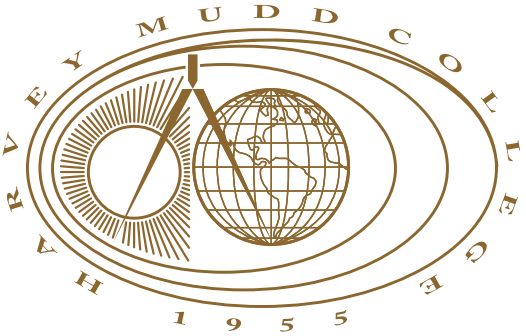
2008

Rigid Divisibility Sequences Generated by Polynomial Iteration

Brian Rice
Harvey Mudd College



Rigid Divisibility Sequences Generated by Polynomial Iteration

Brian Rice

Nicholas Pippenger, Advisor

Christopher Towse, Reader

May, 2008

HARVEY MUDD
COLLEGE
Department of Mathematics

Abstract

The goal of this thesis is to explore the properties of a certain class of sequences, *rigid divisibility sequences*, generated by the iteration of certain polynomials whose coefficients are algebraic integers. The main goal is to provide, as far as is possible, a classification and description of those polynomials which generate rigid divisibility sequences.

Contents

Abstract **iii**

Acknowledgments **vii**

1 Introduction and Background **1**
1.1 Arithmetic Dynamics 1
1.2 Rigid Divisibility Sequences 2
1.3 The Main Problem 3
1.4 Previous Results 4

2 Original Results and Proofs **5**
2.1 Sufficient Conditions 5
2.2 Necessary Conditions 11

3 Future Work **17**
3.1 Conjectures and Difficulties 17
3.2 Further Directions 19

Bibliography **21**

Acknowledgments

I would like to thank my advisor, Nicholas Pippenger, and reader, Christopher Towse, for helpful advice over the past year. I would also like to thank Rafe Jones for useful comments and for getting me interested in arithmetic dynamics in the first place.

Chapter 1

Introduction and Background

1.1 Arithmetic Dynamics

The main topic of the current work falls under the purview of a subject known as arithmetic dynamics. Like many other subjects in mathematics, arithmetic dynamics is a crossover field; in this case the combination is of number theory and discrete dynamical systems. In a general sense arithmetic dynamics is the study of the arithmetic (number-theoretic) properties of sequences which are generated by some sort of iteration.

The iteration in question can vary substantially, but generally it is taken to be a function which takes one or more integer (or rational) arguments and outputs some integer (respectively, rational number). This function can be a linear recurrence, a polynomial, a rational function, or something more esoteric such as a function associated with an elliptic curve. When we begin with some (given) initial values, iterating this function gives a sequence of integers (or rational numbers). We then may ask questions about the sequence. Some such questions regard the primes which divide the terms of the sequence (or, in the case of rational sequences, the primes dividing the numerators).

To clarify this, it is expedient to give some examples. Let us begin with a well-known recurrence sequence: the Fibonacci numbers. Recall that the Fibonacci numbers are given by the recurrence $a_{n+1} = a_n + a_{n-1}$, together with the initial conditions $a_1 = a_2 = 1$, so that $a_3 = 2$, $a_4 = 3$, $a_5 = 5$, $a_6 = 8$, and so on. It is an easy result that for each prime p, there is some Fibonacci number a_n such that $p|a_n$, which is a result of this kind. Thus, the (natural) density of primes p which divide some Fibonacci number is $D(\{a_n\}) = 1$.

Consider another sequence, given by the same recursion $b_{n+1} = b_n + b_{n-1}$, but with the initial conditions $b_1 = 1$ and $b_2 = 3$. This sequence is called the Lucas sequence, and it bears many resemblances to the Fibonacci sequence: the same growth rate, similar combinatorial interpretations, and so on. But it has important differences in its arithmetic dynamics. It is, for instance, a deep modern result [4] that the density of primes dividing some Lucas number is $D(\{b_n\}) = \frac{2}{3}$. For many other related sequences, it is not even known whether such a density exists.

Of course, it is not only this density D of primes dividing a sequence that we might be interested in. Another question of interest is that of primitive prime divisors. A term a_n of a sequence is said to have a primitive prime divisor if there is a prime $p|a_n$ such that $p \nmid a_k$ for any $1 \leq k < n$. A relatively recent paper [1] showed that for certain classes of sequences (the Lucas and Lehmer sequences, some of which are given by linear recurrences) all but finitely many terms of the sequence have primitive prime divisors.

The arithmetic dynamics of linear recurrence relations was (and is) a fruitful field of study, but there are other iteratively-generated sequences which have also proven interesting. I mentioned above polynomials and rational functions as the function to iterate; similar sorts of questions are considered in these cases as well. In [5] I looked at the question of primitive prime divisors for certain classes of sequences generated by polynomials; in [2] Ingram and Silverman explore the same question for a rational functions where 0 is a periodic point. In [3] Jones shows that for sequences generated by some classes of polynomials, the density $D(\{a_n\})$ of primes dividing some term in the sequence must by 0.

1.2 Rigid Divisibility Sequences

In addition to examining the sets of primes which divide some term of a sequence and looking at when terms of the sequence have primitive prime divisors, we might also consider what exactly happens when a particular prime divides a term of the sequence. For instance, we might be interested in sequences all of whose terms are squarefree (every prime divides each term either with exponent 1 or not at all; this is a very strong condition), or sequences where primes appear as divisors of a term of the sequence at regular intervals. One such condition, which can be seen as a weakening of the squarefree condition, is known as *rigid divisibility*.

Before we can define a rigid divisibility sequence, we need another definition.

Definition 1. *A sequence $a_1, a_2, \ldots$ of (algebraic) integers is a* divisibility sequence *if whenever $m|n$, $a_m|a_n$.*

The criterion of rigid divisibility strengthens this.

Definition 2. *A sequence $a_1, a_2, \ldots$ of integers is a* rigid divisibility sequence *if it is a divisibility sequence, and for every prime p, there is an exponent d_p such that for every term a_n of the sequence, either $p \nmid a_n$ or $p^{d_p} \| a_n$.*

Essentially, this means that if a prime p divides the nth term of the sequence, it divides, for all m, the mnth term to exactly the same power.

Example 1. *The sequence $-4, 12, 140, 19596, \ldots$ given by $a_1 = -4$ and $a_{n+1} = a_n^2 - 4$ is a rigid divisibility sequence: for instance, each term is divisible by $4 = 2^2$, but no term is divisible by 2^3, and each term divisible by 3 (every other term) is divisible by 3^1 but not by 3^2.*

It turns out that it is useful to talk about rigid divisibility sequences whose terms are elements of the ring of integers $\mathcal{O}_K$ of some number field K rather than just ordinary rational integers. Since in many such cases we do not have unique factorization of elements, we need to adjust our definition to be in terms of prime ideals instead.

Definition 3. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. A sequence $a_1, a_2, \ldots$ is a* rigid divisibility sequence *in $\mathcal{O}_K$ if it is a divisibility sequence, and for every prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$, there is an exponent $d_\mathfrak{p}$ such that, for each term a_n, if $a_n \in \mathfrak{p}$, then $a_n \in \mathfrak{p}^{d_\mathfrak{p}}$ and $a_n \notin \mathfrak{p}^{d_\mathfrak{p}+1}$.*

It is easy to see that this is equivalent to the first definition when $\mathcal{O}_K = \mathbb{Z}$ (that is, when $K = \mathbb{Q}$). Many results about rational integer rigid divisibility sequences extend easily to the more general case, and working in more generality allows us to approach even the rational integer case better.

1.3 The Main Problem

Definition 4. *Let $f(x) \in \mathcal{O}_k[x]$ be a polynomial with coefficients in $\mathcal{O}_K$, and define the sequence $\{a_n\}$ by $a_1 = f(0)$ and $a_{n+1} = f(a_n)$ for $n \geq 1$. This sequence is called the* sequence generated by $f(x)$*, and conversely we say that $f(x)$* generates *$\{a_n\}$.*

A straightforward induction shows that every such sequence is a divisibility sequence. Sometimes it will be the case that it is also a rigid divisibility sequence in $\mathcal{O}_K$, and sometimes it will not. The main goals of this project are to determine and classify, as explicitly as possible, the set of polynomials $f(x) \in \mathcal{O}_K[x]$ which generate rigid divisibility sequences, and to describe any additional properties of these polynomials and the sequences they generate.

Since we are only concerned with sequences which are generated by the iteration of polynomials in this way, we will from here on use "rigid divisibility sequence" to refer to a rigid divisibility sequence generated by some polynomial in the manner given above.

1.4 Previous Results

There are a few results which were already known about rigid divisibility sequences in $\mathbb{Z}$ and the polynomials which generate them. They come from [5], where rigid divisibility sequences were considered in order to shed light on primitive prime divisors.

Proposition 1. *Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic polynomial with linear coefficient 0. Then the sequence $\{a_n\}$ generated by $f(x)$ is a rigid divisibility sequence.*

Example 2. *The sequence $-4, 12, 140, 19596, \ldots$ given earlier is generated by the polynomial $f(x) = x^2 - 4$, and thus is a rigid divisibility sequence.*

Proposition 2. *Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic polynomial all of whose roots lie in $\mathbb{Z}$. Further suppose that the sequence generated by $f(x)$ is a rigid divisibility sequence. Let r be a root of $f(x)$, and define $g(x) = f(x + r) - r$. Then the sequence generated by $g(x)$ is also a rigid divisibility sequence.*

Example 3. *We note that this result shows that the polynomial $f(x) = x^3 - 2x^2 - 15x + 3$ generates a rigid divisibility sequence. This is because $f(x) = g(x - 3) + 3$, where $g(x) = (x + 6)(x - 2)(x + 3) = x^3 + 7x^2 - 36$ has linear coefficient 0 and thus generates a rigid divisibility sequence by Proposition 1.*

The first part of my new work consists of extending and strengthening these results to apply more generally in rings $\mathcal{O}_K$. Afterwords, I will work in the opposite direction, determining necessary conditions for a polynomial to generate a rigid divisibility sequence.

Chapter 2

Original Results and Proofs

This section consists of results and their proofs, together with some short comments. K and L are always number fields, and $\mathcal{O}_K$ and $\mathcal{O}_L$ are their rings of integers.

2.1 Sufficient Conditions

We begin with theorems which show that certain classes of polynomials always generate rigid divisibility sequences. The following theorem is a generalization of Proposition 1. It gives us a large, easily-described class of polynomials which generate rigid divisibility sequences. These are, with Theorem 3 the indirect source of nearly all known polynomials which generate rigid divisibility sequences.

Theorem 1. *Let $f(x) \in \mathcal{O}_K[x]$, and suppose that the linear coefficient of $f(x)$ is 0. Then the sequence generated by $f(x)$ is a rigid divisibility sequence in $\mathcal{O}_K$ provided that it has no terms equal to 0.*

Proof. We will show that the sequence satisfies the required property with respect to every prime ideal $\mathfrak{p}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. If no term of the sequence $\{a_n\}$ is contained in $\mathfrak{p}$, then we are done. Otherwise, let n be minimal such that $a_n \in \mathfrak{p}$, and suppose that $a_n \in \mathfrak{p}^d$ but $a_n \notin \mathfrak{p}^{d+1}$. Then it follows that $a_n = \alpha + \beta$, where $\beta \in \mathfrak{p}^{d+1}$ and $\alpha \in \mathfrak{p}^d$ but $\alpha \notin \mathfrak{p}^{d+1}$.

Now we show by induction on k that for $k \geq 1$, $a_{n+k} = a_k + \beta_k$, where $\beta_k \in \mathfrak{p}^{d+1}$. Consider first $k = 1$. Then

$$a_{n+1} = f(a_n) = f(0) + \sum_{i=2}^{D} \gamma_i (\alpha + \beta)^i = a_1 + \sum_{i=2}^{D} \gamma_i \sum_{\ell=0}^{i} \binom{i}{\ell} \alpha^\ell \beta^{i-\ell},$$

where D is the degree of f and the γ_i are its coefficients. Now whenever $\ell < i$, each such term has a factor of $\beta \in \mathfrak{p}^{d+1}$, and so lies in $\mathfrak{p}^{d+1}$. But when $\ell = i > 2$, the term α^ℓ lies in $(\mathfrak{p}^d)^2 = \mathfrak{p}^{2d} \subseteq \mathfrak{p}^{d+1}$, so those terms lie in $\mathfrak{p}^{d+1}$ as well. It follows that all of the terms except for a_1 lie in $\mathfrak{p}^{d+1}$, so we obtain $a_{n+1} = a_1 + \beta_1$, where $\beta_1 \in \mathfrak{p}^{d+1}$.

This is our base case. Now we proceed to the inductive step; let us suppose that $a_{n+k} = a_k + \beta_k$ with $\beta_k \in \mathfrak{p}^{d+1}$. Then we have

$$a_{n+k+1} = f(a_k + \beta_k) = \sum_{i=0}^{D} \sum_{\ell=0}^{i} \gamma_i \binom{i}{\ell} a_k^\ell \beta_k^{i-\ell}.$$

Whenever $\ell < i$, these terms have a factor of $\beta_k \in \mathfrak{p}^{d+1}$, and thus lie in $\mathfrak{p}^{d+l}$. Hence it follows that

$$a_{n+k+1} = \sum_{i=0}^{D} \gamma_i a_k^i + \beta_{k+1} = f(a_k) + \beta_{k+1} = a_{k+1} + \beta_{k+1}$$

for some $\beta_{k+1} \in \mathfrak{p}^{d+1}$. This completes the inductive step.

Now consider a_m. By repeated application of the above result, we obtain that

$$a_m = a_{m-n} + \beta_{m-n} = a_{m-2n} + \beta_{m-2n} + \beta_{m-n} = \cdots = a_r + B,$$

where $1 \leq r \leq n$ is congruent to m modulo n and $B \in \mathfrak{p}^{d+1}$. But we know that $a_r \notin \mathfrak{p}^{d+1}$, since $a_r \notin \mathfrak{p}$ for $r < n$ by our choice of n and $a_n \notin \mathfrak{p}^{d+1}$ by our choice of e. It follows that $a_m \notin \mathfrak{p}^{d+l}$.

On the other hand, if $r < n$, then since $a_r \notin \mathfrak{p}$, also $a_m \notin \mathfrak{p}$, whereas if $r = n$, then $a_r = a_n + B \in \mathfrak{p}^d$, so that $a_m \in \mathfrak{p}^d$. It follows that for every m, if $a_m \in \mathfrak{p}$, then $a_m \in \mathfrak{p}^d$ but $a_m \notin \mathfrak{p}^{d+1}$, which is just the property we wanted. Since this holds for each prime $\mathfrak{p} \lhd \mathcal{O}_K$, the sequence $\{a_n\}$ is a rigid divisibility sequence in $\mathcal{O}_K$. □

The next result is not just about rigid divisibility sequences, or even about polynomials with algebraic integer coefficients. It applies to any polynomial. The sequences $a(n,k)$ are called the *sequence factors* of $a(n)$, and this process is called sequence factorization. In case that $f(x)$ does have algebraic integer coefficients, so will each of $f_k(x)$, and thus this sequence factorization will be able to give us information about the sequences $a(n,k)$. The result first appeared in [5].

Proposition 3. *Let $f(x) \in \mathbb{C}[x]$ be a monic polynomial of degree D, and call the sequence it generates $a(n)$. Let the roots of $f(x)$ be $r_1, \ldots, r_d$, and define*

$f_k(x) := f(x + r_k) - r_k$. Let $a(n,k)$ be the sequence generated by $f_k(x)$. Then for every $n \geq 1$,

$$a(n) = \prod_{k=1}^{D} a(n,k).$$

Proof. We begin with a lemma:

Lemma 1. *For each $n \geq 1$, $a(n+1,k) = a(n,k) - r_k$.*

Proof. By induction on n. We have that

$$a(2,k) = f_k(a(1,k)) = f(-r_k + r_k) - r_k = f(0) - r_k = a(1) - r_k.$$

This is the base case $n = 1$. Then we have

$$a(n+2,k) = f_k(a(n+1,k)) = f(a(n) - r_k + r_k) - r_k = f(a(n)) - r_k = a(n+1) - r_k.$$

This completes the inductive step and the proof. □

Now we prove our proposition by induction on n.

First, note that $f_k(0) = f(r_k) - r_k = -r_k$, since r_k is a root of $f(x)$. It follows that

$$\prod_{k=1}^{d} a(1,k) = \prod_{k=1}^{d} f_k(0) = \prod_{k=1}^{d}(-r_k) = (-1)^d \prod_{k=1}^{d} r_k = f(0) = a(1).$$

This is the base case.

Now suppose that the statement holds for n, and consider $n+1$. We have

$$\prod_{k=1}^{d} a(n+1,k) = \prod_{k=1}^{d}(a(n) - r_k) = f(a(n)) = a(n+1);$$

the first equality holds by the lemma and the second since $f(x) = \prod(x - r_k)$ as the r_k are all the roots of $f(x)$. This completes the inductive step and the proof. □

Example 4. *Consider again the polynomial $f(x) = x^2 - 4$, which generates the sequence $-4, 12, 140, 19596, \ldots$. Then we have $f_1(x) = x^2 - 4x + 2$ and $f_2(x) = x^2 + 4x - 2$. These polynomials generate the sequences $2, -2, 14, 142, \ldots$ and $-2, -6, 10, 138, \ldots$ respectively. We have $(2)(-2) = -4$, $(-2)(-6) = 12$, $(14)(10) = 140$, and so on.*

We might want to know whether the extension of the notion of rigid divisibility to rings of integers in arbitrary number fields is actually reasonable. For instance, is it really a property of the sequence, or just of the sequence-ring pairing? The following theorem asserts that the answer is the former.

Theorem 2. *Let $f(x) \in \mathcal{O}_L[x]$, with $K \leq L$. Suppose further that the terms of the sequence generated by $f(x)$ all lie in $\mathcal{O}_K$ (in particular this occurs when $f(x) \in \mathcal{O}_K[x]$). Then the sequence generated by $f(x)$ is a rigid divisibility sequence in $\mathcal{O}_K$ if and only if it is a rigid divisibility sequence in $\mathcal{O}_L$.*

Proof. We have two directions to show.

First suppose that $\{a_n\}$ is a rigid divisibility sequence in $\mathcal{O}_K$, and let $\mathfrak{p} \lhd \mathcal{O}_L$ be a prime ideal of $\mathcal{O}_L$. Then $\mathfrak{p}$ lies over a unique prime $\mathfrak{p}_0$ of $\mathcal{O}_K$. Since $\mathfrak{p} \cap \mathcal{O}_K = \mathfrak{p}_0$, it follows that $a_n \in \mathfrak{p}$ if and only if $a_n \in \mathfrak{p}_0$.

If there is no n such that $a_n \in \mathfrak{p}_0$, then there is no n such that $a_n \in \mathfrak{p}$, and the required condition is satisfied trivially. So suppose instead that there are some n such that $a_n \in \mathfrak{p}_0$.

Let d be the exponent associated with $\mathfrak{p}_0$ in the definition of rigid divisibility sequence in $\mathcal{O}_K$, and let e be the ramification index of $\mathfrak{p}$ over $\mathfrak{p}_0$. Then I claim that the exponent de will work: that is, whenever $a_n \in \mathfrak{p}$, then $a_n \in \mathfrak{p}^{de}$, but $a_n \notin \mathfrak{p}^{de+1}$.

On the one hand, we have $\mathfrak{p}_0\mathcal{O}_L \subseteq \mathfrak{p}^e$; hence exponentiating we obtain $\mathfrak{p}_0^d\mathcal{O}_L \subseteq \mathfrak{p}^{de}$. Thus we have: if $a_n \in \mathfrak{p}$, then $a_n \in \mathfrak{p}_0$, and so $a_n \in \mathfrak{p}_0^d$, hence $a_n \in \mathfrak{p}_0^d\mathcal{O}_L$, and finally $a_n \in \mathfrak{p}^{de}$.

On the other hand, suppose that $a_n \in \mathfrak{p}^{de+1}$. Consider $(A \cap \mathcal{O}_K)\mathcal{O}_L$ for an ideal $A \lhd \mathcal{O}_L$. We have $(A \cap \mathcal{O}_K)\mathcal{O}_L \subseteq A\mathcal{O}_L = A$. Now apply this in the case $A = \mathfrak{p}^{de+1}$. We thus have that $(\mathfrak{p}^{de+1} \cap \mathcal{O}_K)\mathcal{O}_L \subseteq \mathfrak{p}^{de+1}$. Let $B = \mathfrak{p}^{de+1} \cap \mathcal{O}_K$, so that $B\mathcal{O}_L \subseteq \mathfrak{p}^{de+1}$. But $\mathfrak{p}_0^d\mathcal{O}_L = \left(\prod \mathfrak{p}_i^{e_i}\right)^d = \mathfrak{p}^{de}\prod \mathfrak{p}_i^{de^i} \nsubseteq \mathfrak{p}^{de+1}$, where the p_i are the other primes lying over $\mathfrak{p}_0$, with corresponding ramification indices e_i. It follows that $B \not\supseteq \mathfrak{p}_0^d$. Now since $\mathfrak{p}^{ef+1}$ is a primary ideal, it follows also that B is primary, since $ab \in B$, $a, b \in \mathcal{O}_K$ implies that $ab \in \mathfrak{p}^{ef+1}$, and thus $a \in \mathfrak{p}^{ef+1}$ or $b^g \in \mathfrak{p}^{ef+1}$, thus $a \in B$ or $b^g \in B$ for some positive integer g. But also $B \subset \mathfrak{p} \cap \mathcal{O}_K = \mathfrak{p}_0$, so since primary ideals in Dedekind domains are just powers of prime ideals, $B = \mathfrak{p}_0^h$ for some h. Since $B \not\supseteq \mathfrak{p}_0^d$, it follows that $h \geq d + 1$; hence $B \subseteq \mathfrak{p}_0^{d+1}$. Thus, since $a_n \in B$, it follows that $a_n \in \mathfrak{p}_0^{d+1}$, which contradicts our choice of d. It follows that $a_n \notin \mathfrak{p}^{de+1}$.

Thus it follows that $\{a_n\}$ satisfies the rigid divisibility criterion for $\mathfrak{p}$ with exponent de; this shows that $\{a_n\}$ is a rigid divisibility sequence in

$\mathcal{O}_L$.

Conversely, suppose that $\{a_n\}$ is a rigid divisibility sequence in $\mathcal{O}_L$. Let $\mathfrak{p}_0 \lhd \mathcal{O}_K$ be a prime. If there is no $a_n \in \mathfrak{p}_0$, then the condition holds trivially, so suppose that $a_n \in \mathfrak{p}_0$ for some n. Let d be the exponent such that $a_n \in \mathfrak{p}_0^d$ but $a_n \notin \mathfrak{p}_0^{d+1}$, and let $\mathfrak{p}$ be a prime in $\mathcal{O}_L$ lying over $\mathfrak{p}_0$. Let its ramification index be e. Hence $a_n \in \mathfrak{p}^{de}$, but as above $a_n \notin \mathfrak{p}^{de+1}$. Since $\{a_n\}$ is a rigid divisibility sequence in $\mathcal{O}_L$, whenever $a_m \in \mathfrak{p}$, then $a_m \in \mathfrak{p}^{de}$ but $a_m \notin \mathfrak{p}^{de+1}$. Thus we have: whenever $a_m \in \mathfrak{p}_0$, then $a_m \in \mathfrak{p}$, whence $a_m \in \mathfrak{p}^{de}$ but $a_m \notin \mathfrak{p}^{de+1}$, so that $a_m \in \mathfrak{p}_0^d$ but $a_m \notin \mathfrak{p}^{d+1}$. It follows that $\{a_n\}$ satisfies the rigid divisibility criterion for $\mathfrak{p}_0$ with exponent d; this shows that $\{a_n\}$ is a rigid divisibility sequence in $\mathcal{O}_K$. □

This is a very comforting result because it means that rigid divisibility is really a single property, not something which can vary depending on which field we examine it in, and thus justifies the our extending of the definition beyond the rational integers. It also means that we can speak about a sequence being a rigid divisibility sequence without indicating in which ring we are looking at it, because it must be a rigid divisibility sequence in any ring of integers where its terms lie.

We next want to apply Proposition 3 to obtain more rigid divisibility sequences. First, though, we need a few general lemmas about divisibility of terms in sequences generated by polynomials.

Lemma 2. *Let $f(x) \in \mathcal{O}_K[x]$, and let $\{a_n\}$ be the sequence generated by $f(x)$, and let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal. Suppose that $a_n \in \mathfrak{p}^d$. Then $a_{tn} \in \mathfrak{p}^d$ for all $t \geq 1$.*

Proof. The proof is by induction. The base case $t = 1$ is given.

Note that $a_n = f^m(0)$ (the m-th iterate of f at 0), so we have (for polynomial $g(x) = x^{-1}(f^{tn}(x) - f^{tn}(0))$)

$$a_{(t+1)n} = f^{(t+1)n}(0) = f^{tn}(a_n) = f^{tn}(0) + a_n g(a_n) \in \mathfrak{p}^d$$

by the inductive hypothesis. This completes the proof. □

Lemma 3. *Let $f(x) \in \mathcal{O}_K[x]$, and let $\{a_n\}$ be the sequence generated by $f(x)$, and let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal. Suppose that $m > n$ and $a_n \in \mathfrak{p}^d$ and $a_m \in \mathfrak{p}^d$. Then $a_{m-n} \in \mathfrak{p}^d$.*

Proof. We have similarly to above

$$a_m = f^{m-n}(a_n) = a_n g(a_n, a_m) + f^{m-n}(0)$$

for a polynomial $g(x, y)$. Since $a_m \in \mathfrak{p}^d$ and $a_n \in \mathfrak{p}^d$, it follows that

$$a_{m-n} = f^{m-n}(0) = a_m - a_n g(a_n, a_m) \in \mathfrak{p}^d,$$

as required. □

Corollary 1. *Let $f(x) \in \mathcal{O}_K[x]$, and let $\{a_n\}$ be the sequence generated by $f(x)$, and let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal. Suppose that $m > n$ and $a_n \in \mathfrak{p}^d$ and $a_m \in \mathfrak{p}^d$. Then $a_{(m,n)} \in \mathfrak{p}^d$.*

Proof. This follows from Lemma 3 by the Euclidean algorithm (naive form). □

The next theorem allows us to find new rigid divisibility sequences from old ones using sequence factorization.

Theorem 3. *Let $f(x) \in \mathcal{O}_K$ be monic, and suppose that the sequence generated by $f(x)$ is a rigid divisibility sequence. Let r be a root of $f(x)$. Then the sequence generated by $f(x + r) - r$ is also a rigid divisibility sequence.*

Proof. Let L be the splitting field of $f(x)$ over K. Then all of the roots of $f(x)$ lie in $\mathcal{O}_L$; hence the coefficients of all the polynomials $f(x + r) - r$ (for each root r) lie in $\mathcal{O}_L$. Let the sequence $\{a(n)\}$ be the sequence generated by $f(x)$, and $\{a(n, k)\}$ be the sequence generated by $f(x + r_k) - r_k$ for each root r_k of $f(x)$. Let the degree (and thus number of roots, including repetitions) of $f(x)$ be D. Note that $a(n, k) \in \mathcal{O}_L$ for all n and k.

Now let $\mathfrak{p} \lhd \mathcal{O}_L$ be a prime. If $a(n) \notin \mathfrak{p}$ for any n, then it follows that $a(k, n) \notin \mathfrak{p}$, since $\mathfrak{p}$ is an ideal. So the rigid divisibility condition vacuously holds for $\mathfrak{p}$ in this case.

On the other hand, suppose that n is minimal such that $a(n) \in \mathfrak{p}$. Let the exponent associated with $\mathfrak{p}$ be d; so that $a(n) \in \mathfrak{p}^d$ but $a(n) \notin \mathfrak{p}^{d+1}$. Now by Corollary 1 we know that only for multiples of n is $a(m) \in \mathfrak{p}$.

For each k let d_k be the exponent such that $a(n, k) \in \mathfrak{p}^{d_k}$ but $a(n, k) \notin \mathfrak{p}^{d_k+1}$. Since $\prod a(n, k) = a(n) \in \mathfrak{p}^d$, it follows that $\sum d_k \geq d$. And since $a(n) \notin \mathfrak{p}^{d+1}$, it follows that $\sum d_k < d + 1$. Hence $\sum d_k = d$.

Let m be such that $a(m) \in \mathfrak{p}$ (since only for such m can $a(m, k) \in \mathfrak{p}$, as noted above), and consider h_k, the exponents such that $a(n, k) \in \mathfrak{p}^{h_k}$ but $a(n, k) \in \mathfrak{p}^{h_k}$. Now as noted above, $n|m$, and thus it follows from Lemma 2 that $h_k \geq d_k$ when $d_k \geq 1$, and of course $h_k \geq d_k$ trivially when $d_k = 0$. But since $a(n)$ is a rigid divisibility sequence, we know that $a(m) \in \mathfrak{p}^d$ but $a(m) \notin \mathfrak{p}^{d+1}$, and thus $\sum h_k = d = \sum d_k$ as before. Thus it follows that adding the inequalities $h_k \geq d_k$ yields an equality: so each of those

inequalities must have in fact been an equality, and thus $h_k = d_k$ for each k. But this held for any m such that $a(m) \in \mathfrak{p}$, thus for any m such that $a(m,k) \in \mathfrak{p}$, and it therefore follows that for $\{a(n,k)\}$ the rigid divisibility condition holds for $\mathfrak{p}$ with exponent d_k.

This applied for all primes $\mathfrak{p} \lhd \mathcal{O}_K$, the sequences generated by $f(x + r_k) - r_k$ are rigid divisibility sequences, and in particular the sequence generated by $f(x + r) - r$ is a rigid divisibility sequence, as claimed. □

This can be expressed simply as *sequence factors of rigid divisibility sequences are rigid divisibility sequences*. It is worth noting that this result is, even in the case $\mathcal{O}_K = \mathbb{Z}$, strictly stronger than Proposition 2. For a polynomial $f(x)$ might have some integer roots and some roots which are not integers: in that case Proposition 2 does not apply, so we cannot conclude from it that even the sequence factors which consist of rational integers are rigid divisibility sequences. However, the above theorem shows that this is, in fact, the case. This is an example of the utility of expanding beyond $\mathbb{Z}$.

Example 5. *The polynomial $f(x) = x^3 - 3x^2 + 3x + 1$ is equal to $g(x-1)+1$, where $g(x) = x^3 + 1$. Since $g(x)$ has linear coefficient 0, it generates a rigid divisibility sequence by Theorem 1. Since -1 is a root of $g(x)$, it follows from Theorem 3 that the sequence $1, 2, 3, 10, 731, \ldots$ generated by $f(x)$ is also a rigid divisibility sequence. Since the other roots of $g(x)$ are not rational integers, this result would not follow from Proposition 2.*

2.2 Necessary Conditions

All of the above theorems are geared toward giving sufficient conditions for a polynomial to generate a rigid divisibility sequence. However, if we want to characterize the polynomials which give rise to rigid divisibility sequences, we need necessary conditions as well. The following theorem is a step in this direction.

Theorem 4. *Let $f(x) \in \mathcal{O}_K$, and let $\{a_n\}$ be the sequence generated by $f(x)$. Define the polynomials $\{f_n(x)\}$ by $f_1(x) = f(x)$ and $f_{n+1}(x) = f(f_n(x))$; so that, in particular, $a_n = f_n(0)$. Define c_n to be the linear coefficient of $f_n(x)$ for each $n \geq 1$. Then $\{a_n\}$ is a rigid divisibility sequence if and only if the following holds:*

For all prime ideals $\mathfrak{p} \lhd \mathcal{O}_K$, if $a_n \in \mathfrak{p}$ then $c_n \in \mathfrak{p}$.

Proof. We note that the linear coefficient of a polynomial is the constant term of its derivative; in particular, $c_n = f_n'(0)$. This is useful because we can do many computations more easily by working with derivatives rather than linear coefficients of the polynomials.

For convenience of notation we define $a_0 = 0$. Note also that we have dropped the number of iterations of f into a subscript to avoid confusion with the derivative. We first wish to show the following result (the messy part of the proof):

Lemma 4. *Suppose that $a_n \in \mathfrak{p}^d$, $d \geq 1$. Then for all $k \geq 1$,*

$$a_{n+k} \in a_n \prod_{r=0}^{k-1} f'(a_r) + a_k + \mathfrak{p}^{d+1}.$$

Proof. The proof is by induction on k. Let $f(x) = \sum_{i=1}^{D} \gamma_i x^i$. For $k = 1$, we have

$$a_{n+1} = f(a_n) = \sum_{i=0}^{D} \gamma_i (a_n)^i = \gamma_0 + \gamma_1 a_n + (a_n)^2 \sum_{i=2}^{D} \gamma_i (a_n)^{i-2} = a_1 + a_n f'(a_0) + \beta,$$

where $\beta \in \mathfrak{p}^{d+1}$. Thus

$$a_{n+1} \in a_n \prod_{r=0}^{0} f'(a_r) + a_1 + \mathfrak{p}^{d+1}.$$

This is the base case.

To do the inductive step we write

$$a_{n+k} = a_n \prod_{r=0}^{k-1} f'(a_r) + a_k + \beta,$$

where $\beta \in \mathfrak{p}^{d+1}$. Then we have

$$\begin{aligned}
a_{n+k+1} &= f(a_{n+k}) = f\left(a_n \prod_{r=0}^{k-1} f'(a_r) + a_k + \beta\right) \\
&= \sum_{i=0}^{D} \gamma_i \left(a_n \prod_{r=0}^{k-1} f'(a_r) + a_k + \beta\right)^i \\
&= \sum_{i=0}^{D} \gamma_i \sum_{\ell=0}^{i} \binom{i}{\ell} a_k^\ell \left(a_n \prod_{r=0}^{k-1} f'(a_r) + \beta\right)^{i-\ell} \\
&= f(a_k) + \sum_{i=1}^{D} \gamma_i \sum_{\ell=0}^{i-1} \binom{i}{\ell} a_k^\ell \left(a_n \prod_{r=0}^{k-1} f'(a_r) + \beta\right) \\
&= a_{k+1} + \sum_{i=1}^{D} \gamma_i \sum_{\ell=0}^{i-1} \binom{i}{\ell} \sum_{c=0}^{i-\ell} \binom{i-\ell}{c} a_k^\ell \left(a_n \prod_{r=0}^{k-1} f'(a_r)\right)^c \beta^{i-\ell-c} \\
&= f(a_k) + \left(a_n \prod_{r=0}^{k-1} f'(a_r)\right) \sum_{i=1}^{D} \gamma_i \binom{i}{i-1} (a_k)^{i-1} \\
&\quad + \sum_{i=1}^{D} \gamma_i \sum_{\ell=0}^{i-1} \binom{i}{\ell} \sum_{c=0}^{i-\ell-1} \binom{i-\ell}{c} a_k^\ell \left(a_n \prod_{r=0}^{k-1} f'(a_r)\right)^c \beta^{i-\ell-c}
\end{aligned}$$

$$\begin{aligned}
a_{n+k} &= f(a_k) + \left(a_n \prod_{r=0}^{k-1} f'(a_r)\right) f'(a_k) + \delta \\
&= f(a_k) + a_n \prod_{r=0}^{k} f'(a_r) + \delta,
\end{aligned}$$

where δ is a sum, each of whose terms contains either $\beta \in \mathfrak{p}^{d+1}$, or two terms $a_n \in \mathfrak{p}^d$; in either case contained in $\mathfrak{p}^{d+1}$, and thus $\delta \in \mathfrak{p}^{d+1}$. It follows that

$$a_{n+k+1} \in f(a_k) + a_n \prod_{r=0}^{k} f'(a_r) + \mathfrak{p}^{d+1},$$

as required. □

Now consider the quantity $f'(a_{n+m})$. We have that

$$\begin{aligned}
f'(a_{n+m}) &= f'(f_m(a_n)) = f'(f_m(0) + g(a_n, a_m)a_n) = f'(a_m + \beta) \\
&= f'(a_m) + h(a_m, \beta)\beta = f'(a_m) + \delta,
\end{aligned}$$

where $\beta, \delta \in \mathfrak{p}$. By induction we see that

$$f'(a_{n+m}) = f'(a_m) + \beta,$$

for some $\beta \in \mathfrak{p}$.

It follows that

$$a_n \prod_{r=0}^{kn-1} f'(a_r) = a_n \left(\prod_{r=0}^{n-1} f'(a_r) \right)^k + a_n\beta = a_n \left(\prod_{r=0}^{n-1} f'(a_r) \right)^k + \delta,$$

where $\beta \in \mathfrak{p}$ and thus $\delta \in \mathfrak{p}^{d+1}$.

Now we substitute $a_r = f_r(0)$ into the product and apply the chain rule, obtaining that

$$\prod_{r=0}^{n-1} f'(a_r) = \prod_{r=0}^{n-1} f'(f_r(0)) = f_n'(0).$$

Now, we wish to determine under what circumstances we never have $a_m \in \mathfrak{p}^{d+1}$ while $a_n \in \mathfrak{p}^d$ but $a_n \notin \mathfrak{p}^{d+1}$. By Corollary 1 and Lemma 2, it suffices to determine such circumstances when n is minimal such that $a_n \in \mathfrak{p}$. By Corollary 1, all terms a_m with $a_m \in \mathfrak{p}$ have $n|m$ for such an n. Together with Lemma 2, this shows that if for such a minimal n, $a_n \in \mathfrak{p}^d$, then $a_m \in \mathfrak{p}^d$ for all m with $a_m \in \mathfrak{p}$.

Hence we wish to determine, for such minimal n, under what conditions $a_{tn} \notin \mathfrak{p}^{d+1}$.

We have, from Lemma 4 and the succeeding discussion, that

$$a_{tn} \in a_n \prod_{r=0}^{(t-1)n-1} f'(a_r) + a_{(t-1)} + \mathfrak{p}^{d+1} = a_n (f_n'(0))^{(t-1)} + a_{(t-1)n} + \mathfrak{p}^{d+1}.$$

But we can apply the same result to the term $a_{(t-1)n}$, yielding a similar expression with a term $a_{(t-2)n}$, and we can continue applying the result $t-1$ times to obtain

$$\begin{aligned} a_{tn} &\in a_n (f_n'(0))^{(t-1)} + a_n (f_n'(0))^{(t-2)} + \cdots + a_n (f_n'(0)) + a_n + \mathfrak{p}^{d+1} \\ &= a_n \left(1 + \sum_{s=1}^{t-1} (f_n'(0))^s \right) + \mathfrak{p}^{d+1}. \end{aligned}$$

Now in the case that $f_n'(0) \in \mathfrak{p}$, then this becomes $a_{tn} \in a_n + \mathfrak{p}^{d+1}$ (since $a_n \in \mathfrak{p}^d$), so it is impossible that $a_n \in \mathfrak{p}^{d+1}$.

On the other hand, if $f_n'(0) \notin \mathfrak{p}$, then $f_n'(0)^z + \mathfrak{p} = 1 + \mathfrak{p}$ for some z, because $\mathcal{O}_K/\mathfrak{p}$ is a finite field, and $f_n'(0) + \mathfrak{p}$ is a nonzero element of that

field. Then consider a_{pzn}, where p is the characteristic of $\mathcal{O}_K/\mathfrak{p}$. We have, for some $\beta \in \mathfrak{p}^{d+1}$ and $\delta_i, \delta, \alpha \in \mathfrak{p}$,

$$\begin{aligned} a_{pzn} &= a_n\left(\sum_{s=0}^{pz-1}(f_n'(0))^s\right)+\beta = a_n\left(\sum_{q=0}^{p-1}\left(\sum_{s=0}^{z-1}(f_n'(0))^s+\delta_{qz+s}\right)\right)+\beta \\ &= a_n\left(\delta+p\left(\sum_{s=0}^{z-1}(f_n'(0))^s\right)\right)+\beta = a_n\alpha+\beta \in \mathfrak{p}^{d+1}. \end{aligned}$$

Hence in this case, $\{a_n\}$ cannot be a rigid divisibility sequence.

It follows that a_n is a rigid divisibility sequence if and only if, for each prime p and each n such that $a_n \in \mathfrak{p}$, also $f_n'(0) \in \mathfrak{p}$. Since $c_n = f_n'(0)$, This completes the proof. □

This is a sufficient as well as a necessary condition, but it is not as nice as the other sufficient conditions, and shows most promise at helping with the more difficult problem of finding good necessary conditions for a polynomial to generate a rigid divisibility sequence.

By using this theorem together with the fact that sequence factors of a rigid divisibility sequence are also rigid divisibility sequences (Theorem 3), we can give another necessary condition.

Theorem 5. *Let $\{a_n\}$ be a rigid divisibility sequence generated by $f(x) \in \mathcal{O}_K$. Let $r_1, \ldots, r_k$ be the roots of $f(x)$. Define as above $f_n(x)$ to be the n-th iterate of $f(x)$, and let c_n be the linear coefficient of $f_n(x)$. Then one of the following holds:*

1. *$r_i = r_j$ for some $i \neq j$*
2. *For all sufficiently large n and prime ideals $\mathfrak{p} \lhd \mathcal{O}_K$, $a_{n+1} \in \mathfrak{p}$ implies that $c_n \in \mathfrak{p}$.*

Proof. Consider the polynomials $f^i(x) := f(x + r_i) - r_i$. Analogously to the definitions above let a_n^i be the sequence generated by $f^i(x)$ and c_n^i be the linear coefficient of $f_n^i(x)$. We have that

$$f_{n+1}^i(x) = f_n(f(x + r_i)) - r_i.$$

Now because r_i is a root of $f(x)$, $f(r_i) = 0$ and thus $f(x + r_i)$ has no constant term. It follows that the linear term of $f_{n+1}^i(x)$ is just the product of the linear terms of $f(x + r_i)$ and $f_n(x)$; that is, $c_{n+1}^i = c_1^i \cdot c_n$.

Now by Theorem 3, we know that the sequences $\{a_n^i\}$ are also rigid divisibility sequences. Let L be the splitting field of $f(x)$ over K. Then each

$f^i(x) \in \mathcal{O}_L[x]$. By Theorem 4 we know that for every prime ideal $\mathfrak{p} \lhd \mathcal{O}_L$ with $a_{n+1}^i \in \mathfrak{p}$, also $c_{n+1}^i \in \mathfrak{p}$. Since $c_{n+1}^i = c_1^i \cdot c_n$, we know that either $c_1^i \in \mathfrak{p}$ or $c_n \in \mathfrak{p}$.

Now let $\mathfrak{p} \lhd \mathcal{O}_L$ be a prime such that $a_{n+1} \in \mathfrak{p}$. Then since $a_{n+1} = \prod_i a_{n+1}^i$, it follows that $c_n \in \mathfrak{p}$ or $c_1^i \in \mathfrak{p}$ for some i. There are two cases. Either $c_1^i = 0$ for some i, or not. In case $c_1^i = 0$, it follows that $f_i(x)$ has no linear term, hence $f(x + r_i)$ has no linear term. But $f(x + r_i)$ has no constant term since r_i is a root of $f(x)$, so in fact $f(x + r_i)$ has a multiple root at $x = 0$, and hence $f(x)$ has a multiple root at $x = r_i$. Thus $r_i = r_j$ for some $i \neq j$, which is the first case cited above.

So suppose that no $c_1^i = 0$. Then there are only finitely many primes $\mathfrak{p} \lhd \mathcal{O}_L$ such that $c_1^i \in \mathfrak{p}$ for some i; let n be large enough that for all $\mathfrak{p}$, if $a_m \in \mathfrak{p}$ for some m and $c_1^i \in \mathfrak{p}$ for some i, then $a_m \in \mathfrak{p}$ for some $m \leq n$. (Certainly this is true for all sufficiently large n; in particular we may take n to be the largest of all norms $N(\mathfrak{p})$ where $c_1^i \in \mathfrak{p}$ for some i.)

Consider c_{m+1}. We have

$$c_{m+1} = \sum_{k \geq 1} k b_k c_m b_0^{k-1},$$

where k is the degree of $f(x)$ and b_k the coefficient of x^k in $f(x)$. Hence $c_m \in \mathfrak{p}$ implies that $c_{m+1} \in \mathfrak{p}$. By induction it follows that $c_m \in \mathfrak{p}$ implies that $c_n \in \mathfrak{p}$ for all $n \geq m$.

Now by Theorem 4, $a_m \in \mathfrak{p}$ implies that $c_m \in \mathfrak{p}$; so for every p such that $a_m \in \mathfrak{p}$ for some m and $c_1^i \in \mathfrak{p}$, we have $c_m \in \mathfrak{p}$ for some $m \leq n$ and hence $c_n \in \mathfrak{p}$. Thus, for every prime $\mathfrak{p} \lhd \mathcal{O}_L$ such that $a_{n+1} \in \mathfrak{p}$, we have $c_n \in \mathfrak{p}$.

Now we want to show the same for primes $\mathfrak{p} \lhd \mathcal{O}_K$. Let $\mathfrak{p}$ be such a prime such that $a_{n+1} \in \mathfrak{p}$. Let $\mathfrak{p}'$ be a prime lying over $\mathfrak{p}$ in $\mathcal{O}_L$. Certainly, then, $a_{n+1} \in \mathfrak{p}'$. Therefore, $c_n \in \mathfrak{p}'$. But $c_n \in \mathcal{O}_K$, so since $\mathfrak{p}' \cap \mathcal{O}_K = \mathfrak{p}$, it follows that $c_n \in \mathfrak{p}$. This gives the second case in the theorem, and completes the proof. □

Chapter 3

Future Work

The results presented in the last section give substantial information on the polynomials which generate rigid divisibility sequences, but they are far from forming a complete characterization. The general goal of future work will be to develop Theorem 4 to get better characterizations of which polynomials generate rigid divisibility sequences.

3.1 Conjectures and Difficulties

As of this writing, the polynomials which are known to generate rigid divisibility sequences can be divided into three classes.

1. Polynomials of the form $f(x) = (x + a)^n$ for some algebraic integer a and integer $n \geq 2$. It can be shown that the sequence generated by such a polynomial $f(x)$ has terms which are the nth power of the terms of the sequence generated by $g(x) = x^n + a$. Since this polynomial generates a rigid divisibility sequence by Theorem 1, $f(x)$ does as well.

2. Polynomials $f(x)$ which have linear coefficient 0. These all generate rigid divisibility sequences by Theorem 1.

3. Polynomials which can by found from those in class (2) by some number of iterations of the sequence factorization process.

Since the rigid divisibility criterion, or equivalently, the conclusion of Theorem 4, is so restrictive, it seems unlikely that there will be any sporadic polynomials which generate rigid divisibility sequences "by accident" and

are not part of any broader class. Though it is conceivable that some other classes of polynomials exist which generate rigid divisibility sequences, this also seems unlikely at this point.

Conjecture 1. *The three classes describe above encompass all monic polynomials which generate rigid divisibility sequences.*

This is a very strong statement, however, so it perhaps will be useful to give a weaker conjecture which is more intuitively connected to what we know about these polynomials, in particular via Theorems 4 and 5. The interesting and relevant observation is that, with the exception of class (1) above, all polynomials which generate rigid divisibility sequences satisfy the conclusions of those theorems in a somewhat degenerate manner. In particular, the conclusion of Theorem 4, that $a_n \in \mathfrak{p}$ implies that $c_n \in \mathfrak{p}$, is trivially true if $c_n = 0$. Furthermore, it is not difficult to show that whenever $c_n = 0$, then $c_m = 0$ for all $m \geq n$, so that the condition will be satisfied for all larger n as well.

It happens that for both classes (2) and (3) of polynomials $f(x)$, eventually $f_n(x)$ has linear coefficient 0: that is, $c_n = 0$ for some n. This suggests that with only a few exceptions (class (1) above, for instance), the only polynomials which satisfy the conclusion of Theorem 4 satisfy it in this degenerate manner. Thus we make the following conjecture.

Conjecture 2. *Let $f(x)$ be a monic polynomial which generates a rigid divisibility sequence. Then either $f(x) = (x + a)^n$ for some algebraic integer a and integer $n \geq 2$, or there is some n such that the linear coefficient of $f_n(x)$ is 0.*

This, if true, would not immediately imply the first conjecture, but proving it would be a strong step on that path.

Unfortunately, the natural approaches to proving these conjectures meet with a number of difficulties. The natural way to approach proving that the linear coefficient of $f_n(x)$ is 0 is to try to show that it is divisible by "too many" primes: either that an infinite number of different primes must divide it, or giving a lower bound on the number of different primes which divide it, together with an upper bound on the number of primes which could divide it if it were nonzero. Theorem 5 suggests a way to attempt this, but it runs into problems. Trying to iterate the argument to get $p|a_{n+m} \Rightarrow p|c_n$ for large m is difficult not only because of the possibility that the first conclusion holds at some point, but because we cannot control how large n must be in order to be sufficiently large. For larger m, the minimum size of n depends not only on the linear terms of the polynomials obtained from

$f(x)$ by sequence factorization, but upon the linear terms of the polynomial obtained from *them* by sequence factorization, and so on. Putting any kinds of bounds on n from this is difficult, because these linear coefficients could be contained in prime ideals with very large norms, despite being of manageable absolute value.

This problem is one example of what makes this topic difficult in general. While the asymptotics of such discrete dynamical systems (e.g., growth rates) are relatively well-understood, they tell us little about their arithmetic properties. In number rings which have units with (ordinary) absolute value less than 1, the growth rate of the sequence tells us nearly nothing about the primes dividing it. Since we need to be able to deal with such rings to prove most of the interesting results even about $\mathbb{Z}$ (for example, Theorem 3), this limits the tools at our disposal with which to attack the problem. It seems quite likely that results like those conjectured will be provable, but doing so will probably require developing powerful and novel techniques.

3.2 Further Directions

In addition to the above conjectures, there are other directions in which the notions developed here could be extended.

The first way is to expand to include sequences generated by polynomials other than those which are monic with algebraic integer coefficients. Non-monic polynomials are a natural extension, and not pursued here primarily because the sequence factorization methods do not apply. Additionally, there are polynomials whose coefficients are not all integers, but which take integer values for integer inputs (e.g., $f(x) = x^3 + \frac{1}{2}x^2 + \frac{1}{2}x + 1$), and considering these polynomials as well may prove interesting.

Another direction would be to consider rigid divisibility sequences generated by other discrete dynamical systems. For instance, by extending the notion of rigid divisibility sequences to the rationals (perhaps looking at the numerators), we could examine which rational functions generate rigid divisibility sequences.

It is so far uncertain how useful the particular notion of rigid divisibility will be to arithmetical dynamics as a whole, but if the results here are any indication, it is deep enough to be worth pursuing. Identifying the set of functions within certain classes which generate rigid divisibility sequences could prove useful to examining other arithmetic properties of their dynamics. This work on the rigid divisibility sequences generated by

polynomials should serve as a beginning.

Bibliography

[1] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[2] Patrick Ingram and Joseph Silverman. Primitive divisors in arithmetic dynamics. arXiv:0707.2505v2, 2007. Preprint.

[3] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. arXiv: math.NT/0612415, 2006. Preprint.

[4] J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118(2):449–461, 1985.

[5] Brian Rice. Primitive prime divisors in polynomial arithmetic dynamics. *Integers*, 7:A26, 16 pp. (electronic), 2007.