proposition 2.4].

Chapter 4

Primitive Prime Divisors and Periodic Orbits

For this chapter, K will denote a number field, with an algebraic closure $\overline{K}$ and a ring of integers R. A prime ideal in R is denoted $\mathfrak{p}$ and induces the discrete valuation $\nu_{\mathfrak{p}}$. The localization of K with respect to the valuation $\nu_{\mathfrak{p}}$ is denoted $K_{\mathfrak{p}}$ with a ring of integers $R_{\mathfrak{p}}$ and the residue field $k_{\mathfrak{p}} := R_{\mathfrak{p}}/\mathfrak{p}$. Recall that the reduction of the point $r \in R_{\mathfrak{p}}$ modulo $\mathfrak{p}$ is denoted by $\widetilde{r}$, and the reduction of the polynomial $f(x) \in R_{\mathfrak{p}}[x]$ modulo $\mathfrak{p}$ is denoted by $\widetilde{f}(x)$. Similar to [13], we consider a prime $\mathfrak{p}$ to be a primitive prime divisor for $f_{d,c}^n(0)$ if $\nu_{\mathfrak{p}}(f_{d,c}^n(0)) > 0$, and for all $1 \leq l < n$, $\nu_{\mathfrak{p}}(f_{d,c}^l(0)) = 0$.

In this chapter, we show some connections between the existence of a primitive prime divisor $\mathfrak{p}$ for $f_{d,c}^n(0)$ and the periodicity of the critical orbit of the reduction of $f_{d,c}(x)$ in $k_{\mathfrak{p}}$. With this connection, for any integer $r \geq 1$, we build methods to construct a polynomial such that $\nu_{\mathfrak{p}}\left(f_{d,c}^n(0)\right) = r$. These methods will be used in the next chapter to link Question 2.27 with Question 2.29. We then use the tools developed in this chapter together with Chapter 3 to develop a one-to-one correspondence between PCF polynomials of the form $f_{d,c}(x)$ in $\mathbb{F}_p[x]$ and the PCF polynomials of the form $f_{d,c}(x)$ in $\mathbb{Z}_p[x]$.

At the end of the chapter, we answer Question 2.24 by giving an elementary upper bound on the count of primitive prime divisors of $f_{d,c}^n(0)$ for some $d \geq 2$, $n \geq 1$ and $c \in \mathbb{Q}$. This bound gives rise to an additional question that will be answered in the following chapter.

4.1 Polynomial dynamical systems modulo prime powers

We establish in the following proposition a link between primitive prime divisors in the critical orbit of a certain polynomial $f_{d,c}(x) \in K$, and the periodicity of the critical orbit of the reduction of $f_{d,c}(x)$ modulo those primes.

Proposition 4.1. *The critical orbit of $f_{d,c}(x) = x^d + c \in K[x]$ has a primitive prime divisor $\mathfrak{p}$ for $f_{d,c}^n(0)$ such that $\nu_{\mathfrak{p}}\left(f_{d,c}^n(0)\right) \geq t$ for some integer $t \geq 1$ if and only if the reduced polynomial $f_{d,c}(x) + \mathfrak{p}^t$ has periodic critical orbit with exact period n.*

This follows directly from the definition of the primitive prime divisor and the definition of the exact period of an orbit.

Proof. First, we note that $\nu_{\mathfrak{p}}(c) \geq 0$. Otherwise, assuming $\nu_{\mathfrak{p}}(c) = \alpha < 0$, we have that $f_{d,c}(0) = c$, and assuming $\nu_{\mathfrak{p}}(f_{d,c}^n(0)) = \beta \leq \alpha$ gives us that $\nu_{\mathfrak{p}}\left(\left(f_{d,c}^n(0)\right)^d\right) = d\beta \leq d\alpha < \alpha$. Then by the non-archimedean properties of $\nu_{\mathfrak{p}}$, we have

$$\begin{aligned} \nu_{\mathfrak{p}}\left(f_{d,c}^{n+1}(0)\right) &= \nu_{\mathfrak{p}}\left(\left(f_{d,c}^n(0)\right)^d + c\right) \\ &= \min(d\beta, \alpha) \\ &= d\beta \\ &< \alpha. \end{aligned}$$

So, if $\mathfrak{p}$ is a primitive prime divisor of $f_{d,c}^n(0)$, then $\nu_{\mathfrak{p}}(f_{d,c}^n(0)) > 0$ implies that $\nu_{\mathfrak{p}}(c) \geq 0$. On the other hand if 0 is periodic for $f_{d,c}(x) + \mathfrak{p}^t$, then 0 is periodic for $\widetilde{f_{d,c}}(x)$ which implies that $\tilde{c}$ is well defined. This means that we can say that $f_{d,c}(x)$ is well defined in $R_{\mathfrak{p}}[x]$ for $\mathfrak{p}$ being either a prime such that $\mathfrak{p}$ is a primitive prime divisor $f_{d,c}^n(0)$, or $\mathfrak{p}$ being a prime such that $f_{d,c}(x) + \mathfrak{p}$ has periodic critical orbit with exact period n.

With this, we first assume that $\mathfrak{p}$ is a primitive prime divisor of $f_{d,c}^n(0)$ with $\nu_{\mathfrak{p}}(f_{d,c}^n(0)) \geq t$ then for all $1 \leq l < n$, $\nu_{\mathfrak{p}}(f_{d,c}^l(0)) = 0$, i.e, $f_{d,c}^n(0) + \mathfrak{p}^t = 0 + \mathfrak{p}^t$, and for all $1 \leq l < n$, $f_{d,c}^l(0) + \mathfrak{p}^t \neq 0 + \mathfrak{p}^t$ concluding the periodicity.

On the other hand, if 0 is periodic with exact period n for $f_{d,c}(x) + \mathfrak{p}^t$, then $f_{d,c}^n(0) + \mathfrak{p}^t = 0 + \mathfrak{p}^t$, and for all $1 \leq l < n$, $f_{d,c}^l(0) + \mathfrak{p}^t \neq 0 + \mathfrak{p}^t$. So, $\nu_{\mathfrak{p}}(f_{d,c}^n(0)) \geq t$, and for all $1 \leq l < n$, $\nu_{\mathfrak{p}}(f_{d,c}^l(0)) = 0$, which finishes the proof. □

This connection gives a different way of looking at the primitive prime divisors. This leads to the following result.

Theorem 4.2. *Let $c_0 \in K$ be such that $\mathfrak{p}$ is a primitive prime divisor for $f_{d,c_0}^n(0)$. If $\nu_{\mathfrak{p}}\left(f_{d,c_0}^n(0)\right) > 2\nu_{\mathfrak{p}}\left(\frac{\partial f_{d,c}^n(0)}{\partial c}|_{c=c_0}\right)$, then there is a unique $\overline{c_0} \in R_{\mathfrak{p}}$ such that the following occur:*

(1) $\nu_{\mathfrak{p}}\left(\overline{c_0} - c_0\right) > \nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right) \geq 0.$

(2) The point 0 is periodic with exact period n *for* $f_{d,\overline{c_0}}(x) \in R_{\mathfrak{p}}[x]$

In particular, $\nu_{\mathfrak{p}}\left(\overline{c_0} - c_0\right) = \nu_{\mathfrak{p}}\left(f^n_{d,c_0}(0)\right) - \nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right).$

Proof. That $\mathfrak{p}$ is a primitive prime divisor for $f^n_{d,c_0}(0)$ means that $\widetilde{f^n_{d,c_0}}(0) = \widetilde{0}$. Also, since $\nu_{\mathfrak{p}}\left(f^n_{d,c_0}(0)\right) > 2\nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right)$, it follows by Hensel's lemma [18, Theorem 6.28], that there's a unique $\overline{c_0} \in R_{\mathfrak{p}}$ such that $\nu_{\mathfrak{p}}\left(\overline{c_0} - c_0\right) \geq \nu_{\mathfrak{p}}\left(f^n_{d,c_0}(0)\right) - \nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right)$ and $f^n_{d,\overline{c_0}}(0) = 0 \in R_{\mathfrak{p}}$. We also have that $\nu_{\mathfrak{p}}\left(\overline{c_0} - c_0\right) = \nu_{\mathfrak{p}}\left(f^n_{d,c_0}(0)\right) - \nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right)$.

Since $\widetilde{\overline{c_0}} = \widetilde{c_0}$, then $\widetilde{f^t_{d,\overline{c_0}}}(0) = \widetilde{f^t_{d,c_0}}(0)$ for all integers $t \geq 1$. Since $\mathfrak{p}$ is primitive for $f^n_{d,c_0}(0)$, we have that for any $t < n$, $\widetilde{f_{d,\overline{c_0}}}^t(0) = \widetilde{f_{d,c_0}}^t(0) \neq \widetilde{0}$. This implies that $f^t_{d,\overline{c_0}}(0) \neq 0 \in R_p$, i.e, 0 has exact period n for $f_{d,\overline{c_0}}(x) \in R_p[x]$. □

Example 4.3. *Fix* $K = \mathbb{Q}$, $d = 2$, $c_0 = 1$, $p = 5$, $n = 3$. *We have that 5 is a primitive prime divisor for* $f^3_{2,1}(0)$. *We also have that,*

$$\nu_5(f^3_{2,1}(0)) = 1 > 0 = 2 \cdot \nu_5\left(\frac{\partial f^3_{2,c}(0)}{\partial c}|_{c=1}\right).$$

By Theorem 4.2, there is $\overline{c_0} \in \mathbb{Z}_5$ *such that,* $\overline{c_0} \equiv 1 \mod 5$, *and* $f^3_{2,\overline{c_0}}(0) = 0 \in \mathbb{Z}_5$, *i.e,* $\overline{c_0} = 1 + 5t_0$ *for some* $t_0 \in \mathbb{Z}_p$ *and* $f^3_{2,1+5t_0}(0) = 0$.

For comparison with the next example, we calculate that $t_0 = 3 + 25t_1$ *for some* $t_1 \in \mathbb{Z}_5$, *This means that* $\overline{c_0} = 16 + 125t_1$. *Working modulo* 125, *then,* $f^3_{2,16}(0) \equiv 0 \mod 125$.

We also give another example to show that it is not always true that we can lift the value of c_0 as mentioned in the theorem. For that, we check an example with the hypothesis of the statement not satisfied. In that example, we can see for any value close to c_0, that is, $\overline{c_0} = c_0 + p \cdot t$ where $t \in \mathbb{Z}_p$, we get $\nu_p(f^n_{2,\overline{c_0}}(0)) \leq \nu_p(f^n_{2,c_0}(0))$. This means that $\nu_p(f^n_{2,\overline{c_0}}(0)) < \infty$, and so 0 is not periodic of period n for $f^n_{2,\overline{c_0}}(0)$.

Example 4.4. *Fix* $K = \mathbb{Q}$, $d = 2$, $c_0 = 3$, $p = 13$, $n = 5$. *the prime 13 is a primitive prime divisor for* $f^5_{2,3}(0)$. *We see that* $\nu_{13}(f^5_{2,3}(0)) = 1$, *and* $\nu_{13}\left(\frac{\partial f^5_{2,c}(0)}{\partial c}|_{c=3}\right) = 1$.

We can see that for any $t_0 \in \mathbb{Z}_{13}$, $f^5_{2,3+13t_0}(0) \not\equiv 0 \mod 13^2$, *which implies that* $f^5_{2,3+13t_0}(0) \neq 0 \in \mathbb{Z}_{13}$. *The value of* t_0 *only need to be checked modulo 13.*

For simplification, we need to introduce the following definition.

Definition 4.5. *[12, p. 610] Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ such that $\alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{K}$ are the roots of $f(x)$ in the algebraic closure of K. The discriminant of $f(x)$ is defined by*

$$\mathrm{Disc}_x(f(x)) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Furthermore, $\mathrm{Disc}_x(f(x)) \in K$*, and* $\mathrm{Disc}_x(f(x)) = 0$ *if and only if $f(x)$ has a repeated root in $\overline{K}$.*

We note that if $f(x)$ is a monic polynomial with integer coefficients, then the discriminant is an algebraic integer. Since $f \in \mathbb{Z}[x]$, then $\mathrm{Disc}_x(f) \in \mathbb{Q}$ is an algebraic integer implying that $\mathrm{Disc}_x(f) \in \mathbb{Z}$.

We remark that the Gleason polynomials $G_{d,n}(c)$ are monic polynomials with integer coefficients by [3, Corollary 3.4]. Thus, we can talk about $\mathrm{Disc}_c(G_{d,n}(c))$ as an integer.

To replace the condition that $\nu_{\mathfrak{p}}\left(f^n_{d,c_0}(0)\right) > 2\nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right)$ in Theorem 4.2 by a simpler one, we introduce the following lemma.

Lemma 4.6. *Let $\mathfrak{p}$ be a primitive prime divisor for $f^n_{d,c_0}(0)$, then*

$$\nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right) > 0 \text{ implies that } \mathrm{Disc}_c(G_{d,n}(c)) \in \mathfrak{p}$$

where $G_{d,n}(c) := \phi_{d,n}(0,c)$ is the Gleason polynomial.

Proof. Note that $\mathfrak{p}$ is a primitive prime divisor for $f^n_{d,c_0}(0)$ means that 0 is periodic for $\widetilde{f_{d,c_0}}(x)$ in $k_{\mathfrak{p}}$ with exact period n. As mentioned in Remark 2.9, the point 0 has formal period n if and only if 0 has exact period n. This implies that $\widetilde{c_0}$ is a root of $\widetilde{G_{d,n}}(c)$, that is, $\widetilde{G_{d,n}}(\widetilde{c_0}) = 0$.
Now consider the derivative of $f^n_{d,c}(0) = \prod_{t|n} G_{d,t}(c)$ as follows.

$$\frac{\partial f^n_{d,c}(0)}{\partial c} = \sum_{t|n} \frac{\partial G_{d,t}(c)}{\partial c} \prod_{\substack{k|n \\ k \neq t}} G_{d,k}(c)$$

Since $\widetilde{G_{d,n}}(\widetilde{c_0}) = 0$ and $G_{d,n}(c_0)$ divides each term except when $t = n$ then,

$$\frac{\partial \widetilde{f_{d,c}}^{\,n}(0)}{\partial c}|_{c=\widetilde{c_0}} = \frac{\partial \widetilde{G_{d,n}}(c)}{\partial c}|_{c=\widetilde{c_0}} \prod_{\substack{k|n \\ k \neq n}} \widetilde{G_{d,k}}(\widetilde{c_0})$$

Since $\mathfrak{p}$ is primitive to $f^n_{d,c}(0)$, we have that $\widetilde{G_{d,k}}(\widetilde{c_0}) \neq 0$ for any $k < n$. So, we get that,

$$\frac{\partial \widetilde{f_{d,c}}^n(0)}{\partial c}|_{c=\widetilde{c_0}} = 0 \text{ if and only if } \frac{\partial \widetilde{G_{d,n}}^n(0)}{\partial c}|_{c=\widetilde{c_0}} = 0$$

Since $\widetilde{G_{d,n}}(\widetilde{c_0}) = 0$, then

$\dfrac{\partial \widetilde{f_{d,c}}^n(0)}{\partial c}|_{c=\widetilde{c_0}} = 0$ if and only if $\widetilde{c_0}$ is a repeated root of $\widetilde{G_{d,n}}$ implying that $\operatorname{Disc}_c(\widetilde{G_{d,n}}(c)) = 0$.

This means that $\operatorname{Disc}_c(G_{d,n}(c)) \in \mathfrak{p}$, concluding the proof. □

Remark 4.7. *The converse of the previous lemma does not hold in general. For example,* $G_{2,3}(c) = c^3 + 2c^2 + c + 1 \equiv (c+8)^2(c+9) \mod 23$. *From the factorization, we can see that* $23 | \operatorname{Disc}_c(G_{2,3})$. *In addition, we can see that 23 is a primitive prime divisor for* $f^3_{2,-9}(0)$ *but* $23 \nmid \frac{\partial f^3_{2,c}(0)}{\partial c}|_{c=-9}$.

This lemma leads to a simplification of the condition in Theorem 4.2 as follows.

Corollary 4.8. *Let* $c_0 \in K$ *be such that* $\mathfrak{p}$ *is a primitive prime divisor for* $f^n_{d,c_0}(0)$. *If* $\operatorname{Disc}_c(G_{d,n}(c)) \notin \mathfrak{p}$, *then there is a unique* $\overline{c_0} \in R_{\mathfrak{p}}$ *such that the following occur:*

(1) $\nu_{\mathfrak{p}}(\overline{c_0} - c_0) > 0$.

(2) The point 0 is periodic with exact period n for $f_{d,\overline{c_0}}(x) \in R_{\mathfrak{p}}[x]$.

Furthermore, $\nu_{\mathfrak{p}}(\overline{c_0} - c_0) = \nu_{\mathfrak{p}}\left(f^n_{d,c_0}(0)\right)$.

This is a direct consequence since $\mathfrak{p}$ being a primitive prime divisor for $f^n_{d,c_0}(0)$ implies that $\nu_{\mathfrak{p}}(f^n_{d,c_0}(0)) > 0$, and by Lemma 4.6, $\operatorname{Disc}_c(G_{d,n}(c)) \notin \mathfrak{p}$ implies that $\nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0}\right) = 0$. So, the conditions of Theorem 4.2 are satisfied.

As seen in Example 4.3, we can find values of c such that specific powers of p divide $f^n_{d,c}(0)$. Indeed, we introduce the following corollary.

Corollary 4.9. *Let* $c_0 \in K$ *be such that* $\mathfrak{p}$ *is a primitive prime divisor for* $f^n_{d,c_0}(0)$. *If* $\operatorname{Disc}_c(G_{d,n}(c)) \notin \mathfrak{p}$, *then, for any integer* $r \geq 1$, *there is* $c_r \in R_{\mathfrak{p}}$ *such that* $\mathfrak{p}$ *is a primitive prime divisor for* $f^n_{d,c_r}(0)$ *and* $\nu_{\mathfrak{p}}(f^n_{d,c_r}(0)) = r$.

Proof. This is a direct consequence of Corollary 4.8. If $\nu_{\mathfrak{p}}(f^n_{d,c_0}(0)) = r$, then we are done. Assume $\nu_{\mathfrak{p}}(f^n_{d,c_0}(0)) \neq r$. Let $\overline{c_0}$ be as in Theorem 4.8, and $c_r \in K$ be such that $\nu_{\mathfrak{p}}(c_r - \overline{c_0}) = r$. By the choice of c_r, we have $\widetilde{c_r} = \widetilde{\overline{c_0}} = \widetilde{c_0}$. This means that c_r is a point such that $\mathfrak{p}$ is a primitive prime divisor of $f^n_{d,c_r}(0)$. This means that there is a unique lift of c_r, such that $\nu_{\mathfrak{p}}(\overline{c_r} - c_r) > 0$, and $f_{d,\overline{c_r}} = 0$. Since the lift is unique, we have $\overline{c_r} = \overline{c_0}$. Again, by Corollary 4.8, we get that

$$r = \nu_{\mathfrak{p}}(\overline{c_0} - c_r) = \nu_{\mathfrak{p}}(\overline{c_r} - c_r) = \nu_{\mathfrak{p}}(f^n_{d,c_r}(0)),$$

concluding the proof. □

Let $r \geq 1$ be an integer, Corollary 4.9 implies that except for finitely many primes, once we know that a prime $\mathfrak{p}$ can appear as a primitive prime divisor of $f^n_{d,c_0}(0)$ for some $c_0 \in K$, there is another value $c_1 \in K$ for which $\mathfrak{p}$ is a primitive prime divisor of $f^n_{d,c_1}(0)$, and $\nu_{\mathfrak{p}}(f^n_{d,c_1}(0)) = r$.

Example 4.10. *Fix $d = 2$, $c = 1, p = 5$, and $n = 3$. We find that 5 is a primitive divisor for $f^3_{2,1}(0)$ with $\nu_5(f^3_{2,1}(0)) = 1$ and $\nu_5\left(\frac{\partial f^3_{2,c}(0)}{\partial c}|_{c=1}\right) = 0$. One can see that for $c_2 = -9$, $5^2 || f^3_{2,-9}(0)$ where $f_{2,-9}(x) = x^2 - 9$.*

Theorem 4.11. *Fix an integer $d \geq 2$, and $\{\mathfrak{p}_i\}$ a finite set of distinct primes. If there is a set of K-rational numbers $\{c_i\}$ such that $\mathfrak{p}_i$ is a primitive prime divisor for $f^{n_i}_{d,c_i}(0)$ and $\nu_{\mathfrak{p}_i}(f^{n_i}_{d,c_i}(0)) = k_i$ for some $n_i \geq 1$ and $k_i \geq 1$. Then, there exists $\overline{c} \in R$ such that, for all $\mathfrak{p}_i$,*

(1) $\nu_{\mathfrak{p}_i}(f^{n_i}_{d,\overline{c}}(0)) = k_i$, and

(2) p_i is a primitive prime divisor for $f^{n_i}_{d,\overline{c}}(0)$.

Proof. This is a simple corollary of the Chinese remainder theorem [16, Theorem 5.33]. Taking an element $\overline{c} \in R$ such that $\overline{c} + \mathfrak{p}_i^{k_i+1} = c_i + \mathfrak{p}_i^{k_i+1}$, and noting that $\nu_{\mathfrak{p}}(f^n_{d,c}(0)) = r$ where $\mathfrak{p}$ is primitive to $f^n_{d,c}(0)$ if and only if 0 is periodic for $f_{d,c}(x) + \mathfrak{p}^r$ but 0 is not periodic for $f_{d,c}(x) + \mathfrak{p}^{r+1}$, gives the required proof. □

4.1.1 Special case $K = \mathbb{Q}$

For Theorem 4.2, we also give an alternative proof for the case that $K = \mathbb{Q}$ with a constructive proof similar to the proof of Hensel's lemma, but specialized to the polynomial $f_{d,c}(x) \in \mathbb{Q}[x, c]$. This gives insight on how to choose $c \in \mathbb{Z}$ such that we get a specific power of p. For the alternative proof, we start by the following lemma.

Lemma 4.12. *[11, Lemma 3.7] Let $f_{d,c}(x) = x^d + c \in \mathbb{Q}[x, c]$ and $a \in \mathbb{Q}$, then we have $\frac{\partial f^n_{d,c}(a)}{\partial c} = 1 + \sum_{j=1}^{n-1}(d^{n-j}\prod_{i=j}^{n-1}(f^i_{d,c}(a))^{d-1})$*

Proof. By induction. For $n=1$, it is trivial.
Assume it's true for $k \leq n$ then

$$\begin{aligned}
\frac{\partial f_{d,c}^{n+1}(a)}{\partial c} &= \frac{\partial (f_{d,c}^{n}(a))^d}{\partial c} + 1 \\
&= 1 + d \cdot (f_{d,c}^{n}(a))^{d-1} \cdot \frac{\partial f_{d,c}^{n}(a)}{\partial c} \\
&= 1 + d \cdot (f_{d,c}^{n}(a))^{d-1} \cdot (1 + \sum_{j=1}^{n-1} (d^{n-j} \prod_{i=j}^{n-1} (f_{d,c}^{i}(a))^{d-1})) \\
&= 1 + \sum_{j=1}^{n} (d^{n+1-j} \prod_{i=j}^{n} (f_{d,c}^{i}(a))^{d-1}).
\end{aligned}$$

□

This leads to the following lemma.

Lemma 4.13. *Let $f_{d,c}(x) = x^d + c$ and $g(x) = f_{d,c+tp^{k_1}} = x^d + c + tp^{k_1}$ where $k_1 \geq 1$. Then*

$$g^n(0) \equiv f_{d,c}^n(0) + tp^{k_1} \frac{\partial f_{d,c}^n(0)}{\partial c} \mod p^{2k_1}.$$

Proof. For $n=1$, it is trivial. Assuming the statement is true for $l \leq n$, then

$$\begin{aligned}
g^{n+1}(0) &= [g^n(0)]^d + c + tp^{k_1} \\
&\equiv \left[f_{d,c}^n(0) + tp^{k_1} \frac{\partial f_{d,c}^n(0)}{\partial c} \right]^d + c + tp^{k_1} \mod p^{2k_1} \\
&= \left[f_{d,c}^n(0) + tp^{k_1} \left(1 + \sum_{j=1}^{n-1} (d^{n-j} \prod_{i=j}^{n-1} (f_{d,c}^i(0))^{d-1}) \right) \right]^d + c + tp^{k_1} \\
&\equiv \left[f_{d,c}^n(0) \right]^d + d (f_{d,c}^n(0))^{d-1} tp^{k_1} \left(1 + \sum_{j=1}^{n-1} (d^{n-j} \prod_{i=j}^{n-1} (f_{d,c}^i(0))^{d-1}) \right) + c + tp^{k_1} \mod p^{2k_1} \\
&= f_{d,c}^{n+1}(0) + tp^{k_1} \left(1 + d (f_{d,c}^n(0))^{d-1} \left(1 + \sum_{j=1}^{n-1} (d^{n-j} \prod_{i=j}^{n-1} (f_{d,c}^i(0))^{d-1}) \right) \right) \\
&= f_{d,c}^{n+1}(0) + tp^{k_1} \frac{\partial f_{d,c}^{n+1}(0)}{\partial c}.
\end{aligned}$$

□

With these two lemmas, we can prove the following.

Theorem 4.14. *Let $f_{d,c_0}(x) = x^d + c_0 \in \mathbb{Q}[x]$ and p is a prime such that p is a primitive divisor for $f_{d,c_0}^n(0)$. Let $k_1 = \nu_p \left(f_{d,c_0}^n(0) \right)$, and $k_2 = \nu_p \left(\frac{\partial f_{d,c}^n(0)}{\partial c} |_{c=c_0} \right)$. If $k_1 > 2k_2$, then there exists a unique integer t such that*

(1) $1 \leq t \leq p-1$,

(2) p *is a primitive prime divisor for* $f^n_{d,c_0+tp^{k_1-k_2}}(0)$, *and*

(3) $p^{k_1+1} \mid f^n_{d,c_0+tp^{k_1-k_2}}(0)$.

Furthermore, for all integers $r \geq 1$ *such that* $r > 2k_2$, *there is a* p*-adic integer* $t_r \in p^{k_2+1}\mathbb{Z}_p$ *such that for the polynomial* $f_{d,c_0+t_r}(x) \in \mathbb{Z}[x]$, p *is a primitive divisor for* $f^n_{d,c_0+t_r}(0)$, *and* $p^r \mid\mid f^n_{d,c_0+t_r}(0)$.

Remark 4.15. *We will also see in the proof that* $t_r \in p^{k_2+1}\mathbb{Z}_p$ *is unique mod* p^{r-k_2}, *and* $t_{r+1} \equiv t_r \mod p^{r-k_2}$. *Due to that, we notice that the sequence* $\{t_{k_1}, t_{k_1+1}, t_{k_1+2}, \dots\}$ *is a Cauchy sequence in the local ring* $\mathbb{Z}_p$. *This gives the convergence of this sequence to an element* $t_\infty \in \mathbb{Z}_p$. *The uniqueness of* $t_{k_1+i} \mod p^{k_1-k_2+i}$, *and the fact that* $t_\infty \equiv t_{k+i} \mod p^{k_1-k_2+i}$ *gives also the uniqueness of* $t_\infty \in \mathbb{Z}_p$. *This implies the special case of Theorem 4.2 when* $K = \mathbb{Q}$.

Proof. Let $\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0} = s \cdot p^{k_2}$, and $t \geq 1$ be an integer. By Lemma 4.13, we have

$$f^n_{d,c_0+tp^{k_1-k_2}}(0) \equiv f^n_{d,c_0}(0) + tp^{k_1-k_2}\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0} \mod p^{2(k_1-k_2)} \geq p^{k_1+1}$$

Since $p^{k_1} \mid\mid f^n_{d,c_0}(0)$, we can divide by p^{k_1} to get

$$\frac{f^n_{d,c_0+tp^{k_1-k_2}}(0)}{p^{k_1}} \equiv \frac{f^n_{d,c_0}(0)}{p^{k_1}} + \frac{t \cdot p^{k_1-k_2} \cdot s \cdot p^{k_2}}{p^{k_1}} \equiv \frac{f^n_{d,c_0}(0)}{p^{k_1}} + ts \mod p$$

Solving for t to get $\frac{f^n_{d,c_0+tp^{k_1-k_2}}(0)}{p^{k_1}} \equiv 0 \mod p$, we find the unique solution $t \equiv -\frac{f^n(0)}{p^{k_1}}s^{-1} \mod p$. So, $p \mid \frac{f^n_{d,c_0+tp^{k_1-k_2}}(0)}{p^{k_1}}$ or $p^{k_1+1} \mid f^n_{d,c_0+tp^{k_1-k_2}}(0)$.

For the second part of the statement, Let $r > 2k_2$, and $\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0} = s \cdot p^{k_2}$. We then follow an algorithm to find t_r. The algorithm is recursive and depends on the initial value c_0. Due to that, we will denote the output by $t_r(c_0)$.

(1) Set $k_1 = \nu_p(f^n_{d,c_0}(0))$.

(2) Compare r with k_1

(a) If $r < k_1$, return $t_r(c_0) = lp^{r-k_2}$ where $l \not\equiv 0 \mod p$.

(b) If $r = k$, return $t_r(c_0) = lp^{r-k_2}$where $l \not\equiv -\frac{f^n(0)}{p^{k_1}}s^{-1} \mod p$.

(c) If $r > k$, set $l \equiv -\frac{f^n(0)}{p^{k_1}}s^{-1} \mod p$ and return $t_r(c_0) = lp^{k_1-k_2} + t_r(c_0 + lp^{k_1-k_2})$.

We need to show that this algorithm is effective, terminates and gives the desired value of $t_r \in p^{k_2+1}\mathbb{Z}_p$. We also note in each case that the value of t_r is unique modulo certain powers of p, which implies the uniqueness of the final output mod p^{r-k_2}. We now check the three cases separately.

Case 1 ($r < k_1$): By Lemma 4.13, we first assume $2\nu(t_r) \geq r+1$, then

$$f^n_{d,c_0+t_r}(0) \equiv f^n_{d,c_0}(0) + t_r s p^{k_2} \mod p^{r+1}.$$

Since $k_1 > r$, then $k_1 \geq r+1$ and so $f^n_{d,c_0}(0) \equiv 0 \mod p^{r+1}$. We want $p^r || f^n_{d,c_0+t_r}(0)$. So, we substitute $f^n_{d,c_0+t_r}(0) = \beta p^r$ such that $p \nmid \beta$. We then look at the following.

$$\beta p^r = t_r s p^{k_2} \mod p^{r+1},$$

i.e,

$$t_r = \beta s^{-1} p^{r-k_2} \mod p^{r+1}.$$

taking $\beta s^{-1} = l$, we get the desired result and terminate. We note that indeed $2\nu(t_r) = 2(r-k_2) > r+1$. For the uniqueness, we note that under the assumption that $2\nu(t_r) \geq r+1$ of the solution, t_r must be divisible by p^{r-k_2}, i.e., the solution is uniquely determined to be 0 mod p^{r-k_2}. On the other hand, to check if there is another solution, we assume that $2\nu(t_r) < r+1$, and we get

$$0 \equiv 0 + t_r s p^{k_2} \mod p^{2\nu(t_r)}.$$

This means that

$$\nu(t_r) \leq k_2,$$

contradicting the choice of $t_r \in p^{k_2+1}\mathbb{Z}_p$.

Case 2 ($r = k_1$): Similar to case 1, by Lemma 4.13, we first assume $2\nu(t_r) \geq r+1$ then,

$$f^n_{d,c_0+t_r}(0) \equiv f^n_{d,c_0}(0) + t_r s p^{k_2} \mod p^{r+1}.$$

Since $k_1 = r$, then $f^n_{d,c_0}(0) \equiv \alpha p^r \mod p^{r+1}$ for some α not divisible by p. We want $p^r || f^n_{d,c_0+t_r}(0)$. So, we substitute $f^n_{d,c_0+t_r}(0) = \beta p^r$ such that $p \nmid \beta$. We then look at the following.

$$\beta p^r = \alpha p^r + t_r s p^{k_2} \mod p^{r+1},$$

i.e.,

$$t_r = (\beta-\alpha)s^{-1}p^{r-k_2} \mod p^{r+1}.$$

taking $(\beta-\alpha)s^{-1} = l$, we get the desired result and conclude. Again, $2\nu(t_r) = 2(r-k_2) > r+1$. For the uniqueness, with the assumption that $2\nu(t_r) \geq r+1$, t_r must be divisible by p^{r-k_2}, that is, the solution is uniquely determined to be 0 mod p^{r-k_2}. Similarly, we assume that $2\nu(t_r) < r+1$. This means that both the desired $f^n_{d,c_0+t_r}(0)$ and the original $f^n_{d,c_0}(0)$ are divisible by $p^{2\nu(t_r)}$. So, again

$$0 \equiv 0 + t_r s p^{k_2} \mod p^{2\nu(t_r)}.$$

With

$$\nu(t_r) \leq k_2,$$

we get the same contradiction.

Case 3 ($r > k_1$): For this case, we make use of the first part of the theorem. We choose the unique value $l \equiv -\frac{f^n(0)}{p^{k_1}}s^{-1} \mod p$, which gives rise to the unique value $lp^{k_1-k_2}$ mod $p^{k_1-k_2+1}$. We also note that $f_{d,c_0+lp^{k_1-k_2}} \equiv f_{d,c_0} \mod p^{k_2+1}$. This means that $\frac{\partial f^n_{d,c_0+lp^{k_1-k_2}}(0)}{\partial c}|_{c=c_0} \equiv s \cdot p^{k_2} \mod p^{k_2+1}$. On the other hand, as seen in the first part of the proof, $p^{k_1+1}|f^n_{d,c_0+lp^{k_1-k_2}}(0)$. This means that the conditions for the initiation of the algorithm are met for $f^n_{d,c_0+lp^{k_1-k_2}}(0)$.

In case 3, we also note that if the algorithm gives a unique value $t_r(c_0)$ mod p^{r-k_2} when $r-k_1 \leq e$, then for $r-k_1 = e+1$, we get a unique l mod p by the algorithm and a unique $t_r(c_0+lp^{k_1-k_2})$ mod p^{r-k_2} by induction. Then, it is simple to show that $lp^{k_1-k_2}+t_r(c_0+lp^{k_1-k_2})$ is a unique lift mod p^{r-k_2}. Also, cases 1 and 2 give the basis of the induction where the unique lift is achieved with $r-k_1 \leq 0$, concluding the proof. □

4.2 Correspondence between PCF polynomials in $\mathbb{F}_p$ and $\mathbb{Z}_p$

In this section, we use Theorem 4.2 to give conditions that allow a one to one correspondence between polynomials $f_{d,c}(x) \in \mathbb{F}_p[x]$ with periodic critical orbit and polynomials $f_{d,c}(x) \in \mathbb{Z}_p[x]$ with periodic critical orbit.

Theorem 4.2 along with Theorem 3.10 lead to the following result.

Theorem 4.16. *Let $d \geq 2$ be a positive integer, $p > d$ be a prime integer, and $1 \leq n \leq p$ be a positive integer such that the following holds.*

For all $c \in \mathbb{F}_p$, if 0 is periodic with exact period n for $f_{d,c}(x) \in \mathbb{F}_p[x]$, then c is a simple root of $f^n_{d,c}(0) \in \mathbb{F}_p[c]$. $(*)$

Then there is a one-to-one correspondence

$$\left\{\begin{array}{c} f_{d,c}(x) \in \mathbb{F}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \\ \textit{of exact period } n \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} f_{d,c}(x) \in \mathbb{Z}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \\ \textit{of exact period } n \end{array}\right\}$$

Moreover, for $n > p$, there are no polynomials of the form $f_{d,c}(x) \in \mathbb{Z}_p[x]$ with periodic critical orbit of exact period n.

Proof. We assume that $1 \leq n \leq p$. The proof comes from setting $K = \mathbb{Q}$ in Theorem 3.10, and Theorem 4.2. First, we define the map $\iota : \mathbb{F}_p \to \mathbb{Z}_p$, where $\iota(c_0) = t_0 \in \mathbb{Z}_p$ such that, $0 \leq t_0 \leq p-1$, and $\widetilde{t_0} = c_0$. We also denote the set of polynomials in $\mathbb{F}_p[x]$ with periodic critical orbit of period n by A_n, and the corresponding set of polynomials in $\mathbb{Z}_p[x]$ by B_n.

With this notation, condition $(*)$ means that if $c_0 \in \mathbb{F}_p$ is a root of $f^n_{d,c}(0) \in \mathbb{F}_p[c]$, where n is the exact period of 0 under the iterations of $f_{d,c_0}(x) \in \mathbb{F}_p[x]$, then $\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=c_0} \neq 0$. This means that for $f_{d,\iota(c_0)}(x) \in \mathbb{Z}_p[x]$ has p as a primitive prime divisor of $f^n_{d,\iota(c_0)}(0)$ with $\nu_{\mathfrak{p}}\left(\frac{\partial f^n_{d,c}(0)}{\partial c}|_{c=\iota(c_0)}\right) = 0$. So Theorem 4.2 can be applied to get a unique value $c_1 \in \mathbb{Z}_p$ such that $\nu_p(c_1 - \iota(c_0)) > 0$, and 0 is periodic for $f_{d,c_1}(x) \in \mathbb{Z}_p[x]$. The condition that $\nu_p(c_1 - \iota(c_0)) > 0$ implies that $\widetilde{c_1} = \widetilde{\iota(c_0)} = c_0$. With this, we define the map $\psi : A_n \to B_n$, where $\psi(f_{d,c_0}(x)) = f_{d,c_1}(x)$, with c_0 and c_1 are as above.

Let $c_0 \in \mathbb{F}_p$, where $f_{d,c_0} \in A_n$. Assume that $\psi(f_{d,c_0}(x)) = f_{d,c_1}(x)$ and $\psi(f_{d,c_0}(x)) = f_{d,c_2}(x)$. Then $\widetilde{c_1} = c_0 = \widetilde{c_2}$ and 0 is periodic with exact period n for both $f_{d,c_1}(x)$ and $f_{d,c_2}(x)$. By the uniqueness given in Theorem 4.2, we get that $c_1 = c_2$. So, ψ is a well defined map.

Let $f_{d,c_0}(x), f_{d,c_3}(x) \in A_n$ with $\psi(f_{d,c_0}(x)) = \psi(f_{d,c_3}(x)) = f_{d,c_2}(x)$. Then we get that $c_0 = \widetilde{c_2} = c_3$, i.e, ψ is injective.

Let $f_{d,c_1}(x) \in B_n$. Then 0 is periodic with exact period m for $\widetilde{f_{d,c_1}(x)} = f_{d,\widetilde{c_1}}(x)$, where $m|n$. By Theorem 3.10, since $p > d$, we have that $m = n$, i.e, $f_{d,\widetilde{c_1}}(x) \in A_n$. So, ψ is surjective.

For the case that $n > p$, if $f_{d,c_1}(x) \in B_n$, then again by Theorem 3.10, $\widetilde{f_{d,c_1}(x)} \in A_n$. However, the orbit length in $\mathbb{F}_p$ can not have a length $n > p$. Thus, B_n is empty. □

Corollary 4.17. *Let $d \geq 2$ be a positive integer and $p > d$ be a prime integer such that the following holds.*

For all $c \in \mathbb{F}_p$, if 0 is periodic with exact period n for $f_{d,c}(x) \in \mathbb{F}_p[x]$ for some $n \geq 1$, then c is a simple root of $f^n_{d,c}(0) \in \mathbb{F}_p[c]$. (∗∗)

Then there is a one to one correspondence

$$\left\{ \begin{array}{c} f_{d,c}(x) \in \mathbb{F}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} f_{d,c}(x) \in \mathbb{Z}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \end{array} \right\}$$

Proof. This is a direct corollary of Theorem 4.16. Since for each $n \geq 1$, there is a one to one correspondence between A_n and B_n, we get the one to one correspondence between $\underset{1 \leq n \leq p}{\cup} A_n$ and $\underset{1 \leq n \leq p}{\cup} B_n$, where each union is a disjoint union.

□

Remark 4.18. *For $d = 2$, the first 50 prime numbers were tested for the condition in Corollary 4.17 using* Mathematica *and was found to be satisfied for 47 of these primes. An example of the other three primes is the prime 13 illustrated in Example 4.4.*

The condition of the previous can be relaxed using Lemma 4.6 as follows.

Corollary 4.19. *Let d be a positive integer and $p > d$ be a prime integer such that, $p \nmid \mathrm{Disc}_c(G_{d,n}(c))$ for any $n \leq p$. Then there is a one to one correspondence*

$$\left\{ \begin{array}{c} f_{d,c}(x) \in \mathbb{F}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} f_{d,c}(x) \in \mathbb{Z}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \end{array} \right\}$$

Proof. This follows by noting that for all $1 \leq n \leq p$, if $p \nmid \mathrm{Disc}_c(G_{d,n}(c))$, then condition (∗∗) follows. □

This also means that, if the conditions on p are satisfied, we can find all polynomials with periodic critical orbit in $\mathbb{Z}_p$ by checking finitely many values of c in $\mathbb{F}_p$ and then lifting each value uniquely by Corollary 4.8.

In both Corollary 4.17 and Corollary 4.19, we have strong conditions for strong results. However, the condition can be made simpler with a simpler result as follows.

Corollary 4.20. *Let d be a positive integer and $p > d$ be a prime integer. Then, for all $n \leq p$, if $p \nmid \text{Disc}_c(G_{d,n}(c))$, then there is a one to one correspondence*

$$\left\{ \begin{array}{c} f_{d,c}(x) \in \mathbb{F}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \\ \textit{of exact period } n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} f_{d,c}(x) \in \mathbb{Z}_p[x] \textit{ with} \\ \textit{periodic critical orbit} \\ \textit{of exact period } n \end{array} \right\}$$

Moreover, for $n > p$, there are no polynomials of the form $f_{d,c}(x) \in \mathbb{Z}_p[x]$ with periodic critical orbit of exact period n.

Proof. Similar to the proof of Corollary 4.19, this follows by noting that for all $1 \leq n \leq p$, if $p \nmid \text{Disc}_c(G_{d,n}(c))$, then condition $(*)$ follows. □

We conclude this section by an example for the one to one correspondence using Corollary 4.19.

Example 4.21. *For $d = 3$ and $p = 5$,*

$$\text{Disc}_c(G_{3,1}(c)) \equiv 1 \not\equiv 0 \textit{ mod } 5$$

$$\text{Disc}_c(G_{3,2}(c)) \equiv 1 \not\equiv 0 \textit{ mod } 5$$

$$\text{Disc}_c(G_{3,3}(c)) \equiv 1 \not\equiv 0 \textit{ mod } 5$$

$$\text{Disc}_c(G_{3,4}(c)) \equiv 1 \not\equiv 0 \textit{ mod } 5$$

$$\text{Disc}_c(G_{3,5}(c)) \equiv 4 \not\equiv 0 \textit{ mod } 5$$

So, in order to find functions of the form $f_{3,c}(x) \in \mathbb{Z}_5[x]$ such that, 0 has a periodic orbit, it suffices to find those in $\mathbb{F}_5[x]$. This means we only check $0 \leq c \leq 4$. In $\mathbb{F}_5[x]$,

$$c = 0,\ f_{3,0}(0) = 0 \implies 0 \textit{ has orbit type } (0,1)$$

$$c = 1,\ f_{3,1}^4(0) = 0,\ \textit{and } f_{3,1}^2(0) = 2 \neq 0 \implies 0 \textit{ has orbit type } (0,4)$$

$$c = 2,\ f_{3,2}^2(0) = 0,\ \textit{and } f_{3,2}(0) = 2 \neq 0 \implies 0 \textit{ has orbit type } (0,2)$$

$$c = 3,\ f_{3,3}^2(0) = 0,\ \textit{and } f_{3,3}(0) = 3 \neq 0 \implies 0 \textit{ has orbit type } (0,2)$$

$$c = 4,\ f_{3,4}^4(0) = 0,\ \textit{and } f_{3,4}^2(0) = 3 \neq 0 \implies 0 \textit{ has orbit type } (0,4)$$

This means that there are exactly 5 polynomials of the form $f_{3,c}(x) \in \mathbb{F}_5[x]$ such that, 0 is periodic. By Corollary 4.19, we get that there are exactly 5 polynomials of the form $f_{3,c}(x) \in \mathbb{Z}_5[x]$ such that, 0 is periodic.

Note that, although, in general, we don't have a one to one correspondence for *functions with 0 being preperiodic, we can see that there are no such polynomials in $\mathbb{Z}_5[x]$. This is due to Theorem 3.10.*

The contra-position of Theorem 3.10 tells us that if 0 has a strictly preperiodic orbit for $f_{3,c}(x)$ in $\mathbb{Z}_5[x]$, then 0 is not periodic for $f_{3,c}(x)$ in $\mathbb{F}_5[x]$. Since this does not happen in $\mathbb{F}_5[x]$ for any $0 \leq c \leq 4$, we get that there are no polynomials of the form $f_{3,c}(x) \in \mathbb{Z}_p[x]$ such that 0 is preperiodic. This means that there are exactly 5 *PCF polynomials in $\mathbb{Z}_p[x]$ of the form $f_{3,c}$.*

4.3 Rough bounds for the count of primitive prime divisors

For this section, we only work over $K = \mathbb{Q}$. We give an elementary upper bound on the count of primitive prime divisors to answer Question 2.24. This will be give an insight to direct us in the next chapter.

We use notations as in [19] defining $f^n_{d,c}(0) = \frac{a_n}{b^{d^{n-1}}}$ where a_n, b are integers. Let $\varrho_d(n,c)$ be the number of primitive prime divisors of a_n and $\omega(a_n)$ be the total number of prime divisors of a_n.

Lemma 4.22. *If $c \leq -2$ and d is even then,* $\log_2|c| \leq \log_2|f^n_{d,c}(0)| \leq d^{n-1}\log_2|c|$.

Proof. The proof is by induction. For $n = 1$, it is clear. Assume the statement is true for n, then

$$|f^n_{d,c}(0)|^d \geq |c|^d \geq |c| = -c \text{ implies that } |f^n_{d,c}(0)|^d + c \geq 0.$$

This means that

$$\begin{aligned} \log_2|f^{n+1}_{d,c}(0)| &= \log_2|f^n_{d,c}(0)^d + c| \\ &\leq \log_2(f^n_{d,c}(0)^d) \\ &= d\log_2|f^n_{d,c}(0)| \\ &\leq d \cdot d^{n-1}\log_2|c| \\ &= d^n\log_2|c|. \end{aligned}$$

Since $c \leq -2$, we get that $\log_2|c^{d-1}+1| = \log_2(|c|^{d-1}-1) \geq \log_2(2^{d-1}-1) \geq 0$. So,

$$\begin{aligned}\log_2|f_{d,c}^{n+1}(0)| &= \log_2|f_{d,c}^{n}(0)^d + c| \\ &\geq \log_2|c^d + c| \\ &= \log_2|c(c^{d-1}+1)| \\ &= \log_2|c| + \log_2|c^{d-1}+1| \\ &\geq \log_2|c|.\end{aligned}$$

□

Theorem 4.23. *Let $f_{d,c}(x) \in \mathbb{Q}[x]$ be a polynomial with infinite critical orbit. Then, $\varrho_d(n,c) \leq B_d(n,c)$ where*

$$B_d(n,c) := \begin{cases} d^{n-1}\log_2|a_1| & c \leq -2 \text{ and } d \text{ is even} \\ d^{n-1}(3+\log_2|b|)-1 & -2 < c < -2^{\frac{1}{d-1}} \text{ and } d \text{ is even} \\ (d^{n-1}-1)\log_2|b| + \log_2|a_1| & -2^{\frac{1}{d-1}} < c < 0 \text{ and } d \text{ is even} \\ (d^{n-1}-1)(\frac{1}{d-1}+\log_2|b|)+\log_2|a_1| & 0 < c < 1;\text{ or } -1 < c < 0 \text{ and } d \text{ is odd} \\ d^{n-1}(\frac{1}{d-1}+\log_2|a_1|)-\frac{1}{d-1} & c \leq 1;\text{ or } c \leq -1 \text{ and } d \text{ is odd} \end{cases}$$

In general, $\varrho_d(n,c) \leq d^{n-1}(3+\log_2 h\left(\frac{a_1}{b})\right) + \log_2|a_1|$, where h denotes the height function $\left(h\left(\frac{a}{b}\right) = max\left(|a|,|b|\right)\right)$.

Proof. It is clear that $\varrho_d(n,c) \leq \omega(a_n) \leq \log_2|a_n|$. So for an elementary bound, it is enough to bound $\log_2|a_n|$. For $c \leq -2$ and d being even, we have by Lemma 4.22 that

$$\log_2|a_n| - d^{n-1}\log_2|b| = \log_2|f_{d,c}^n(0)| \leq d^{n-1}\log_2|c|$$

$$\log_2|a_n| \leq d^{n-1}\log_2|a_1|.$$

For $-2 < c < -2^{\frac{1}{d-1}}$ and an even d, we use [19, Proposition 5.8].

$$\log_2|a_n| - d^{n-1}\log_2|b| = \log_2|f_{d,c}^n(0)| \leq (3d^{n-1}-1)$$

implying that,

$$\log_2|a_n| \leq d^{n-1}(3+\log_2|b|)-1$$

For $-2^{\frac{1}{d-1}} < c < 0$ with an even d, [19, Lemma 3.1, Proposition 5.7] imply that $|f_{d,c}^n(0)| \leq |c|$. So,

$$\log_2|a_n| \leq d^{n-1}\log_2|b| + \log_2|a_1| - \log_2|b| = (d^{n-1}-1)\log_2|b| + \log_2|a_1|$$

For an odd d, if $c<0$, then it is clear that $f^n_{d,c}(0) = -f^n_{d,-c}(0)$. So, it is enough to prove the remaining for positive c.

For $0<c<1$, by [19, Lemma 5.5] (with $C(n)=c$ in the notation of the [19]),

$$\log_2|a_n| \le d^{n-1}\log_2|b| + \frac{d^{n-1}-1}{d-1} + \log_2|a_1| - \log_2|b| = (d^{n-1}-1)(\frac{1}{d-1} + \log_2|b|) + \log_2|a_1|$$

Last case is $c\ge 2$. Using same [19, Lemma 5.5] but with $C(n)=c^{d^{n-1}}$ in the notation of [19],

$$\log_2|a_n| \le d^{n-1}\log_2|b| + \frac{d^{n-1}-1}{d-1} + d^{n-1}(\log_2|a_1| - \log_2|b|) = d^{n-1}(\frac{1}{d-1} + \log_2|a_1|) - \frac{1}{d-1}$$

□

Theorem 4.23 shows us a bound that depends on the degree d, the iteration number n, and the value of c. The dependency on d and n seems reasonable, even though the bound might not be optimal. However, the dependency on c raises the following question.

Question 4.24. *Fix $d\ge 2$ and $n\ge 1$, is there a uniform bound on the count of primitive prime divisors in $f^n_{d,c}(0)$, $\varrho_d(n,c)$, that doesn't depend on the value of c?*

For the case $n=1$; or $n=2$ and d is even, choosing $c=p_1\cdot\dots\cdot p_r$; or $c=p_1\cdot\dots\cdot p_r-1$ respectively gives us r primitive prime divisors in $f^n_{d,c}(0)$. So, the bound must depend on c for these two cases. However, for other values of n, the answer is not as trivial.

Chapter 5

Density Questions on Critical Orbit

In this chapter, we work on polynomials with rational coefficients. First we tackle Question 2.27 by reducing the question from the density of primes that can appear in the critical orbit to the density of primes such that the Gleason polynomial has a root modulo those primes. This allows us to use the Frobenius density Theorem to measure the density. We also note that Corollary 4.9 links the answer of Question 2.27 to Question 2.29. That is, the density of the primes in the set $\{\mathfrak{p} : \mathfrak{p} \text{ is a primitive prime divisor of } f_{d,c}^n(a_0), \text{ and } \nu_{\mathfrak{p}}(f_{d,c}^n(a_0)) = t \text{ for some } c \in K\}$ does not depend on t. Moreover, this density is the same as the one of the set $\{\mathfrak{p} : \mathfrak{p} \text{ is a primitive prime divisor of } f_{d,c}^n(a_0) \text{ for some } c \in K\}$. This means that the density in Question 2.29 is the same as the density in Question 2.27. So, it suffices to calculate one of these densities in this chapter. After that, we use the results from the density along with Corollary 4.11 to answer Question 4.24.

5.1 Frobenius' Density and Possible Primes in the Critical Orbit

We start by linking our question to the Frobenius density Theorem. First we recall Question 2.27.

Question 5.1. *Fixing $d \geq 2$, $n \geq 1$, Let K be a number field, and $a_0 \in K$. What is the density of the primes in the set $\{\mathfrak{p} : \mathfrak{p} \text{ is a primitive prime divisor of } f_{d,c}^n(a_0) \text{ for some } c \in K\}$?*

We take a simpler case where $K = \mathbb{Q}$ and $a_0 = 0$. In this case, we are interested in the set $\{p : p \text{ is a primitive prime divisor of } f_{d,c}^n(0) \text{ for some } c \in \mathbb{Q}\}$.

As seen in Proposition 4.1, we see that the latter mentioned set is the same as the set $\{p:$ The critical orbit of $f_{d,c}(x) \in \mathbb{F}_p[x]$ is periodic with **exact** period n for some $c \in \mathbb{F}_p\}$.

As seen in Remark 2.9, for the critical orbit, i.e, the orbit of the point $x=0$, x has formal period n if and only if x has exact period n. So, we look at the set $\{p:$ The critical orbit of $f_{d,c}(x) \in \mathbb{F}_p[x]$ is periodic with **formal** period n for some $c \in \mathbb{F}_p\}$. This, by the definition of the formal period, is the same as $\{p:$ There exists $c \in \mathbb{F}_p$ such that $\widetilde{G_{d,n}}(c) = 0\}$. In other words, we need to look for primes p such that $\widetilde{G_{d,n}}(c)$ has a linear factor in $\mathbb{F}_p$. Therefore, we will need the Frobenius' Density Theorem.

Theorem 5.2. *[14, Theorem 9.15] The kronecker density D_k of the primes p for which $f(x) \equiv 0 \pmod p$ has exactly k incongruent integral solutions $\mod p$ equals the fraction of elements of the Galois group of f that fix exactly k of its roots.*

We note that this is a special case of the Frobenius' Density Theorem, [14, Theorem 9.20], which in turn is a direct consequence of the Chebotarev's Density theorem [22, p. 545].

In the notations of Theorem 5.2, the set $\{p:$ There exists $c \in \mathbb{F}_p$ such that $\widetilde{G_{d,n}}(c) = 0\}$ has a density that is equal to the fraction of the elements of the Galois group of $G_{d,n}(c)$ that fix at least one root. We denote the splitting field of $G_{d,n}(c)$ by $\mathbb{K}_{d,n}$, and with that, the fraction that we are interested in, denoted by the Fixed Point Proportion, $\mathrm{FPP}_{d,n}$, is as follows:

$$\mathrm{FPP}_{d,n} = \frac{\#\{\sigma \in \mathrm{Gal}(\mathbb{K}_{d,n}/\mathbb{Q}) : \sigma \text{ fixes at least one root of } G_{d,n}(c)\}}{\#\,\mathrm{Gal}(\mathbb{K}_{d,n}/\mathbb{Q})}.$$

5.2 Galois Group and Primitive Divisors

In this section, we use the connection developed in the previous section to calculate the density of possible primitive prime divisors. First, we give special results when $d = 2$.

5.2.1 $d = 2$

To calculate the density, we start by investigating the Galois group structure. For that purpose, we used MAGMA. The code is attached in Appendix A along with screenshots of the output. In that code, we calculate the Galois group of $G_{2,n}(c)$ for $1 \le n \le 11$. We also calculate $D_{2,n} := \deg_c(G_{2,n}(c)) = \sum\limits_{t|n} 2^{t-1}\mu\left(\frac{n}{t}\right)$. Comparing the size of the Galois group of $G_{2,n}(c)$ with the size of $S_{D_{2,n}} = D_{2,n}!$, we get that the Galois group of $G_{2,n}(c)$ is isomorphic to $S_{D_{2,n}}$ for all $1 \le n \le 11$. However, due to the exponential growth of the degree of $G_{2,n}(c)$, and due to the capabilities of MAGMA software, we were unable to calculate the Galois group when $n > 11$. Furthermore, we remind the reader that the irreducibility of $G_{2,n}(c)$ over $\mathbb{Q}[c]$ was conjectured in [7, Conjecture 1.4] for all $n \ge 1$, however, no proof has yet been established.

Due to the output of our MAGMA calculations, we have the following conditional result.

Theorem 5.3. *Let $\mathbb{K}_{2,n}$ be the splitting field of $G_{2,n}(c)$. If $\mathrm{Gal}(\mathbb{K}_{2,n}/\mathbb{Q}) \cong S_{D_{2,n}}$, then the density $\mathrm{FPP}_{2,n}$ is given by*

$$\mathrm{FPP}_{2,n} = \sum_{i=1}^{D_{2,n}} \frac{(-1)^{i+1}}{i!}.$$

Proof. With the assumption in the theorem that $\mathrm{Gal}(\mathbb{K}_{2,n}/\mathbb{Q}) \cong S_{D_{2,d}}$, the problem reduces to the density of elements of $S_{D_{2,n}}$ that fix at least one element in the set $\{1, \dots, D_{2,n}\}$. The following is a simple combinatorial argument for the count. We have $D_{2,n}$ elements to choose one to fix and with each fixed element we get $D_{2,n} - 1$ elements to freely permute. That's $\binom{D_{2,n}}{1} \cdot (D_{2,n} - 1)!$. Removing the double count when two elements are fixed gives the second term of the count $(-\binom{D_{2,n}}{2} \cdot (D_{2,n} - 2)!)$ with a similar argument. Continuing in the same way, we get the count $n_T := \#\{\sigma \in \mathrm{Gal}(\mathbb{K}_{2,n}/\mathbb{Q}) : \sigma \text{ fixes at least one root of } G_{d,n}(c)\}$ to be

$$\begin{aligned} n_T = \binom{D_{2,n}}{1} \cdot (D_{2,n} - 1)! - \binom{D_{2,n}}{2}(D_{2,n} - 2)! + \binom{D_{2,n}}{3}(D_{2,n} - 3)! + \dots + (-1)^{D_{2,n}+1}\binom{D_{2,n}}{D_{2,n}}(0)! \\ = \sum_{i=1}^{D_{2,n}} (-1)^{i+1} \binom{D_{2,n}}{i} (D_{2,n} - i)! \\ = \sum_{i=1}^{D_{2,n}} (-1)^{i+1} \frac{D_{2,n}!}{i!(D_{2,n} - i)!} (D_{2,n} - i)! \\ = D_{2,n}! \sum_{i=1}^{D_{2,n}} \frac{(-1)^{i+1}}{i!}. \end{aligned}$$

So that means that $\mathrm{FPP}_{2,n} = \frac{n_T}{D_{2,n}!} = \sum_{i=1}^{D_{2,n}} \frac{(-1)^{i+1}}{i!}$. □

Remark 5.4. *If* $\mathrm{Gal}(\mathbb{K}_{2,n}/\mathbb{Q}) \cong S_{D_{2,n}}$ *for all n large enough, then*

$$\lim_{n\to\infty} \mathrm{FPP}_{2,n} = 1 - \frac{1}{e}, \qquad \textit{and}$$

$$|\,\mathrm{FPP}_{2,n} - 1 + \frac{1}{e}| \le \frac{1}{(D_{2,n}+1)!} \le \frac{1}{2^{n-2}!} \quad \mathit{for} \quad n \ge 2.$$

Proof. The limit is a direct consequence of the fact that $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.

The first inequality comes from the series being an alternating series. So, this inequality comes from the error term of the alternating series. For The second inequality, for $n \le 4$, it can be checked with straightforward computations. For $n > 4$, we have $n-2 > \frac{n}{2}$ so,

$$\begin{aligned}
D_{2,n} &= \sum_{m|n} \mu(\frac{n}{m}) 2^{m-1} \\
&\ge 2^{n-1} - \sum_{m|n \ \&\ m\neq n} 2^{m-1} \\
&\ge 2^{n-1} - \sum_{m=1}^{\frac{n}{2}} 2^{m-1} \\
&\ge 2^{n-1} - \sum_{m=1}^{n-2} 2^{m-1} \\
&= 2^{n-1} - \sum_{m=0}^{n-3} 2^{m} \\
&= 2^{n-1} - (2^{n-2} - 1) \\
&\ge 2^{n-1} - (2^{n-2}) \\
&= 2^{n-2}.
\end{aligned}$$

□

5.2.2 $d \ge 2$

Remark 5.5. *We tried to check if there is a similar pattern for $f_{d,c}(x)$ with $d > 2$. However, our computations did not show an obvious pattern in* $\mathrm{Gal}(\mathbb{K}_{d,n}/\mathbb{Q})$.

The assumption on the Galois group in Theorem 5.3 seems to be specific to only degree $d = 2$. Also, the assumption seems far fetched to be proven given that even the irreducibility is only conjectured. However, for any $d \geq 2$, the following result is unconditional.

Lemma 5.6. *For all $d \geq 2$ and $n \geq 1$,*

$$\mathrm{FPP}_{d,n} > 0.$$

Proof. This is because of the fact that $\mathrm{Gal}(\mathbb{K}_{d,n}/\mathbb{Q}) \leq S_{D_{d,n}}$, and there is at least one element in $\mathrm{Gal}(\mathbb{K}_{d,n}/\mathbb{Q})$ fixing at least one root of $G_{d,n}(c)$, namely the identity element. This means that

$$\mathrm{FPP}_{d,n} = \frac{\#\{\sigma \in \mathrm{Gal}(\mathbb{K}_{d,n}/\mathbb{Q}) : \sigma \text{ fixes at least one root of } G_{d,n}(c)\}}{\#\,\mathrm{Gal}(\mathbb{K}_{d,n}/\mathbb{Q})} \geq \frac{1}{D_{d,n}!} > 0.$$

□

Theorem 5.7. *For all $d \geq 2$ and $n \geq 1$, there are infinitely many primes p such that there is $c \in \mathbb{Q}$ such that p is a primitive prime divisor of $f_{d,c}^{n}(0)$.*

Proof. As seen in Section 5.1, the density of primes p such that there is $c \in \mathbb{Q}$ such that p is a primitive prime divisor of $f_{d,c}^{n}(0)$ is equal to $\mathrm{FPP}_{d,n}$. Since $\mathrm{FPP}_{d,n} > 0$, the count of these primes is infinite. □

5.3 Polynomials with Arbitrarily Many Primitive Divisors

In this section, we use the result of Theorem 5.7 to answer Question 4.24. First, we introduce the following theorem.

Theorem 5.8. *Fix integers $d \geq 2$ and $m \geq 1$. For $1 \leq i \leq m$, let*

(1) n_i be distinct positive integers,

(2) t_i be positive integers,

(3) $(k_{i,1}, k_{i,2}, \ldots, k_{i,t_i})$ be t_i-tuples of positive integers.

Then there exists an integer c such that for each $1 \leq i \leq m$ and $1 \leq j \leq t_i$, there is a prime $p_{i,j}$ such that $p_{i,j}$ is a primitive prime divisor for $f_{d,c}^{n_i}(0)$ and $p_{i,j}^{k_{i,j}} || f_{d,c}^{n_i}(0)$.

Proof. As mentioned in Theorem 5.7, there exists infinitely many primes p that can appear as a primitive prime divisor in iteration n_i. Let the set of these primes be S_{n_i}. We also let the finite set of primes dividing $\mathrm{Disc}_c(G_{d,n_i}(c))$ be T_{n_i}.

Setting $P_{n_i} := S_{n_i} \setminus T_{n_i}$, we define the following sets by a recurrence relation.

$$A_1 \subset P_{n_1} \text{ with } |A_1| = t_1, \text{ and } B_1 = A_1$$

And for $2 \leq i \leq m$

$$A_i \subset P_{n_i} \setminus B_{i-1} \text{ with } |A_i| = t_i, \text{ and } B_i = B_{i-1} \cup A_i$$

By construction of the sets, it is clear that B_m is a set of distinct rational primes.

Also, B_m is the union of the disjoint sets A_i's where $|A_i| = t_i$. Now we find the set of constants $\{c\}$ that correspond to the set of primes B_m that we use in Theorem 4.11.

Let $A_i = \{p_{i,j}\}_{j=1}^{t_i}$. For each $p_{i,j} \in A_i \subset P_{n_i}$, we have that $p_{i,j}$ can appear as a primitive prime divisor in iteration n. That is, there exists $c_{i,j,0}$ such that $p_{i,j}$ is a primitive prime divisor for $f^{n_i}_{d,c_{i,j,0}}(0)$.

Since $p_{i,j} \notin T_{n_i}$, then $p_{i,j} \nmid \mathrm{Disc}_c(G_{d,n_i}(c))$. By Corollary 4.9, there exists an integer $c_{i,j,1}$ such that $p_{i,j}$ is a primitive prime divisor for $f^{n_i}_{d,c_{i,j,1}}(0)$, and $p_{i,j}^{k_{i,j}} || f^{n_i}_{d,c_{i,j,1}}(0)$. We now set $C_i = \{c_{i,j,1}\}_{1 \leq j \leq t_i}$, and $C = \bigcup\limits_{i=1}^{m} C_i$.

For the set of primes B_m, the set of C satisfies the hypothesis of Theorem 4.11. So, using the aforementioned theorem, we get the desired constant c.

□

The proof gives an explicit description of how to construct polynomials with the desired property. In what follows, we discuss the details of an explicit example.

Example 5.9. *Fix $d = 2$ and $m = 3$. For $1 \leq i \leq 3$, let n_i, t_i, and $(k_{i,1}, k_{i,2}, \ldots, k_{i,t_i})$ be as follows.*

Set $n_1 = 2$, $t_1 = 3$, and $(k_{1,1}, k_{1,2}, k_{1,3}) = (29, 17, 5)$,

$n_2 = 3$, $t_2 = 2$, and $(k_{2,1}, k_{2,2}) = (8, 3)$,

$n_3 = 4$, $t_3 = 1$, and $(k_{3,1}) = (21)$.

We first check the primes that divide the discriminants. That is the sets

$$T_2 = \emptyset,\ T_3 = \{23\},\ \textit{and}\ T_4 = \{23, 2551\}.$$

We can now find some of the primes in S_2, S_3, and S_4. Instead of checking each prime to see if it can appear in a specific iteration, we can instead check the primes appearing as primitive divisors in iterations of some polynomials, and then we can use the primes appearing in their critical orbits. For example,

$$f_{2,1}^2(0) = 2,\ f_{2,1}^3(0) = 5,\ \textit{and}\ f_{2,1}^4(0) = 2 \cdot 13.$$

This means we can use $p_{1,1} = 2$ with $c_{1,1,0} = 1$. Using Corollary 4.9, we get $c_{1,1,1} = 2^{29} - 1$.

Continuing in the same manner, we can get,

$$A_1 = \{2, 3, 7\}\ \textit{with}\ C_1 = \{2^{29} - 1, 3^{17} - 1, 7^5 - 1\}$$

$$A_2 = \{5, 19\}\ \textit{with}\ C_2 = \{326391, 4866\}$$

$$A_3 = \{13\}\ \textit{with}\ C_3 = \{198396633106433791392520\}$$

Using Theorem 4.11, we obtain that c may be chosen as follows.

$$c \equiv 2435198184778773753305234185205633067189478620345139 1$$

$$\bmod\ 40010031061893159449171265710098679720076040470528000000000.$$

Verifying the result using Mathematica *software, we can see that for*

$$f(x) := f_{2,24351981847787737533052341852056330671894786203451391}(x),$$

we get,

$$2^{29} || f^2(0),\ 3^{17} || f^2(0),\ 7^5 || f^2(0)$$

$$5^8 || f^3(0),\ 19^3 || f^3(0)$$

$$13^{21} || f^4(0)$$

with each of the mentioned primes being a primitive prime divisor for the corresponding iteration.

Theorem 5.8 gives an answer to Question 4.24 in the following corollary.

Corollary 5.10. *Let d be a positive integer and $U = \{(n_i, t_i)\}_{i=1}^m$ be a finite set of* *pairs of positive integers. Then there exists an integer c such that $f_{d,c}^{n_i}(0)$ has at least t_i primitive prime divisors for each $1 \leq i \leq m$.*

Proof. This is a direct consequence of 5.8 by choosing all constants $k_{i,j}$ to be equal to 1. □

Corollary 5.10 implies that by fixing the degree d and the iteration n, we can construct a polynomial of the form $f_{d,c}(x)$ for some $c \in \mathbb{Q}$ such that $f_{d,c}^n(0)$ has arbitrarily many primitive prime divisors. This implies that the upper bound of the count of primitive prime divisors of $f_{d,c}^n(0)$, see Theorem 4.23, can not be independent from c. So, the answer to Question 4.24 is negative. There can not be a uniform bound that does not depend on c.

Example 5.11. *For $d = 2$ and $U = \{(3, 33)\}$,*
We can do similar calculations as in the last example to reach that,

$$c \equiv 1344322207561736181245392014239768913384753174649268488506977 1$$

$$\text{mod } \; 70321927694409533965768410131069970323274232658951676172460495.$$

So, defining

$$f(x) := f_{2,13443222075617361812453920142397689133847531746492684885069771},$$

and verifying using Mathematica*, we can find that*

$$70321927694409533965768410131069970323274232658951676172460495 | f^3(0),$$

where this divisor is a square free number with 33 prime factors. Each of these factors is a primitive prime divisor for $f^3(0)$. Note that Corollary 5.10 implies that there are at least these 33 primitive prime divisors, but they are not necessarily the only such primes. In fact, one may see that there are exactly 37 primitive prime divisors for this specific iteration.

Corollary 5.10 along with Theorem 2.28 gives rise to the following result.

Corollary 5.12. *Let $d = 2$, and $m \geq 1$. There exists an integer c such that the splitting field of $f_{d,c}^m(x)$, denoted by F_m, has Galois group $\mathrm{Gal}(F_m/\mathbb{Q})$ of order 2^{2^m-1}.*

Proof. For $1 \leq i \leq m$, choose $n_i = i$, $t_i = 1$, and $(k_{i,1}) = (1)$. Then by Theorem 5.8, there is an integer c such that, for all $1 \leq i \leq m$, there is a prime p_i such that $p_i || f^i_{d,c}(0)$. Using Theorem 2.28, we get that for all $2 \le i \le m$, $\mathrm{Gal}(F_i/F_{i-1}) \cong (\mathbb{Z}/2\mathbb{Z})^{2^{i-1}}$.

Since there is a prime p_1 such that $p_1 || f(0)$, then $-c$ is not a square in $\mathbb{Q}$. So, $f_{d,c}(x)$ is irreducible with $\mathrm{Gal}(F_1/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})$.

By induction, for $2 \le i \le m$, assuming $\mathrm{Gal}(F_{i-1}/\mathbb{Q})$ has order $2^{2^{i-1}-1}$, and knowing that $\mathrm{Gal}(F_i/F_{i-1}) \cong (\mathbb{Z}/2\mathbb{Z})^{2^{i-1}}$, we can use the fundamental theorem of Galois theory [12, p. 574, Theorem 14] to see that $\mathrm{Gal}(F_i/\mathbb{Q})/\mathrm{Gal}(F_{i-1}/\mathbb{Q}) \cong \mathrm{Gal}(F_i/F_{i-1}) \cong (\mathbb{Z}/2\mathbb{Z})^{2^{i-1}}$. This directly concludes the order. □

We conclude with the following example.

Example 5.13. *Fix $d = 2$ and $m = 29$. Using Corollary 5.12, and using the calculations mentioned in Corollary 5.10, we find that for the polynomial*

$$f(x) = x^2 + 1168184310110489945509811544546782641527527693907326,$$

$f^{29}(x)$ has Galois group with order $2^{2^{29}}$. This is because, with

$$\{p_i\}_{1 \le i \le 29} := \{2,3,5,13,11,29,19,31,43,101,59,47,67,61,97,89,\\ 83,107,113,149,137,127,173,191,197,181,223,157,229\},$$

we get that p_i is a primitive prime divisor of $f^i(0)$ with $p_i || f^i(0)$.

BIBLIOGRAPHY

[1] J. Anderson, M. Manes, and B. Tobin. Cubic post-critically finite polynomials defined over $\mathbb{Q}$. *Open Book Series*, 4:23–38, 12 2020. doi: 10.2140/obs.2020.4.23.

[2] R. L. BENEDETTO and V. GOKSEL. Misiurewicz polynomials and dynamical units, Part I. preprint, 2022. URL https://doi.org/10.48550/arXiv.2201.07868.

[3] B.Hutz and A.Towsley. Misiurewicz points for polynomial maps and transversality. *New York J. Math*, 21:297–319, 2015.

[4] Y. Bilu, G. Hanrot, and P. M. Voutier. Existence of Primitive Divisors of Lucas and Lehmer Numbers. Research Report RR-3792, INRIA, 1999. URL https://hal.inria.fr/inria-00072867.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ISSN 0747-7171. doi: 10.1006/jsco.1996.0125. URL http://dx.doi.org/10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993).

[6] X. Buff. On Postcritically Finite Unicritical Polynomials. *New York Journal of Mathematics*, 24:1111–1122, 2018.

[7] X. Buff, W. Floyd, S. Koch, and W. Parry. Factoring gleason polynomials modulo 2. J. Théor. Nombres Bordeaux. To appear.

[8] R. D. Carmichael. On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$. *Annals of Mathematics Second Series*, 15:30–70, 1913. doi: doi:10.2307/1967797. URL https://doi.org/10.2307/1967797.

[9] L. DANIELSON and B. FEIN. On the irreducibility of the iterates of $x^n - b$. *Proceedings of the American Mathematical Society*, 130, 01 2002. doi: 10.2307/2699748.

[10] K. Doerksen and A. Haensch. Primitive prime divisors in zero orbits of polynomials. 12(3):465–472, 2012. doi: doi:10.1515/integers-2011-0117. URL https://doi.org/10.1515/integers-2011-0117.

[11] J. R. Doyle. Preperiodic portraits for unicritical polynomials over a rational function field. *Proc. Amer. Math. Soc.*, 144:2885–2899, 2016. doi: https://doi.org/10.1090/proc/13075.

[12] D. S. Dummit and R. M. Foote. *Abstract algebra.* Wiley, 3rd ed edition, 2004.

[13] S. Hamblen, R. Jones, and K. Madhu. The density of primes in orbits of $z^d + c$. *International Mathematics Research Notices*, 2015(7):1924–1958, 2015. doi: 10.1093/imrn/rnt349.

[14] T. Hawkins. *The Mathematics of Frobenius in Context.* Springer New York, NY, 2013. doi: https://doi.org/10.1007/978-1-4614-6333-7.

[15] W. R. Inc. Mathematica, Version 12.0. Champaign, IL, 2019.

[16] F. Jarvis. *Algebraic Number Theory*. Springer Cham, 2014. doi: https://doi.org/10.1007/978-3-319-07545-7.

[17] R. Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *Journal of the London Mathematical Society*, 78(2):523–544, 07 2008. ISSN 0024-6107. doi: 10.1112/jlms/jdn034. URL https://doi.org/10.1112/jlms/jdn034.

[18] A. W. Knapp. *Advanced Algebra*. Cornerstones. Birkhäuser Boston, 1 edition, 2007. ISBN 0817645225; 9780817645229. URL libgen.li/file.php?md5=00f1a11f04f7adcab8f52143a823528b.

[19] H. Krieger. Primitive prime divisors in the critical orbit of z^d+c. *International Mathematics Research Notices*, 2013(23):5498–5525, 2013. doi: 10.1093/imrn/rns213.

[20] D. Lukas, M. Manes, and D. Yap. A census of quadratic post-critically finite rational functions defined over $\mathbb{Q}$. *LMS Journal of Computation and Mathematics*, 17(A):314–329, 2014. doi: 10.1112/S1461157014000266.

[21] C. Mullen. *The Critical Orbit Structure of Quadratic Polynomials in $\mathbb{Z}_p$*. PhD thesis, University of Illinois at Chicago, 10 2017. URL https://indigo.uic.edu/articles/thesis/The_Critical_Orbit_Structure_of_Quadratic_Polynomials_in_Zp/10910657.

[22] J. Neukirch and N. Schappacher. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013. ISBN 9783662039830. URL https://books.google.com.tr/books?id=hS3qCAAAQBAJ.

[23] R. W. K. Odoni. On the Prime Divisors of the Sequence Wn+1 = 1 + W1. . . Wn. *Journal of the London Mathematical Society*, s2-32(1):1–11, 08 1985. ISSN 0024-6107. doi: 10.1112/jlms/s2-32.1.1. URL https://doi.org/10.1112/jlms/s2-32.1.1.

[24] J. H. Silverman. *The Arithmetic of Dynamical Systems*. Springer, 2007.

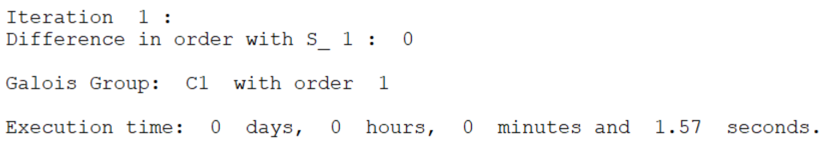
[25] M. Ward. The Intrinsic Divisors of Lehmer Numbers. *Annals of Mathematics Second Series*, 62(2):230–236, 1955. doi: doi:10.2307/1969677. URL https://doi.org/10.2307/1969677.

APPENDIX A

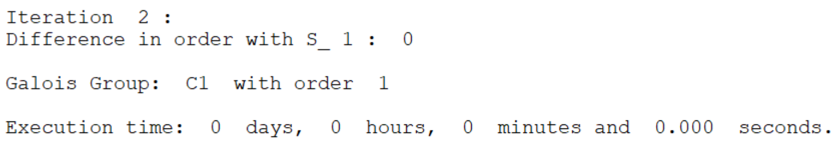
MAGMA Code for calculating the Galois group of $G_{d,n}(c)$

```
P< c >:=PolynomialAlgebra(Rationals());

f:= func<x|x^2+c>;

h:=function(n)
    t:=0;
    for i in [1..n] do
        t:=f(t);
    end for;
    return t;
end function;

g:= function(n)
    t := 1;
    t2 := 1;
    for i in Reverse(Divisors(n)) do
        if (0 gt MoebiusMu(n div i)) then
            t2 := t2 * h(i);
        else
            t := t * h(i)^(MoebiusMu(n div i));
        end if;
    end for;
    t := t div t2;
    return t;
 end function;
 timenow:= Realtime();
 timediff:=0;
for i in [1..11] do
    G:=GaloisGroup(g(i));
    deg := 0;
    for j in Divisors(i) do
        deg := deg + MoebiusMu(i div j) * 2^(j-1);
    end for;
  timediff:=Integers()!(Realtime()*1000)-Integers()!(timenow*1000);
  days:= timediff div ((3600000*24));
  hours:=  timediff div (3600000)-days*24;
  minutes:= (timediff div (60000))-days*24*60-hours*60;
  seconds:= Real(timediff/1000)-days*24*3600-hours*3600-minutes*60;
  print "Iteration ", i, ":";
    print "Difference in order with S_", deg ,": ", (Order(G) - Factorial(deg));
  print "";
  print "Galois Group: ", GroupName(G), " with order ", Order(G);
  print "";
  print "Execution time: ", days, " days, ", hours, " hours, ", minutes, " minutes and ", ChangePrecision(seconds,3), " seconds.";
  print "";
  print "";
  print "";
  print "";
  timenow:=Realtime();
end for;
```

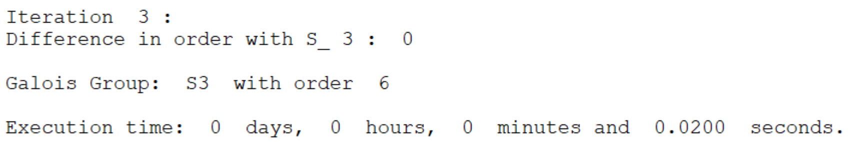
Screenshots of the results



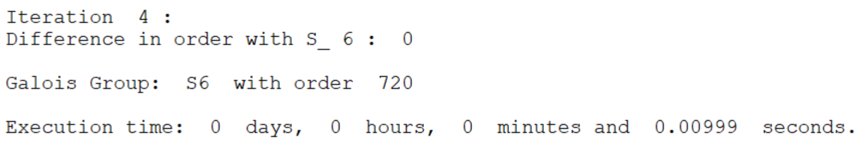
```
Iteration  1 :
Difference in order with S_ 1 :  0

Galois Group:  C1  with order  1

Execution time:  0  days,  0  hours,  0  minutes and  1.57  seconds.
```



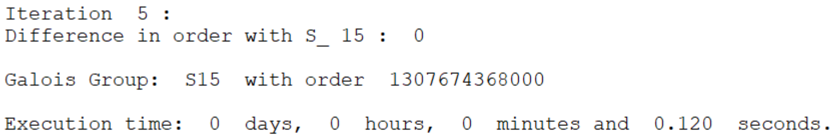
```
Iteration  2 :
Difference in order with S_ 1 :  0

Galois Group:  C1  with order  1

Execution time:  0  days,  0  hours,  0  minutes and  0.000  seconds.
```



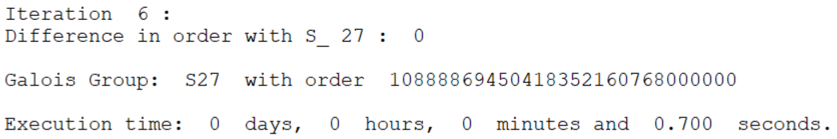
```
Iteration  3 :
Difference in order with S_ 3 :  0

Galois Group:  S3  with order  6

Execution time:  0  days,  0  hours,  0  minutes and  0.0200  seconds.
```



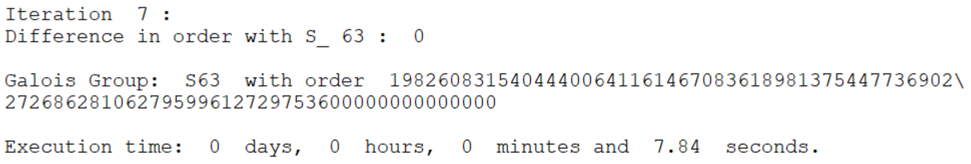
```
Iteration  4 :
Difference in order with S_ 6 :  0

Galois Group:  S6  with order  720

Execution time:  0  days,  0  hours,  0  minutes and  0.00999  seconds.
```



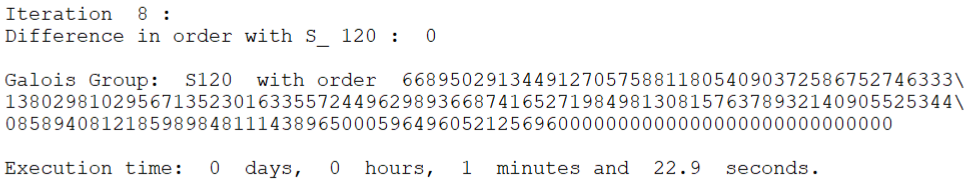
```
Iteration  5 :
Difference in order with S_ 15 :  0

Galois Group:  S15  with order  1307674368000

Execution time:  0  days,  0  hours,  0  minutes and  0.120  seconds.
```



```
Iteration  6 :
Difference in order with S_ 27 :  0

Galois Group:  S27  with order  10888869450418352160768000000

Execution time:  0  days,  0  hours,  0  minutes and  0.700  seconds.
```



```
Iteration  7 :
Difference in order with S_ 63 :  0

Galois Group:  S63  with order  198260831540444006411614670836189813754477369022\
27268628106279599612729753600000000000000

Execution time:  0  days,  0  hours,  0  minutes and  7.84  seconds.
```



```
Iteration  8 :
Difference in order with S_ 120 :  0

Galois Group:  S120  with order  668950291344912705758811805409037258675274633\
1380298102956713523016335572449629893668741652719849813081576378932140905525344\
085894081218598984811143896500059649605212569600000000000000000000000000000

Execution time:  0  days,  0  hours,  1  minutes and  22.9  seconds.
```

```
Iteration  9 :
Difference in order with S_ 252 :  0

Galois Group:  S252  with order  204484624215022882284756162044645354527365854\
3030197473314085439974032768035589422258671078304827567167012994710393801148158\
4892698594287523178247211816724109883700996451372905507541113381204196195195435\
4602552934775737522106316625395829324060862622528287468179375458308423270020892\
1330261563050465069579042111765917781670636204387327004971416564536955446374888\
8564282896170368904334765715609531606271737867415895310398229305913612697600000\
000000000000000000000000000000000000000000000000000000000

Execution time:  0  days,  0  hours,  29  minutes and  48.1  seconds.



Iteration  10 :
Difference in order with S_ 495 :  0

Galois Group:  S495  with order  3983552793542744265330724639088913357445505892\
9474360918831440169865373173062205245987407819877230158625954248105449553737789\
4847542028791304536833110347982510406474482399963235957295292424605580229871166\
4785321420030964088354936445249913174074891823131488443414382315837518622467364\
1496062809972380056937780444997576203214305328732152335729333031277824713798129\
1561128525906362017816581704020001386425304401708218472339006972427900320373500\
2785254413791829786239119189698174151879946884617473825813834965557868606323611\
9130723929973173232037676743659319972210894275877710333185091850615091699690800\
7786516743990809096188935555200413406930218098869280980433623941260807503371676\
6497765574522576174251984125865283214736699007200752059050671833024509448597964\
4081447888376081078472943701147302371285456158635432103502841496876705880085878\
1598837503612232779281356521173745791203565992056112674550583179528930967612423\
3865515678106534297900427631905101401638137736951936596960636275672496134536478\
8510720000000000000000000000000000000000000000000000000000000000000000000000000\
000000000000000000000000000000000000000000000000

Execution time:  0  days,  6  hours,  40  minutes and  44.2  seconds.

Iteration  11 :
Difference in order with S_ 1023 :  0

Galois Group:  S1023  with order  529153202740122781550480658660532689257964254\
2517591254377802998714072863352906839583145492320522057342850769977626765175117\
1305250994860181684973958371283116051516407496581422828934816107215934155828189\
4202878854799334379772146164605591004584311768763356713400354912861458704302535\
3988604774121957384488815334350765531767038401150472684884362520135291075808652\
9680218292072479184398367883814618253340953344838348116590682410315356650785771\
0269482367090193244541253842104528754017471490411529502796829370347046762713475\
0503732710934126548254324112606469599065416122296419019327457770948695667031493\
0744183877708453303454006884985624699858698531969823316283964172620615693600575\
1628868615364283434725559792829897101374176198991839906827231520082796344066853\
2586462991572087657036120193037562444068411537273233649391927486015990968619885\
4097818907801238422877279008058853920103726274104070778648529719407958366862784\
6776322039172798663697894391092800601939189737834636450845353785962947523822152\
8465937269723393645412193288214417607258701068760280587160031733667005020231214\
8976263299881037230146671122633531554399817049797843406446144119311714401065517\
8553446515844247955457654441182866433381475900767340770331439120009676751631713\
3953717315414170120115759924624651708807100642361714206470034175997104382886567\
5166579085914452451555631352152941520180795422963819693105553618782701939441897\
0314245395490788854799225797386984631833201089537144818424069727553541968354 81\
5973990808599247278073053293800796585956452073101150396595986872610591306582118\
5532143243421861401375513994025412570272022006325557772525066681742325904789126\
8164730317329203471678528209766910694874721360730784512550550605189054015988817\
0641941245481604897630560425441532223892558251008214928978014557615263636418604\
2000855311020951908425075295337407217023366780363101313301288712995394258294657\
5699389982380640060989406681914444699616912003575393614297124834038119030068410\
2695560632231002157601409840213736902049929598850817552454523203784017114390909\
4078406825549524638103863855860392453893491644441121609207867022307333052839357\
3249204036269448787317141008134648223290663159505708710130686367677607002405885\
3517922515502952496049700308960052541202342387415388395043007806672816018023215\
4098014969399838765363841894502985071447585190016285345473770322656171253311356\
0957529393142045433660260641984856580358752174080000000000000000000000000000000\
0000000000000000000000000000000000000000000000000000000000000000000000000000000\
0000000000000000000000000000000000000000000000000000000000000000000000000000000\
0000000000000000000000000000000000000000000000000000000000000000

Execution time:  2  days,  10  hours,  52  minutes and  35.1  seconds.
```