ABSTRACT

AHRENS, KATHARINE A. Combinatorial Applications of the k-Fibonacci Numbers: A Cryptographically Motivated Analysis. (Under the direction of Ernest Stitzinger and Scott Batson.)

Recent exploration of hard problems conjectured to be quantum secure has opened a number of fascinating problems in mathematics and computer science. In this thesis, we present our research on one such problem.

To begin, we explore polynomial and matrix properties of a class of polynomials which could be relevant for a certain variant of a cryptographic hard problem currently being considered for post-quantum security. We conjecture singular value bounds tighter than those which appear in the current literature and provide heuristic evidence for these conjectures.

In the second part, we embark on a combinatorial deep dive and explore a certain generalization of Fibonacci number which arose over the course of our research. Our contributions include answering two questions specifically posed in the last decade: we defined a bijection between the k-Fibonacci numbers and a certain class of restricted integer composition, and found a general form of the generating function for the k-Fibonacci numbers.

Finally, we provide a new singular value bound for a restricted class of Vandermonde matrix and offer ideas on how this could be generalized. We also offer avenues for future work, including cryptographic and combinatorial problems.

Combinatorial Applications of the k-Fibonacci Numbers: A Cryptographically Motivated Analysis

by
Katharine A. Ahrens

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Mathematics

Raleigh, North Carolina

2020

APPROVED BY:

Agnes Szanto	Arvind Krishna Saibaba
Ernest Stitzinger Co-chair of Advisory Committee	Scott Batson Co-chair of Advisory Committee

DEDICATION

To my parents, Annette and Michael Ahrens, who sparked a love of learning in me from a very early age.

Mom, thanks for all the years of homeschooling, and for cultivating a love of books, science, and exploration. My math career would have stopped before it started if you hadn't made me take the algebra placement test a year early. Thanks for your patience with me when I "hated math" because I was "bad at it," and for the shining example of being a brilliant woman in math. I must have been in middle school when you told me the story of your math master's thesis, and how you proved the conjecture your advisor gave you—except for an edge case you discovered was false. That was the first time I thought "I want to do that."

Dad, thanks for the help with the tricky word problems: from the 8th grade "train problems," to the nasty ones about physics when I was studying for the graduate qualifying exam in mathematical modeling. I promise that for the rest of my career, I will always draw a picture.

You two are the best.

BIOGRAPHY

Katie Ahrens was born in Erie, Pennsylvania. She was homeschooled until high school, which she liked because she could get her schoolwork done early and spend the rest of the day reading books. Her 5th grade self would often take a suitcase to the library so she could more easily haul the withdrawal limit's worth of books back to the car.

In high school, Katie fell in love with music. She practiced piano many hours a day; her high school highlights included playing a Mozart piano concerto with the Erie Chamber Orchestra and twice appearing live on WQLN Radio, Erie's local NPR affiliate. She also took 47 college credits of AP and college classes. She thought she was bad at math, despite getting an A in Calculus II at Penn State Behrend her senior year.

She attended Ithaca College, and became a music school dropout eight weeks in. Two days later, she found herself on the 5th floor of the library reading a math book for fun, and she knew she had found her new major. Katie graduated Summa Cum Laude with departmental honors in both English literature and mathematics, with a minor in music.

Katie then attended North Carolina State for graduate school, where she at first couldn't decide where her research interests lay. She switched from pure to applied math and then back again. Eventually, she began research with Dr. Ernest Stitzinger on a project which involved knowing about a little bit of everything, exactly how she likes it.

When Katie is not doing math, she is out running with friends. While in grad school, she took over 45 minutes off her best half marathon time, and she is currently on a quest to qualify for the Boston Marathon.

ACKNOWLEDGEMENTS

To my family: my parents Michael and Annette, and my siblings Michelle, Matthew, and Rachel. Thank you for believing in me, putting up with me, and adding ridiculous sketches to my research notes. (Michelle, I know it was you.)

My high school teachers were instrumental in me becoming who I am today: Mrs. Nicolia, who told me an independent study of Algebra II was an option; Mrs. Lucas, who encouraged me to test out of trigonometry; and Mr. Komorek, who asked me to switch into his harder calculus section. Thank you all for seeing a mathematician in me well before I did.

My math professors at Ithaca College were amazing, and they laid the foundation for my success in graduate school and beyond. A few that come immediately to mind are Emilie Wiesner, who encouraged me to start research my sophomore year; Teresa Moore, who taught me proof writing, and that good proofs have to have words in them; Thomas Pfaff, who introduced me to both discrete math and mathematical modeling, and who only made fun of me a little bit after I forgot to set an alarm and almost slept through his final; and of course David Brown, my wonderful undergraduate research advisor. My love of Fibonacci numbers, generating functions, and interdisciplinary math started with him.

I participated in the EDGE (Enhancing Diversity in Graduate Education) program during the summer of 2015. This experience, and the people in it, convinced me that I could, in fact, cut it as a mathematician if I worked hard at it. Thanks to all the Women Math Warriors for being friendly, supportive, encouraging, and brilliant.

I have many, many people to thank from my time at NC State. First of all, my peers, without whom I would not have finished. From the Combinatorics Five to Modelers Anonymous, thank you for getting me through my quals. There was hard work but also laughter.

To Jane Ivy Coons, Katherine Harris, and Tricity Andrew. Where to start. Thank you for too many late nights, quality conversations, long runs, tasty beverages, and Mitch's lunches to count.

Along those lines, to the entire Raleigh running community. Thanks for getting me out of SAS Hall and into some fresh air, as well as providing a continual example of how a

little hard work everyday over many years leads to big dreams coming true.

Paul Erdős famously claimed that a mathematician is simply a machine for turning coffee into theorems. Thus I am grateful Raleigh has so many great local coffee spots. Thanks to Cup A Joe, where I spent most of the summer of 2016 studying for quals. And thanks to Pine State Coffee, where there are the best cappuccinos in the entire universe, and which always provided me a friendly, welcoming space to write. And party.

To all my professors at NC State, especially my committee members Agnes Szanto and Arvind Saibaba. Thank you for sharing your knowledge with me, for your helpful comments and suggestions, and for your kindness and patience.

To Scott Batson. Thank you for agreeing to be my coadvisor, driving up to NC State to meet with me, and providing advice and encouragement on everything from choosing an advisor to imposter syndrome to picking a career.

And finally, to my advisor, Ernest Stitzinger. I can confidently say that you are the main reason I survived grad school. From the day I walked into your office in 2016, completely unsure of what I wanted to do in grad school or beyond, you have been supportive and encouraging. You constantly remind me that the main point of all of this is to have fun. Thank you for believing in me, even when I didn't. I could not have done it without you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

Cryptography is ubiquitous in modern society. From email to online shopping to health and medical information, keeping data safe is of utmost importance.

Accomplishing this, especially online, relies on public key (also known as asymmetric) cryptography. In a more traditional symmetric key setup, two parties wishing to communicate securely would first have to meet in person to exchange a shared key. Since this is completely infeasible in the computer world—surely no Amazon customer would fly to Seattle to exchange a key before impulse-buying a new pair of headphones—a solution had to be reached. The RSA cryptosystem proposed in 1978 [31] neatly met this need, and variants of it are used across the internet today.

RSA has sufficed for decades, and it continues to be used today. However, RSA might be rendered obsolete in the future. RSA is based on the difficulty of factoring the product of large prime numbers, and Schor's algorithm [34] gives an efficient way to factor integers given a quantum computer. While a fully scalable quantum computer doesn't actually exist yet, Schor's algorithm—and recent success in physically constructing quantum computers, including Google's recent claim of achieving quantum supremacy [4], or a quantum computer with a discernible advantage over a classical version—has motivated a deep exploration of quantum resistant algorithms.

In the face of the quantum threat, mathematicians and computer scientists have attempted to come up with a cryptosystem which would be immune to quantum attacks. The largest effort to this end is the 2017 NIST Competition [2], which gives various schemes which are conjectured to be quantum hard. One of the leading candidates for a quantum-resistant hard problem is the learning with errors problem (LWE), first proposed in [28], and its ring-based variant ring learning with errors (RLWE) which was first proposed in [21]. It is proved in [21] that the RLWE problem is at least as hard as the problem of finding a short vector in an ideal lattice, which is widely conjectured, although not proven, to be quantum hard. Almost a third of the original NIST proposals are based on some variant of the LWE problem.

RLWE itself exists in various forms. The standard form is the form on which most of the RLWE NIST proposals are based. There is also a tweaked version, known as the non-dual form of RLWE. While only a slight difference apparently separates the dual and the non-dual form, the non-dual form does not have a security reduction to a lattice problem as the dual form does. In fact, a series of papers [16] [17] [9] [26] [32] revealed that the non-dual form is not secure in some instantiations, even *without* using a quantum computer. The attacks depend on properties of a Vandermonde matrix associated with the polynomial used to define the base ring.

This thesis is essentially in two parts. In the first part, we review some previous literature on the RLWE problem, including the cryptographic attack which motivated our work. Then we give some conjectures and heuristic evidence for the expansion of the attack into other polynomial classes. Our contributions include improving the singular value bound on our class of Vandermonde matrix, proposals for further generalizations of previously considered classes of polynomials, and heuristic observations of root behavior and singular value properties of the expanded class.

The second part of the thesis is a rabbit hole, though it is a combinatorially interesting rabbit hole which neatly answers some open questions in enumerative combinatorics. While attempting to use the Schur-Cohn theorem to prove an observed behavior of polynomial roots in the complex plane, we stumbled across a generalization of Fibonacci numbers which has not been studied in much depth in the current literature. Intrigued, we explored these numbers, known as the k-Fibonacci numbers, in connection with the Schur-Cohn matrix and obtained some exciting new results. Our contributions include defining a new class of restricted permutation; providing a new proof for the permanent of a k-tridiagonal matrix; exhibiting explicit bijections among 4 classes of combinatorial objects which the k-Fibonacci numbers count; stating and proving the general form of the k-Fibonacci generating function; and discovering a previously unknown tensor variant of Pascal's triangle.

The combinatorial contributions we made, which were motivated by questions in an entirely different mathematical field, are interesting and novel. That one branch of math can so seamlessly blend together, and that one fascinating question can give rise to another, is one of the delights of math. It was an honor to work on these questions and to be able to follow their windy, unpredictable path wherever they happened to lead.

Chapter 2

Background

In this chapter, we give some background on the ring learning with errors problem, as well as some important definitions for understanding our work in the theory of algebraic numbers, polynomials, and matrices.

We will later need some combinatorial background as well; these definitions appear in Chapter 6.

2.1 LWE and RLWE

The ring learning with errors (RLWE) problem is an adaptation of the learning with errors (LWE) problem. It was first introduced in [28]. The LWE problem is defined in [29] as follows.

Definition 1. ([29], section 1) Fix a size parameter $n \geq 1$, a modulus $q \geq 2$, and an error probability distribution χ on $\mathbb{Z}_q$. Let $A_{\mathbf{s},\chi}$ on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ be the probability distribution obtained by choosing a vector $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly random, choosing $e \in \mathbb{Z}_q$ according to χ and outputting $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle) + e$ where additions are performed in $\mathbb{Z}_q$. An algorithm solves the (search version) LWE for modulus q and error distribution χ if for any $\mathbf{s} \in \mathbb{Z}_q^n$ given an arbitrary number of independent samples from $A_{s,\chi}$ it outputs $\mathbf{s}$ with high probability.

It is shown in [28] that the LWE problem reduces quantumly to an approximate version of some lattice problem. While [28] constructs a cryptosystem around the LWE problem, the main restriction to implementing it with key sizes on cryptographic scale is the question of efficiency. One LWE pair creates only one sample, rather than a vector of samples, and as a result key sizes and computation times are very large.

The RLWE problem is a ring-based version of LWE with more efficient storage requirements and computation times. It was introduced in [21] and it is shown that the RLWE problem is hard given worst-case assumptions on the hardness of ideal lattice problems in quantum polynomial time.

Before we can define RLWE, we recall some definitions from algebra.

2.1.1 Algebraic Number Theory

RLWE is defined over algebraic extensions of fields and the rings of integers in those fields. Thus we begin by recalling some basic algebraic number theory definitions, following [23].

Let α be an algebraic number, e.g. α is the root of some degree d polynomial in $\mathbb{C}$ and is not a root of a polynomial of degree less than d. The field $\mathbb{Q}[\alpha]$ formed by adjoining α to the rational field $\mathbb{Q}$ is called the algebraic number field of degree d over $\mathbb{Q}$.

Furthermore, α has a unique minimal polynomial $m(x)$ over $\mathbb{Q}$ and this polynomial is irreducible. By the first isomorphism theorem, $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/m(x)$.

We can generalize the notion of a ring of integers to algebraic number fields. We say that algebraic integers are the algebraic numbers whose minimal polynomials have coefficients in $\mathbb{Z}$ and denote the algebraic integers of an algebraic number field K as $\mathcal{O}_K$.

A basis for $\mathcal{O}_K$ over $\mathbb{Z}$, sometimes called a $\mathbb{Z}$-basis, is called an integral basis for K. While K is guaranteed an integral basis, it is *not* necessarily true that $\mathcal{O}_K = \mathbb{Z}[\alpha]$; in other works, a basis over $\mathbb{Z}$ of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. In the special case where K has this integral power basis, K is called monogenic. Whether K is monogenic or not, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module, since it has some (not necessarily power) basis.

We use algebraic number theory to define a mapping from the ring of integers in an extension field to the real numbers as follows.

2.1.2 Canonical embeddings

Recall that a complex embedding of a number field $K = \mathbb{Q}[x]/m(x)$ for a polynomial $m(x)$ irreducible over $\mathbb{Q}$ is defined as $\sigma_i : K \to \mathbb{C}$ such that σ_i fixes every element of $\mathbb{Q}$. There are $n = \text{degree}(m(x))$ embeddings σ_i of K and these are connected to the n roots of $m(x)$. In fact, where $\alpha_1, \ldots, \alpha_n$ are the roots of $m(x)$, $\sigma_i(\alpha_1) = \alpha_i$.

If $\sigma_i(\alpha) \in \mathbb{R}$, then σ_i corresponds to a real root of $m(x)$ and σ_i is called a *real embedding.* Clearly, complex σ_i come in conjugate pairs. We denote the number of real embeddings by r_1 and the number of complex embeddings by r_2. Then $\{r_1, r_2\}$ is called the *signature* of K.

The signature of K is used to define a subspace $H \subset \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$, where

$$H = \{(x_1, \ldots, x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \ : \ x_{r_1+r_2+j} = \overline{x_{r_1+j}} \ \forall \ j \in 1, \ldots, r_1\}. \tag{2.1}$$

Note H is isomorphic to $\mathbb{R}^n$ via multiplication by the unitary matrix

$$U = \begin{bmatrix} I_{r_1+r_2} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} I_{r_2 \times r_2} & \frac{1}{\sqrt{2}} I_{r_2 \times r_2} \\ 0 & \frac{1}{\sqrt{2}} I_{r_2 \times r_2} & \frac{1}{\sqrt{2}} I_{r_2 \times r_2} \end{bmatrix}.$$

We use the n embeddings of a number field to define an $n \times n$ matrix of the embeddings. This embedding is called the *canonical embedding*, also known as the *Minkowski embedding.*

Definition 2. The matrix of the canonical embedding $M = \sigma(\mathcal{O}_K)$ of the ring of integers $\mathcal{O}_K$ in K with basis $\{b_i\}$ is defined by

$$M_{i,j} = \sigma_i(b_j)$$

where $\sigma_1, \ldots, \sigma_{r_1}$ are the real embeddings and $\sigma_{r_2}, \ldots, \sigma_n$ are the complex embeddings ordered so that $x_{r_1+r_2+j} = \overline{x_{r_1+j}}$.

While we can perform this embedding with respect to any basis, throughout we will consider the case of K monogenic and take the power basis $\{1, x, \ldots, x^{n-1}\}$ of $\mathcal{O}_K$. We denote the canonical embedding of a basis B as $\mathbf{B}$.

We can use the embeddings to define not just the image of the ring of integers $\mathcal{O}_K$, but of any ideal I within K. This works essentially the same way as the canonical embedding of $\mathcal{O}_K$: for a $\mathbb{Z}$-basis $B = \{b_1, \ldots, b_n\}$ of I, the ideal lattice L is generated by the columns of $\mathbf{B}$ where $\mathbf{B}_{i,j} = \sigma_i(b_j)$ for the n complex embeddings σ_i of K.

Important for RLWE purposes is the idea of a *dual lattice*, denoted $R^\vee$. For any ideal I, the dual lattice is $I^\vee = \{x \in K : \mathrm{Tr}(x\mathcal{L}) \subseteq \mathbb{Z}\}$ which embeds as the conjugate of the dual lattice of $I^\vee$. Where $B = (b_j)$ is an integer basis for I, then $B^\vee = (b_j^\vee)$ is an integer basis for $I^\vee$. Thus, we have $\mathbf{B}^\vee = (\mathbf{B}^{-1})^*$ where $\mathbf{B} = \sigma(B)$.

We can define the *discriminant* of a number field using the matrix $\mathbf{B}$ of the canonical embedding.

Definition 3. Let $\mathbf{B}$ be the image of a $\mathbb{Q}$ basis for K under the canonical embedding. Then the discriminant Δ_K of K is defined as $\det(\mathbf{B})^2$.

A dimension-normalized version of the discriminant is called the *root discriminant* and is defined as $\delta_K = \sqrt{\Delta_K}^{1/n} = \det(\mathbf{B})^{1/n}$.

2.1.3 Tensor products

Definition 4. A tensor product $A \otimes B$ of two matrices A and B is defined as all blocks $a_{i,j}B$ arranged in the same order as the entries of A.

A tensor product of two vector spaces V, W is defined axiomatically; see [26] or [13] for details. Mostly notably, if (v_i) and (w_j) are a basis for V and W respectively, then $(v_i \otimes w_j)$ is a basis for $V \otimes W$. A tensor product of $\mathbb{Z}$ modules is defined analogously.

Additionally, the tensor product is well-behaved multiplicatively under norms and duals, as $||a \otimes b|| = ||a||||b||$, $(A \otimes B)^\vee = A^\vee \otimes B^\vee$. Additionally, for modules $R = M \otimes N$, the root discriminant is multiplicative and thus $\delta_R = \delta_M \delta_N$.

2.1.4 Gaussians

The RLWE problem uses samples drawn from the multidimensional discrete Gaussian distribution, which is defined as follows.

Definition 5. ([21]) Let H be defined by Equation 2.1. For $r > 0$, define the Gaussian function $\rho_r : H \to (0,1]$ as $\rho_r(\mathbf{x}) = \exp(-\pi||\mathbf{x}||^2/r^2)$.The continuous Gaussian probability distribution D_r of width r has density given by $r^{-n}\rho_r(x)$.

See Figures 2.1 and 2.2 for the plot of a Gaussian distribution for varying values of r, which gives a good intuition for why r is sometimes called the "width" of the Gaussian.

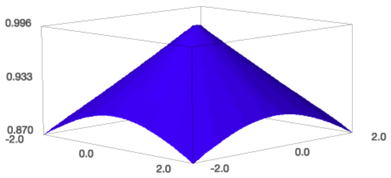


Figure 2.1: Gaussian of width $r = 8$

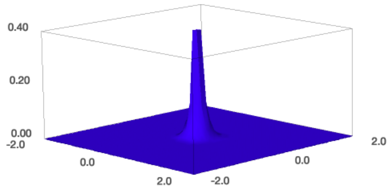


Figure 2.2: Gaussian of width $r = 0.5$

2.1.5 RLWE

Now we proceed with the RLWE definition. Note that this definition considers the Gaussian drawn from $K_{\mathbb{R}}/qR^\vee$ where $K_{\mathbb{R}} = K \otimes \mathbb{R}$, but as noted in [26], $K_{\mathbb{R}} \cong H$. While [26] uses $K_{\mathbb{R}}$ to be formal, we can view the distribution as over H which is isomorphic to K via σ^{-1}.

Definition 6 ([26] definition 2.6)**.** Fix parameters R, the ring of integers of a number field K, a positive integer modulus q, and an error distribution ψ over $K_{\mathbb{R}}$. The search RLWE$_{q,\psi}$ problem is to find a uniformly random secret $s \in R_q^\vee$ given many independent samples of the form $(a_i, b_i = sa_i + e_i \mod qR^\vee) \in R_q \times K_{\mathbb{R}}/qR^\vee$ where each $a_i \leftarrow R_q$ is uniformly random and each $e_i \leftarrow \psi$ is drawn from the error distribution. The decision RLWE problem is to distinguish with some noticible advantage between samples generated as above and uniformly random samples $R_q \times K_{\mathbb{R}}/qR^\vee$.

While it may at first seem more natural to choose $s \in R_q$ (called the non-dual form of RLWE) instead of using the dual lattice, and while they are equivalent up to choice of distribution, a spherical Gaussian in the dual form may convert to a highly elliptical Gaussian in the nondual form, giving rise to unwanted patterns in the errors which allow for solving both search and decision. It is this type of weakness which is explored in [16], [10], [26] and which we will exploit for new classes of examples.

2.2 Matrix Theory

One of the most important quantities of a matrix A is the determinant.

Definition 7. Let $A \in \mathbb{C}^{n \times n}$ be a matrix. The determinant of A is

$$\det(A) = \sum_{\pi \in S_n} \big(sign(\pi) \prod_{i=1}^{n} a_{i,\pi} \big)$$

where S_n is the set of all permutations π of the set $\{1, 2, \ldots, n\}$ and $sign(\pi) = 1$ if π is even and -1 if π is odd.

We now recall the definition of the singular value decomposition.

Definition 8. ([22]) Let $A \in \mathbb{C}^{m \times n}$ of $\text{rank}(A) = r$. There exist orthogonal matrices $U \in \mathbb{C}^{m \times m}, V \in \mathbb{C}^{n \times n}$ and a diagonal matrix $\Sigma_r = \text{diag}(s_1, s_2, \ldots, s_r)$ such that

$$A = U \begin{bmatrix} \Sigma_r & \\ & 0 \end{bmatrix} V^*$$

with $s_1 \geq s_2 \geq \cdots \geq s_r > 0$. This factorization is called a singular value decomposition of A and the s_i are called singular values.

Definition 9. ([22]) Let A be an $m \times n$ matrix.

1. The condition number of $\kappa(A)$ is s_1/s_n if $s_n > 0$ and ∞ if $s_n = 0$.
2. The Frobenius norm $||A||_F$ of $A = (a_{ij})$ is $\sqrt{\sum_{i,j} |a_{ij}|^2}$.
3. The 1-norm of A is $\|A\|_1 = \max_{1 \leq j \leq n} \sum_{i=1}^{m} |a_{i,j}|$ and the infinity norm is $\|A\|_\infty = \max_{1 \leq i \leq n} \sum_{i=1}^{n} |a_{i,j}|$.
4. The 2-norm $||A||_2$ is s_1.
5. For $p \geq 1$, let $x \in \mathbb{C}^n$ and let the vector p-norm of x be defined as $||x||_p = (\sum_{i=1}^{n})|x_i|^p)^{\frac{1}{p}}$. Then the matrix p-norm $||A||_p$ is $\sup_{x \neq 0} \frac{||Ax||_p}{||x||_p}$.

Norms are submultiplicative and various relationships exist between the common norms above.

Proposition 1. *For matrices A and B with the same number of columns,*

1. *For a p-norm $\| \cdot \|_p$, $\|AB\|_p \leq \|A\|_p \|B\|_p$.*

2. $\|A\|_2 \leq \sqrt{\|A\|_1 \|A\|_\infty}$

3. $\|A\|_2 \leq \|A\|_F$

The rest of the singular value spectrum is not submultiplicative, but the following relationship does hold.

Proposition 2. *For the singular values s_i of compatible matrices A, B,*

$$s_i(AB) \leq s_1(A)s_i(B)$$

for $1 \leq i \leq min(m, n)$.

If we happen to know the singular value spectrum of A, calculating its determinant up to absolute value is easy.

Proposition 3. $|\det(A)| = \prod_{i=1}^{n} s_i(A)$.

Singular values and the condition number have an important geometric interpretation: $s_i(A)$ is the distortion of a unit ball under multiplication by A in n-space along the ith axis, and $\kappa(A)$ quantifies the total amount of distortion in the system.

The following theorem gives an important connection from the singular values of A to a low-rank approximation of A.

Theorem 1. *([25]) Let A_{j-1} be the closest approximation of A of rank at most $j-1$. Then*

$$s_j = ||A - A_{j-1}||_2$$

for $1 \leq j \leq n$.

2.3 Polynomial Roots

Our analysis of polynomials for RLWE base rings will depend on the the following results. The theorems and definitions in this section come from [27].

Definition 10. Let $a_0, \ldots, a_n$ be a sequence of real numbers. We define $V(a_0, \ldots, a_n)$ as the total number of variations of sign in the reduced sequence obtained by ignoring all the zero elements. We agree that V assumes the value zero if only one or none of the elements is different from zero.

Example 1. $V(1, -2, 3, 0, -4, 5) = 4$, since there is one variation in sign between the 1 and -2, the -2 and 3, the 3 and -4 (here we ignore the 0), and -4 and 5. Similarly, $V(7, 0, 8, 9) = 0$.

Theorem 2 (Sturm). *Let f be a polynomial with real coefficients. Let*

$$f_{i+1} = -rem(f_i, f_{i-1})$$

where $rem(f_i, f_{i-1})$ is the remainder of the polynomials f_i, f_{i-1} as produced by the Euclidean algorithm. Then consider $f_0, f_1, f_2, \dots, f_m$ where $f_0 = f$ and $f_1 = f'$. Suppose that f does not vanish at a and b where $a < b$. Then

$$N_f[a, b] = V(f_0(a), \dots, f_m(a)) - V(f_0(b), \dots, f_m(b))$$

where $N_f[a, b]$ denotes the number of distinct zeros of f in $[a, b]$.

To find the total number of real roots, we can consider the sequences

$$V(f_0(-\infty), f_1(-\infty) \dots f_m(-\infty))$$

and

$$V(f_0(\infty), f_1(\infty) \dots f_m(\infty)),$$

where we define $f(\infty)$ as the sign of its leading coefficient, and $f(-\infty)$ as the sign of the leading coefficient of f for even degree f, and $f(-\infty)$ as the opposite sign of the leading coefficient of f for odd degree f.

Theorem 3 (Montel). *Every polynomial $f_k(z) = a_0 + a_1 z + \cdots + a_p z_p + c_1 z^{n_1} + \cdots + c_k z^{n_k}$ ($a_p \neq 0, 1 \leq n_1 < \cdots < n_k$) has a zero of modulus not exceeding $|a_0/a_p|^{1/p} r_k$ where $r_0 = 1$ and*

$$r_k = (\frac{n_1}{n_1 - k} \cdots \frac{n_k}{n_k - p})^{1/p} \leq \binom{p+k}{k}^{1/p}, k \in \mathbb{N}.$$

Theorem 4 (Budan-Fourier). *Let f be a polynomial of degree n with real coefficients. Let I be any interval and $N_f(I)$ denote the number of zeros of f in I. Let $V_f(x) = V\big(f(x), f'(x), \dots, f^{(n)}(x)\big)$. Then*

$$N_f(a, b] = V_f(a) - V_f(b) - 2k$$

for some $k \in \mathbb{N}_0$.

We will make use of the following facts from [27] below.

Definition 11. Let $f(z) = a_0 + a_1 z + \cdots + a_n z^n$ be a polynomial of degree n. Then the Cauchy bound of f, denoted $\rho[f]$, is defined as the unique positive root of the equation

$$|a_0| + |a_1|x + \cdots + |a_{n-1}|x^{n-1} = |a_n|x^n$$

when f is not a monomial and 0 otherwise.

Theorem 5 (Cauchy)**.** *All zeros of a non-constant polynomial f lie in the closed disc with center at the origin and the Cauchy bound $\rho[f]$ as radius. Moreover, for such a disc, $\rho[f]$ is the smallest radius that depends only on the moduli of the coefficients of f.*

Of course, calculating the Cauchy bound of Theorem 5 seems just as difficult as finding a root of f itself. However, this bound is useful because there are many ways of estimating it. We will make use of the following; other methods appear in Chapter 8 of [27].

Theorem 6. *For the Cauchy bound $\rho[f]$ of a polynomial f as above, then for positive numbers $\lambda_0, \ldots, \lambda_{n-1}$ such that $\sum_{\nu=0}^{n-1} \lambda_\nu = 1$, we have*

$$\rho[f] \leq \max_{0 \leq \nu \leq n-1} \left(\frac{1}{\lambda_\nu}\left|\frac{a_\nu}{a_n}\right|\right)^{\frac{1}{n-\nu}}.$$

2.4 Constructing the Vandermonde Matrix

We recall the definition of a Vandermonde matrix, since properties of Vandermonde matrices play a large role in our analysis.

Definition 12. ([19]) An $n \times n$ Vandermonde matrix $V = [v_{ij}]$ has the form $v_{ij} = \alpha_i^{j-1}$ for scalars α_i. The α_i are sometimes called the nodes of the Vandermonde matrix.

Example 2. For $n = 3$, $\alpha_i = i$, the Vandermonde matrix of the α_i is

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix}.$$

We will use some well-known properties of the Vandermonde matrix throughout.

Proposition 4. *([19]) The determinant of a Vandermonde matrix V with nodes α_i is*

$$\det(V) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i).$$

It is clear from Definition 4 that the Vandermonde matrix is nonsingular if and only if the nodes are distinct.

While the Vandermonde matrix is often notoriously ill-conditioned even in the nonsingular case, it is possible to write down an analytic inverse.

Proposition 5. *([19]) Let the i, j entry of the inverse V^{-1} of a Vandermonde matrix V with nodes α_i be denoted v_{ij}. Then*

$$v_{ij} = (-1)^{i-1} \left(\frac{\displaystyle\sum_{\substack{1 \le m_1 < \ldots < m_{n-i} \le n \\ m_1, \ldots, m_{n-i} \ne j}} \alpha_{m_1} \cdots \alpha_{m_{n-i}}}{\displaystyle\prod_{\substack{1 \le k \le n \\ k \ne j}} (\alpha_k - \alpha_j)} \right), 1 \le i < n$$

We note that the canonical embedding of R as defined above is simply the Vandermonde matrix of the roots of the minimal polynomial.

Lemma 1. *For a ring $R = \mathbb{Z}[x]/m(x)$ with power basis $B = \{1, x, \ldots, x^{n-1}\}$, let ζ denote a root of the minimal polynomial $m(x)$. Then the matrix of the canonical embedding $\sigma(B)$ is the Vandermonde matrix with nodes $\alpha_i = \zeta^i, 0 \le 1 \le n-1$. We will denote it V_m, or simply V when the polynomial $m(x)$ is clear.*

Proof. Let $\sigma_j, 1 \le j \le n$, denote the jth complex embedding which maps ζ to a root of $m(x)$. By the first isomorphism theorem, the roots of $m(x)$ are $1, \zeta, \ldots, \zeta^{n-1}$ and thus $\sigma_j(\zeta) = \zeta^{j-1}$. Since the σ_j are ring homomorphisms, for ζ^i we have $\sigma_j(\zeta_i) = \zeta^{i(j-1)}$. Letting $\alpha_i = \zeta_i$ gives the definition of a Vandermonde matrix. □

Thus we can leverage the properties of Vandermonde matrices when analyzing this mapping between the canonical and coefficient embeddings.

Chapter 3

Previous Results and Our Contributions

3.1 Previous Results

We give a brief overview of previous results relating to the security of using non-cyclotomic base rings R for the non-dual form of the RLWE problem. The ideas presented here motivated our exploration of the roots of polynomials of the form $x^n + ax^m + b$ where $m < n$ are positive integers and $a, b \in \mathbb{R}$, and the singular value properties of their associated Vandermonde matrices, which appear in Chapters 4 and 5 below.

Throughout, we refer to the matrix Vandermonde matrix M (sometimes V) of an ideal $I \in \mathbb{R}[x]/m(x)$ as the Vandermonde matrix whose nodes are the roots of the minimal polynomial $m(x)$. For short, we may refer to this matrix as "the matrix of the polynomial."

In [16], the authors define the normalized spectral norm of a matrix M as

$$\mathcal{N}(M) = \|M\|_2 / |\det(M)|^{1/n},$$

and note $\mathcal{N}' := \mathcal{N}(M^{-1}) = \|M^{-1}\|_2 |\det(M)|^{1/n}$. They prove that where $\kappa(M)$ is the 2-norm condition number of M, we have

$$\mathcal{N}'(M) \leq 2\kappa(M).$$

Furthermore, the authors plot $\mathcal{N}'$ for $f = x^{32} + ax + b$ for $-60 \le a, b \le 60$ and conjecture based on this plot that most, though not all, of these f satisfy $\mathcal{N}' \le \sqrt{\max(a,b)}$. The authors do not give any heuristic motivation for which choices of coefficients the bound will or will not be satisfied. They do solve the non-dual search RLWE problem for the weak parameter choice of $f(x) = x^{128} + 524288x + 524285$, which satisfies a number of conditions laid out in the paper, including a requirement on the size of the spectral norm of M and a requirement on the modulus q used in RLWE.

The paper [9] extends the ideas expressed in [16]. The authors note that the roots of the polynomial $f(x) = x^{128} + 524288x + 524285$ roughly form a circle and that the singular values decrease roughly geometrically, but they make no attempt to generalize these observations. They provide a simple linear algebra attack on weak instances of RLWE which is independent on the modulus q and depends only on choice of Gaussian width relative to $s_n(M)$.

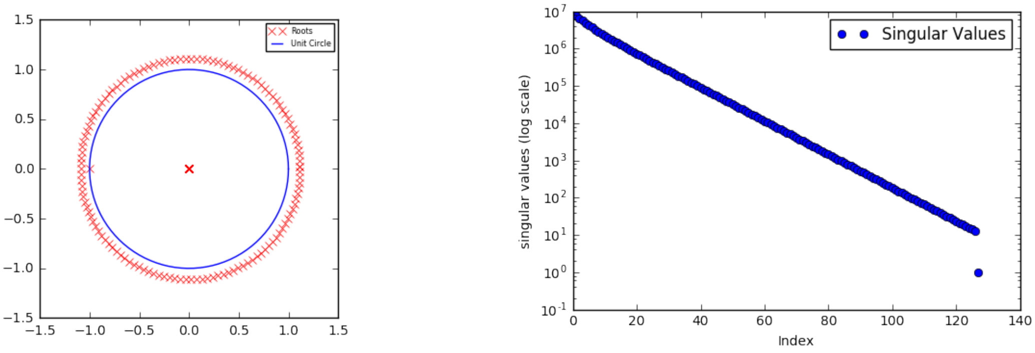


Figure 3.1: Behavior of $x^{128} + 524288x + 524285$ observed in [9].

In [26], the criterion for a successful linear algebra attack on the search version is simplified, showing that independent of singular values magnitude, it suffices only to have a row of M^{-1} that has a small Euclidean norm relative to the Gaussian width parameter.

In [17] the RLWE question is approached from a more number theoretic perspective. With the definition of spectral norm as above, the authors propose as an open problem finding possible values of $\rho(M)$ for M constructed as above, specifically whether possible values for ρ are on a continuum or discrete in regions of $\mathbb{R}$. They also recall that the definition of the Mahler measure $\mathcal{M}(f)$ of a polynomial $f(x) = a(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$ is given by

$$\mathcal{M}(f) = a \prod_{|\alpha_i| \geq 1} |\alpha_i|$$

and ask if there is a connection between small Mahler measure and small spectral norm, giving examples where this is the case. The authors also note that related quantities of M, such as condition number or the entire vector of singular values, could also be of interest.

Finally, [32] gives a tighter connection between hardness results for the RLWE problem and a polynomial LWE problem. As part of their argument, the authors prove the following, by bounding the roots of f using Rouche's Theorem and using the Frobenius norm.

Theorem 7. *([32], Theorem 4.7) Let* $P(x) = \sum_{1 \leq j \leq \rho \cdot n} p_j x^j$ *for complex* p_j*. Let* $g_{n,b} = x^n - b + P(x)$ *and let* V *be the Vandermonde matrix with the roots of* $g_{n,b}$ *as nodes. Denote the Frobenius norm of* V *by* $||V||_F$*. Then for any* $b > (||P||_1 \cdot C^{-1} e^{\rho})^{1/(1\rho)}$ *with* $C = |1 - \cos(a^{-1/n} - \frac{2e^{b^{1/n}}}{nb^{2/n}})|$*, we have*

$$||V||_F \leq bne$$

and

$$||V^{-1}||_F \leq n^{5/2}(||P||_1 + 1)b^{1/n}e^2.$$

While this result is exciting, covering a fairly general class of polynomials, it does not completely clear up the questions of spectral norm proposed in the previous papers. For instance, these estimates of $\|V\|_F$ and $\|V^{-1}\|_F$, which also gives upper bounds for the 2-norm by Proposition 1, are in practice much too large.

3.2 Our Contributions

Broadly, we sought to extend the attacks above to theorems based on more general classes of polynomials. Since the attacks above depend on properties of the polynomial's Vandermonde matrices, which in turn depend on the locations of the polynomial roots, our contributions span branches of analytic polynomial theory, matrix theory, and combinatorics.

We began with an analysis of polynomials of the form $x^n + ax + b$ for $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{R}$.

Our contributions include empirical observations regarding their root locations and a new conjecture about the magnitude of singular values of the associated Vandermonde matrices. We provide a proof of the number of roots with modulus less than 1 when $a = b = 1$ and make significant progress on the proof for the $a, b \neq 1$ case. These results appear in Chapter 4.

Then, we broadened our analysis to polynomials of the more general form $x^n + ax^m + b$ for $a, b \in \mathbb{R}$ and $m < n$. Here we extend the empirical observations with regards to root locations and singular value properties to the more general case. We contribute numerical evidence that these bounds are in practice quite tight. We also provide proofs regarding the number of real roots of these polynomials and prove that they always have at least one root of modulus less than 1. These results appear in Chapter 5.

We provide our most exciting results in Chapter 6. While seeking to generalize a root localization theorem of Chapter 4, we came across an interesting and open combinatorics question regarding the determinant of a certain type of tridiagonal matrix. We proved bijections between 5 classes of combinatorial objects, the overwhelming majority of which were previously unknown in the literature. In doing so, we greatly expanded the current research regarding a certain class of generalized Fibonacci number. We also give the first generating function for this class of Fibonacci number, and prove three new identities on these k-Fibonacci numbers which we use as lemmas to obtain the generating function. Both the generating function question and at least two of the bijections were specifically posed as open combinatorial questions in [14].

Lastly, we briefly explored the Mahler measure question proposed in [17] for Salem and Pisot numbers. Our results indicate that contrary to the conjecture of [17], Mahler measure by itself is *not* sufficient to determine spectral norm. In addition, our approaches in this section, such as leveraging properties of the Vandermonde matrix and our use of the Eckart-Young theorem, could be generalized to other polynomials with known roots, including those of the form $x^n + ax^m + b$ given more information about their root locations. This work is presented in Chapter 7.

Chapter 4

The First Polynomial: $x^n + ax + b$

4.1 Motivation

The polynomials considered in [16] and [9] are of the form $x^n + ax + b$, for a positive integer n and $a, b \in \mathbb{R}$. Initially, we look at properties of the roots for the $a = b = 1$ case, and explore the generalization at the end of the chapter.

In addition, there is cryptographic interest in polynomials of this form besides their use in RLWE. In [8], researchers proposed a new class of polynomials for base ring defined in the cryptosystem NTRU, noting that the polynomials

$$x^p - x - 1$$

for p a prime integer satisfy desired irreducibility requirements and are more secure against certain classes of attacks. While we do not know if a detailed analysis of the roots would be of any use in analyzing the security of NTRU prime, the cryptographic interest in these polynomials motivates further exploration.

The analysis in [32] also motivates the spectral analysis of these polynomials with the following result:

Theorem 8 ([32], Appendix C)**.** *Let V be the Vandermonde matrix of $x^n \pm x \pm 1$. Then for every $n > 2$,*

$$\|V\|_F \leq 2n$$

and

$$\|V^{-1}\| \leq 6n^{7/2}.$$

Since the Frobenius norm bounds the 2-norm, the first part of Theorem 8 gives an upper bound on the largest singular value of V (and, trivially, the entire spectrum). However, we noticed that this bound is in practice much too loose. The bound increases linearly in n, and the maximum singular value increases sublinearly in n. See Figure 4.1 for an illustration.

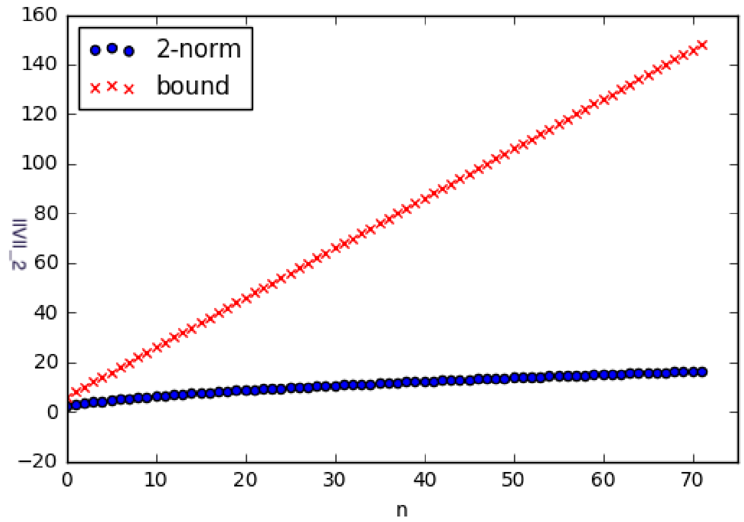
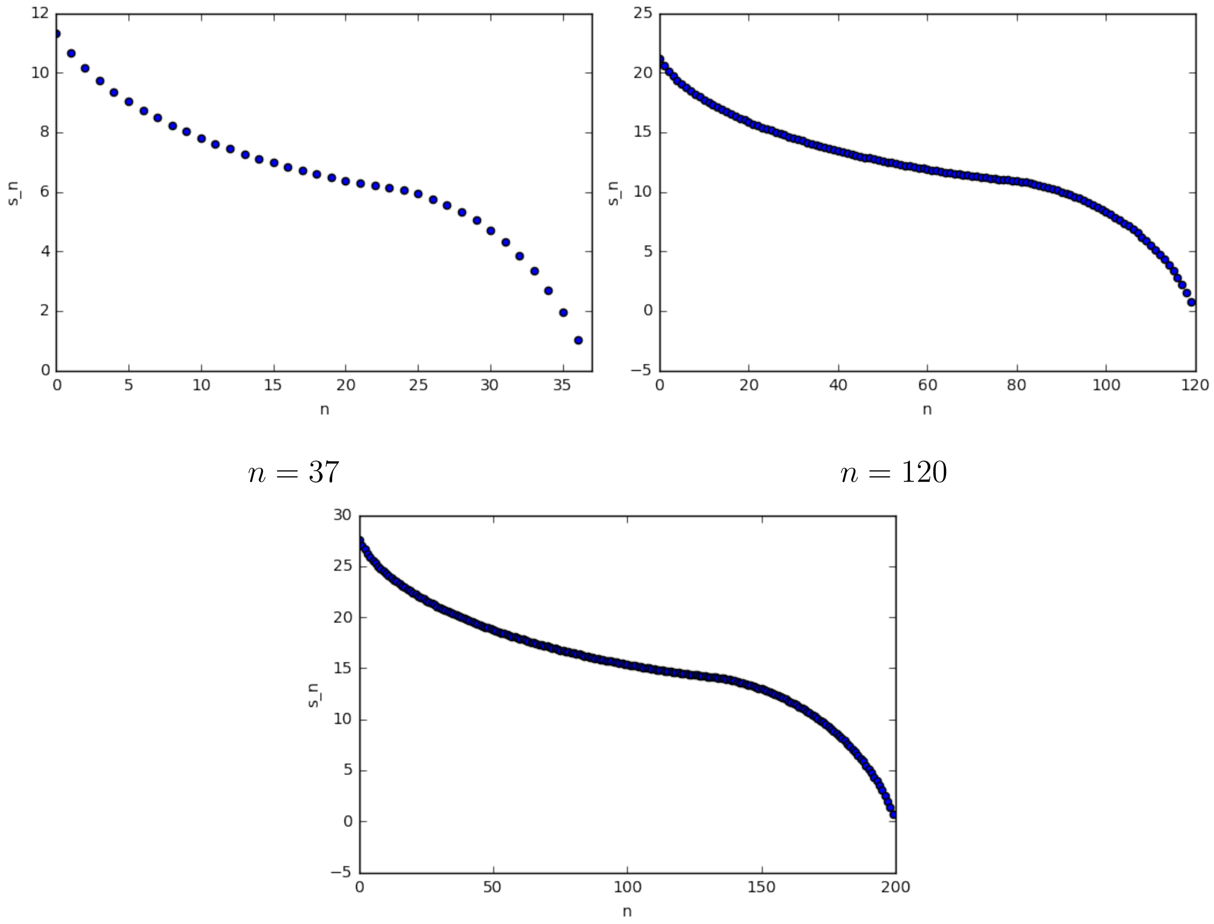


Figure 4.1: An illustration of the 2-norm bound of [32] as polynomial degree increases.

In addition to providing a loose bound for the maximum singular value, Theorem 8 does not give us any useful information about the rest of the spectrum of V. In fact, the behavior of the entire spectrum is intriguing.



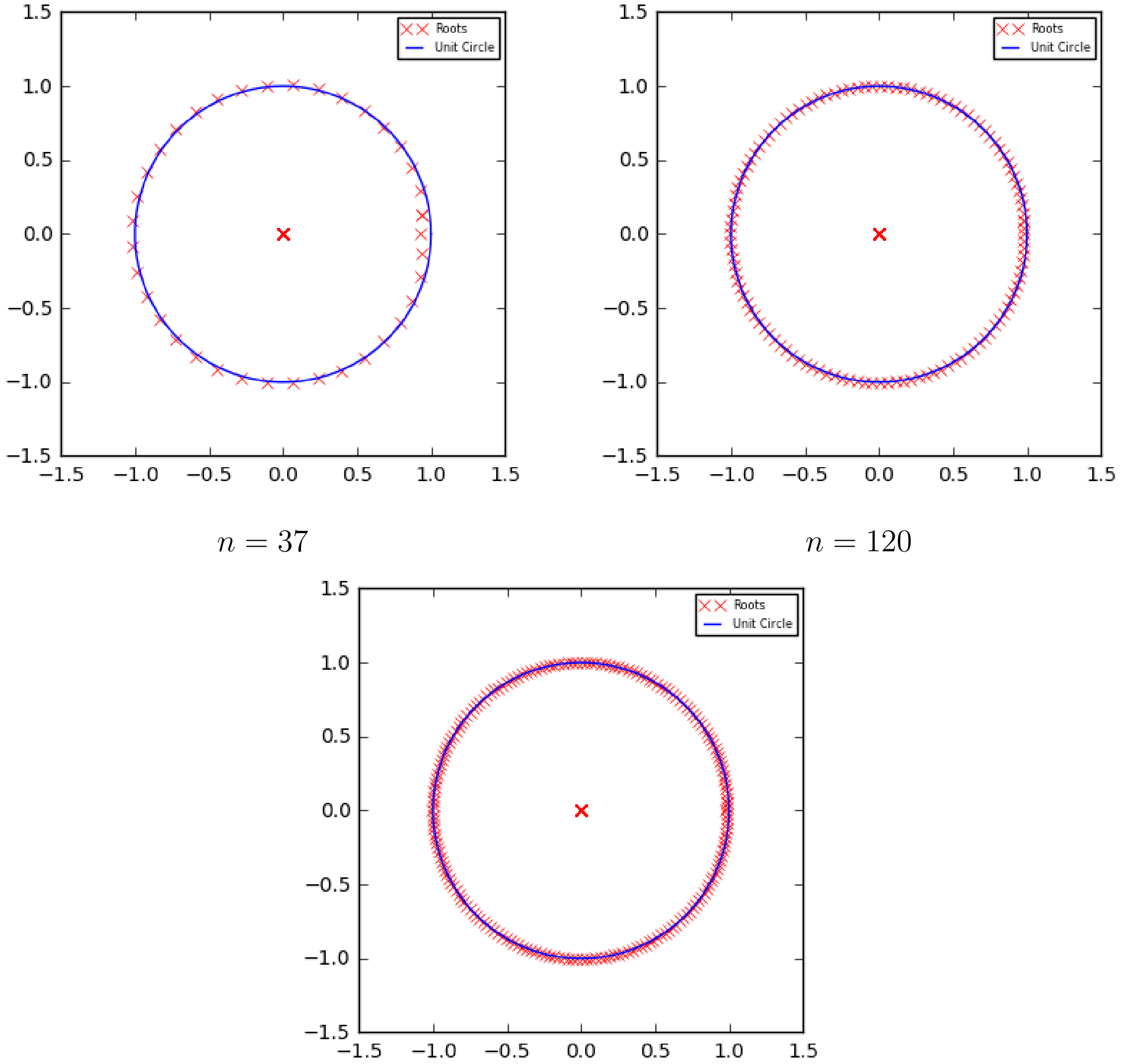
$n = 37$

$n = 120$

$n = 200$

Figure 4.2: Singular values for various choices of n

In all of these examples, an inflection point occurs around index $2\lfloor n/3 \rfloor$. This state of affairs becomes even more curious when we compare the singular value plots to the plots of the roots of the polynomials.



$n = 37$

$n = 120$

$n = 200$

Figure 4.3: Polynomial roots of various choices of n

While it it is hard to tell from the plots for larger n, computations indicate that roughly $\lfloor n/3 \rfloor$ of the roots of the polynomials tested lie inside the unit circle.

Given that the the roots of the polynomial and their powers form the nodes of the Vandermonde matrices, it is perhaps not surprising that there is a connection between the root and matrix properties. However, it was not immediately apparent to us why this connection should be so strong or so pervasive. Thus, in an effort to learn more about the Vandermonde matrix properties of this polynomial, we first investigate the root properties of these polynomials.

4.2 Root Locations

We start by identifying the locations of the roots of $x^n \pm x \pm 1$, and we will show that polynomials of this form do in fact have roughly $\lfloor n/3 \rfloor$ of their roots inside the unit circle. Our approach to the proof is to convert the root finding problem to a matrix problem using the Schur-Cohn Theorem. First recall some basic definitions.

Definition 13 ([22])**.** The inertia of a real-symmetric matrix A is defined as the triple

$$(n_+, n_-, n_0)$$

where n_+, n_-, n_0 are respectively the number of positive, negative, and zero eigenvalues of A.

A symmetric matrix has no complex eigenvalues and thus positive and negative eigenvalues are well-defined.

Definition 14 ([27])**.** The *signature* of A, denoted $\mathrm{sig}(A)$, is $n_+ - n_-$ and the *rank* of A is $n_+ + n_-$.

Definition 15 ([27])**.** A real quadratic form in n real variables $x_1, \ldots, x_n$ is defined by

$$Q(\boldsymbol{x}) := \boldsymbol{x}^T A \boldsymbol{x} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j$$

where $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ is a real symmetric matrix.

The following is the main theorem we will use to analyze the locations of polynomial roots.

Theorem 9 (Schur-Cohn; see [27])**.** *Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial of degree n. Suppose that $f(x)$ and $f^*(x) := f(\frac{1}{x})$ have no common zero, and denote by $sig(f)$ the* *signature of the quadratic form $C = B^T B - A^T A$ where*

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ & a_0 & \dots & a_{n-2} \\ & & \ddots & \vdots \\ & & & a_0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} \bar{a}_n & \bar{a}_{n-1} & \dots & \bar{a}_1 \\ & \bar{a}_n & \dots & \bar{a}_2 \\ & & \ddots & \vdots \\ & & & \bar{a}_n \end{bmatrix}.$$

Then f has exactly $\frac{n+sig(f)}{2}$ zeros inside the unit circle, $\frac{n-sig(f)}{2}$ zeros outside the unit circle, and no zeros on it.

Note that Schur-Cohn in its full generality holds for polynomials with complex coefficients, in which case C is a Hermitian form. As the coefficients of our polynomials are real, we only need the version as stated in Theorem 9.

For $f(x) = x^n - x - 1$, we construct the Schur-Cohn matrix C as in Theorem 9.

Proposition 6. *Let $f(x) = x^n - x - 1$. Then the Hermitian form C as in Theorem 9 is*

$$C = \begin{bmatrix} 0 & -1 & 0 & 0 & \dots & -1 \\ -1 & -1 & -1 & 0 & \dots & 0 \\ 0 & -1 & -1 & -1 & \dots & 0 \\ \vdots & & & & \ddots & -1 \\ -1 & 0 & \dots & 0 & -1 & 0 \end{bmatrix}.$$

Proof. Immediate from Theorem 9. □

Now, to determine how many roots of $f(x)$ are inside the unit circle, we must find the signature of C. If the leading minors of C are all nonzero, we could use the following Theorem 10 to do this.

Theorem 10 (Jacobi; see [27])**.** *Let A be a symmetric matrix of rank m. Suppose that the principal minors $D_1, \dots, D_m$ of A are all different from zero. Then the quadratic form $Q(\boldsymbol{x}) := \boldsymbol{x}^T A \boldsymbol{x}$ has signature $sig(Q) = m - 2V(1, D_1, \dots, D_m)$.*

At first, it seems we cannot use Theorem 10, as the Schur-Cohn matrix C corresponding to the quadratic form has some 0 minors; for instance, the leading 4×4 minor in the $a_0 = a_1 = -1$ case is always zero. Luckily for us, there is a generalization of Theorem 10 that dates back to 1881 and allows zero minors as long as leading minor sequence does not include more than two zeros as successive entries. In the subsequent application of the theorem, a 0 can be counted as an entry of either sign. See [27].

Thus we only need to calculate the sign changes in the leading minor sequence to determine the signature of the quadratic form.

We take a combinatorial approach, for reasons that will soon become clear.

First, recall the definition of a leading matrix minor.

Definition 16. Let M_k be the kth leading minor of a matrix A, that is, the submatrix formed from the $k \times k$ elements in the upper left corner, for $1 \leq k \leq n-1$. Then

$$M_k = \sum_{\pi \in S_k} \left(sign(\pi) \prod_{i=1}^{k} a_{i\pi_i} \right)$$

where S_k is the set of all permutations on the set $\{1, 2, \ldots, k\}$ and $sign(\pi) = 1$ if π is even and -1 if π is odd.

Due to the nearly-tridiagonal structure of the Schur-Cohn matrix C, calculating the leading minor sequence is equivalent to solving a restricted permutation problem. As it turns out, this particular permutation problem has a very nice combinatorial solution.

Proposition 7. *All elements in the sum of Definition 16 for a given k are zero, except for possibly permutations π on k elements $1, \ldots, k$ such that $|\pi(i) - i| \leq 1$ for all $1 \leq i \leq n-1$.*

Proof. All entries a_{ij} of C are zero, unless $j = i \pm 1$. Thus for a given $\pi \in S_k$, we must have $\sigma_i = 1 \pm i$ or $\sigma_i = i$ for all i with $1 \leq i \leq n-1$ for any nonzero term in the sum M_k. □

Thus we begin by counting permutations of the possibly-nonzero form. The result is a familiar integer.

Throughout, let $|\pi_k|$ denote the total number of permutations of the form of Proposition 7.

Proposition 8. *There are f_{k-1} permutations of the form in Proposition 7, where f_{k-1} is the kth Fibonacci number.*

Proof. Let π_k be a length k permutation of the desired form.

First, we must have $\pi_k(1) = 2$ for any k, since $\pi_k(i) - i$ must be true and since $\pi_k(1) = 1$ gives a zero term as $a_{1,1}$ is 0. Similarly, we must have $\pi_k(2) = 1$. Thus $|\pi_1| = |\pi_k(2)| = 1$.

Now consider $\pi_i, i \geq 3$. We must have $\pi_i(i) = i$ or $\pi_i(i) = i-1$. If $\pi_i(i) = i$, then the first $i-1$ elements of π satisfy the $|\pi_k(i) - i| \leq 1$ condition, and so there are $|\pi_{i-1}|$ elements of π_i with $\pi_i(i) = i$. Similarly, if $\pi_i(i) = i-1$, then $\pi_i(i-1) = 1$, and considering only the first $i-2$ elements, by the same logic, gives $|\pi_{i-2}|$ elements of this form.

Thus, $|\pi_k| = |\pi_{k-1}| + |\pi_{k-2}|$ for any $3 \leq k \leq n-1$.

Recall that the Fibonacci numbers are defined recursively by

$$f_0 = 0, f_1 = 1, f_n = f_{n-1} + f_{n-2}.$$

As the recursion on π_i is identical with the same initial conditions, we obtain that the number of $\pi(k) = f_{k-1}$. The length-1 shift occurs because of the +1 shift in indexing for the initial conditions.

□

We have now calculated the ith leading minor of C but discarded the signs in the definition of a determinant (see Definition 7). In the matrix theory literature, this is known as the permanent of a matrix. We remark that it is known that the permanent of a tridiagonal matrix of all 1's is a Fibonacci number; the usual proof is through the definition of a matrix continuant. We present the combinatorial argument above because the typical definition of a matrix continuant does not hold when the off-diagonal elements are not the sub and super diagonals. Our combinatorial argument will generalize to the more complicated cases in Chapter 6 below, while the traditional matrix continuant argument does not.

To find the M_k themselves now that we know the number of terms in the expansion, we need to find the sign each of those terms. Recall that the sign of a permutation π is 1 if π has an even number of transpositions, and -1 if π has an odd number of transpositions. The recursive argument about makes it quite easy to count these transpositions.

Theorem 11. *Define two interlacing recursive sequences t and u with initial conditions $t_0 = t_1 = 0$, $u_0 = 0, u_1 = 1$, and $t_k = t_{k-1} + u_{k-2}$ and $u_k = u_{k-1} + t_{k-2}$. Then there are t_k permutations on π_k with an even number of transpositions and u_k permutations on π_k with an odd number of transpositions.*

Proof. Recall the recursive argument given above. Then the $|\pi_{k-1}|$ terms of π_k have the same number of descents; the terms of π_k constructed from π_{k-2} will have one more descent than the original π_{k-2} by construction. Recalling the initial conditions $\pi_1 = 2$ (one permutation, and no permutations with either an even nor odd number of transpositions) and $\pi_2 = 21$ (one permutation with an odd number of transpositions, no permutations with even number of descents) concludes the argument. □

This theorem naturally partitions the Fibonacci numbers into the sum of two sequences.

Corollary 1. *$F_n = t_n + u_n$, with F_n the nth Fibonacci number and t_n, u_n defined as in Theorem 11.*

The difference between t_k and u_k, and thus the calculation of the minors of C, is predictable.

Lemma 2. *Let $v_k = t_k - u_k$ be the sequences of differences of the entries of the sequences a, b. Then*

$$v_k = \begin{cases} -1, k \equiv 2,3 \mod 6 \\ 0, k \equiv 1,4 \mod 6 \\ 1, k \equiv 5,6 \mod 6 \end{cases}$$

Proof. First, from the initial conditions we have that $v_1 = t_1 - u_1 = 0 - 0 = 0$ and $v_2 = t_2 - u_2 = 0 - 1 = -1$. Now, by the recursive definition of t, u, we have that for $k \geq 3$,

$$\begin{aligned} v_k = t_k - u_k &= t_{k-1} + u_{k-2} - (u_{k-1} + t_{k-2}) \\ &= t_{k-1} - u_{k-1} - (t_{k-2} - u_{k-2}) \\ &= v_{k-1} - v_{k-2}. \end{aligned}$$

From here, we note

$$\begin{aligned}v_{k+3} &= v_{k+2} - v_{k+1}\\ &= v_{k+1} - v_k - v_{k+1}\\ &= -v_k\end{aligned}$$

and thus $v_{k+6} = v_k$. Noting that $v_3 = -1$ from the initial conditions concludes the proof. □

While v_k does not quite count the minor sequence of C, it is quite close.

Lemma 3. *Where M_k, $1 \leq k \leq n-1$, is the kth leading minor of C,*

$$M_k = \begin{cases} 1, k \equiv 0 \mod 3 \\ 0, k \equiv 1 \mod 3 \\ -1, k \equiv 2 \mod 3 \end{cases}.$$

Proof. The proof is simply Lemma 2 combined with our knowledge of C. Since $c_{ij} = 1$ for all the entries of C we are considering, the terms in the product in Definition 16 will contribute a coefficient of 1 if the permutation has even length and -1 if the permutation has odd length. Thus we switch the sign of v_k in Lemma 2 for odd k only which yields the result. □

If the polynomial coefficients $a = b = 1$, we do not switch the signs for odd k, since all $c_{ij} = 1$.

We have now determined M_k for all $1 \leq k \leq n-1$. Calculating the determinant of C is our last lemma.

Lemma 4. *Let C be the Schur-Cohn matrix for $x^n - x - 1$. Then*

$$\det(C) = \begin{cases} -1, n = 0 \mod 3 \\ -1, n = 1 \mod 3 \\ -4, n = 2 \mod 3 \end{cases}.$$

Proof. Throughout, let $\pi = \pi_n$ for clarity. We follow the same permutation argument as above, with the difference is the additional possibilities of $\pi(1) = n$ with the addition of the last row and $\pi(n) = 1$ or $\pi(n) = n - 1$ with the addition of the last column. We also have $\pi(n-1) = n$ case, as before. We consider four cases.

1. If $\pi(1) = 2$ and $\pi(n) = n - 1$, then we must have $\pi(2) = 1$. We can pick entries from all other middle columns in the usual $|\pi(n-3)| = F_{n-4}$ ways.

2. If $\pi(1) = 2$ and $\pi(n) = 1$, then we must have $\pi(n-1) = n$. However, this in turn forces $\pi(n-2) = n-1$, and so on. Thus there is only one permutation in this case.

3. If $\pi(1) = n$ and $\pi(n) = n - 1$, the argument is similar to case 2. We must have $\pi(2) = 1$, which sets $\pi(3) = 2$, and so on til $\pi(n-1) = n - 2$. Thus there is only one permutation in this case as well.

4. If $\pi(1) = n$ and $\pi(n) = 1$, we have to order only the middle elements. This is like case 1, but without the restriction that $\pi(2) = 1$. Thus, there are F_{n-3} permutations here.

So consider the signs of each of these permutations. In case 1, the parity is the same as was determined in Lemma 3. However, in cases 2 through 4 the number of descents does *not* necessarily determine the parity of the permutation; luckily we know enough about the structure of the permutations to determine them by hand.

In case 2, all the elements are in fixed point order, with the exception of the 1 in the nth position. Thus it will take $n-1$ transpositions to order the permutation to $\pi(i) = i$. Thus the case 2 permutation has sign -1^{n-1}. If n is even, $(-1)^{n-1} = -1$, and there is no sign change from the even number of $a_{i,j}$ in the minor expansion, so the term is -1. If n is odd, $(-1)^{n-1} = 1$, but there is a change from the odd number of $a_{i,j} = -1$ in the minor expansion, so the term is still -1. Thus case 2 contributes a -1 to the determinant regardless of the parity of n.

In case 3, the argument is the same as case 2, except the $n-1$ transpositions come from swapping the n in position 1 back to position n. Thus this term always contributes a -1 as well.

In case 4, we need to reorder the middle $n-2$ elements, which follows the Lemma 3 pattern. Then we must consider the number of transpositions from the $\pi(1)$ and $\pi(n)$ elements. As again every element is bigger than $\pi(p)n$, that gives $n-1$ transpositions; since $\pi(1)$ is bigger than all other elements, that is an additional $n-2$ transpositions (we are avoiding double counting $\pi(1) > \pi(n)$). Thus there is an additional $2n-3$ inversions, which is always odd regardless of n.

Thus case 4 is a flipped sign from case 1, with an index-1 offset in the mod since there are c_{n-1} and not c_n transpositions in the middle. Adding, the case-4 coefficient is thus

$$\begin{cases} -1, n \equiv 2 \mod 3 \\ 0, n \equiv 0 \mod 3 \\ 1, n \equiv 1 \mod 3 \end{cases}.$$

Now, we put it all together. Let $n \equiv 0 \mod 3$. Then,

$$\det(C) = 1 - 2 + 0 = -1.$$

Let $n \equiv 1 \mod 3$. Then,

$$\det(C) = 0 - 2 + 1 = -1.$$

Let $n \equiv 2 \mod 3$. Then,

$$\det(C) = -1 - 2 - 1 = -4.$$

□

The determinant calculation yields an important corollary.

Corollary 2. *Rank*$(C) = n$.

Proof. As per Lemma 4, $\det(C) \neq 0$ regardless of the modularity of n. □

This corollary proves that we can in fact use Theorem 9 to count the roots inside the unit circle, since $f(x)$ and $f^*(x)$ have no common roots.

We are now ready to count the sign changes in the minor sequence and thus the number of roots inside the unit circle.

Lemma 5. *Let $V(S)$ be the number of sign changes in a sequence S, where 0 can be counted as either positive or negative. Let $S = 1, M_1, \ldots, M_n$. Then*

$$V(S) = \begin{cases} \frac{2n}{3} - 1, \ n \equiv 0 \mod 3 \\ \frac{2(n-1)}{3} + 1, \ n \equiv 1 \mod 3 \\ \frac{2(n+1)}{3} - 1, \ n \equiv 2 \mod 3 \end{cases}.$$

Proof. As established above, the minor sequence repeats $1, 0, -1, 1, 0, -1 \ldots$ starting at index $k = 0$, with variation in the m_n coordinate. If there are r elements organized into blocks of $1, 0, -1$, there are $\frac{2r}{3} - 1$ sign changes–$r/3$ to account for the r switches from 1 to -1 within each block and $r/3 - 1$ to account for the -1 to 1 switch between the blocks.

If $n = 0 \mod 3$, then we have $n/3$ full blocks, with one more -1 on the end. As the M_n coordinate for the determinant is negative, there is no switch between $M_{n-1} = -1$ and $M_n = -1$, and this observation yields case 1 directly.

If $n = 1 \mod 3$, there are $n - 1$ complete blocks, and then $M_{n-1} = 1$ and $M_n = -1$. This yields an extra 2 sign changes after the full blocks and thus the result.

If $n = 2 \mod 3$, we have $(n - 2)/3$ full blocks, and then $M_{n-2} = 1, M_{n-1} = 0, M_n = -4$. The sign changes are identical to that of $(n+1)/3$ full blocks and counting them as such yields the result. □

The main result is an easy corollary.

Theorem 12. *Let $f(x) = x^n - x - 1$, $n > 1$. Let zer(f) be the number of zeros of f inside the unit circle. Then*

$$zer(f) = \begin{cases} \frac{n}{3} + 1, & n \equiv 0 \mod 3 \\ \left\lceil \frac{n}{3} \right\rceil + 1, & n \equiv 1 \mod 3 \\ \left\lceil \frac{n}{3} \right\rceil, & n \equiv 2 \mod 3 \end{cases}.$$

Proof. From Theorem 10, the signature $\mathrm{sig}(f)$ of the Hermitian form associated with f is $n - 2V(S)$ where S is the minor sequence, and by Theorem 9, the number of roots inside the unit circle is $(n + \mathrm{sig}(f))/2 = (n + n + \mathrm{sig}(f))/2 = n - V(S)$.

If $n \equiv 0 \mod 3$, then

$$n - V(S) = n - \frac{2n}{3} + 1 = \frac{n}{3} + 1.$$

If $n \equiv 1 \mod 3$, then

$$n - V(S) = n - \frac{2(n-1)}{3} + 1 = \frac{n}{3} + \frac{5}{3} = \left\lceil \frac{n}{3} \right\rceil + 1.$$

If $n \equiv 2 \mod 3$, then

$$n - V(S) = n - \frac{2(n+1)}{3} + 1 = \frac{n+1}{3} = \left\lceil \frac{n}{3} \right\rceil .$$

□

As a sanity check, we successfully verified Theorem 12 in Sage for the roots of all polynomials $x^n - x - 1$, $3 \leq n \leq 100$.

4.3 When $a, b \neq 1$

Now, we explore what happens when a, b are not necessarily 1. This analysis depends on the previous case, but also requires the additional knowledge of where the fixed points of the permutations lie. We obtain an expression for the leading minors in a and b, although determining the sign changes is not as clear as the previous section, and we are not able to conclude much as far as root locations. However, the work in this section paves the way for both further exploration of the root locations, as well as providing motivation for the combinatorial results of Chapter 6.

We begin by constructing the Schur-Cohn matrix C for this new class of polynomials.

Proposition 9. *Let $p(x) = x^n - ax - b$. Then $p(x)$ has exactly $n - V(1, C_1, \ldots, C_n)$ zeros inside the unit circle where*

$$C = \begin{bmatrix} 1-b^2 & -ab & 0 & 0 & \ldots & -a \\ -ab & 1-a^2-b^2 & -ab & 0 & \ldots & 0 \\ 0 & -ab & -1-a^2-b^2 & -ab & \ddots & 0 \\ \vdots & \vdots & -ab & \ddots & \ddots & 0 \\ 0 & \vdots & \vdots & \ddots & \ddots & -ab \\ -a & 0 & \ldots & 0 & -ab & 1-b^2 \end{bmatrix}.$$

Proof. Immediate from Schur-Cohn: let

$$A = \begin{bmatrix} -b & -a & 0 & \dots & 0 \\ 0 & -b & -a & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & -a \\ 0 & 0 & \dots & 0 & -b \end{bmatrix}$$

and

$$B = \begin{bmatrix} 1 & 0 & 0 & \dots & -a \\ 0 & 1 & \ddots & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

and construct the quadratic form. □

To find the number of zeros inside the unit circle, we need to construct the leading minor sequence. This differs from the $x^n - x - 1$ case in that now we need to separately count the number of diagonal elements in the matrix; that is, the number of fixed points in the restricted permutation class.

We motivate the investigation of the fixed points by the leading minor definition and the structure of C. Since the diagonal elements of C are different from the sub and super diagonals, and since we will get a contribution of a diagonal element whenever we have a permutation σ such that $a_{i\sigma(i)} = a_{ii}$ in the minor definition, we need to be able to count how many fixed points there are in each restricted permutation of length 1 to $n-1$.

For this class of restricted permutation, such a calculation is not difficult.

Proposition 10. *The total number of fixed points in a length n permutation π with $|\pi(i) - i| \leq 1$ is*

$$\sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}(n-2i).$$

For some given i, there are

$$\sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}$$

total permutations with i fixed points.

Proof. See Chapter 6. □

With this additional knowledge, we can write down an expression for the minors using techniques similar to those of the previous chapter.

Proposition 11. *Let C_i be the ith leading minor of C, $1 \leq i \leq n-1$. Then*

$$C_i = (1-b^2) \sum_{i=0}^{\lceil n/2 \rceil} (-1)^{n+i} \binom{n-1-i}{i} (1-a^2-b^2)^{n-2i-1}(ab)^{2i} + \sum_{i=0}^{\lfloor n/2 \rfloor} (-1)^{n+i} \binom{n-2-i}{i} (1-a^2-b^2)^{n-2i}(ab)^{2i}.$$

Proof. If $\pi(1) = 1$ or $\pi(n) = n$, this contributes a $1-b^2$ term to the minor. We can disregard the $\pi(n) = n$ case, since we only need permutations up to length $n-1$ for the minors we are considering here. For all other fixed points, each permutation with i fixed points contributes a $(1-a^2-b^2)^{n-2i}(ab)^{2i}$ term. So, calculating the minor consists of finding the number of permutations with i fixed points and their signs.

By Proposition 10, there are $\sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}$ permutations with i fixed points. With $t_i = \binom{n-2-i}{i}$ and $u_i = \binom{n-1-i}{i}$ denoting the partition into even and odd permutations as in the $a = b = 1$ case in Lemma 2, there are t_i permutations of length n with $\pi(1) = 1$ and u_i permutations of length n with $\pi(1) = 2$. Each of the $\pi(1) = 1$ permutations has sign $(-1)^{n+i}$ since there is a -1 for each swap and for each term in the permutation; similarly each of the $\pi(1) = 2$ permutations has sign $(-1)^{n+i+1}$, accounting for the initial 21 swap.

Putting it all together, we obtain

$$C_i = (1-b^2) \sum_{i=0}^{\lceil n/2 \rceil} (-1)^{n+i} \binom{n-1-i}{i} (1-a^2-b^2)^{n-2i-1}(ab)^{2i} + \sum_{i=0}^{\lfloor n/2 \rfloor} (-1)^{n+i} \binom{n-2-i}{i} (1-a^2-b^2)^{n-2i}(ab)^{2i}.$$

□

Corollary 3. *The $x^n + ax + b$ case is identical to the $x^n - ax - b$ case from Proposition 9.*

Proof. The only difference in the Schur-Cohn matrix C occurs in the upper right and lower left corners, which does not matter for any minor smaller than the full determinant. □

Remark 1. Letting $a, b = \pm 1$ recovers the case from the previous section.

To prove the number of roots inside the unit circle for $x^n - ax - b$, we would have to count the number of sign changes in the sequence $1, M_1, \ldots, M_n$ for M_n as above. We leave the completion of the proof to future work.

Chapter 5

Generalizing: $x^n + ax^m + b$

Next, we generalize the Chapter 4 analysis of root and singular value properties of the matrix V; we now consider polynomials of the form $f(x) = x^n + ax^m + b$, with $a, b \in \mathbb{R}$ and for integers n, m with $2 \leq m \leq n$. While most of the observations in this chapter are empirical, they do advance the existing literature. In addition, our application of the Cauchy bound to these polynomials is also novel and results in an apparently tighter bound for this class of polynomials than previously known. Furthermore, generalizing the Schur-Cohn approach from the previous chapter naturally leads to fascinating questions in enumerative combinatorics, which we ultimately answer in Chapter 6.

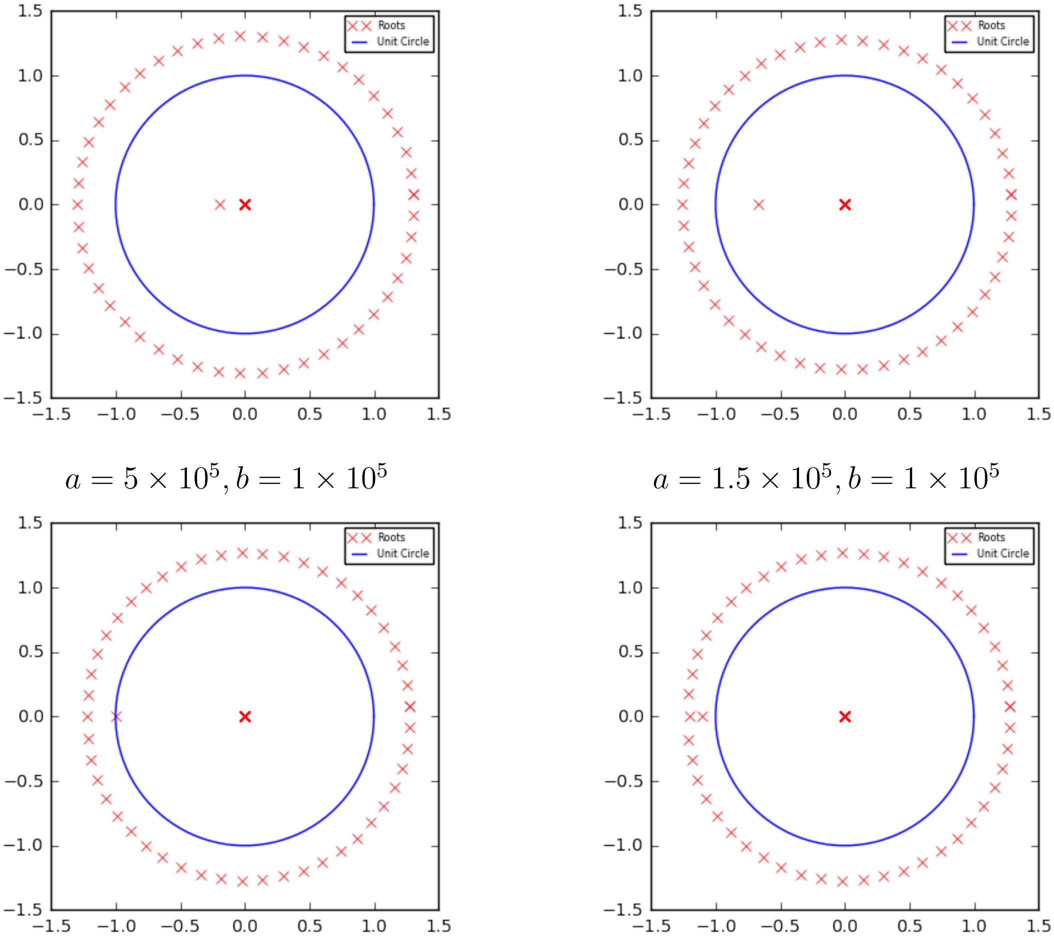
In this chapter, we observe the behavior of the roots in the complex plane for our class of polynomials, and we prove some root properties for the $m = 1$ and $a, b \neq 1$ case.

For the class of polynomials of the form $f(x) = x^n + ax^m + b$, the behavior of the polynomial roots seems to be determined entirely by the (relative) magnitudes of the coefficients a and b and the degrees n, m. Furthermore, properties of V_f are in turn determined by the roots of f. We show below that we can calculate a bound on the spectral distortion of V_f above knowing only the 4 parameters a, b, m, n. Moreover, we provide empirical evidence that the bounds we propose are extremely tight in practice.

5.1 Empirical Observations

To motivate analysis of the root behavior below, we first show trends we observed computationally for the location of the roots of f in terms of the degree and the coefficients.

We begin by fixing $m = 1$. First, observe that the roots of f fall roughly on a circle. f appears to have one real root, and the behavior of that real root is controlled by the relative magnitudes of a and b. To see this, we fix $n = 50$ and vary a and b; the results are show in Figure 5.11. The unit circle is shown in blue.



$a = 5 \times 10^5, b = 1 \times 10^5$

$a = 1.5 \times 10^5, b = 1 \times 10^5$

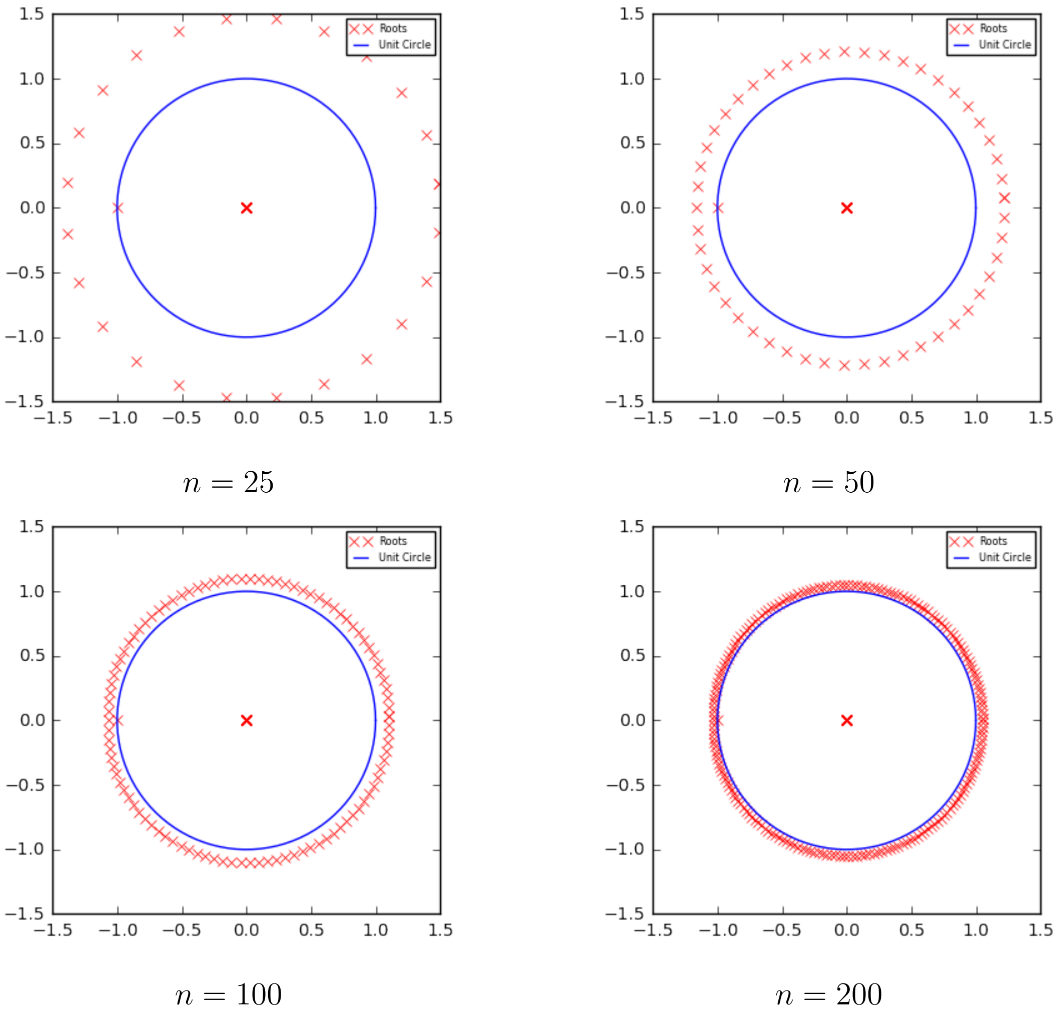
$a = b = 1 \times 10^5$

$a = 1 \times 10^5, b = 1.1 \times 10^5$

Figure 5.1: Root plots for $n = 50$ and various choices of a and b.

Thus taking $a > b$ seems to give a root of modulus less than 1, $a = b$ gives a root of modulus about 1, and $b > a$ gives a root of modulus greater than 1.

The modulus of the outer ring of roots appears to be controlled by n and, to a lesser extent, the magnitudes of a and b. Fixing $a = b = 1000$ and varying n gives Figure 5.12.



$n = 25$

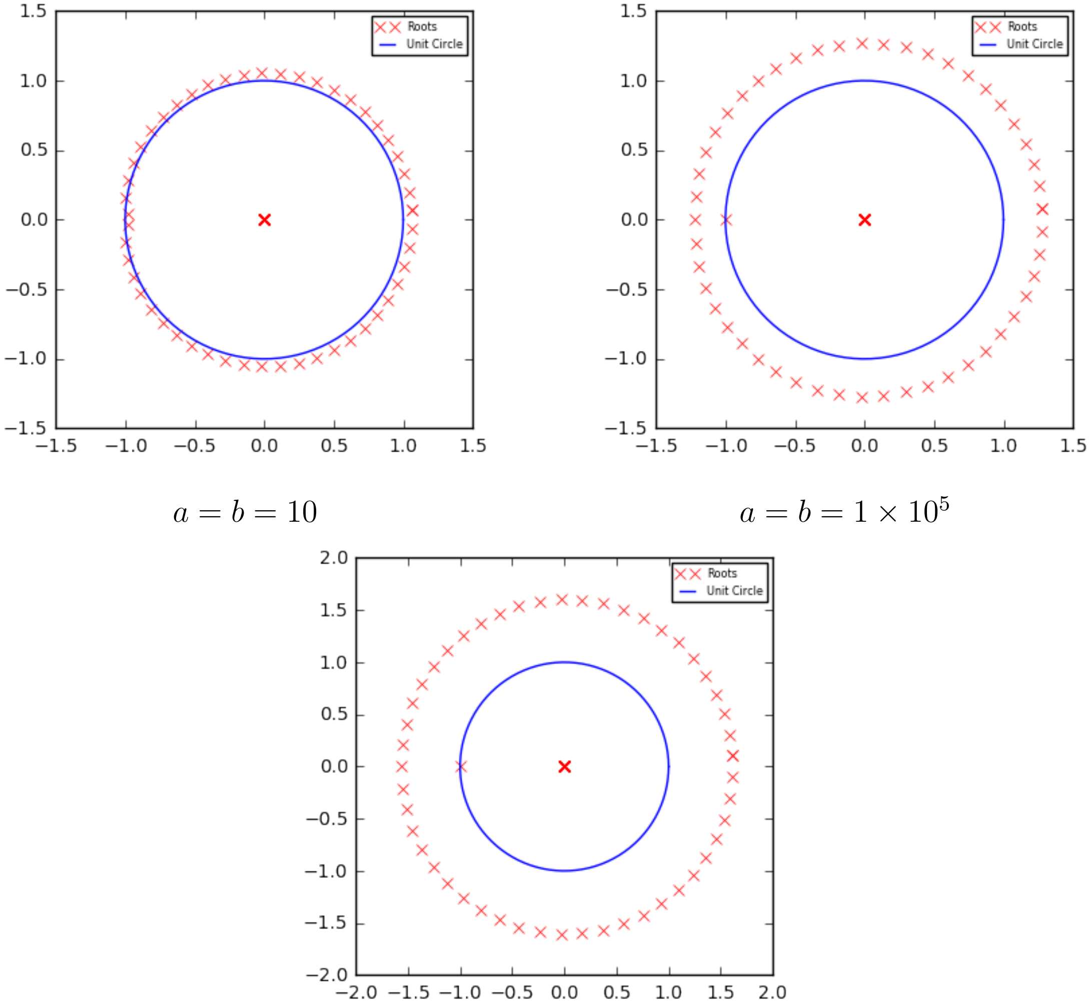
$n = 50$

$n = 100$

$n = 200$

Figure 5.2: Root plots for $a = b = 1000$ and various n.

Furthermore, fixing $n = 50$ and varying $a = b$ gives Figure 5.13.



$a = b = 10$

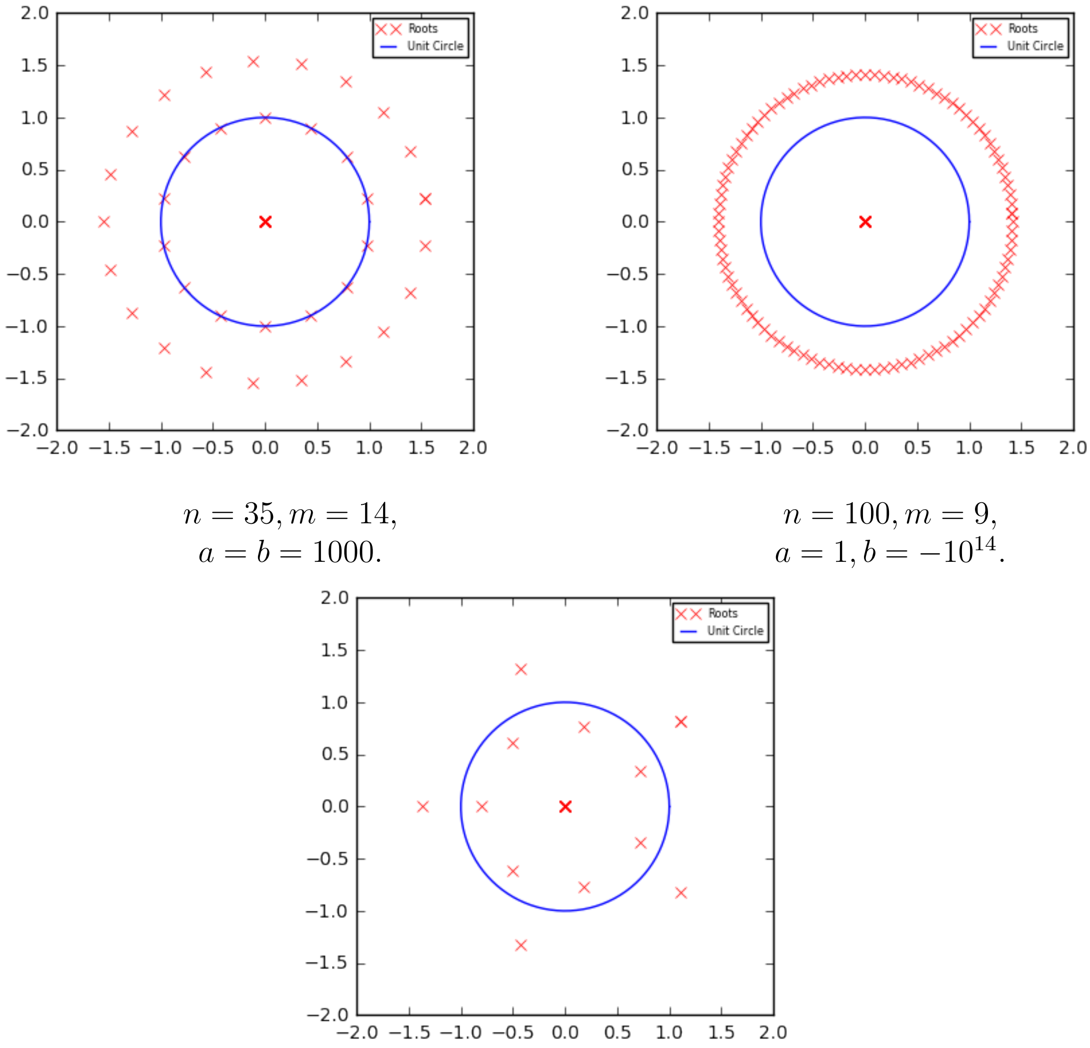
$a = b = 1 \times 10^5$

$a = b = 1 \times 10^{10}$

Figure 5.3: Root plots for $n = 50$ and various a and b.

Thus, it seems like 1 root falls inside the unit circle roughly when $a = b$ or $a > b$ (with possibly more subtle behavior when n is on the same order of magnitude as a, b.) In Chapter 4, we presented a method through the Schur-Cohn theorem which could be used to prove these results. The conclusion would depend on calculating the number of sign changes in the sequence of leading minors for a, b of different relative magnitudes. We explore this approach further below.

The observed behavior generalizes fairly directly to the $m > 1$ case. Where above there was 1 distinguished root on our near the unit circle, there are now m of them, spaced approximately evenly. Other trends in terms of root magnitude depending on a, b, n and tightness to the unit circle depending on n appear to continue.



$n = 35, m = 14,$
$a = b = 1000.$

$n = 100, m = 9,$
$a = 1, b = -10^{14}.$

$n = 12, m = 7,$
$a = 5, b = 1.$

Figure 5.4: Root plots for various n, m, a, b.

We seek an analytic explanation of these observed trends. In the following section, we will prove a bound on the magnitude of the polynomial roots and show that it is in practice quite tight. However, we give no guarantee of tightness, and this bound says nothing about the distribution of roots inside versus outside the unit circle. Yet it is in practice a tighter bound that that given in [32] for this class of polynomials.

5.2 Polynomial Root Analysis

We first bound the magnitudes of all roots of f, using the Cauchy bound of Theorem 5 and its approximation in Theorem 6.

Proposition 12. *Let $\rho[f]$ be the Cauchy bound of a polynomial f. Then the roots of $f(x) = x^n + ax^m + b$, $1 \leq m \leq n$, have modulus at most*

$$\rho[f] = \max((2|a|)^{1/n}, (2|b|)^{1/(n-m)}).$$

Proof. Consider Theorem 6 with $\lambda_0 = \lambda_m = \frac{1}{2}$ and all other $\lambda_i = 0$. Clearly the condition that $\sum_{i=0}^{n-1} \lambda_i = 1$ holds, but note Theorem 6 requires all $\lambda_i > 0$. However, for our $f(x)$ the proof of Theorem 6 in [27] carries through for $\lambda_i = 0, i \neq 0, m$ (that is, when $|a_v/a_n| = 0$), which we now show, following the original proof technique.

Let $R = \max_{0 \leq v \leq n-1} \frac{1}{\lambda_n} \left|\frac{a_v}{a_n}\right|^{1/(n-v)}$ and let $c_v = |\frac{a_v}{a_n}|$. It suffices to show that $c_0 + c_1 R + \cdots + c_{n-1} R^{n-1} \leq R^n$ (see [27], Lemma 8.1.1). Note that $c_v \leq \lambda_v R^{n-v}$ is always true: by definition if $\lambda_v \neq 0, c_v \neq 0$, and trivially if $\lambda_v = c_v = 0$. Thus,

$$\sum_{v=0}^{n-1} c_v R^v \leq \sum_{v=0}^{n-1} \lambda_v R^n = R^n$$

and the result follows.

□

For smaller m, this bound appears to be tighter; it is worth highlighting the $m = 1$ case.

Corollary 4. *The roots of $f(x) = x^n + ax + b$ have modulus at most*

$$\max((2|a|)^{1/n}, (2|b|)^{1/(n-1)}).$$

Proof. Let $m = 1$ in the bound of Theorem 12. □

The bound of Proposition 12 makes intuitive sense when compared with the behavior of the root modulus observed above: decreasing the magnitude of a or b forces the maximum modulus closer to the unit circle gradually, while an increase in n forces the modulus closer to the unit circle more rapidly.

Note that Proposition 12 makes no guarantee of tightness; it could be several orders of magnitude too large, and in fact many of the other upper bounds of $\rho[f]$ listed in [27] we tested but do not list here; they were too loose to give any useful information about the roots of $f(x)$. However, the bound r is in practice extremely tight, as illustrated in Figure 5.5 for the $n = 1$ case.

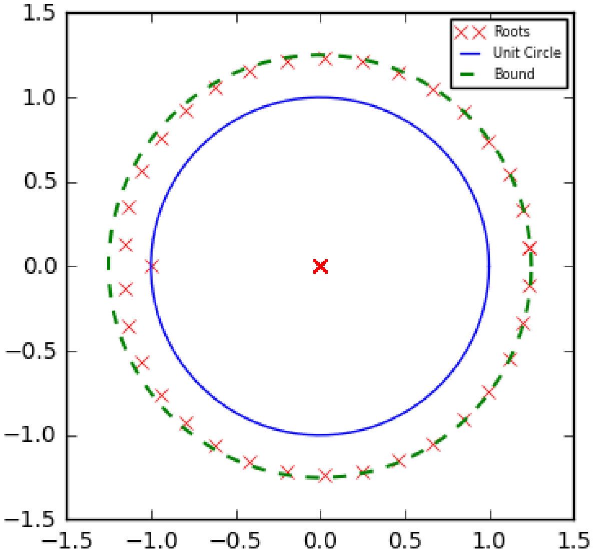


Figure 5.5: Plots of roots and bound, $n = 35, a = b = 1e4$

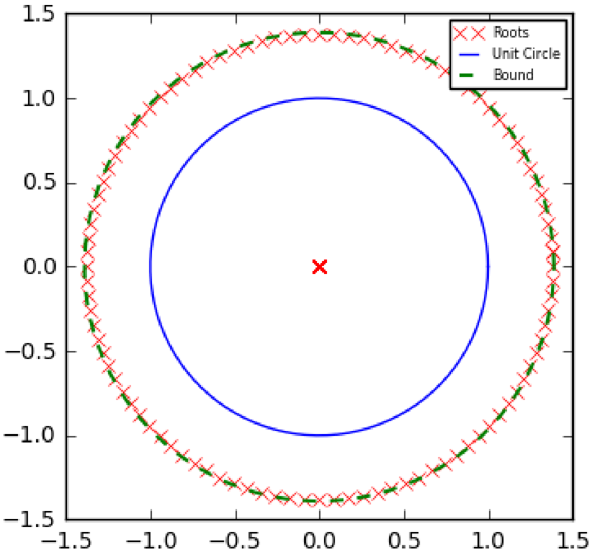


Figure 5.6: Plots of roots and bound, $n = 100, a = 1, b = -10^{14}$

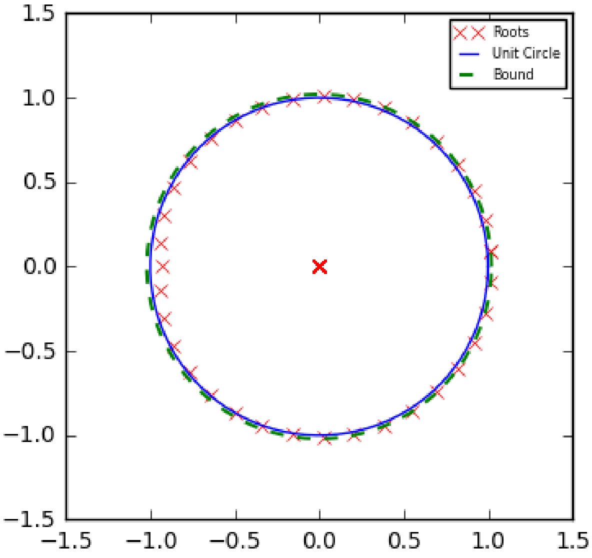


Figure 5.7: Plots of roots and bound, $n = 35, a = b = 1$

In the $m > 1$ case, the bound is less tight on average than in the $a \geq b$ case, due to the nested circle behavior of the roots observed above. The Cauchy bound does not give us any information about the existence of the smaller roots. See Figures 5.8, 5.9, and 5.10

for illustrations of the roots and the Cauchy bound.

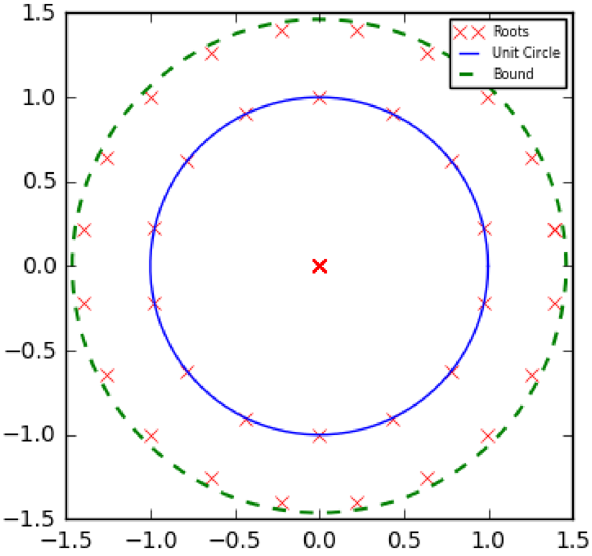


Figure 5.8: Plots of roots and bound, $n = 34, a = b = 1000, m = 14$

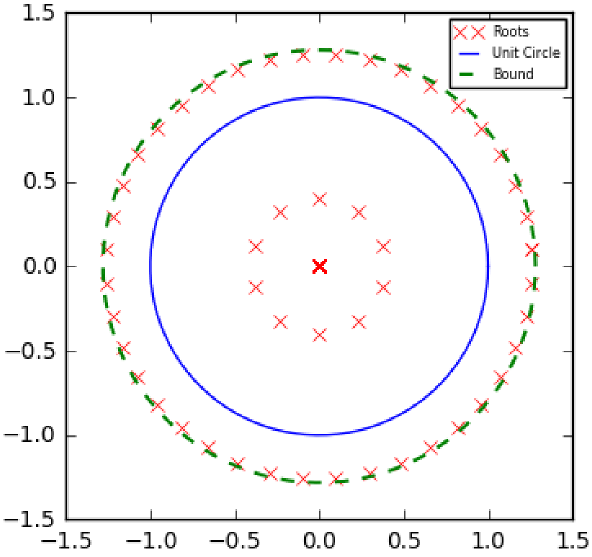


Figure 5.9: Plots of roots and bound, $n = 50, a = 10000, b = 1, m = 10$

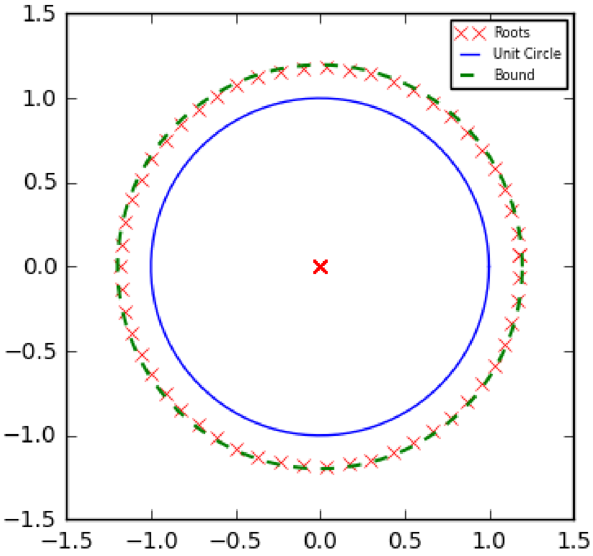


Figure 5.10: Plots of roots and bound, $n = 55, a = 1, b = 10000, m = 25$

Graphically, the root bound appears to be fairly tight. We quantify this tightness more precisely for varying values of a, b, n, m by measuring the distance of various roots to the point closest to them on the unit circle. In Table 5.1, "Max distance to outer root" refers to the the maximum modulus of roots in the outer circle minus 1; "Max distance to inner root" refers to the the maximum modulus of roots in the inner circle minus 1; and "average distance" is the average of the modulus minus 1 over all roots.

Table 5.1: Observed tightness of root bound for various n, m, a, b.

n	m	a	b	Max distance to outer root	Max distance to inner root	Average distance
55	1	1	1000	0.014356	0.014403	0.014379
55	20	1	1000	0.014126	0.014623	0.014379
55	40	1	1000	0.011131	0.017292	0.014377
55	1	1×10^{10}	1×10^{10}	0.005583	0.551529	0.029393
100	1	1×10^{10}	1×10^{10}	0.001440	0.270723	0.0114596
100	10	1×10^{10}	1×10^{10}	0.008979	0.301535	0.039140
100	50	1×10^{10}	1×10^{10}	0.022124	0.607017	0.314571
100	1	1000	1	0.007524	1.078801	0.018246
100	10	1000	1	0.008343	0.586936	0.066207
100	50	1000	1	0.016028	0.293218	0.154623

Thus we see that tightness of the bound to the outer ring is consistently around 10^{-2}, with some variation depending on parameter magnitudes.

Plotting these errors gives an idea of how this tightness varies in each parameter. First, we fix values of a, b and plot the errors for various values of n; see Figures 5.11 through 5.14. The errors decrease as n increases, but the errors increase slightly as the coefficients increase in magnitude.

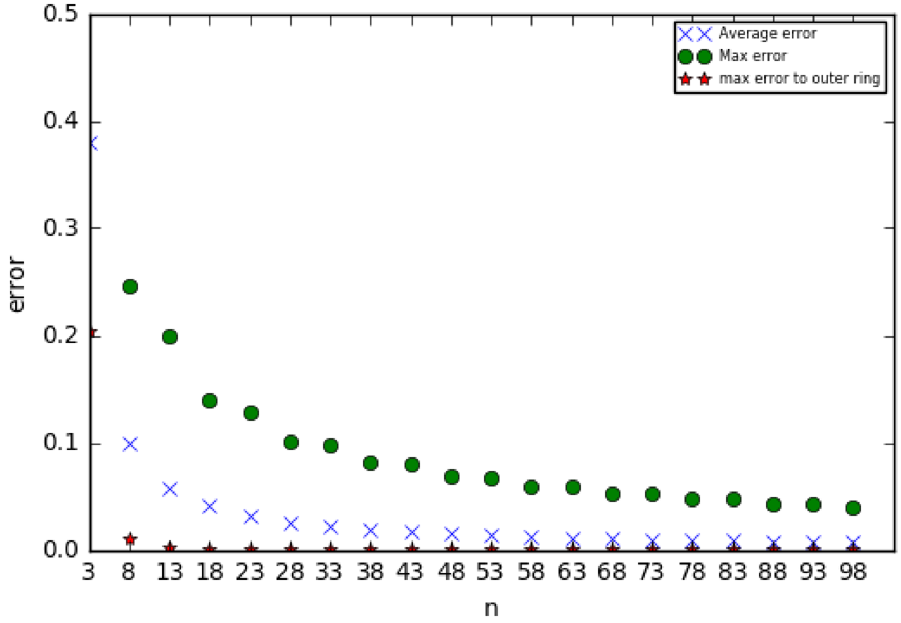


Figure 5.11: Average and maximum error, $a = b = 1, m = 1$

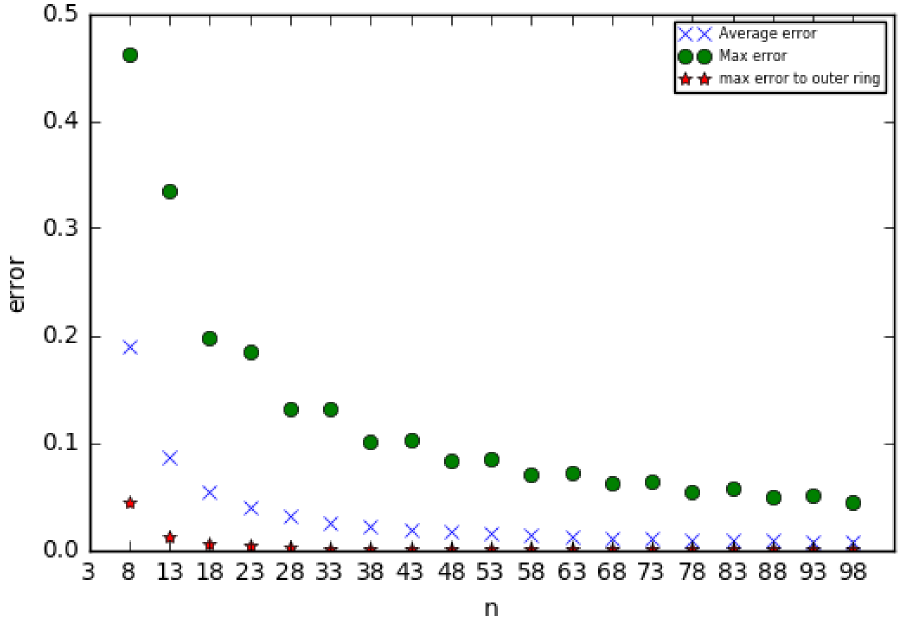


Figure 5.12: Average and maximum error, $a = b = 10, m = 1$

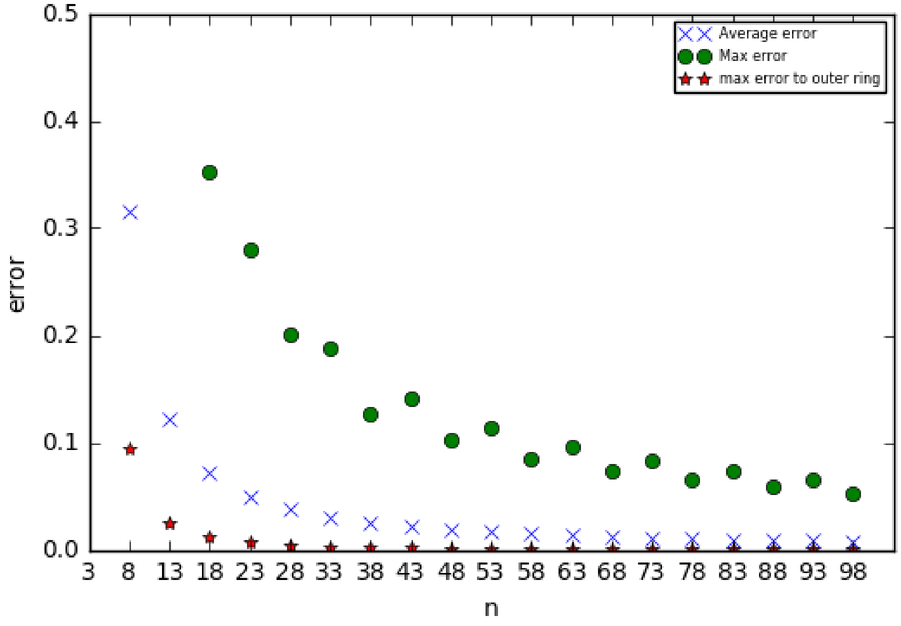


Figure 5.13: Average and maximum error, $a = b = 100, m = 1$

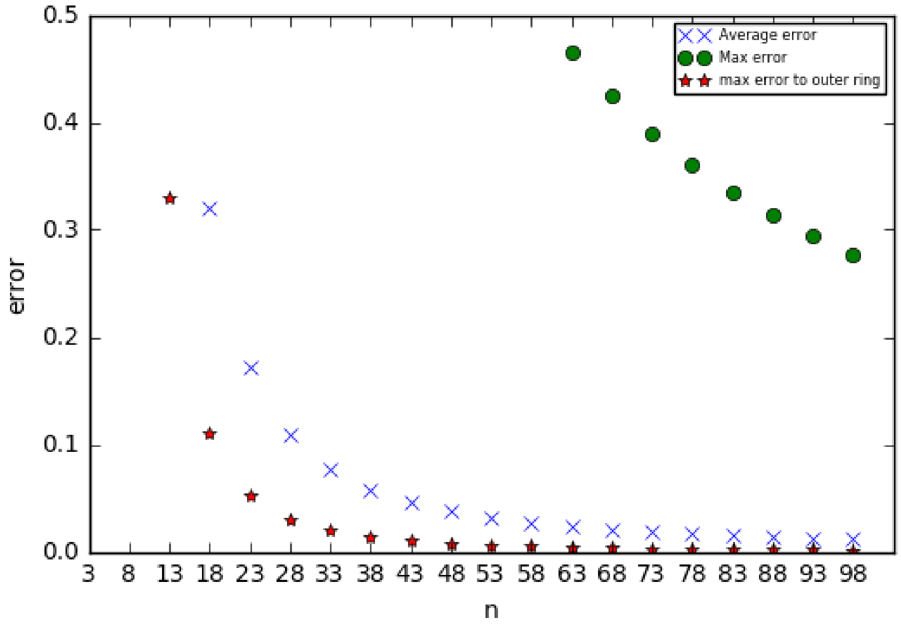


Figure 5.14: Average and maximum error, $a = b = 1 \times 10^9, m = 1$

Now we vary m. Figures 5.15 through 5.18 show the same a, b, n ranges as above, but now we fix $m = \lfloor n/2 \rfloor$. The same sort of behavior as above is apparent, but note that now that the average error especially is higher. This is because there are now m roots near the unit circle and thus have larger distance from the outer maximum modulus, instead of the 1 root as before.

For even n in the $a = b = 1$ cases, the maximum, maximum outer, and average error are all equal. This is due to the fact that $x^{2n} \pm x^n \pm 1$ are cyclotomic polynomials, thus their roots are the roots of unity, and the Cauchy bound happens to be exact.

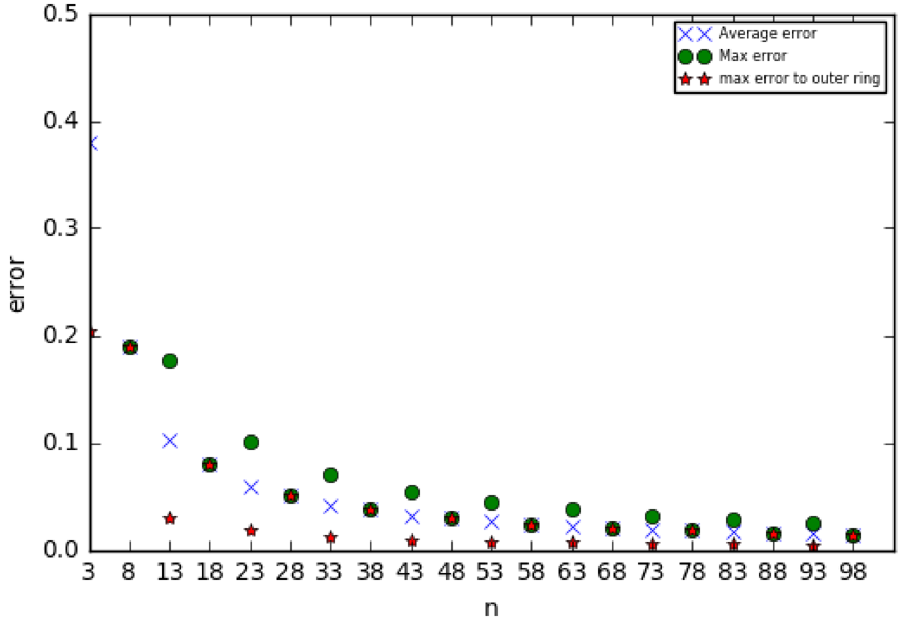


Figure 5.15: Average and maximum error, $a = b = 1, m = \lfloor n/2 \rfloor$

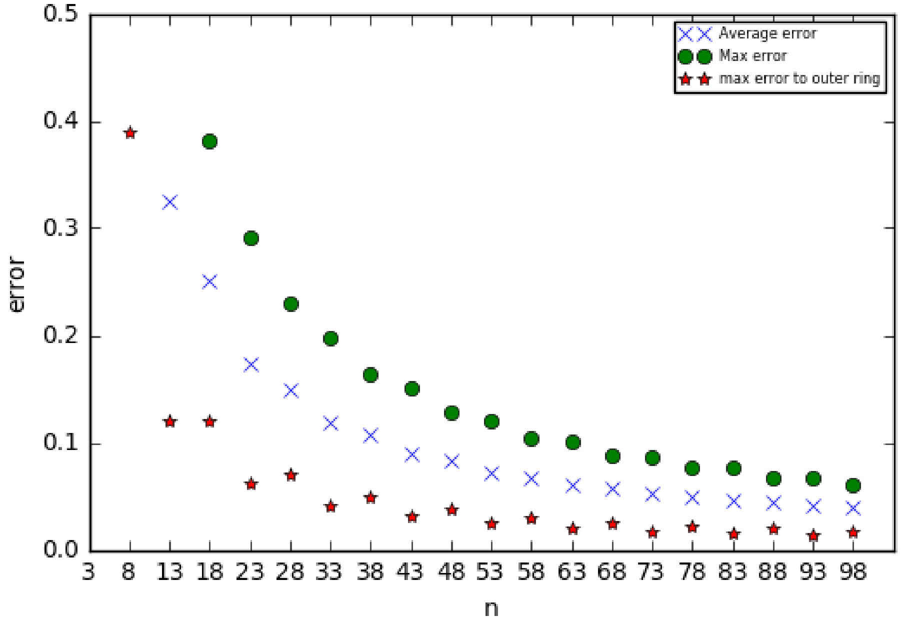


Figure 5.16: Average and maximum error, $a = b = 10, m = \lfloor n/2 \rfloor$

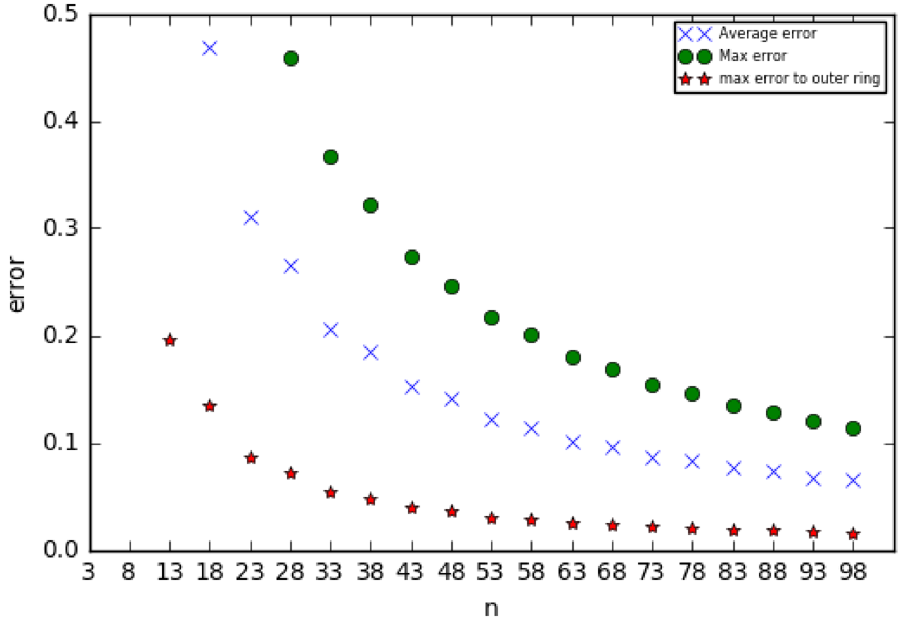


Figure 5.17: Average and maximum error, $a = b = 100, m = \lfloor n/2 \rfloor$

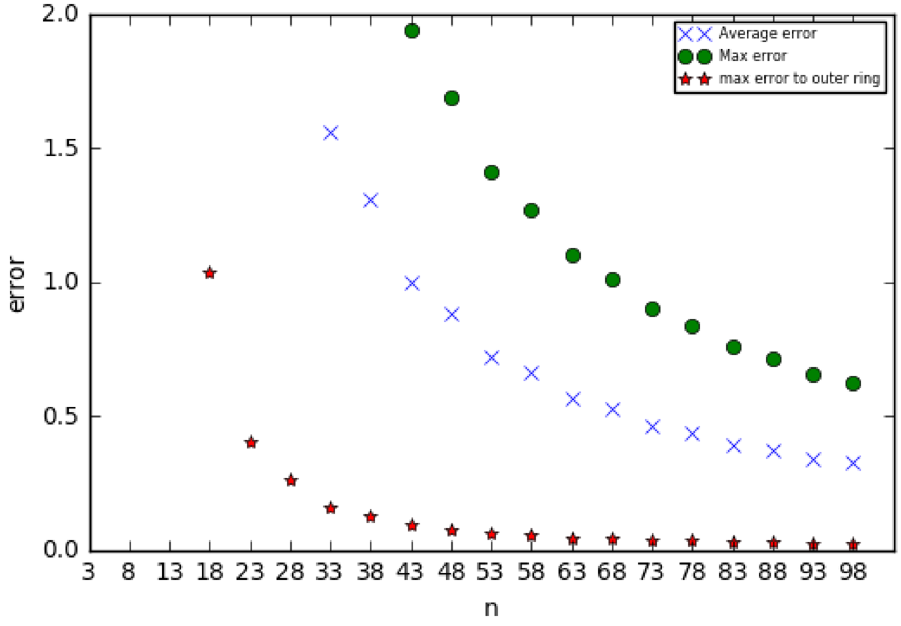


Figure 5.18: Average and maximum error, $a = b = 10^9, m = \lfloor n/2 \rfloor$

Fixing $m = \lfloor n/4 \rfloor$ and repeating these tests gives a results as expected, with the average error somewhere in between the $m = 1$ and $m = \lfloor n/2 \rfloor$ cases. See Figures 5.19 through 5.22.

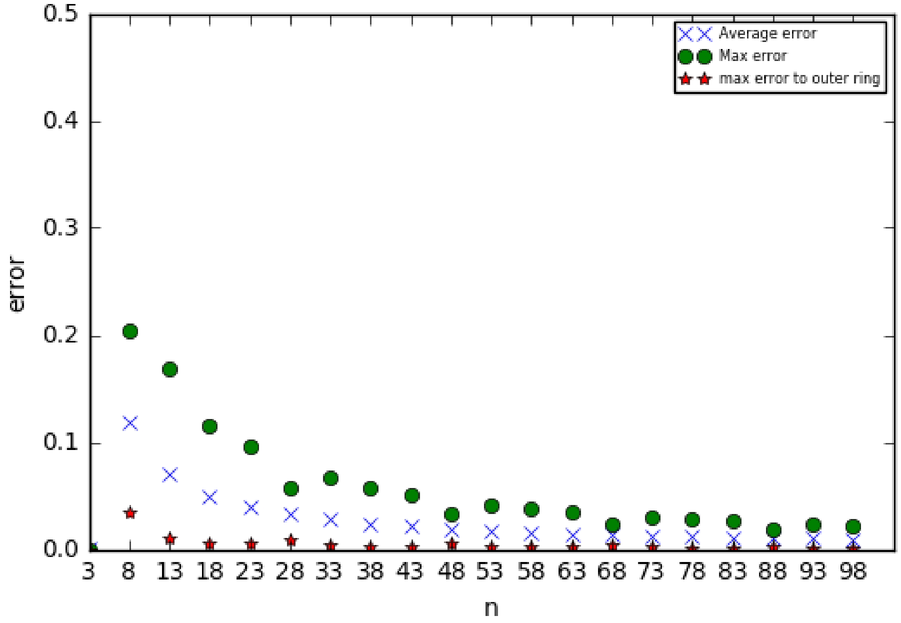


Figure 5.19: Average and maximum error, $a = b = 1, m = \lfloor n/4 \rfloor$

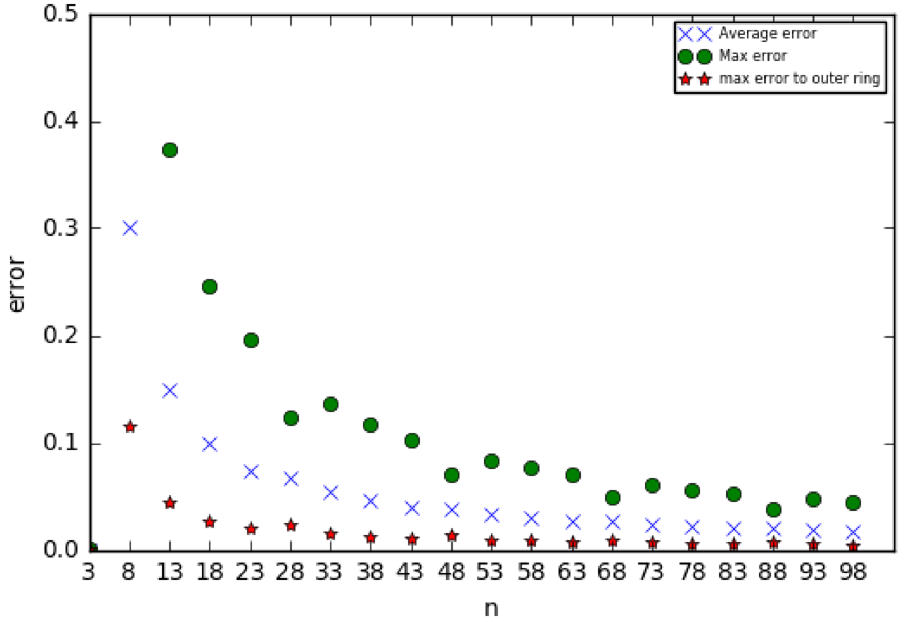


Figure 5.20: Average and maximum error, $a = b = 10, m = \lfloor n/4 \rfloor$

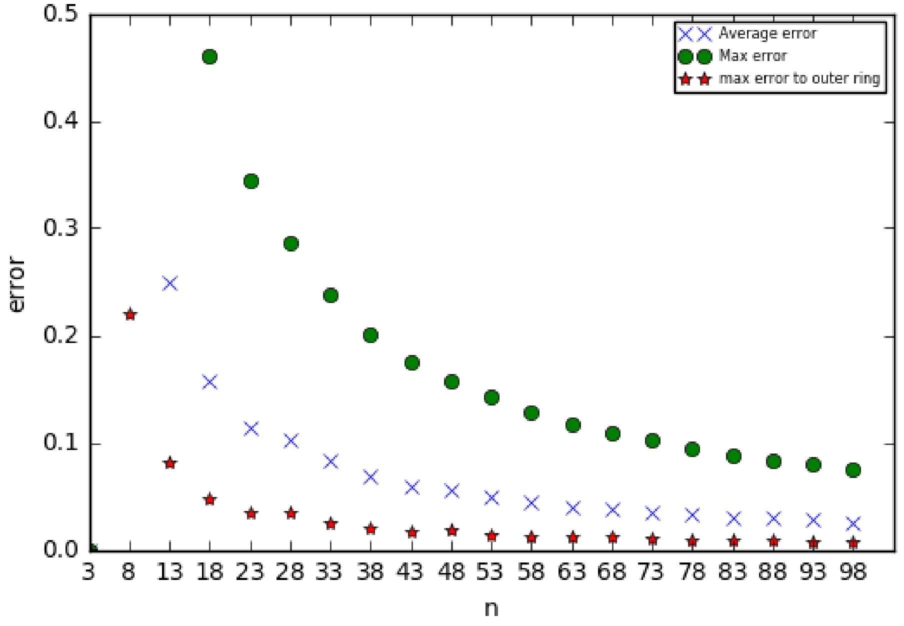


Figure 5.21: Average and maximum error, $a = b = 100, m = \lfloor n/4 \rfloor$

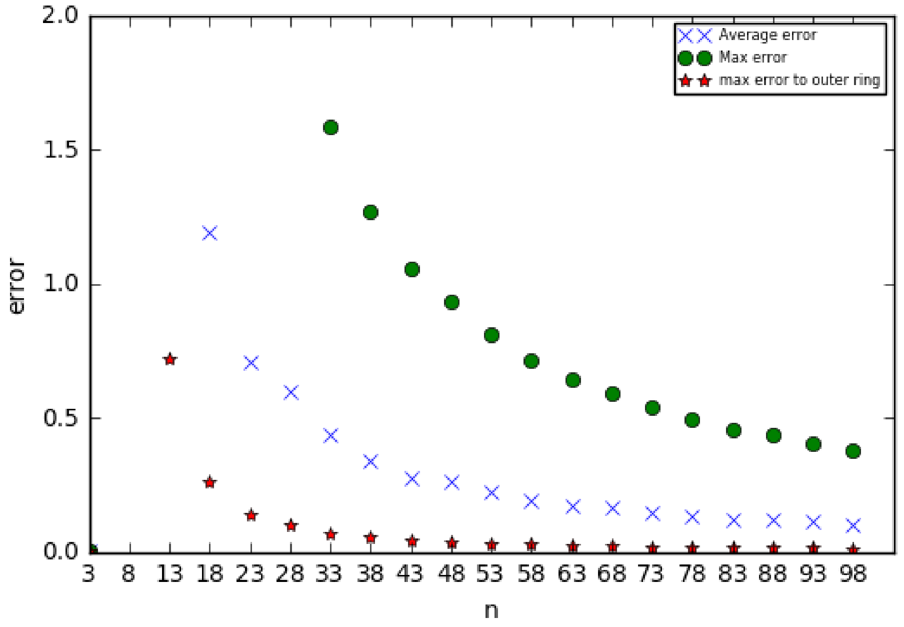


Figure 5.22: Average and maximum error, $a = b = 10^9, m = \lfloor n/4 \rfloor$

Finally, we fix $n = 55$ (arbitrarily; similar results hold for other n) and vary the magnitude of the coefficients. First, we clearly see the dominating behavior of a large b value; as noted above, all roots appear in one ring, so the max inner, outer, and average errors are extremely similar, and basically identical for large enough b. The results are shown in Figures 5.23 through 5.25.

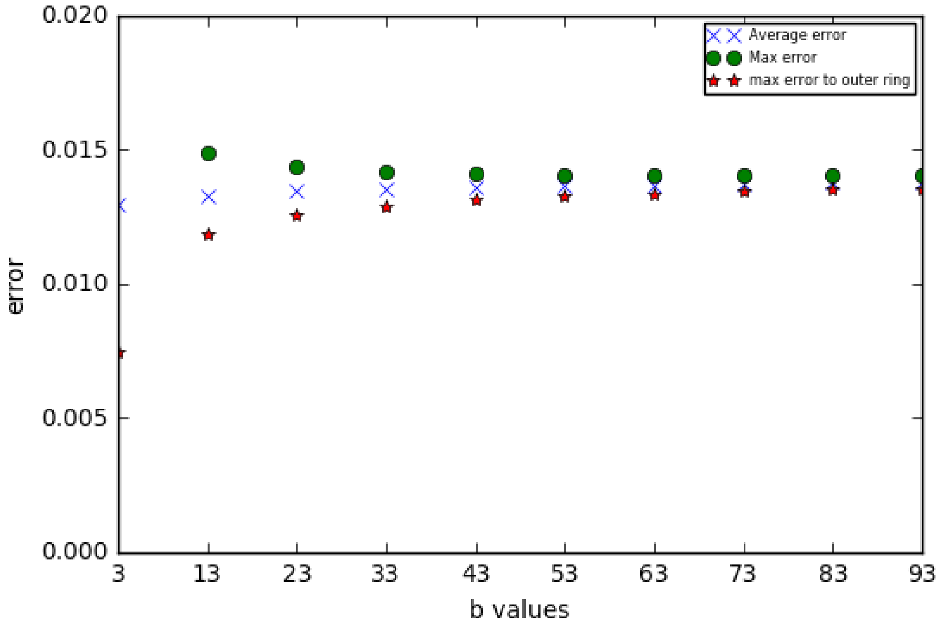


Figure 5.23: Average and maximum error, $n = 55, a = 1, m = 1$

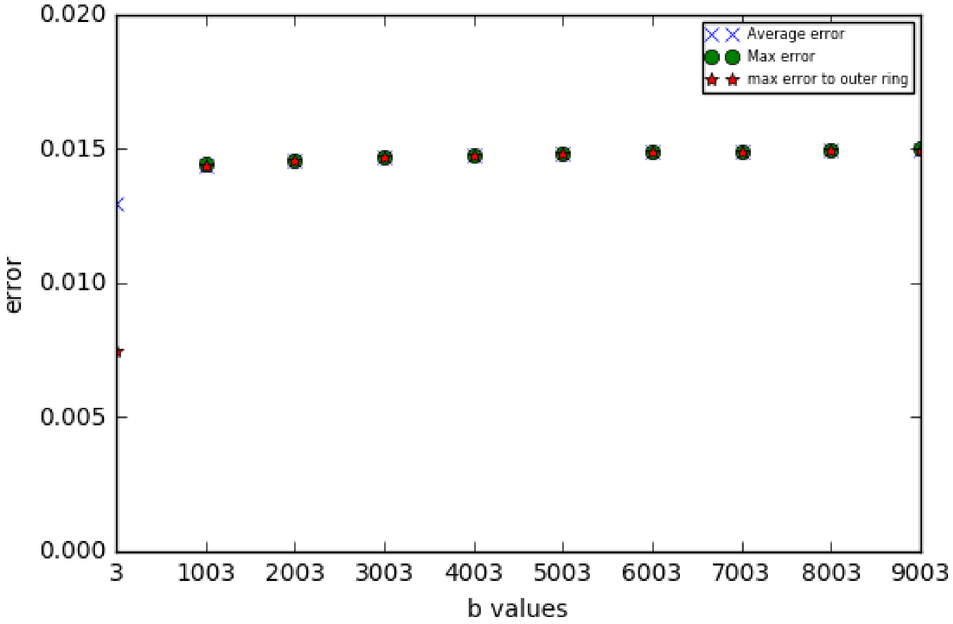


Figure 5.24: Average and maximum error, $n = 55, a = 1, m = 1$

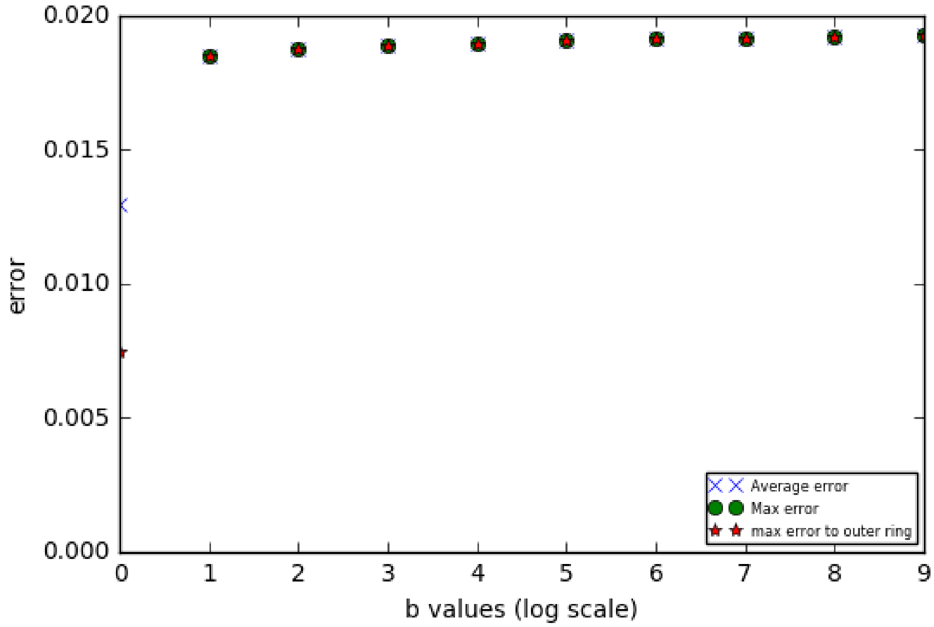


Figure 5.25: Average and maximum error, $n = 55, a = 1, m = 1$

For other values of m, the same trends hold, though convergence takes longer for larger m. See Figures 5.26 through 5.28.

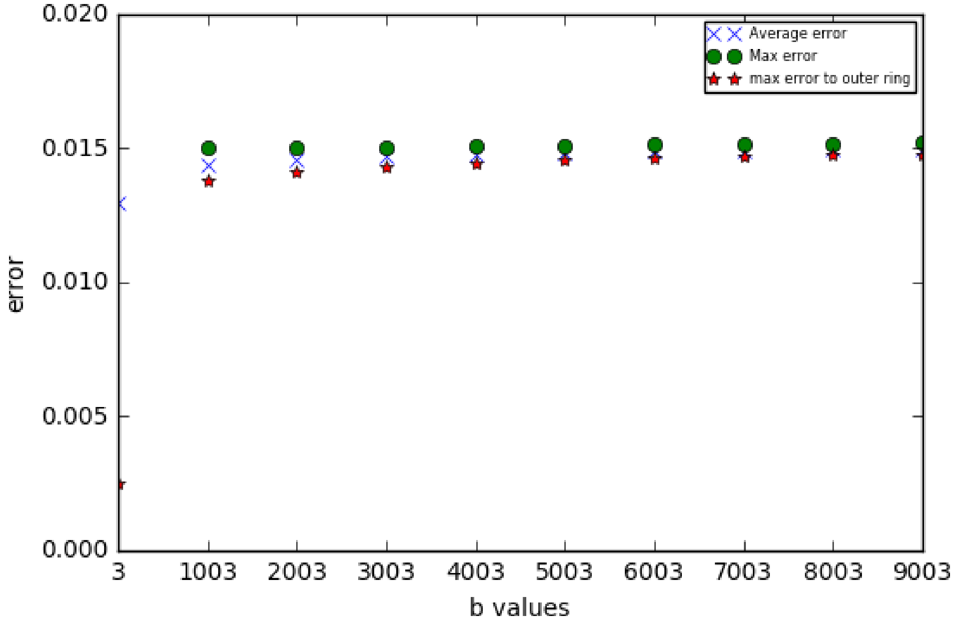


Figure 5.26: Average and maximum error, $n = 55, a = 1, m = 27$

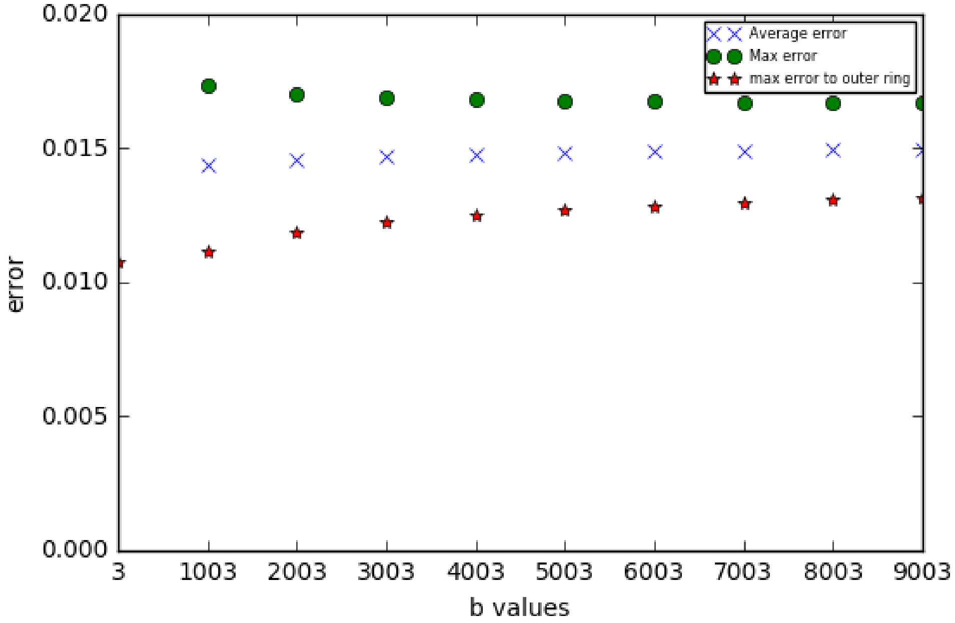


Figure 5.27: Average and maximum error, $n = 55, a = 1, m = 40$

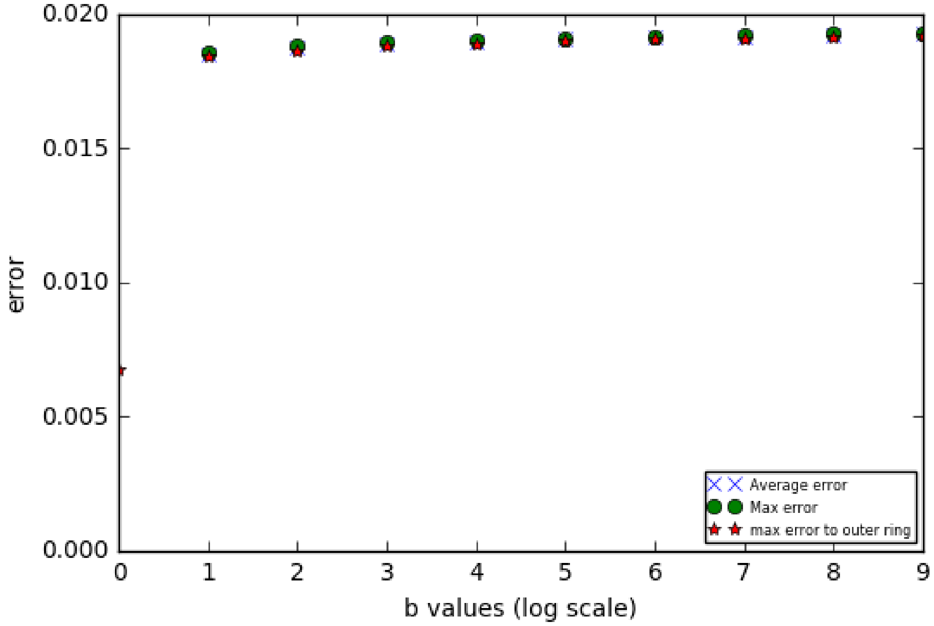


Figure 5.28: Average and maximum error, $n = 55, a = 1, m = 27$

For the $a > b$ case, error to the inner ring of course increases, but error to the outer ring remains consistent with the above trends. See Figures 5.29 and 5.30.

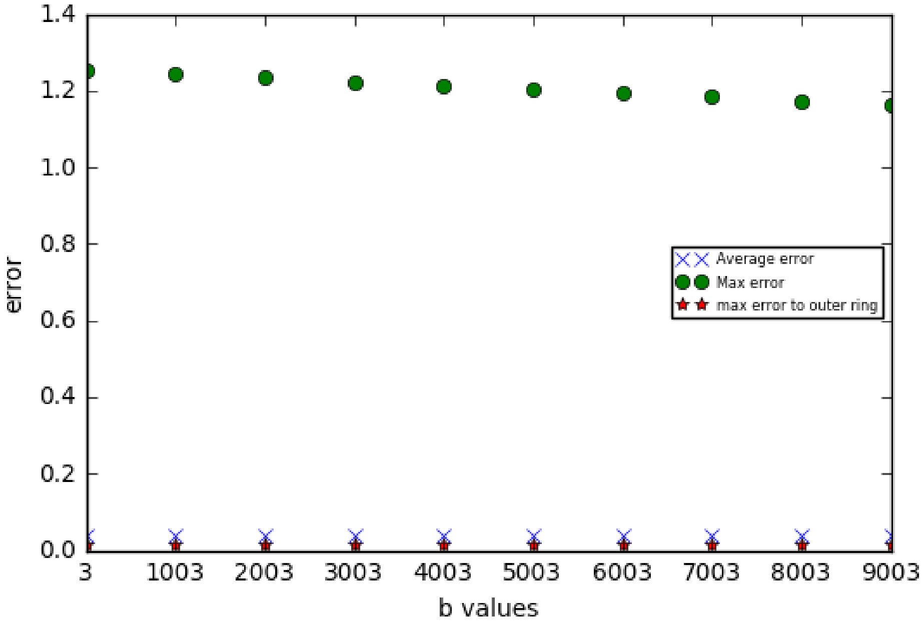


Figure 5.29: Average and maximum error, $n = 55, a = 1 \times 10^5, m = 1$

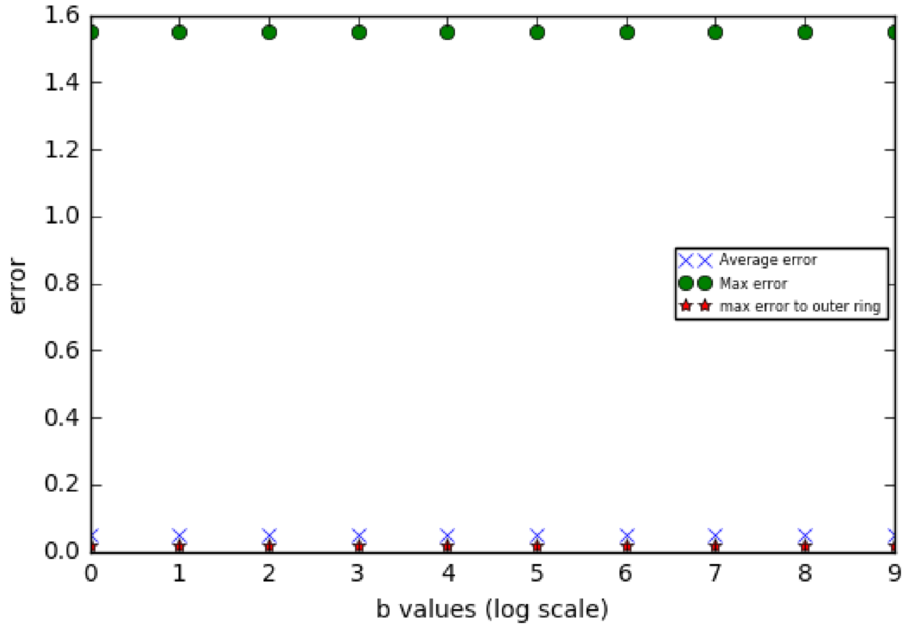


Figure 5.30: Average and maximum error, $n = 55, a = 1 \times 10^{10}, m = 1$

Thus we conjecture that for reasonably large values of n and for a, b, error, at least to the outer ring of roots, is small. We leave proof of a tightness guarantee, either through the Cauchy bound or some other theorem, as an avenue for future work.

Having explored the magnitudes of the roots in some observational depth, we briefly turn to other root properties, and prove some basic results using more conventional root theorems. In the $m = 1$ case, we can easily prove the existence and number of real roots of the polynomial.

Proposition 13. *The polynomial $f(x) = x^n + ax + b$ has 1 real root if n is odd and $a \neq 0$ and $|a| < n\big(\frac{-b}{a(1-\frac{1}{n})}\big)^{n-1}$, and 3 real roots if $a < 0$ and $|a| < n\big(\frac{-b}{a(1-\frac{1}{n})}\big)^{n-1}$. If n is even, f has 2 real roots if $a \neq 0$ and $|a| < n\big(\frac{-b}{a(1-\frac{1}{n})}\big)^{n-1}$, and 0 real roots if $a < 0$ and $|a| > n\big(\frac{-b}{a(1-\frac{1}{n})}\big)^{n-1}$.*

Proof. First, we calculate the Sturm sequence, defined in Theorem 2, of $f(x)$. Clearly $f_0(x) = x^n + ax + b$ and $f_1(x) = nx^{n-1} + a$. The remainder of quo(f_0, f_1) will have degree 1, so the Sturm sequence will have 4 total entries. It is clear from the Euclidean algorithm that $rem(f_0, f_1) = a(1 - \frac{1}{n})x + b$ and so $f_2(x) = -a(1 - \frac{1}{n})x - b$. So we must calculate $rem(f_1, f_2)$. The first entry of the quotient is $\frac{nx^{n-2}}{-a(1-\frac{1}{n})}$; multiplying by b in the next step gives $\frac{bnx^{n-2}}{-a(1-\frac{1}{n})}$. Each subsequent step of the algorithm gives another $a(1-\frac{1}{n})$ in the denominator and another b in the numerator. The sign switches every step, as there are only 0 coefficients between $nx^{n-1}+a$ in f_1. Noting that there are $n-1$ steps of the algorithm gives $f_3(x) = a + n\big(\frac{-b}{a(1-\frac{1}{n})}\big)^{n-1}$.

In summary,

$$\begin{aligned}
f_0(x) &= x^n + ax + b \\
f_1(x) &= nx^{n-1} + a \\
f_2(x) &= -a(1-\frac{1}{n})x - b \\
f_3(x) &= -a - n\big(\frac{-b}{a(1-\frac{1}{n})}\big)^{n-1}
\end{aligned}$$

Now we apply Sturm's Theorem on the interval $(-\infty, \infty)$ to get the total number of real roots. The calculations are not difficult since we know all the f_i; see table below for summary of results. We start with the odd n and consider cases for the sign of a, noting that the sign of b will not change the results. Furthermore, note that f_3 could be positive or negative depending on the relative magnitudes of a and b.

Table 5.2: Sturm sequence signs, $a > 0, n$ odd.

Polynomial	Sign at $-\infty$	Sign at ∞
f_0	$-$	$+$
f_1	$+$	$+$
f_2	$+$	$-$
f_3	$-$	$-$

Table 5.3: Sturm sequence signs, $a < 0, n$ odd.

Polynomial	Sign at $-\infty$	Sign at ∞
f_0	$-$	$+$
f_1	$+$	$+$
f_2	$-$	$+$
f_3	$+$ or $-$	$+$ or $-$

Therefore, the number of real roots is

$$V(-\infty) - V(\infty) = 2 - 1 = 1, \quad a > 0$$

and for the $a < 0$ case, either $a < n\left(\frac{-b}{a(1-\frac{1}{n})}\right)^{n-1}$ and then f_3 is negative, yielding

$$V(-\infty) - V(\infty) = 2 - 1 = 1, \quad a < 0$$

and otherwise

$$V(-\infty) - V(\infty) = 3 - 0 = 3, \quad a < 0.$$

For n even, we repeat the sign calculation. As before, the relative magnitudes of a, b, n determine the sign of the last row.

Table 5.4: Sturm sequence signs, $a < 0, n$ even.

Polynomial	Sign at $-\infty$	Sign at ∞
f_0	$+$	$+$
f_1	$-$	$+$
f_2	$-$	$+$
f_3	$+$ or $-$	$+$ or $-$

If $a < n\left(\frac{-b}{a(1-\frac{1}{n})}\right)^{n-1}$ then f_3 is negative and so

$$V(-\infty) - V(\infty) = 2 - 0 = 2$$

and otherwise

$$V(-\infty) - V(\infty) = 1 - 1 = 0.$$

If $a > 0$, then

Table 5.5: Sturm sequence signs, $a > 0, n$ even.

Polynomial	Sign at $-\infty$	Sign at ∞
f_0	$+$	$+$
f_1	$-$	$+$
f_2	$+$	$-$
f_3	$-$	$-$

Thus in this case

$$V(-\infty) - V(\infty) = 3 - 1 = 2.$$

□

Proposition 14. *The polynomial $f(x) = x^n + ax^m + b$ has at least one root of modulus less than 1 whenever $|a| \geq |b|(\frac{n}{n-m})^{1/m}$.*

Proof. Let $p = m, k = 1, a_1 = a_2 = \cdots = a_{p-1} = 0$ and $n_k = n$ as in Theorem 3. Then $r_1 = (\frac{n}{n-m})^{1/m}$ and by Theorem 3, f has a root of modulus at most $|b/a|(\frac{n}{n-m})^{1/m}$. Thus f has a root of modulus at most 1 when $|a| \geq |b|(\frac{n}{n-m})^{1/m}$. □

Note that $|a| > |b|$ will suffice to have a root of modulus at most 1, since $(\frac{n}{n-m})^{1/m} > 1$. The proposition above gives a stronger condition.

The previous result suffices to show that a polynomial of the given form has at least one root inside the unit circle. However, we previously conjectured a more specific pattern:

that for $m > 1$ and $|a| > |b|$, exactly m of the roots fall inside the unit circle, and that they are roughly equally distributed angularly.

Conjecture 1. *For $|a| \geq b$ the polynomial $f(x) = x^n + ax^m + b$ has m roots spaced roughly evenly on or inside the unit circle and $n - m$ roots spaced roughly evenly outside the unit circle. For $|b| > |a|$ all roots are outside the unit circle.*

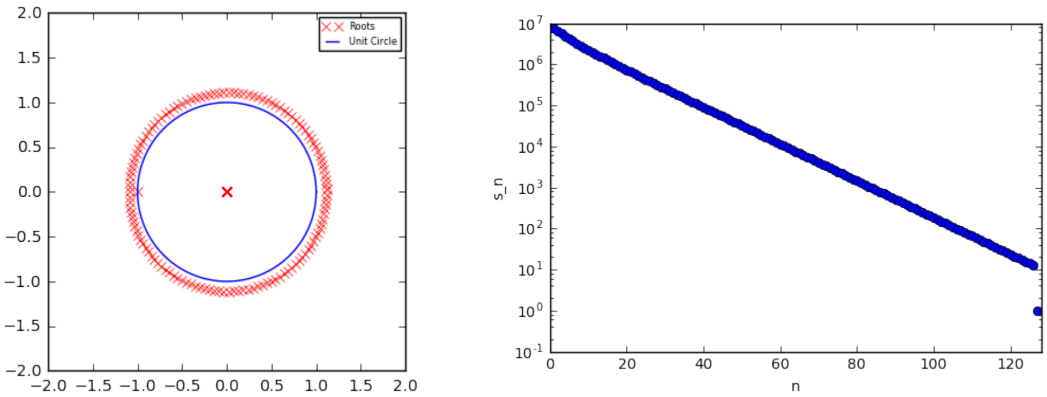
As we show in Section 5.3, the singular value behavior of the Vandermonde matrix associated with this polynomial follows its root behavior closely. Thus we set out to prove Conjecture 1, hoping to use this result to then prove the behavior of the Vandermonde matrix and show its cryptographic implications. We explain our proof tactic (which is an approach similar to the $x^n + ax + b$ case in the previous chapter) and its surprising implications in the next chapter. For now, we go back to the Vandermonde matrix and show some heuristic evidence as far as the root/singular value connection.

5.3 Vandermonde Matrix: Singular value observations

As with the $f(x) = x^n + x + 1$ case in Chapter 4, there appears to be a strong correlation between the root locations and the singular values of the matrix. While we don't prove this correlation, we show our plots here, which motivates future exploration in this area.

In general, having j roots inside the unit circle corresponds to a gap between the j smallest and $n - j$ largest singular values in the Vandermonde matrix.

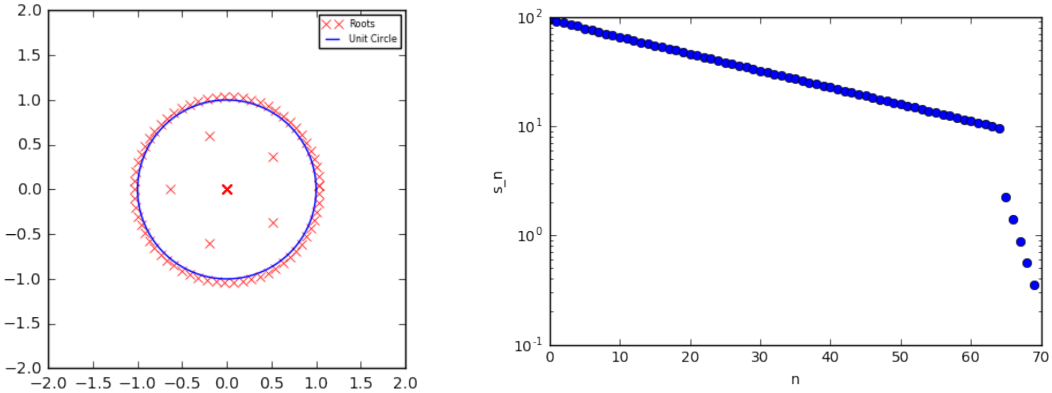
The plots in Figure 5.31 are a re-creation of those in [9]. Other choices of n, m, a, b, shown in Figures 5.32, 5.33, and 5.34 are our observations.



Roots

Singular values

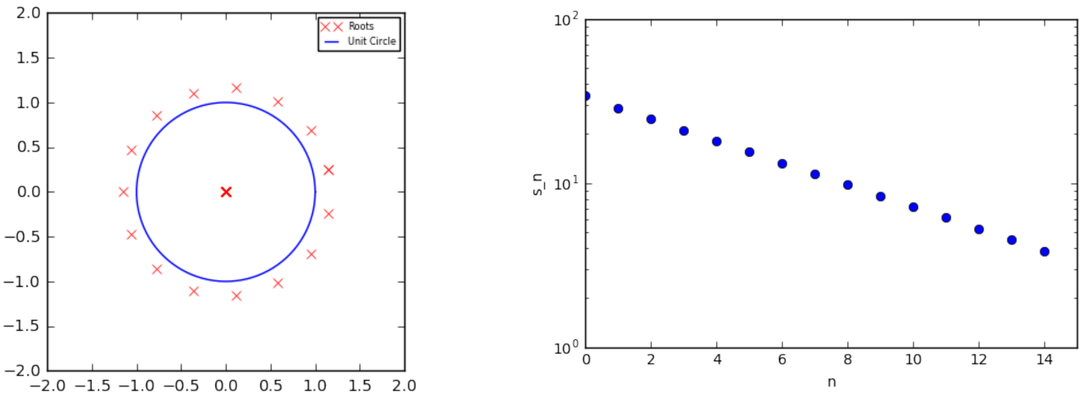
Figure 5.31: Roots and singular value correspondence, $n = 128$, $a = 524288, b = 524285$



Roots

Singular values

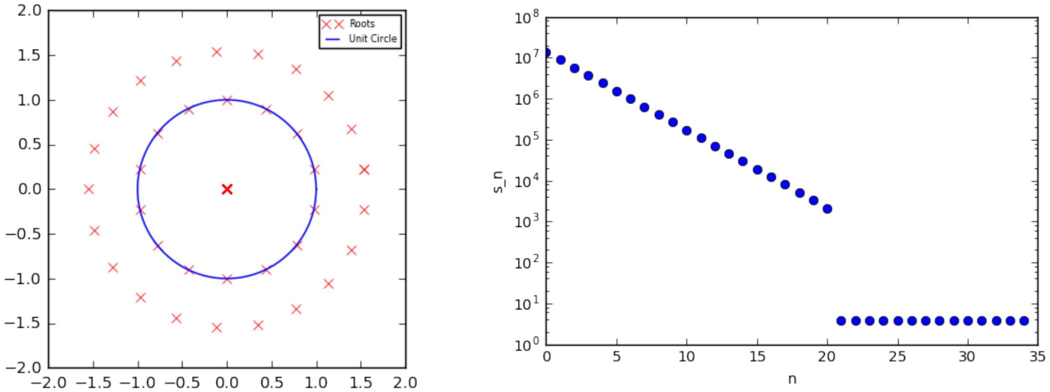
Figure 5.32: Roots and singular value correspondence, $n = 70, m = 5$, $a = 10, b = 1$



Roots

Singular values

Figure 5.33: Roots and singular value correspondence, $n = 15, m = 1,\ a = 1, b = 10$



Roots

Singular values

Figure 5.34: Roots and singular value correspondence, $n = 35, m = 14,\ a = 10^3, b = 10^3$

Chapter 6

Cryptographic Combinatorics: The k-Fibonacci Twist

6.1 Introduction and Motivation

The work in this chapter contains the main results and most exciting contributions of this thesis. It has a much more pure combinatorial flavor than what followed previously, but the motivation for this work arises directly from Chapters 4 and 5. Specifically, consider the Schur-Cohn theorem (Theorem 9) again, which we previously used in Chapter 4 to find the number of roots of $x^n \pm x \pm 1$ inside the unit circle. Unlike before, we now consider a more general polynomial $x^n + ax^m + b$, where now m can be larger than 1. Construction of the Schur-Cohn matrix C in the usual fashion gives a matrix similar to the C of Proposition 9 in Chapter 4, but instead the $-ab$ elements appear on the mth subdiagonal and superdiagonal, instead of immediately above and below the main diagonal. We set out to calculate the leading minor sequence in this matrix using a similar permutation approach to that of Chapter 4.

To begin, we made two simplifying assumptions, along the same lines as those in Chapter 4: we first assumed that we had only a $(0, 1)$ matrix, and we disregarded the signs of the permutations and first calculated how many non-zero terms there are. (We also first changed the 0 in the $(1, 1)$ of C location to a 1, to simplify the initial analysis.) Thus, the simplified problem we began with was to define and solve a permutation problem which is equivalent to computing the permanent of a $0, 1$ m-tridiagonal matrix.

It is important to note that the solution to the tridiagonal permanent problem was already known and is given in [14] and [15]. However, our permutation approach to the proof is new, and we solved two enumerative combinatorics problems specifically posed in [14] and [15]. Full details on previous work and our contributions are given in section 6.4 below.

6.2 Background

A permutation is a bijection from a set of elements $[n]$ to itself. Permutations have been studied extensively, including a wide variety of permutation statistics which calculate various combinatorial properties of permutations [1].

One such statistic is known as drop size.

Definition 17. The drop size of an element i of a permutation π on n elements is defined as $|\pi(i) - i|$, $1 \leq i \leq n$.

There has been much previous work on permutations with *maximum* drop size k, for instance [11], [12]. However, here we will consider a variant, and define permutations with fixed drop size k, where *every* element in the permutation must have drop size 0 or k. We prove that the number of permutations with a fixed drop size k, which we will call a *k-drop permutation*, is a generalization of a Fibonacci number. Furthermore, we provide bijections from k-drop permutations to four other combinatorial objects, which are also counted by the same Fibonacci generalization.

We begin by recalling some elementary background. To start, consider a composition of an integer n.

Definition 18. A *composition* of an integer n is an ordered set of positive integers $(a_1, \ldots, a_k)$ where $a_1 + \cdots + a_k = n$.

There are 2^{n-1} compositions of a number n, and there are $\binom{n-1}{k-1}$ compositions of n with exactly k parts.

Example 3. The 2^3 compositions of 4 are

$$(4), (2,1,1), (1,2,1), (1,1,2), (1,3), (3,1), (2,2), (1,1,1,1).$$

Also, recall the well-known Fibonacci sequence defined by the recursion

$$f_n = f_{n-1} + f_{n-2}, f_0 = 1, f_1 = 1.$$

The first few Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, 21, 34 \ldots$$

The Fibonacci sequence has generating function

$$f(x) = \frac{1}{1 - x - x^2}.$$

A closed form for the Fibonacci numbers is given by the Binet formula

$$F_n = \frac{\psi_+^n - \psi_-^n}{\sqrt{5}}$$

where $\psi_+ = \frac{1+\sqrt{5}}{2}$ and $\psi_- = \frac{1-\sqrt{5}}{2}$. There are of course many more fascinating combinatorial and algebraic properties of the Fibonacci numbers.

A generalization of the Fibonacci numbers is defined in [14] as follows.

Definition 19. The nth k-Fibonacci number is defined by

$$f_{n,k} = f_m^{k-r} f_{m+1}^r$$

where

$$n = mk + r,\ 0 \leq r < k.$$

We will follow the example of the authors and refer to these integers as the k-Fibonacci numbers throughout this paper. (These are not to be confused with the class of Fibonacci generalizations of the form $F_{k,n} = kF_{k,n-1} + F_{k,n-2}$, which have been extensively studied and which is an entirely different generalization.)

Here is the product definition for some small k-Fibonacci numbers, for small values of n and k.

Table 6.1: Some small k-Fibonacci numbers, product definition.

n/k	0	1	2	3	4	5
0	f_0	f_0	f_0^2	f_0^3	f_0^4	f_0^5
1	f_0	f_1	f_0f_1	$f_0^2f_1$	$f_0^3f_1$	$f_0^4f_1$
2	f_0	f_2	f_1^2	$f_0f_1^2$	$f_0^2f_1^2$	$f_0^3f_1^2$
3	f_0	f_3	f_1f_2	f_1^3	$f_0f_1^3$	$f_0^2f_1^3$
4	f_0	f_4	f_2^2	$f_1^2f_2$	f_1^4	$f_0f_1^4$
5	f_0	f_5	f_2f_3	$f_1f_2^2$	$f_1^3f_2$	f_1^5
6	f_0	f_6	f_3^2	f_2^3	$f_1^2f_2^2$	$f_1^4f_2$
7	f_0	f_7	f_3f_4	$f_2^2f_3$	$f_1f_2^3$	$f_1^3f_2^2$
8	f_0	f_8	f_4^2	$f_2f_3^2$	f_2^4	$f_1^2f_2^3$
9	f_0	f_9	f_4f_5	f_3^3	$f_2^3f_3$	$f_1f_2^4$

Some patterns are evident from both the chart and the definition.

- For fixed k, every kth element is a power of a Fibonacci number.
- For any $f_{n,k}$, the Fibonacci numbers which make up $f_{n,k}$ are at most one index apart.
- For a fixed n, any $f_{n,k}$ with $k > \lfloor n/2 \rfloor$ is a power of 2.

This last item is true since $k > \lfloor n/2 \rfloor$ implies $n > m \lfloor n/2 \rfloor + r$ in the notation of Definition 19, which means $m < 2$ since $r \geq 0$.

Here are the evaluated products of some small k-Fibonacci numbers.

Table 6.2: The k-Fibonacci numbers, evaluated.

n/k	0	1	2	3	4	5
0	1	1	1	1	1	1
1	1	1	1	1	1	1
2	1	2	1	1	1	1
3	1	3	2	1	1	1
4	1	5	4	2	1	1
5	1	8	6	4	2	1
6	1	13	9	8	4	2
7	1	21	15	12	8	4
8	1	34	25	18	16	8
9	1	55	40	27	24	16

6.3 Five Problems

To motivate our work, consider the following five problems.

Problem 1. Let π be a permutation on n elements. For some k, $1 \leq k \leq n-1$, we wish to count the number of permutations whose drop size for every i in π is exactly 0 or k. We will call these k-drop permutations for short.

Problem 2. Let M be an $n \times n$ square matrix. Fix some k, $1 \leq k \leq n$. Let

$$M_{ij} = \begin{cases} 1, i = j,\ i = j + k,\ j = i + k \\ 0,\ \text{otherwise.} \end{cases} .$$

We wish to find the permanent of M.

Problem 3. We wish to count the number of subsets of $n - k$ elements, where the difference of no two of the elements is k.

Problem 4. Consider a length $n - k$ binary string on $0, 1$ where for any $1 \leq i \leq n - 2k$, there is not a 1 in both at index i and $i + k$. We call these k-free strings. We wish to count the number of k-free strings of length $n - k$.

For our last problem, we define a special type of restricted integer composition in terms of Problem 4.

Definition 20. A k-free composition of n is an integer composition of n which

1. Uses only the numbers $\{1, 2, \ldots, k-1, k+1, k+2, \ldots, 2k\}$, and the first non-1 number in the composition is greater than k.

2. Satisfies the following mapping property.

Define a mapping $m : c(i) \to b_i$ from an element $c(i)$ of a composition c on $\{1, 2, \ldots, k-1, k+1, k+2, \ldots, 2k\}$ to a binary string b_i as follows:

1. $b_i = m(c(i)) = 11 \ldots 1$, where there are $c(i) - k$ copies of 1, if $c(i) > k$ and this is the first occurrence of a number greater than k in the sequence

2. $b_i = m(c(i)) = 01 \ldots 1$, where there are $c(i) - 1$ copies of 1, if $c(i) < k$

3. $b_i = m(c(i)) = 0 \ldots 01 \ldots 1$, where there are $c(i) - k$ copies of 1 and k copies of 0, if $c(i) > k$ and $c(i)$ is not the first number greater than k.

We call c a k-free composition if the concatenation $m(c) = b_1 b_2 \ldots b_{n-k}$ is a k-free string.

While a cleaner characterization (i.e., one which depends only on the properties of the elements of the composition themselves, and not on the binary string) of these compositions thus far escapes us, a few partial characterizations are immediate from the definition.

Proposition 15. *Consider an element $c(i) = h > k$ of a k-free composition. There is no restriction on the location of h.*

Proof. Let $c(i) = h$. If h is the first occurrence of a number greater than k in the composition, then the only numbers preceeding $m(h)$ in the binary string are 0's corresponding to the preceeding 1's in c, so h may occur wherever. If h is not the first instance of a number greater than k in c, then the binary string corresponding to $c(i)$ is $b_i = 0 \ldots 01 \ldots 1$ where there are $c(i) - k$ copies of 1 and k copies of 0. Since there are k zeros, we do not violate the k-free condition in $m(c)$ regardless of what b_{i-1} is. □

Proposition 16. *Consider an element $c(i) = 1$ of a k-free composition. There is no restriction on the location of $c(i)$.*

Proof. This is clear: $m(c(i)) = 0$ in this case, and appending a zero will not impact the k-free string criterion of the previous $b_1 \ldots b_{i-1}$ elements. □

Proposition 17. *Consider an element $c(i) = h > k$ of a k-free composition. If $c(i)$ is not followed by another element greater than k, it must be followed by a composition of $2k - c(i)$.*

Proof. Let $b_i = m(c(i) = 0 \dots 01 \dots 1$ as above. The index of the first 0 is at $c(i)$ and the last is at index $c(i) + k$, so any element from $c(i) + k$ to $c(i) + 2k$ can be assigned a 1. The order or number of 1's does not matter for the k-free validity of $m(c)$, so we simply say the elements following b_i may form any composition of $2k - c(i)$. □

The characterizations of Propositions 15, 16, and 17 form a sufficient though not necessary characterization of a k-free composition. The characterization of a k-free composition is complete only in the event that the composition consists only of numbers greater than k and numbers less than k which only appear as part of a composition proceeding a number greater than k.

We showcase a series of examples of this definition. In Example 4, it suffices to work from the partial characterization; no bijection to the binary string is needed. In Examples 5 and 6, we use the bijection to the binary string to illuminate some subtleties of the definition.

Example 4. Let $n = 10$, $k = 5$. A generalized k composition of n first must use only the numbers from $S = \{1, 2, 3, 4, 6, 7, 8, 9, 10\}$.

There are no restrictions on compositions only using numbers 6 and larger, by Proposition 15, or 1, by Proposition 16. So, 10, $1 + 9$, $1 + 8 + 1$, $1 + 1 + 1 + 1 + 6$ are all examples of 5-free compositions of 10.

If we would like to use the numbers $2, 3, 4$, we must do so carefully. By Proposition 17, we are always allowed to have these numbers follow:

- 6, as part of a composition of 4
- 7, as part of a composition of 3
- 8 as part of a composition of 2

Technically, the definition allows that these numbers could also be used in a composition of 1 following 9 or 0 following 10, but clearly this is not possible.

Thus some valid 5-free compositions using 2,3,4 are:

- 6+1+1+2

- 6+4

- 6+1+3

- 6+3+1

- 7+3

- 8+2

In this case, since $2k = n$, Propositions 15 16, and 17 happen to be both necessary and sufficient; we will never have to consider a $2, 3, 4$ which does not follow as a subcomposition of $2k - c(i)$. We could enumerate all k-free compositions in this case using only the rules from the propositions.

Some non-examples of 5-free compositions include 3+1+6, 4+2+2+2, and 1+1+1+3+4, which all violate condition (1) of the definition, as a number larger than k is not the first non-1 number.

Example 5. A larger example begins to showcase some of the subtleties of the definition. Let $n = 15$, $k = 6$. The compositions may use only $\{1, 2, 3, 4, 5, 7, 8, 9\}$. Some valid 6-free compositions include:

- $7+1+2+2+1+1+1$. There are no restrictions on the location of 7. $1+2+2 = 5$ is a composition of $12 - 7 = 5$. There is no restriction which prevents the trailing 1's.

- $7 + 8$ is valid. There is no restriction on any number greater than 6.

- $9 + 3 + 1 + 1 + 1$, since $12 - 9 = 3$ and 3 is a composition of 3.

Some invalid compositions, which all violate Proposition 17, are:

- $10 + 1 + 2 + 2$, since $2k - 10 = 2$ and $1 + 2$ is not a composition of 2;

- $9 + 4 + 1$, since $2k - 9 = 3$ and 4 is not a composition of 3;

- $8 + 5 + 1 + 1$, since $2k - 8 = 4$ and 5 is not a composition of 4.

A valid composition, which the 3 propositions do not suffice to construct, is

$$7 + 3 + 1 + 1 + 2 + 1.$$

We can construct $7+3+1+1$ using Proposition 17. However, we do not currently have a proposition which tells us directly whether or not the 2 in the penultimate position is valid. To ascertain this, we construct $m(c) = 101100010$ and note that no two 1's are distance 6 apart.

An invalid composition which violates rule (2) in the definition is the quite similar-looking

$$7+3+1+1+1+2$$

for which $m(c) = 101100001$ and which has 1's at both index 3 and 9.

As n grows relative to k, it becomes more difficult to construct valid k-free compositions using only the propositions.

Example 6. Let $n = 16$, $k = 4$. A 4-free composition can only use parts $\{1, 2, 3, 5, 6, 7, 8\}$. For this example, we provide examples and non-examples which cannot be determined from the propositions alone.

Table 6.3: Valid 4-free compositions.

Composition	Binary String
8512	111100001001
5326	101101000011

Table 6.4: Invalid 4-free compositions.

Composition	Binary String	Violating Indices
53131111	101100010000	4,8
611215	110001000001	2,6

While the definition of a k-free composition at first seems inelegant and unintuitive, the paper will reveal how it arises organically from consideration of k-drop permutations, and how it is one natural generalization of the composition of an integer n using only parts 1 and 2, which is famously counted by the Fibonacci numbers.

Problem 5. Fix some element k, $1 \leq k \leq n$. We wish to count the number of k-free compositions of n.

We now present the first of our main contributions.

Theorem 13. *Problems* 1 *through* 5 *are equivalent, and are all counted by the class of k-Fibonacci numbers defined in Definition 19.*

The proof of Theorem 13 is a consequence of our results in Section 6.5. We give an illustration of which bijections prove which parts of Theorem 13 in Figure 6.1.

6.4 Previous Work and Our Contributions

The k-Fibonacci numbers of Definition 19 which we will consider were originally defined in [14], and it is proven in [15] that these numbers are the permanents of the class of k-tridiagonal matrices defined in Problem 2. Separately, a 2011 note [36] proves that the k-Fibonacci numbers solve the restricted subset problem stated in Problem 3. The k-Fibonacci numbers are sequence number A209434 in the Online Encyclopedia of Integer Sequence (OEIS) database [3], and it is the subset-difference problem which is used to describe them.

Separately again, Baltic in [6] uses matrix permanents to give an algorithm to find the generating function for the number of permutations with certain restrictions. This algorithm does not lend itself to a proof of the general form for the k-Fibonacci generating function, as it involves solving a large system of equations; while we implemented this algorithm in Sage and calculated up to $k = 6$ with this method, the computation required then became prohibitively large, and we will take a more combinatorial approach in the general case. A k-Fibonacci generating function for $k \geq 7$ does not appear in the literature.

6.4.1 Contributions

Our first contribution is to connect these previously disparate results. Our statement and solution to the permutation problem by using the restricted subset problem is new, as is the calculation of the permanent of a k-tridiagonal matrix by using permutations of fixed drop size.

Our second contribution is the statement and proof of the integer composition problem, which is completely novel. The small cases are known: the $k = 1$ case is a standard exercise in elementary combinatorics [35], and it is noted in the OEIS that A006498 and A006500 count the $k = 2$ and $k = 3$ cases respectively. However, there has been no attempt at generalization, and indeed the final paragraph of [14] notes for the $k = 2$ case that it is a surprise A006498 counts both the composition problem and the k-Fibonacci problem. We clear up this mystery by offering not only offering the first explicit bijection between the k-Fibonacci and composition problem in the small k case, but by defining the general form of the compositions.

Perhaps most significantly, the general form and proof for the generating function of the k-Fibonacci numbers is novel. To obtain this generating function, we stated and proved three linear recurrence relations on this class of integers, which as far as we know are also completely novel in their general form.

Finally, we offer a conjecture about the total number of fixed points in k-drop permutations, which is again new. Moreover, our conjecture gives rise to a previously unknown generalized three-dimensional version of Pascal's triangle, which could be of independent interest.

6.5 Combinatorial Proofs

In this section, we provide bijections between the 5 problems we stated in Section 6.3, which combine to give a proof of Theorem 13. We clarify which contributions are ours in Figure 6.1. Solid lines indicate bijections known from [14] and dashed lines are our contributions. Dashed lines with theorem or corollary labels are bijections given explicitly in this section, while dashed lines without labels are implied by other results though not given explicitly here.

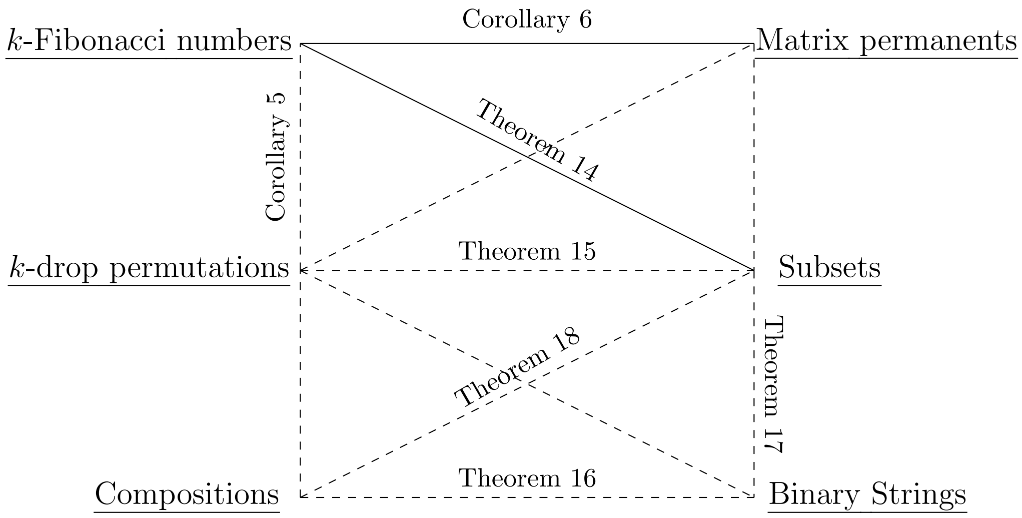


Figure 6.1: A solid line indicates a previously known bijection. A dashed line indicates a new result given in this chapter.

We begin with a result that is already known.

Theorem 14. *The k-Fibonacci number $f_{n,k}$ is the number of subsets on $\{1, 2, \ldots, n-k\}$ such that no two elements have difference k.*

Proof. The proof is given in [36]. □

The following theorem is our first contribution, and explicitly connects the permutation and subset problems.

Theorem 15. *The number of k-drop permutations on n elements is counted by the number of subsets on $n-k$ elements, no two of whose difference is k.*

Proof. Let $\pi(i)$ be an element of a k-drop permutation π. Then, we must have either a fixed point $\pi(i) = i$ so that $|\pi(i) - i| = 0$, or $\pi(i) = i \pm k$ so that $|\pi(i) - i| = |i \pm k - i| = k$. If the second case occurs, then consider the element in position $\pi(i \pm k)$. Since the element $i \pm k$ has already been used, we must have $|\pi(i \pm k) - i \pm k| = k$, and so $\pi(i \pm k) = i$. Thus we can view a k-drop permutation as a permutation whose only non-fixed points occur as part of one swap with one element distance k away.

Intuitively, the restricted subsets of $[n-k]$ encode which elements of π to switch. The restriction that no two elements have difference k ensures that an element part of a swap will not occur as part of a second swap and thus break the $|\pi(i) - i| = k$ condition.

Formally, we define the bijection as follows. Let S be the set of restricted subsets of the above form and let Π be the set of all k-drop permutations. Let $s = \{a_1, \ldots, a_j\} \in S$, $1 \leq j \leq n - k$. Define $f : S \to \Pi$ as

$$f(s) = \begin{cases} \pi(i) = i + k \text{ and } \pi(i+k) = i, i \in s \\ \pi(i) = i, \text{ else} \end{cases}$$

We show f is indeed a bijection.

Let $\pi = \pi(1) \ldots \pi(n) \in \Pi$. We show surjectivity by constructing a subset s from π as follows. If $\pi(1) = 1$, we append nothing to s. If $\pi(1) = k$, we append 1 to s, noting that then we must have $\pi(k) = 1$. By definition of Π, these are the only choices for $\pi(1)$. Working left to right, we continue, appending nothing to s if $\pi(i) = i$ and appending i if $\pi(i) = i + k$. If $\pi(i) = i - k$, we also append nothing; this is simply the second half of a swap already encoded when we appended $i - k$ upon considering $\pi(i - k)$. We stop once we do $\pi(n - k)$, since every element $\pi(i), n - k < i \leq n$ is already determined by the value of $\pi(i - k)$. Since we never append both i and $i + k$, no two elements of s have difference k, and thus $s \in S$ and $f(s) = \pi$.

Let $f(s_1) = \pi, f(s_2) = \sigma \in \Pi$ for some $s_1, s_2 \in S$ and assume $f(s_1) = f(s_2)$. Then we construct the inverse map of both π and σ as above. Since $\sigma = \pi$ fixed points and swaps occur in the same place in both permutations, the same integers do or do not get appended to the respective preimage. Thus $s_1 = s_2$. □

By Theorem 14, we have an exact count for the number of k-permutations of length n.

Corollary 5. *The number of k-drop permutations of length n is counted by the k-Fibonacci number $f_{n,k}$.*

Proof. Immediate from Theorem 15 and Theorem 19. □

Corollary 6. *The k-Fibonacci number $f_{n,k}$ is the permanent of the $n \times n$ square matrix where*

$$M_{ij} = \begin{cases} 1, \ i = j, \ i = k, \ j = k \\ 0, \ \textit{otherwise} \end{cases} .$$

Proof. As stated above, this result is not new; however, we offer a new proof based on the count of k-drop permutations.

Recall that the permanent of an $n \times n$ matrix $M = (m_{ij})$ is given by

$$perm(M) = \sum_{\pi \in S_n} \prod_{i=1}^{n} m_{i,\pi(i)}$$

where S_n is the symmetric group. For any permutation π where $\pi(i) \neq 1, k$ for any $1 \leq i \leq n$, the entire product will be zero by definition of M. Also by definition of M, $\prod_{i=1}^{n} m_{i\pi(i)} = 1$ if and only if $\pi(i) = 1$ or $\pi(i) = k$ for all i. As this is the definition of a k-drop permutation, the permanent is equal to the number of k-drop permutations, which is $f_{n,k}$ by Theorem 15.

□

The class of k-free compositions, k-free binary strings, and k-free subsets are all closely related, and, as we show below, are all counted by $f_{n,k}$. We offer explicit bijections between these class of objects.

Theorem 16. *The number of k-free compositions of n is the same as the number of k-free binary strings of length $n - k$.*

Proof. The definition of a k-free composition already implies a relationship between these two objects; by definition, we cannot have more k-free compositions than k-free binary strings, so the map m defined above is injective.

To show m is surjective, consider a k-free binary string $b = b_1 b_2 \ldots b_{n-k}$. Construct a composition c as follows.

First, find the first b_j where $b_j = 1$; then find the first index $r > j$ where $b_r = 0$. Let $c_j = k + (r - j)$ and $c_i = 1$ for $1 \leq i \leq j - 1$. Since $c_j > k$ is clear, then the first non-1 element of c is greater than k, as required by property 1 of the k-free composition definition.

Next, starting at b_r, section b off into groups where each group has as many 0's as possible and then all the 1's before the next 0. If the chunk has length less than k including at least one 1 following the 0's, append $r + 1$, where r is the number of 1's, to c. Since $r < k - 2$ (because the chunk has length at most $k - 1$ with at least one preceeding 0), we have appended something in the range $2, 3, 4, \ldots, k - 1$ to c. If there are no 1's after the 0 trail (i.e., a run of 0's ends the binary string), append r 1's to c, where r is the number of zeros.

If the chunk has length $r > k$, consider two cases. If the chunk has exactly k 0's following by some number of 1's, append r. Note $r < 2k$, otherwise b would not be k-free. If the chunk has strictly more than k 0's, call the number of 1's e. Append $r - e - k$ $1's$ to c followed by the integer $e + k$. Again, since b is k-free, $e < k$, and thus the $e + k$ we append is less than $2k$.

Thus we have shown c satisfies property 1 of the k-free composition definition. Additionally, any c constructed in this way will satisfy property 2 in the definition of k-free compositions, since it was constructed from a k-free binary string. Thus m is bijective.

□

The next bijection is far more straightforward.

Theorem 17. *The number of subsets on $n-k$ such that no two elements have difference k is the same as the number of k-free binary strings of length $n - k$.*

Proof. Let s be a subset of the desired form and let $b = b_1 \dots b_{n-k}$ be a k-free binary string. Define $m : b \to s$ as

$$m(b_i) = \begin{cases} i, b_i = 1 \\ \emptyset, b_i = 0 \end{cases}$$

Clearly, the image of m is a subset of the desired form, since having two elements of s with difference k implies there were two 1's distance k apart in the k-free string in the preimage.

Furthermore, m is a bijection. To show m is surjective, let $s = \{s_1, s_2, \dots, s_j\}$, $j \leq n-k$, be a subset on $n - k$ such that no two elements have difference k. Construct a binary string $b = b_1 b_2 \dots b_{n-k}$ as follows: for each s_i, assign $b_i = 1$. For any element j which does not appear in s, let $b_j = 0$. Since $s_i - s_j \neq k$ for any i, j, no two 1's in b will be distance k apart.

To show m is injective, let $m(b_1) = S_1 = S_2 = m(b_2)$ for subsets s_1, s_2 and binary strings b_1, b_2. We construct the inverse map as above. Since the same elements appear in S_1

and S_2, the same locations in b_1, b_2 have 1's, which determines where the zeros fall, so $b_1 = b_2$. □

Corollary 7. *There are $f_{n,k}$ k-free binary strings of length $n - k$.*

Proof. Immediate from Theorem 17 and Theorem 14. □

Corollary 8. *There are $f_{n,k}$ k-free compositions of n.*

Proof. Immediate from Theorem 16 and Theorem 17. □

The following theorem is already implied by the above results. However, for your combinatorial entertainment, we offer a direct bijective proof as well.

Theorem 18. *The number of subsets on $n - k$, no two of whom have difference k, is the same as the number of k-free compositions of n. The k-Fibonacci number $f_{n,k}$ counts both these objects.*

Proof. Clearly the result is true by Theorems 16, 17, and 14, but we offer a bijective proof, inspired by though not directly using the count of k-drop permutations.

Construct a map p from k-free compositions c to subsets s as follows. Consider a k-free composition $c = (c_1, \ldots, c_h)$; we will construct a subset $s = \{s_1, \ldots, s_j\}$ from c. Throughout, let $r_i = \sum_{j=1}^{i-1} c_j$ for some specified index i.

Find the first index i where $c_i > 1$. Let $s_1 = r_i + 1, s_2 = r_i + 2, \ldots, s_{c_i - k} = r_i + c_i - k$. Then continue scanning c. For every $c_i > k$, append $r_i + 1, r_i + 2 \ldots r_i + c_i - k$ to s. For every $1 < c_i < k$, append $r_i + c_i - k, r_i + c_i - k - 1, \ldots, r_i + c_i - k - (c_i - 2) = r_i - k + 2$. If $c_i = 1$, append nothing to s and move on to c_{i+1}.

The image of p is in fact a subset with the desired property; note that violating the k-free subset property is equivalent to violating the k-free string property in the binary string $m(c)$.

p is surjective. To show this, we show that for some subset S such that no 2 elements have difference k, there is some k-free composition c such that $S = p(c)$. We will do this by constructing a binary string b from S and then finding c such that $m(c) = b$ according to Definition 20.

Define a run of S as one or more consecutive elements, and the run length r as the number of elements in the run. (Thus we, somewhat clunkily, define an element of $s \in S$ with $s+1, s-1 \notin S$ as a run of length 1.)

Consider the first run $s_1, s_2, \ldots, s_{r_1}$ of some length $1 \leq r_1 \leq n-k$. Say $s_1 = i_1$; let $b_j = 0$ for all $j < i_1$ and let $b_{i_1} = b_{i_1+1} = \cdots = b_{i_1+r_1-1} = 1$. Since $s_h - s_g \neq k$ for any h, g, no 1s of b are distance k apart.

Continue in this fashion and look for the next run. If there is no next run (e.g. there are no more elements in the subset), we pad $c_i = 1$ the rest of c. If there is a second run, call this run $s_j, s_{j+1}, \ldots, s_{j+r_2-1}$ of length r_2. Say $s_j = i_2$. Let $b_{i_2} = b_{i_2+1} = \ldots b_{i_2+r_2-1} = 1$ and $b_j = 0$, $i_1 + r_1 \leq < i_2$. Again, since $s_h - s_g \neq k$ for any h, g, no 1s of b are distance k apart.

Iterating, we eventually end up with a binary string b, and we can easily construct a k-free composition c according to the map in the proof of Theorem 16. Since given any subset S with no two elements with difference k, we can construct a k-free c such that $S = p(m(c))$, p is surjective.

Following this same method show p is also injective, since any $S_1 = S_2$ will give identical $b_1 = b_2$ and thus $c_1 = c_2$.

□

As Theorems 19 and 15 imply, there is indeed a direct bijection between restricted permutations and restricted compositions of this type. Similarly to the restricted subset case, one can read off fixed points and the k-drops in the permutation problem directly from the k-compositions. While we do not walk through the formal proof, we present the bijection here.

Intuitively, a 1 in the composition corresponds to a fixed point in the permutation; an element $i > k$ in the composition corresponds to a chunk of the permutation where, for any non-fixed point element j swapped with element $j-k$, then $j-k$ is also contained within the chunk; and an element $i < k$ in the composition corresponds to a chunk of the permutation where, for any non-fixed point element j swapped with some element $j-k$, $j-k$ is not contained within the chunk.

Formally, define a map f from k-free compositions to k-drop permutations as follows. Consider a k-free composition $c = (c_1, \ldots, c_h)$; we will construct a length n permutation $p = \{p_1 \ldots p_n\}$ from c. There are 3 cases.

Let $r_i = \sum_{j=0}^{i-1} c_j$. Then:

1. If $c_i = 1$, then $p_{1+r+i} = 1 + r_i$.
2. If $c_i > k$, then consider the chunk from p_{r_i+1} to $p_{1+r_i+c_i}$. Starting with $p_{1+r_i+c_i}$, swap with $p_{1+r_i+c_i-k}$. Continue, until reaching some j such that $1+r_i+c_i-k-j < 1+r_i$.
3. If $c_i < k$, swap p_{r+1+j} with $p_{r+1+j-k}$ for every $2 \leq j \leq c_i$.

It can be shown this is in fact a bijection.

6.6 Examples

Example 7 (Subsets and Permutations)**.** Let $n = 12, k = 4$. The following are the correspondences between some subsets on 8 elements with no two elements having difference 4, and 4-drop permutations of length 12.

Table 6.5: Subsets and permutations for the $n = 7, k = 4$ case.

Subset	Permutation
$\{1, 2, 4\}$	5 6 3 8 1 2 9 4 10 11 12
$\{3, 5, 6, 8\}$	1 2 7 4 9 10 3 12 5 6 11 8
$\{1, 2, 3, 4\}$	5 6 7 8 1 2 3 4 10 11 12
$\{2\}$	1 6 3 4 5 2 7 8 9 10 11 12

Let $n = 6, n = 2$. There are $f_{n,k} = f_3 f_3 = 9$ total 2-drop permutations. This is all of them, with their corresponding subsets.

Table 6.6: All subsets and permutations for the $n = 6, k = 2$ case.

Subset	Permutation
$\{\}$	1 2 3 4 5 6
$\{1\}$	3 2 1 4 5 6
$\{2\}$	1 4 3 2 5 6
$\{3\}$	1 2 5 4 3 6
$\{4\}$	1 2 3 6 5 4
$\{1, 2\}$	3 4 1 2 5 6
$\{2, 3\}$	1 4 5 2 3 6
$\{3, 4\}$	1 2 5 6 3 4
$\{1, 4\}$	3 2 1 6 5 4

Example 8 (Compositions and Permutations)**.** Now we illustrate the bijection between k-free compositions and k-drop permutations. Similarly to the previous example, the compositions illustrate which elements of the permutation to swap.

We begin by showing all $f_4 f_3 = 15$ examples for the $n = 7, k = 2$ case.

Table 6.7: All permutations and compositions for the $n = 7, k = 2$ case.

Permutation	Composition
1 2 3 4 5 6 7	1+1+1+1+1+1+1
3 2 1 4 5 6 7	3+1+1+1+1
1 4 3 2 5 6 7	1+3+1+1+1
1 2 5 4 3 6 7	1+1+3+1+1
1 2 3 6 5 4 7	1+1+1+3+1
1 2 3 4 7 6 5	1+1+1+1+3
3 4 1 2 5 6 7	4+1+1+1
1 4 5 2 3 6 7	1+4+1+1
1 2 5 6 3 4 7	1+1+4+1
1 2 3 6 7 4 5	1+1+1+4
3 2 1 6 7 4 5	3+4
3 4 1 2 7 6 5	4+3
3 2 1 6 5 4 7	3+3+1
1 4 3 2 7 6 5	1+3+3
3 2 1 4 7 6 5	3+1+3

For a larger example, here are a few instances of the $n = 13, k = 5$ case.

Table 6.8: Some permutations and compositions for the $n = 13, k = 5$ case.

Permutation	Composition
1 7 3 4 5 6 2 13 9 10 11 12 8	7+6
6 2 8 4 5 1 12 3 9 10 11 7 13	6+2+1+1+2+1
6 7 8 4 5 1 2 3 9 10 1 12 13	8+1+1+1+1+1
1 2 3 9 5 11 12 13 4 6 7 8	1+1+1+6+4
6 7 3 9 10 1 2 13 4 5 11 12 8	7+3+1+2

Example 9 (Compositions and Permutations: The Deception of Small Examples)**.** The bijection between compositions and permutations is not immediately apparent for examples with $k \leq 3$. Indeed, these examples may appear somewhat mysterious, while in fact they are simply examples of the general case.

Consider $k = 1$. $2k = 2$, so we construct compositions using only parts 1 and 2. (Note that since $k = 1$ the definition could imply that we find the number of compositions without 1, but since we defined a k-free composition as always including 1, we resolve the conflict by choosing to include it.) It is already well-known, and a standard exercise in elementary combinatorics [35], that the number of such compositions is the Fibonacci number f_n. (Indeed, these compositions are sometimes called Fibonacci compositions). Here, we use our definition of k-free compositions to show that these Fibonacci compositions are 1-free, providing a roundabout proof for the standard exercise.

Let $c = (c_1, \ldots c_j)$ be a composition of n using only parts 1 and 2. Then where m is the mapping to binary strings, $m(1) = 0$ and $m(2) = 01$. Thus, no matter the order of the 1's and 2's in c, we will never have a 11 in $m(c)$, and thus c is 1-free, which we know is counted by the Fibonacci number f_n.

Consider $k = 2$. In this case, $2k = 4$. Thus we must construct compositions using only parts $\{1, 3, 4\}$. By Propositions 15 and 16, there are no restrictions on either of 3 or 4 (both greater than k) or 1. Thus a 2-free composition is any composition on $1, 3, 4$. This is the characterization of the $k = 2$ case found in [14] and OEIS A006498, although no bijection from the characterization to either permutations or subsets is given.

Consider $k = 3$. In this case, $2k = 6$. Thus our compositions must contain only

$\{1, 2, 4, 5, 6\}$. There are no restrictions on $4, 5, 6$, but there are restrictions on 2. 2 can appear after 4, since $2 + 4 = 2k$; 2 can also appear after 2 (or any number of 2's), since this corresponding binary string to 22 is 0101 and the 1's will always be 2 indices apart. 2 cannot appear after 5 or 6, both by Proposition 17 and from the binary sequences corresponding to $52 = 0001101$ and $62 = 00011101$. It remains to consider whether 2 can come after a 1. To guarantee compliance with the k-free sequence criterion, we would need at least two 1's to precede the 2. However, 112 gives the same binary sequence as 4, so we would just write a 4 instead. The same is true as we increase the number of 1's: instead of $1 \ldots 12$ with p 1's, we write $p - 2\ 0's$ and a 4.

Thus, a k-free composition uses parts $1, 2, 4, 5, 6$ such that 2 can only come after 4 or another 2. This is precisely the characterization of the $k = 3$ case found in the OEIS A006500 (although, again, no bijection to the permutation is given).

After $k = 4$, a direct characterization for k-free compositions becomes less clear, and for this k and larger we continue to use the binary sequence characterization instead.

Example 10 (Subsets and Compositions)**.** Here we show some examples of the run-length direct bijection between subsets and compositions given in Theorem 18.

First, consider $k = 1$; as above, this counts subsets on $n-1$ with no consecutive elements, and compositions of n using only parts 1 and 2. We know that the number of both such objects is a Fibonacci number. Here, we simply illustrate our bijection between them. Let $S = \{s_1, \ldots, s_r\}$, with the s_i in increasing order, be a subset with no consecutive elements. Consider $s_i - s_{i-1}$ for each $1 \leq i \leq r$. If $s_i - s_{i-1} = 2$, we append 2. If $s_i - s_{i-1} = m > 2$, we append $m - 1$ 1's followed by a 2. Thus we have constructed a composition using only parts 1 and 2, which is sufficient for a 1-free composition as argued in Example 9.

Now consider $k = 2$. As in the $k = 1$ case, consider the consecutive differences $s_i - s_{i-1}$ for $S = \{s_1, \ldots, s_r\}$ with no two elements having difference 2.

Now let $n = 7, k = 3$. We know there are $f_{7,3} = f_2 f_2 f_3 = 12$ subsets on $n - k = 4$ with no difference $k = 3$, and 3-free compositions on 7. They are:

- $\{\} \leftrightarrow 1 + 1 + 1 + 1 + 1 + 1 + 1$
- $\{1\} \leftrightarrow 4 + 1 + 1 + 1$
- $\{2\} \leftrightarrow 1 + 4 + 1 + 1$

- $\{3\} \leftrightarrow 1+1+4+1$
- $\{4\} \leftrightarrow 1+1+1+4$
- $\{1,2\} \leftrightarrow 5+1+1$
- $\{2,3\} \leftrightarrow 1+5+1$
- $\{3,4\} \leftrightarrow 1+1+5$
- $\{2,4\} \leftrightarrow 5+2$
- $\{1,3\} \leftrightarrow 4+2+1$
- $\{1,2,3\} \leftrightarrow 6+1$
- $\{2,3,4\} \leftrightarrow 1+6$

Example 11 (A Big Example)**.** We construct a table of all 4 correspondences for $n = 11, k = 4$. There are $f_{11,4} = (2)(3)(3)(3) = 54$ such elements.

Table 6.9: All bijections, $k = 4, n = 11$.

Permutation	Subset	Binary String	Composition
1 2 3 4 5 6 7 8 9 10 11	{}	0000000	1+1+1+1+1+1+1
5 2 3 4 1 6 7 8 9 10 11	{1}	1000000	5+1+1+1+1+1+1
1 6 3 4 5 2 7 8 9 10 11	{2}	0100000	1+5+1+1+1+1+1
1 2 7 4 5 6 3 8 9 10 11	{3}	0010000	1+1+5+1+1+1+1
1 2 3 8 5 6 7 4 9 10 11	{4}	0001000	1+1+1+5+1+1+1
1 2 3 4 9 6 7 8 5 10 11	{5}	0000100	1+1+1+1+5+1+1
1 2 3 4 5 10 7 8 9 6 11	{6}	0000010	1+1+1+1+1+5+1
1 2 3 4 5 6 11 8 9 10 7	{7}	0000001	1+1+1+1+1+1+5
5 6 3 4 1 2 7 8 9 10 11	{1,2}	1100000	6+1+1+1+1+1
5 2 7 4 1 6 3 8 9 10 11	{1,3}	1010000	5+2+1+1+1+1
5 2 3 8 1 6 7 4 9 10 11	{1,4}	1001000	5+1+2+1+1+1
5 2 3 4 1 10 7 8 9 6 11	{1,6}	1000010	5+1+1+1+2+1
5 2 3 4 1 6 11 8 9 10 7	{1,7}	1000001	5+1+1+1+1+2
1 6 7 4 5 2 3 8 9 10 11	{2,3}	0110000	1+6+1+1+1+1
1 6 3 8 5 2 7 4 9 10 11	{2,4}	0101000	1+5+2+1+1+1
1 6 3 4 9 2 7 8 5 10 11	{2,5}	0100100	1+5+1+2+1+1
1 6 3 4 5 2 11 8 9 10 7	{2,7}	0100001	1+5+1+1+1+2
1 2 7 8 5 6 3 4 9 10 11	{3,4}	0011000	1+1+6+1+1+1
1 2 7 4 9 6 3 8 5 10 11	{3,5}	0010100	1+1+5+2+1+1
1 2 7 4 5 10 3 8 9 6 11	{3,6}	0010010	1+1+5+1+2+1
1 2 3 8 9 6 7 4 5 10 11	{4,5}	0001100	1+1+1+6+1+1
1 2 3 8 5 10 7 4 9 6 11	{4,6}	0001010	1+1+1+5+2+1
1 2 3 8 5 6 11 4 9 10 7	{4,7}	0001001	1+1+1+5+1+2
1 2 3 4 9 10 7 8 5 6 11	{5,6}	0000110	1+1+1+1+6+1
1 2 3 4 9 6 11 8 5 10 7	{5,7}	0000101	1+1+1+1+5+2
1 2 3 4 5 10 11 8 9 6 7	{6,7}	0000011	1+1+1+1+1+6
5 6 7 4 1 2 3 8 9 10 11	{1,2,3}	1110000	7+1+1+1+1
5 6 3 8 1 2 7 4 9 10 11	{1,2,4}	1101000	6+2+1+1+1
5 6 3 4 1 2 11 8 9 10 7	{1,2,7}	1100001	6+1+1+1+2
5 2 7 8 1 6 3 4 9 10 11	{1,3,4}	1011000	5+3+1+1+1
5 2 7 4 1 10 3 8 9 6 11	{1,3,6}	1010010	5+2+1+2+1
5 2 3 8 1 10 7 4 9 6 11	{1,4,6}	1001010	5+1+2+2+1
5 2 3 8 1 6 11 4 9 10 7	{1,4,7}	1001001	5+1+2+1+2
5 2 3 4 1 10 11 8 9 6 7	{1,6,7}	1000011	5+1+1+1+3
1 6 7 8 5 2 3 4 9 10 11	{2,3,4}	0111000	1+7+1+1+1
1 6 7 4 9 2 3 8 5 10 11	{2,3,5}	0110100	1+6+2+1+1
1 6 3 8 9 2 7 4 5 10 11	{2,4,5}	0101100	1+5+3+1+1
1 6 3 8 5 2 11 4 9 10 7	{2,4,7}	0101001	1+5+2+1+2
1 6 3 4 9 2 11 8 5 10 7	{2,5,7}	0100101	1+5+1+2+2
1 2 7 8 9 6 3 4 5 10 11	{3,4,5}	0011100	1+1+7+1+1
1 2 7 8 5 10 3 4 9 6 11	{3,4,6}	0011010	1+1+6+2+1
1 2 7 4 9 10 3 8 5 6 11	{3,5,6}	0010110	1+1+5+3+1
1 2 3 8 9 10 7 4 5 6 11	{4,5,6}	0001110	1+1+1+7+1
1 2 3 8 9 6 11 4 5 10 7	{4,5,7}	0001101	1+1+1+6+2
1 2 3 8 5 10 11 4 9 6 7	{4,6,7}	0001011	1+1+1+5+3
1 2 3 4 9 10 11 8 5 6 7	{5,6,7}	0000111	1+1+1+1+7
5 6 7 8 1 2 3 4 9 10 11	{1,2,3,4}	1111000	8+1+1+1
5 6 3 8 1 2 11 4 9 10 7	{1,2,4,7}	1101001	6+2+1+2
5 2 7 9 1 10 3 8 4 6 11	{1,3,4,6}	1011010	5+3+2+1
5 2 3 9 1 10 11 8 4 6 7	{1,4,6,7}	1001011	5+1+2+3
1 6 7 8 9 2 3 4 5 10 11	{2,3,4,5}	0111100	1+8+1+1
1 6 3 8 9 2 11 4 5 10 7	{2,4,5,7}	0101101	1+5+3+2
1 2 7 8 9 10 3 4 5 6 11	{3,4,5,6}	0011110	1+1+8+1
1 2 3 8 9 10 11 4 5 6 7	{4,5,6,7}	0001111	1+1+1+8

6.7 Generating Function

The previous sections provided new combinatorial interpretations and new uses of the k-Fibonacci numbers, while connecting previously disparate results.

The purpose of the following section is to focus in more narrowly on the k-Fibonacci numbers themselves. Specifically, we state and prove the previously unknown general form of the k-Fibonacci generating function.

6.7.1 Introduction and Main Result

The late Herbert Wilf wrote that "a generating function is a clothesline on which we hang up a sequence of numbers for display." More specifically, the generating function of a sequence $\{a_n\}$ is defined by $A(x) = \sum_{n\geq 0} a_n x^n$. Generating functions have all sorts of fascinating properties. Informally, the denominator of a rational generating function $A(x)$ for a sequence a_n reveals the recurrence relation on $\{a_n\}$. Specifically, we have from Stanley [35] that the following conditions are equivalent.

Theorem 19 ([35])**.** *Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be a fixed sequence of complex numbers, $d \geq 1$ and $a_d \neq 0$. The following conditions on a function $f : \mathbb{N} \to \mathbb{C}$ are equivalent.*

1. $$\sum_{n\geq 0} f(n)x^n = \frac{P(x)}{Q(x)}$$

   where $Q(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_d x^d$ and $P(x)$ is a polynomial in x of degree less than d.

2. *For all $n \geq 0$,*

   $$f(n+d) + \alpha_1 f(n+d-1) + \alpha_2 f(n+d-2) + \cdots + \alpha_d f(n) = 0.$$

It is stated specifically in [14] that the general form of a generating function for the k-Fibonacci numbers for all $k > 3$ is an open problem. While generating functions up to $k = 6$ have since been given on the OEIS (see A209434 for the link to all $k = 1$ through $k = 6$; specifically A208743 has the $k = 6$ case), a generating function or recursion remained elusive in its general form. The following theorem gives such a general form for the first time.

Theorem 20. *The generating function for the k-Fibonacci numbers $f_{k,n}$, denoted as $F_k(x)$, satisfies*

$$F_k(x) = \frac{\sum_{j=0}^{k-3}\sum_{i=0}^{k-1} N(k-1,i,j)x^{j+ik}}{(1-x-x^2)(\sum_{i=0}^{k-1}\hat{b}_{k-1,i}x^{ik})}$$

where $\hat{b}_{k,i}$ is the signed Fibonomial coefficient of Definition 21 and the $N(a,b,c)$ is the recursive three-dimentional array defined by

$$\begin{aligned}
&N(a,0,c) = (-1)^c f_{c(a-1),a-1} + \sum_{j=1}^{c}(-1)^{j+1}b_{a+j-1,j}N(a,2,c-j)\\
&N(a,1,c) = 0\\
&N(a,b,c) = (-1)^{c+1}f_{c(a-1)+b-2,a-1} + \sum_{j=1}^{c}(-1)^{j}b_{a+j-1,j}N(a,b,c-j), b \geq 2
\end{aligned}$$

with initial condition

$$\begin{aligned}
N(a,0,0) &= 1\\
N(a,1,0) &= 0\\
N(a,b,0) &= \begin{cases} -1, \ 2 \leq b \leq a \\ 0, \ b > a. \end{cases}
\end{aligned}$$

We give the proof of Theorem 20 in the proof of Corollary 9. Essentially, the proof is a consequence of three lemmas, which we spend the next three sections stating and proving.

6.7.2 The Fibonomials

The Fibonomials are a number triangle with a series of fascinating properties; for instance, see [7] and its references. Intuitively, the Fibonomials arise from replacing every integer i in the definition of the binomial coefficient $\binom{n}{k}$ with its corresponding Fibonacci number f_i. A more precise definition is below.

Definition 21. The Fibonomials are defined by

$$b_{n,k} = \frac{f_{n-1} \cdots f_{n-k}}{f_{k-1} \cdots f_1}$$

Note that since we index from $f_0 = 1$ (the some Fibonomial definitions in the literature use $f_0 = 0$) we take $f_{-1} = 0$ for formality's sake.

Other true, but perhaps not immediately obvious, facts are below.

Theorem 21. *The following are true of the Fibonomial coefficients $b_{n,k}$.*

1. *$b_{n,k}$ is always an integer.*
2. *The Fibonomial coefficients satisfy the recurrence $b_{n,k} = f_{n-k-2}b_{n-1,k-1} + f_k b_{n-1,k}$.*

The first few Fibonomials are as follows.

Table 6.10: The first few Fibonomials.

n/k	0	1	2	3	4	5	6	7	8	9
0	1									
1	1	1								
2	1	1	1							
3	1	2	2	1						
4	1	3	6	3	1					
5	1	5	15	15	5	1				
6	1	8	40	60	40	8	1			
7	1	13	104	260	260	104	13	1		
8	1	21	273	1092	1820	1092	273	21	1	
9	1	34	714	4641	12376	12376	4641	714	34	1

We will use a signed version of the Fibonomials for the generating function.

Definition 22. The signed Fibonomials $\hat{b}_{n,k}$ are

$$\hat{b}_{n,k} = (-1)^{\lfloor \frac{k}{2} \rfloor} b_{n,k}.$$

The first few signed Fibonomials are listed below.

Table 6.11: The first few signed Fibonomials $\hat{b}_{n,k}$.

n/k	0	1	2	3	4	5	6	7	8	9
0	1									
1	1	1								
2	1	1	-1							
3	1	2	-2	-1						
4	1	3	-6	-3	1					
5	1	5	-15	-15	5	1				
6	1	8	-40	-60	40	8	-1			
7	1	13	-104	-260	260	104	-13	-1		
8	1	21	-273	-1092	820	1092	-273	-21	1	
9	1	34	-714	-4641	12376	12376	-4641	-714	34	1

Interestingly, the signed Fibonomial triangle gives the coefficients of a signed version of the Fibonomial generating function.

Theorem 22. *Let $\hat{b}_{n,k}$ be an entry of the signed Fibonomial triangle. Then*

$$B_n(x) := \sum_{i\geq 0}(-1)^i b_{n,i}x^i = \frac{1}{p(n+1,x)},$$

where $p(n,x) = \sum_{i\geq 0}\hat{b}_{n,i}x^i$.

Proof. We know from the OEIS A055870 that for the offset signed Fibonacci triangle $c_{n,k}$ defined by $c_{n,k} = (-1)^{\lfloor\frac{(n+1)}{2}\rfloor}b_{n,k}$, we have

$$C_n(x) := \sum_{i\geq 0} c_{n,i}x^i = \frac{1}{p(n+1,x)},$$

where $q(n,x) = \sum_{i\geq 0} c_{n,i}x^i$. Furthermore, note that $\hat{b}_{n,k} = (-1)^k c_{n,k}$ and $q(n,x) = p(n,-x)$.

Thus,

$$B_n(x) = C_n(-x) = \frac{1}{q(n+1,-x)} = \sum_{i\geq 0}(-1)^i b_{n,i}x^i = \frac{1}{p(n+1,x)}$$

as desired.

□

6.7.3 The Denominators: Some Lemmas

As we know from Theorem 19, the denominator of a generating function gives the recursion for the sequence. Thus, once we find a recursion for the k-Fibonacci numbers, we know the denominator of the generating functions. We build this recursion through a series of lemmas below, culminating in the recursion given in Theorem 23.

Lemma 6. *Where f_n is the nth Fibonacci number,*

1. $f_n^2 = f_{n-1}f_n + f_{n-1}f_{n-1} + (-1)^n$
2. $f_nf_{n-1} + f_n^2 = f_nf_{n+1}$

The proof of (2) is trivial from the Fibonacci recursion, and one proof of (1) can be found in section 1.2 of [7].

Using Lemma 6, we can build a similar identity for the product of Fibonacci numbers.

Lemma 7. *Where f_j is the jth Fibonacci number, m is an integer, and $0 \leq i \leq m-1$,*

$$f_j^{m-i-2}f_{j+1}^{i+2} = f_j^{m-i}f_{j+1}^{i} + f_j^{m-i-1}f_{j+1}^{i+1} + (-1)^{j-1}f_j^{m-i-2}f_{j+1}^{i}$$

if $0 \leq i \leq m-2$

and

$$f_jf_{j+1}^{m-1} + f_{j+1}^{m} = f_{j+1}^{m-1}f_{j+2}$$

if $i = m-1$.

Proof. This proof is straightforward from the Fibonacci recursion. If $0 \leq i \leq m-2$,

$$\begin{aligned} f_j^{m-i} f_{j+1}^i + f_j^{m-i-1} f_{j+1}^{i+1} &= f_j^{m-i-2} f_{j+1}^i (f_j^2 + f_{j+1} f_j) \\ &= f_j^{m-i-2} f_{j+1}^i (f_{j+1}^2 + (-1)^j) && \text{(by Lemma 6)} \\ &= f_j^{m-i-2} f_{j+1}^{i+2} + (-1)^j f_j^{m-i-2} f_{j+1}^i \end{aligned}$$

If $i = m-1$,

$$\begin{aligned} f_j f_{j+1}^{m-1} + f_{j+1}^m &= f_{j+1}^{m-1}(f_j + f_{j+1}) \\ &= f_{j+1}^{m-1} f_{j+2} \end{aligned}$$

□

Lemma 8 gives an identity on the k-Fibonacci numbers using the k and $k-2$ Fibonacci numbers. Note this is not yet a recursion in only the k-Fibonacci numbers, since this lemma uses a $f_{n,k-2}$ term.

Lemma 8. *Let*

$$\alpha(n,k) = \frac{(-1)^{\lfloor n/k \rfloor} + (-1)^{\lfloor (n+1)/k \rfloor}}{2}$$

Then

$$f_{n+2,k} = f_{n+1,k} + f_{n,k} + \alpha(n-k,k) f_{\lfloor n/k \rfloor (k-2) + n \ mod \ (k), k-2} \tag{6.1}$$

Proof. The proof follows from Lemma 7. Our main task is to translate the statement of Lemma 7 from Fibonacci products to k-Fibonacci numbers, being sure to track the indices appropriately.

First, we consider the signs of the Fibonacci terms. When n mod $k = 0$, then

$$\alpha(n-k,k) = \frac{(-1)^{\lfloor (n-k)/k \rfloor} + (-1)^{\lfloor (n-k+1)/k \rfloor}}{2} = \frac{(-1)^{\lfloor (n/k - 1/k \rfloor} + (-1)^{\lfloor n/k \rfloor}}{2} = 0,$$

since the exponent of the first -1 will always be one less than the exponent of the second -1. Then equation 6.1 follows immediately from the $i = m-1$ case of Lemma 7 with $m = k$, since $f_{n,k} = f_{n/k}^k$ when k divides n.

Now consider $n \mod k = r, 0 < r < k$. The exponent of the first -1 in α is

$$\left\lfloor \frac{n-k}{k} \right\rfloor = \left\lfloor \frac{n-r}{k} + \frac{r}{k} - 1 \right\rfloor = \frac{n-r}{k} - 1 + \left\lfloor \frac{r}{k} \right\rfloor = \frac{n-r}{k} - 1$$

and the second is

$$\left\lfloor \frac{n-k+1}{k} \right\rfloor = \left\lfloor \frac{n-r}{k} + \frac{r}{k} - 1 + \frac{1}{k} \right\rfloor = \frac{n-r}{k} + -1 + \left\lfloor \frac{r}{k} \right\rfloor = \frac{n-r}{k} - 1$$

so the parity of the exponents is identical. Furthermore, this identical parity occurs in length $k-1$ chunks that alternate sign. That is, if $\frac{n-1}{k} - 1$ is even, then $\frac{n-r}{k} - 1$ is even for all $0 < r < k$; same if $\frac{n-r}{k} - 1$ is odd. Also, if $\frac{n-r}{k} - 1$ is even, then $\frac{n-r+k}{k} - 1 = \frac{n-r}{k}$ is odd, and vice versa.

Consider the j in Lemma 7. If j is odd, then $(-1)^{j-1} = 1$. Furthermore, by definition of the k-Fibonacci numbers, $n - r = jk$, and thus

$$\frac{n-r}{k} - 1 = \frac{jk}{k} - 1 = j - 1$$

which must be even and thus $(-1)^{\frac{n-r}{k}-1} = 1$, so $\alpha(n-k-1, k) = 1$. Similarly, $\alpha(n-k-1, k) = -1$ when j is even. Thus, the signs in equation 6.1 are the same as the signs in Lemma 7.

Now we consider the Fibonacci terms themselves. By definition, $f_{n,k} = f_m^{k-r} f_{m+1}^r$ with $n = mk + r, 0 \leq r < n$. We considered the $r = 0$ case above, so now assume $0 < r < n$. Then $f_{n+1,k} = f_m^{k-r-1} f_{m+1}^{r+1}$ since $m(k-r-1) + (m+1)(r+1) = mk + r + 1 = n + 1$ and thus the equation 6.1 terms match up to Lemma 7 in all but the all but the $-(1)^j$ term in Lemma 7.

Thus we lastly consider $f_m^{k-r-2} f_{m+1}^r$ of Lemma 7. Where $n = mk + r$ as usual, we have

$$m = \frac{n-r}{k} = \left\lfloor \frac{n}{k} \right\rfloor$$

and furthermore $r = n \mod k$. This gives

$$(k-r-2)m + (m+1)r = m(k-2) + r$$

by the k-Fibonacci definition. Thus $m(k-2) + r = \left\lfloor \frac{n}{k} \right\rfloor (k-2) + n \mod k$, as desired.

□

The next lemma will be extremely important in the generation function proof. A version for only the pure Fibonacci powers is already known in the literature [30] but this proof is the first for the full sequence of k-FIbonacci numbers. We will use the existing paper as a base case in the proof.

Lemma 9. *Let $c_{n,k} = (-1)\hat{c}_{n,k}$ for $n \geq 1$, $c_{n,k} = 1$, $n = 0$ where $\hat{c}_{n,k} = (-1)^{\lfloor (k+1)/2 \rfloor + 1} b_{n,k}$ for the Fibonomials $b_{n,k}$ defined above. Then*

$$f_{n,k} = \sum_{j=1}^{k+1} f_{n-jk,k} c_{k+1,j}.$$

Proof. The proof is through double induction on both n and k. For the $k = 1$ base case, since $f_{n,1} = f_{n-1,1} + f_{n-2,1}$ and $c_{0,1} = c_{0,2} = 1$, the lemma is true by the Fibonacci recursion.

For a base case in n, recall from [30] that the statement is true if $f_{n,k}$ is the power of some Fibonacci number, which occurs exactly when $n \bmod k = 0$. Thus, the statement is true for $n = k(k+1)$, where we have $f_{n,k} = f_{k+1}^k$. Since the recursion in the lemma statement has depth $k(k+1)$, this is the smallest possible n we can take for a base case.

Now we proceed by strong induction on n and k; assume the statement is true up to $n+1, k$ and consider $f_{n+2,k}$. By Lemma 8:

$$\begin{aligned}
f_{n+2,k} &= f_{n+1,k} + f_{n,k} + \alpha(n-k,k) f_{\lfloor n/k \rfloor (k-2) + n \bmod k, k-2} \\
&= \sum_{j=1}^{k+1} f_{n+1-jk,k} c_{k,j} + \sum_{j=1}^{k+1} f_{n-jk,k} c_{k,j} + \alpha(n-k,k) f_{\lfloor n/k \rfloor (k-2) + n \bmod k, k-2} \\
&= \sum_{j=1}^{k+1} (f_{n+2-jk,k} + \alpha(n-k-jk,k) f_{\lfloor \frac{n-jk}{k} \rfloor (k-2) + (n-jk) \bmod k, k-2}) c_{k,j} \\
&+ \alpha(n-k,k) f_{\lfloor n/k \rfloor (k-2) + n \bmod k, k-2} \\
&= \sum_{j=1}^{k+1} f_{n+2-jk,k} c_{k,j} + \sum_{j=1}^{k+1} \alpha(n-k-jk,k) f_{\lfloor \frac{n-jk}{k} \rfloor (k-2) + (n-jk) \bmod k, k-2} c_{k,j} \\
&+ \alpha(n-k,k) f_{\lfloor n/k \rfloor (k-2) + n \bmod k, k-2} \\
&= \sum_{j=1}^{k+1} f_{n+2-jk,k} c_{k,j} + \sum_{j=1}^{k+1} \alpha(n-k-jk,k) f_{\lfloor \frac{n}{k} - j \rfloor (k-2) + n \bmod k, k-2} c_{k,j}
\end{aligned}$$

$$+\alpha(n-k,k)f_{\lfloor n/k\rfloor(k-2)+n \mod k,k-2}$$
$$=\sum_{j=1}^{k+1} f_{n+2-jk,k}c_{k,j}+\sum_{j=0}^{k+1}\alpha(n-k-jk,k)f_{\left\lfloor \frac{n}{k}-j\right\rfloor(k-2)+n \mod k,k-2}c_{k,j}$$

Thus, it suffices to show

$$\sum_{j=0}^{k+1}\alpha(n-k-jk,k)f_{\left\lfloor \frac{n}{k}-j\right\rfloor(k-2)+n \mod k,k-2}c_{k,j}=0.$$

If $\alpha(n-k,k)=0$, then $\alpha(n-k-jk,k)=0$ for all j, and so the statement is true.

Otherwise, we have more work to do. We first take care of the signs. By the proof of Lemma 8, the signs of α alternate every k indices, and thus $\alpha(n-k-jk)=-\alpha(n-j-jk+1)$. Thus, the sign of the jth term is

$$(-1)^{\lfloor n/k\rfloor-1+\lfloor(n+3)\rfloor/2+1}b_{n,k}=(-1)^{\lfloor n/k\rfloor+1}\hat{b}_{n,k}$$

where $\hat{b}_{n,k}$ is the signed Fibonomial coefficient.

Thus, we consider

$$(-1)^{\lfloor n/k\rfloor+1}\sum_{j=0}^{k+1}f_{\left\lfloor \frac{n}{k}-j\right\rfloor(k-2)+n \mod k,k-2}\hat{b}_{k+1,j}=0.$$

We would like to use the induction hypothesis; however, the Fibonacci product is in $k-2$, so we need $\hat{b}_{k-1}$ before we can proceed. Using the second half of Theorem 21 twice,

$$b_{n,k}=f_{n-k-2}(f_{n-k-4}b_{n-2,k-2}+f_{k-1}b_{n-2,k-1})+f_k(f_{n-k-3}b_{n-2,k-1}+f_kb_{n-2,k}).$$

So

$$(-1)^{\lfloor n/k\rfloor+1}\sum_{j=0}^{k+1}f_{\left\lfloor \frac{n}{k}-j\right\rfloor(k-2)+n \mod k,k-2}(-1)^{\lfloor j/2\rfloor}f_{k-j-2}(f_{k-j-4}b_{k-2,j-2}$$
$$+f_{j-1}b_{k-2,j-1})+f_j(f_{k-j-3}b_{k-2,j-1}+f_jb_{k-2,j})$$

The result follows from the induction hypothesis.

□

We show a few examples of Lemma 9.

Example 12. Let $n = 20, k = 4$. Then

$$\begin{aligned} f_{22,4} &= \sum_{j=1}^{5} f_{n-4j,4} c_{5,j} \\ &= 1600(5) + 135(15) - 36(15) - 4(5) + 1 \\ &= 10816 \\ &= 8^2 13^2 \\ &= f_{22,4} \end{aligned}$$

Example 13. Let $n = 18, k = 3$. Then

$$\begin{aligned} f_{18,3} &= \sum_{j=1}^{4} f_{n-43,4} c_{4,j} \\ &= 512(3) + 125(6) - 27(3) - 8(1) \\ &= 2197 \\ &= 13^3 \\ &= f_{18,3} \end{aligned}$$

Here are some examples which show Lemma 8 in action.

Example 14. Let $n = 12, k = 4$. Then

$$\begin{aligned} f_{14,4} &= f_{13,4} + f_{12,4} + \alpha(10,4) f_{2(2)+2,2} \\ 225 &= 135 + 81 + \frac{(-1)^2 + (-1)^2}{2}(f_{6,2}) \\ 225 &= 135 + 81 + (1)(9) \\ &= 225 \end{aligned}$$

Example 15. Let $n = 19, k = 2$. Then

$$f_{21,2} = f_{20,2} + f_{19,2} + \alpha(17,2) f_{19 \bmod 2,0}$$

$$\begin{aligned}12816 &= 7921 + 4895 + \frac{(-1)^8 + (-1)^9}{2}(1)\\ &= 12816\end{aligned}$$

Example 16. Let $n = 13, k = 3$. Then

$$\begin{aligned}f_{15,3} &= f_{14,3} + f_{13,3} + \alpha(10,3) f_{(4)(1)+13 \bmod 3,1}\\ 512 &= 320 + 200 + \frac{(-1)^{10} + (-1)^{11}}{2}(8)\\ &= 320 + 200 - 8\\ &= 512\end{aligned}$$

Using Lemma 8, we state and prove a recursion on the k-Fibonacci numbers only which does not need the $f_{n,k-2}$. This paves the way for the statement and proof of the generating function.

Theorem 23. *The k-Fibonacci numbers can be written as*

$$f_{n,k} = \sum_{j=0}^{n} \alpha(j+k-2,k) f_{n-j} \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor}.$$

Proof. Here is the formal proof of Theorem 23, which follows through strong induction on n.

To begin, let $n = 1$. Then,

$$\begin{aligned}f_{1,k} &= \sum_{j=0}^{1} \alpha(j+k-2) f_{i-j} \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor}\\ &= \alpha(k-2,2) f_1 \prod_{m=0}^{k-3} f_{\lfloor \frac{m}{k} \rfloor} + \alpha(k-1,2) f_1 \prod_{m=0}^{k-3} f_{\lfloor \frac{m+1}{k} \rfloor}\\ &= f_1 \prod_{m=0}^{k-3} f_{\lfloor \frac{m}{k} \rfloor}\\ &= f_1 \prod_{m=0}^{k-3} f_{\lfloor \frac{m}{k} \rfloor}\end{aligned}$$

$$
\begin{aligned}
&= f_1 \prod_{m=0}^{k-3} f_0 \\
&= f_1 \\
&= 1
\end{aligned}
$$

which is true for all k by the definition of the k-Fibonacci numbers.

Now assume

$$f_{t,k} = \sum_{j=0}^{t} \alpha(j+k-2,k) f_{t-j} \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor}$$

for all $t \leq n$ and consider $f_{n+1,k}$. By Lemma 8,

$$f_{n+1,k} = f_{n,k} + f_{n-1,k} + \alpha(n-k-1,k) f_{\lfloor n/k \rfloor (k-2)+n \bmod (k)-1,k-2}.$$

Proceeding using the inductive hypothesis,

$$
\begin{aligned}
f_{n+1,k} &= f_{n,k} + f_{n-1,k} + \alpha(n-k-1,k) f_{\lfloor n/k \rfloor (k-2)+n \bmod (k)-1,k-2} \\
&= \sum_{j=0}^{n} \alpha(j+k-2,k) f_{n-j} \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor} + \sum_{j=0}^{n-1} \alpha(j+k-2,k) f_{n-j-1} \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor} \\
&+ \alpha(n-k-1,k) f_{\lfloor n/k \rfloor (k-2)+n \bmod (k)-1,k-2} \\
&= \sum_{j=0}^{n-1} \alpha(j+k-2,k)(f_{n-j} + f_{n-j-1}) \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor} + \alpha(n+k-2,k) f_0 \prod_{m=0}^{k-3} f_{\lfloor \frac{n+m}{k} \rfloor} \\
&+ \alpha(n-k-1,k) f_{\lfloor n/k \rfloor (k-2)+n \bmod (k)-1,k-2} \\
&= \sum_{j=0}^{n-1} \alpha(j+k-2,k) f_{n+1-j} \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor} + \alpha(n+k-2,k) f_0 \prod_{m=0}^{k-3} f_{\lfloor \frac{n+m}{k} \rfloor} \\
&+ \alpha(n-k-1,k) f_{\lfloor n/k \rfloor (k-2)+n \bmod (k)-1,k-2} \\
&= \sum_{j=0}^{n} \alpha(j+k-2,k) f_{n+1-j} \prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor} + \alpha(n-k-1,k) f_{\lfloor n/k \rfloor (k-2)+n \bmod (k)-1,k-2}
\end{aligned}
$$

where the last equality looks like cheating, but follows since $f_0 = f_1$; we switch the index and assimilate it back in. To finish the proof, we need to write the $\alpha(n-k-1,k) f_{\lfloor n/k \rfloor (k-2)+n \bmod (k)-1,k-2}$ in the sum. We will do this by showing that

$$\alpha(n-k-1,k)f_{\lfloor (n-1)/k\rfloor(k-2)+(n-1) \bmod (k),k-2} = \alpha(n+k-1,k)f_0\prod_{m=0}^{k-3} f_{\lfloor \frac{n+1+m}{k}\rfloor}.$$

First we consider the α. Note

$$\alpha(n-k-1,k) = \frac{(-1)^{\lfloor (n-k-1)/k\rfloor} + (-1)^{\lfloor n-k/k\rfloor}}{2} = \frac{(-1)^{\lfloor (n-1)/k\rfloor -1} + (-1)^{\lfloor n/k\rfloor -1}}{2}$$

and

$$\alpha(n+k-1,k) = \frac{(-1)^{\lfloor (n+k-1)/k\rfloor} + (-1)^{\lfloor n+k/k\rfloor}}{2} = \frac{(-1)^{\lfloor (n-1)/k\rfloor +1} + (-1)^{\lfloor n/k\rfloor +1}}{2}.$$

Since $\lfloor \frac{n-1}{k}\rfloor - 1$ and $\lfloor \frac{n-1}{k}\rfloor + 1$ have the same parity, as do $\lfloor \frac{n}{k}\rfloor - 1$ and $\lfloor \frac{n}{k}\rfloor + 1$, then $\alpha(n-k-1,k) = \alpha(n+k-1,k)$.

Now consider $f_{\lfloor (n-1)/k\rfloor(k-2)+(n-1) \bmod (k),k-2}$ and $\prod_{m=0}^{k-3} f_{\lfloor \frac{n+1+m}{k}\rfloor}$, noting that we disregard the f_0; since $f_0 = 1$, we can ignore it at will.

Begin with $f_{\lfloor (n-1)/k\rfloor(k-2)+(n-1) \bmod (k),k-2}$ and note that by the proof of Lemma 23,

$$f_{\lfloor (n-1)/k\rfloor(k-2)+(n-1) \bmod (k),k-2} = f_{\lfloor (n-1)/k\rfloor}^{k-2-((n-1) \bmod k)} f_{\lfloor (n-1)/k\rfloor+1}^{(n-1) \bmod k}.$$

Note that where $r = n \bmod k$, since

$$\left\lfloor \frac{n-1}{k}\right\rfloor = \left\lfloor \frac{n-r+r-1}{k}\right\rfloor = \frac{n-r}{k} + \left\lfloor \frac{r-1}{k}\right\rfloor$$

and

$$\left\lfloor \frac{n+1}{k}\right\rfloor = \left\lfloor \frac{n-r+r+1}{k}\right\rfloor = \frac{n-r}{k} + \left\lfloor \frac{r+1}{k}\right\rfloor$$

then $\lfloor \frac{n-1}{k}\rfloor = \lfloor \frac{n+1}{k}\rfloor$ as long as $0 < r < k-1$.

Furthermore, note that if $r = 0$, then $\alpha(n+k-1) = \alpha(n-k-1) = 0$, since $\frac{n-1}{k} - 1$ and $\frac{n-1}{k}$ (equivalently, $\frac{n}{k} - 1$ and $\frac{n}{k}$) have opposite signs.

Thus, assume $0 < r \leq k-2$. (We will treat the $k-1$ case below.) The Fibonacci numbers making up $\prod_{m=0}^{k-3} f_{\lfloor \frac{n+1+m}{k} \rfloor}$ are $f_{\lfloor \frac{n+1+m}{k} \rfloor} = f_{\lfloor \frac{n+1}{k} \rfloor}$ (for small enough m), and $\lfloor \frac{n+1}{k} \rfloor = \lfloor \frac{n-1}{k} \rfloor$ as shown above. Since $0 \leq r \leq k-2$, there is some m—call it m^*—at which we will reach the threshold value such that $f_{\lfloor \frac{n+1+m}{k} \rfloor} = f_{\lfloor \frac{n+1}{k} \rfloor + 1}$. As previously argued, $f_{\lfloor \frac{n+1}{k} \rfloor + 1} = f_{\lfloor \frac{n-1}{k} \rfloor + 1}$.

Thus, in this case the 2 consecutive Fibonacci numbers making up

$$f_{\lfloor (n-1)/k \rfloor (k-2) + (n-1) \bmod (k), k-2}$$

and

$$\prod_{m=0}^{k-3} f_{\lfloor \frac{n+1+m}{k} \rfloor}$$

are the same. We now have to prove that the power of each Fibonacci number is the same between the two expressions.

First, observe that since $\lfloor \frac{n+1}{k} \rfloor = \lfloor \frac{n-r+r+1}{k} \rfloor = \frac{n-r}{k} + \lfloor \frac{r+1}{k} \rfloor$, there are $(n-1) \bmod k$ copies of $f_{\lfloor (n-1)/k \rfloor + 1}$. To determine how many copies there are of $f_{\lfloor (n+1)/k \rfloor + 1} = f_{\lfloor (n-1)/k \rfloor + 1}$ in $\prod_{m=0}^{k-3} f_{\lfloor \frac{n+1+m}{k} \rfloor}$, consider the index m^* at which

$$\left\lfloor \frac{n+1+m^*}{k} \right\rfloor > \left\lfloor \frac{n+1+m}{k} \right\rfloor$$

for all $0 \leq m < m^*$. (Since $0 < r < k-2$, such an m^* exists). Once we find the m^*, then there are $k-3-m^*+1 = k-2-m^*$ copies of $f_{\lfloor (n+1)/k \rfloor + 1}$.

So, we must determine what m^*. Clearly, it is the first index such that $\lfloor \frac{n+1+m^*}{k} \rfloor$ is an integer; thus,

$$\left\lfloor \frac{n+1+m^*}{k} \right\rfloor = q, q \in \mathbb{Z}.$$

So,

$$\begin{aligned} n+1+m^* &= kq \\ m^* &= kq-n-1 \\ m^* &= -(n+1) \bmod k \\ m^* &= k-(n+1) \bmod k \ (\textit{since we need } 0 \leq m^* \leq k-3). \end{aligned}$$

Thus, the number of copies of $f_{\lfloor (n+1)/k \rfloor + 1}$ is:

$$\begin{aligned}
k-2-m^* &= k-2-(k-(n+1) \bmod k) \\
&= -2+(n+1) \bmod k \\
&= -2+n+1+k\left\lfloor\frac{n+1}{k}\right\rfloor \\
&= n-1+k\left\lfloor\frac{n+1}{k}\right\rfloor \\
&= n-1+k\left\lfloor\frac{n-1}{k}\right\rfloor \\
&= (n-1) \bmod k.
\end{aligned}$$

Thus, we have shown

$$\alpha(n-k-1,k)f_{\lfloor(n-1)/k\rfloor(k-2)+(n-1) \bmod (k),k-2} = \alpha(n+k-1,k)f_0\prod_{m=0}^{k-3} f_{\lfloor\frac{n+1+m}{k}\rfloor}$$

as long as $0 \leq r \leq k-2$.

Finally, consider $r = k-1$. First, consider $\prod_{m=0}^{k-3} f_{\lfloor\frac{n+1+m}{k}\rfloor}$ and note that $m^* = 0$, since when $m = 0$,

$$\begin{aligned}
\left\lfloor\frac{n+1+0}{k}\right\rfloor &= \left\lfloor\frac{n+(k-1)-(k-1)+1}{k}\right\rfloor \\
&= \frac{n-(k-1)}{k} - 1
\end{aligned}$$

and when $m = k-3$,

$$\begin{aligned}
\left\lfloor\frac{n+1+k-3}{k}\right\rfloor &= \left\lfloor\frac{n+(k-1)-(k-1)+k-3}{k}\right\rfloor \\
&= \left\lfloor\frac{n-(k-1)}{k}\right\rfloor + \left\lfloor\frac{k-3+1-k-1}{k}\right\rfloor \\
&= \left\lfloor\frac{n-(k-1)}{k}\right\rfloor + \left\lfloor\frac{2k-3}{k}\right\rfloor \\
&= \frac{n-(k-1)}{k} + 2 + \left\lfloor\frac{-3}{k}\right\rfloor
\end{aligned}$$

$$= \frac{n-(k-1)}{k} + 1$$

Thus there are $k-2$ copies of $f_{\lfloor \frac{n+1}{k} \rfloor}$ and no copies of $f_{\lfloor \frac{n+1}{k}+1 \rfloor}$.

Similarly, consider $\alpha(n-k-1,k)f_{\lfloor (n-1)/k \rfloor (k-2)+(n-1) \bmod (k), k-2}$. As previously argued, there are $(n-1)\text{mod } k$ copies of $f_{\lfloor \frac{n-1}{k} \rfloor +1}$. Now, note that

$$\begin{aligned}\left\lfloor \frac{n-1}{k} \right\rfloor + 1 &= \left\lfloor \frac{n-(k-1)+(k-1)-1}{k} \right\rfloor + 1 \\ &= \frac{n-(k-1)}{k} + \left\lfloor \frac{k-2}{k} \right\rfloor + 1 \\ &= \frac{n-(k-1)}{k} + 1\end{aligned}$$

and

$$\begin{aligned}\left\lfloor \frac{n+1}{k} \right\rfloor &= \left\lfloor \frac{n-(k-1)+(k-1)+1}{k} \right\rfloor \\ &= \frac{n-(k-1)}{k} + \left\lfloor \frac{k}{k} \right\rfloor \\ &= \frac{n-(k-1)}{k} + 1\end{aligned}$$

so $f_{\lfloor \frac{n+1}{k} \rfloor} = f_{\lfloor \frac{n-1}{k} \rfloor +1}$.

So, we find $(n-1)\text{mod } k$ given that $r = k-1$:

$$\begin{aligned}(n-1)\text{mod } k &= n-1-k(\left\lfloor \frac{n-1}{k} \right\rfloor) \\ &= n-1-k\left\lfloor \frac{n-1+(k-1)-(k-1)}{k} \right\rfloor \\ &= n-1-k(\frac{n-(k-1)}{k} + \left\lfloor \frac{k-2}{k} \right\rfloor) \\ &= n-1-(n-k+1) \\ &= k-2.\end{aligned}$$

Therefore, $\alpha(n-k-1,k)f_{\lfloor(n-1)/k\rfloor(k-2)+(n-1) \bmod (k),k-2} = \alpha(n+k-1,k)f_0\prod_{m=0}^{k-3} f_{\lfloor\frac{n+1+m}{k}\rfloor}$ when $r = k-1$.

Thus we have shown

$$\alpha(n-k-1,k)f_{\lfloor(n-1)/k\rfloor(k-2)+(n-1) \bmod (k),k-2} = \alpha(n+k-1,k)f_0\prod_{m=0}^{k-3} f_{\lfloor\frac{n+1+m}{k}\rfloor}$$

for all $r, 0 \le r \le k-1$, and so:

$$\begin{aligned} f_{n+1,k} &= \sum_{j=0}^{n}\alpha(j+k-2,k)f_{n+1-j}\prod_{m=0}^{k-3} f_{\lfloor\frac{j+m}{k}\rfloor} + \alpha(n-k-1,k)f_{\lfloor n/k\rfloor(k-2)+n \bmod (k)-1,k-2} \\ &= \sum_{j=0}^{n}\alpha(j+k-2,k)f_{n+1-j}\prod_{m=0}^{k-3} f_{\lfloor\frac{j+m}{k}\rfloor} + \alpha(n+k-1,k)f_0\prod_{m=0}^{k-3} f_{\lfloor\frac{n+1+m}{k}\rfloor} \\ &= \sum_{j=0}^{n+1}\alpha(j+k-2,k)f_{n+1-j}\prod_{m=0}^{k-3} f_{\lfloor\frac{j+m}{k}\rfloor} \end{aligned}$$

concluding the proof.

□

We offer the following examples to illustrate Theorem 23 in action.

Example 17. We start with a big one. Let $n = 10, k = 4$. Then

$$36 = f_{10,4} = \sum_{j=0}^{10}\alpha(j+2,4)f_{10-j}\prod_{m=0}^{1} f_{\lfloor\frac{j+m}{4}\rfloor}$$

$$\begin{aligned} &= \alpha(2,4)f_{10}(f_{\lfloor\frac{0}{4}\rfloor}f_{\lfloor\frac{1}{4}\rfloor}) + \alpha(3,4)f_9(f_{\lfloor\frac{1}{4}\rfloor}f_{\lfloor\frac{2}{4}\rfloor}) + \alpha(4,4)f_8(f_{\lfloor\frac{2}{4}\rfloor}f_{\lfloor\frac{3}{4}\rfloor}) \\ &+ \alpha(5,4)f_7(f_{\lfloor\frac{3}{4}\rfloor}f_{\lfloor\frac{4}{4}\rfloor}) + \alpha(6,4)f_6(f_{\lfloor\frac{4}{4}\rfloor}f_{\lfloor\frac{5}{4}\rfloor}) + \alpha(7,4)f_5(f_{\lfloor\frac{5}{4}\rfloor}f_{\lfloor\frac{6}{4}\rfloor}) \\ &+ \alpha(8,4)f_4(f_{\lfloor\frac{6}{4}\rfloor}f_{\lfloor\frac{7}{4}\rfloor}) + \alpha(9,4)f_3(f_{\lfloor\frac{7}{4}\rfloor}f_{\lfloor\frac{8}{4}\rfloor}) + \alpha(10,4)f_2(f_{\lfloor\frac{8}{4}\rfloor}f_{\lfloor\frac{9}{4}\rfloor}) \\ &+ \alpha(11,4)f_1(f_{\lfloor\frac{9}{4}\rfloor}f_{\lfloor\frac{10}{4}\rfloor}) + \alpha(12,4)f_0(f_{\lfloor\frac{10}{4}\rfloor}f_{\lfloor\frac{11}{4}\rfloor}) \end{aligned}$$

$$
\begin{aligned}
&= f_{10}(f_{\lfloor \frac{0}{4} \rfloor} f_{\lfloor \frac{1}{4} \rfloor}) - f_8(f_{\lfloor \frac{2}{4} \rfloor} f_{\lfloor \frac{3}{4} \rfloor}) - f_7(f_{\lfloor \frac{3}{4} \rfloor} f_{\lfloor \frac{4}{4} \rfloor}) + f_6(f_{\lfloor \frac{4}{4} \rfloor} f_{\lfloor \frac{5}{4} \rfloor}) \\
&- f_4(f_{\lfloor \frac{6}{4} \rfloor} f_{\lfloor \frac{7}{4} \rfloor}) - f_3(f_{\lfloor \frac{7}{4} \rfloor} f_{\lfloor \frac{8}{4} \rfloor}) - f_2(f_{\lfloor \frac{8}{4} \rfloor} f_{\lfloor \frac{9}{4} \rfloor}) + f_0(f_{\lfloor \frac{10}{4} \rfloor} f_{\lfloor \frac{11}{4} \rfloor})
\end{aligned}
$$

$$
\begin{aligned}
&= f_{10}f_0f_0 - f_8f_0f_0 - f_7f_0f_1 - f_6f_1f_1 + f_4f_1f_1 + f_3f_1f_2 + f_2f_2f_2 - f_0f_2f_2 \\
&= 89 - 34 - 21 - 13 + 5 + (3)(2) + (2)(2)(2) - (2)(2) \\
&= 36
\end{aligned}
$$

Example 18. Now we do one with a bigger k, so the product term is slightly less boring. Let $n = 12, k = 5$. Then

$$
f_{12,5} = \sum_{j=0}^{12} \alpha(j+3,5) f_{12-j} \prod_{m=0}^{2} f_{\lfloor \frac{j+m}{5} \rfloor}
$$

$$
\begin{aligned}
&= \alpha(3,5)f_{12}(f_{\lfloor \frac{0}{5} \rfloor} f_{\lfloor \frac{1}{5} \rfloor} f_{\lfloor \frac{2}{5} \rfloor}) + \alpha(4,5)f_{11}(f_{\lfloor \frac{1}{5} \rfloor} f_{\lfloor \frac{2}{5} \rfloor} f_{\lfloor \frac{3}{5} \rfloor}) + \alpha(5,5)f_{10}(f_{\lfloor \frac{2}{5} \rfloor} f_{\lfloor \frac{3}{5} \rfloor} f_{\lfloor \frac{4}{5} \rfloor}) \\
&+ \alpha(6,5)f_9(f_{\lfloor \frac{3}{5} \rfloor} f_{\lfloor \frac{4}{5} \rfloor} f_{\lfloor \frac{5}{5} \rfloor}) + \alpha(7,5)f_8(f_{\lfloor \frac{4}{5} \rfloor} f_{\lfloor \frac{5}{5} \rfloor} f_{\lfloor \frac{6}{5} \rfloor}) + \alpha(8,5)f_7(f_{\lfloor \frac{5}{5} \rfloor} f_{\lfloor \frac{6}{5} \rfloor} f_{\lfloor \frac{7}{5} \rfloor}) \\
&+ \alpha(9,5)f_6(f_{\lfloor \frac{6}{5} \rfloor} f_{\lfloor \frac{7}{5} \rfloor} f_{\lfloor \frac{8}{5} \rfloor}) + \alpha(10,5)f_5(f_{\lfloor \frac{7}{5} \rfloor} f_{\lfloor \frac{8}{5} \rfloor} f_{\lfloor \frac{9}{5} \rfloor}) + \alpha(11,5)f_4(f_{\lfloor \frac{8}{5} \rfloor} f_{\lfloor \frac{9}{5} \rfloor} f_{\lfloor \frac{10}{5} \rfloor}) \\
&+ \alpha(12,5)f_3(f_{\lfloor \frac{9}{5} \rfloor} f_{\lfloor \frac{10}{5} \rfloor} f_{\lfloor \frac{11}{5} \rfloor}) + \alpha(13,5)f_2(f_{\lfloor \frac{10}{5} \rfloor} f_{\lfloor \frac{11}{5} \rfloor} f_{\lfloor \frac{12}{5} \rfloor}) \\
&+ \alpha(14,5)f_1(f_{\lfloor \frac{11}{5} \rfloor} f_{\lfloor \frac{12}{5} \rfloor} f_{\lfloor \frac{13}{5} \rfloor}) + \alpha(15,5)f_0(f_{\lfloor \frac{12}{5} \rfloor} f_{\lfloor \frac{13}{5} \rfloor} f_{\lfloor \frac{14}{5} \rfloor})
\end{aligned}
$$

$$
\begin{aligned}
&= f_{12}(f_{\lfloor \frac{0}{5} \rfloor} f_{\lfloor \frac{1}{5} \rfloor} f_{\lfloor \frac{2}{5} \rfloor})) - f_{10}(f_{\lfloor \frac{2}{5} \rfloor} f_{\lfloor \frac{3}{5} \rfloor} f_{\lfloor \frac{4}{5} \rfloor}) - f_9(f_{\lfloor \frac{3}{5} \rfloor} f_{\lfloor \frac{4}{5} \rfloor} f_{\lfloor \frac{5}{5} \rfloor}) - f_8(f_{\lfloor \frac{4}{5} \rfloor} f_{\lfloor \frac{5}{5} \rfloor} f_{\lfloor \frac{6}{5} \rfloor}) \\
&- f_7(f_{\lfloor \frac{5}{5} \rfloor} f_{\lfloor \frac{6}{5} \rfloor} f_{\lfloor \frac{7}{5} \rfloor}) + f_5(f_{\lfloor \frac{7}{5} \rfloor} f_{\lfloor \frac{8}{5} \rfloor} f_{\lfloor \frac{9}{5} \rfloor}) + f_4(f_{\lfloor \frac{8}{5} \rfloor} f_{\lfloor \frac{9}{5} \rfloor} f_{\lfloor \frac{10}{5} \rfloor}) + f_3(f_{\lfloor \frac{9}{5} \rfloor} f_{\lfloor \frac{10}{5} \rfloor} f_{\lfloor \frac{11}{5} \rfloor}) \\
&+ f_2(f_{\lfloor \frac{10}{5} \rfloor} f_{\lfloor \frac{11}{5} \rfloor} f_{\lfloor \frac{12}{5} \rfloor}) - f_0(f_{\lfloor \frac{12}{5} \rfloor} f_{\lfloor \frac{13}{5} \rfloor} f_{\lfloor \frac{14}{5} \rfloor})
\end{aligned}
$$

$$
\begin{aligned}
&= f_{12}f_0f_0f_0 - f_{10}f_0f_0f_0 - f_9f_0f_0f_1 - f_8f_0f_1f_1 - f_7f_1f_1f_1 + f_5f_1f_1f_1 + f_4f_1f_1f_2 \\
&+ f_3f_1f_2f_2 + f_2f_2f_2f_2 - f_0f_2f_2f_2
\end{aligned}
$$

$$
\begin{aligned}
&= 233 - 89 - 55 - 34 - 21 + 8 + (5)(2) + (3)(2)(2) + (2)(2)(2)(2) - (2)(2)(2) \\
&= 233 - 89 - 55 - 34 - 21 + 8 + 10 + 12 + 16 - 8 \\
&= 72
\end{aligned}
$$

$$= f_{12,5}.$$

Example 19. Let $n = 4, k = 3$. Then

$$\begin{aligned}
2 = f_{4,3} &= \sum_{j=0}^{4} \alpha(j+1,3) f_{4-j} \prod_{m=0}^{0} f_{\left\lfloor \frac{j+m}{3} \right\rfloor} \\
&= \alpha(1,3) f_4 (f_{\left\lfloor \frac{0}{3} \right\rfloor}) + \alpha(2,3) f_3 (f_{\left\lfloor \frac{1}{3} \right\rfloor}) \\
&+ \alpha(3,3) f_2 (f_{\left\lfloor \frac{2}{3} \right\rfloor}) + \alpha(4,3) f_1 (f_{\left\lfloor \frac{3}{3} \right\rfloor}) + \alpha(5,3) f_0 (f_{\left\lfloor \frac{4}{3} \right\rfloor}) \\
&= f_4 f_0 - f_2 f_0 - f_1 f_1 \\
&= 5 - 2 - 1 \\
&= 2
\end{aligned}$$

Example 20. Similarly, let $n = 5, k = 3$. Then

$$\begin{aligned}
4 = f_{5,3} &= \sum_{j=0}^{5} \alpha(j+1,3) f_{5-j} \prod_{m=0}^{0} f_{\left\lfloor \frac{j+m}{3} \right\rfloor} \\
&= \alpha(1,3) f_5 (f_{\left\lfloor \frac{0}{3} \right\rfloor}) + \alpha(2,3) f_4 (f_{\left\lfloor \frac{1}{3} \right\rfloor}) + \alpha(3,3) f_3 (f_{\left\lfloor \frac{2}{3} \right\rfloor}) \\
&+ \alpha(4,3) f_2 (f_{\left\lfloor \frac{3}{3} \right\rfloor}) + \alpha(5,3) f_1 (f_{\left\lfloor \frac{4}{3} \right\rfloor}) + \alpha(6,3) f_0 (f_{\left\lfloor \frac{5}{3} \right\rfloor}) \\
&= f_5 f_0 - f_3 f_0 - f_2 f_1 + f_0 f_1 \\
&= 8 - 3 - 2 + 1 \\
&= 4
\end{aligned}$$

Example 21. Now, we give an example of the technique used in the proof of Theorem 23 by computing $f_{6,3}$ using Lemma 8; we wind up with an expression of the form Theorem 23.

$$\begin{aligned}
f_{6,3} &= f_{5,3} + f_{4,3} + \alpha(1,3) f_{\lfloor 4/3 \rfloor (1) + 4 \mod 3, 1} \\
&= f_5 f_0 - f_3 f_0 - f_2 f_1 + f_0 f_1 + f_4 f_0 - f_2 f_0 - f_1 f_1 + f_{2,1}
\end{aligned}$$

$$
\begin{aligned}
&= f_5 f_0 + f_4 f_0 - f_3 f_0 - f_2 f_0 - f_2 f_1 - f_1 f_1 + f_0 f_1 + f_2 \\
&= f_6 f_0 - f_4 f_0 - f_3 f_1 + f_0 f_1 + f_2 \\
&= f_6 f_0 - f_4 f_0 - f_3 f_1 + f_1 f_1 + f_0 f_2 \\
&= \sum_{j=0}^{6} \alpha(j+1,3) f_{6-j} \prod_{m=0}^{0} f_{\lfloor \frac{j+m}{3} \rfloor}
\end{aligned}
$$

6.7.4 The Numerators: A Recursive Array

The Fibonomials will play a large role in determining the denominator of the generating function $F_k(x)$. The numerators of $F_k(x)$ can also be constructed in a systematic way and can be represented by a number triangle for each k, but they do not already have a name in the literature. We provide a description of them here.

These numerators serve as a bridge between the Fibonomials and the k-Fibonacci numbers. The reason for viewing them this way will become apparent in the next section, but the motivation comes from Theorem 23. For now, we define the "bridge series" as follows.

Definition 23. For some fixed k, define the series $B_k(x)$ as

$$B_k(x) = \sum_{i \geq 0} \alpha(i+k-2,k) \prod_{m=0}^{k-3} f_{\lfloor \frac{i+m}{k} \rfloor} x^i$$

where $F_{i,k}$ is the ith k-Fibonacci number and $\alpha(n,k) = \frac{(-1)^{\lfloor n/k \rfloor} + (-1)^{\lfloor (n+1)/k \rfloor}}{2}$.

Recall that the numerators of a generating function encode the initial conditions of the recursion given in the denominators. Thus, determining the numerators is a simple matter of methodically solving for the coefficient of the desired resulting series.

We choose to represent these coefficients as a three-dimensional array, which makes it easy to write a recursive definition.

Definition 24. Let $N(a,b,c)$ be an array defined recursively as follows. Throughout let $f_{n,k}$ be the nth k-Fibonacci number and let $b_{i,k}$ be the Fibonomials.

1. For $c > 0, a > c+2$, and $b \geq c$,

$$\begin{aligned}
N(a,0,c) &= (-1)^c f_{c(a-1),a-1} + \sum_{j=1}^{c}(-1)^{j+1} b_{a+j-1,j} N(a,2,c-j)\\
N(a,1,c) &= 0\\
N(a,b,c) &= (-1)^{c+1} f_{c(a-1)+b-2,a-1} + \sum_{j=1}^{c}(-1)^{j} b_{a+j-1,j} N(a,b,c-j), b \geq 2
\end{aligned}$$

2. The initial condition is

$$\begin{aligned}
N(a,0,0) &= 1\\
N(a,1,0) &= 0\\
N(a,b,0) &= \begin{cases} -1, \ 2 \leq b \leq a \\ 0, \ b > a \end{cases}
\end{aligned}$$

We show some examples of this definition. Throughout, note that a blank space at any i, j location with $j > i$ is an implied 0.

Example 22. Layer 1 of the array, that is, the $c = 0$ initial condition, for some small a, b is given by

Table 6.12: $N(a, b, 0)$ for small a, b.

a/b	0	1	2	3	4	5
2	1	0	-1			
3	1	0	-1	-1		
4	1	0	-1	-1	-1	
5	1	0	-1	-1	-1	-1
6	1	0	-1	-1	-1	-1

Example 23. Layer 2 of the array, when $c = 1$, for some small a, b is given by

Table 6.13: $N(a, b, 1)$ for small a, b.

a/b	0	1	2	3	4	5	6	7	8	9
3	1	0	-1							
4	2	0	-2	-1	1					
5	4	0	-4	-3	-1	3				
6	7	0	-7	-6	-4	0	8			
7	12	0	-12	-11	-9	-5	3	19		
8	20	0	-20	-19	-17	-13	-5	11	43	
9	33	0	-33	-32	-30	-26	-18	-2	30	94

Example 24. Layer 3 of the array, when $c = 2$, for some small a, b is given by

Table 6.14: $N(a, b, 2)$ for small a, b.

a/b	0	1	2	3	4	5	6	7	8	9
4	-1	0	1							
5	-4	0	4	1	-1	-1				
6	-16	0	16	8	0	-4	6			
7	-53	0	53	34	12	-8	-12	34		
8	-166	0	166	123	69	9	-39	-27	159	
9	-492	0	492	398	274	122	-38	-142	-26	692

As the name may suggest, $N(a, b, c)$ gives the numerator coefficients for our new generating function. We formalize this relationship now.

Theorem 24. *Where $N(a, b, c)$ is defined as in Definition 24, the numerator for the generating function for the bridge series $B_k(x)$ for fixed k is*

$$\sum_{j=0}^{k-3} \sum_{i=0}^{k-1} N(k-1, i, j) x^{i+jk}.$$

In fact,

$$B_k(x) = \frac{\sum_{j=0}^{k-3}\sum_{i=0}^{k-1} N(k-1,i,j)x^{i+jk}}{\sum_{j=0}^{k-1}\hat{b}_{k-1,j}x^{jk}}$$

Proof. Fix some $k \geq 3$.

At a high level, recall that the numerator of a generating function encodes the initial conditions for the recurrence encoded in the denominator. We solve for the numerators coefficient by coefficient such that we obtain the desired $B_k(x)$. Intuitively, we move across the columns of N from the bottom up in row $k-1$ of the array. That is, the coefficients of $x^{rk}, x^{1+rk}, \ldots x^{k+rk}$, $0 \leq r \leq k-3$, are given by the k entries in row $k-1$ of layer r in N.

Throughout, denote the coefficient of x^i in some series $S(x)$ by $[x^i]_{S(x)}$. Also, let $C_k(x) = \sum_{j=0}^{k}\hat{b}_{k,j}x^{jk}$.

First, consider $[x^i]_{B_k(x)}$ for $0 \leq i \leq k-1$. Note that in the convolution of the numerator and $C_k(x)$, the only contribution of $C_k(x)$ to $B_k(x)$ is $[x^0] = 1$, since $[x^k]$ is the next smallest-powered term in $C_k(x)$. First let $i = 0$. Since $\alpha(k-2,k) = 1$ and $\prod_{m=0}^{k-3} f_{\lfloor m/k \rfloor} = 1$, then $1 = [x^0]$. Since $[x^0] = 1$ in $C_k(x)$, then $N(k-1,0,0) = 1$.

For $i = 1$, note that $\alpha(k-1,k) = 0$ so $[x^1]$ in $B_k(x) = 0$. Thus, we must have $N(k-1,1,0) = 0$ since $[x^0] = 1 \neq 0$ in $B_k(x)$.

Finally, for $2 \leq i \leq k-1$, note that $\alpha(i+k-2) = -1$ for all $2 \leq i \leq k-1$, and since $f_{\lfloor (k-1+k-3)/k \rfloor} = f_{2-\lfloor 4/k \rfloor} = 1$, $[x^i] = -1$, $2 \leq i \leq k-1$. Since the only contribution from $C_k(x)$ is again only $[x^0] = 1$, then we must have $N(k-1,b,0) = -1$ for $2 \leq b \leq a$. This proves the initial condition at the $c = 0$ layer of the array.

Now, consider layer $c > 0$ of $N(a,b,c)$. Clearly, there are more contributions from $C_k(x)$ than just simply $[x^0]$. In fact, for any $[x^i]$ in $B_k(x)$ for $i \leq (k-1)(k-3)$, let $r = i \bmod k$. Then we get contributions from all $[x^{r+jk}]$ in $C_k(x)$ for $0 \leq j \leq \lfloor i/k \rfloor - 1$. Specifically,

$$[x^i]_{B_k(x)} = \sum_{j=0}^{\lfloor n/k \rfloor - 1} [x^{r+jk}]_{C_k(x)} N(k-1, r, \lfloor i/k \rfloor - j).$$

Now, we determine the coefficients $[x^i]_{B_k(x)}$ and $[x^i]_{C_k(x)}$. Recall from Definition 23 that $[x^i]_{B_k(x)} = \alpha(i+k-2,k)\prod_{m=0}^{k-3} f_{\lfloor \frac{i+m}{k} \rfloor}$. Furthermore, from the proof of Theorem 23, $\prod_{m=0}^{k-3} f_{\lfloor \frac{i+m}{k} \rfloor} = f_{\lfloor \frac{i}{k} \rfloor (k-2) + (i-2) \bmod k, k-2}$.

Also, $[x^{jk}]_{C_k(x)} = (-1)^j b_{k+j-2,j}$. Thus,

$$\begin{aligned} [x^i]_{B_k(x)} &= \sum_{j=0}^{\lfloor i/k \rfloor} [x^{r+jk}]_{C_k(x)} N(k-1, i \bmod k, \lfloor i/k \rfloor - j) \\ \alpha(i+k-2,k) f_{\lfloor \frac{i-2}{k} \rfloor (k-2) + (i-2) \bmod k, k-2} &= \sum_{j=0}^{\lfloor n/k \rfloor} (-1)^j b_{k+j-2,j} N(k-1, i \bmod k, \lfloor i/k \rfloor - j) \end{aligned}$$

Since $b_{0,k} = 1$, we pull off the $j = 1$ term of the sum and solve for $N(k-1, i \bmod k, \lfloor i/k \rfloor)$ to obtain

$$\begin{aligned} N(k-1, i \bmod k, \lfloor i/k \rfloor) = &-\alpha(i+k-2,k) f_{\lfloor \frac{i-2}{k} \rfloor (k-2) + (i-2) \bmod k, k-2} \\ &+ \sum_{j=1}^{\lfloor i/k \rfloor} (-1)^j b_{k+j-2,j} N(k-1, i \bmod k, \lfloor i/k \rfloor - j) \end{aligned}$$

Letting $a = k-1, b = i \bmod k, c = \lfloor i/k \rfloor$ yields the recursive definition of $N(a,b,c)$ from Definition 24.

For any $i = jk - 1$, $\alpha(i+k-2,k) = 0$. Thus $N(a,1,c) = 0$ since $[x^i] \neq 0$ in $C_k(x)$ for any i by the definition of the Fibonomials.

Now, we have defined the initial conditions for the $k-2$ Fibonacci numbers using $N(a,b,c)$. Since we have defined all the numbers up to the $k(k+1)$ recursion depth, we are done with the initial conditions. From here on out, the coefficients of all x^i in the bridge series are determined by the recursion, which as we showed in Lemma 9, is exactly the Fibonomials defined in the denominator.

□

At first glance, a complaint might be raised about the recursive nature of the numerator definition. If we, say, wanted the generating function for the k-Fibonacci numbers for $k = 20$, we surely do not want to calculate the generating functions for all $k \leq 19$. However, this complaint is easily answered by noting that the recursion in the array only goes through the z-axis–that is, only through numbers that we need to know for a fixed k generating function anyway. Since the only other numbers in the numerators are some

k-Fibonacci numbers and some Fibonomials, both of which have closed forms, we argue that we do not in fact need to do a burdensome amount of work to obtain a generating function for some given k. That said, a closed form for the $N(a,b,c)$ would certainly be desirable, but we leave it to future work.

6.7.5 The Generating Function: Gluing the Pieces Together

One more lemma suffices to obtain the proof of Theorem 20.

Lemma 10. *Where $B_k(x)$ is the bridge series from Definition 23,*

$$\frac{B_k(x)}{1-x-x^2} = \sum_{i\geq 0} f_{i,k}x^i$$

where $f_{n,k}$ is the nth k-Fibonacci number.

Proof. Recall the definition of convolution of polynomials: if $f(x) = \sum_{n\geq 0} a_n x^n$ and $g(x) = \sum_{n\geq 0} b_n x^n$, then $f(x)g(x) = \sum_{n\geq 0}\sum_{r=0}^{n} a_r b_{n-r} x^n$. By Definition 23,

$$B_k(x) = \sum_{i\geq 0} \alpha(i+k-2,k) \prod_{m=0}^{k-3} f_{\lfloor \frac{i+m}{k} \rfloor} x^i$$

and we know that

$$\frac{1}{1-x-x^2} = \sum_{i\geq 0} f_i x^i.$$

Thus,

$$\begin{aligned} B_k(x)(\frac{1}{1-x-x^2}) &= \sum_{i\geq 0}\sum_{j=0}^{i} \big(\alpha(j+k-2,k)\prod_{m=0}^{k-3} f_{\lfloor \frac{j+m}{k} \rfloor}\big)\big(f_{n-j}\big)x^i \\ &= \sum_{i\geq 0} f_{i,k}x^i \end{aligned}$$

where the last inequality follows from Theorem 23. □

Now, we are finally ready to prove Theorem 20.

Corollary 9. *Theorem 20 is true.*

Proof. We have already proved the theorem in the lemmas. Theorem 24 gives us $B_k(x)$, and Lemma 10 gives us that $B_k(x)$ multiplied by the Fibonacci generating function gives the desired result. □

Example 25. A generating function for $k = 7$ is not known either in the OEIS or in the literature. Using the code in Appendix B, we obtain it here. The numerator is

$$\begin{aligned}-(&x^{30} - x^{28} + x^{27} - x^{26} + x^{25} - x^{24} - 7\,x^{23} + 7\,x^{21} - 6\,x^{20} + 4\,x^{19} - 8\,x^{17} - 16\,x^{16} \ldots \\ &+16\,x^{14} - 8\,x^{13} + 4\,x^{11} + 6\,x^{10} + 7\,x^{9} - 7\,x^{7} + x^{6} + x^{5} + x^{4} + x^{3} + x^{2} - 1)\end{aligned}$$

with denominator

$$\left(x^{42} - 8\,x^{35} - 40\,x^{28} + 60\,x^{21} + 40\,x^{14} - 8\,x^{7} - 1\right)\left(x^{2} + x - 1\right)$$

Example 26. Furthermore, the numerator of the generating function for $k = 10$ is

$$\begin{aligned}&x^{72} - x^{70} + x^{69} - x^{68} + x^{67} - x^{66} + x^{65} - x^{64} + x^{63} + 33\,x^{62} - 33\,x^{60} + 32\,x^{59} \\ &- 30\,x^{58} + 26\,x^{57} - 18\,x^{56} + 2\,x^{55} + 30\,x^{54} - 94\,x^{53} - 492\,x^{52} + 492\,x^{50} - 398\,x^{49} \\ &+ 274\,x^{48} - 122\,x^{47} - 38\,x^{46} + 142\,x^{45} - 26\,x^{44} - 692\,x^{43} - 1784\,x^{42} + 1784\,x^{40} \\ &- 1092\,x^{39} + 426\,x^{38} + 72\,x^{37} - 222\,x^{36} - 72\,x^{35} + 426\,x^{34} + 1092\,x^{33} + 1784\,x^{32} \\ &- 1784\,x^{30} + 692x^{29} - 26\,x^{28} - 142\,x^{27} - 38\,x^{26} + 122\,x^{25} + 274\,x^{24} + 398\,x^{23} \\ &+ 492\,x^{22} - 492\,x^{20} + 94\,x^{19} + 30\,x^{18} - 2\,x^{17} - 18\,x^{16} - 26\,x^{15} - 30\,x^{14} - 32\,x^{13} - 33\,x^{12} \\ &+ 33x^{10} - x^{9} - x^{8} - x^{7} - x^{6} - x^{5} - x^{4} - x^{3} - x^{2} + 1\end{aligned}$$

with denominator

$$\begin{aligned}-(&x^{90} + 34\,x^{80} - 714\,x^{70} - 4641\,x^{60} + 12376\,x^{50} + 12376 \\ &x^{40} - 4641\,x^{30} - 714\,x^{20} + 34\,x^{10} + 1)(x^{2} + x - 1)\end{aligned}$$

Of course, as k gets bigger, the k-Fibonacci numbers only get bigger. This makes the generating function quite unwieldy as k gets large. In fact, the coefficient of the x^{194} term in the numerator for $k = 15$ is the 31-digit number

$$-4466655663433116095405828866048.$$

Thus, this generating function might be more useful for theoretical rather than computational purposes.

6.8 Fixed Points and the Pascal's Array Conjecture

A natural question about any class of restricted permutations is: how many fixed points do they have? Since the fixed points of k-drop permutations correspond to the main diagonals of a k-tridiagonal matrix, calculating the number of fixed points is a natural avenue for learning more about this class of matrices. Here we identify the total number of fixed points in all k-drop permutations of length n.

6.8.1 $k = 1$

We begin with the $k = 1$ case. Throughout, let $p_{n,k}$ be the total number of fixed points in all k-drop permutations of length n, and let $p_{n,k,i}$ be the number of length n k-drop permutations with i elements in the corresponding k-free subset. Since each element in a subset corresponds to 2 non-fixed elements (since a subset entry encodes a switch), $p(n, k, i)$ is equivalent to having a length n k-drop permutation having $n-2i$ fixed points.

We consider first the $k = 1$ case.

Proposition 18. $p_{n,1,i} = \binom{n-i}{i}$.

Proof. We wish to choose i elements of $n - 1$ such that no two of them have distance 1 apart. For each element j that we choose, we cannot choose element $j + 1$. Thus, the number of subsets is the number of ways to choose i elements from $n - i$ elements. □

Proposition 19. $p_{n,1} = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j}(n - 2j)$.

Proof. Immediate from Proposition 18, since there are $n-2i$ fixed points for each $p_{n,1,i}$. We can have at most n fixed points and at minimum $n-2(\lfloor n/2 \rfloor)$ fixed points, since this is 0 or 1 depending on the parity of n. Note we cannot have fewer than 1 fixed point for odd n, since there is no element available to swap with the last element. □

There is another way to write $p_{n,1}$, and this argument is combinatorial and somewhat direct from the Fibonacci recurrence.

Proposition 20. *$p_{n,1} = s_n$, where s_n is the nth element of the sequence given by $s_0 = 0, s_1 = 1$, $s_n = s_{n-1} + s_{n-2} + f_{n-1}$ for f_{n-1} the nth Fibonacci number.*

Proof. When $n = 0$, there are 0 fixed points, and when $n = 1$, there is one fixed point corresponding to (1), the only entry in the only permutation.

Now, consider the number of fixed points in all 1-drop permutations on n elements. Every permutation must be formed by either

1. Appending $\pi(n) = n$ to the end of any 1-drop permutation of length $n-1$
2. Appending $\pi(n-1) = n, \pi(n) = n-1$ to the end of any 1-drop permutation of length $n-2$

Case (1) contributes the existing s_{n-1} fixed points from the length $n-1$ permutations, and also creates one new fixed point for each permutation. We already know there are f_{n-1} such permutations, so case (1) contributes $s_{n-1} + f_{n-1}$ fixed points. Case (2) creates no new fixed points, so we have only the s_{n-2} existing fixed points. □

To keep track of the coefficients, we write a series of polynomials $P_{n,k}(x)$ for fixed n, k where $[x^i]_{P_{n,k}(x)}$ is the number of length n k-drop permutations with $n-2i$ fixed points.

Definition 25. Let $P_{n,1}(x) = \sum_{i=0}^{k} \binom{k-i}{i} x^i$.

The $P_{n,1}(x)$ are known as the Fibonacci polynomials in the literature.

An interesting corollary follows.

Corollary 10. $P_{n,1}(x) = (\frac{1}{1-x-x^2})^2$.

Proof. We have a recursion for $p_{n,1}$ from Proposition 20. From the OEIS $A001629$, we know that the self-convolution of the Fibonacci numbers, defined by $(\frac{1}{1-x-x^2})^2$ follow the same recursion with the same initial conditions. □

A combinatorial proof of this corollary—a direct explanation of why squaring the generating function gives the fixed points of the generating function, without recourse to the recursion—we leave as an avenue for future work.

Example 27. The first few self-convolved Fibonacci numbers are

$$0, 1, 2, 5, 10, 20, 38, 71, 130, 235, \ldots$$

Example 28. Here are the $p_{n,1,i}$ for various n and i. These are the jagged diagonals from Pascal's triangle. Note that the row sums give the Fibonacci numbers f_n.

Table 6.15: Number of subsets on $n-1$ for $k=1$ with exactly i elements.

n/i	0	1	2	3	4
1	1				
2	1	1			
3	1	2			
4	1	3	1		
5	1	4	3		
6	1	5	6	1	
7	1	6	10	4	
8	1	7	15	10	1

Multiplying the n, i entry by $n-2i$ yields the number of fixed points. Summing the rows yields the numbers in Example 27.

Table 6.16: Number of permutations with i fixed points for $k = 1$.

n/i	0	1	2	3	4
1	1				
2	2	0			
3	3	2			
4	4	6	0		
5	5	12	3		
6	6	20	12	0	
7	7	30	30	4	
8	8	42	60	20	0

Example 29. Let $k = 1, n = 5$. We count the number of permutations with $n - 2i$ fixed points for $0 \le i \le \lfloor n/2 \rfloor$.

For $i = 0$, we expect $\binom{5}{0} = 1$ permutation with 5 fixed points. This is

$$12345.$$

For $i = 1$, we expect $\binom{4}{1} = 4$ permutations with 3 fixed points. These are

$$21345$$

$$13245$$

$$12435$$

$$12354$$

For $i = 2$, we expect $\binom{3}{2} = 3$ permutations with 1 fixed point. These are

$$21435$$

$$21354$$

$$13254$$

These are all $f_5 = 8$ permutations of length 5. We count $(5)(1)+(3)(4)+(3)(1) = 20 = s_6$

total fixed points, as expected.

6.8.2 $k > 1$

An interesting phenomenon occurs when finding the number of fixed points for permutations with $k \geq 2$. To find the number of fixed points, we conjecture that we must simply multiply k copies of the $P_{n,1}(x)$ corresponding to the Fibonacci numbers making up $f_{n,k}$. The coefficients of the resulting generating function yield a generalized version of Pascal's triangle, which does not appear in the literature as far as we know, and which seem to give the number of permutations with a set number of fixed points.

Conjecture 2. $P_{n,k}(x) = \prod_{i=0}^{k-1} P_{\lfloor \frac{n+i}{k} \rfloor,1}(x)$

We do not yet have a proof of this conjecture. However, letting $x = 1$ shows the coefficient sums of the right side for a given k do in fact add to $f_{n,k}$.

Example 30. For $k = 2$, we compute the following. The row sums give the Fibonacci numbers $f_{n,2}$.

Table 6.17: Number of subsets on $n - 2$ for $k = 2$ with exactly i elements.

n/i	0	1	2	3	4
2	1				
3	1	1			
4	1	2	1		
5	1	3	2		
6	1	4	4		
7	1	5	7	2	
8	1	6	11	6	1
9	1	7	16	13	3
10	1	8	22	24	9

Multiplying the ith row pointwise with the vector v where $v_i = n - 2i$ yields the following. The row sums give column 2 in Table 6.21 below.

Table 6.18: Number of permutations with i fixed points for $k = 2$.

n/i	0	1	2	3	4	5
2	2					
3	3	1				
4	4	4				
5	5	9	2			
6	6	16	8			
7	7	25	21	2		
8	8	36	44	12	0	
9	9	49	80	39	3	
10	10	64	132	96	18	
11	11	81	203	200	66	3

Example 31. For $k = 3$, we compute the following. The row sums give the Fibonacci numbers $f_{n,3}$.

Table 6.19: Number of subsets on $n - 3$ for $k = 3$ with exactly i elements.

n/i	0	1	2	3	4		
4	1						
5	1	1					
6	1	3	3	1			
7	1	4	5	2			
8	1	5	8	4			
9	1	6	12	8			
10	1	7	17	16	4		
11	1	8	23	28	13	2	
12	1	9	30	45	30	9	1

Multiplying the nth row pointwise with the vector v where $v_i = n-2i$ yields the following. The row sums give column 3 in Table 6.21 below.

Table 6.20: Number of permutations with i fixed points for $k = 3$.

n/i	0	1	2	3	4	
2	2					
3	3					
4	4	2				
5	5	6	1			
6	6	12	6	0		
7	7	20	15	2		
8	8	30	32	8		
9	9	42	60	24		
10	10	56	102	64	8	
11	11	72	161	140	39	2

Example 32. The row sums of layer k of Pascal's array yield the following. We conjecture that each n, k entry is the total number of fixed points in a k-drop permutation on n elements (equivalently, the total number of elements in all subsets on $n - k$ elements, no two of whom have difference k.)

Table 6.21: Conjecture: the n, k entry gives the total number of fixed points in all k-drop permutations of length n.

n/k	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2	2
3	5	4	3	3	3	3	3	3	3	3
4	10	8	6	4	4	4	4	4	4	4
5	20	16	12	8	5	5	5	5	5	5
6	38	30	24	16	10	6	6	6	6	6
7	71	55	44	32	20	12	7	7	7	7
8	130	100	78	64	40	24	14	8	8	8
9	235	180	135	112	80	48	28	16	9	9
10	420	320	240	192	160	96	56	32	18	10
11	744	564	425	324	272	192	112	64	36	20
12	1308	988	750	540	456	384	224	128	72	40
13	2285	1721	1300	945	756	640	448	256	144	80
14	3970	2982	2240	1650	1242	1056	896	512	288	160
15	6865	5144	3840	2875	2025	1728	1472	1024	576	320
16	11822	8840	6592	5000	3510	2808	2400	2048	1152	640
17	20284	15140	11284	8500	6075	4536	3888	3328	2304	1280
18	34690	25850	19266	14400	10500	7290	6264	5376	4608	2560
19	59155	44015	32747	24320	18125	12555	10044	8640	7424	5120
20	100610	74760	55524	40960	31250	21600	16038	13824	11904	10240

Chapter 7

Proof of Concept: Salem Numbers and Known Roots

In Chapters 4 to 6, we spent a lot of time considering the locations of the roots of various classes of polynomials. We could save some of this effort if we first choose where the roots lie in the complex plane, and then constructed polynomials based on these locations. This would reduce the work involved in conjecturing and proving the locations of the roots, and we could move on to attempting to prove properties of the Vandermonde matrix right away.

To explore this avenue, we briefly consider some properties of the Salem and Pisot numbers. An exploration of these numbers was suggested in [17], and a hypothesis as to the relationship between root location and Vandermonde matrix properties was given. We do a more extensive computational study here, and give some evidence that root magnitude alone is *not* sufficient to determine certain Vandermonde matrix properties.

7.1 Vandermonde matrix properties

Definition 26. A Salem number is a real algebraic integer α with $|\alpha| > 1$ in which one or more of its conjugates are on the unit circle and all the others have magnitude less than 1.

Definition 27. A Pisot number is an algebraic integer α with $|\alpha| > 1$ and all its conjugates of magnitude less than 1.

As was proven in 1944 [33], the smallest Pisot number is the positive root of $x^3 - x - 1$, and is around 1.3247.

The smallest Salem number is unknown.

Conjecture 3 (Lehmer, 1933). *The smallest Salem number is the largest real root of*

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

which is about equal to 1.17628*.*

This is Lehmer's conjecture, proposed in [20], and is a famous open problem in algebraic number theory.

There is one more type of algebraic integer we will work with.

Definition 28. A complex Pisot number is a complex algebraic integer α with $|\alpha| > 1$ and $|\bar{\alpha}| > 1$ and all its conjugates of magnitude less than 1.

We recall some theorems and lemmas from the matrix theory literature we will use below.

Theorem 25. *[[25] Theorem 3.1] Let V be a nonsingular Vandermonde matrix and let $r_i, 1 \leq i \leq n$ be its nodes. Let $r_+ = \max_{i=0}^{n-1} |r_i|$ and $|V| = \max\{1, r_+^{n-1}\}$. Then*

$$|V| \leq \sigma_1(V) \leq n|V|.$$

The following is a useful lower bound on $\sigma_n(V)$.

Theorem 26 ([18]). *Let V be a Vandermonde matrix with distinct nodes $r_1, \dots, r_n$. Then*

$$\max_{1 \leq i \leq n} \prod_{j=1, j\neq i}^{n} \frac{\max(1, |r_j|)}{|r_i - r_j|} \leq ||V^{-1}||_\infty$$

An easy corollary results.

Corollary 11 ([5]). *Let V be a Vandermonde matrix with distinct nodes $r_1, \dots, r_n$. Then*

$$\frac{1}{\sqrt{n}} \max_{1 \leq i \leq n} \prod_{j=1, j\neq i}^{n} \frac{\max(1, |r_j|)}{|r_i - r_j|} \leq ||V^{-1}||_2.$$

We construct the Vandermonde matrix V from the roots of the minimal polynomial of α

and bound its spectral distortion.

Theorem 27. *Where α is a Pisot number or a Salem number and V is the Vandermonde matrix of α, then*

$$|\alpha|^{n-1} \leq \sigma_1(V) \leq n|\alpha|^{n-1} \tag{7.1}$$

and

$$\sigma_i(V) \leq \sqrt{n(n-i+1)} \tag{7.2}$$

and

$$\frac{|\alpha|}{\sqrt{n}|\alpha+2|^{n-1}} \leq \sigma_n(V) \tag{7.3}$$

Proof. Without loss of generality, let $r_1 = \alpha$. By construction, the r_i of V with largest modulus is α. Thus equation 7.1 is immediate from Theorem 25.

For equation 7.2, let $2 \leq i \leq n$ and let V_{approx} be V with the last $i-1$ rows set to 0. Then by Theorem 1,

$$\sigma_i(V) \leq \|V - V_{approx}\|_2 = \| \begin{bmatrix} 0 & 0 & \dots & 0 \\ & & & \vdots \\ 0 & 0 & \dots & 0 \\ 1 & r_i & \dots & r_i^{n-1} \\ & & & \vdots \\ 1 & r_n & \dots & r_n^{n-1} \end{bmatrix} \|_2 \leq \sqrt{n(n-i+1)}$$

where the last inequality follows from Proposition 1 and that $r_i^k \leq 1$ for all k.

For equation 7.3, we consider Corollary 11. Since the bound holds for the index i that maximizes the quantity, we can choose any index i^* and the bound will still hold (though perhaps more loosely). We let $i^* = 1$ and so α is the distinguished node.

The product of the numerator is simply α, since $r_i \leq 1$ for $i = 2 \leq i \leq n$. For the product of denominators, we consider the maximum distance between α and the rest of the roots. As α lies on the real axis and the rest of the roots are complex (because a conjugate of α would have the same modulus as α and thus lie outside the unit circle), the maximum distance is from α to the opposite side of the circle, and thus is $\alpha + 2$. Replacing the product of the denominators with $n-1$ copies of $|\alpha + 2|$ yields the result. □

We have no reason to believe the above bound should be tight; we made numerous estimates in the proof which revised this bound downward. With more knowledge of the location of the roots of the minimal polynomial, we could potentially make fewer estimates and tighten the bound. However, the bound is useful is at stands, especially for small α in low n, and as a way of bounding condition number and spectral distortion, as we now show.

Corollary 12. *Where V is a Vandermonde matrix of Salem numbers, its* 2 *norm condition number κ satisfies*

$$\kappa(V) \leq n^{3/2}|\alpha|^{n-2}|\alpha+2|^{n-1}.$$

Proof. Immediate from equations 7.1 and 7.3. □

Upper and lower bounds for spectral distortion follow easily as well.

Corollary 13. *Where V is a Vandermonde matrix of Salem numbers, its* 2 *normalized spectral norm ρ satisfies*

$$\rho(V) \leq n^{3/2}|\alpha+2|^{n}.$$

Proof. First recall that $|\det(V)| = \prod_{i=1}^{n} \sigma_i(V)$. By equations 7.1 and 7.2,

$$\begin{aligned}|\det(V)| \leq n|\alpha|^{n-1}\prod_{i=2}^{n-1}\sqrt{n(n-i+1)} &\leq n|\alpha|^{n-1}\sqrt{n}^{n-1}\prod_{i=2}^{n-1}\sqrt{(n-i+1)}\\ &\leq n|\alpha|^{n-1}\sqrt{n}^{n-1}\sqrt{n}^{n-1}.\end{aligned}$$

Thus

$$|\det(V)|^{1/n} \leq n|\alpha|.$$

Combining with equation 7.3,

$$\rho = |\det(V)|^{1/n}\|V^{-1}\|_2 \leq n|\alpha|(\frac{\sqrt{n}|\alpha+2|^{n-1}}{|\alpha|}) = n^{3/2}|\alpha+2|^{n-1}.$$

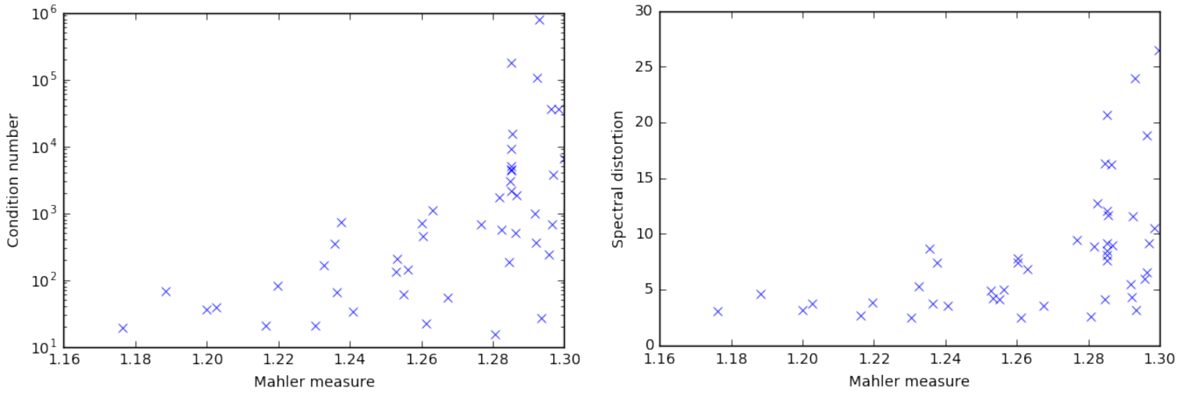
□

Note we sacrificed some tightness of the bound for the sake of readability in the proof above. Reverting to the factorial on the first line would give a tighter bound, should it be needed.

From the bounds above, we have shown that a large κ or a large ρ implies a large n and/or α. However, nothing in these inequalities implies the converse: a large α does not imply a large κ or ρ. This becomes evident when we compute κ and ρ for various small values of α, n below.

7.2 Computational results

Our methodology was as follows. We considered the databases in [24] and wrote a Python script to parse the raw text files and convert it into a set of polynomials in Sage. We began with the 47 polynomials with degree at most 44 which have maximal root modulus (equivalently, Mahler measure) at most 1.3 and plotted condition number and spectral distortion as a function of Mahler measure.



Condition number

Spectral distortion

Figure 7.1: Condition number and spectral distortion as a function of Mahler measure.

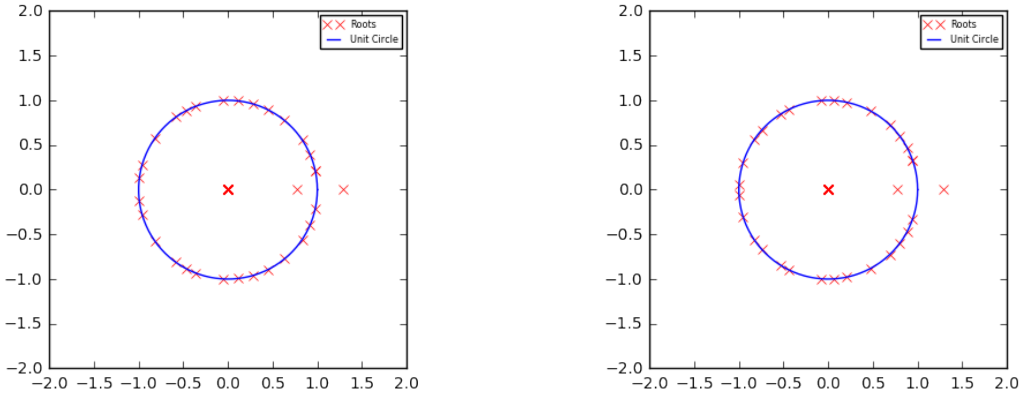
While we can see that higher Mahler measure on average does tend towards both larger condition numbers and spectral distortions, this correspondence is not one to one. For instance, there are many Mahler measure values between 1.28 and 1.3 with much different condition numbers.

Taking into account the role of n, as indicated by the theoretical bounds should influence the behavior, does not completely explain the difference:

Table 7.1: Evidence that n and α do not suffice to determine the magnitude of the condition number.

Mahler measure	n	Condition number
1.2851215	30	9139.26
1.2851857	30	4552.20

Thus, there is at least one other factor which influences the condition number and spectral distortion. While we not yet know what the mystery factor is, it seems like it has to do with the distribution of roots in the complex plane. For the set of roots used in the polynomials in the table above, the roots for the smaller condition number appear slightly more equidistributed around the unit circle.



Roots for line 1 in Table 7.1

Roots for line 2 in Table 7.1

Figure 7.2: Condition number and spectral distortion as a function of Mahler measure.

Formalizing this relationship is an avenue for future work.

Chapter 8

Future Work and Conclusions

While we have made significant contributions to the known literature about k-Fibonacci numbers and have made some interesting observations about the Vandermonde matrices of polynomials of the form $x^n + ax^m + b$, there are of course many further avenues of exploration.

First, consider the relationship between roots of polynomials and singular values of Vandermonde matrices. Some ideas for future work which are based on this thesis include:

- A proof of the root locations and equidistribution properties for $x^n + ax^m + b$ for $m \geq 1$, using either Schur-Cohn or some other method.
- A proof of the singular value gap in the resulting Vandermonde matrix.
- A tightness guarantee on either the root bounds or the singular values.
- Other Vandermonde matrix properties: for instance, bounds on the 2 norm of the inverse, or the norm of the smallest row in the inverse.
- Exploiting the properties of the Vandermonde matrix for non-dual RLWE instances, as was done in the papers cited in Chapter 3.

On the combinatorial side, our first priority is to prove Conjecture 2. Conjecturing and proving any further properties of the three-dimensional analogue of Pascal's triangle (Table 6.21), could also be of independent interest.

On the k-Fibonacci topic, we are also interested in any conjectures and proofs on further permutation statistics of these restricted permutations, and their correspondences in the subsets and compositions. A cleaner criterion of a k-free composition—one which does not depend on the mapping to the binary strings—is also desirable. Furthermore, a non-recursive definition of the numerator tensors could be of interest. Finally, it could be fun to find combinatorial proofs of any of the Chapter 6 lemmas which we proved by induction.

Separately, a solution to the lattice path problem presented in Appendix A is another avenue of exploration.

In conclusion, considering the non-dual RLWE problem leads to an array of fascinating problems: not only in cryptography, but in matrix theory, polynomial theory, and combinatorics, all with varying degrees of relevance to the post quantum problem itself. When we started work on this thesis, we did not expect it to end in Fibonacci numbers. We are excited to see what other mathematical results and problems the post-quantum quest brings to the world in the next many years.

Chapter 9

Appendix A: An Exercise for the Reader

While the permutation argument in Chapter 4 suffices to prove the determinant of the tridiagonal matrix, an attempt using an ultimately less successful method leads to an interesting question in enumerative combinatorics and a possible connection to spectral graph theory. Thus we outline that attempt here.

We begin as above, calculating the Schur-Cohn matrix C for $x^n - x - 1$ as in Chapter 4; recall this is the $0, -1$ matrix that is nearly tridiagonal. Now, instead of calculating the minor sequence of C to obtain the signature and ultimately the number of roots inside the unit circle, we attempt to calculate the characteristic polynomial p and use the Decartes Sign Rule or a similar technique to identify the number of its positive and negative roots. Our thought was that this would avoid the problem of finding the leading minors of the Schur-Cohn matrix. However, we were ultimately less successful with the characteristic polynomial approach, though it did raise some an interesting combinatorics question separate from the k-Fibonacci case already considered.

Proposition 21 ([22])**.** *The eigenvalues of a matrix M are the roots of its characteristic polynomial $p_M(x)$.*

Thus, we have reduced the problem of finding the signature of M to the problem of finding the number of positive and negative roots of the polynomial $p_M(x)$. Since there are many techniques for finding the parity of roots—for instance, Sturm's Theorem or the Descartes Sign Rule—if $p_M(x)$ happens to be easy to construct, this might be a better approach to the signature problem than calculating the Schur-Cohn minors.

So, how do we construct $p_m(x)$? Recall that

$$p_M(x) = \sum_{k=0}^{n} x^{n-k}(-1)^k tr(\Lambda^k M),$$

where

$$tr(\Lambda^k M) = \frac{1}{k!}\begin{vmatrix} trM & k-1 & 0 & \cdots & \\ trA^2 & trM & k-2 & \cdots & \\ \vdots & \vdots & & \ddots & \vdots \\ trM^{k-1} & trM^{k-2} & & \cdots & 1 \\ trM^k & trM^{k-1} & & \cdots & trM \end{vmatrix}$$

So we must first construct the powers of the matrix C, or at least find their diagonals, as a first step to calculating the characteristic polynomial.

One way to find these diagonal powers is to use the following result from graph theory. Note that we can view C as the adjacency matrix of a graph G, where we view a -1 in location i, j as an edge between i and j, and 0 as no edge. Since C is symmetric, the graph is undirected. G looks like this, where more looped nodes could appear in the dotted line areas.

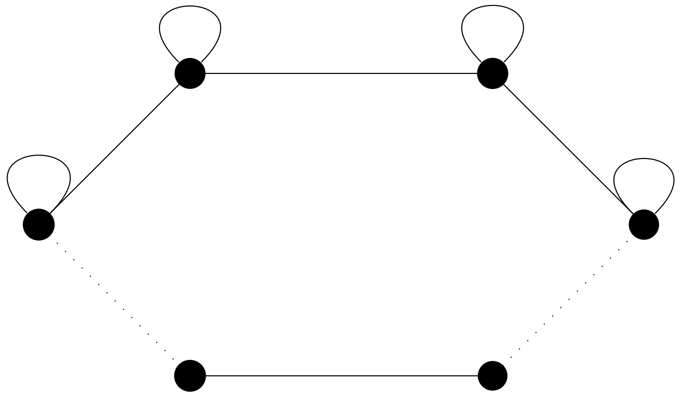


Figure 9.1: The graph G. We wish to count the number of length k closed walks from each vertex.

Then recall the following result.

Proposition 22 ([22])**.** *The i, j entry of the kth power of the adjacency matrix of a graph* *gives the number of walks of length k between vertices i and j.*

Thus, to find the i, i entry of C^k, we would have to count the number of length k closed walks starting and ending at each vertex of the graph which has C as its adjacency matrix.

Label the vertices as follows: let v_0 be the leftmost vertex which has no loop, v_1 as the rightmost vertex with no loop, and proceed to label in counterclockwise order. (This ordering is without loss of generality; other orders simply change the indexing.) Label a clockwise step with a -1, a counterclockwise step with a 1, and staying on a vertex (taking a loop) as 0. Viewed in this way, the definition immediately recalls the idea of a lattice path from combinatorics.

Definition 29 ([35])**.** A lattice path L in $\mathbb{Z}^d$ of length k with steps in S is a sequence $v_0, v_1, \ldots, v_k \in \mathbb{Z}^d$ such that each consecutive difference $v_i - v_{i-1}$ lies in$S$.

Since we allow 3 steps, we wish to count a lattice path variant known as a grand Motzkin path.

Definition 30. A grand Motzkin path of length n is a lattice path on $\mathbb{Z} \times \mathbb{Z}$ whose steps are $U = (1, 1), D = (1, -1), H = (1, 0)$ beginning at $(0, 0)$ and ending at $(0, n)$.

We associate a counterclockwise move on G with U, a clockwise move with D, and a loop with H. Thus, the problem statement, which would give us the number of closed walks on G and starting at each vertex and thus the trace of C^k for all k, is the following.

Problem 6. How many grand Motzkin paths of length k have horizontal steps that do not occur at location $y = 0$ or $y = 1$? Or in general, some i and $i+1$, for any $0 \leq i \leq \frac{n-1}{2}$?

Example 33. The total number of grand Motzkin paths of this form (i.e., with no horizontal step restriction) is

$$\sum_{0 \leq i \leq \lfloor k/2 \rfloor} \binom{k}{i, i, k-2i}.$$

These are the central trinomial coefficients, which are the largest coefficient of $(1+x+x^2)^n$. This sequence begins $1, 1, 3, 7, 19, 51, 141, 393$ and is number $A002426$.

As an example, we constructed the first few powers of the $n = 20$ adjacency matrix in Sage. Since G is symmetric, we only display up to $k = 10$ for each power, as the second half is always the same.

Neither this triangle nor its subsequences appear to be catalogued in the OEIS.

Table 9.1: Number of length n closed walks on the graph G with 20 nodes for each vertex k.

n/k	1	2	3	4	5	6	7	8	9	10
0	0	1	1	1	1	1	1	1	1	1
1	2	3	3	3	3	3	3	3	3	3
2	1	6	7	7	7	7	7	7	7	7
3	7	16	19	19	19	19	19	19	19	19
4	9	38	50	51	51	51	51	51	51	51
5	33	100	136	141	141	141	141	141	141	141
6	65	255	369	392	393	393	393	393	393	393
7	191	677	1013	1107	1107	1107	1107	1107	1107	1107
8	454	1789	3100	3138	3139	3139	3139	3139	3139	3139
9	1248	4813	7720	8774	8944	8953	8953	8953	8953	8953

Of course, there are many problems with the graph approach as a potential method for solving the root location problem. To start, once we solve the path problem, we have to take the determinant of the matrix in equation 9, and the way to do that is not apparent. Furthermore, there is the matter of generalization to the $x^n + ax^m + b$ case, which we have not yet considered with this method.

Chapter 10

Appendix B: Code

Here we present the Sage code for the two tasks we thought would be of most interest.

This method constructs the generalized Pascal triangle for given n and k, which we conjecture to count the total number of fixed points in all length n k-drop permutations.

```
import numpy as np
var(’x’)

def fib_indices(n,k):
    """calculates the product and returns which fibonacci
    generating functions we need to be using"""
    inds=[floor((n+i)/(k)+1) for i in range(k)]
    return inds

def fib_diags(n):
    """calculates the tuple of coefficients for the k=1 case"""
    return [binomial(n-i,i) for i in range(0,floor(n/2)+1)]



def fib_poly(diag_list):
    """returns the polynomial given coefficients"""
    return sum([diag_list[i]*x^i for i in range(len(diag_list))])
```

```
def construct_multiplier(n,length):
    """constructs the even/odd multipliers to take the dot product"""
    return [n-2*i for i in range(length)]



def create_poly(n,k):
    """builds the polynomial P_(n,k) from the building blocks"""
    poly_list=[]
    if k==1:
        inds=fib_indices(n,k)
        poly_list.append(fib_poly(fib_diags(n)))
    else:
        inds=fib_indices(n,k)
        for i in range(len(inds)):
            poly_list.append(fib_poly(fib_diags(inds[i]-k+1)))
    coef_list=np.prod(poly_list).expand().coefficients()
    simple_list=[elem[0] for elem in coef_list]
    return simple_list

#to see the first 30 rows of the k=4 layer:

for i in range(5,30):
    print i,create_poly(i,4)
    print
```

The following method constructs the k-Fibonacci generating function for given k. This is a toy implementation. As k of the k-Fibonacci numbers increases, the coefficients of both the tensor and the denominator quickly become quite large, and numerical considerations may have to be taken into account for a full scale implementation. That said, Sage will display the generating functions using this code at least until $k = 15$ with no additional work; recall the current literature only has $k \leq 6$.

```
import numpy as np
def fib_ind(n,k):
    """calculates the product and returns which fibonacci
    generating functions we need to be using"""
    inds=[floor((n+i)/(k)+1) for i in range(k)]
    return inds

def kfib(n,k):
    return np.prod([fibonacci(i) for i in fib_ind(n,k)])

def fibonomial(n,k):
    return np.prod([fibonacci(n-i+1) for i in range(1,k+1)])/...
    (np.prod([fibonacci(i+1) for i in range(1,k)]))

def sfibonomial(n,k):
"""signed fibonomials"""
    return (-1)^(floor(k/2))*np.prod([fibonacci(n-i+1) for i in...
    range(1,k+1)])
    (np.prod([fibonacci(i+1) for i in range(1,k)]))

def N(a,b,c):
"""the numerator tensors """
  if b>a:
      return 0
  if b==c==0:
      return 1
  if b==1:
      return 0
  if c==0:
      if b>a:
          return 0
      else:
          return -1
  else:
      if b==0:
          return -((-1)^(c+1)*kfib(c*(a-1)+2-2,a-1)-...
          sum([(-1)^j*fibonomial(a+j-1,j)*(N(a,2,c-j)) ...
          for j in range(1,c+1)]))
      else:
          return (-1)^(c+1)*kfib(c*(a-1)+b-2,a-1)-...
          sum([(-1)^j*fibonomial(a+j-1,j)*(N(a,b,c-j))...
           for j in range(1,c+1)])

#the whole generating function

def make_gfun(k):
    dim=k*(k-1)
    denom=sum([int(sfibonomial(k-1,i))*x^(i*k) for i in range(0,k)])
    ind=0 #keeping track of the numerator powers
    num=0
    for i in range(0,k-2): #layer
        for j in range(k): #column
            num=num+sum([int(N(k-1,j,i))*x^(ind)])
            ind=ind+1
    return num/(denom*(1-x-x^2))


#to get the generating function for k=7:

make_gfun(7)

#to expand and obtain first 50 coefficients of the series:

taylor(make_gfun(7),x,0,50)
```

References

[1] FindStat combinatorial statistics database: findstat.org.

[2] NIST post quantum competition: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[3] Online encyclopedia of integer sequences: oeis.org, 2019.

[4] Frank Arunte and Kunal Arya. Quantum supremacy using a programmable superconducting processor. *Nature*, 57(7779):505–510, 2019.

[5] Céline Aubel and Helmut Bölcskei. *Vandermonde matrices with nodes in the unit disk and the large sieve.* pplied and Computational Harmonic Analysis, aug 2017.

[6] Vladimir Baltic. On the number of certain types of strongly restricted permutations. *Applicable Analysis and Discrete Mathematics*, 2009.

[7] Arthur Benjamin. *Proofs That Really Count.* MAA, 2003.

[8] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. Ntru prime: reducing attack surface at low cost. *Cryptology ePrint Archive*, 2017.

[9] Wouter Castryk, Ilia Iliashenko, and Frederik Vercauteren. *Provably Weak Instances of Ring-LWE Revisited*, volume 9665 of *Lecture Notes in Computer Science*, chapter Advances in Cryptology – EUROCRYPT, pages 147–167. Springer, Berlin, Heidelberg, 2016.

[10] Hao Chen, Kristin Lauter, and Katherine E. Stange. Attacks on the search RLWE problem with small errors. *SIAM Journal of Applied Algebra and Geometry*, 2017.

[11] Joanna N Chen and William Y.C Chen. On permutations with bounded drop size. *Arxiv*, 2013.

[12] Fan Chung, Anders Claesson, Mark Dukes, and Ron Graham. Descent polynomials for permutations with bounded drop size. *Arxiv*, 2010.

[13] David S Dummit and Richard M Foote. *Abstract Algebra.* Prentice Hall, 1991.

[14] Moawwad El-Mikkawy and Tomohipo Sogabe. A new family of k-Fibonacci numbers. *Applied Mathematics and Computation*, 2010.

[15] Moawwad El-Mikkawy and Tomohipo Sogabe. Fast block diagonalization of k-tridiagonal matrices. *Applied Mathematics and Computation*, 2011.

[16] Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. *Provably Weak Instances of Ring-LWE*, volume 9215 of *Lecture Notes in Computer Science*, chapter Advances in Cryptology – CRYPTO. Springer, Berlin, Heidelberg, 2015.

[17] Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. *Ring-LWE Cryptography for the Number Theorist*, volume 3 of *Association for Women in Mathematics Series*. Springer, Cham, 2016.

[18] Walter Gautschi. On inverses of vandermonde and confluent vandermonde matrices iii. *Numerische Mathematik*, 29:445–450, 1978.

[19] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, 2012.

[20] D. H. Lehmer. Factorization of certain cyclotomic functions. *Annals of Mathematics*, 34(3):461–479, 1933.

[21] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Eurocrypt*, 2010.

[22] Carl Meyer. *Matrix Analysis and Applied Linear Algebra*. SIAM, 2000.

[23] Richard A. Mollin. *Algebraic Number Theory*. Chapman and Hall/CRC, 1999.

[24] Michael Mossinghoff. Lehmer's problem homepage.

[25] Victor Y. Pan. How bad are Vandermonde matrices? *SIAM Journal of Matrix Analysis and Applications*, 2015.

[26] Chris Peikert. How (not) to instantiate ring-LWE. In *Proceedings of the 10th International Conference on Security and Cryptography for Networks*, pages 411–430, Berlin, Heidelberg, 2016. Springer.

[27] Q.I. Rahman and G. Schmeisser. *Analytic Theory of Polynomials*. Oxford Science Publications, 2002.

[28] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Proceedings of the thirty-seventh annual ACM symposium on theory of computing*, 2005.

[29] Oded Regev. The learning with errors problem. *Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity*, pages 191–204, 2010.

[30] J. Riordan. Generating functions for the powers of Fibonacci numbers. *Duke Mathematical Journal*, 29:5–12, 1962.

[31] Ron Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[32] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-LWE and polynomial-LWE problems. *EUROCRYPT*, pages 146–173, 2018.

[33] R. Salem. A remarkable class of algebraic integers. proof of a conjecture of vijayaraghavan. *Duke Mathematical Journal*, 11(1):103–108, 1944.

[34] Peter Schor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[35] Richard Stanley. *Enumerative Combinatorics Volume 1.* Cambridge, 2nd edition, 2012.

[36] M. Tetiva. Subsets that make no difference d. *Mathematics Magazine*, 2011.