Some Results on Pell Equations and Sequence Autocorrelations

by

Daniel Tarnu

M.Sc., Western Washington University, 2019
B.Sc., Western Washington University, 2017

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Summer 2023

Declaration of Committee

Name:	**Daniel Tarnu**
Degree:	**Doctor of Philosophy**
Thesis title:	**Some Results on Pell Equations and Sequence Autocorrelations**
Committee:	**Chair:** Ralf Wittenberg Associate Professor, Mathematics
	Stephen Choi Supervisor Professor, Mathematics
	Imin Chen Committee Member Professor, Mathematics
	Marni Mishna Examiner Professor, Mathematics
	Daniel Katz External Examiner Associate Professor, Mathematics California State University - Northridge

Abstract

Pell equations are Diophantine equations of the form $x^2 - Dy^2 = 1$. For fixed D, all positive solutions are generated by powers of a single solution, known as the fundamental solution. In the first chapter, we introduce the concept of the "gap order" of any integer polynomial f, which concerns the finiteness of ordered tuples $(s_0, s_1, \cdots, s_\ell)$ with $f(s_i) \mid f(s_{i+1})$ and s_ℓ/s_0 bounded. We determine the gap order for all integer polynomials, answering a conjecture by Chan-Choi-Lam. The proof of this result partially relies upon bounds for solutions to systems of Pell equations, and the existence of solutions to Pell equations that satisfy certain congruence conditions.

In Chapter 2, we explore the multiplicative order $g(D)$ of solutions $(x, y) = (s, t)$ of the Pell equation $x^2 - Dy^2 = 1$, viewed as elements $s + t\sqrt{D}$ of $\mathbb{Z}[\sqrt{D}]/\langle D \rangle$. Our main results for this chapter are establishing a method of constructing the solution set for $x^2 - D^{2n+1}y^2 = 1$ from the fundamental solution of $x^2 - Dy^2 = 1$ for any $n \in \mathbb{N}$, and using this to find $g(D^{2n+1})$ for sufficiently large n.

Afterwards, we focus on Rudin-Shapiro (R-S) sequences and their autocorrelations. Our main result for this chapter is an alternative proof of the order of the maximal aperiodic autocorrelation of R-S sequences originally proven by Allouche, Choi, Denise, Erdélyi, and Saffari, and we extend this to periodic autocorrelations. We also discuss the connection between our main result and the burgeoning field of joint spectral radius theory.

In Chapter 4, we present an extension of the main result of the previous chapter and a result on the sum of squares of R-S sequence autocorrelations, proven implicitly by Littlewood and explicitly by Høholdt-Jensen-Justesen. We also establish bounds on the sum of magnitudes of R-S sequence autocorrelations. Finally, we present a conjecture on which autocorrelation is maximal, and we provide evidence for this by proving an analogous result for a function we construct from the autocorrelations.

Keywords: Pell equation; Diophantine equation; binary sequence; Rudin-Shapiro sequence; sequence autocorrelation

Dedication

To Abby and Mew.

Acknowledgements

I feel lucky to have been under the supervision of Stephen Choi, whose mentorship I appreciate immensely. Your unwavering support and enthusiasm kept me in high spirits throughout this process, and your openness to exploring problems and discussing ideas left an impression on me as a researcher and collaborator.

Similarly, I am very grateful for the guidance of Imin Chen. Thank you for the insightful conversations, and for your feedback and moral support.

Thank you to Árpád, Andy, Jeff, Sean, and Chris, without whom I would not have pursued this degree.

Thank you to Jesse, Aniket, and Alex for giving me the warmest of welcomes to Burnaby, and to all my friends at SFU and abroad, and the weary souls of K9506, for keeping me in good company.

Thank you to Maggie, who blessed me with her patience and encouragement.

And of course, I would like to thank my family. I would not have gotten this far without them.

Table of Contents

Introduction

This thesis consists of four chapters, the first two of which are related to the theory of Pell equations, and the last two of which have to do with a famous class of binary sequences called the Rudin-Shapiro sequences and their autocorrelations. In Chapter 1, for $p \in \mathbb{Z}[x]$, we study the finiteness of ordered tuples $(s_0, s_1, \cdots, s_\ell)$ with $p(s_i) \mid p(s_{i+1})$ and s_ℓ/s_0 bounded by a fixed $N \in \mathbb{N}$. We determine that, up to multiplication by scalars,

(i) if p is of degree 0 or a positive power of a linear polynomial, then there exists an infinite sequence of such ordered tuples for all $\ell \in \mathbb{N}$;

(ii) if p is a positive power of a quadratic polynomial with two distinct roots, then there exists an infinite sequences of such ordered tuples only for $\ell = 1$;

(iii) if p is any polynomial other than those mentioned in (i) and (ii), then there does not exist an infinite sequence of such ordered tuples for all $\ell \in \mathbb{N}$.

This fully determines the *gap order* of integer polynomials which was introduced by Chan-Choi-Lam in [18], and answers the main conjecture of their paper. In the process of proving (ii) above, we must consider solutions to simultaneous Pell equations and solutions (x, y) to Pell equations which also have congruence conditions on x and y modulo D, that is

$$\begin{aligned} x^2 - Dy^2 &= 1, \\ x &\equiv a \pmod{D}, \\ y &\equiv b \pmod{D}. \end{aligned} \tag{1}$$

In Chapter 2, we expound on the methods used to deal with the Pell equation and congruence conditions in (1). We first observe that the solution set to (1) is generated by powers of small positive solutions of (1). In particular, these powers are multiples of $g(D)$, which denotes the smallest positive integer n such that $(x_0 + y_0\sqrt{D})^n \equiv 1 \pmod{\langle D \rangle}$ in $\mathbb{Z}[\sqrt{D}]$, where (x_0, y_0) is the fundamental solution of $x^2 - Dy^2 = 1$. In view of this, we

study $g(D^{2n+1})$ and find that

$$g(D^{2n+1}) = \begin{cases} D^{2n+1} & \text{if } D \text{ is odd and } \operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 1, \\ 2D^{2n+1} & \text{if } D \text{ is odd and } \operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 2, \\ D^{2n+1} & \text{if } D \text{ is even} \end{cases}$$

for sufficiently large $n \in \mathbb{N}$. In order to prove this, we compute the power $M \in \mathbb{N}$ such that (x_M, y_M) is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$, where

$$(x_0 + y_0\sqrt{D})^M = x_M + y_M\sqrt{D^{2n+1}}.$$

In Chapter 3, we provide a simpler proof of the bound

$$\max_{k \neq 0} |C_m(k)| \asymp \lambda^m, \tag{2}$$

originally proven by Allouche-Choi-Denise-Erdélyi-Saffari and Choi, where $C_m(k)$ is the aperiodic autocorrelation at shift k of the m-th Rudin-Shapiro sequence and λ is the real root of $x^3 + x^2 - 2x - 4$. Similarly to Allouche et al., we also establish that there exist matrices $M_1, M_2 \in \mathbb{Z}^{3\times 3}$ and a vector $v_m \in \mathbb{Z}^3$ with $C_m(k)$ as its first component and

$$v_m = \left(\prod_{i=0}^{m-2} M_1^{\delta_i} M_2^{1-\delta_i} \right) v$$

for some $\delta_i \in \{0, 1\}$ and $v \in \mathbb{Z}^3$. We also explore the connection between (2) and the joint spectral radius of M_1 and M_2.

Finally, in Chapter 4, we extend the methods developed in Chapter 3 to get the bounds

$$\max_{0<k\leq x} |C_m(k)| \asymp x^{\log_2(\lambda)},$$
$$\sum_{0<k\leq x} C_m(k)^2 \asymp x^2,$$

and

$$x^{\log_2(4/\lambda)} \ll \sum_{0<k\leq x} |C_m(k)| \ll x^{3/2}.$$

We conclude with the construction of a function $f : [0, 1] \to \mathbb{R}$ with

$$f(x) = \lim_{m\to\infty} \frac{|C_m(\lfloor x2^m \rceil)|}{\lambda^{m-2}}.$$

We find that $x = 2/3$ is the unique global maximum of f, supporting our conjecture that the shift that gives maximal $|C_m(k)|$ is unique and tends to $(2/3) \cdot 2^m$.

Chapter 1

The gap principle

The results of this chapter come from joint work with Stephen Choi and Peter Lam (see [20]).

1.1 Introduction

1.1.1 Notation

Here, we list all potentially ambiguous notation used in this chapter:

(i) For functions f and g from $\mathbb{R} \to \mathbb{R}$, we write

$$f(x) \ll g(x)$$

for $x \in I \subset \mathbb{R}$ if and only if there exists an absolute constant $K > 0$ such that

$$|f(x)| \leq K|g(x)|$$

for all $x \in I$.

(ii) For R a commutative ring and $x \in R$, we denote by $\langle x \rangle \subset R$ the ideal generated by x, defined by

$$\langle x \rangle = \{xr : r \in R\}.$$

(iii) For R a commutative ring, we denote by $R^\times$ its group of units.

1.1.2 Overview

The idea of the gap principle starts with [26], in which Erdős and Rosenfeld consider the differences, or "gaps", between complementary positive divisors of a positive integer n. In particular, they consider

$$D(n) := \{d : d = |a - b|,\ n = ab\} = \{d_0, d_1, \ldots, d_k\}, \tag{1.1}$$

where $d_i < d_{i+1}$ for all $0 \leq i < k$ in the context of the question: for all $k \in \mathbb{N}$, do there exist integers $N_1 < N_2 < \cdots < N_k$ such that $|\bigcap_{i=1}^{k} D(N_i)| \geq k$? This question arose from an attempt to answer a question put forth by Erdős on the number of odd distances that can be attained between points in the plane. In the notation of (1.1), they find that $d_1 \geq 2n^{1/4}$, which leads them to study how many gaps that n could have that are smaller than $cn^{1/4}$ for fixed $c > 2$. It turns out that this is essentially asking how many divisors n has between $n^{1/2}$ and $n^{1/2} + cn^{1/4}$. They note that the number of such divisors is bounded above by $1 + c^2$. Thus, they follow this by inquiring if the number of divisors between $n^{1/2}$ and $cn^{1/4}$ is *absolutely* bounded for *any* c, given that n is sufficiently large. More precisely, they pose the following question.

Question 1. Is there an absolute constant K so that for every c, there exists $n_0 = n_0(c)$ such that the number of divisors of n between $n^{1/2}$ and $n^{1/2}+cn^{1/4}$ is at most K for $n > n_0$?

Chan, in [16], answers this question in the affirmative for $c \geq 3$ and n being a perfect square. In [17], Chan studies a strengthening of Question 1 and in the process considers the following question.

Question 2. Suppose $a < b$ and $a^2(a^2 + 1)$ divides $b^2(b^2 + 1)$. Must it be true that there is some "gap" between a and b in the sense that $\frac{b}{a} > a^{\lambda}$ for some small $\lambda > 0$?

Under the conditions $\gcd(a^2, b^2 + 1) = a^2/\gcd(a^2, b^2)$ and $\gcd(a^2 + 1, b^2) = b^2/\gcd(a^2, b^2)$, Chan shows that

$$\frac{b}{a} \gg \frac{(\log a)^{1/8}}{(\log\log a)^{12}},$$

where the implicit constant does not depend on a or b. This leads Chan-Choi-Lam in [18] to pursue a more general setting to study these gaps (in the sense of Chan's Question 2) between integers related by a divisibility criterion:

Definition 1.1.1. *Let $f \in \mathbb{Z}[x]$ and $\ell \in \mathbb{N}$. We say that f satisfies the* **gap principle of order** *ℓ if and only if for any sequence $\{\boldsymbol{s}_j\}_{j=1}^{\infty}$ with $\boldsymbol{s}_j = (s_{0j}, s_{1j}, \ldots, s_{\ell j}) \in \mathbb{N}^{\ell+1}$ for all j such that*

(i) $s_{ij} < s_{(i+1)j}$,

(ii) $f(s_{ij}) \mid f(s_{(i+1)j})$,

(iii) $\lim_{j\to\infty} s_{0j} = \infty$

for all $0 \leq i \leq \ell - 1$, we have

$$\lim_{j\to\infty} \frac{s_{\ell j}}{s_{0j}} = \infty.$$

Definition 1.1.2. *Let $f \in \mathbb{Z}[x]$. We define the* **gap order** *of f to be the smallest $\ell \in \mathbb{N}$ such that f satisfies the gap principle of order ℓ. If such an ℓ does not exist, we say that f* **does not satisfy the gap principle**.

In other words, for $f \in \mathbb{Z}[x]$ to satisfy the gap principle of order ℓ, we must have, for any sequence $(s_0, \ldots, s_{\ell+1}) \in \mathbb{N}^{\ell+1}$ satisfying conditions (i) and (ii) of Definition 1.1.1, that $f(s_{\ell+1})/f(s_0)$ can be made arbitrarily large if we insist that s_0 is sufficiently large. One can see that the study of Question 2 is basically the study of the gap principle of order 1 for $f(x) = x^2(x^2+1)$, although the lower bound of b/a as defined in the question may be weakened to $g(a)$ for any $g : \mathbb{N} \to \mathbb{R}$ such that $\lim_{a\to\infty} g(a) = \infty$. We now verify the existence of the sequences mentioned in Definition 1.1.1 for every ℓ, so that a polynomial may not vacuously satisfy the gap principle of order ℓ for some ℓ.

Lemma 1.1.3. *Let $f \in \mathbb{Z}[x]$ and $\ell \in \mathbb{N}$. For sufficiently large $s_0 \in \mathbb{N}$, there exists $(s_0, \ldots, s_\ell) \in \mathbb{N}^{\ell+1}$ such that $s_i < s_{i+1}$ and $f(s_i) \mid f(s_{i+1})$ for all $0 \le i \le \ell - 1$.*

Proof. Let $a \in \mathbb{N}$. Observe that

$$(a \pm f(a))^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} (\pm f(a))^k,$$

so

$$(a \pm f(a))^n \equiv a^n \pmod{f(a)}.$$

It follows that

$$f(a \pm f(a)) \equiv f(a) \equiv 0 \pmod{f(a)}.$$

For sufficiently large a, we may insist that either $a < a + f(a)$ or $a < a - f(a)$. Suppose without loss of generality that $a < a + f(a)$ and let $g(x) = x + f(x)$ with

$$g^\ell = \underbrace{g \circ g \circ \cdots \circ g}_{\ell \text{ of } g}.$$

Taking $(s_0, s_1, \ldots, s_\ell)$ to be $(a, g(a), \ldots, g^\ell(a))$ proves the claim. □

Since Lemma 1.1.3 guarantees, for *every* sufficiently large positive integer s_0, the existence of a sequence $(s_0, \ldots, s_\ell) \in \mathbb{N}^{\ell+1}$ that satisfies the conditions (i) and (ii) of Definition 1.1.1, we have existence of an infinite collection of sequences, $\{(s_{0j}, s_{1j}, \ldots, s_{\ell j})\}_j$ with $s_{0j} = j$ for j sufficiently large, which satisfies all conditions of Definition 1.1.1. For any polynomial f that is of degree 0 or is a power of a linear polynomial, these sequences have, for all ℓ, the ratio $s_{\ell j}/s_{0j}$ bounded absolutely, showing that f does not satisfy the gap principle. At the end of this chapter, we show that the same cannot be said for all other polynomials, making these sequences not particularly when studying their gap orders.

We may pare down our study of the gap principle by disregarding rational multiples or powers of any $f \in \mathbb{Z}[x]$ as the following lemma shows.

Lemma 1.1.4. *Let $f \in \mathbb{Z}[x]$. Then, f satisfies the gap principle of order ℓ if and only if Kf^n for $K \in \mathbb{Q} \setminus \{0\}$ and $n \in \mathbb{N}$ satisfies the gap principle of order ℓ.*

Proof. Let $K \in \mathbb{Q} \setminus \{0\}$ and $n \in \mathbb{N}$ and suppose that $\{\mathbf{s}_j\}_{j=1}^{\infty}$ with $\mathbf{s}_j = (s_{0j}, s_{1j}, \ldots, s_{\ell j}) \in \mathbb{N}^{\ell+1}$ satisfies conditions (i) and (iii) of Definition 1.1.1. We see that

$$f(s_{ij}) \mid f(s_{(i+1)j}) \quad \text{if and only if} \quad K(f(s_{ij}))^n \mid K(f(s_{(i+1)j}))^n$$

for all $0 \leq i \leq \ell - 1$. Thus, the sequences $\mathbf{s}_j \in \mathbb{N}^{\ell+1}$ satisfying conditions (i)-(iii) of Definition 1.1.1 are exactly the same for both f and Kf^n, and so f satisfies the gap principle of order ℓ if and only if Kf^n satisfies the gap principle of order ℓ. □

Chan-Choi-Lam, in [18], conjectured that the only polynomials which do not satisfy the gap principle are those that are of degree 0 or powers of linear polynomials, up to multiplication by rational scalars. The following theorem is the main result of this chapter, and it not only confirms the conjecture by Chan-Choi-Lam, but also establishes the gap order of all other polynomials with integer coefficients.

Theorem 1.1.5. *For any polynomial $f \in \mathbb{Z}[x]$, we have that*

(i) if $f = Kg$ where $K \in \mathbb{Q}$ and $g \in \mathbb{Z}[x]$ is either of degree 0 or a power of linear polynomial, then f does not satisfy the gap principle,

(ii) if $f = Kg$ where $K \in \mathbb{Q} \setminus \{0\}$ and $g \in \mathbb{Z}[x]$ is a power of a quadratic with two distinct roots, then f is of gap order 2,

(iii) if $f(x) \neq K(c_2x^2 + c_1x + c_0)^n$ for any $K \in \mathbb{Q}$, $c_j \in \mathbb{Z}$, and $n \geq 0$, then f is of gap order 1.

Part (i) of this theorem was shown in [17] and [18], but we provide another proof in Section 1.4. As mentioned in the introduction to this thesis, the idea of the gap principle is tangentially related to the theory of Pell equations in that proving (ii) prompts consideration of certain Pell equations. We develop some of the ideas used for proving (ii) in the next chapter. We conclude this introductory section with an equivalent definition of the gap principle of order 1 which is simpler and is used several times throughout this chapter.

Lemma 1.1.6. *A polynomial $f \in \mathbb{Z}[x]$ does not satisfy the gap principle of order 1 if and only there exists $N > 1$ such that*

$$S_N(f) := \{(x, y) \in \mathbb{N}^2 : f(x) \mid f(y), 1 < y/x \leq N\}$$

is infinite.

Proof. Suppose that f does not satisfy the gap principle of order 1. Then, by Lemma 1.1.3, there exists a sequence $\{(x_j, y_j)\}_{j=0}^{\infty}$ with $x_j < y_j$ and $f(x_j) \mid f(y_j)$ with $\lim_{j\to\infty} x_j = \infty$ and $\{y_j/x_j\}_{j=0}^{\infty}$ does not diverge. Then, there exists a subsequence $\{(x'_j, y'_j)\}_{j=0}^{\infty} \subset \{(x_j, y_j)\}_{j=0}^{\infty}$ with $\{y'_j/x'_j\}_{j=0}^{\infty}$ bounded. Note that since $\lim_{j\to\infty} x_j = \infty$, this subsequence is also infinite as a set. So, there exists $N > 1$ such that $1 < y'_j/x'_j \leq N$ for all $j \geq 0$. Since $\{(x'_j, y'_j)\}_{j=0}^{\infty} \subset S_N(f)$, we have shown that $S_N(f)$ is infinite.

Now, suppose that $S_N(f)$ is infinite. Then, there exists an infinite sequence $\{(x_j, y_j)\}_{j=0}^{\infty}$ of distinct points in $S_N(f)$. We wish to show that this sequence satisfies conditions (i)-(iii) of Definition 1.1.1. By the definition of $S_N(f)$, we have conditions (i) and (ii). We claim that $\lim\limits_{j\to\infty} x_j = \infty$. Suppose for contradiction that it does not, so that there exists a subsequence

$$\{(x'_j, y'_j)\}_{j=0}^{\infty} \subset \{(x_j, y_j)\}_{j=0}^{\infty}$$

for which the x'_j converge, so we have $x'_j = k$ for sufficiently large j because $x'_j \in \mathbb{N}$ for all j. Then, since $1 < y'_j/x'_j \leq N$ for all j, we must have that two points in $\{(x'_j, y'_j)\}_{j=0}^{\infty}$ are the same, which is a contradiction due to all (x_j, y_j) being distinct. Thus, we have shown condition (iii) of Definition 1.1.1. Finally, we note that since $1 < y_j/x_j \leq N$ for all j, we have that

$$\limsup_{j\to\infty} \frac{y_j}{x_j} \leq N < \infty.$$

So, f does not satisfy the gap principle of order 1. □

We phrase the lemma above in the contrapositive as we use it more so to show that certain polynomials do *not* satisfy the gap principle of certain orders.

1.1.3 Pell equations

A *Pell equation* is a Diophantine equation of the form

$$x^2 - Dy^2 = 1 \tag{1.2}$$

with non-square $D \in \mathbb{N}$. Of course, if $D = N^2$ for some $N \in \mathbb{N}$, we would have by (1.2) that $(x - Ny)(x + Ny) = 1$, implying that $(x - Ny, x + Ny) = \pm(1, 1)$, which restricts (1.2) to having only finitely many solutions. Considering only non-square D guarantees us infinitely many solutions, as we shall see. We are only concerned with integer solutions (referred to simply as solutions) of (1.2), which we denote by tuples (x, y) and sometimes by the expression $x + y\sqrt{D}$ for convenience.

Up to this point, we have barely touched upon how the gap principle connects to the theory of Pell equations. We provide a brief description here, and will elaborate in Sections 1.3 and 1.4. If $f(a) \mid f(b)$ for some $a, b \in \mathbb{Z}$, then we have $f(b) = kf(a)$ for some $k \in \mathbb{Z}$. In the case of f being quadratic, one can use a and b to construct an integer solution to the

generalized Pell equation

$$x^2 - ky^2 = N \tag{1.3}$$

for some $N \in \mathbb{Z}$. This is essentially how Pell equations appear in this chapter. In particular, the proof of Theorem 1.1.5 requires us, roughly, to bound b given that b is somehow critical to solving a system of two generalized Pell equations. Also, we at some point must find infinitely many solutions to a Pell equation that satisfy certain congruences. In Chapter 2, we explore new ways of constructing solutions to $x^2 + D^{2n+1}y^2 = 1$ for $n \in \mathbb{N}$ from those of (1.2). For this, we need more basic results concerning Pell equations, which we leave for Chapter 2 as we do not need them for this chapter.

The concept of the Pell equation has persisted through millennia, having been considered even by Archimedes in ancient Greece. In 628, Brahmagupta showed that for two solutions (s_1, t_1) and (s_2, t_2) of (1.2), we have that

$$(s_1 + \sqrt{D}t_1)(s_2 + \sqrt{D}t_2) = (s_1s_2 + Dt_1t_2) + (s_1t_2 + s_2t_1)\sqrt{D} \tag{1.4}$$

is another solution of (1.2) (see [39, p. 248]). In fact, if each (s_i, t_i) for $1 \leq i \leq 2$ is a solution to the *generalized* Pell equation

$$x^2 - Dy^2 = k_i$$

for some $k_i \in \mathbb{Z}$, then (1.4) gives a solution to the generalized Pell equation $x^2 - Dy^2 = k_1k_2$. This gives a way to generate (infinitely many) solutions of a given (generalized) Pell equation from two known (nontrivial, i.e., not $\pm(1, 0)$) solutions.

1.2 Polynomials of gap order 1

We begin by showing that polynomials f such that

$$f(x) \neq K(c_2x^2 + c_1x + c_0)^n$$

for any $K \in \mathbb{Q}$ and $c_j \in \mathbb{Z}$ satisfy the gap principle of order 1. As Theorem 1.1.5 suggests, these are the only polynomials of gap order 1. We will use the following powerful and celebrated result of Bilu and Tichy.

Theorem 1.2.1 (Bilu and Tichy, 2000)**.** *The equation*

$$f(x) = g(y),$$

for non-constant polynomials $f, g \in \mathbb{Q}[x]$, has infinitely many rational solutions $(x, y) \in \mathbb{Q}^2$ with bounded denominator if and only if

$$f = \varphi \circ \hat{f} \circ \lambda,$$
$$g = \varphi \circ \hat{g} \circ \lambda$$

for some $\varphi \in \mathbb{Q}[x]$, linear polynomials $\lambda, \mu \in \mathbb{Q}[x]$, and either $(\hat{f}(x), \hat{g}(x))$ or $(\hat{g}(x), \hat{f}(x))$ being one of the following "standard pairs" such that $\hat{f}(x) = \hat{g}(y)$ has infinitely many rational solutions with bounded denominator (i.e., reduced fractions p_0/q_0 with $|q_0|$ bounded):

1. *$(x^m, ax^r p(x)^m)$, where $a \in \mathbb{Q}$, $0 \leq r < m$, $\gcd(r, m) = 1$, and $r + \deg(p) > 0$,*
2. *$(x^2, (ax^2 + b)p(x)^2)$ where $a, b \in \mathbb{Q}$ and $p \in \mathbb{Q}(x)$,*
3. *$(D_m(x, a^n), D_n(x, a^m))$, where $a \in \mathbb{Q}$, $\gcd(n, m) = 1$, and D_j is the j-th Dickson polynomial of degree j, defined by*

$$D_j(x + a/x, a) = x^j + (a/x)^j,$$

4. *$(a^{-m/2} D_m(x, a), -b^{-n/2} D_n(x, b))$, where $a, b \in \mathbb{Q}$ and $\gcd(n, m) = 2$,*
5. *$((ax^2 - 1)^3, 3x^4 - 4x^3)$ where $a \in \mathbb{Q}$.*

Proof. This is Theorem 1.1 in [7]. □

The following lemma is just a technical lemma that we will use in the lemma that follows it.

Lemma 1.2.2. *Let $\nu \in \mathbb{Q}[x]$ with $\nu(x) = cx + d$ and $c \neq 1$. Then,*

$$\nu^j(x) = c^j x + d\left(\frac{c^j - 1}{c - 1}\right)$$

for all $j \geq 1$.

Proof. We proceed by induction on j. For $j = 1$,

$$\nu^1(x) = cx + d = c^1 x + d\left(\frac{c^1 - 1}{c - 1}\right),$$

so the claim is verified. Assume for some $n \geq 2$ that

$$\nu^n(x) = c^n x + d\left(\frac{c^n - 1}{c - 1}\right).$$

Then, for $j = n+1$, we see that

$$\begin{aligned}\nu^{n+1}(x) &= c\left[c^n x + d\left(\frac{c^n-1}{c-1}\right)\right] + d \\ &= c^{n+1}x + d\left(\frac{c^{n+1}-c}{c-1}\right) + d \\ &= c^{n+1}x + d\left(\frac{c^{n+1}-c+(c-1)}{c-1}\right) \\ &= c^{n+1}x + d\left(\frac{c^{n+1}-1}{c-1}\right),\end{aligned}$$

which concludes the proof. □

Lemma 1.2.3. *Let $f \in \mathbb{Z}[x]$ be a polynomial such that $f(x) \neq K(c_2x^2 + c_1x + c_0)^n$ for any $K \in \mathbb{Q}$, $c_j \in \mathbb{Z}$, and $n \geq 0$. Let k be an integer greater than 2. Then, the Diophantine equation $f(y) = kf(x)$ does not have infinitely many solutions with bounded denominator.*

Proof. Let $f \in \mathbb{Z}[x]$ be a polynomial such that

$$f(x) \neq K(c_2x^2 + c_1x + c_0)^n \tag{1.5}$$

for any $K \in \mathbb{Q}$, $c_j \in \mathbb{Z}$, and $n \geq 0$. In view of Theorem 1.2.1, it suffices to show that

$$(f, kf) \neq (\varphi \circ \hat{f} \circ \lambda, \varphi \circ \hat{g} \circ \mu)$$

for any $\varphi \in \mathbb{Q}[x]$, linear $\lambda, \mu \in \mathbb{Q}[x]$, and $(\hat{f}, \hat{g})$ being one of the standard pairs given in Theorem 1.2.1, as this would show that $f(y) = kf(x)$ has only finitely many rational solutions with bounded denominator and thus only finitely many integer solutions.

Suppose for contradiction that there exist $\varphi, \hat{f}, \hat{g}, \lambda, \mu \in \mathbb{Q}[x]$ as above such that

$$(f, kf) = (\varphi \circ \hat{f} \circ \lambda, \varphi \circ \hat{g} \circ \mu). \tag{1.6}$$

Since $\deg f = \deg kf$, we must have that $\deg \hat{f} = \deg \hat{g}$. Because of this, $(\hat{f}, \hat{g})$ being a standard pair of the fifth kind is impossible. Also, if $(\hat{f}, \hat{g})$ is a standard pair of the third kind, then we need $\deg D_n = \deg D_m$, meaning $n = m = 1$ and so

$$(\hat{f}, \hat{g}) = (D_1(x, a), D_1(x, a)) = (x, x),$$

which is subsumed by Case 1 below. We will now consider $(\hat{f}, \hat{g})$ being a standard pair of the first, second, or fourth kinds.

Case 1 (first kind): Suppose that $(\hat{f}, \hat{g})$ is a standard pair of the first kind, so without

loss of generality

$$(\hat{f}(x), \hat{g}(x)) = (x^m, ax^r p(x)^m)$$

for some $p \in \mathbb{Q}[x]$. Since $\deg \hat{f} = \deg \hat{g}$, we must have that $(r, \deg p) = (0, 1)$ in which case $m = 1$ because $\gcd(r, m) = 1$, or that $(r, \deg p) = (m, 0)$ and so $r = m = 1$ because $\gcd(r, m) = 1$. In either case, we have that $\hat{f} \circ \lambda$ and $\hat{g} \circ \mu$ are linear polynomials. Using this fact with (1.6), we write

$$(f, kf) = (\varphi \circ \hat{\lambda}, \varphi \circ \hat{\mu})$$

for some linear $\hat{\lambda}, \hat{\mu} \in \mathbb{Q}[x]$. From this, we get the following relations:

$$\begin{aligned} f \circ \hat{\lambda}^{-1} &= \varphi, \\ kf &= \varphi \circ \hat{\mu}. \end{aligned} \tag{1.7}$$

For simplicity, we let

$$\nu(x) = (\hat{\mu} \circ \hat{\lambda}^{-1})(x) = cx + d \in \mathbb{Q}[x]. \tag{1.8}$$

Combining (1.7) with (1.8) yields

$$k\varphi = kf \circ \hat{\lambda}^{-1} = \varphi \circ \nu. \tag{1.9}$$

Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ for $\ell \geq 2$ are the distinct zeros of φ. We will show that, in fact, φ cannot have more than one distinct zero. By (1.9), the zeros of φ are exactly the zeros of $\varphi \circ \nu$. Thus, we must have that ν permutes the zeros of φ. Suppose for contradiction that ν is the trivial permutation on $\{\alpha_i : 1 \leq i \leq \ell\}$, so that $\nu(\alpha_i) = \alpha_i$ for all $1 \leq i \leq \ell$. Then, since ν is a linear polynomial, it follows that $\nu(x) = x$, and applying (1.9) yields $k\varphi = \varphi$, implying that $k = 1$ — a contradiction as $k \geq 2$ by assumption. Since we can view ν as an element of the symmetric group defined over the zeros of φ, denoted by $\mathrm{Sym}(\{\alpha_i : 1 \leq i \leq \ell\})$, and the cardinality of $\mathrm{Sym}(\{\alpha_i : 1 \leq i \leq \ell\})$ is $\ell!$, we know that for all $1 \leq i, j \leq \ell$ with $i \neq j$ that

$$\frac{\nu^{\ell!}(\alpha_i) - \nu^{\ell!}(\alpha_j)}{\alpha_i - \alpha_j} = \frac{\alpha_i - \alpha_j}{\alpha_i - \alpha_j} = 1. \tag{1.10}$$

Recall that $\nu(x) = cx + d \in \mathbb{Q}[x]$. Since $k\varphi = \varphi \circ \nu$, we may not have $c = 1$ or else $k = 1$ by comparing leading coefficients, and this is a contradiction because $k \geq 2$ by assumption. So, we may use Lemma 1.2.2 to assert that for any i, j such that $j \geq 1$ and $1 \leq i \leq \ell$, we have

$$\nu^j(\alpha_i) = c^j \alpha_i + d\left(\frac{c^j - 1}{c - 1}\right). \tag{1.11}$$

In view of (1.10) and the fact that $c \neq 1$, (1.11) implies that

$$\frac{\nu^{\ell!}(\alpha_i) - \nu^{\ell!}(\alpha_j)}{\alpha_i - \alpha_j} = \frac{c^{\ell!}(\alpha_i - \alpha_j)}{\alpha_i - \alpha_j} = c^{\ell!} = 1$$

for $i \neq j$, which gives $c = -1$ and so

$$\nu(x) = -x + d.$$

However, since $k\varphi = \varphi \circ \nu$, this implies that $k = \pm 1$, which is a contradiction since $k \geq 2$ by assumption. Thus, we have shown by contradiction that φ has only one (repeated) zero and is therefore of the form

$$\varphi(x) = K'(c_1'x + c_0')^n \tag{1.12}$$

for some $K', c_j' \in \mathbb{Q}$. This contradicts our assumption (1.5). We conclude that $(\hat{f}, \hat{g}) \neq (x^m, ax^r p(x)^m)$.

Case 2 (second and fourth kinds): Since $\deg f = \deg kf$, if $(\hat{f}, \hat{g})$ is a standard pair of the second or fourth kinds, then both $\hat{f}$ and $\hat{g}$ are quadratic. Also, since $\hat{f}$ has rational coefficients, we must have that its axis of symmetry is $x = v$ for some $v \in \mathbb{Q}$. Then, letting

$$\hat{\lambda}(x) = x + v \in \mathbb{Q}[x],$$

we have that the axis of symmetry of $\hat{f} \circ \lambda \circ \hat{\lambda}$ is $x = 0$. Thus,

$$(\hat{f} \circ \lambda \circ \hat{\lambda})(x) = a_2x^2 + a_0 \tag{1.13}$$

for some $a_j \in \mathbb{Q}$. Using (1.13) on (1.6), we have that

$$(kf \circ \hat{\lambda})(x) = k\varphi(a_2x^2 + a_0) = (\varphi \circ \hat{g} \circ \mu \circ \hat{\lambda})(x) = \varphi(a_2'x^2 + a_1'x + a_0') \tag{1.14}$$

for some $a_j' \in \mathbb{Q}$, where the last equality is due to the fact that $\hat{g} \circ \mu \circ \hat{\lambda}$ is quadratic. Since $a_2x^2 + a_0$ is even, (1.14) tells us that $a_1' = 0$. So,

$$k\varphi(a_2x^2 + a_0) = \varphi(a_2'x^2 + a_0'),$$

and since this holds for all $x \in \mathbb{R}$, we have that

$$k\varphi(a_2x + a_0) = \varphi(a_2'x + a_0') \tag{1.15}$$

for all $x \geq 0$. Since (1.15) holds for all $x \geq 0$ and φ is a polynomial, we actually have that (1.15) holds for all $x \in \mathbb{C}$. We may pick a linear $\nu \in \mathbb{Q}[x]$ such that $k\varphi = \varphi \circ \nu$ and we may treat this in the same way as (1.9) in Case 1. Thus, we arrive at a result analogous to (1.12) in Case 1:

$$\varphi(x) = K'(c_1'x + c_0')^n$$

for some $K, c_j' \in \mathbb{Q}$. However, by (1.14), we have that $(f \circ \hat{\lambda})(x) = \varphi(a_2x^2 + a_0)$, so

$$f = \varphi(a_2(\hat{\lambda}^{-1}(x))^2 + a_0)$$

where $\hat{\lambda}^{-1}$ is linear, which contradicts our assumption (1.5). We conclude that $(\hat{f}, \hat{g})$ is not a standard pair of the second or fourth kinds.

This completes the proof. □

From this result, we may use the helpful equivalent definition of the gap principle given in Definition 1.1.1 in order to conclude that for any $f \in \mathbb{Z}[x]$ with $f(x) \neq K(c_2x^2+c_1x+c_0)^n$, the set $S_N(f)$ as in Lemma 1.1.6 is finite and so f satisfies the gap principle of order 1. We leave the details of this brief argument to Section 1.4.

1.3 Polynomials of gap order 2

In this section, we will first show that for $f = kg$, where g is a quadratic with two distinct roots, we have that f satisfies the gap principle of order 2. We will do so with the original definition given in Definition 1.1.1. Afterwards, we will show that f does not satisfy the gap principle of order 1 using the equivalent definition given by Lemma 1.1.6. Thus, this section is devoted to showing that such f are the only polynomials of gap order 2. We begin with some technical lemmas that extend the ideas formed by Chan in [17] (in the pursuit of answering Question 2 in Section 1.1) and Chan-Choi-Lam in [18].

Lemma 1.3.1. *Let $s_1, s_2 \in \mathbb{Z}$, and $f \in \mathbb{Z}[x]$ be such that $f(x) = ax^2 + bx + c$ with $a \neq 0$ and $\Delta := b^2 - 4ac \neq 0$. Suppose $f(s_2) = d^2 f(s_1)$ for some integer $d > 1$. Then, we have*

$$\frac{2|2as_2 + b| - 1 + |\Delta|}{|\Delta|} \leq d^2.$$

Proof. We will use $f'(s_1) = 2as_1 + b$ (and likewise for s_2) throughout for notational clarity. We first note that

$$4af(x) = (2ax)^2 + 4abx + 4ac = (2ax + b)^2 - (b^2 - 4ac) = (f'(x))^2 - \Delta. \tag{1.16}$$

Our assumption $f(s_2) = d^2 f(s_1)$ is equivalent to $4af(s_2) = d^2(4af(s_1))$, so (1.16) yields

$$|f'(s_2)|^2 - \Delta = |df'(s_1)|^2 - d^2\Delta. \tag{1.17}$$

Let k be such that

$$k = d|f'(s_1)| - |f'(s_2)|.$$

Note that $k \in \mathbb{Z}$ as $f \in \mathbb{Z}[x]$ and $d \in \mathbb{Z}$. We now extend (1.17) to

$$(d|f'(s_1)|)^2 - 2dk|f'(s_1)| + k^2 - \Delta = (d|f'(s_1)| - k)^2 - \Delta = |f'(s_2)|^2 - \Delta = (d|f'(s_1)|)^2 - d^2\Delta.$$

Isolating k^2 on the left side gives

$$\begin{aligned} k^2 &= (d|f'(s_1)|)^2 - d^2\Delta - (d|f'(s_1)|)^2 + 2dk|f'(s_1)| + \Delta \\ &= (1-d^2)\Delta + 2dk|f'(s_1)|, \end{aligned}$$

which implies that

$$k^2 - (1-d^2)\Delta = 2dk|f'(s_1)| = 2k(|f'(s_2)| + k) = 2k|f'(s_2)| + 2k^2.$$

Isolating for d^2 yields

$$d^2 = \frac{k^2 + 2k|f'(s_2)| + \Delta}{\Delta}. \tag{1.18}$$

We will consider Δ being positive and negative separately. Beforehand, note that (1.17) gives us that

$$|f'(s_2)|^2 = (d|f'(s_1)|)^2 + \Delta(1-d^2),$$

so if $\Delta > 0$, then $|f'(s_2)| < d|f'(s_1)|$ and so $k > 0$, and similarly $\Delta < 0$ implies $k < 0$.

First, suppose that $\Delta > 0$. Then $k > 0$, and since $k \in \mathbb{Z}$, we actually have $k \geq 1$. Therefore, by (1.18), we have

$$d^2 \geq \frac{1 + 2|f'(s_2)| + \Delta}{\Delta} \geq \frac{2|f'(s_2)| - 1 + |\Delta|}{|\Delta|},$$

which proves the lemma for $\Delta > 0$.

Now, suppose that $\Delta < 0$, so $k < 0$. In view of (1.18), we have $k \mid \Delta(1-d^2)$, so $1 \leq |k| \leq |\Delta|(d^2-1)$. Again, from (1.18), we deduce that

$$|f'(s_2)| = \frac{-k^2 + \Delta(d^2-1)}{2k} = \frac{|k|^2 + |\Delta|(d^2-1)}{2|k|} = g(|k|)$$

where $g(x) = \frac{x^2 + |\Delta|(d^2-1)}{2x}$. Since $g''(x) = \frac{|\Delta|(d^2-1)}{x^3} > 0$ for $x > 0$, we can assert that

$$|f'(s_2)| = g(|k|) \leq \max\{g(1), g(|\Delta|(d^2-1))\} = \frac{1 + |\Delta|(d^2-1)}{2}.$$

Isolating for d^2 yields

$$\frac{2|f'(s_2)| - 1 + |\Delta|}{|\Delta|} \leq d^2,$$

which proves the lemma for $\Delta < 0$. □

The following result by Turk is Proposition 3 in [51], which we restate it for convenience. In the subsequent lemma, we create a solution to a simultaneous system of Pell equations from a tuple (s_1, s_2, s_3) satisfying the conditions given by the definition of the gap principle for a quadratic polynomial f with two distinct roots. We use the result of Turk to bound $f(s_3)/f(s_1)$ by something that goes to infinity as s_1 goes to infinity, thus proving that f satisfies the gap principle of order 2.

Lemma 1.3.2 (Turk)**.** *Let a, b, c, d be squarefree, positive integers with $a \neq b$ and $c \neq d$ and let $e, f \in \mathbb{Z}$. If $af = ce$, then we also assume that $abcd$ is not a perfect square. Then, every positive solution (x, y, z) of the system*

$$\begin{aligned} ax^2 - by^2 &= e \\ cx^2 - dz^2 &= f \end{aligned}$$

satisfies

$$\max\{x, y, z\} < e^{K\alpha^2(\log\alpha)^3\gamma\log\gamma},$$

where $\alpha = \max\{a, b, c, d\}$ and $\gamma = \max\{\alpha\log\alpha, \log\beta\}$ for $\beta = \max\{|e|, |f|, 3\}$, and K is an absolute constant.

Proof. This is Proposition 3 in [51]. □

Lemma 1.3.3. *Let $f \in \mathbb{Z}[x]$ be such that $f(x) = ax^2 + bx + c$ with $a \neq 0$ and $b^2 - 4ac \neq 0$. If $1 < s_1 < s_2 < s_3$ and $f(s_1) \mid f(s_2) \mid f(s_3)$ with $f(s_i) \neq f(s_j)$ for $i \neq j$ and all $f(s_i)$ have the same sign, then*

$$\frac{f(s_3)}{f(s_1)} \gg (\log s_3)^{1/8},$$

where the implicit positive constant depends only on a, b, c.

Proof. It suffices to consider s_3 sufficiently large so that $f(s_3) \neq 0$, so suppose this. Since $f(s_1) \mid f(s_2) \mid f(s_3)$ and $f(s_i) \neq f(s_j)$ for $i \neq j$, we have

$$\begin{aligned} f(s_3) &= n_1 d_1^2 f(s_1), \\ f(s_3) &= n_2 d_2^2 f(s_2), \end{aligned} \tag{1.19}$$

for $n_i, d_i \in \mathbb{N}$ and n_i squarefree. Since we insist that all $f(s_i)$ have the same sign, we also have that $n_i \geq 1$ for all i. Let $\Delta = b^2 - 4ac$ as in the previous lemma. If $n_2 = 1$, then we have $f(s_3) = d_2^2 f(s_2)$ and $d_2 > 1$, and so Lemma 1.3.1 implies that

$$\frac{f(s_3)}{f(s_1)} = \frac{f(s_3)}{f(s_2)}\frac{f(s_2)}{f(s_1)} > \frac{f(s_3)}{f(s_2)} = d_2^2 \geq \frac{2|2as_3 + b| - 1 + |\Delta|}{|\Delta|} \gg s_3 \gg (\log s_3)^{1/8},$$

where the implicit constant depends only on a, b, c. Similarly, if $n_1 = 1$, then

$$\frac{f(s_3)}{f(s_1)} = d_1^2 \gg (\log s_3)^{1/8},$$

where the implicit constant depends only on a, b, c.

We now assume that $n_1 \neq 1$ and $n_2 \neq 1$. For notational simplicity, we let

$$m_1 = n_1 d_1^2,$$
$$m_2 = n_2 d_2^2.$$

As in (1.16) of the previous lemma, the fact that $f(s_3) = n_1 d_1^2 f(s_1)$ implies

$$(2as_3 + b)^2 - n_1(d_1(2as_1 + b))^2 = \Delta(1 - n_1 d_1^2).$$

Similarly, $f(s_3) = n_2 d_2^2 f(s_2)$ implies

$$(2as_3 + b)^2 - n_2(d_2(2as_2 + b))^2 = \Delta(1 - n_2 d_2^2).$$

Hence, we have a system of generalized Pell equations

$$x^2 - n_1 y^2 = \Delta(1 - m_1),$$
$$x^2 - n_2 z^2 = \Delta(1 - m_2)$$

with positive integer solution

$$(x, y, z) = (|2as_3 + b|, d_1|2as_1 + b|, d_2|2as_2 + b|).$$

By our assumption that $f(s_i) \neq f(s_j)$ for $i \neq j$, we have

$$\Delta(1 - m_1) \neq \Delta(1 - m_2),$$

and recall that $n_i \geq 2$ for all i, so the requirements of Lemma 1.3.2 are satisfied. Define α, β, γ as in Lemma 1.3.2, and observe that by (1.19) and the fact that $m_1 > m_2$, we have

$$\begin{aligned} \alpha &= \max\{1, n_1, n_2\} \leq n_1 d_1^2 = m_1, \\ \beta &= \max\{|\Delta(1 - m_1)|, |\Delta(1 - m_2)|, 3\} \leq 3|\Delta| m_1, \\ \gamma &= \max\{\alpha \log \alpha, \log \beta\} \leq (|\Delta| m_1) \log(|\Delta| m_1) + \log(3|\Delta| m_1). \end{aligned} \tag{1.20}$$

We also have

$$\max\{|2as_3 + b|, d_1|2as_1 + b|, d_2|2as_2 + b|\} \gg s_3, \tag{1.21}$$

where the implicit constants depend only on a, b, c. Finally, we use Lemma 1.3.2 along with (1.20) and (1.21) to get that

$$s_3 \ll e^{Km_1^2(\log m_1)^3(|\Delta|m_1)\log(|\Delta|m_1)\log((|\Delta|m_1)\log(|\Delta|m_1))}$$

for some constant K, and taking logs yields

$$\begin{aligned}\log s_3 &\ll m_1^2(\log m_1)^3(|\Delta|m_1)\log(|\Delta|m_1)\log((|\Delta|m_1)\log(|\Delta|m_1)) \\ &\leq (|\Delta|m_1)^3(\log(|\Delta|m_1))^4\log(|\Delta|m_1\log(|\Delta|m_1)) \\ &\leq (|\Delta|m_1)^8,\end{aligned}$$

and taking roots gives

$$(\log s_3)^{1/8} \ll m_1,$$

where the implicit constants depend only on a, b, c. Recognizing that $m_1 = \frac{f(s_3)}{f(s_1)}$ completes the proof. □

This last result pairs nicely with the original definition of the gap principle, and should give us that any rational multiple of powers of f, where $f(x) = ax^2+bx+c$ has two distinct roots, satisfies the gap principle of order 2. We leave the details of this argument for Section 1.4. Now, we focus on showing that such f are not of gap order 1. We again rely on the theory of Pell equations — this time to construct an $S_N(f)$ as in Lemma 1.1.6 which is infinite.

Recall that for a non-square $k \in \mathbb{N}$, the positive integer solutions of the Pell equation

$$x^2 - ky^2 = 1$$

form an infinite semigroup with operation $*$ satisfying

$$(s,t) * (s',t') = (ss' + ktt', st' + s't) \tag{1.22}$$

for every pair of solutions $(s,t), (s',t') \in \mathbb{N}^2$. Equivalently, we can think of the operation above as multiplying quadratic surds:

$$(s + \sqrt{k}t)(s' + \sqrt{k}t') = (ss' + ktt') + \sqrt{k}(st' + s't).$$

Lemma 1.3.4. *Fix an integer $a > 1$. There are infinitely many integer solutions $(s,t) \in \mathbb{N}^2$ of*

$$x^2 - ky^2 = 1$$

satisfying

$$\begin{aligned} s + t &\equiv 1 \pmod{a}, \\ s + kt &\equiv 1 \pmod{a}. \end{aligned} \tag{1.23}$$

Proof. Let $(s,t) \in \mathbb{N}^2$ be a nontrivial solution to $x^2 - ky^2 = 1$ and let $a = \prod_{i=1}^{m} p_i^{\ell_i}$ be the prime power decomposition of a. Fix p_i. Note that

$$s^2 - kt^2 = (s + t\sqrt{k})(s - t\sqrt{k}) \equiv 1 \pmod{\langle p_i^{\ell_i} \rangle}.$$

Thus, we have that $s + \sqrt{k}t$ is a unit in $\mathbb{Z}[\sqrt{k}]/\langle p_i^{\ell_i} \rangle$. Denote the cardinality of the group of units of $\mathbb{Z}[\sqrt{k}]/\langle p_i^{\ell_i} \rangle$ by n_i. As a consequence of Lagrange's theorem, we have for any finite group G with $z \in G$ that $z^{|G|} = 1$. So, we get a solution (s', t') to $x^2 - ky^2 = 1$ such that

$$s' + t'\sqrt{k} = (s + t\sqrt{k})^{n_i} \equiv 1 \pmod{\langle p_i^{\ell_i} \rangle}.$$

We use this idea to get infinitely many solutions (s_j, t_j) to $x^2 - ky^2 = 1$, where

$$s_j + t_j\sqrt{k} = (s + t\sqrt{k})^{j \cdot \operatorname{lcm}\{n_i : 1 \le i \le m\}} \equiv 1 \pmod{\langle p_i^{\ell_i} \rangle} \tag{1.24}$$

for all i. Of course, ideals $\langle p_i^{\ell_i} \rangle$ and $\langle p_{i'}^{\ell_{i'}} \rangle$ are coprime for $i \neq i'$ since $p_i^{\ell_i}$ and $p_{i'}^{\ell_{i'}}$ are themselves coprime. By the Chinese remainder theorem for rings (see [24, p. 265]), we have that

$$\mathbb{Z}[\sqrt{k}]/\langle a \rangle \cong \bigoplus_{i=1}^{m} \mathbb{Z}[\sqrt{k}]/\langle p_i^{\ell_i} \rangle$$

as rings via the isomorphism

$$(z \pmod{\langle a \rangle} \mapsto (z \pmod{\langle p_1^{\ell_1} \rangle}, \ldots, z \pmod{\langle p_m^{\ell_m} \rangle}).$$

So,

$$s_j + t_j\sqrt{k} \equiv 1 \pmod{\langle a \rangle},$$

which implies that $s_j \equiv 1 \pmod{a}$ and $t_j \equiv 0 \pmod{a}$, giving us $s_j + t_j \equiv 1 \pmod{a}$ and $s_j + kt_j \equiv 1 \pmod{a}$. □

Example 1.3.5. *Take $a = 6$ and $k = 3$. It is easy to verify that $(s,t) = (2,1)$ is a solution of $x^2 - 3y^2 = 1$ (in fact, it is the solution with smallest positive x and y). Note that*

$$\begin{aligned} s + t &= 3 \not\equiv 1 \pmod{6}, \\ s + kt &= 5 \not\equiv 1 \pmod{6}, \end{aligned}$$

so (s,t) *is not an example of a solution satisfying* (1.23). *We investigate which elements of* $\mathbb{Z}[\sqrt{3}]/\langle 3\rangle$ *are units and find that*

$$\begin{aligned}(\sqrt{3})^2 &\equiv 3 \equiv 0 \pmod{\langle 3\rangle},\\ (1+\sqrt{3})^3 &= 10+6\sqrt{3} \equiv 1 \pmod{\langle 3\rangle},\\ (1+2\sqrt{3})^3 &= 37+30\sqrt{3} \equiv 1 \pmod{\langle 3\rangle},\\ (2+\sqrt{3})^6 &= 1351+780\sqrt{3} \equiv 1 \pmod{\langle 3\rangle},\\ (2+2\sqrt{3})^6 &= 256(5+3\sqrt{3})^2 \equiv 1 \pmod{\langle 3\rangle},\end{aligned}$$

so

$$\left|(\mathbb{Z}[\sqrt{3}]/\langle 3\rangle)^\times\right| = \left|\left\{a+b\sqrt{3} : 1\le a\le 2,\ 0\le b\le 3\right\}\right| = 6.$$

Similarly, we find that

$$\left|(\mathbb{Z}[\sqrt{3}]/\langle 2\rangle)^\times\right| = |\{1,\sqrt{3}\}| = 2.$$

As in (1.24), *we take*

$$s_j + t_j\sqrt{3} = (2+\sqrt{3})^{\mathrm{lcm}(6,2)j} = (2+\sqrt{3})^{6j},$$

and see that of course these are solutions to $x^2-3y^2=1$, *and*

j	(s_j,t_j)
1	$(1351, 780)$
2	$(3650401, 2107560)$
3	$(9863382151, 5694626340)$
4	$(26650854921601, 15386878263120)$
5	$(72010600134783751, 41575339372323900)$

with $s_j+t_j\equiv 1 \pmod 6$ *and* $s_j+3t_j\equiv 1 \pmod 6$ *for all* $1\le j\le 5$ *(and, as proven, we have this for all* $j\in\mathbb{N}$*).*

Now, we must show that quadratic polynomials f with two distinct roots do not satisfy the gap principle of order 1. Coupled with the previous lemma, this would show that quadratic polynomials with two distinct roots are of gap order 2, which is essentially the statement of (ii) in Theorem 1.1.5. To do this, we first construct a generalized Pell equation of the form $x^2-ky^2=-(k-1)\Delta$ for some nonzero integers k and Δ. We find infinitely many solutions of this generalized Pell equation and, in order to translate them into tuples that satisfy the conditions in the definition of the gap principle of order 1, they must satisfy some congruence conditions modulo D. We find that this is indeed the case and that all of these tuples are bounded above by a constant, and so f does not satisfy the gap principle of order 1.

Lemma 1.3.6. *If $f \in \mathbb{Z}[x]$ is such that $f(x) = ax^2 + bx + c$ with $a \neq 0$ and $b^2 - 4ac \neq 0$, then f does not satisfy the gap principle of order 1.*

Proof. Without loss of generality, assume $a > 0$. Let $\Delta = b^2 - 4ac$. As in the proof of Lemma 1.1.3, we may pick

$$(s_0, s_1) = (s_0, s_0 + f(s_0)) \in \mathbb{N}^2$$

with $s_0 < s_1$ and $f(s_1) = kf(s_0)$ for some integer $k > 1$. To guarantee that k is not a perfect square, we also require that

$$s_0 > \frac{|\Delta| - 2b}{4a}. \tag{1.25}$$

We now show that k is not a perfect square. We see that

$$\begin{aligned}
k &= \frac{f(s_0 + f(s_0))}{f(s_0)} \\
&= \frac{a(s_0 + f(s_0))^2 + b(s_0 + f(s_0)) + c}{f(s_0)} \\
&= \frac{as_0^2 + 2as_0 f(s_0) + af(s_0)^2 + bs_0 + bf(s_0) + c}{f(s_0)} \\
&= \frac{f(s_0) + 2as_0 f(s_0) + af(s_0)^2 + bf(s_0)}{f(s_0)} \\
&= 1 + 2as_0 + b + af(s_0) \\
&= 1 + 2as_0 + b + a^2 s_0^2 + bas_0 + ac \\
&= \left(as_0 + \frac{b}{2} + 1\right)^2 - \frac{b^2 - 4ac}{4} \\
&= \left(as_0 + \frac{b}{2} + 1\right)^2 - \frac{\Delta}{4}.
\end{aligned}$$

Also, by (1.25), we have

$$as_0 + \frac{b}{2} > \frac{|\Delta|}{4}.$$

If $\Delta > 0$, then

$$\begin{aligned}
k &= (as_0 + b/2 + 1)^2 - \frac{\Delta}{4} > (as_0 + b/2 + 1)^2 - (as_0 + b/2) \\
&= (as_0 + b/2 + 1/2)^2 + \frac{3}{4} > (as_0 + b/2 + 1/2)^2
\end{aligned}$$

and

$$k = (as_0 + b/2 + 1)^2 - \frac{\Delta}{4} < (as_0 + b/2 + 1)^2,$$

so

$$(as_0 + b/2 + 1/2)^2 < k < (as_0 + b/2 + 1)^2$$

and thus k cannot be a perfect square.

If $\Delta < 0$, then we can similarly show that

$$(as_0 + b/2 + 1)^2 < k < (as_0 + b/2 + 3/2)^2$$

and again k cannot be a perfect square.

As in (1.17) of Lemma 1.3.1, $f(s_1) = kf(s_0)$ is equivalent to $4af(s_1) = 4akf(s_0)$, which is equivalent to $(f'(s_1))^2 - \Delta = k((f'(s_0))^2 - \Delta)$, which is again equivalent to the generalized Pell equation

$$x^2 - ky^2 = -(k-1)\Delta \tag{1.26}$$

having solution $(x, y) = (f'(s_1), f'(s_0))$. We now find infinitely many solutions of this generalized Pell equation that satisfy certain congruence conditions. Recall that for any solution $(s, t) \in \mathbb{N}^2$ of

$$x^2 - ky^2 = 1, \tag{1.27}$$

we have by Brahmagupta's lemma (1.4) that

$$(s,t) * (f'(s_1), f'(s_0)) = (sf'(s_1) + ktf'(s_0), sf'(s_0) + tf'(s_1)) \tag{1.28}$$

gives another solution of (1.26) that is unique to each (s, t), where $*$ refers to the operation in (1.22). We want these solutions to be of the form $(f'(x), f'(y))$ as that would guarantee integer solutions to $f(x) = kf(y)$ as mentioned in the presentation of (1.26). That is to say that we have

$$(sf'(s_1) + ktf'(s_0), sf'(s_0) + tf'(s_1)) = (f'(x), f'(y)) = (2ax + b, 2ay + b)$$

which gives the integer solutions to $f(x) = kf(y)$

$$\begin{aligned}(x, y) &= \left(\frac{sf'(s_1) + ktf'(s_0) - b}{2a}, \frac{sf'(s_0) + tf'(s_1) - b}{2a}\right) \\ &= \left(ss_1 + kts_0 + \frac{(s + kt - 1)b}{2a}, ss_0 + ts_1 + \frac{(s + t - 1)b}{2a}\right).\end{aligned} \tag{1.29}$$

Since we want to find infinitely many integer solutions given by (1.29), we need $(s + kt - 1)b/2a$ and $(s + t - 1)b/2a$ to be integers, meaning that

$$\begin{aligned}s + t &\equiv 1 \pmod{2a}, \\ s + kt &\equiv 1 \pmod{2a}.\end{aligned} \tag{1.30}$$

By Lemma 1.3.4, there are infinitely many solutions of (1.27) satisfying these congruence conditions. By (1.29), we have infinitely many solutions of (1.26) of the form $(f'(x), f'(y))$ and thus of $f(x) = kf(y)$. We require infinitely many of these solutions to be positive integers in order to fulfill the conditions of Lemma 1.1.6, and by (1.29), it suffices to have $f'(s_1)$ and $f'(s_0)$ sufficiently large, which we may get by requiring s_0 to be sufficiently large. Since k is fixed, we have for any $(x, y) \in \mathbb{N}^2$ with $f(x) = kf(y)$ that

$$k = \frac{f(x)}{f(y)} \gg \frac{x^2}{y^2},$$

where the implicit constant depends only on a, b, c, so x/y is bounded absolutely. By Lemma 1.1.6, we conclude that f does not satisfy the gap principle of order 1. □

Lemma 1.3.6 gives us a process with which we may construct a sequence $\{(s_{0j}, s_{1j})\}_{j=1}^{\infty}$ which fulfills conditions (i)-(iii) of Definition 1.1.1 and has s_{1j}/s_{0j} converge as $j \to \infty$. Each fixed (s_{1j}, s_{0j}) is of the form given in (1.29), which we have shown gives us conditions (ii) automatically. Condition (iii) follows from the fact that $s = s_j$ and $t = t_j$ fulfill

$$s + t\sqrt{k} = (x_0 + y_0\sqrt{k})^j,$$

where (x_0, y_0) is the fundamental solution of $x^2 - ky^2 = 1$, so s and t go to infinity as $j \to \infty$, implying

$$s_{0j} = ss_0 + ts_1 + \frac{(s + t - 1)b}{2a}$$

goes to infinity as $j \to \infty$. Concerning condition (i), it could be that $s_{0j} \geq s_{1j}$, but this may be remedied by taking s_{0j} to be sufficiently large.

Example 1.3.7. *Take $f(x) = x^2 + 1$. We let $s_0 = 0$, so*

$$(s_0, s_1) = (0, 0 + f(0)) = (0, 1),$$
$$k = \frac{f(s_1)}{f(s_0)} = \frac{f(1)}{f(0)} = 2.$$

Now, we need the solutions of $x^2 - 2y^2 = 1$ to generate solutions to $f(x) = 2f(y)$ as in (1.28). Since $b = 0$, we have

$$(s + kt - 1)b/2a = (s + t - 1)b/2a = 0$$

in (1.29) for any s, t, so we do not need the solutions of $x^2 - 2y^2 = 1$ to satisfy (1.30). Note that the smallest solution of $x^2 - 2y^2 = 1$ with positive x and y is $(3, 2)$, so we have the

following solutions $(x, y) = (x_j, y_j)$ *to* $f(y) = 2f(x)$ *with*

$$(x_j, y_j) = \left(s'_j s_1 + k t'_j s_0 + \frac{(s'_j + k t'_j - 1)b}{2a}, s'_j s_0 + t'_j s_1 + \frac{(s'_j + t'_j - 1)b}{2a} \right) = (s'_j, t'_j)$$

and

$$s'_j + t'_j \sqrt{2} = (3 + 2\sqrt{2})^j,$$

given by (1.29). *For* $1 \leq j \leq 5$, *we have*

j	(x_j, y_j)	$f(x_j)/f(y_j)$	x_j/y_j
1	$(3, 2)$	2	1.5
2	$(17, 12)$	2	$1.416\ldots$
3	$(99, 70)$	2	$1.414\ldots$
4	$(577, 408)$	2	$1.414\ldots$
5	$(3363, 2378)$	2	$1.414\ldots$

and we can see from this table that $f(x_j)/f(y_j) = 2$ *for all* $1 \leq j \leq 5$ *and, as a consequence,* x_j/y_j *converges to* $2^{1/\deg(f)} = \sqrt{2} = 1.414\ldots$. *We claim that* $\{(y_j, x_j)\}_{j=1}^{\infty}$ *satisfies conditions (i)-(iii) of Definition 1.1.1. We have already shown how any sequence derived from this construction satisfies conditions (ii) and (iii). Now, since* $x_1 > 0$ *and* $x^2 + 1$ *is strictly increasing for* $x \in (0, \infty)$, *the fact that* $f(x_j) = 2f(y_j)$ *implies that* $y_j < x_j$, *so* $\{(y_j, x_j)\}_{j=1}^{\infty}$ *satisfies condition (i). However, as mentioned,* x_j/y_j *converges and so* $x^2 + 1$ *cannot fulfill the gap principle of order 1 by definition.*

Example 1.3.8. *Take* $f(x) = 3x^2 - x + 1$. *We let* $s_0 = 0$, *so*

$$(s_0, s_1) = (0, 0 + f(0)) = (0, 1),$$
$$k = \frac{f(s_1)}{f(s_0)} = \frac{f(1)}{f(0)} = 3.$$

Now, we need the solutions of $x^2 - 3y^2 = 1$ *to generate solutions to* $f(x) = 3f(y)$ *as in* (1.28). *Taking the solutions* (s_j, t_j) *given in Example 1.3.5, we use* (1.29) *to generate*

$$\begin{aligned}(x_j, y_j) &= \left(s'_j s_1 + k t'_j s_0 + \frac{(s'_j + k t'_j - 1)b}{2a}, s'_j s_0 + t'_j s_1 + \frac{(s'_j + t'_j - 1)b}{2a} \right) \\ &= \left(s'_j - \frac{s'_j + 3t'_j - 1}{6}, t'_j - \frac{s'_j + t'_j - 1}{6} \right),\end{aligned}$$

where

$$s'_j + t'_j \sqrt{3} = (2 + \sqrt{3})^{6j}.$$

For $1 \leq j \leq 5$, *we have*

j	(x_j, y_j)	$f(x_j)/f(y_j)$	x_j/y_j
1	$(736, 425)$	3	$1.731\ldots$
2	$(1988221, 1147900)$	3	$1.732\ldots$
3	$(5372171956, 3101624925)$	3	$1.732\ldots$
4	$(14515606636441, 8380589399000)$	3	$1.732\ldots$
5	$(39221163759491176, 22644349454472625)$	3	$1.732\ldots$

and we can see from this table that $f(x_j)/f(y_j) = 3$ *for all* $1 \leq j \leq 5$ *and, as a consequence,* x_j/y_j *converges to* $2^{1/\deg(f)} = \sqrt{3} = 1.732\ldots$. *As in the previous example,* $\{(y_j, x_j)\}_{j=1}^{\infty}$ *satisfies conditions (ii) and (iii) of Definition 1.1.1. Now, since* $x_1 > 1$ *and* x^2+1 *is strictly increasing for* $x \in (1, \infty)$, *the fact that* $f(x_j) = 3f(y_j)$ *implies that* $y_j' < x_j$, *so* $\{(y_j, x_j)\}_{j=1}^{\infty}$ *satisfies condition (i). However,* x_j/y_j *converges and so* $3x^2 - x + 1$ *cannot fulfill the gap principle of order 1 by definition.*

Remark 1.3.9. *The construction given in the proof of Lemma 1.3.6 does not work for quadratic polynomials that are a square of a linear polynomial as we need* $k = f(s_1)/f(s_0)$ *to be not a perfect square, but if* $f(x) = (ax + b)^2$ *for some* $a, b \in \mathbb{Z}$, *we have*

$$k = \frac{f(s_1)}{f(s_0)} = \frac{(a(s_0 + as_0 + b) + b)^2}{(as_0 + b)^2} = \frac{(a(a+1)s_0 + b(a+1))^2}{(as_0 + b)^2} = (a+1)^2,$$

so k *is a perfect square and the Pell equation* (1.27) *has only the trivial solutions* $(x, y) = (\pm 1, 0)$.

So, we have essentially proven part (ii) of the main theorem, Theorem 1.1.5. We now dedicate a brief section to synthesizing the results of Sections 1.2 and 1.3 and proving Theorem 1.1.5.

1.4 Proof of the main theorem

We are now equipped to prove Theorem 1.1.5, which we restate below.

Theorem 2.1.5 *For any polynomial* $f \in \mathbb{Z}[x]$, *we have that*

(i) if $f = Kg$ *where* $K \in \mathbb{Q}$ *and* $g \in \mathbb{Z}[x]$ *is either of degree 0 or a power of linear polynomial, then* f *does not satisfy the gap principle,*

(ii) if $f = Kg$ *where* $K \in \mathbb{Q} \setminus \{0\}$ *and* $g \in \mathbb{Z}[x]$ *is a power of a quadratic with two distinct roots, then* f *is of gap order 2,*

(iii) if $f(x) \neq K(c_2x^2 + c_1x + c_0)^n$ *for any* $K \in \mathbb{Q}$ *and* $c_j \in \mathbb{Z}$, *then* f *is of gap order 1.*

Proof. We consider each case above separately.

Proof of (i): By Lemma 1.1.4, it suffices to consider $K = 1$ and g being either of degree 0 or just a linear polynomial. This statement is obviously true if f is of degree 0, so we only consider f being a linear polynomial. Let $f(x) = c_1x + c_0$ for $c_j \in \mathbb{Z}$ and assume without loss of generality that $c_1 > 0$, and let $h(x) = x + f(x)$. As in Lemma 1.1.3, we consider $\{j, h(j), \dots, h^\ell(j)\}_{j=n}^\infty$ for any $\ell \in \mathbb{N}$ and n sufficiently large so that this sequence satisfies conditions (i)-(iii) of Definition 1.1.1. We will show by induction that

$$\frac{f(h^\ell(j))}{f(j)} = (1 + c_1)^\ell$$

for all $j \in \mathbb{R}$ and $\ell \in \mathbb{N}$. First, we see that

$$\frac{f(h(j))}{f(j)} = \frac{f(j + f(j))}{f(j)} = \frac{c_1(j + c_1j + c_0) + c_0}{c_1j + c_0} = 1 + c_1$$

for all $j \in \mathbb{R}$. Assume that

$$\frac{f(h^\ell(j))}{f(j)} = (1 + c_1)^\ell$$

for all $j \in \mathbb{R}$ for some $\ell \in \mathbb{N}$. It follows that

$$\frac{f(h^{\ell+1}(j))}{f(j)} = \frac{c_1h^{\ell+1}(j) + c_0}{f(j)} = \frac{c_1h^\ell(j) + c_1f(h^\ell(j)) + c_0}{f(j)} = (1 + c_1)\frac{f(h^\ell(j))}{f(j)} = (1 + c_1)^{\ell+1}.$$

Thus, we have shown by induction that

$$\lim_{j\to\infty} \frac{f(h^\ell(j))}{f(j)} = (1 + c_1)^\ell < \infty$$

so f does not satisfy the gap principle of order ℓ for any $\ell \in \mathbb{N}$, meaning f does not satisfy the gap principle.

Proof of (ii): Again, by Lemma 1.1.4, it suffices to consider $K = 1$ and g being a quadratic with two distinct roots. Consider $\{\mathbf{s}_j\}_{j=1}^\infty$ with $\mathbf{s}_j = (s_{0j}, s_{1j}, s_{2j}) \in \mathbb{N}^3$ for all j satisfying conditions (i)-(iii) of Definition 1.1.1. For large j, we have s_{0j} is large enough to satisfy $f(s_{ij}) \neq f(s_{kj})$ for $i \neq k$ and all $f(s_{ij})$ have the same sign, so we may use Lemma 1.3.3 to get that

$$\frac{f(s_{2j})}{f(s_{0j})} \gg (\log s_{3j})^{1/8}$$

where the implicit constant depends only on a, b, c. Since $\log s_{3j} \to \infty$ as $j \to \infty$, we deduce that f satisfies the gap principle of order 2. By Lemma 1.3.6, f does not satisfy the gap principle of order 1, so we conclude that f is of gap order 2 by definition.

Proof of (iii): Fix $N > 1$ and suppose that $f(x) \mid f(y)$ with $1 < y/x \leq N$. We see

that

$$\left|\frac{f(y)}{f(x)}\right| \leq M\left|\left(\frac{y}{x}\right)^{\deg f}\right| \leq MN^{\deg f},$$

for some $M = M(f) > 0$. Thus, we have that

$$S_N(f) = \{(x,y) \in \mathbb{N}^2 : f(x) \mid f(y), 1 < y/x \leq N\} \subset \bigcup_{k=2}^{MN^{\deg f}} \{(x,y) \in \mathbb{N}^2 : f(y) = kf(x)\}, \tag{1.31}$$

where $S_N(f)$ is as in Lemma 1.1.6. By Lemma 1.2.3, $f(y) = kf(x)$ has finitely many integer solutions, so the set on the right side of (1.31) is finite. Thus, $S_N(f)$ is finite, and since $N > 1$ was made arbitrary, we have by Lemma 1.1.6 that f satisfies the gap principle of order 1. □

We note that the sequences in Lemma 1.1.3 that we used to show part (i) would not help us in showing that the polynomials mentioned in part (ii) do not satisfy the gap principle of order 1. To see this, let $f \in \mathbb{Z}[x]$ be quadratic, so $f(x) = ax^2 + bx + c$. We pick any $s \in \mathbb{N}$ and consider $(s, s + f(s)) \in \mathbb{N}^2$. We have that

$$\begin{aligned}\frac{f(s+f(s))}{f(s)} &= \frac{a(s+as^2+bs+c)^2 + b(s+as^2+bs+c)+c}{as^2+bs+c} \\ &= as^2 + O(s),\end{aligned}$$

which tends to infinity as s tends to infinity. So, this approach does not work for our purposes and our foray into Pell equation theory is justified.

Chapter 2

A notion of multiplicative order for solutions of Pell equations

In this chapter, we build upon the idea of finding the solution set of a generalized Pell equation $x^2 - Dy^2 = k$ subject to congruence conditions, as we touched upon in the proof of Lemma 1.3.6 at the end of the previous chapter. It turns out that these solution sets are given by powers of finitely many small positive solutions, and these powers are multiples of the smallest integer $M = M(D)$ such that the smallest positive solution (x_0, y_0) of $x^2 - Dy^2 = 1$ satisfies $(x_0 + y_0\sqrt{D})^M \equiv 1 \pmod{D}$ in $\mathbb{Z}[\sqrt{D}]$. One of our main results in this chapter essentially determines M for D being a perfect power. The results of this chapter come from joint work with Stephen Choi (see [21]).

2.1 Introduction

2.1.1 Notation

Here, we list all potentially ambiguous notation used in this chapter:

(i) For a ring R, we denote by $\mathrm{ord}_R(r)$ the multiplicative order of $r \in R$ — that is, the smallest $n \in \mathbb{N}$ such that $r^n = 1$ in R — if it exists.

(ii) For $M \in \mathbb{N}$, we denote by $v_M(k)$ for $k \in \mathbb{Z}$ the largest $n \in \mathbb{N}$ such that $M^n \mid k$. In the case that M is prime, $v_M(k)$ is the M-adic valuation of k.

(iii) For R a commutative ring and $x \in R$, we denote by $\langle x \rangle \subset R$ the ideal generated by x, defined by

$$\langle x \rangle = \{xr : r \in R\}.$$

2.1.2 Generating all solutions to Pell equations

We now continue our exposition of Pell equation theory. In Section 1.1, we stated Brahmagupta's lemma (1.4), which gives a way to generate infinitely many solutions to a (generalized) Pell equation, given one nontrivial solution. A more thorough investigation into

Pell equations began in the late eighteenth century, in which Legendre, using the machinery of continued fractions, showed that all the solutions of (1.2) can be generated from a single, particular solution. We call the nontrivial solution of the Pell equation (1.2) with positive x and y, and the smallest value of x (equivalently, of y), the *fundamental solution of* (1.2) and denote it by (x_0, y_0). It was shown by Legendre, following work by Euler and Lagrange, that the set of solutions of (1.2) is precisely the set

$$\left\{\pm\left(x_0 + y_0\sqrt{D}\right)^{\pm n} : n \in \mathbb{N}\right\} = \left\{\pm\left(x_0 \pm y_0\sqrt{D}\right)^{n} : n \in \mathbb{N}\right\}. \tag{2.1}$$

For a proof of this result, we refer the reader to Theorem 6.4 of [49]. Thus, the task of finding all solutions to a Pell equation amounts to finding its fundamental solution. For this, we need to introduce continued fractions. For any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, let

$$\alpha_0 := \alpha, \qquad \alpha_n := [\alpha_n] + \frac{1}{\alpha_{n+1}} \qquad \text{for } n \in \mathbb{N}, \tag{2.2}$$

where $[z]$ denotes the integer part of any $z \in \mathbb{R}$. Since α is irrational, the iteration (2.2) does not terminate. Making the substitution $a_n = [\alpha_n]$, we have

$$\alpha = a_0 + \frac{1}{\alpha_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{\alpha_n}}}$$

for all $n \in \mathbb{N}$. We call

$$[a_0, a_1, \ldots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$$

the n-th convergent of α. Define the *continued fraction representation of* α to be $\lim_{n\to\infty}[a_0, a_1, \ldots, a_n]$, and denote it by $[a_0, a_1, \ldots]$. It holds that

$$\alpha = \lim_{n\to\infty}[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots].$$

This is Theorem 3.6 in [49]. If there exists an $\ell \in \mathbb{N}$ such that $a_{n+\ell} = a_n$ for all $n \geq n_0$ for some $n_0 = n_0(\ell) \in \mathbb{N}$, we say that α has a *periodic* continued fraction representation, and we call ℓ the *period length* of the continued fraction representation of α. In this case, we write

$$\alpha = [a_0, a_1, \ldots, a_{n_0-1}, \overline{a_{n_0}, \ldots, a_{n_0+\ell-1}}].$$

If $\alpha = \sqrt{D}$, it follows that

$$\alpha = [a_0, \overline{a_1, \ldots, a_\ell}],$$

and furthermore that

$$\frac{x_0}{y_0} = \begin{cases} [a_0, a_1, \ldots, a_{\ell-1}] & \ell \text{ is even}, \\ [a_0, a_1, \ldots, a_{2\ell-1}] & \ell \text{ is odd}, \end{cases} \tag{2.3}$$

where x_0/y_0 is assumed to be reduced. This is given by Theorem 5.4 and Lemma 6.3 in [49], respectively. For proofs of these basic results on continued fractions and their connection to fundamental solutions, we refer the reader to Chapters 3 and 6 and Section 5.2 of [49].

We can view the fundamental solution of a Pell equation through the lens of algebraic number theory. Consider D squarefree. The quadratic field

$$K = \mathbb{Q}(\sqrt{D}) = \left\{ a + b\sqrt{D} : a, b \in \mathbb{Q} \right\}$$

has ring of integers

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3, \pmod 4, \\ \mathbb{Z}[(1+\sqrt{D})/2] & \text{if } D \equiv 1 \pmod 4, \end{cases} \tag{2.4}$$

which is the subring containing all elements of $\mathbb{Q}(\sqrt{D})$ that are roots of monic polynomials with integer coefficients [48, p. 27-28; Section 2.5, Theorem 1]. The units in K are precisely the elements $a + b\sqrt{D}$ with

$$a^2 - Db^2 = \pm 1.$$

That is, they are exactly the elements that satisfy the standard Pell equation $x^2 - Dy^2 = 1$ or the negative Pell equation $x^2 - Dy^2 = -1$ [48, Section 4.4, Theorem 1]. Furthermore, the group of units of $\mathcal{O}_K$ is generated by one element, called the *fundamental unit*, which we will denote by ω. This is to say that any unit in $\mathcal{O}_K$ is a power of ω up to sign [48, Section 4.4]. Since the fundamental solution (x_0, y_0) of $x^2 - Dy^2 = 1$ is a unit in K and an element of $\mathbb{Z}[\sqrt{D}]$, which is always a subring of $\mathcal{O}_K$ by (2.4), we have that (x_0, y_0) is a power of ω. We can actually find out exactly which power. If $D \equiv 2, 3 \pmod 4$, the fundamental unit is the fundamental solution of $x^2 - Dy^2 = -1$ if it exists (the conditions given by Lemma 2.1.3), and $\omega^2 = (x_0, y_0)$ [48, p.63-64]. Otherwise, $\omega = (x_0, y_0)$. In the case that $D \equiv 1 \pmod 4$, the fundamental unit is the smaller of the fundamental solution(s) to the generalized Pell equations $x^2 - Dy^2 = \pm 4$ (the negative equation may not have a solution). Let $\omega = a + b\sqrt{D}$. If a, b are both odd, then $\omega^3 = (x_0, y_0)$, and otherwise $\omega = (x_0, y_0)$ [48, p. 64]. To summarize,

$$(x_0, y_0) \in \{\omega, \omega^2, \omega^3\}. \tag{2.5}$$

Many results in this chapter have to do with powers of fundamental solutions of Pell equations, so one can interpret these results as having to do with powers of the fundamental units of the appropriate quadratic fields in the case that D is squarefree.

2.1.3 The order g(D)

Consider the Pell equation

$$x^2 - Dy^2 = 1 \tag{2.6}$$

with fundamental solution — i.e., smallest positive solution — $(x_0, y_0) \in \mathbb{N}^2$. Recall that all integer solutions of (2.6) are given by

$$\left\{\pm(x_0 \pm y_0\sqrt{D})^n : n \in \mathbb{Z}\right\}. \tag{2.7}$$

Let $\varphi_m : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}]/\langle m\rangle$ be the standard reduction map, so that

$$\varphi_m(x + y\sqrt{D}) = \overline{x} + \overline{y}\sqrt{D}$$

with $\overline{x}, \overline{y} \in \{0, 1, \ldots, m-1\}$, and

$$\overline{x} \equiv x \pmod{m} \quad \text{and} \quad \overline{y} \equiv y \pmod{m}.$$

By the properties of modular arithmetic, φ_m is obviously a ring homomorphism. If there exists a positive n such that $\varphi_m(z^n) = 1$ for $z \in \mathbb{Z}[\sqrt{D}]$, we call the smallest such n the *multiplicative order of z in $\mathbb{Z}[\sqrt{D}]/\langle m\rangle$* and denote it by $g_D(m)$. Note that

$$(x_0 + y_0\sqrt{D})(x_0 - y_0\sqrt{D}) = x_0^2 - Dy_0^2 = 1,$$

so $(\overline{x_0} + \overline{y_0}\sqrt{D})(\overline{x_0} - \overline{y_0}\sqrt{D}) = \overline{1}$ when $m = D$, which means that $x_0 + y_0\sqrt{D}$ is a unit in $\mathbb{Z}[\sqrt{D}]/\langle D\rangle$ and thus its multiplicative order in $\mathbb{Z}[\sqrt{D}]/\langle D\rangle$ always exists. Throughout this chapter, we will study only the case that $m = D$, and, for simplicity, we let $g(D) = g_D(D)$. Determining $g(D^{2n+1})$ for sufficiently large n is one of our two main results for this chapter. Along the way, we will determine for any $n \in \mathbb{N}$ the smallest power of the fundamental solution of $x^2 - Dy^2 = 1$ which is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$, which is our other main result.

There seems to be little literature on this notion of the order of the fundamental solutions of Pell equations aside from [15]. In [15], Chahal and Priddis study the order of the solution set (2.7), realized as a group of 2×2 matrices with integer entries, in the general linear group $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ for $m \in \mathbb{Z}$. Their notion of order is more general than $g_D(m)$.

In the proof of Lemma 1.3.6, namely when considering (1.30), we essentially studied $g_k(2a)$ to find infinitely many solutions $(s, t) \in \mathbb{N}^2$ of $x^2 - ky^2 = 1$ with $s + t \equiv 1 \pmod{2a}$ and $s + kt \equiv 1 \pmod{2a}$, where $a \in \mathbb{N}$. The order $g(D)$ is also useful in finding the solutions

of the generalized Pell equation

$$x^2 - Dy^2 = k \tag{2.8}$$

with $\gcd(k, D) = 1$, that satisfy the congruence conditions

$$x \equiv a \pmod{D} \quad \text{and} \quad y \equiv b \pmod{D}. \tag{2.9}$$

If $u = x_0 + y_0\sqrt{D}$, then it is known (see [1, p. 244] and [23]) that every solution (s, t) of (2.8) is in the form

$$s + t\sqrt{D} = \pm(x' \pm y'\sqrt{D})(x_0 + y_0\sqrt{D})^n \tag{2.10}$$

for some $n \in \mathbb{N}$ and solution (x', y') of (2.8) satisfying

$$|x'| \leq \frac{|k| + u}{2} \quad \text{and} \quad |y'| \leq \frac{|k| + u}{2\sqrt{D}}. \tag{2.11}$$

If there exist no simultaneous solutions (x_i, y_i) of (2.8) and (2.9) satisfying the bounds (2.11), then there exist no solutions of (2.8) satisfying (2.9). In order to find all solutions of generalized Pell equations satisfying certain congruences, we employ the following result which makes use of $g(D)$.

Proposition 2.1.1. *Let $(x_i, y_i) \in \mathbb{Z}^2$ for $1 \leq i \leq q$ be the simultaneous solutions of (2.8) and (2.9) satisfying the bounds (2.11). Then all the simultaneous solutions of (2.8) and (2.9) are given by*

$$\pm(x_i + y_i\sqrt{D})(x_0 + y_0\sqrt{D})^{ng(D)} \tag{2.12}$$

for $n \in \mathbb{Z}$ and $1 \leq i \leq q$.

Proof. Let (s, t) be a solution of the generalized Pell equation (2.8). Note that $\gcd(s, D) = 1$ because $\gcd(k, D) = 1$. We claim that if

$$s + t\sqrt{D} = (s' + t'\sqrt{D})(x' + y'\sqrt{D}) = (x's' + y't'D) + (y's' + x't')\sqrt{D}, \tag{2.13}$$

then

$$\begin{cases} s \equiv s' \pmod{D}, \\ t \equiv t' \pmod{D}, \end{cases} \quad \text{if and only if} \quad \begin{cases} x' \equiv 1 \pmod{D}, \\ y' \equiv 0 \pmod{D}. \end{cases}$$

By (2.10), this is sufficient for showing that (2.12) yields all desired solutions, since (2.10) yields all solutions to (2.8), and if

$$x' + y'\sqrt{D} = (x_0 + y_0\sqrt{D})^{ng(D)},$$

then by definition of $g(D)$, we must have $x' \equiv 1 \pmod{D}$ and $y' \equiv 0 \pmod{D}$. Indeed, if $x' \equiv 1 \pmod{D}$ and $y' \equiv 0 \pmod{D}$, then by (2.13), we have

$$s \equiv s'x' \equiv s' \pmod{D} \quad \text{and} \quad t \equiv t'x' \equiv t' \pmod{D}.$$

Conversely, if $s \equiv s' \pmod{D}$ and $t \equiv t' \pmod{D}$, then by (2.13) again, we have

$$s = x's' + y't'D \equiv x's + y'tD \equiv x's \pmod{D}.$$

Thus, $x' \equiv 1 \pmod{D}$ since $\gcd(s, D) = 1$. We use this with (2.13) to get

$$t = y's' + x't' \equiv y's + x't \equiv y's + t \pmod{D},$$

which implies $y's \equiv 0 \pmod{D}$ and so $y' \equiv 0 \pmod{D}$. Therefore, the solutions of (2.8) satisfying (2.9) are precisely those given by (2.12). □

We find that $g(D)$ has a nice explicit formula that can be derived from the binomial expansion of a power of the fundamental solution, which we show below. This result reduces the problem of computing $g(D)$ (and later of computing $g(D^{2n+1})$) to computing $x_0 \pmod{D}$ and $\gcd(y_0, D)$).

Theorem 2.1.2. *Suppose $D \in \mathbb{N}$ is not a perfect square and $x_0 + y_0\sqrt{D}$ is the fundamental solution of $x^2 - Dy^2 = 1$. Then,*

$$g(D) = \operatorname{lcm}\left(\operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0), \frac{D}{\gcd(y_0, D)}\right),$$

where $\operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0)$ is the multiplicative order of x_0 in $\mathbb{Z}/D\mathbb{Z}$.

Proof. We see that

$$\begin{aligned}(x_0 + y_0\sqrt{D})^n &= \sum_{k=0}^{n} \binom{n}{k} x_0^{n-k} y_0^k D^{k/2} \\ &= \left(\sum_{0 \le 2k \le n} \binom{n}{2k} x_0^{n-2k} y_0^{2k} D^k\right) + \left(\sum_{0 < 2k+1 \le n} \binom{n}{2k+1} x_0^{n-2k-1} y_0^{2k+1} D^k\right)\sqrt{D} \\ &\equiv x_0^n + n x_0^{n-1} y_0 \sqrt{D} \pmod{\langle D \rangle}.\end{aligned}$$

Thus, $(x_0 + y_0\sqrt{D})^n = 1$ in $\mathbb{Z}[\sqrt{D}]/\langle D \rangle$ if and only if

$$x_0^n \equiv 1 \pmod{D} \quad \text{and} \quad n x_0^{n-1} y_0 \equiv 0 \pmod{D}. \tag{2.14}$$

If $n = \operatorname{lcm}\left(\operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0), \frac{D}{\gcd(y_0, D)}\right)$, then clearly (2.14) holds. Now, suppose (2.14) holds. The first condition gets us that

$$\operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0) \mid n. \tag{2.15}$$

Combining the congruences in (2.14) yields $nx_0^n y_0 \equiv ny_0 \equiv 0$, implying that

$$\frac{D}{\gcd(y_0, D)} \mid n. \tag{2.16}$$

By (2.15) and (2.16), we have that

$$\operatorname{lcm}\left(\operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0), \frac{D}{\gcd(y_0, D)}\right) \mid n.$$

Since $g(D)$ is the smallest such n, we can take n to be $g(D)$, which completes the proof. □

As mentioned prior, our main goal for this chapter is to establish $g(D^{2n+1})$ for sufficiently large n. Let (x_n, y_n) be the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$. In view of Theorem 2.1.2, we must find $\operatorname{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n)$ and $\gcd(y_n)$. To do this, we express $x_n + y_n\sqrt{D^{2n+1}}$ as a power of $x_0 + y_0\sqrt{D}$, which gives us some information on the factors of y_n, helping us to find $\gcd(y_n)$. The majority of the following section is devoted to determining this power, and we find that it depends on congruence conditions on y_0 and D. In particular, the power depends on the divisibility of y_0 and D by 3. This result is of independent interest, as it also provides a computationally simple method to compute the fundamental solutions of $x^2 - D^{2n+1}y^2 = 1$ for all n. In order to find the desired order for x_n, we rely on results due to Perron and Mollin-Srinivasan, which connect $x_n \pmod{D^{2n+1}}$ to the solvability of certain generalized Pell equations. These results are presented in the next section, concluding our introduction. Finally, we show for sufficiently large n that

$$g(D^{2n+1}) = \begin{cases} D^{2n+1} & \text{if } D \text{ is odd and } \operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 1, \\ 2D^{2n+1} & \text{if } D \text{ is odd and } \operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 2, \\ D^{2n+1} & \text{if } D \text{ is even.} \end{cases}$$

2.1.4 Solvability conditions for generalized Pell equations

Again, let $x_0 + y_0\sqrt{D}$ be the fundamental solution of $x^2 - Dy^2 = 1$. In view of Theorem 2.1.2, we need to determine if $x_0 \equiv 1 \pmod{D}$ in order to compute $g(D)$. Mollin and Srinivasan in [42] show that the values of $x_0 \pmod{D}$ are closely related to the solvability of the following generalized Pell equations:

$$\begin{aligned} x^2 - Dy^2 &= -1, \\ x^2 - Dy^2 &= 2, \\ x^2 - Dy^2 &= -2. \end{aligned} \tag{2.17}$$

In view of the formula derived in Theorem 2.1.2 which involves $x_0 \pmod D$, these results are very useful when computing $g(D)$. We first mention a well-known fact about the negative Pell equation $x^2 - Dy^2 = -1$, and a classical result by Perron.

Lemma 2.1.3. *Suppose the continued fraction representation of $\sqrt{D}$ is $[a_0; \overline{a_1, \ldots, a_{\ell-1}}]$. Then, the negative Pell equation $x^2 - Dy^2$ has a solution if and only if ℓ is odd. Moreover, if $(x_{-1}, y_{-1}) \in \mathbb{N}^2$ is the fundamental solution of the negative Pell equation, we have*

$$x_0 + y_0\sqrt{D} = (x_{-1} + y_{-1}\sqrt{D})^2 \tag{2.18}$$

is the fundamental solution of $x^2 - Dy^2 = 1$.

Proof. See Theorem 5.15(b) in [43]. □

Theorem 2.1.4 (Perron, 1954)**.** *(i) If $D > 2$ is an integer that is not a perfect square, then at most one of the equations in (2.17) is solvable.*

(ii) If $D = p^n$ or $D = 2p^n$ for some odd prime p and $n \in \mathbb{N}$, then exactly one equation in (2.17) is solvable.

Proof. Part (i) is Satz 21 and part (ii) is Satz 23 of §26 in [46]. □

Theorem 2.1.5 ([42])**.** *Let $D > 1$ be an integer that is not a perfect square, $x_0 + y_0\sqrt{D}$ be the fundamental solution to $x^2 - Dy^2 = 1$, and let the continued fraction representation of $\sqrt{D}$ be $[a_0; \overline{a_1, \ldots, a_{\ell-1}}]$. If ℓ is even, then there is a solution to the Diophantine equation $x^2 - Dy^2 = 2(-1)^{\ell/2}$ if and only if $x_0 \equiv (-1)^{\ell/2} \pmod D$.*

Proof. This is Theorem 4.3 in [42]. □

Corollary 2.1.6. *Let $D > 2$ be an integer that is not a perfect square and let $x_0 + y_0\sqrt{D}$ be the fundamental solution to $x^2 - Dy^2 = 1$. Then, we have the following:*

(i) The equation

$$x^2 - Dy^2 = 2 \tag{2.19}$$

is solvable if and only if $x_0 \equiv 1 \pmod D$.

(ii) The equation $x^2 - Dy^2 = -2$ is solvable if and only if $x_0 \equiv -1 \pmod D$ and $x_0 \not\equiv -1 \pmod{2D}$.

(iii) The equation $x^2 - Dy^2 = -1$ is solvable if and only if $x_0 \equiv -1 \pmod{2D}$.

Proof. Part (iii) is shown in [44], and we note that although the authors state that $D \equiv 1, 2 \pmod 4$, it is not necessary.

We now focus on parts (i) and (ii). Suppose the continued fraction representation of $\sqrt{D}$ has period length ℓ. If one of

$$x^2 - Dy^2 = 2,$$
$$x^2 - Dy^2 = -2$$

has a solution, then Theorem 2.1.4 implies that $x^2 - Dy^2 = -1$ does not have a solution, meaning that ℓ is even by Lemma 2.1.3. Thus, Theorem 2.1.5 gives us the forward directions of (i) and (ii).

Now, suppose that either

$$x_0 \equiv 1 \pmod{D}$$

or

$$x_0 \equiv -1 \pmod{D} \quad \text{and} \quad x_0 \not\equiv -1 \pmod{2D}.$$

We now use part of the proof of Theorem 1.1 of [44]. Let $(x_{-1}, y_{-1}) \in \mathbb{N}^2$ be the fundamental solution of $x^2 - Dy^2 = -1$. Then, (2.18) tells us that

$$x_0 = x_{-1}^2 + Dy_{-1}^2 = -1 + 2Dy_{-1}^2,$$

which implies

$$x_0 \equiv -1 \pmod{D} \quad \text{and} \quad x_0 \equiv -1 \pmod{2D}.$$

Since these congruences cannot both hold in the reverse directions of (i) and (ii), we must have that $x^2 - Dy^2 = -1$ is not solvable, so again ℓ is even by Lemma 2.1.3 and Theorem 2.1.5 yields the claim. □

2.2 Connections between $x^2 - Dy^2 = 1$ and $x^2 - D^{2n+1}y^2 = 1$

2.2.1 Constructing solutions to $x^2 - D^{2n+1}y^2 = 1$

In this section, we show that the solutions of $x^2 - D^{2n+1}y^2 = 1$ can be constructed in a very straightforward way from the solutions of $x^2 - Dy^2 = 1$, which is a drastic improvement both in memory and computation time from the standard approach involving computing the continued fraction representation of $\sqrt{D^{2n+1}}$. We start with $D = 2$, which is slightly different than the case in which $D > 2$. In either case, the main idea is that we construct $M \in \mathbb{N}$ for which we claim that

$$x_M + y_M\sqrt{D^{2n+1}} = (x_0 + y_0\sqrt{D})^M$$

is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$, where (x_0, y_0) is the fundamental solution of $x^2 - Dy^2 = 1$. Then, letting (x_0', y_0') be the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$,

we notice that it can be seen as a solution of $x^2 - Dy^2 = 1$ because

$$(x_0')^2 - D^{2n+1}(y_0')^2 = (x_0') - D(D^n y_0')^2 = 1.$$

Thus, we may write

$$x_0' + y_0'\sqrt{D^{2n+1}} = (x_0 + y_0\sqrt{D})^k,$$

and using the fact that (x_M, y_M) must be a power of the fundamental solution (x_0', y_0'), we compile the previous equations and get

$$(x_0 + y_0\sqrt{D})^M = x_M + y_M\sqrt{D^{2n+1}} = (x_0' + y_0'\sqrt{D^{2n+1}})^j = (x_0 + y_0\sqrt{D})^{jk}.$$

We then show that $j = 1$, and so it must be that $(x_0 + y_0\sqrt{D})^M$ gives the fundamental solution to $x^2 - D^{2n+1}y^2 = 1$. We note that the exact notation for the fundamental solutions of both equations in this recurring argument varies throughout this chapter. This is the content of Theorem 2.2.1 and Theorem 2.2.5. Making use of (2.5), in the case that D is squarefree, Theorems 2.2.1 and 2.2.5 give us the smallest power M of the fundamental unit of $\mathbb{Q}(\sqrt{D})$, which we call ω, such that $\omega^M \in \mathbb{Z}[\sqrt{D^{2n+1}}] = \mathbb{Z}[D\sqrt{D}]$.

Theorem 2.2.1. *For $n \in \mathbb{N}$, we have that*

$$(3 + 2\sqrt{2})^{2^{n-1}} = x_0 + y_0\sqrt{2^{2n+1}}, \tag{2.20}$$

where $3 + 2\sqrt{2}$ is the fundamental solution of $x^2 - 2y^2 = 1$ and $x_0 + y_0\sqrt{2^{2n+1}}$ is the fundamental solution of $x^2 - 2^{2n+1}y^2 = 1$. Furthermore, we have that

$$g(2^{2n+1}) = 2^{2n+1}.$$

Proof. We prove (2.20) by induction on $n \in \mathbb{N}$. For $n = 1$, we have

$$(3 + 2\sqrt{2})^{2^0} = 3 + 2\sqrt{2} = 3 + \sqrt{2^{2(1)+1}},$$

and clearly $(3, 1)$ is the minimal positive solution of $x^2 - 8y^2 = 1$, so we have verified (2.20) for $n = 1$.

Suppose that

$$(3 + 2\sqrt{2})^{2^{n-1}} = s + t\sqrt{2^{2n+1}} \tag{2.21}$$

holds for some $n, s, t \in \mathbb{N}$ with odd s, t. Then,

$$(3 + 2\sqrt{2})^{2^n} = (s + t\sqrt{2^{2n+1}})^2 = \left(s^2 + 2^{2n+1}t^2\right) + st\sqrt{2^{2(n+1)+1}}.$$

We have that s, t are odd by assumption, so $s^2 + 2^{2n+1}t^2$ and st are odd and give a solution to $x^2 - 2^{n+3}y^2 = 1$. Therefore, (2.21) holds for all $n \in \mathbb{N}$.

Now, we show that (s,t) is the fundamental solution of $x^2 - 2^{2n+1}y^2 = 1$. If (x_0, y_0) is the fundamental solution of $x^2 - 2^{2n+1}y^2 = 1$, then

$$s + t\sqrt{2^{2n+1}} = (x_0 + y_0\sqrt{2^{2n+1}})^j \tag{2.22}$$

for some $j \in \mathbb{N}$. Clearly, $(x_0, y_0 2^n)$ is a solution to $x^2 - 2y^2 = 1$, so

$$x_0 + y_0 2^n \sqrt{2} = (3 + 2\sqrt{2})^k \tag{2.23}$$

for some $k \in \mathbb{N}$. Combining (2.22) and (2.23) yields

$$(3 + 2\sqrt{2})^{2^{n-1}} = s + t\sqrt{2^{2n+1}} = (x_0 + y_0\sqrt{2^{2n+1}})^j = (3 + 2\sqrt{2})^{jk},$$

so $2^{n-1} = jk$ and, in particular, $k = 2^{k'}$ for some $k' \in \mathbb{N}_0$. In view of (2.21) and (2.23), we have that

$$x_0 + y_0\sqrt{2^{2n+1}} = (3 + 2\sqrt{2})^k = (3 + 2\sqrt{2})^{2^{k'}} = s' + t'\sqrt{2^{2(k'+1)+1}}$$

for some odd $s', t' \in \mathbb{N}$. If $k' + 1 < n$, then we have that $2^{n-k'-1}y_0 = t'$, but that makes t' even, which is a contradiction. If $k'+1 > n$, then we have that $2^{k'+1-n}t' = y_0$, contradicting the minimality of y_0. So, we must have that $n = k' + 1$, which makes $j = 1$. Therefore, (s,t) is the fundamental solution of $x^2 - 2^{2n+1}y^2 = 1$ by (2.22). We have shown the first part of our claim.

We have that $\mathrm{ord}_{\mathbb{Z}/2^{2n+1}\mathbb{Z}}(x_0) \leq 2$ and, by our induction, we have that y_0 is odd. So, we use Theorem 2.1.2 to conclude that

$$g(2^{2n+1}) = \mathrm{lcm}\left(\mathrm{ord}_{\mathbb{Z}/2^{2n+1}\mathbb{Z}}(x_0), \frac{2^{2n+1}}{\gcd(y_0, 2^{2n+1})}\right) = 2^{2n+1}.$$

□

Now, we show the analogous result for $D > 2$. We first need to establish the following three technical lemmas. As in the previous theorem, the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$, for $n \in \mathbb{N}$ fixed, is a power of the fundamental solution $x_0 + y_0\sqrt{D}$ of $x^2 - Dy^2 = 1$. Say that

$$x_M + y_M\sqrt{D^{2n+1}} = (x_0 + y_0\sqrt{D})^M$$

for some $M \in \mathbb{N}$ is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$. Using the binomial expansion of this power, we obtain an expression for y_M which is a sum of terms in the form $\binom{M}{2j+1}x_0^{M-2j-1}y_0^{2j+1}D^j$. The first of these technical lemmas allows us to simplify most of the expression for y_n as a multiple of DM, and subsequently we express y_n simply as

a multiple of My_0. This is useful for computing $\gcd(y_M, D^{2n+1})$, which appears in the formula for the order $g(D)$ given by Theorem 2.1.2. In turn, the lemma also plays a role in determining what M is, as we will see that M depends on the factors of y_0 and D.

Lemma 2.2.2. *Let $D \in \mathbb{N}$ and let $M \in \mathbb{N}$ be such that, for any prime p, $p \mid D$ if $p \mid M$. Then, we have*

$$DM \mid \binom{M}{2j+1} D^j$$

for any $2 \leq j \leq (M-1)/2$.

Proof. It suffices to show that

$$v_p(DM) \leq v_p\left(\binom{M}{2j+1} D^j\right) \tag{2.24}$$

for all primes p. We make use of the useful identity

$$\binom{M}{2j+1} D^j = (DM)\left(\frac{(M-1)\cdots(M-2j)D^{j-1}}{(2j+1)!}\right), \tag{2.25}$$

which transforms the problem of showing (2.24) into the equivalent problem of showing

$$v_p((2j+1)!) \leq v_p((M-1)\cdots(M-2j)D^{j-1}) \tag{2.26}$$

for all primes p. Legendre's formula gives us that, for any prime p and $m \in \mathbb{N}$, we have

$$v_p(m!) = \sum_{k=1}^{\infty} \left\lfloor \frac{m}{p^k} \right\rfloor \leq \sum_{k=1}^{\infty} \frac{m}{p^k} = m \sum_{k=1}^{\infty} \frac{1}{p^k} = \frac{m}{p-1}. \tag{2.27}$$

Let p be a prime dividing D. Consider the case when $p \geq 5$. By (2.27), we have

$$v_p((2j+1)!) \leq \frac{2j+1}{p-1} \leq \frac{2j+1}{4},$$

and since $v_p((2j+1)!)$ is an integer, we get further that

$$v_p((2j+1)!) \leq \left\lfloor \frac{2j+1}{4} \right\rfloor \leq \frac{j}{2} \leq j-1 \leq v_p(D)(j-1) = v_p(D^{j-1}),$$

which shows (2.26) and thus (2.24) for primes $p \geq 5$.

Now, let $p = 3$. By (2.27), we have

$$v_3((2j+1)!) \leq \frac{2j+1}{2} = j + \frac{1}{2}$$

and since $v_3((2j+1)!)$ is an integer, we get further that

$$v_3((2j+1)!) \leq j.$$

Since $j \geq 2$, there are at least 4 consecutive integers among $M-1,\ M-2, \ldots, M-2j$, and so $3 \mid (M-1)\ldots(M-2j)$. This implies that

$$v_3((M-1)\cdots(M-2j)D^{j-1}) \geq 1 + v_3(D)(j-1) \geq 1 + (j-1) = j \geq v_3((2j+1)!),$$

which proves (2.26) and thus (2.24) for $p = 3$.

Finally, let $p = 2$. Note that

$$\begin{aligned} v_2(5!) &= v_2(2^3(15)) = 3, \\ v_2(7!) &= v_2(2^4(315)) = 4. \end{aligned}$$

Since one of $M-1, \ldots, M-4$ is divisible by 4, we have $2^3 \mid (M-1)\cdots(M-4)$, and $2^4 \mid (M-1)\cdots(M-6)$, showing (2.26) for $j = 2, 3$. For $j \geq 4$, among $M-1, \ldots, M-2j$, there are j even numbers, and at least two of them are divisible by 4 because there are at least 8 consecutive integers. Thus, $2^{j+2} \mid (M-1)\cdots(M-2j)$. Note also that (2.27) gives us that

$$v_2((2j+1)!) \leq 2j+1.$$

It follows that

$$\begin{aligned} v_2((M-1)\cdots(M-2j)D^{j-1}) &\geq (j+2) + v_2(D)(j-1) \\ &\geq j+2+j-1 \\ &= 2j+1 \\ &\geq v_2((2j+1)!), \end{aligned}$$

which shows (2.26) for $j \geq 4$. Therefore, we have shown (2.26) and thus (2.24) for $p = 2$.

Since we have shown (2.24) for all primes $p \mid D$ and any $2 \leq j \leq (M-1)/2$, we are done. □

As previously mentioned, taking a power of the fundamental solution $x_0 + y_0\sqrt{D}$ of $x^2 - Dy^2 = 1$, say (x_M, y_M) defined by

$$x_M + y_M\sqrt{D} = (x_0 + y_0\sqrt{D})^M,$$

we may use the binomial expansion for y_M and the preceding lemma to express y_M as a multiple of My_0 and a factor containing the term

$$\frac{(M-1)(M-2)}{6}y_0^2 D.$$

Depending on whether if 3 divides y_0 and M, how many times 3 divides D, and the value of $D/3$ modulo 3, $\gcd(y_M/(My_0), D)$ is either 3 or 1. So, remarkably, the divisibility of y_0, D, and M by 3 is crucial in determining the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$ and the order $g(D^{2n+1})$.

Lemma 2.2.3. *Let $D \in \mathbb{N}$ be not a perfect square, and $M \in \mathbb{N}$ be such that, for any prime p, $p \mid D$ if $p \mid M$. If $(x_0, y_0) \in \mathbb{N}^2$ is a solution of $x^2 - Dy^2 = 1$ and*

$$(x_0 + y_0\sqrt{D})^M = x_M + y_M\sqrt{D}$$

for some $x_M, y_M \in \mathbb{N}$, then $y_M = My_0z_M$ with

$$\gcd(z_M, D) = \begin{cases} 3, & \text{if } 3 \nmid y_0,\ v_3(D) = 1,\ \frac{D}{3} \equiv -1 \pmod 3, \text{ and } 3 \mid M, \\ 1, & \text{else.} \end{cases} \tag{2.28}$$

Proof. We see that

$$\begin{aligned}
&(x_0 + y_0\sqrt{D})^M \\
&= \sum_{j=0}^{M} \binom{M}{j} x_0^{M-j}(y_0\sqrt{D})^j \\
&= \left(\sum_{0\le j\le M/2} \binom{M}{2j} x_0^{M-2j} y_0^{2j} D^j\right) + \left(\sum_{0\le j\le (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1} y_0^{2j+1} D^j\right)\sqrt{D} \\
&= x_M + y_M\sqrt{D}.
\end{aligned}$$

We shift our focus to y_M. By Lemma 2.2.2, we can write

$$\sum_{2\le j\le (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1} y_0^{2j+1} D^j = DMy_0k$$

for some $k \in \mathbb{N}$. Hence, we have

$$\begin{aligned} y_M &= \sum_{0 \le j \le (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1} y_0^{2j+1} D^j \\ &= M x_0^{M-1} y_0 + \binom{M}{3} x_0^{M-3} y_0^3 D + \sum_{2 \le j \le (M-1)/2} \binom{M}{2j+1} x_0^{M-2j-1} y_0^{2j+1} D^j \\ &= M x_0^{M-1} y_0 + \binom{M}{3} x_0^{M-3} y_0^3 D + DM y_0 k \\ &= M y_0 \left(x_0^{M-1} + \frac{(M-1)(M-2)}{6} x_0^{M-3} y_0^2 D + Dk \right) \\ &:= M y_0 z_M, \end{aligned}$$

where

$$z_M = \left(x_0^{M-1} + \frac{(M-1)(M-2)}{6} x_0^{M-3} y_0^2 D + Dk \right). \tag{2.29}$$

We now evaluate $\gcd(z_M, D)$. We use the fact that $\gcd(x_0, D) = 1$ since $x_0^2 - D y_0^2 = 1$ throughout.

If $3 \nmid D$, then $3 \nmid M$ by assumption and so $6 \mid (M-1)(M-2)$, meaning that $(M-1)(M-2)/6$ is an integer. Therefore, by (2.29), we have $\gcd(z_M, D) = \gcd(x_0^{M-1}, D) = 1$.

We now suppose that $3 \mid D$.

If $3 \mid y_0$, then $6 \mid (M-1)(M-2) y_0^2$, meaning that $(M-1)(M-2) y_0^2/6$ is an integer. Therefore, by (2.29), we have $\gcd(z_M, D) = \gcd(x_0^{M-1}, D) = 1$.

If $3 \nmid y_0$, then

$$\begin{aligned} \gcd(z_M, D) &= \gcd\left(x_0^{M-1} + \frac{(M-1)(M-2)}{2} x_0^{M-3} y_0^2 \frac{D}{3}, D \right) \\ &= \gcd\left(1 + \frac{(M-1)(M-2)}{2} y_0^2 \frac{D}{3}, D \right). \end{aligned} \tag{2.30}$$

Let p be a prime such that $p \mid D$ and $p \neq 3$. Then, $p \mid D/3$, so

$$p \nmid 1 + \frac{(M-1)(M-2)}{2} y_0^2 \frac{D}{3}.$$

Thus, the only possible prime divisor of $\gcd(z_M, D)$ is 3.

Still in the case in which $3 \nmid y_0$, suppose that $v_3(D) > 1$. Then, $3 \mid D/3$ and so

$$3 \nmid 1 + \frac{(M-1)(M-2)}{2} y_0^2 \frac{D}{3}.$$

It follows from (2.30) that

$$\gcd(z_M, D) = 1.$$

Still in the case in which $3 \nmid y_0$, suppose that $v_3(D) = 1$. Then,

$$\gcd(z_M, D) = \gcd\left(1 + \frac{(M-1)(M-2)}{2} y_0^2 \frac{D}{3}, D\right) \in \{1, 3\}.$$

We observe that

$$1 + \frac{(M-1)(M-2)}{2} y_0^2 \frac{D}{3} \equiv 0 \pmod 3 \tag{2.31}$$

if and only if

$$\frac{(M-1)(M-2)}{2} \frac{D}{3} \equiv 2 \pmod 3 \tag{2.32}$$

because we are in the case in which $3 \nmid y_0$ and so $y_0^2 \equiv 1 \pmod 3$. Since $3 \nmid D/3$, we have that $D/3 \equiv \pm 1 \pmod 3$. In the case that $D/3 \equiv 1 \pmod 3$, then (2.32) yields $(M-1)(M-2) \equiv 1 \pmod 3$, but this cannot hold for any $M \in \mathbb{Z}$. Thus, we must have that (2.31) cannot hold. It follows from (2.30) that $\gcd(z_M, D) = 1$. In the case that $D/3 \equiv -1 \pmod 3$, then (2.32) gives $(M-1)(M-2) \equiv 2 \pmod 3$, which is equivalent to having $3 \mid M$, which holds by assumption. Thus, (2.31) holds and it follows from (2.30) that $\gcd(z_M, D) = 3$. We conclude that (2.28) holds. □

Lemma 2.2.3 demonstrates that a power of the fundamental solution of $x^2 - Dy^2 = 1$ may yield a solution to $x^2 - D^{2n+1}y^2 = 1$, in particular by taking $M = D^n$ so $D^n \mid y_M$. Also, by taking $M = D^{2n+1}$, we have that $D^{2n+1} \mid y_M$, so

$$(x_n - y_n\sqrt{D^{2n+1}})^{\mathrm{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n) D^{2n+1}} \equiv 1 \pmod{\langle D^{2n+1} \rangle}$$

in $\mathbb{Z}[\sqrt{D^{2n+1}}]/D^{2n+1}\mathbb{Z}$, where (x_n, y_n) is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$. This implies that $g(D^{2n+1})$ divides $\mathrm{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n) D^{2n+1}$, and we shall see at the end of this section that the two quantities are very close for sufficiently large n. In the case that $3 \mid M$ and $3 \nmid y_0$, and letting $n = v_3(M)$, we may write

$$x_M + y_M\sqrt{D} = (x_0 + y_0\sqrt{D})^M = \left((x_0 + y_0\sqrt{D})^{3^n}\right)^{M/3^n} := (x_n + y_n\sqrt{D})^{M/3^n}.$$

The following lemma gives information on the divisibility properties of y_n, which will be useful when we establish the fundamental solution for $x^2 - D^{2k+1}y^2 = 1$ when (2.28) holds.

Lemma 2.2.4. *Let $D \in \mathbb{N}$ be not a perfect square. Suppose (x_0, y_0) is a solution of $x^2 - Dy^2 = 1$ such that $3 \nmid y_0$ and the following equation holds for $n = 1$:*

$$(x_0 + y_0\sqrt{D})^{3^n} = x_n + y_n\sqrt{D}, \tag{2.33}$$

where $v_3(y_n) = n + v_3(y_1) - 1 \geq 1$ and $y_n = 3^{v_3(y_n)} y_0 z_n$ for some $z_n \in \mathbb{N}$ with $3 \nmid z_n$ and $\gcd(z_n, D) = 1$. Then, (2.33) holds for all $n \in \mathbb{N}$.

Proof. We proceed by induction on $n \in \mathbb{N}$. The case $n = 1$ holds by our initial assumption. Suppose that (2.33) holds for some $n \in \mathbb{N}$. We see that

$$(x_0 + y_0)^{3^{n+1}} = (x_n + y_n\sqrt{D})^3 = (x_n^3 + 3x_n y_n^2 D) + (3x_n^2 y_n + y_n^3 D)\sqrt{D} := x_{n+1} + y_{n+1}\sqrt{D},$$

which gives

$$\begin{aligned} y_{n+1} &= 3x_n^2 y_n + y_n^3 D \\ &= 3y_n\left(x_n^2 + \frac{y_n^2}{3}D\right) \\ &= 3^{v_3(y_n)+1} y_0 z_n \left(x_n^2 + \frac{y_n^2}{3}D\right) \\ &:= 3^{v_3(y_n)+1} y_0 z_{n+1}. \end{aligned}$$

Since $x_n^2 - Dy_n^2 = 1$ and $3 \mid y_n$, we must have that $3 \nmid x_n$ and $\gcd(x_n, D) = 1$, giving us immediately that $3 \nmid z_{n+1}$ and $\gcd(z_{n+1}, D) = 1$. Moreover, we have that

$$v_3(y_{n+1}) = v_3\left(3y_n\left(x_n^2 + \frac{y_n^2 D}{3}\right)\right) = v_3(3y_n) = n + v_3(y_1).$$

This concludes the proof.

□

We now establish the result giving the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$ from that of $x^2 - Dy^2 = 1$.

Theorem 2.2.5. *Let $D \in \mathbb{N}$ be not a perfect square and let $x_0 + y_0\sqrt{D}$ be the fundamental solution of $x^2 - Dy^2 = 1$. Let $n_3 = v_3(3x_0^2 y_0 + Dy_0^3)$. We have three cases:*

(i) In the case that $0 \le n \le v_D(y_0)$, we have that $(x_0, y_0 D^{-n})$ is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$.

(ii) In the case that $v_D(y_0) < n$,

$$3 \nmid y_0,\ v_3(D) = 1,\ \text{and}\ \frac{D}{3} \equiv -1 \pmod 3, \tag{2.34}$$

and

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{3^{\min\{n, n_3\}-1}\gcd(y_0, D^n)}} = x_n + y_n\sqrt{D},$$

we have that $(x_n, y_n D^{-n})$ is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$.

(iii) In the case that $v_D(y_0) < n$, (2.34) does not hold, and

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{\gcd(y_0, D^n)}} = x_n + y_n\sqrt{D},$$

we have that $v_D(y_n) = n$ *and* $(x_n, y_n D^{-n})$ *is the fundamental solution of* $x^2 - D^{2n+1}y^2 = 1$.

Proof. (i) If $0 \leq n \leq v_D(y_0)$, we can write

$$1 = x_0^2 - Dy_0^2 = x_0^2 - D^{2n+1}(y_0 D^{-n})^2$$

with $y_0 D^{-n}$ being an integer, so $(x_0, y_0 D^{-n})$ is a solution of $x^2 - D^{2n+1}y^2 = 1$, and we claim that it is the smallest such solution. Indeed, if $(s,t) \in \mathbb{N}^2$ is a solution of $x^2 - D^{2n+1}y^2 = 1$, then (s, tD^n) is a solution of $x^2 - Dy^2 = 1$. By minimality of the fundamental solution, we must have that $tD^n \geq y_0$, which implies that $t \geq y_0 D^{-n}$, proving the minimality of $(x_0, y_0 D^{-n})$ as a solution for $x^2 - D^{2n+1}y^2 = 1$. This proves part (i).

(ii) We now consider the case in which $v_D(y_0) < n$ and (2.34) holds. We write

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}} = x_n + y_n\sqrt{D}.$$

Note that the exponent on the left-hand side is an integer in this case, so (x_n, y_n) is a solution of $x^2 - Dy^2 = 1$. By Lemma 2.2.4, we may write

$$(x_0 + y_0\sqrt{D})^{3^{n-\min\{n,n_3\}+1}} = x_0' + y_0'\sqrt{D},$$

with $v_3(y_0') = n - \min\{n, n_3\} + n_3 = \max\{n, n_3\}$ and

$$y_0' = 3^{\max\{n,n_3\}} y_0 z_0.$$

with $3 \nmid z_0$. It follows from this and Lemma 2.2.3 that

$$\begin{aligned}(x_0 + y_0\sqrt{D})^{\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}} &= \left((x_0 + y_0)^{3^{n-\min\{n,n_3\}+1}}\right)^{\frac{(D/3)^n}{\gcd(y_0,D^n)}} \\ &= (x_0' + y_0'\sqrt{D})^{\frac{(D/3)^n}{\gcd(y_0,D^n)}} \\ &= x_n + y_n\sqrt{D},\end{aligned} \tag{2.35}$$

where

$$\begin{aligned}y_n &= \frac{(D/3)^n}{\gcd(y_0, D^n)} y_0' z_0' \\ &= \frac{(D/3)^n}{\gcd(y_0, D^n)} 3^{\max\{n,n_3\}} y_0 z_0 z_0' \\ &= \left(\frac{D}{3}\right)^n 3^{\max\{n,n_3\}} \frac{y_0}{\gcd(y_0, D^n)} z_0 z_0'.\end{aligned} \tag{2.36}$$

Now, we wish to show that $(x_n, y_n D^{-n})$ is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$. Note that $\frac{y_0}{\gcd(y_0,D^n)}$ and $\frac{3^{\max\{n,n_3\}}}{3^n}$ are integers, so $D^n \mid y_n$ by (2.36). Thus, we have that

$(x_n, y_n D^{-n})$ is a solution of $x^2 - D^{2n+1}y^2 = 1$, and now we wish to show its minimality. Suppose $(s,t) \in \mathbb{N}^2$ is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$. Then,

$$x_n + y_n\sqrt{D} = (s + tD^n\sqrt{D})^j$$

for some $j \in \mathbb{N}$. Moreover, we have

$$s + tD^n\sqrt{D} = (x_0 + y_0\sqrt{D})^k \tag{2.37}$$

for some $k \in \mathbb{N}$. Therefore, we have

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}} = x_n + y_n\sqrt{D} = (s + tD^n\sqrt{D})^j = (x_0 + y_0\sqrt{D})^{jk}. \tag{2.38}$$

We claim that $j = 1$. Note that

$$k \mid \frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0, D^n)}. \tag{2.39}$$

We use Lemma 2.2.3 on (2.37) to get that

$$tD^n = ky_0z_0''$$

for some $z_0'' \in \mathbb{N}$.

Now, we will show that for each prime $p \mid D$ that

$$v_p\left(\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0, D^n)}\right) \leq v_p(k), \tag{2.40}$$

which will in turn imply that $j = 1$. Fix $p = 3$. Note that if $3 \nmid k$, then $\gcd(z_0'', D) = 1$ by (2.28) of Lemma 2.2.3, so $3 \nmid ky_0z_0'' = tD^\ell$, which contradicts the original assumption that $3 \mid D$. Thus, we have that $3 \mid k$. Write $k = 3^{v_3(k)}k'$, so $3 \nmid k'$. We write

$$s + tD^n\sqrt{D} = \left((x_0 + y_0\sqrt{D})^{3^{v_3(k)}}\right)^{k'} = (s' + t'\sqrt{D})^{k'},$$

where

$$tD^n = k't'z$$

with $3 \nmid z$ by Lemma 2.2.3 and $v_3(t') = v_3(k) + n_3 - 1$ by Lemma 2.2.4. Hence,

$$v_3(k) + n_3 - 1 = v_3(t') = v_3(tD^n) \geq v_3(D)n = n,$$

implying that

$$v_3(k) \geq n - n_3 + 1$$

and furthermore

$$v_3\left(\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}\right) = n - \min\{n,n_3\} + 1 \leq v_3(k),$$

proving (2.40) for $p = 3$.

Now suppose $p \mid D$ with $p \neq 3$. We have that $tD^n = ky_0z_0''$ with $\gcd(z_0'', D) \in \{1, 3\}$, so

$$v_p(k) + v_p(y_0) = v_p(tD^n) \geq v_p(D)n,$$

which implies that

$$\begin{aligned} v_p\left(\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}\right) &= v_p\left(\frac{D^n}{\gcd(y_0,D^n)}\right) \\ &= v_p(D)n - \min\{v_p(D)n, v_p(y_0)\} \\ &\leq v_p(k). \end{aligned}$$

Thus, we have shown (2.40) for all primes $p \mid D$, which shows that $k = \frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}$ and $j = 1$, meaning that (x_0, y_0D^{-n}) is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$ by (2.38).

(iii) Now, we consider the case in which $v_D(y_0) < n$ and (2.34) does not hold. We write

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{\gcd(y_0,D)}} = x_n + y_n\sqrt{D}.$$

Note that (x_n, y_n) is a solution of $x^2 - Dy^2 = 1$ and, by Lemma 2.2.3, we have $D^n \mid y_n$. So, (x_n, y_nD^{-n}) is a solution of $x^2 - D^{2n+1}y^2 = 1$ and we now show its minimality. Suppose (s, t) is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$. Then, as in case (ii), we have

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{\gcd(y_0,D)}} = x_n + y_n\sqrt{D} = (s + tD^n\sqrt{D})^j = (x_0 + y_0\sqrt{D})^{jk}$$

for some $j, k \in \mathbb{N}$ and so $j = 1$. □

Example 2.2.6. *Take $D = 6$. The fundamental solution of $x^2 - 6y^2 = 1$ is $(x_0, y_0) = (5, 2)$. Note that (2.34) holds and $v_D(y_0) = v_6(2) = 0$. Let (x_n, y_n) be the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$.*

If we take $n = 3$, we have $D^{2n+1} = 6^7 = 279936$. We observe that

$$\begin{aligned} \sqrt{279936} = [529;&\overline{11, 7, 3, 1, 7, 1, 1, 28, 1, 6, 3, 65, 1, 4, 2, 117, 8, 3, 1, 6, 1, 1, 2, 3, 1, 263,} \\ &\overline{1, 3, 2, 1, 1, 6, 1, 3, 8, 117, 2, 4, 1, 65, 3, 6, 1, 28, 1, 1, 7, 1, 3, 7, 11, 1058}], \end{aligned}$$

so

$$\begin{aligned} x_n &= 346916755974118654636389556531588801, \\ y_n &= 655685984072699434567329085653415. \end{aligned} \tag{2.41}$$

As in Theorem 2.2.5, we define $n_3 = v_3(3x_0^2y_0 + Dy_0^3)$. *Using Theorem 2.2.5(ii), we get immediately that*

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}} = (5+2\sqrt{6})^{\frac{216}{3^{\min\{3,2\}-1}\gcd(2,216)}} = (5+2\sqrt{6})^{36}$$

is the fundamental solution of $x^2 - 279936y^2 = 1$, *which coincides with (2.41).*

If we take $n = 7$, *we have* $D^{2n+1} = 6^{15} = 470184984576$. *Using Theorem 2.2.5(iii), we get immediately that*

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}} = (5+2\sqrt{6})^{\frac{279936}{3^{\min\{7,2\}-1}\gcd(2,279936)}} = (5+2\sqrt{6})^{46656}$$

is the fundamental solution of $x^2 - 470184984576y^2 = 1$.

Example 2.2.7. *Take* $D = 7$. *The fundamental solution of* $x^2 - 7y^2 = 1$ *is* $(x_0, y_0) = (8, 3)$. *Note that* $v_D(y_0) = v_7(3) = 0$, *and (2.34) does not hold as* $3 \nmid D$. *Let* (x_n, y_n) *be the fundamental solution of* $x^2 - D^{2n+1}y^2 = 1$.

If we take $n = 2$, *we have* $D^{2n+1} = 7^5 = 16807$. *We observe that*

$$\begin{aligned} \sqrt{16807} = [129;&\overline{1,1,1,3,1,4,9,2,1,1,6,4,2,1,1,13,1,4,2,1,3,2,42,1,3,2,2,1,1,6,2,2,} \\ &\overline{1,2,1,3,1,4,1,1,85,1,7,2,1,1,1,28,5,2,13,5,4,1,1,1,1,8,3,129,3,8,1,} \\ &\overline{1,1,1,4,5,13,2,5,28,1,1,1,2,7,1,85,1,1,4,1,3,1,2,1,2,2,6,1,1,2,2,3,} \\ &\overline{1,42,2,3,1,2,4,1,13,1,1,2,4,6,1,1,2,9,4,1,3,1,1,1,258}], \end{aligned}$$

so

$$\begin{aligned} x_n &= 41422006647842553948901599356619504905181932650376191205768, \\ y_n &= 319511161502786076679418767861070536190781689470984996467. \end{aligned} \tag{2.42}$$

Using Theorem 2.2.5(iii), we get immediately that

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{\gcd(y_0,D^n)}} = (8+3\sqrt{7})^{\frac{49}{\gcd(3,49)}} = (8+3\sqrt{7})^{49}$$

is the fundamental solution of $x^2 - 16807y^2 = 1$, *which coincides with (2.42).*

If we take $n = 7$, *we have* $D^{2n+1} = 7^{15} = 4747561509943$. *Using Theorem 2.2.5(iii), we get immediately that*

$$(x_0 + y_0\sqrt{D})^{\frac{D^n}{\gcd(y_0,D^n)}} = (8+3\sqrt{7})^{823543}$$

is the fundamental solution of $x^2 - 4747561509943y^2 = 1$.

2.2.2 Determining $g(D^{2n+1})$

We now determine the order $g(D^{2n+1})$ for sufficiently large n. To do so, we use the formula given by Theorem 2.1.2 on the fundamental solution (x_n, y_n) of $x^2 - D^{2n+1}y^2 = 1$ for cases (ii) and (iii) of Theorem 2.2.5 (we omit case (i) as n is made to be larger than $v_D(y_0)$). We first compute $\gcd(y_n, D^{2n+1})$ by using Lemma 2.2.3. Afterwards, we compute $\mathrm{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n)$ by showing that

$$\mathrm{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n) = \mathrm{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0)$$

in the case that D is odd, and in the case that D is even, Theorem 3.1.5 gives us $\mathrm{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n)$ immediately. In view of (2.5), we can interpret this result as giving us the minimal power M such that the fundamental unit of $\mathbb{Q}(\sqrt{D})$, which we call ω, such that $\omega^M \in \mathbb{Z}[\sqrt{D^{2n+1}}] = \mathbb{Z}[D\sqrt{D}]$ and $\omega^M \equiv 1 \pmod{\langle D\sqrt{D}\rangle}$.

Theorem 2.2.8. *Let $D > 2$ be an integer that is not a perfect square and $x_0 + y_0\sqrt{D}$ be the fundamental solution of $x^2 - Dy^2 = 1$. Recall that $n_3 := v_3(3x_0^2y_0 + Dy_0^3)$. If (2.34) does not hold and*

$$n \geq \max\{v_3(y_0) + 1, v_p(y_0)/v_p(D) : p \text{ prime and } p \mid D\},$$

or (2.34) holds and

$$n \geq \max\{v_3(y_0) + 1, n_3, v_p(y_0)/v_p(D) : p \text{ prime and } p \mid D\},$$

where n_3 is defined as in Theorem 2.2.5, then we have

$$g(D^{2n+1}) = \begin{cases} D^{2n+1} & \text{if } D \text{ is odd and } \mathrm{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 1, \\ 2D^{2n+1} & \text{if } D \text{ is odd and } \mathrm{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 2, \\ D^{2n+1} & \text{if } D \text{ is even.} \end{cases}$$

Proof. Suppose (2.34) does not hold and $n \geq \max\{v_3(y_0) + 1, v_p(y_0)/v_p(D) : p \mid D\}$. By Theorem 2.2.5(iii), we have that

$$(x_0 + y_0)^{\frac{D^n}{\gcd(y_0, D)}} := x_n + y_n\sqrt{D^{2n+1}}$$

is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$, and as in the proof of Theorem 2.2.5(iii), we use Lemma 2.2.3 to write

$$y_n = \frac{y_0 z_n}{\gcd(y_0, D^n)}$$

and $\gcd(z_n, D) = 1$. In view of Theorem 2.1.2, we must determine $\frac{D^{2n+1}}{\gcd(y_n, D^{2n+1})}$. For all $p \mid D$, we have $n \geq v_p(y_0)/v_p(D)$, so $v_p(D^n) \geq v_p(y_0)$, and so $\gcd(y_0, D^n) = y_0$ and $y_n = z_n$.

Since $\gcd(z_n, D) = 1$, we get

$$\frac{D^{2n+1}}{\gcd(y_n, D^{2n+1})} = \frac{D^{2n+1}}{\gcd(z_n, D^{2n+1})} = D^{2n+1},$$

so

$$g(D^{2n+1}) = \operatorname{lcm}\left(\operatorname{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n), D^{2n+1}\right) \tag{2.43}$$

by Theorem 2.1.2. Now, suppose (2.34) holds and $n \geq \max\{v_3(y_0) + 1, n_3, v_p(y_0)/v_p(D) : p \mid D\}$. By Theorem 2.2.5(ii), we have that

$$(x_0 + y_0)^{\frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}} := x_n + y_n\sqrt{D^{2n+1}}$$

is the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$, and as in the proof of Theorem 2.2.5(ii), we write

$$y_n = 3^{\max\{n,n_3\}-n}\frac{y_0}{\gcd(y_0, D^n)}z_0z_0'$$

and $\gcd(z_0z_0', D) = 1$. Since $n \geq n_3$, we have that $\max\{n, n_3\} - n = 0$, and again since $n \geq v_p(y_0)/v_p(D)$ for all $p \mid D$, we have $\gcd(y_0, D^n) = y_0$. Hence, $y_n = z_0z_0'$ and $\gcd(y_n, D^{2n+1}) = 1$, and (2.43) holds.

We now consider $\operatorname{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_0)$. We claim that if D is odd, then

$$\operatorname{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n) = \operatorname{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_0).$$

Equivalently, we claim that $x_n \equiv 1 \pmod{D^{2n+1}}$ if and only if $x_0 \equiv 1 \pmod{D}$. If $x_n \equiv 1 \pmod{D^{2n+1}}$, then using Corollary 2.1.6(i), we have that $x^2 - D^{2n+1}y^2 = 2$ is solvable, implying that $x^2 - Dy^2 = 1$ is solvable, so $x_0 \equiv 1 \pmod{D}$. Conversely, suppose $x_0 \equiv 1 \pmod{\text{D}}$. From the proof of Lemma 2.2.3, we have

$$x_n = \sum_{0 \leq j \leq M/2} \binom{M}{2j} x_0^{M-2j} y_0^{2j} D^j \equiv x_0^M \equiv 1 \pmod{\text{D}},$$

where $M = \frac{D^n}{\gcd(y_0, D^n)}$ or $M = \frac{D^n}{3^{\min\{n,n_3\}-1}\gcd(y_0,D^n)}$. We claim that D may be replaced by D^{2n+1} in the above equation. Indeed, x_n is a solution of $x^2 \equiv 1 \pmod{D^{2n+1}}$. For any odd prime $p \mid D$, we have that

$$x_n \equiv 1 \pmod{p} \tag{2.44}$$

and

$$x_n^2 \equiv 1 \pmod{p^2}. \tag{2.45}$$

It is well-known that the group of units of $\mathbb{Z}/p^r\mathbb{Z}$ for odd prime p is cyclic (see [6, p. 23]), so (2.44) implies that $x_n \equiv \pm 1 \pmod{p^2}$. Furthermore, (2.44) restricts us to having $x_n \equiv 1 \pmod{p^2}$. We may keep "lifting" x_n to a solution of $x \equiv 1 \pmod{p^{v_p(D)(2n+1)}}$ and

so by the Chinese remainder theorem, we conclude that

$$x_n \equiv 1 \pmod{D^{2n+1}}.$$

Suppose D is even. Then, by checking residues modulo 4, we have that $x^2 - D^{2n+1}y^2 = 2$ is not solvable, so $x_n \not\equiv 1 \pmod{D^{2n+1}}$ by Theorem 2.1.5.

Using our deductions about $\text{ord}_{\mathbb{Z}/D^{2n+1}\mathbb{Z}}(x_n)$ and (2.43), we conclude that

$$\begin{aligned} g(D^{2n+1}) &= \begin{cases} \text{lcm}\,(1, D^{2n+1}) & D \text{ is odd and } \text{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_n) = 1, \\ \text{lcm}\,(2, D^{2n+1}) & D \text{ is odd and } \text{ord}_{\mathbb{Z}/D\mathbb{Z}}(x_n) = 2, \\ \text{lcm}\,(2, D^{2n+1}) & D \text{ is even} \end{cases} \\ &= \begin{cases} D^{2n+1} & \text{if } D \text{ is odd and } ord_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 1, \\ 2D^{2n+1} & \text{if } D \text{ is odd and } ord_{\mathbb{Z}/D\mathbb{Z}}(x_0) = 2, \\ D^{2n+1} & \text{if } D \text{ is even.} \end{cases} \end{aligned}$$

□

We end this chapter with three examples for each case of $g(D^{2n+1})$ above.

Example 2.2.9. *Take $D = 3$. The fundamental solution of $x^2 - 3y^2 = 1$ is $(x_0, y_0) = (2, 1)$, and (2.34) does not hold because $D/3 = 1 \not\equiv -1 \pmod 3$. Note that*

$$\max\{v_3(y_0) + 1, v_p(y_0)/v_p(D) : p \mid D\} = \max\{1, v_3(1)/v_3(3)\} = 1.$$

Let (x_n, y_n) be the fundamental solution of $x^2 - D^{2n+1}y^2 = 1$.

If we take $n = 1$, we have $D^{2n+1} = 3^3 = 27$. We find that

$$\begin{aligned} x_n &= 26, \\ y_n &= 5. \end{aligned}$$

Since D is odd and $\text{ord}_{\mathbb{Z}/3\mathbb{Z}}(x_0) = 2$, Theorem 2.2.8 tells us that

$$g(27) = 2 \cdot 27 = 54,$$

meaning that $M = 54$ is the smallest $M \in \mathbb{N}$ such that

$$s_M + t_M\sqrt{27} = (26 + 5\sqrt{27})^M$$

satisfies $s_M + t_M\sqrt{27} \equiv 1 \pmod{\langle 27\rangle}$*, so*

$$s_M \equiv 1 \pmod{27},$$
$$t_M \equiv 0 \pmod{27}.$$

We explicitly compute s_M *and* t_M *for when* $M = 54$ *and get*

$$\begin{aligned} s_M &= 22618963758880140259918823160616036780646614307747750\ldots \\ &\quad \ldots 619327917682316129832507922626469725415 1 \equiv 1 \pmod{27}, \\ t_M &= 435302160499327947100141288840371984606408951934707 60\ldots \\ &\quad \ldots 207821404787288765908343800404526759020 \equiv 0 \pmod{27}. \end{aligned}$$

We set M *to be any proper divisor of* 54 *to check if* 54 *is the correct order and find that*

m	t_M	$t_M \pmod{27}$
2	260	17
3	13515	15
6	1898208780	24
9	266607219555045	18
18	738678891952086826989119042340	18

and finally $M = 27$ *yields*

$$s_M = 106346047784767582917770570173182418227924882 26 \equiv -1 \pmod{27},$$

confirming that 54 *is the correct order.*

Example 2.2.10. *Take* $D = 7$*. The fundamental solution of* $x^2 - 7y^2$ *is* $(x_0, y_0) = (8, 3)$*, and* (2.34) *does not hold because* $3 \nmid D$*. Note that*

$$\max\{v_3(y_0) + 1, v_p(y_0)/v_p(D) : p \mid D\} = \max\{2, v_7(3)/v_7(7)\} = 2.$$

Let (x_n, y_n) *be the fundamental solution of* $x^2 - D^{2n+1}y^2 = 1$*.*

If we take $n = 2$*, we have* $D^{2n+1} = 7^5 = 16807$*. We find that*

$$\begin{aligned} x_n &= 41422006647842553948901599356619504905181932650376191205768, \\ y_n &= 31951116150278607667941876786107053619078168947098 4996467. \end{aligned}$$

Note that

$$\mathrm{ord}_{\mathbb{Z}/16807\mathbb{Z}}(x_n) = 1.$$

By Theorem 2.2.8, we have

$$g(16807) = 16807,$$

meaning that $M = 16807$ *is the smallest* $M \in \mathbb{N}$ *such that*

$$s_M + t_M\sqrt{16807} = (x_n + y_n)^M$$

satisfies $s_M + t_M\sqrt{16807} \equiv 1 \pmod{\langle 16807\rangle}$*, so*

$$\begin{aligned} s_M &\equiv 1 \pmod{16807}, \\ t_M &\equiv 0 \pmod{16807}. \end{aligned}$$

Example 2.2.11. *Take* $D = 2$*. The fundamental solution of* $x^2 - 2y^2 = 1$ *is* $(x_0, y_0) = (3, 2)$ *and* (2.34) *does not hold because* $3 \nmid D$*. Note that*

$$\max\{v_3(y_0) + 1, v_p(y_0)/v_p(D) : p \mid D\} = \max\{1, v_2(2)/v_2(2)\} = 1.$$

Let (x_n, y_n) *be the fundamental solution of* $x^2 - D^{2n+1}y^2 = 1$*.*

If we take $n = 2$*, we have* $D^{2n+1} = 2^5 = 32$*. We find that*

$$\begin{aligned} x_n &= 17 \\ y_n &= 3. \end{aligned}$$

By Theorem 2.2.8, we have $M = 32$ *is the smallest* $M \in \mathbb{N}$ *such that*

$$s_M + t_M\sqrt{32} = (17 + 3\sqrt{32})^M$$

satisfies $s_M + t_M\sqrt{32} \equiv 1 \pmod{\langle 32\rangle}$*, so*

$$\begin{aligned} s_M &\equiv 1 \pmod{32}, \\ t_M &\equiv 0 \pmod{32}. \end{aligned}$$

We explicitly compute s_M *and* t_M *for when* $M = 32$ *and get*

$$\begin{aligned} s_M &= 4946041176255201878775086487573351061418968498177 \equiv 1 \pmod{32}, \\ t_M &= 8743448139394852930052129630176407298594910531 52 \equiv 0 \pmod{32}. \end{aligned}$$

We set M *to be any proper divisor of* 32 *to check if* 32 *is the correct order and find that*

m	t_M	$t_M \pmod{32}$
2	102	6
4	117708	12
8	156753391512	24
16	277996211087467034484528	16

which confirms that 32 *is the correct order.*

Chapter 3

Rudin-Shapiro sequences and their autocorrelations

Now, we shift our focus to the study of Rudin-Shapiro sequences and their autocorrelations for the rest of this thesis. Code for several of the computations in this chapter is given in Appendix A. The results of this chapter are published in [50].

3.1 Introduction

3.1.1 Notation

Here, we list all potentially ambiguous notation used in this chapter:

(i) For functions f and g from $\mathbb{C} \to \mathbb{C}$, we write

$$f(x) \ll g(x)$$

for $x \in S$ (where S is some subset of $\mathbb{R}$) if and only if there exists an absolute constant $K > 0$ such that

$$|f(x)| \leq K|g(x)|$$

for all $x \in S$.

(ii) For a ring R, we define $R^{n\times n}$ to be the n-by-n matrices with entries in R.

(iii) For a ring R and matrices $M_j, M_{j+1}, \cdots, M_k \in R^{n\times n}$, we use the convention

$$\prod_{i=j}^{k} M_i := M_k M_{k-1} \cdots M_j.$$

3.1.2 Binary sequences and autocorrelations

A *length-n binary sequence* for $n \in \mathbb{N}$ is defined to be an element of $\{-1, 1\}^n$. Binary sequences are ubiquitous objects that are studied in many different contexts.

In number theory, one may encounter the famous Liouville lambda function $\lambda : \mathbb{N} \to \{-1, 1\}$ with

$$\lambda(m) = \begin{cases} 1 & m \text{ is a product of an even number of primes} \\ -1 & m \text{ is a product of an odd number of primes} \end{cases},$$

for which one may consider finite binary sequences

$$(\lambda(m_0), \lambda(m_1), \ldots, \lambda(m_{n-1}))$$

for $\{m_i\}_{i=0}^{n-1} \subset \mathbb{N}$. We also have the *Legendre sequences*

$$\left(\left(\frac{1}{n}\right), \cdots, \left(\frac{n-1}{n}\right)\right)$$

for n prime, where $\left(\frac{\cdot}{n}\right)$ is the Legendre symbol. The *Thue-Morse sequences* $(t_0, t_1, \ldots, t_{n-1})$ are defined by

$$t_i = \#\text{ of 1's in the binary expansion of } i.$$

The Thue-Morse sequences find their way into game theory, differential geometry, and give rise to a solution for the Prouhet-Tarry-Escott problem, which is concerned with finding sets of integers $A, B \subset \mathbb{N}$ such that

$$\sum_{a \in A} a^i = \sum_{b \in B} b^i$$

for all $1 \leq i \leq k$ for some $k \in \mathbb{N}$, among other things [5]. The related binary sequences $((-1)^{t_0}, (-1)^{t_1}, \ldots, (-1)^{t_n})$ have also been extensively studied. Similar to these are the *Rudin-Shapiro sequences* $(a_0, a_1, \ldots, a_{n-1})$ (also called the *Golay-Rudin-Shapiro sequences*), which we study in Chapters 3 and 4, and are defined by

$$a_i = (-1)^{\#\text{ of 11's in the binary expansion of } i}.$$

Consider a length-n binary sequence $\mathbf{s} = (s_0, s_1, \ldots, s_{n-1})$. We define the *aperiodic autocorrelation of* $\mathbf{s}$ *at shift* k to be

$$\sum_{i=0}^{n-1} s_i s_{i+k},$$

where $s_i = 0$ for $i \notin [0, n-1]$. Likewise, we can define the *periodic autocorrelation of* $\mathbf{s}$ *at shift* k to be the same sum but taking $s_i = s_{i \bmod n}$ for all $i \in \mathbb{Z}$. For instance, if we take

$\mathbf{s} = (-1, 1, 1, -1)$, we have

aperiodic autocorrelation of $\mathbf{s}$ at shift 2:

	-1	1	1	-1		
×			-1	1	1	-1
			-1	-1		

(-1) + (-1) = -2,

periodic autocorrelation of $\mathbf{s}$ at shift 2:

	-1	1	1	-1
×	1	-1	-1	1
	-1	-1	-1	-1

(-1) + (-1) + (-1) + (-1) = -4,

where the multiplication is understood to be component-wise. Aperiodic autocorrelation and periodic autocorrelation are also referred to as *acyclic* autocorrelation and *cyclic* autocorrelation, respectively. Of course, the periodic autocorrelation of $\mathbf{s}$ at shift k can be expressed as the sum of the aperiodic autocorrelations of $\mathbf{s}$ at shifts k and $n-k$. Because of this, we are mostly interested in studying the aperiodic autocorrelations of binary sequences. Denote by $C(k)$ the aperiodic autocorrelation of $\mathbf{s}$ at shift k. Clearly, the peak autocorrelation $C(0)$ is always equal to n. If a sequence resembles itself at a particular shift, then either autocorrelation at that shift will be relatively large in magnitude. Thus, both notions of autocorrelation are used as measures of the similarity of a sequence to its translates. In some contexts (e.g. signal processing), it is desirable to find binary sequences with small aperiodic autocorrelation at every nonzero shift, i.e., sequences with the ℓ^∞ norm of the vector of off-peak autocorrelations

$$v_C := \begin{bmatrix} C(1) \\ C(2) \\ \vdots \\ C(n-1) \end{bmatrix}$$

being small. If $\mathbf{s}$ has minimal autocorrelations (i.e., $|C(k)| \leq 1$ for all $k > 1$), then we call $\mathbf{s}$ a *Barker sequence*. It is widely believed that no Barker sequences of length greater than 13 exist, as this has been verified for lengths up to 10^{22} by Leung and Schmidt and for all odd lengths greater than 13 by Turyn and Storer [12, 34]. In this chapter, we study $\|v_C\|_\infty$ in the case that $\mathbf{s}$ is a Rudin-Shapiro sequence. The worst possible case for $\|v_C\|_\infty$ for $\mathbf{s}$ being an arbitrary binary sequence is that it is equal to the length of the sequence. Remarkably, in the case that $\mathbf{s}$ is a Rudin-Shapiro sequence of length $n = 2^m$, we have $\|v_C\|_\infty = \lambda^m$, where λ is a number less than 2. We devote Chapter 4 to further study of the $\|v_C\|_\infty$ as well as investigating v_C under other ℓ^p norms in the case that $\mathbf{s}$ is a Rudin-Shapiro sequence. One can view the study of $\|v_C\|_2$ as the study of the *merit factor*.

In [27], Golay defines the merit factor of a binary sequence $(s_0, s_1, \ldots, s_{n-1})$ with aperiodic autocorrelations $C(k)$ as

$$\frac{n^2}{2\sum_{k=1}^{n-1} C(k)^2}.$$

In [31], it is shown that an equivalent definition is given by

$$\frac{n^2}{\left\|\sum_{j=0}^{n-1} s_j z^j\right\|_4^4 - n^2},$$

where the norm used is the L^4 norm on the unit circle in $\mathbb{C}$. This connects the well-studied areas of autocorrelations of binary sequences and L^p norms of *Littlewood polynomials* (i.e., polynomials with ± 1 coefficients). The history of the hunt for Littlewood polynomials with small L^p norms is briefly summarized in [35]. In fact, Littlewood shows in [36] that, when $\mathbf{s}$ is a Rudin-Shapiro sequence, we have $\|\sum_{j=0}^{n-1} s_j z_j\|_4$ is asymptotically $4/3$ as $m \to \infty$ — see [11] for a proof of a stronger result on the L^4 norm of polynomials in a broader class. It is of interest to find sequences with large merit factor because this implies that the sums of squares of their autocorrelations are small, and these sequences are quite rare as the expected merit factor of a length-n binary sequence is asymptotically 1 as $n \to \infty$ [11, 45]. Littlewood's result on $\|p_m\|_4^4$ shows that the merit factor of the m-th Rudin-Shapiro sequence tends to 3 as $m \to \infty$, and a much simpler argument was given by Høholdt-Jensen-Justesen in [32] through use of a recursive relation on $\sum_{k=1}^{2^m} C(k)^2$ in the case that $\mathbf{s}$ is a Rudin-Shapiro sequence. In particular, we have that

$$\sum_{k=1}^{2^m} C(k)^2 \sim \frac{4^m}{6} \tag{3.1}$$

when $\mathbf{s}$ is the m-th Rudin-Shapiro sequence. In [34], Jedwab-Katz-Schmidt give a class of sequences – derived from Legendre sequences – with asymptotic (in terms of increasing sequence length) merit factor approximately 6.34, which stands as the record for greatest asymptotic merit factor for a class of binary sequences. It is widely believed that there exists a uniform bound for the merit factor of all binary sequences, and the search for infinite families of sequences with easily computable and large asymptotic merit factors is ongoing. As mentioned in [34], if $\mathbf{s}$ is a Barker sequence, then it has merit factor

$$\frac{n^2}{2\sum_{k=1}^{n-1} C(k)^2} \geq \frac{n^2}{2n} = \frac{n}{2},$$

which of course tends to infinity as $n \to \infty$, so proving the existence of a uniform bound for merit factors would also prove that there are only finitely many Barker sequences. For a broad overview of the merit factor problem, see [10, 30, 33, 34].

3.1.3 Overview

The *m-th Rudin-Shapiro sequence* $(a_0, a_1, \ldots, a_{2^m-1})$ is defined by

$$a_i = (-1)^{\#\text{ of pairs of consecutive ones in the binary expansion of } i}.$$

For example, we have

$$\begin{aligned}
\text{1st Rudin-Shapiro sequence} &= ((-1)^0, (-1)^0) = (1, 1),\\
\text{2nd Rudin-Shapiro sequence} &= (1, 1, 1, -1),\\
\text{3rd Rudin-Shapiro sequence} &= (1, 1, 1, -1, 1, 1, -1, 1).
\end{aligned}$$

There are several popular recursive definitions for the Rudin-Shapiro sequences [32, 41, 3, 4, 38]. For instance, we may define the *m-th Shapiro polynomial* p_m by

$$\begin{aligned}
q_0(z) &= 1,\\
p_0(z) &= 1,\\
q_m(z) &= p_{m-1}(z) - z^{2^{m-1}} q_{m-1}(z),\\
p_m(z) &= p_{m-1}(z) + z^{2^{m-1}} q_{m-1}(z),
\end{aligned} \tag{3.2}$$

and the m-th Rudin-Shapiro sequence arises as the coefficients of p_m, so

$$p_m(x) = \sum_{i=0}^{2^m-1} a_i x^i.$$

The definition of Rudin-Shapiro sequences using the relations (3.2) is a very popular one due to the many identities one can easily derive from the relations. The Shapiro polynomials are an example of Littlewood polynomials (i.e., polynomials with ± 1 coefficients), which are extensively studied. The reason for restricting our study of autocorrelations to those of Rudin-Shapiro sequences is due to their rich structure, from which interesting combinatorial properties arise. Some of these properties allow us to more easily compute and bound autocorrelations, as we show in Section 2.2. For each Rudin-Shapiro sequence $(a_0, a_1, \ldots, a_{2^m-1})$ and $0 \le k < 2^m$, we define

$$\begin{aligned}
C_m(k) &= \sum_{i=0}^{2^m-1} a_i a_{i+k}, \qquad \text{where } a_j = 0 \text{ for } j \ge 2^m,\\
P_m(k) &= \sum_{i=0}^{2^m-1} a_i a_{i+k}, \qquad \text{where } a_j = a_{j \bmod 2^m} \text{ for } j \ge 2^m,
\end{aligned}$$

so $C_m(k)$ is the aperiodic autocorrelation at shift k, and $P_m(k)$ is the periodic autocorrelation at shift k. In view of (3.1), the order of the ℓ^2 norm of the sequence of all $C_m(k)$ is established, and we extend this result in Section 4.3. We devote Chapters 3 and 4 to focus on other ℓ^p norms. In particular, the main objective of this chapter is to provide an alternative proof of the following result on the ℓ^∞ norm of $C_m(k)$:

Theorem 3.1.1. *For all $m \in \mathbb{N}$, there exist $K_1, K_2 > 0$ such that*

$$K_1\lambda^m \leq \max_{k\neq 0} |C_m(k)| \leq K_2\lambda^m,$$

where $\lambda = 1.659\cdots$ is the real root of $x^3 + x^2 - 2x - 4$.

In [38], Katz and van der Linden prove Theorem 3.1.1 with the best possible K_2 (being $5/\lambda^4$, which is approximately 0.660) using algebraic number theory and recursive relations derived from the polynomials p_m and q_m. Theorem 3.1.1 was originally proven in [4, 19], in which the first step was translating the problem of showing $\max_{k\neq 0} |C_m(k)| \ll \lambda^m$ into the problem of showing

$$\max_{(\alpha_1,\alpha_2,\ldots,\alpha_m)} \left\| \prod_{i=1}^{m} T_{\alpha_i} \right\|_2 \ll \lambda^m$$

for $(\alpha_1, \alpha_2, \ldots, \alpha_m) \in \{1, 2, 3, 4\}^m$, some $T_{\alpha_i} \in \mathbb{Z}^{3\times 3}$, and $\|\cdot\|_2$ being the standard matrix 2-norm defined by

$$\|A\|_2 = \max_{\|x\|_2=1} \|Ax\|_2,$$

for any matrix $T \in \mathbb{Z}^{3\times 3}$, or, equivalently,

$$\|A\|_2 = \sqrt{\sigma(A^T A)},$$

where $\sigma(A^T A)$ denotes the largest eigenvalue (the spectral radius) of $A^T A$. Allouche et al. in [4] reduce the number of matrices considered in the product, which led to showing

$$\max_{k\neq 0} |C_m(k)| \ll (1.00000100000025\lambda)^m$$

which is very close to the desired result. Additionally, the lower bound of Theorem 3.1.1 is proven in [4]. Finally, in [19], Choi uses these advances to establish the upper bound of Theorem 3.1.1 with $K_2 < 3.783$. We note that in [19], Choi misinterprets their Theorem 1.1 as being for periodic autocorrelation when it actually concerns aperiodic autocorrelation. This result on $C_m(k)$ is used to establish results on the oscillation of the modulus of Shapiro polynomials on the unit circle [25]. We use roughly the same ideas as in [4, 19], although constants are left implicit and the crux of our computations given in Lemma 3.2.6 is simpler than those of the computations given in [38, 19], so we have a shorter and more easily verifiable proof of Theorem 3.1.1 at the expense of precision — for explicit bounds, see [38]. We follow this with Theorem 3.2.12, an analogous result for $P_m(k)$, which we briefly state below:

Theorem 3.2.12. *For $m \geq 3$, we have that $P_m(k)$ is either 0 or $4C_{m-2}(|2^{m-1} - k|)$ depending on k, and also that*

$$\lambda^m \ll \max_{k\neq 0} |P_m(k)| \ll \lambda^m.$$

This is inspired by a private communication by B. Saffari, in which they state that for Rudin-Shapiro sequences, both their periodic autocorrelations and aperiodic autocorrelations behave similarly. Finally, in Section 3.3, we discuss how the problem of proving Theorem 3.1.1 is essentially the problem of computing a so-called joint spectral radius which was introduced in [47], and provide a heuristic proof of Theorem 3.1.1 using an algorithm introduced in [28]. We begin with some preliminary work for the proof of Theorem 3.1.1.

3.2 Proof of the main theorem

We begin with a sketch of the proof of Theorem 3.1.1. First, we fix $m \in \mathbb{N}$ and $1 \leq k < 2^m$ and we consider a vector $v_m = v_m(k) \in \mathbb{R}^3$ with its first component being $C_m(k)$, so

$$v_m = \begin{bmatrix} C_m(k) \\ \vdots \end{bmatrix}. \tag{3.3}$$

The other entries of v_m are defined piecewise, depending on k, so we leave the full definition of v_m for (3.5) and (3.7). Next, we derive a decomposition of v_m as a matrix-vector product:

$$v_m = \prod_{i=1}^{m} \left(U^{\alpha_i} V^{\beta_i} \right) \cdot v$$

for some $U, V \in \mathbb{Z}^{3\times 3}$, $(\alpha_i, \beta_i) \in \{(1,0),(0,1)\}$, and $v \in \mathbb{R}^3$. The lower bound in Theorem 3.1.1 is proven quickly by diagonalizing U. Finally, we prove the upper bound by showing that

$$\max_{\alpha_i,\beta_i} \left\| \prod_{i=1}^{m} U^{\alpha_i} V^{\beta_i} \right\|_2 \ll \lambda^m, \tag{3.4}$$

and using the fact that

$$|C_m(k)| \leq \|v_m\|_2 \ll \max_{\alpha_i,\beta_i} \left\| \prod_{i=1}^{m} U^{\alpha_i} V^{\beta_i} \right\|_2.$$

We now begin developing our actual proof of Theorem 3.1.1. The following lemma reduces the problem studying $C_m(k)$ only for odd k.

Lemma 3.2.1 (Høholdt et al., 1985)**.** *For all $m \in \mathbb{N}$ and even $k \in \mathbb{Z}$, we have that*

$$C_m(k) = P_m(k) = 0.$$

Proof. This is Theorem 2.1 in [32]. □

Now, we construct the v_m in (3.3) for fixed m. For $m \in \mathbb{N}$ and fixed k_m with $0 \leq k_m \leq 2^m$, define

$$k'_m = 2^m - k_m,$$
$$k_{m-1} = \begin{cases} k_m & \text{if } k_m \leq 2^{m-1}, \\ k'_m & \text{else.} \end{cases} \tag{3.5}$$

We wish to split $[0, 2^m]$ into four equal-length subintervals. For $1 \leq n \leq 4$, define the open intervals

$$S_m^n = ((n-1)2^{m-2}, n2^{m-2}). \tag{3.6}$$

We now only consider only odd k_m and turn our attention to

$$v_m = v_m(k_m) := \begin{bmatrix} C_m(k_m) \\ C_m(k'_m) \\ C_{m-1}(k_{m-1}) \end{bmatrix}. \tag{3.7}$$

Throughout the rest of this chapter, we use

$$M = \begin{bmatrix} 0 & 1 & 2 \\ 0 & -1 & 2 \\ 1 & 0 & 0 \end{bmatrix}, \quad A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Note that $A^2 = I$.

Lemma 3.2.2. *For $m \geq 3$, there exist $\alpha_i, \beta_i, c \in \{0, 1\}$ for $i = 3, \ldots, m$ such that*

$$v_m = \left(\prod_{i=3}^{m} A^{\alpha_i} M B^{\beta_i} \right) A^c \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}. \tag{3.8}$$

Proof. Let $m \geq 3$ and k_m be such that $0 \leq k_m \leq 2^m$ and k_m is odd. Høholdt, Jensen, and Justesen in Theorem 2.2 of [32] showed, for $m \geq 3$, that

$$C_m(k_m) = \quad C_{m-1}(2^{m-1} - k_m) \qquad \text{if } \ k_m \in S_m^1, \tag{3.9}$$
$$C_m(k_m) = \quad C_{m-1}(2^{m-1} - k_m) + 2C_{m-2}(2^{m-1} - k_m) \qquad \text{if } \ k_m \in S_m^2, \tag{3.10}$$
$$C_m(k_m) = -C_{m-1}(k_m - 2^{m-1}) + 2C_{m-2}(k_m - 2^{m-1}) \qquad \text{if } \ k_m \in S_m^3, \tag{3.11}$$
$$C_m(k_m) = -C_{m-1}(k_m - 2^{m-1}) \qquad \text{if } \ k_m \in S_m^4. \tag{3.12}$$

Let $k_m \in S_m^1$ be as defined in (3.5). We see that $k_{m-1} = k_m$, which implies $k'_{m-1} = 2^{m-1} - k_{m-1} = 2^{m-1} - k_m$. Using this along with the relations above, we get

$$C_m(k_m) = C_{m-1}(k'_{m-1})$$

by (3.9), and

$$C_m(k'_m) = C_m(2^m - k_m) = -C_{m-1}(k'_{m-1})$$

by (3.12). Thus,

$$v_m = \begin{bmatrix} C_m(k_m) \\ C_m(k'_m) \\ C_{m-1}(k_{m-1}) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} C_{m-1}(k_{m-1}) \\ C_{m-1}(k'_{m-1}) \\ C_{m-2}(k_{m-2}) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} v_{m-1} = MBv_{m-1}.$$

Now, let $k_m \in S_m^2$. We see that $k_{m-1} = k_m$ and $k'_{m-1} = k_{m-2}$ by (3.5), so using (3.10) and (3.11) respectively, we get

$$C_m(k_m) = \quad C_{m-1}(k'_{m-1}) + 2C_{m-2}(k'_{m-1}) = \quad C_{m-1}(k'_{m-1}) + 2C_{m-2}(k_{m-2}),$$

and

$$C_m(k'_m) = -C_{m-1}(k'_{m-1}) + 2C_{m-2}(k'_{m-1}) = -C_{m-1}(k'_{m-1}) + 2C_{m-2}(k_{m-2}).$$

Thus,

$$v_m = \begin{bmatrix} 0 & 1 & 2 \\ 0 & -1 & 2 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} C_{m-1}(k_{m-1}) \\ C_{m-1}(k'_{m-1}) \\ C_{m-2}(k_{m-2}) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 \\ 0 & -1 & 2 \\ 1 & 0 & 0 \end{bmatrix} v_{m-1} = Mv_{m-1}.$$

Now, let $k_m \in S_m^3$. We see that $k_{m-1} = k'_m$ and $k'_{m-1} = k_{m-2}$ by (3.5), so using (3.11) and (3.10) respectively, we get

$$C_m(k_m) = -C_{m-1}(k'_{m-1}) + 2C_{m-2}(k'_{m-1}) = -C_{m-1}(k'_{m-1}) + 2C_{m-2}(k_{m-2}),$$

and

$$C_m(k'_m) = \quad C_{m-1}(k'_{m-1}) + 2C_{m-2}(k'_{m-1}) = \quad C_{m-1}(k'_{m-1}) + 2C_{m-2}(k_{m-2}).$$

Thus,

$$v_m = \begin{bmatrix} 0 & -1 & 2 \\ 0 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} C_{m-1}(k_{m-1}) \\ C_{m-1}(k'_{m-1}) \\ C_{m-2}(k_{m-2}) \end{bmatrix} = \begin{bmatrix} 0 & -1 & 2 \\ 0 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix} v_{m-1} = AMv_{m-1}.$$

Now, let $k_m \in S_m^4$. We see that $k_{m-1} = k'_m$, so using (3.12) and (3.9) respectively, we get

$$\begin{aligned} C_m(k_m) &= -C_{m-1}(k'_{m-1}), \\ C_m(k'_m) &= \quad C_{m-1}(k'_{m-1}). \end{aligned}$$

Thus,

$$v_m = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} C_{m-1}(k_{m-1}) \\ C_{m-1}(k'_{m-1}) \\ C_{m-2}(k_{m-2}) \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} v_{m-1} = AMBv_{m-1}.$$

In summary, we have shown that

$$v_m = T_m v_{m-1}, \tag{3.13}$$

where

$$T_m = \begin{cases} MB, & k_m \in S_m^1 \\ M, & k_m \in S_m^2 \\ AM, & k_m \in S_m^3 \\ AMB, & k_m \in S_m^4 \end{cases}. \tag{3.14}$$

Finally, let

$$v = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}.$$

We see that $C_1(k_1) = C_1(1) = 1$ and

$$\begin{bmatrix} C_2(k_2) \\ C_2(k'_2) \end{bmatrix} = \begin{cases} \begin{bmatrix} 1 \\ -1 \end{bmatrix} & k_2 = 1, \\ \begin{bmatrix} -1 \\ 1 \end{bmatrix} & k_2 = 3. \end{cases}$$

Since $k_2 = 1$ if and only if $k_3 \in \{1, 7\}$ and $k_2 = -1$ if and only if $k_3 \in \{3, 5\}$, we have

$$v_2 = \begin{cases} v, & k_3 \in S_3^1 \cup S_3^4 \\ Av, & k_3 \in S_3^2 \cup S_3^3 \end{cases}. \tag{3.15}$$

Inductively applying (3.13), we are done. □

It is worth noting that Høholdt et al. use the relations (3.9)-(3.12) to obtain upper bounds for $\max_{k \neq 0} |C_m(k)|$, but they do not have a way to address the branching recursion depending on k_m, leading to a weaker bound of 1.85^m up to an absolute constant. The consideration of the maximum norm over all matrix products given by Lemma 3.2.2 of fixed length m gives a tractable alternative method to bounding $\max_{k \neq 0} |C_m(k)|$. We may express v_m more simply. We express v_m as a matrix-vector product depending only on the matrices MA and MB. To do so, we first need to define a new class of sequences. Fix

$k_m \in (0, 2^m)$ odd, and define the left-infinite sequence

$$Gray(1) = (\cdots, 0, 0)$$

and let the left-infinite sequence $Gray(k_m) = (\cdots, g_1, g_0)$ be defined by

$$\begin{aligned}(\cdots, g_{m+1}, g_m) &= (\cdots, 0, 0),\\ (g_{m-1}, \cdots, g_1, g_0) &= \begin{cases}(0, g'_{m-3}, \cdots, g'_1, g'_0) & k_m < 2^{m-1},\\ (1, g'_{m-3}, \cdots, g'_1, g'_0) & k_m > 2^{m-1},\end{cases}\end{aligned} \tag{3.16}$$

where $(\cdots, g'_1, g'_0) = Gray(k_{m-1})$ and k_{m-1} is as in (3.5). We call $Gray(k)$ the *modified Gray code representation of* k, and one can see that $Gray(k)$ is the *Gray code representation* for $\frac{k-1}{2}$ (see [40]). For instance, we have

$$\begin{aligned}Gray(3) &= (\cdots, 0, 0, 1),\\ Gray(5) &= (\cdots, 0, 1, 1),\\ Gray(7) &= (\cdots, 0, 1, 0),\\ Gray(9) &= (\cdots, 1, 1, 0).\end{aligned} \tag{3.17}$$

Note that $Gray(k)$ and $Gray(k+2)$ differ in only one entry, i.e. it requires only one bit shift to get the modified Gray code representation of $k+2$ from the Gray code representation of k.

Lemma 3.2.3. *Fix $m \geq 3$ and let $0 < k_m < 2^m$ be odd. Let v_m be as in (3.7). Let $(\cdots, g_1, g_0)$ be the modified Gray code representation of k_m and define*

$$\begin{aligned}\varphi(0) &= MB,\\ \varphi(1) &= MA.\end{aligned}$$

Then, we have that

$$v_m = A^{g_{m-2}} \left(\prod_{i=0}^{m-3} \varphi(g_i) \right) \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}. \tag{3.18}$$

Proof. We first establish some multiplication rules for the matrices given in (3.13). By Lemma 3.2.2, we have that

$$v_m = (T_m T_{m-1} \cdots T_3) A^c \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix},$$

where

$$T_i \in \{MB, M, AM, AMB\}$$

for all i. In the notation of (3.5) and (3.6), if $k_m \in S^1_m$, then $k_{m-1} \in S^1_{m-1}$ or $k_{m-1} \in S^2_{m-1}$. Thus, if $T_i = MB$, then $T_{i-1} \in \{MB, M\}$ for all $3 < i \leq m$. Likewise, we consider $k_m \in S^n_m$ for $2 \leq n \leq 4$ and observe that

$$T_i T_{i-1} \in \{MBMB, MBM, MAM, MAMB, AMAM, AMAMB, AMBMB, AMBM\}. \tag{3.19}$$

Note that all possibilities for $T_i T_{i-1}$ are products of exclusively MA and MB up to left-multiplication and right-multiplication by A. We proceed by induction on m. By (3.17), this is true for $m = 3$. Assume (3.18) is true for $m-1$ in place of m. We use our inductive hypothesis:

$$v_m = T_m A^{g'_{m-3}} \left(\prod_{i=0}^{m-4} \varphi(g'_i) \right) \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = A^a M B^b A^{g'_{m-3}} \left(\prod_{i=0}^{m-4} \varphi(g'_i) \right) \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}, \tag{3.20}$$

where $a, b \in \{0, 1\}$ and $(\cdots, g'_1, g'_0)$ is the modified Gray code representation of k_{m-1}. Due to (3.14), we have

$$a = \begin{cases} 0 & k_m \in S^1_m \cup S^2_m, \\ 1 & \text{otherwise.} \end{cases} \tag{3.21}$$

Due to (3.19), we have

$$(b, g'_{m-3}) = \begin{cases} (1,0) & k_m \in S^1_m \cup S^4_m, \\ (0,1) & \text{otherwise.} \end{cases} \tag{3.22}$$

Using (3.20) and (3.22), we have shown that

$$v_m = A^a \left(\prod_{i=0}^{m-3} \varphi(g'_i) \right) \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix},$$

and by (3.16) and (3.21), we know that

$$(\cdots, 0, 0, a, g'_{m-3}, \cdots, g'_1, g'_0) = Gray(k_m),$$

so we are done. □

To the best of our knowledge, there is nothing currently in the literature expressing a connection between Rudin-Shapiro sequences and Gray codes. It is known from [4] that

v_m can be expressed as a matrix-vector product in which the matrix can be factored as a product of two particular matrices ("M_1" and "B" in [4], and MA and MB in our approach). However, it is remarkable that the product exhibits this well-known structure given by Gray codes.

Remark 3.2.4. *Let*

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

The matrix M_1 in Lemma 3 of [4] is our $SMAS$, and the matrix B is our $SMBS$. Since S is an isometry and $S^2 = I$, the matrix products in [4] and [19] are exactly the same as ours in norm. Due to this matrix similarity, we can pass to the calculations given in [19]. However, we will take a different approach to the computations through Lemma 3.2.6 and Lemma 3.2.8. The nature of the proof of Lemma 3.2.6 is asymptotic and will require a check of several base cases. We note that the number of base cases is small enough as to not require a computer. Throughout the rest of this paper, we denote $\|\cdot\|_2$ by $\|\cdot\|$.

The following three technical lemmas are the crux of our argument and are used along with the submultiplicativity of $\|\cdot\|$ (i.e., $\|M_1M_2\| \leq \|M_1\|\|M_2\|$ for all $M_1, M_2 \in \mathbb{R}^{3\times 3}$) to show that

$$\left\| \prod_{i=1}^{m} (MA)^{\alpha_i} (MB)^{\beta_i} \right\| \ll \prod_{i=1}^{m} \lambda^{\alpha_i+\beta_i} \tag{3.23}$$

as in (3.4). We assume $\alpha_i, \beta_i \geq 1$, and we take care of the case with general $\alpha_i, \beta_i \geq 0$ in the proof of Theorem 3.1.1. We first consider the case when $m = 2$ and the implicit constant is 1, and we begin this by establishing bounds for the entries of $\lambda^{-\alpha}(MA)^{\alpha}(MB)^{\beta} := W(\alpha, \beta)$, which allows us to obtain bounds for the Frobenius norm $\|W(\alpha,\beta)\|_F$, where $\|T\|_F = \left(\sum_{i,j} |T_{ij}|^2\right)^{1/2}$ for any matrix T. The bounds we obtain are quickly monotonically decreasing functions of α, so that

$$\|W(\alpha,\beta)\|_F \leq \epsilon(\alpha)\lambda,$$

where ϵ is our bounding function. It is well-known that $\|T\| = \|T\|_2 \leq \|T\|_F$, so in turn we have that $\|W(\alpha,\beta)\|_2 \leq \epsilon(\alpha)\lambda$, which implies that

$$\left\|(MA)^{\alpha}(MB)^{\beta}\right\| \leq \epsilon(\alpha)\lambda^{\alpha+1}.$$

In tandem with the submultiplicativity of $\|\cdot\|$, this allows us to say that

$$\left\| \prod_{i=1}^{2} (MA)^{\alpha_i} (MB)^{\beta_i} \right\| \leq \epsilon(\alpha_2)\epsilon(\alpha_1)\lambda^{\alpha_2+\alpha_1+2} \leq \prod_{i=1}^{2} \epsilon(\alpha_i)\lambda^{\alpha_i+\beta_i},$$

and for sufficiently large α_i, we have that $\epsilon(\alpha_2)\cdot\epsilon(\alpha_1)<1$, thus reducing our problem to the case in which our α_i are bounded by a small constant, which is a tractable problem for a computer check. This is how we establish that

$$\left\|\prod_{i=1}^{2}(MA)^{\alpha_i}(MB)^{\beta_i}\right\| \leq \prod_{i=1}^{2}\lambda^{\alpha_i+\beta_i}.$$

To extend this to (3.23) for all $n\in\mathbb{N}$, we again use submultiplicativity of $\|\cdot\|$ to favorably split the norm of the product over subproducts of the form $\left\|\prod_{i=j}^{j+1}(MA)^{\alpha_i}(MB)^{\beta_i}\right\|$ to get

$$\left\|\prod_{i=1}^{m}(MA)^{\alpha_i}(MB)^{\beta_i}\right\| \leq \left\|\prod_{i=m-(m+1 \bmod 2)}^{m}(MA)^{\alpha_i}(MB)^{\alpha_i}\right\|\cdots\left\|\prod_{i=1}^{2}(MA)^{\alpha_i}(MB)^{\alpha_i}\right\| \ll \prod_{i=1}^{m}\lambda^{\alpha_i+\beta_i}, \tag{3.24}$$

where the left-most product is $\prod_{i=m-1}^{m}(MA)^{\alpha_i}(MB)^{\beta_i}$ if m is even, and $(MA)^{\alpha_i}(MB)^{\beta_i}$ if m is odd. This establishes (3.23).

Lemma 3.2.5. *Let $\alpha,\beta\in\mathbb{N}$ and $W=W(\alpha,\beta)\in\mathbb{Z}^3$ be defined by*

$$\frac{(MA)^{\alpha}(MB)^{\beta}}{\lambda^{\alpha}} = W = [W_{ij}].$$

Then, we have that

$$\begin{aligned}
|W_{11}/\lambda| &\leq 0.210 + (0.936)^{\alpha}(0.755),\\
|W_{21}/\lambda| &\leq 0.462 + (0.936)^{\alpha}(0.509),\\
|W_{31}/\lambda| &\leq 0.278 + (0.936)^{\alpha}(0.328),\\
|W_{12}/\lambda| &\leq 0.131 + (0.936)^{\alpha}(1.352),\\
|W_{22}/\lambda| &\leq 0.288 + (0.936)^{\alpha}(0.910),\\
|W_{32}/\lambda| &\leq 0.174 + (0.936)^{\alpha}(0.586).
\end{aligned} \tag{3.25}$$

Proof. Note that for $\beta\geq 2$, we have $(MB)^{\beta}=\pm(MB)^2$, so we may assume $1\leq\beta\leq 2$ without loss of generality. We find that $(MA)^{\alpha}=PD^{\alpha}P^{-1}$ with

$$\begin{aligned}
P &= \begin{bmatrix} 2-\lambda^2 & 2-\overline{\nu}^2 & 2-\nu^2 \\ -\lambda & -\overline{\nu} & -\nu \\ 1 & 1 & 1 \end{bmatrix},\\
D^{\alpha} &= \left((-1)^{\alpha}\begin{bmatrix} \lambda^{\alpha} & 0 & 0 \\ 0 & \overline{\nu}^{\alpha} & 0 \\ 0 & 0 & \nu^{\alpha} \end{bmatrix}\right),\\
P^{-1} &= \left(\frac{1}{\gamma}\begin{bmatrix} (\nu-\overline{\nu}) & (\overline{\nu}-\nu)(\overline{\nu}+\nu) & (\overline{\nu}-\nu)(2+\overline{\nu}\nu) \\ (\lambda-\nu) & (\nu-\lambda)(\nu+\lambda) & (\nu-\lambda)(2+\nu\lambda) \\ (\overline{\nu}-\lambda) & (\lambda-\overline{\nu})(\lambda+\overline{\nu}) & (\lambda-\overline{\nu})(2+\lambda\overline{\nu}) \end{bmatrix}\right),
\end{aligned} \tag{3.26}$$

where $\lambda = 1.659\cdots$ and $\nu = -1.329\cdots - 0.802\cdots i$ are roots of $x^3 + x^2 - 2x - 4$, and

$$\gamma = (\lambda - \overline{\nu})(\lambda - \nu)(\overline{\nu} - \nu) = \sqrt{-236}.$$

Let

$$\lambda_{3i} = \lambda, \quad \lambda_{3i+1} = \overline{\nu}, \quad \lambda_{3i+2} = \nu \tag{3.27}$$

for all $i \in \mathbb{Z}$. Let T_{ij} denote the ij-th entry of a matrix T where $i, j \geq 1$. Let $\gamma P^{-1} = [p_{ij}]$. We see that

$$\begin{aligned} p_{i1} &= \gamma(P^{-1})_{i1} = \lambda_{i+1} - \lambda_i, \\ p_{i2} &= \gamma(P^{-1})_{i2} = (\lambda_i - \lambda_{i+1})(\lambda_i + \lambda_{i+1}), \\ p_{i3} &= \gamma(P^{-1})_{i3} = (\lambda_i - \lambda_{i+1})(2 + \lambda_i\lambda_{i+1}) \end{aligned} \tag{3.28}$$

for $1 \leq i \leq 3$. Note also that

$$(MB)^\beta = \begin{bmatrix} 0 & -(-1)^\beta & 0 \\ 0 & (-1)^\beta & 0 \\ 2-\beta & \beta - 1 & 0 \end{bmatrix} \tag{3.29}$$

as $1 \leq \beta \leq 2$. We use (3.26), (3.28), and (3.29) to see that

$$(MA)^\alpha (MB)^\beta =$$
$$\frac{(-1)^j}{\gamma} \begin{bmatrix} (2-k)\sum(2\lambda_{i-1}^\alpha - \lambda_{i-1}^{\alpha+2})p_{i3} & \sum(2\lambda_{i-1}^\alpha - \lambda_{i-1}^{\alpha+2})((-1)^\beta(p_{i2} - p_{i1}) + (\beta-1)p_{i3}) & 0 \\ (2-k)\sum -\lambda_{i-1}^{\alpha+1}p_{i3} & \sum -\lambda_{i-1}^{\alpha+1}((-1)^\beta(p_{i2} - p_{i1}) + (\beta-1)p_{i3}) & 0 \\ (2-k)\sum \lambda_{i-1}^\alpha p_{i3} & \sum \lambda_{i-1}^\alpha((-1)^\beta(p_{i2} - p_{i1}) + (\beta-1)p_{i3}) & 0 \end{bmatrix}, \tag{3.30}$$

where all summations are taken over $1 \leq i \leq 3$. Consider the matrix $W = W(\alpha, \beta) \in \mathbb{Z}^{3\times 3}$ defined by

$$\frac{(MA)^\alpha (MB)^\beta}{\lambda^\alpha} = W.$$

We use (3.27) and (3.30) to get that

$$\begin{aligned} |\gamma W_{32}| &= \left| \sum_{i=1}^{3} \left(\frac{\lambda_{i-1}}{\lambda}\right)^\alpha ((-1)^\beta(p_{i2} - p_{i1}) + (\beta-1)p_{i3}) \right| \\ &= \Big| 2\mathrm{Im}(\overline{\nu})((-1)^\beta(2\mathrm{Re}(\nu) + 1) + (\beta-1)(2 + |\nu|^2)) \\ &\quad + 2\mathrm{Im}\left(\left(\frac{\overline{\nu}}{\lambda}\right)^\alpha (\nu - \lambda)((-1)^\beta(\nu + \lambda + 1) + (\beta-1)(2 + \nu\lambda))\right) \Big| \\ &\leq \left|2\mathrm{Im}(\nu)(2\mathrm{Re}(\nu) + |\nu|^2 + 3)\right| + \left| 2\left(\frac{\overline{\nu}}{\lambda}\right)^\alpha (\nu - \lambda)((-1)^\beta(\nu + \lambda + 1) + (\beta-1)(2 + \nu\lambda)) \right|. \end{aligned}$$

We go through the same calculations for the rest of the entries of W and find that

$$
\begin{aligned}
|\gamma W_{11}| &\leq \left|2(2-\lambda^2)\mathrm{Im}(\nu)(2+|\nu|^2)\right| + \left|2\left(\frac{\overline{\nu}}{\lambda}\right)^{\alpha}(2-\overline{\nu}^2)(\nu-\lambda)(2+\nu\lambda)\right|,\\
|\gamma W_{21}| &\leq \left|2\lambda\mathrm{Im}(\nu)(2+|\nu|^2)\right| + \left|2\left(\frac{\overline{\nu}}{\lambda}\right)^{\alpha}\overline{\nu}(\nu-\lambda)(2+\nu\lambda)\right|,\\
|\gamma W_{31}| &\leq \left|2\mathrm{Im}(\nu)(2+|\nu|^2)\right| + \left|2\left(\frac{\overline{\nu}}{\lambda}\right)^{\alpha}(\nu-\lambda)(2+\nu\lambda)\right|,\\
|\gamma W_{12}| &\leq \left|2(2-\lambda^2)\mathrm{Im}(\nu)(2\mathrm{Re}(\nu)+|\nu|^2+3)\right|\\
&\quad + \left|2\left(\frac{\overline{\nu}}{\lambda}\right)^{\alpha}(2-\overline{\nu}^2)(\nu-\lambda)((-1)^{\beta}(\nu+\lambda+1)+(\beta-1)(2+\nu\lambda))\right|,\\
|\gamma W_{22}| &\leq \left|2\lambda\mathrm{Im}(\nu)(2\mathrm{Re}(\nu)+|\nu|^2+3)\right| + \left|2\left(\frac{\overline{\nu}}{\lambda}\right)^{\alpha}\overline{\nu}(\nu-\lambda)((-1)^{\beta}(\nu+\lambda+1)+(\beta-1)(2+\nu\lambda))\right|,\\
|\gamma W_{32}| &\leq \left|2\mathrm{Im}(\nu)(2\mathrm{Re}(\nu)+|\nu|^2+3)\right| + \left|2\left(\frac{\overline{\nu}}{\lambda}\right)^{\alpha}(\nu-\lambda)((-1)^{\beta}(\nu+\lambda+1)+(\beta-1)(2+\nu\lambda))\right|.
\end{aligned}
$$

We focus again on bounding $|\gamma W_{32}|$. Note that when $\beta = 2$, we have

$$|(\nu-\lambda)(\nu+\lambda+1+(2+\nu\lambda))| = 7.460\cdots$$

and when $\beta = 1$, we have

$$|(\nu-\lambda)(\nu+\lambda+1)| = 4.804\cdots$$

With this, we use rational approximations to get

$$\left|2\left(\frac{\overline{\nu}}{\lambda}\right)^{\alpha}(\nu-\lambda)(\nu+\lambda-1+(\beta-1)(\nu\lambda))\right| \leq 2\left|\frac{\nu}{\lambda}\right|^{\alpha}\cdot(7.461) \leq (0.936)^{\alpha}(14.922).$$

Thus, we achieve the bound

$$|\gamma W_{32}| \leq \left|2\mathrm{Im}(\nu)(2\mathrm{Re}(\nu)+|\nu|^2+3)\right| + (0.936)^{\alpha}(14.922) \leq 4.416 + (0.936)^{\alpha}(14.922).$$

Similarly, we get bounds for the rest of the $|\gamma W_{ij}|$ above and divide by $|\gamma|$ and λ to obtain (3.25). □

Lemma 3.2.6. *There exists $\epsilon \in (0,1)$ such that for all $\alpha_n, \beta_n \in \mathbb{N}$, we have*

$$\left\|\prod_{n=1}^{2}(MA)^{\alpha_n}(MB)^{\beta_n}\right\| < \epsilon\prod_{n=1}^{2}\lambda^{\alpha_n+\beta_n}.$$

Proof. Note that for $\beta_n \geq 2$, we have $(MB)^{\beta_n} = \pm(MB)^2$, so we may assume $1 \leq \beta_n \leq 2$ for all $n \in \{1,2\}$ without loss of generality. Fix n and, as in the previous lemma, let

$W = W(\alpha_n, \beta_n) \in \mathbb{Z}^3$ be such that

$$\frac{(MA)^{\alpha_n}(MB)^{\beta_n}}{\lambda^{\alpha_n}} = W = [W_{ij}].$$

We will show that $\|(1/\lambda)W\| \leq 1$ for $\alpha_n \geq 26$ so that

$$\|(MA)^{\alpha_n}(MB)^{\beta_n}\| = \|\lambda^{\alpha_n} W\| \leq \lambda^{\alpha_n+1} \leq \lambda^{\alpha_n+\beta_n}$$

for $\alpha_n \geq 26$, and afterwards we will take care of the other cases. We rely on the Frobenius norm $\|\cdot\|_F$ and make use of the well-known fact that

$$\|W\| \leq \|W\|_F = \left(\sum_{i,j} |W_{ij}|^2\right)^{1/2}.$$

Using Lemma 3.2.5, we find that $\|(1/\lambda)W\|_F = \left(\sum_{i,j}(W_{ij}/\lambda)^2\right)^{1/2} \leq 0.970 < 1$ if $\alpha_n \geq 26$. This gives us that

$$\|(MA)^{\alpha_n}(MB)^{\beta_n}\| = \|\lambda^{\alpha_n} W\| \leq \|\lambda^{\alpha_n} W\|_F \leq 0.970 \cdot \lambda^{\alpha_n+1} \leq 0.970 \cdot \lambda^{\alpha_n+\beta_n}$$

for $\alpha_n \geq 26$ and β_n such that $1 \leq \beta_n \leq 2$. A computation using `numpy` improves this and shows that $\|(MA)^{\alpha_n}(MB)^{\beta_n}\| \leq 0.970 \cdot \lambda^{\alpha_n+\beta_n}$ holds for all α_n, β_n with $2 \leq \alpha_n \leq 25$ and $1 \leq \beta_n \leq 2$ and for $(\alpha_n, \beta_n) = (1, 2)$. The only exception is when $(\alpha_n, \beta_n) = (1, 1)$, where

$$\lambda^2 < \|MAMB\| \leq 1.028\lambda^2.$$

Since $0.970 < \frac{1}{1.028}$, we use the submultiplicativity of $\|\cdot\|$ to get that

$$\left\|\prod_{n=1}^{2}(MA)^{\alpha_n}(MB)^{\beta_n}\right\| \leq 0.998 \prod_{n=1}^{2} \lambda^{\alpha_n+\beta_n} \tag{3.31}$$

when $\alpha_n, \beta_n \geq 1$ and when only one of (α_1, β_1) or (α_2, β_2) is equal to $(1, 1)$. It is readily seen that when $(\alpha_1, \beta_1) = (\alpha_2, \beta_2) = (1, 1)$, we have

$$\left\|(MAMB)^2\right\| = \sqrt{\frac{35 + \sqrt{1097}}{2}} = 5.836\cdots < \lambda^4,$$

and so we conclude that (3.31) holds for all $\alpha_n, \beta_n \geq 1$. □

Remark 3.2.7. *Very similar to our diagonalization of MA are the following diagonalizations of M and AM:*

$$\gamma M = \begin{bmatrix} \lambda & \nu & \overline{\nu} \\ \lambda^2-2 & \nu^2-2 & \overline{\nu}^2-2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \nu & 0 \\ 0 & 0 & \overline{\nu} \end{bmatrix} \begin{bmatrix} (\overline{\nu}-\nu)(\nu+\overline{\nu}) & (\nu-\overline{\nu}) & (\nu-\overline{\nu})(2+\nu\overline{\nu}) \\ (\lambda-\overline{\nu})(\lambda+\overline{\nu}) & (\overline{\nu}-\lambda) & (\overline{\nu}-\lambda)(2+\lambda\overline{\nu}) \\ (\nu-\lambda)(\lambda+\nu) & (\lambda-\nu) & (\lambda-\nu)(2+\lambda\nu) \end{bmatrix},$$

$$\gamma AM = \begin{bmatrix} -\lambda & -\overline{\nu} & -\nu \\ 2-\lambda^2 & 2-\overline{\nu}^2 & 2-\nu^2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} -\lambda & 0 & 0 \\ 0 & -\overline{\nu} & 0 \\ 0 & 0 & -\nu \end{bmatrix} \begin{bmatrix} (\nu-\overline{\nu})(\nu+\overline{\nu}) & (\overline{\nu}-\nu) & (\nu-\overline{\nu})(2+\nu\overline{\nu}) \\ (\lambda-\overline{\nu})(\lambda+\overline{\nu}) & (\overline{\nu}-\lambda) & (\lambda-\overline{\nu})(2+\lambda\overline{\nu}) \\ (\nu-\lambda)(\lambda+\nu) & (\lambda-\nu) & (\nu-\lambda)(2+\lambda\nu) \end{bmatrix}. \tag{3.32}$$

The following lemma justifies the the second inequality in (3.24), which comes from the possibility that m is not divisible by 2, so there may be a factor of $\left\|(MA)^\alpha(MB)^\beta\right\|$ in (3.24).

Lemma 3.2.8. *For $\alpha, \beta \in \mathbb{N} \cup \{0\}$, we have*

$$\left\|(MA)^\alpha(MB)^\beta\right\| \ll \lambda^{\alpha+\beta},$$

where the implicit constant does not depend on α or β.

Proof. Again, note that for $\beta \geq 2$, we have $(MB)^\beta = \pm(MB)^2$, so we may assume $\beta \leq 2$ without loss of generality. Using the diagonalization found for MA in Lemma 3.2.6, we have that $\|(MA)^\alpha\| \ll \lambda^\alpha$ and this result follows immediately. □

We prove (3.23) in the proof of Theorem 3.1.1. Now, we present a lemma that is used solely for proving the lower bound in Theorem 3.1.1. We use the notation $\lfloor x \rfloor$ to denote the *floor* of x, which is the biggest integer less than or equal to x, and $\lceil x \rceil$ to denote the *ceiling* of x, which is the smallest integer greater than or equal to x.

Lemma 3.2.9. *Fix $m \in \mathbb{N}$. If m is odd, then*

$$\left\lfloor \frac{2^{m+1}}{3} \right\rfloor = 2^{m+1} - \left\lceil \frac{2^{m+2}}{3} \right\rceil.$$

Similarly, if m is even, then

$$\left\lceil \frac{2^{m+1}}{3} \right\rceil = 2^{m+1} - \left\lfloor \frac{2^{m+2}}{3} \right\rfloor.$$

Proof. Suppose $m \in \mathbb{N}$ is odd. For $x \in \mathbb{R}$, let $\{x\}$ denote the fractional part of x. Then,

$$\begin{aligned}\left\lfloor \frac{2^{m+1}}{3} \right\rfloor + \left\lceil \frac{2^{m+2}}{3} \right\rceil &= \frac{2^{m+1}}{3} - \left\{ \frac{2^{m+1}}{3} \right\} + \frac{2^{m+2}}{3} + 1 - \left\{ \frac{2^{m+2}}{3} \right\} \\ &= \frac{2^{m+1} + 2^{m+2}}{3} \\ &= 2^{m+1}\end{aligned}$$

and so we are done in this case. The proof of the lemma follows similarly for even m. □

Remark 3.2.10. *For $x \in \mathbb{R}$, let $\{x\}$ denote the fractional part of x, and let*

$$\lfloor x \rceil = \begin{cases} \lfloor x \rfloor, & \{x\} \leq \frac{1}{2}, \\ \lceil x \rceil, & \{x\} > \frac{1}{2} \end{cases}.$$

This is essentially the nearest integer to x but removes ambiguity if $\{x\} = \frac{1}{2}$. In the notation of (3.5) and (3.6), if we pick $k_m = \left\lfloor \frac{2^{m+1}}{3} \right\rceil$, then we have that $k_m \in (3 \cdot 2^{m-2}, 2^m) = S_m^3$. Lemma 3.2.9 tells us that

$$\begin{aligned} k_{m-1} = k'_m &= \left\lfloor \frac{2^m}{3} \right\rceil \in S_{m-1}^3 \\ k_{m-2} = k'_{m-1} &= \left\lfloor \frac{2^{m-1}}{3} \right\rceil \in S_{m-2}^3 \\ &\vdots \\ k_3 = k'_4 &= 5 \in S_3^3 \end{aligned}$$

so that by Lemma 3.2.2 we have

$$v_m = \begin{bmatrix} C_m(k_m) \\ C_m(k'_m) \\ C_{m-1}(k_{m-1}) \end{bmatrix} = (AM)^{m-2} \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}.$$

Obtaining a lower bound on $C_m(\lfloor 2^{m+1}/3 \rceil)$ is how we establish the lower bound in Theorem 3.1.1.

We are now ready to prove the main theorem, which we restate below.

Theorem 3.1.1. *For all $m \in \mathbb{N}$, we have*

$$\lambda^m \ll \max_{k \neq 0} |C_m(k)| \ll \lambda^m,$$

where the implicit constants do not depend on m, and $\lambda = 1.659\cdots$ is the real root of $x^3 + x^2 - 2x - 4$.

Proof. A quick computation shows that $\max_{k\neq 0} |C_m(k)| \neq 0$ for $1 \leq m \leq 2$. Fix $m \geq 3$. First, we focus on the upper bound. For even k, we have that $C_m(k) = 0$ by Lemma 3.2.1. Using the notation in (3.5), fix k_m so that $0 \leq k_m \leq 2^m$ and k_m is odd, and let

$$v_m = \begin{bmatrix} C_m(k_m) \\ C_m(k'_m) \\ C_{m-1}(k_{m-1}) \end{bmatrix}.$$

The idea is to use the fact that

$$|C_m(k_m)| \leq \|v_m\|$$

and, in view of the decomposition given in Lemma 3.2.3, we can bound $\|v_m\|$ by bounding the norm of products of MA and MB using Lemma 3.2.6 and Lemma 3.2.8. By Lemma 3.2.3, we have that

$$v_m = A^{\delta}\left(\prod_{i=3}^{m} MA^{\delta_i}B^{1-\delta_i}\right)\begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$$

where $\delta, \delta_i \in \{0, 1\}$. We see that

$$\left\|A^{\delta}\left(\prod_{i=3}^{m} MA^{\delta_i}B^{1-\delta_i}\right)\begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}\right\| \ll \left\|A^{\delta}\left(\prod_{i=3}^{m} MA^{\delta_i}B^{1-\delta_i}\right)\right\| = \left\|\prod_{i=3}^{m} MA^{\delta_i}B^{1-\delta_i}\right\|.$$

Note that $\|MBv\| \leq \|MAv\|$ for all $v \in \mathbb{R}^3$, so we assume that $\delta_m = 1$ without loss of generality. With this assumption, we have that

$$\prod_{i=3}^{m} MA^{\delta_i}B^{1-\delta_i} = \prod_{i=1}^{n}(MA)^{\alpha_i}(MB)^{\beta_i}$$

where $\alpha_i, \beta_i \in \mathbb{N}\cup\{0\}$ and $\sum_{i=1}^{n}(\alpha_i+\beta_i) = m-3$. We can assume without loss of generality that there is no i such that $\alpha_i = \alpha_{i+1} = 0$ or $\beta_i = \beta_{i+1} = 0$ since that would be redundant, as we could then replace (α_i, β_i) and $(\alpha_{i+1}, \beta_{i+1})$ with $(\alpha_i + \alpha_{i+1}, \beta_i + \beta_{i+1})$. Furthermore, for the same reason, we can assume without loss of generality that there is no i such that $\alpha_i = 0$ and $\beta_{i+1} = 0$. It follows that $\alpha_i, \beta_i \in \mathbb{N}$ for $2 \leq i \leq n-1$. Similarly to how we

justified (3.24), we use Lemma 3.2.8 and Lemma 3.2.6 (in that order) to get that

$$\begin{aligned}\left\|\prod_{i=1}^{n}(MA)^{\alpha_i}(MB)^{\beta_i}\right\| &\leq \left\|(MA)^{\alpha_n}(MB)^{\beta_n}\right\| \cdot \left\|\left(\prod_{i=2}^{n-1}(MA)^{\alpha_i}(MB)^{\beta_i}\right)\right\| \cdot \left\|(MA)^{\alpha_0}(MB)^{\beta_0}\right\| \\ &\ll \lambda^{\alpha_n+\beta_n+\alpha_0+\beta_0}\left\|\left(\prod_{i=2}^{n-1}(MA)^{\alpha_i}(MB)^{\beta_i}\right)\right\| \\ &\leq \prod_{i=1}^{n}\lambda^{\alpha_i+\beta_i} < \lambda^m.\end{aligned}$$

We conclude that

$$|C_m(k_m)| \leq \|v_m\| \ll \left\|\prod_{i=3}^{m} MA^{\delta_i}B^{1-\delta_i}\right\| \ll \left\|\prod_{i=1}^{n}(MA)^{\alpha_i}(MB)^{\beta_i}\right\| \ll \prod_{i=1}^{n}\lambda^{\alpha_i+\beta_i} < \lambda^m,$$

where the implicit constants are independent of m, n. This proves the upper bound.

Now, we concentrate on the lower bound. For this, we use the same idea as Allouche et al. in [4]; namely, we exhibit $C_m(\ell_m)$ for a specific ℓ_m such that $|C_m(\ell_m)| \gg \lambda^m$. Let

$$\ell_m = \left\lfloor \frac{2^{m+1}}{3} \right\rceil$$

where $\lfloor x \rceil$ denotes the nearest integer to x. By Lemma 3.2.2 and Lemma 3.2.9 (see Remark 3.2.10), we have that

$$C_m(\ell_m) = \begin{bmatrix}1 & 0 & 0\end{bmatrix}(AM)^{m-2}\begin{bmatrix}-1\\1\\1\end{bmatrix}.$$

Using this equation and the diagonalization of AM given in (3.32), we find that there exist some $a, b, c \in \mathbb{C}$ so that

$$C(m, \ell_m) = a(-\lambda)^{m-1} + b(-\overline{\nu})^{m-1} + c(-\nu)^{m-1}$$

where $\nu = -1.329\cdots - 0.802\cdots i$ is a root of $x^3 + x^2 - 2x - 4$. Using the diagonalization of AM given in (3.32), we find that

$$a = \frac{-2\mathrm{Re}(\nu)(2\mathrm{Re}(\nu) + |\nu|^2 - 1)}{\gamma} \neq 0.$$

We also have that $C_m(\ell_m) \neq 0$ as ℓ_m is odd. In other words,

$$a(-\lambda)^{m-1} + b(-\overline{\nu})^{m-1} + c(-\nu)^{m-1} = (-\lambda)^{m-1}\left(a + O\left(\left(\frac{\nu}{\lambda}\right)^m\right)\right) \neq 0,$$

so

$$C(m, \ell_m) = |a(-\lambda)^{m-1} + b(-\overline{\nu})^{m-1} + c(-\nu)^{m-1}| \gg \lambda^m. \tag{3.33}$$

This concludes the proof. □

Remark 3.2.11. *In Theorem 2.2 of [32], Høholdt et al. provide relations (3.9)-(3.12) used in our Lemma 3.2.2 for a class of sequences that is more general than the class of Rudin-Shapiro sequences. In particular, they consider the class of sequences* $(a_0, a_1, \ldots, a_{2^m-1})$ *with*

$$\begin{aligned} a_0 &= 1, \\ a_{2^i+j} &= (-1)^{j+f(i)} a^{2^i-j-1}, \qquad 0 \le i \le m-1, \quad 0 \le j \le 2^i - 1 \end{aligned}$$

for all $m \in \mathbb{N}$ *and* $f : \mathbb{N} \to \{0, 1\}$ *being an arbitrary function. This class of sequences is closely related to Welti codes [52, 53]. The Rudin-Shapiro sequences are recovered by choosing* f *so that* $f(0) = f(2k-1) = 0$ *and* $f(2k) = 1$ *for all* $k \in \mathbb{N}$*. Høholdt et al. show the aforementioned relations but the right-hand side of each is multiplied by* $(-1)^{f(m-1)+f(m-2)+1}$ *for general* $f : \mathbb{N} \to \{0, 1\}$*.*

As remarked in the introduction to this chapter, B. Saffari mentioned in a private communication that $P_m(k)$ and $C_m(k)$ behave essentially in the same way. On this topic, we show that Theorem 3.1.1 holds analogously for $P_m(k)$, and we give a useful relation between the periodic and aperiodic autocorrelations.

Theorem 3.2.12. *Using the notation of (3.6), we have for* $m \ge 3$ *and odd* $k \in (0, 2^m)$ *that*

$$P_m(k) = \begin{cases} 0 & k \in S_m^1 \cup S_m^4, \\ 4C_{m-2}(|2^{m-1} - k|) & k \in S_m^2 \cup S_m^3. \end{cases} \tag{3.34}$$

Additionally, for all $m \in \mathbb{N}$*, we have that*

$$\lambda^m \ll \max_{k \neq 0} |P_m(k)| \ll \lambda^m \tag{3.35}$$

where the implicit constants do not depend on m*, and* λ *is the real root of* $x^3 + x^2 - 2x - 4$*.*

Proof. First, we prove (3.34). Since $P_m(k) = C_m(k) + C_m(2^m - k)$, we have the symmetry

$$P_m(k) = P_m(2^m - k) \tag{3.36}$$

for $k \in (0, 2^{m-1})$. Fix $k \in S_m^1$. By (3.9) and (3.12), we have that

$$P_m(k) = C_m(k) + C_m(2^m - k) = C_m(k) - C_m(k) = 0.$$

By symmetry (3.36) of $P_m(k)$, the same holds for $k \in S_m^4$. Now, fix $k \in S_m^2$. We use (3.10) and (3.11) to get that

$$\begin{aligned} P_m(k) &= C_m(k) + C_m(2^m - k) \\ &= \Big(C_{m-1}(2^{m-1} - k) + 2C_{m-2}(2^{m-1} - k)\Big) + \Big(-C_{m-1}(2^{m-1} - k_m) + 2C_{m-2}(2^{m-1} - k)\Big) \\ &= 4C_{m-2}(2^{m-1} - k). \end{aligned}$$

By symmetry (3.36) of $P_m(k)$, the same holds for $k \in S_m^3$. Thus, we have shown (3.34). Now, we will prove (3.35). A quick computation shows that $\max_{k \neq 0} |P_m(k)| \neq 0$ for $1 \leq m \leq 4$. Fix $m \geq 5$. The upper bound of (3.35) follows directly from Theorem 3.1.1. For the lower bound, we use (3.34) and Lemma 3.2.9 to get that

$$P_m\left(\left\lfloor \frac{2^m}{3} \right\rceil\right) = 4C_{m-2}\left(\left\lfloor \frac{2^{m-1}}{3} \right\rceil\right),$$

and by (3.33), we have

$$4C_{m-2}\left(\left\lfloor \frac{2^{m-1}}{3} \right\rceil\right) \gg \lambda^m,$$

so we are done. □

3.3 Connections to Joint Spectral Radius Theory

Let $\|\cdot\|$ be a matrix norm and $\mathcal{T}$ be a bounded set of matrices in $\mathbb{R}^{n \times n}$, so there exists $K \in \mathbb{R}$ such that $\|T\| \leq K$ for all $T \in \mathcal{T}$. For $m \geq 1$, let $\mathcal{M}^m$ denote the set of products of m matrices in $\mathcal{T}$. We define the *joint spectral radius of* $\mathcal{T}$, or $JSR(\mathcal{T})$, by

$$\lim_{m \to \infty} \sup_{\Pi \in \mathcal{M}^m} \|\Pi\|^{1/m}.$$

This limit always exists (see [47] and Lemma 1.2 in [37]) and is independent of the matrix norm chosen by the equivalence of norms in finite-dimensional spaces. The case in which $\mathcal{T}$ consists of a single matrix T, we have Gelfand's formula:

$$\lim_{m \to \infty} \|T^m\|^{1/m} = \rho(T)$$

where $\rho(T)$ denotes the spectral radius of T. The problem of proving Theorem 3.1.1 is slightly harder than that of proving

$$JSR(\{MA, MB\}) = \lambda, \tag{3.37}$$

as we have shown

$$K_1\lambda^m \leq \max_{\Pi\in\{MA,MB\}^m} \|\Pi\| \leq K_2\lambda^m$$

for some $K_1, K_2 > 0$, and taking everything to the power $1/m$ and passing to the limit yields (3.37). Computing the joint spectral radius is in general NP-hard and sometimes incomputable [8, 9]. There are several popular algorithms for approximating and even exactly computing the joint spectral radius in special cases, some of which can be found in [28, 37]. A *branch-and-bound* method of computing $JSR(\mathcal{T})$ is defined to be any method that consists of computing $\sup_{\Pi\in\mathcal{M}^m} \|\Pi\|$ for increasing m, eventually converging to $JSR(\mathcal{T})$. The approach taken in Section 3.2 can be considered a sort of branch-and-bound method of computing $JSR(\{MA, MB\})$, although instead of considering finite products of matrices in $\{MA, MB\}$, we consider finite products of arbitrarily large powers of matrices in $\{MA, MB\}$. Equation (3.37) tells us that

$$JSR(\{MA, MB\}) = \max\{\rho(MA), \rho(MB)\}. \tag{3.38}$$

In other words, the joint spectral radius of $\{MA, MB\}$ is minimal, as

$$\lambda = \lim_{m\to\infty} \|(MA)^m\|^{1/m} = JSR(\{MA\}) \leq JSR(\{MA, MB\}).$$

This minimality property can be asserted for certain families of matrices, such as simultaneously upper triangularizable matrices and normal matrices (see Section 2.3.2 in [37]). To the best of our knowledge, $\{MA, MB\}$ is not in any family of matrices shown to guarantee the property (3.38). So, it is necessary to compute $JSR(\{MA, MB\})$ by other means.

We will give a heuristic proof of (3.37) using the "invariant polytope algorithm" given in Section 2.1 of [28], a simple overview of which can be found Section 2.1 of [29]. To summarize, we need an bounded set of matrices $\mathcal{T}$ that is also *irreducible*, which means that there is no proper subspace of $\mathbb{R}^n$ that is invariant under all matrices in $\mathcal{T}$. Irreducibility is convenient in the context of working with $JSR(\mathcal{T})$ as it implies that $JSR(\mathcal{T}) > 0$ and that $\mathcal{T}$ is nondefective, i.e. there exists $K > 0$ such that for all m, we have

$$\sup\{\|\Pi\| : \Pi \in \mathcal{M}^m\} \leq K \cdot JSR(\mathcal{T})^m,$$

or equivalently that $\mathcal{T}$ admits an extremal norm, i.e. a vector norm $|\cdot|$ such that for all $x \in \mathbb{R}^n$ and $T \in \mathcal{T}$, we have

$$|Tx| \leq JSR(\mathcal{T})|x|.$$

On these topics, we refer the reader to [37, 54]. The extremal norm is a crucial object for this algorithm.

Continuing with the explanation of the invariant polytope algorithm, we choose a suitable matrix $T \in \mathcal{M}^m \subset \mathcal{T}$ as a candidate for a *spectrum-maximizing product*, which generally

speaking is a matrix $\Pi \in \mathcal{M}^m$ such that

$$(\rho(\Pi))^{1/m} = JSR(\mathcal{T}).$$

If we can construct a polytope $\mathcal{P} \subset \mathbb{R}^n$ such that $\mathcal{P}$ is invariant under $(\rho(T))^{-1/m}\ \mathcal{T}$, i.e.,

$$\bigcup_{T' \in \mathcal{T}} T'\mathcal{P} \subset (\rho(T))^{1/m}\ \mathcal{P},$$

which we do through the iterative process outlined in [29], then this unit ball corresponds to the extremal norm associated with $\mathcal{T}$ and so T is indeed a spectrum-maximizing product.

In our case in which $\mathcal{T} = \{MA, MB\}$, we first show that $\{MA, MB\}$ is an irreducible set of matrices. Note first that the eigenspaces of MA differ entirely from those of MB, so we consider only 2-dimensional subspaces. We suppose for contradiction that V is such a 2-dimensional subspace. Of course, we must have that $(MB)^2V \subset V$. We see that

$$(MB)^2 = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

and

$$\ker\ (MB)^2 = \text{span}\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}, \quad \text{image}\ (MB)^2 = \text{span}\left\{ \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \right\}.$$

We cannot have that $V = \ker\ (MB)^2$ because $\begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^T \in \ker(MB)^2$, but $MA \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 2 & 2 & 0 \end{bmatrix}^T \notin \ker(MB)^2$. So, we must have that V contains a vector that is not sent to 0 by $(MB)^2$. Since $(MB)^2V \subset V$, we have $V \cap \text{image}\ (MB)^2 \neq \{0\}$, so

$$\text{span}\left\{ \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \right\} \subset V.$$

However, since

$$\left\{ (MA)^j \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} : 1 \leq j \leq 3 \right\} = \left\{ \begin{bmatrix} 1 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 9 \\ 3 \\ 1 \end{bmatrix} \right\}$$

is a linearly independent set and $(MA)^jV \subset V$ for all $j \geq 1$, we get that V is of dimension 3. This is a contradiction as we assumed that V is of dimension 2, so there is no proper subspace of $\mathbb{R}^3$ that is invariant under both MA and MB and $\{MA, MB\}$ is irreducible by definition. We now choose MA as a candidate for a spectrum-maximizing product. Using `ConvexHull` in the `SciPy` library for `Python`, we employ the aforementioned iterative

process in [29], and find that the invariant polytope algorithm halts in 8 steps, after which we have found a polytope $\mathcal{P}$ with 30 vertices such that

$$(MA)\mathcal{P} \cup (MB)\mathcal{P} \subset \lambda\mathcal{P}. \tag{3.39}$$

Of course, this is not a formal proof, and it is also possible that this output was due to numerical imprecision. The polytope $\mathcal{P}$ in (3.39) would be the unit ball of an extremal norm associated with $\{MA, MB\}$. If (3.39) is true, it would tell us that MA is indeed a spectrum-maximizing product, which would prove (3.37). Going through 8 steps of this algorithm requires consideration of about the same number of cases as our method, being bounded above by $2^8 = 256$. We believe our method to be useful for computation of the JSR for sets of matrices consisting mostly of matrices T with $\{T, T^2, T^3, \dots\}$ being finite. However, as our method was created around attacking Theorem 3.1.1, we have no evidence of its ability to compute joint spectral radii in general, unlike the algorithm in [28]. It is purely luck that the product of $(MA)^{\alpha_n}(MB)^{\beta_n}$ in Lemma 3.2.6 did not exceed a length of 2.

Chapter 4

Further study of Rudin-Shapiro sequence autocorrelations

Code for several of the computations in this chapter is given in Appendix A. The results of this chapter come from ongoing joint work with Stephen Choi [22].

4.1 Introduction

4.1.1 Notation

Here, we list all potentially ambiguous notation used in this chapter:

(i) For functions f and g from $\mathbb{C} \to \mathbb{C}$, we write

$$f(x) \ll g(x)$$

for $x \in S$ (where S is some subset of $\mathbb{R}$) if and only if there exists an absolute constant $K > 0$ such that

$$|f(x)| \leq K|g(x)|$$

for all $x \in S$.

(ii) For functions f and g from $\mathbb{C} \to \mathbb{C}$, we write

$$f(x) \asymp g(x)$$

for $x \in S \subset \mathbb{R}$ if and only if

$$g(x) \ll f(x) \ll g(x)$$

for all $x \in S$. That is, there exist absolute constants $K_1, K_2 > 0$ such that

$$K_1|g(x)| \leq |f(x)| \leq K_2|g(x)|$$

for all $x \in S$.

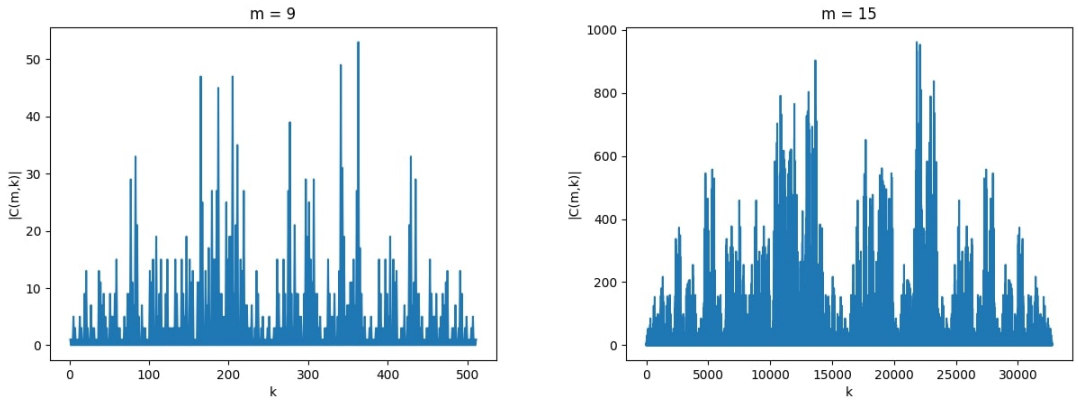
(iii) For a ring R, we define $R^{n\times n}$ to be the n-by-n matrices with entries in R.

(iv) For a ring R and matrices $M_j, M_{j+1}, \cdots, M_k \in R^{n\times n}$, we use the convention

$$\prod_{i=j}^{k} M_i := M_k M_{k-1} \cdots M_j.$$

4.1.2 Overview

In the previous chapter, we proved Theorem 3.1.1, which gives us the asymptotic order of growth of $\max_{k\neq 0} |C_m(k)|$, where the maximum is taken over all k such that $1 \leq k \leq 2^m - 1$. This result by itself does not tell us much about the $|C_m(k)|$ as a function of k. We note that $|C_m(k)|$ generally increases as k increases from $k = 1$ to a local maximum at $k \approx \frac{2^{m+1}}{3}$ as we can see in the following graphs:



This is especially interesting because autocorrelations of binary sequences at small shifts are likely to be greater in absolute value than those at large shifts, the worst case being $n - k$ at shift k, where n is the length of the binary sequence. This is because there are more terms summed for autocorrelations at small shifts. Thus, one would expect that the absolute values of autocorrelations of a binary sequence would be decreasing as shifts get larger. To capture this vaguely increasing behavior of $|C_m(k)|$ on the interval $(0, 2^{m+1}/3)$, we consider instead the partial maxima $\max_{0<k\leq x} |C_m(k)|$ for $x \in (0, 2^m) \subset \mathbb{R}$. In the next section, we prove the following extension of Theorem 3.1.1.

Theorem 4.3.2. We have

$$\max_{0<k\leq x} |C_m(k)| \asymp x^{\log_2(\lambda)}$$

for all $x \in [1, 2^m]$, where the implicit constants do not depend on m.

Littlewood, in [36], and Høholdt et al., in [32], show that

$$\sum_{k=1}^{2^m-1} C_m(k)^2 = \frac{4^m - (-2)^m}{6}.$$

We extend this result to

Theorem 4.3.6. *We have that*

$$\sum_{0<k\leq x} C_m(k)^2 \asymp x^2$$

for all $x \in [1, 2^m]$*, where the implicit constants do not depend on* m*.*

We use our improved bounds on $C_m(k)$ and relevant sums to obtain bounds on $\sum_k |C_m(k)|$, which we do not believe has seen much attention in the literature. In particular, we show

Theorem 4.3.7. *We have that*

$$x^{\log_2(4/\lambda)} \ll \sum_{0<k\leq x} |C_m(k)| \ll x^{3/2}$$

for all $x \in [1, 2^m]$*, where the implicit constants do not depend on* m *and* $\log_2(4/\lambda) \approx 1.269$*.*

We are led to pose the following conjecture, for which we provide evidence at the end of Section 4.2.

Conjecture 4.1.1. *We have* $\sum_k |C_m(k)| \asymp x^{2\log_2(\lambda+\epsilon)}$ *where* $\epsilon \in [0, 0.008]$*.*

We also provide analogous bounds for $P_m(k)$ and relevant sums as follows.

Theorem 4.3.9. *We have that*

(i) $\max_{0<k\leq x} |P_m(k)| \asymp (x - 2^{m-2})^{\log_2(\lambda)}$,

(ii) $\sum_{0<k\leq x} P_m(k)^2 \asymp (x - 2^{m-2})^2$,

(iii) $(x - 2^{m-2})^{\log_2(4/\lambda)} \ll \sum_{0<k\leq x} |P_m(k)| \ll (x - 2^{m-2})^{3/2}$

for all $x \in [2^{m-2} + 1, 2^m]$*, where the implicit constants do not depend on* m*.*

In Section 4.3, we concern ourselves with which k gives the maximal $C_m(k)$. Fix m and suppose that $k = k_m^*$ gives maximal $C_m(k)$.

Conjecture 4.1.2. *We have that k_m^* is unique for each m and* $\lim_{m\to\infty} \frac{3k_m^*}{2^{m+1}} = 1$.

In other words, the k that gives maximal autocorrelation of the m-th Rudin-Shapiro sequence is asymptotically $2/3$ the length of the m-th Rudin-Shapiro sequence. Let $\ell_m = \left\lfloor \frac{2^{m+1}}{3} \right\rceil$ where $\lfloor x \rceil$ denotes the nearest integer to x. We find that k_m^* is unique for each $3 \leq m \leq 16$ and that:

m	$\lvert k_m^* - \ell_m \rvert$	k_m^*/ℓ_m
3	2	0.6
4	0	1
5	8	0.619...
6	0	1
7	34	0.6
8	2	1.011...
9	22	1.064...
10	8	1.011...
11	0	1
12	34	1.012...
13	86	1.015...
14	136	1.012...
15	18	0.999...
16	0	1

Note that for $m = 4, 6, 11, 16, \ldots$ we have $k_m^* = \ell_m$. That leads us to pose the following question.

Question. Assuming that k_m^* is unique for each m, do there exist infinitely many integers m such that $k_m^* = \ell_m$?

We provide evidence for Conjecture 4.1.2 by way of constructing $f : [0,1] \to [0,1]$, a continuous analogue of $C_m(k)$ for which $\lim_{m\to\infty} \frac{|C_m(\lfloor x2^m \rceil)|}{\lambda^{m-2}} = f(x)$, and we find that $f(x) < f(2/3)$ for all $x \neq 2/3$.

Throughout this chapter, we refer to the recurrence relations given for $C_m(k)$ at the beginning of Section 3.2, namely

$$C_m(k_m) = \quad C_{m-1}(2^{m-1} - k_m) \qquad \text{if } k_m \in S_m^1, \tag{4.7}$$

$$C_m(k_m) = \quad C_{m-1}(2^{m-1} - k_m) + 2C_{m-2}(2^{m-1} - k_m) \qquad \text{if } k_m \in S_m^2, \tag{4.8}$$

$$C_m(k_m) = -C_{m-1}(k_m - 2^{m-1}) + 2C_{m-2}(k_m - 2^{m-1}) \qquad \text{if } k_m \in S_m^3, \tag{4.9}$$

$$C_m(k_m) = -C_{m-1}(k_m - 2^{m-1}) \qquad \text{if } k_m \in S_m^4, \tag{4.10}$$

along with the matrices

$$M = \begin{bmatrix} 0 & 1 & 2 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

4.2 Basic symmetries

Here, we explore some symmetries in $C_m(k)$, the former of which we use in Section 4.3 and also to prove the latter.

Lemma 4.2.1. *For all $m \geq 3$ and odd k with $0 < k < 2^{m-2}$, we have*

$$C_m(k) = -C_m(2^m - k).$$

Proof. For k odd with $0 < k < 2^{m-2}$, we have by (3.9) and (3.12) that

$$\begin{aligned} C_m(k) &= C_{m-1}(2^{m-1} - k), \\ C_m(2^m - k) &= -C_{m-1}(2^m - k - 2^{m-1}) = -C_{m-1}(2^{m-1} - k), \end{aligned}$$

so we are done. □

Lemma 4.2.2. *For all $m \geq 5$ and odd k with $0 < k < 2^{m-4}$, we have*

$$C_m(2^{m-2} + k) = C_m(2^{m-2} - k).$$

Proof. Fix k odd with $0 < k < 2^{m-4}$. We see that (3.9) and (3.11) imply

$$\begin{aligned} C_m(2^{m-2} - k) &= C_{m-1}(2^{m-1} - (2^{m-2} - k)) \\ &= C_{m-1}(2^{m-2} + k) \\ &= -C_{m-2}(k) + 2C_{m-3}(k). \end{aligned}$$

By (3.10), we have

$$C_m(2^{m-2} + k) = C_{m-1}(2^{m-2} - k) + 2C_{m-2}(2^{m-2} - k),$$

where, again by (3.10), we have

$$C_{m-1}(2^{m-2} - k) = C_{m-2}(k) + 2C_{m-3}(k).$$

Using these relations, we find that $C_m(2^{m-2} + k) = C_m(2^{m-2} - k)$ is equivalent to

$$C_{m-2}(k) + 2C_{m-3}(k) + 2C_{m-2}(2^{m-2} - k) = -C_{m-2}(k) + 2C_{m-3}(k)$$

which holds if and only if

$$C_{m-2}(2^{m-2} - k) = -C_{m-2}(k)$$

which is true by Lemma 4.2.1. □

Now the only $C_m(k)$ to study are those with $k \in (0, 2^{m-2}) \cup (5 \cdot 2^{m-4}, 3 \cdot 2^{m-2})$.

4.3 Moments of $C_m(k)$

Define

$$\begin{aligned}
\mu_m(x) &= \max_{0<k\leq x} |C_m(k)|, \\
\sigma_m(x) &= \sum_{0<k\leq x} |C_m(k)|, \\
\Lambda_m(x) &= \sum_{0<k\leq x} C_m(k)^2.
\end{aligned}$$

For legibility we denote

$$\mu_m(2^m) = \mu_m$$

and similarly for σ and Λ – these can be thought of as the ℓ^∞, ℓ^1, and ℓ^2 moments of $C_m(k)$, respectively. In this section, we establish asymptotic bounds for μ_m, σ_m, and Λ_m and the analogous functions for $P_m(k)$. Throughout this section, the implicit constants arising in the proofs are absolute.

We begin with a short technical lemma that extends the idea in Remark 3.2.10.

Theorem 4.3.1. *For all m, we have that*

$$|C_m(\lfloor 2^n/3 \rceil)| \asymp \lambda^n$$

for all $1 \leq n \leq m$, where the implicit constants do not depend on n or m.

Proof. It suffices to consider $m \geq 3$. It suffices to consider $3 \leq n \leq m$. Fix $k_m = \lfloor 2^n/3 \rceil$. By (3.5), we have $k_n \in S_n^2 = (2^{n-2}, 2^{n-1})$ as in (3.6) and

$$k_m = k_{m-1} = \cdots = k_{n+1} \in S_{n+1}^1$$

and by the fact that

$$\left\lfloor \frac{2^q}{3} \right\rceil = 2^q - \left\lfloor \frac{2^{q+1}}{3} \right\rceil$$

for all $q \in \mathbb{N}$, we have that

$$k_j \in S_j^3$$

for all $3 \leq j < n$ as in Remark 3.2.10. So, by (3.13), we use the notation of (3.7) to get that

$$\begin{aligned} v_m(k_m) &= (MB)^{m-n} v_n \\ &= (MB)^{m-n} M (AM)^{n-3} v_2. \end{aligned} \tag{4.1}$$

Note that

$$(MB)^j = \pm (MB)^2 = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{4.2}$$

for all $j \geq 2$, so

$$C_m(k_m) = \pm C_n(k_n')$$

by (3.7) and the first line of (4.1). Thus, by Theorem 3.1.1, we get that $|C(m, k_m)| \ll \lambda^n$. Now, we consider the second line of (4.1). The fact that $\lambda^n \ll |C(m, k_m)|$ follows from (4.2) and the fact that AM is diagonalizable and has spectral radius λ. Recall that $k_m = \lfloor 2^n/3 \rceil$, so we are done. □

Now, we are equipped to extend Theorem 3.1.1 so that it addresses the order of the maximal $|C_m(k)|$ over all k up to x for any $x \in [1, 2^m]$, rather than just $x = 2^m$.

Theorem 4.3.2. *We have*

$$\mu_m(x) = \max_{0 < k \leq x} |C_m(k)| \asymp x^{\log_2(\lambda)}$$

for all $x \in [1, 2^m]$, where the implicit constants do not depend on m.

Proof. Fix m sufficiently large. By Lemma 4.3.1 and Theorem 3.1.1, we have that

$$\mu_m(2^m) \asymp \lambda^m.$$

Now, fix $x = 2^j$ for any $0 \leq j \leq m-1$ and fix $k_m \leq 2^j$ odd. By (3.5), we have

$$k_m = k_{m-1} = \cdots = k_{j+2} \in S^1_{j+2},$$

so by (3.13), we have

$$v_m = (MB)^{m-j-1} v_{j+1},$$

and note that $(MB)^m = \pm (MB)^2$ for $m \geq 2$. This, in conjunction with the definition of v_{j+1} and Theorem 3.1.1, gets us that

$$\mu_m(2^j) \ll \lambda^j. \tag{4.3}$$

By Lemma 4.3.1, we have

$$\lambda^j \ll \mu_m(2^j).$$

Thus, we have proven the theorem for $x = 2^j$ with $0 \leq j \leq m$. To fill the gaps, take $\rho \in [1, 2]$. We use (4.3) to get that

$$\frac{\mu_m(\rho x)}{(\rho x)^{\log_2(\lambda)}} \asymp \frac{\lambda}{\rho^{\log_2(\lambda)}} \frac{\mu_m(x)}{x^{\log_2(\lambda)}}.$$

Since $\frac{\lambda}{\rho^{\log_2(\lambda)}}$ is bounded, we are done. □

We extend the following result of Littlewood and Høholdt et al. on $\sum_{k \neq 0} C_m(k)^2$ in much the same way as the prior theorem, so that it deals with partial sums of $C_m(k)^2$.

Theorem 4.3.3. *For all $m \geq 1$, we have*

$$\Lambda_m = \sum_{0 < k \leq 2^m} C_m(k)^2 = \frac{4^m - (-2)^m}{6}.$$

Proof. This can be found in a different form in [36] (see Theorem 1 in [11]). A simple proof is given in the proof of Theorem 2.3 in [32]. □

When computing $\sum_{0 < k \leq x} C_m(k)^2$, we do not have the same cancellation as when computing the full sum $\sum_k C_m(k)^2$. What follows are a couple of lemmas that compensate for lack of easy cancellation.

Lemma 4.3.4. *For all $m \geq 1$, we have*

$$\sum_{k=1}^{2^m} C_m(2^m - k) C_m(k) = (-2)^{m-1}.$$

Proof. A quick check verifies the claim for $m = 1, 2$. Fix $m \geq 3$. We use Lemma 4.2.1 to get

$$\sum_{k=1}^{2^m} C_m(2^m - k) C_m(k) = -2 \sum_{k=1}^{2^{m-2}} C_m(k)^2 + 2 \sum_{k=2^{m-2}}^{2^{m-1}} C_m(2^m - k) C_m(k). \tag{4.4}$$

From (3.9), we have

$$\sum_{k=1}^{2^{m-2}} C_m(k)^2 = \sum_{k=1}^{2^{m-2}} (C_{m-1}(2^{m-1} - k))^2. \tag{4.5}$$

From (3.10) and (3.11), we have

$$\begin{aligned}\sum_{k=2^{m-2}}^{2^{m-1}} C_m(2^m-k)C_m(k) &= \sum_{k=2^{m-2}}^{2^{m-1}} \left(-C_{m-1}(2^{m-1}-k)+2C_{m-2}(2^{m-1}-k)\right)\\ &\quad\cdot\left(C_{m-1}(2^{m-1}-k)+2C_{m-2}(2^{m-1}-k)\right)\\ &= \sum_{k=2^{m-2}}^{2^{m-1}} \left(-(C_{m-1}(2^{m-1}-k))^2+4(C_{m-2}(2^{m-1}-k))^2\right)\\ &= \sum_{k=1}^{2^{m-2}} \left(-(C_{m-1}(k))^2+4(C_{m-2}(k))^2\right).\end{aligned} \tag{4.6}$$

Using (4.4), (4.5), (4.6), and Theorem 4.3.3, we conclude that

$$\sum_{k=1}^{2^m} C_m(2^m-k)C_m(k) = -2\Lambda_{m-1}+8\Lambda_{m-2} = (-2)^{m-1}.$$

□

Lemma 4.3.5. *Fix $m \geq 2$. We have that*

$$\sum_{k=1}^{2^{m-1}} C_m(k)C_{m-1}(k) = \begin{cases} 2^{m-2} & m \text{ is even,}\\ -2^{m-1} & m \text{ is odd.}\end{cases}$$

Proof. A quick check verifies the claim for $m = 2, 3$. Suppose $m \geq 4$. Using (3.9), (3.10), and Lemma 4.3.4, we see that

$$\begin{aligned}\sum_{k=1}^{2^{m-1}} C_m(k)C_{m-1}(k) &= \sum_{k=1}^{2^{m-2}} C_{m-1}(2^{m-1}-k)C_{m-1}(k)\\ &\quad+\sum_{k=2^{m-2}}^{2^{m-1}} \left(C_{m-1}(2^{m-1}-k)+2C_{m-2}(2^{m-1}-k)\right)C_{m-1}(k)\\ &= \sum_{k=1}^{2^{m-1}} C_{m-1}(2^{m-1}-k)C_{m-1}(k)+2\sum_{k=2^{m-2}}^{2^{m-1}} C_{m-1}(k)C_{m-2}(2^{m-1}-k)\\ &= (-2)^{m-2}+2\sum_{k=2^{m-2}}^{2^{m-1}} C_{m-1}(k)C_{m-2}(2^{m-1}-k).\end{aligned} \tag{4.7}$$

Similarly, using (3.11), (3.12), and Lemma 4.3.4, we see that

$$\begin{aligned}\sum_{k=2^{m-2}}^{2^{m-1}} C_{m-1}(k)C_{m-2}(2^{m-1}-k) &= -\sum_{k=1}^{2^{m-2}} C_{m-2}(2^{m-2}-k)C_{m-2}(k) + 2\sum_{k=1}^{2^{m-3}} C_{m-2}(2^{m-2}-k)C_{m-3}(k) \\ &= -(-2)^{m-3} + 2\sum_{k=2^{m-3}}^{2^{m-2}} C_{m-2}(k)C_{m-3}(2^{m-2}-k).\end{aligned} \tag{4.8}$$

Note that

$$\sum_{k=2^2}^{2^3} C_3(k)C_2(2^3-k) = 0. \tag{4.9}$$

Using (4.8) inductively on (4.7) with (4.9) as the base case yields

$$\sum_{k=1}^{2^{m-1}} C_m(k)C_{m-1}(k) = (-2)^{m-2} - \sum_{j=1}^{m-4}(-1)^{j+1}2^{m-2}, \tag{4.10}$$

which simplifies to

$$\sum_{k=1}^{2^{m-1}} C_m(k)C_{m-1}(k) = \begin{cases}(-2)^{m-2} & m \text{ is even},\\ -(-2)^{m-1} & m \text{ is odd},\end{cases} = \begin{cases}2^{m-2} & m \text{ is even},\\ -2^{m-1} & m \text{ is odd}.\end{cases}$$

as desired. □

We now prove the extension of Theorem 4.3.3.

Theorem 4.3.6. *We have*

$$\Lambda_m(x) = \sum_{0<k\le x} C_m(k)^2 \asymp x^2$$

for all $x \in [1, 2^m]$. *In particular, for all* $m \ge 4$, *we have that*

$$\Lambda_m(2^j) = \begin{cases}\frac{2\cdot 4^j - 5\cdot 2^j}{6} & \text{if } j \text{ is even},\\ \\ \frac{2\cdot 4^j + 11\cdot 2^j}{6} & \text{if } j \text{ is odd},\end{cases} \tag{4.11}$$

for $4 \le j \le m-2$, *and*

$$\Lambda_m(2^{m-1}) = \begin{cases}\frac{2\cdot 4^{m-1} - 13\cdot 2^{m-1}}{6} & \text{if } m \text{ is even},\\ \\ \frac{2\cdot 4^{m-1} + 7\cdot 2^{m-1}}{6} & \text{if } m \text{ is odd}.\end{cases} \tag{4.12}$$

Proof. As in Theorem 4.3.2, it is sufficient to show (4.11) and (4.12), as that implies

$$\sum_{k=1}^{2^j} C_m(k)^2 \asymp 4^j$$

for all $m \geq 4$ and $4 \leq j \leq m-1$. The case $j = m$ is settled by Theorem 4.3.3. Let $m \geq 4$ and suppose $4 \leq j \leq m-2$. If $1 \leq k \leq 2^j$, then $k \in S_m^1$. Using (3.9), we get that

$$\sum_{k=1}^{2^j} C_m(k)^2 = \sum_{k=1}^{2^j} (C_{m-1}(2^{m-1}-k))^2.$$

If $j \leq m-3$, then for any odd $1 \leq k \leq 2^j - 1$, we have $2^{m-1} - k \in S_{m-1}^4$. Using (3.12), we get that

$$\sum_{k=1}^{2^j} C_m(k)^2 = \sum_{k=1}^{2^j} (C_{m-1}(2^{m-1}-k))^2 = \sum_{k=1}^{2^j} (C_{m-2}(2^{m-2}-k))^2.$$

Hence, using (3.12) repeatedly, we get

$$\sum_{k=1}^{2^j} C_m(k)^2 = \sum_{k=1}^{2^j} (C_{j+1}(2^{j+1}-k))^2 = \sum_{k=1}^{2^{j-1}} (C_{j+1}(2^{j+1}-k))^2 + \sum_{k=2^{j-1}+1}^{2^j} (C_{j+1}(2^{j+1}-k))^2.$$

For odd $1 \leq k \leq 2^{j-1}$, we have $2^{j+1} - k \in S_{j+1}^4$ and so by (3.12), we have

$$\sum_{k=1}^{2^{j-1}} (C_{j+1}(2^{j+1}-k))^2 = \sum_{k=1}^{2^{j-1}} (C_j(2^j-k))^2.$$

For odd $2^{j-1}+1 \leq k \leq 2^j$, we have $2^{j+1} - k \in S_{j+1}^3$ and so by (3.11), we have

$$\begin{aligned}
&\sum_{k=2^{j-1}+1}^{2^j} (C_{j+1}(2^{j+1}-k))^2 \\
= &\sum_{k=2^{j-1}+1}^{2^j} \Big(-C_j(2^j-k) + 2C_{j-1}(2^j-k)\Big)^2 \\
= &\sum_{k=2^{j-1}+1}^{2^j} C_j(2^j-k)^2 - 4\sum_{k=2^{j-1}+1}^{2^j} C_j(2^j-k)C_{j-1}(2^j-k) + 4\sum_{k=2^{j-1}+1}^{2^j} C_{j-1}(2^j-k)^2 \\
= &\sum_{k=2^{j-1}+1}^{2^j} C_j(2^j-k)^2 - 4\sum_{k=1}^{2^{j-1}} C_j(k)C_{j-1}(k) + 4\sum_{k=1}^{2^{j-1}} C_{j-1}(k)^2.
\end{aligned}$$

Therefore, for $4 \le j \le m-2$, we have

$$\begin{aligned}\sum_{k=1}^{2^j} C_m(k)^2 &= \sum_{k=1}^{2^j} (C_j(2^j-k))^2 - 4\sum_{k=1}^{2^{j-1}} C_j(k)C_{j-1}(k) + 4\sum_{k=1}^{2^{j-1}} C_{j-1}(k)^2 \\ &= \Lambda_j + 4\Lambda_{j-1} - 4\sum_{k=1}^{2^{j-1}} C_j(k)C_{j-1}(k). \end{aligned} \tag{4.13}$$

If j is even, then by Theorem 4.3.3 and Lemma 4.3.5, we have

$$\sum_{k=1}^{2^j} C_m(k)^2 = \frac{4^j - 2^j}{6} + 4\left(\frac{4^{j-1}+2^{j-1}}{6}\right) - 4(2^{j-2}) = \frac{2\cdot 4^j - 5\cdot 2^j}{6}.$$

Similarly, if j is odd, we have

$$\sum_{k=1}^{2^j} C_m(k)^2 = \frac{4^j + 2^j}{6} + 4\left(\frac{4^{j-1}-2^{j-1}}{6}\right) + 4(2^{j-1}) = \frac{2\cdot 4^j + 11\cdot 2^j}{6}.$$

This proves (4.11) .

For $j = m-1$, it can be proved similarly that

$$\sum_{k=1}^{2^{m-1}} C_m(k)^2 = \Lambda_{m-1} + 4\Lambda_{m-1} + 4\sum_{k=1}^{2^{m-2}} C_{m-1}(k)C_{m-2}(k).$$

Hence by Theorem 4.3.3 and Lemma 4.3.5 again, we have

$$\sum_{k=1}^{2^{m-1}} C_m(k)^2 = \begin{cases} \frac{2\cdot 4^j - 13\cdot 2^j}{6} & \text{if } m \text{ is even,} \\ \frac{2\cdot 4^j + 7\cdot 2^j}{6} & \text{if } m \text{ is odd.} \end{cases}$$

This proves (4.12). □

We are not aware of any literature concerned with computing $\sum_k |C_m(k)|$ or any partial sums thereof. We may use our work in this section to obtain decent bounds for $\sum_k |C_m(k)|$ as we show in the following theorem.

Theorem 4.3.7. *We have that*

$$x^{\log_2(4/\lambda)} \ll \sigma_m(x) = \sum_{0<k\le x} |C_m(k)| \ll x^{3/2}$$

for all $x \in [1, 2^m]$, *where the implicit constants do not depend on* m, *and* $\log_2(4/\lambda) \approx 1.269$.

Proof. Again, it is sufficient to show the claim for $x \in \{2^j : 0 \le j \le m\}$. It is immediate from Theorem 4.3.6 and Cauchy-Schwarz that

$$\sigma_m(2^j) \le 2^{j/2}\sqrt{\Lambda_m(2^j)} \ll 2^{3j/2}.$$

Using Theorem 4.3.2 and Theorem 4.3.6, we also get the lower bound

$$\left(\frac{4}{\lambda}\right)^j \ll \frac{\Lambda_m(2^j)}{\mu_m(2^j)} \le \sigma_m(2^j).$$

This concludes the proof. □

Corollary 4.3.8. *We have that*

$$\left(\frac{4}{\lambda}\right)^m \ll \sum_{k\neq 0} |C_m(k)| \ll (2^{3/2})^m$$

where the implicit constants do not depend on m.

We follow with the analogous results for $P_m(k)$.

Theorem 4.3.9. *We have that*

(i) $\max_{0<k\le x} |P_m(k)| \asymp (x - 2^{m-2})^{\log_2(\lambda)}$,

(ii) $\displaystyle\sum_{0<k\le x} P_m(k)^2 \asymp (x - 2^{m-2})^2$,

(iii) $(x - 2^{m-2})^{\log_2(4/\lambda)} \ll \displaystyle\sum_{0<k\le x} |P_m(k)| \ll (x - 2^{m-2})^{3/2}$

for all $x \in [2^{m-2} + 1, 2^m]$, where the implicit constants do not depend on m.

Proof. This follows from Theorem 4.3.2, Theorem 4.3.6, Theorem 4.3.7, and Theorem 3.2.12. □

We would like to determine the exact order of $\sigma_m(x) = \displaystyle\sum_{0<k\le x} |C_m(k)|$ as we have for $\mu_m(x)$ and $\lambda_m(x)$. Let

$$r_k = \frac{\sigma_m(k)}{k^{2\log_2(\lambda)}}.$$

We will show that r_k is likely to be absolutely bounded, which would imply that $\sigma_m(k) \asymp k^{2\log_2(\lambda)}$. If this is true, then $\log(\sigma_m(2^m))/m$ should converge to $2\log_2(\lambda)$, but we do not focus on this logarithm because the convergence is too slow, and we are unable to obtain convincing evidence for $m \le 19$. We observe these ratios between $\sigma_m(x)$ and $x^{2\log_2(\lambda)}$ in the following table. We would like the maximum and minimum ratios be bounded by absolute, positive constants.

m	$\min_{k\neq 0} r_k$	$\arg\min_{k\neq 0} r_k$
3	$0.3498\ldots$	2^3-1
4	$0.2332\ldots$	2^3-1
5	$0.2918\ldots$	2^4-1
6	$0.2684\ldots$	2^5-1
7	$0.2723\ldots$	2^6-1
8	$0.2578\ldots$	2^7-1
9	$0.2568\ldots$	2^8-1
10	$0.2549\ldots$	2^9-1
11	$0.2541\ldots$	$2^{10}-1$
12	$0.2512\ldots$	$2^{11}-1$
13	$0.2481\ldots$	$2^{12}-1$
14	$0.2460\ldots$	$2^{13}-1$
15	$0.2438\ldots$	$2^{14}-1$
16	$0.2416\ldots$	$2^{15}-1$
17	$0.2394\ldots$	$2^{16}-1$
18	$0.2371\ldots$	$2^{17}-1$
19	$0.2350\ldots$	$2^{18}-1$

The values of $\max_{k\neq 0} r_k$ and $\arg\max_{k\neq 0} r_k$ are both 1 for $3 \leq m \leq 19$. It could be that $\min_{k\neq 0} r_k$ stabilizes for larger m, but given the data above, there is still concern that $\min_{k\neq 0} r_k$ tends to 0. Adjusting r_k so that now

$$r_k = \frac{\sigma_m(k)}{k^{2\log_2(\lambda-0.008)}},$$

we obtain the following table.

m	$\min\limits_{k\neq 0} r_k$	$\arg\min\limits_{k\neq 0} r_k$
3	0.3594...	2^3-1
4	0.2396...	2^3-1
5	0.3062...	2^4-1
6	0.2844...	2^5-1
7	0.2913...	2^6-1
8	0.2786...	2^7-1
9	0.2801...	2^8-1
10	0.2808...	2^9-1
11	0.2826...	$2^{10}-1$
12	0.2821...	$2^{11}-1$
13	0.2814...	$2^{12}-1$
14	0.2816...	$2^{13}-1$
15	0.2819...	$2^{14}-1$
16	0.2820...	$2^{15}-1$
17	0.2822...	$2^{16}-1$
18	0.2822...	$2^{17}-1$
19	0.2823...	$2^{18}-1$

Again, the values of $\max_{k\neq 0} r_k$ and $\arg\max_{k\neq 0} r_k$ are both 1 for $3 \leq m \leq 19$. It appears that $\min_{k\neq 0} r_k$ stabilizes for this adjusted r_k, so it seems likely that $x^{2\log_2(\lambda-0.008)}$ is closer to $\sigma_m(x)$ on $[1, 2^m]$ than $x^{2\log_2(\lambda)}$. Thus, we are led to give the following conjecture.

Conjecture 4.3.10. *We have for $m \geq 3$ that*

$$\sigma_m(x) = \sum_{0<k\leq x} |C_m(k)| \asymp x^{2\log_2(\lambda^*)}$$

for some $\lambda^* \in [\lambda - 0.008, \lambda]$ and all $x \in [1, 2^m]$, where the implicit constants do not depend on m and $2.725 < (\lambda^*)^2 < 2.753$.

However, given our results Theorem 3.2.12 and Theorem 4.3.6, we find the small correction for λ to be peculiar and we do not know from where this term may be coming. Whereas we had the liberty of essentially only concerning ourselves with one k when calculating the order of $\max_k |C_m(k)|$, and we had the convenience of easy cancellations of terms when calculating the order of $\sum_{k\neq 0} C_m(k)^2$, we have neither of these advantages when working with $\sum_{k\neq 0} |C_m(k)|$. We need finer control on the off-peak autocorrelations. We may approach this as the problem of getting finer control on the norms of products of the matrices referenced in (3.13), which is difficult to obtain for arbitrary products. We note that Theorem 4.3.7 gives us a fairly close, although trivial, upper bound, and the lower bound of Theorem 4.3.7 is not very tight to our predicted bound.

4.4 Continuous analogue of $C_m(k)$

We introduce an analogue f of $|C_m(k)|$ (as a function of k) on $[0,1]$, which is essentially the limit as $m \to \infty$ of the normalized (in view of Theorem 3.1.1) autocorrelation map $k \mapsto |C_m(k)|/\lambda$, but rescaled so that its domain is $[0,1]$ rather than $[0,\infty)$. As mentioned in the introduction to this chapter, we have that

$$\lim_{m\to\infty} \frac{|C_m(\lfloor x2^m \rceil)|}{\lambda^{m-2}} = f(x).$$

The objective of this section is to provide heuristic evidence for Conjecture 4.1.2 by showing that this analogue function has a maximum at $x = 2/3$. Define $K : [0,1] \to [0,1]$ by

$$K(x) = \begin{cases} 2x & x \in [0, 1/2], \\ 2 - 2x & x \in (1/2, 1]. \end{cases}$$

Note that x and $K(x)$ are analogous to k_m and k_{m-1} in (3.5), respectively. Also note that K is the *tent map*, which is a well-studied function, especially in the fields of ergodic theory and chaos theory (see [14], [2, section 3.2], [13, chapter 10]). Recall

$$M = \begin{bmatrix} 0 & 1 & 2 \\ 0 & -1 & 2 \\ 1 & 0 & 0 \end{bmatrix}, \quad A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Define $T : [0,1] \to \mathbb{Z}^{3\times 3}$ by

$$T(x) = \begin{cases} MB & x \in [0, 1/4] \\ M & x \in (1/4, 1/2] \\ AM & x \in (1/2, 3/4] \\ AMB & x \in (3/4, 1] \end{cases}.$$

Define

$$f_m(x) = \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \frac{T(x) \cdot T(K(x)) \cdot \ldots \cdot T(K^m(x))}{\lambda^{m+1}} A^{c_m} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right|, \tag{4.14}$$

where

$$c_m = \begin{cases} 1, & K^m(x) \in (1/4, 3/4] \\ 0, & \text{else} \end{cases},$$

and finally

$$f(x) := \lim_{m\to\infty} f_m(x).$$

We will make sure that f is well-defined. To do so, we will show that if x does not eventually map to $2/3$ through K, then $f(x) = 0$. Otherwise, if x eventually maps to $2/3$ through K, then $f(x)$ converges to a nonzero value. In other words, the support of f is precisely $\bigcup_{j=0}^{\infty} f^{-j}(2/3)$. We first characterize the points that eventually map to $2/3$ through K.

Lemma 4.4.1. *If* $\{x, K(x), K^2(x), \cdots, K^n(x)\} \subset (1/2, 3/4]$, *then*

$$\left| x - \frac{2}{3} \right| \leq \frac{1}{2^n}. \tag{4.15}$$

Proof. We proceed by induction on $n \geq 0$. For $n = 0$, we have $1/2^n = 1$, so the result follows immediately. Assume that (4.15) holds for n. Now, suppose that

$$\{x, K(x), K^2(x), \cdots, K^{n+1}(x)\} \subset (1/2, 3/4].$$

Then, we have that

$$\left| K(x) - \frac{2}{3} \right| \leq \frac{1}{2^n}.$$

Since $K(x) = 2 - 2x$, we get further that

$$\left| 2 - 2x - \frac{2}{3} \right| = \left| 2x - \frac{4}{3} \right| \leq \frac{1}{2^n},$$

and dividing through by 2 yields the desired result. □

The following characterization of points x that eventually map to $2/3$ through K is very useful in that it tells us that they are the only points such that $f(x) = \lim_{m \to \infty} f_m(x)$ as in (4.14) has a tail composed entirely of AM in the infinite product. This allows for easy computation of the values of f over these points.

Corollary 4.4.2. *For any* $n_0 \in \mathbb{N}_0$, *we have*

$$T(K^n(x)) = AM$$

for all $n \geq n_0$ *if and only if*

$$K^{n_0}(x) = \frac{2}{3}.$$

Proof. The backwards direction is immediate since $2/3$ is a fixed point of K. For the forwards direction, note that $T(K^n(x)) = AM$ if and only if $K^n(x) \in (1/2, 3/4]$. Thus, we have that

$$\{K^{n_0}(x), K^{n_0+1}(x), K^{n_0+2}(x), \cdots\} \subset (1/2, 3/4].$$

By Lemma 4.4.1, we must have that

$$\left| K^{n_0}(x) - \frac{2}{3} \right| \leq \frac{1}{2^n}$$

for all $n \geq n_0$, which implies that $K^{n_0}(x) = 2/3$. $\square$

Points x that do not eventually map to $2/3$ through K therefore have infinitely many factors that are not AM in the infinite product given by $f(x)$, which seemingly makes computing $f(x)$ intractable. However, we will see that $f(x) = 0$ in this case.

Our last characterization of points x that eventually map to $2/3$ through K is explicit, although not as useful for computing $f(x)$ as the prior two.

Lemma 4.4.3. *We have $K^n(x) = 2/3$ for some $n \in \mathbb{N}_0$ if and only if $x = \frac{\ell}{3 \cdot 2^{n-1}}$ for some $1 \leq \ell < 3 \cdot 2^{n-1}$ with $3 \nmid \ell$.*

Proof. For any $x \in [0, 1)$, we have that $|K^{-1}(x)| = 2$, where $|S|$ denotes the cardinality of a set S. Since $K(1) = 0$ and 0 is a fixed point of K, we have that $1 \notin K^{-n}(2/3)$ for any $n \in \mathbb{N}$. Thus,

$$|K^{-n}(2/3)| = 2^n \tag{4.16}$$

for all $n \in \mathbb{N}$. We claim that

$$\left| \left\{ \frac{\ell}{3 \cdot 2^{n-1}} : 1 \leq \ell < 3 \cdot 2^{n-1},\ 3 \nmid \ell \right\} \right| = 2^n. \tag{4.17}$$

We will show (4.17) by induction on $n \in \mathbb{N}$. Clearly this holds for $n = 1$. Assume (4.17) holds for fixed $n \geq 1$. We see that

$$\begin{aligned} \left\{ \frac{\ell}{3 \cdot 2^n} : 1 \leq \ell < 3 \cdot 2^n,\ 3 \nmid \ell \right\} = &\left\{ \frac{1}{2} \cdot \frac{\ell}{3 \cdot 2^{n-1}} : 1 \leq \ell < 3 \cdot 2^{n-1}, 3 \nmid \ell \right\} \\ &\cup \left\{ \frac{1}{2} \cdot \frac{3 \cdot 2^{n-1} + \ell}{3 \cdot 2^{n-1}} : 1 \leq \ell < 3 \cdot 2^{n-1}, 3 \nmid \ell \right\} \end{aligned}$$

and the size of both sets on the right-hand side of this equation is 2^n by our induction hypothesis. Thus, we have shown that (4.17) holds for all $n \in \mathbb{N}$. Since the cardinalities of both sets in (4.16) and (4.17) are equal, it suffices to show that

$$\left\{ \frac{\ell}{3 \cdot 2^{n-1}} : 1 \leq \ell < 3 \cdot 2^{n-1},\ 3 \nmid \ell \right\} \subset K^{-n}(2/3) \tag{4.18}$$

for all $n \in \mathbb{N}$. For this, we again proceed by induction on n. For $n = 1$, $K^{-1}(2/3) = \{1/3, 2/3\}$, so (4.18) holds for this case. Assume (4.18) holds for fixed $n \geq 1$. Fix ℓ such that $1 \leq \ell < 3 \cdot 2^n$ and $3 \nmid \ell$. If $\frac{\ell}{3 \cdot 2^n} < \frac{1}{2}$, then $1 \leq \ell < 3 \cdot 2^{n-1}$ and

$$K^{n+1}\left(\frac{\ell}{3 \cdot 2^n}\right) = K^n\left(K\left(\frac{\ell}{3 \cdot 2^n}\right)\right) = K^n\left(\frac{2\ell}{3 \cdot 2^n}\right) = K^n\left(\frac{\ell}{3 \cdot 2^{n-1}}\right) = \frac{2}{3}$$

by the induction hypothesis. If $\frac{\ell}{3\cdot 2^n} > \frac{1}{2}$, then $3\cdot 2^{n-1} < \ell < 3\cdot 2^n$ and so $1 \leq 3\cdot 2^n - \ell < 3\cdot 2^{n-1}$ and

$$K^{n+1}\left(\frac{\ell}{3\cdot 2^n}\right) = K^n\left(K\left(\frac{\ell}{3\cdot 2^n}\right)\right) = K^n\left(2 - \frac{2\ell}{3\cdot 2^n}\right) = K^n\left(\frac{3\cdot 2^n - \ell}{3\cdot 2^{n-1}}\right) = \frac{2}{3}$$

by the induction hypothesis. Thus, we have shown (4.18) holds for all $n \in \mathbb{N}$ and this concludes the proof. □

The following lemma is used several times in this section to handily deal with infinite products of matrices with tails comprised exclusively of MA, which arise from (4.14).

Lemma 4.4.4. *Let $M_1, M_2 \in \mathbb{R}^{n\times n}$ and suppose M_2 is diagonalizable with distinct eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_r$ with respective eigenspaces $E_1, E_2, \cdots, E_r$ with $\dim E_i = n_i$. Assume λ_r is the spectral radius of M_2 and that $\sum_{i=1}^r n_i = n$, so we may write*

$$M_2 = P\begin{bmatrix} \lambda_r I_{n_r} & & & \\ & \lambda_{r-1} I_{n_{r-1}} & & \\ & & \ddots & \\ & & & \lambda_1 I_{n_1} \end{bmatrix} P^{-1}, \tag{4.19}$$

where I_ℓ denotes the $\ell \times \ell$ identity matrix and P is some invertible matrix. Then, for any $v \in \mathbb{R}^3$, we have that

$$\lim_{m\to\infty} M_1\left(\frac{M_2}{\lambda_r}\right)^m v = M_1 P\begin{bmatrix} I_{n_r} & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix} P^{-1}v,$$

where convergence is componentwise (and thus also in norm).

Proof. Let v_i be the projection of $P^{-1}v$ onto E_i. We have by (4.19) that

$$\begin{aligned} M_1\left(\frac{M_2}{\lambda_r}\right)^m v &= M_1 P\begin{bmatrix} I_{n_r} & & & \\ & \left(\frac{\lambda_{r-1}}{\lambda_r}\right)^m I_{n_{r-1}} & & \\ & & \ddots & \\ & & & \left(\frac{\lambda_1}{\lambda_r}\right)^m I_{n_1} \end{bmatrix} P^{-1}v \\ &= M_1 v_r + \left(\frac{\lambda_{r-1}}{\lambda_r}\right)^m M_1 v_{r-1} + \cdots + \left(\frac{\lambda_1}{\lambda_r}\right)^m M_1 v_1, \end{aligned}$$

which converges pointwise (and thus in norm) to $M_1 v_r$, proving the claim. □

The next lemma is also a technical one, needed solely to be able to work with the entries of $\prod_{j=1}^n (MA)^{a_j}(MB)^{b_j}$ for $n, a_j, b_j \in \mathbb{N}$ while being agnostic about their actual values.

Lemma 4.4.5. *Let $\mathcal{M} \subset \mathbb{Z}^{3\times 3}$ be defined by*

$$\mathcal{M} := \left\{ \begin{bmatrix} e_1 & o_1 & 0 \\ e_2 & o_2 & 0 \\ e_3 & o_3 & 0 \end{bmatrix} : e_j \text{ is even and } o_j \text{ is odd for all } 1 \le j \le 3 \right\}.$$

Then,

$$\prod_{j=1}^{n} (MA)^{a_j}(MB)^{b_j} \in \mathcal{M}$$

for $n, a_j, b_j \in \mathbb{N}$.

Proof. Since $(MB)^\ell = (-1)^\ell (MB)^2$ for $\ell \ge 2$, we may assume that $1 \le b_j \le 2$. We first see that if

$$M_1 = \begin{bmatrix} e_1 & o_1 & 0 \\ e_2 & o_2 & 0 \\ e_3 & o_3 & 0 \end{bmatrix} \in \mathcal{M} \quad \text{and} \quad M_2 = \begin{bmatrix} e_1' & o_1' & 0 \\ e_2' & o_2' & 0 \\ e_3' & o_3' & 0 \end{bmatrix} \in \mathcal{M},$$

then

$$M_1 M_2 = \begin{bmatrix} e_1e_1' + o_1e_2' & e_1o_1' + o_1o_2' & 0 \\ e_2e_1' + o_2e_2' & e_2o_1' + o_2o_2' & 0 \\ e_3e_1' + o_3e_2' & e_3o_1' + o_3o_2' & 0 \end{bmatrix} \in \mathcal{M},$$

so $\mathcal{M}$ is closed under multiplication. Hence it suffices to show that

$$(MA)^a (MB)^b \in \mathcal{M} \tag{4.20}$$

for $a \ge 1$ and $1 \le b \le 2$. We proceed by induction on a. If $a = 1$, we confirm that

$$(MA)(MB) = \begin{bmatrix} 2 & 1 & 0 \\ 2 & -1 & 0 \\ 0 & -1 & 0 \end{bmatrix} \in \mathcal{M} \quad \text{and} \quad (MA)(MB)^2 = \begin{bmatrix} 2 & -1 & 0 \\ -2 & -3 & 0 \\ 2 & -1 & 0 \end{bmatrix} \in \mathcal{M}.$$

Suppose (4.20) holds for a and $1 \le b \le 2$ (recall that $(MB)^b = \pm(MB)^2$ for $b \ge 2$) and let

$$(MA)^a (MB)^b = \begin{bmatrix} e_1 & o_1 & 0 \\ e_2 & o_2 & 0 \\ e_3 & o_3 & 0 \end{bmatrix} \in \mathcal{M}.$$

Then,

$$(MA)^{a+1}(MB)^b = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} e_1 & o_1 & 0 \\ e_2 & o_2 & 0 \\ e_3 & o_3 & 0 \end{bmatrix} = \begin{bmatrix} 2e_3 + e_1 & 2o_3 + o_1 & 0 \\ 2e_3 - e_1 & 2o_3 - o_1 & 0 \\ e_2 & o_2 & 0 \end{bmatrix} \in \mathcal{M},$$

which verifies the claim. □

Finally, we are able to prove that f is well-defined by showing that $f(x)$ converges if x eventually maps to $2/3$ through K, so $x \in \bigcup_{j=0}^{\infty} f^{-j}(2/3)$, and otherwise $f(x) = 0$. The idea of the proof is to consider the limit of the product of matrices in (4.14), for which we have two cases. In the first case, x is such that the tail of the infinite product is composed entirely of AM (equivalently, of MA), in which case Lemma 4.4.4 and Lemma 4.4.5 allow us to show that $f(x)$ converges and is nonzero. In the second case, x is such that the tail of said infinite product is not composed entirely of AM, and we split the product similarly to how we did in the proof of Theorem 3.1.1, so that each subproduct has norm less than 1, giving us that $f(x) = 0$.

Theorem 4.4.6. *We have that f is well-defined, i.e. $f_m \to f$ pointwise. Furthermore, $f(x) = 0$ if and only if $K^n(x) \neq 2/3$ for any $n \in \mathbb{N}$.*

Proof. First, suppose that $K^{n_0}(x) = 2/3$ for some $n_0 \in \mathbb{N}_0$. Without loss of generality, suppose n_0 is the smallest such n such that $K^n(x) = 2/3$. Then, since $2/3$ is a fixed point of K, we have $K^{n_0+k}(x) = 2/3$ and so $T(K^{n_0+k}(x)) = AM$ for all $k \in \mathbb{N}$. If $n_0 = 0$, then using Lemma 4.4.4 and the decomposition given in Lemma 3.2.3, we have that

$$\begin{aligned} f(x) &= \lim_{k\to\infty} \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} A \left(\frac{MA}{\lambda}\right)^k \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right| \\ &= \lim_{k\to\infty} \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} AP \begin{bmatrix} 1 & 0 & 0 \\ 0 & \left(\frac{\overline{\nu}}{\lambda}\right)^k & 0 \\ 0 & 0 & \left(\frac{\nu}{\lambda}\right)^k \end{bmatrix} P^{-1} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right| \\ &= \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} AP \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} P^{-1} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right| \\ &= |\mu| \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} A \begin{bmatrix} 2-\lambda^2 \\ -\lambda \\ 1 \end{bmatrix} \right| \\ &= |\mu|\lambda, \end{aligned} \tag{4.21}$$

where $\mu = \frac{-2\mathrm{Re}(\nu)(2\mathrm{Re}(\nu)+|\nu|^2-1)}{\sqrt{-236}}$, which is denoted a in the proof of Theorem 3.1.1. Now, suppose that $n_0 \geq 1$. Note that

$$K^{-1}(2/3) \setminus \{2/3\} = \{1/3\} \quad \text{and} \quad K^{-2}(2/3) \setminus \{2/3\} = \{1/6, 5/6\},$$

so

$$T(K^{-1}(2/3)\setminus\{2/3\})=\{M\}\quad\text{ and }\quad T(K^{-2}(2/3)\setminus\{2/3\})=\{MB,AMB\}.$$

Again we use Lemma 4.4.4 and the decomposition given in Lemma 3.2.3 to obtain

$$\begin{aligned} f(x)&=\lim_{k\to\infty}\left|\begin{bmatrix}1&0&0\end{bmatrix}A^{\delta}\left(\frac{MB}{\lambda}\right)^{\ell_1}\prod_{j=1}^{\ell_2}\left(\frac{(MA)^{a_j}(MB)^{b_j}}{\lambda^{a_j+b_j}}\right)\left(\frac{MA}{\lambda}\right)^{k+2}\begin{bmatrix}1\\-1\\1\end{bmatrix}\right| \\ &=\left|\begin{bmatrix}1&0&0\end{bmatrix}A^{\delta}\left(\frac{MB}{\lambda}\right)^{\ell_1}\prod_{j=1}^{\ell_2}\left(\frac{(MA)^{a_j}(MB)^{b_j}}{\lambda^{a_j+b_j}}\right)\begin{bmatrix}2-\lambda^2\\-\lambda\\1\end{bmatrix}\right| \end{aligned} \tag{4.22}$$

for some $\delta\in\{0,1\}$, $a_j,b_j\geq 1$, and $\ell_1+\sum_{j=1}^{\ell_2}(a_j+b_j)=n_0-2$. Since n_0 is fixed, (4.22) implies that $f(x)$ converges. Now, we would like to show that $f(x)\neq 0$. Note that $(MB)^{\ell}=\pm(MB)^2$ for $\ell\geq 2$, hence

$$\begin{bmatrix}1&0&0\end{bmatrix}A^{\delta}(MB)^{\ell_1}\in\left\{\begin{bmatrix}1&0&0\end{bmatrix},\pm\begin{bmatrix}0&1&0\end{bmatrix}\right\}.$$

So, showing $f(x)\neq 0$ amounts to showing that if

$$\prod_{j=1}^{\ell_2}\left(\frac{(MA)^{a_j}(MB)^{b_j}}{\lambda^{a_j+b_j}}\right)\begin{bmatrix}2-\lambda^2\\-\lambda\\1\end{bmatrix}=\begin{bmatrix}x\\y\\z\end{bmatrix}, \tag{4.23}$$

then $x,y\neq 0$. If $\ell_2=0$, then this is obviously true. If $\ell_2\geq 1$, then we may use Lemma 4.4.5 to get that

$$\prod_{j=1}^{\ell_2}\left(\frac{(MA)^{a_j}(MB)^{b_j}}{\lambda^{a_j+b_j}}\right)\begin{bmatrix}2-\lambda^2\\-\lambda\\1\end{bmatrix}=\begin{bmatrix}e_1&o_1&0\\e_2&o_2&0\\e_3&o_3&0\end{bmatrix}\begin{bmatrix}2-\lambda^2\\-\lambda\\1\end{bmatrix}=\begin{bmatrix}e_1(2-\lambda^2)-o_1\lambda\\e_2(2-\lambda^2)-o_2\lambda\\e_3(2-\lambda^2)-o_3\lambda\end{bmatrix}$$

for even e_j and odd o_j. We have that $e_j(2-\lambda^2)-o_j\lambda\neq 0$ for all j because λ is a root of x^3+x^2-2x-4, which is irreducible over $\mathbb{Z}$. Thus, we have shown that f is well-defined and $f(x)\neq 0$ in this case.

Now, suppose that $K^n(x)\neq 2/3$ for any $n\in\mathbb{N}$. Then, by Corollary 4.4.2, there are infinitely many n such that $T(K^n(x))\neq AM$. That is, there are infinitely many n such that

$$T(K^n(x))\in\{MB,M,AMB\}. \tag{4.24}$$

We wish to show that MB occurs infinitely many times in the product given in (4.14) as we take the limit. The matrix multiplication rules (3.19) hold for the product given in (4.14),

so that

$$\begin{aligned} T(K^n(x))T(K^{n+1}(x)) &\in \{MAM, MAMB\} && \text{if } T(K^n(x)) = M, \\ T(K^n(x))T(K^{n+1}(x)) &\in \{AMAM, AMAMB\} && \text{if } T(K^n(x)) = AM. \end{aligned} \tag{4.25}$$

If $T(K^{n_0}(x)) = M$ for fixed n_0, we may not have that $T(K^{n_0+k}(x)) = AM$ for all $k \in \mathbb{N}$ or else we have that $K^{n_0+1}(x) = 2/3$ by Corollary 4.4.2, which contradicts our assumption for this case. Thus, we must have that $T(K^{n_0+k}(x)) = AMB$ for some $k \in \mathbb{N}$. This fact, in conjunction with (4.24) and (4.25), implies that MB occurs infinitely many times in the product given in (4.14) as we take the limit. More rigorously, there exists a strictly monotonic sequence $\{m_n\}_{n=1}^{\infty} \subset \mathbb{N}$ such that

$$\begin{aligned} f_{m_n}(x) &= \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} A^{\delta} \frac{(MA)^{a_1}(MB)^{b_1}}{\lambda^{a_1+b_1}} \cdots \frac{(MA)^{a_n}(MB)^{b_n}}{\lambda^{a_n+b_n}} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right| \\ &\leq \left\| \frac{(MA)^{a_1}(MB)^{b_1}}{\lambda^{a_1+b_1}} \cdots \frac{(MA)^{a_n}(MB)^{b_n}}{\lambda^{a_n+b_n}} \right\| \cdot \sqrt{3}, \end{aligned} \tag{4.26}$$

where $\delta \in \{0, 1\}$, $a_j \geq 0$ and $b_j \geq 1$ for all j, and we used the fact that $\left\| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} A^{\delta} \right\| = 1$. We claim that the norm in (4.26) vanishes as $n \to \infty$. This is clearly the case if $a_n = 0$ for all sufficiently large n, since then the product in (4.26) has a tail of the form $(MB/\lambda)^{\ell}$, and $(MB)^{\ell} = \pm MB^2$ for $\ell \geq 2$, so $\|(MB/\lambda)^{\ell}\| \to 0$. Else, we have that $a_n \geq 1$ for infinitely many n, so we may use the submultiplicativity of $\|\cdot\|$ (i.e., $\|M_1 M_2\| \leq \|M_1\|\|M_2\|$ for all $M_1, M_2 \in \mathbb{R}^{3\times 3}$) and Lemma 3.2.6 to conclude that

$$f(x) = \lim_{n\to\infty} f_{m_n}(x) = 0.$$

This proves the claim.

□

Now that we have established that f is well-defined, we concern ourselves with showing that f is indeed a good analogue for $|C_m(k)|$ on the unit interval; namely, we show that

$$\lim_{m\to\infty} \frac{|C_m(\lfloor x2^m \rceil)|}{\lambda^{m-2}} = f(x).$$

To show this, we must first prove that if $k_m = \lfloor x2^m \rfloor$ is odd for $x \in (0, 1)$, then $k_m \mapsto k_{m-1}$ is essentially the same mapping as $x \mapsto K(x)$, in that

$$k_{m-1} = \lfloor K(x)2^{m-1} \rceil,$$

and $K(x)$ and k_{m-1} are in the same fourths of $[0,1]$ and $[0,2^m]$, respectively (e.g., $K(x) \in (0,1/4)$ if and only if $k_{m-1} \in S_{m-1}^1 = (0, 2^{m-3})$).

Lemma 4.4.7. *Let $x \in [0,1]$ and $m \geq 3$ be such that*

$$x = k_m 2^{-m} + y, \quad 0 < |y| < 2^{-(m+1)} \tag{4.27}$$

for some odd k_m with $1 \leq k_m < 2^m$. Then, we have that

$$\lfloor K^j(x) 2^{m-j} \rceil = k_{m-j} \tag{4.28}$$

and

$$k_{m-j} \in S_{m-j}^n \quad \text{if and only if} \quad K^j(x) \in \left(\frac{n-1}{4}, \frac{n}{4} \right) \tag{4.29}$$

for all $0 \leq j \leq m-3$ and any $1 \leq n \leq 4$, where k_{m-j} and S_{m-j}^n are defined as in (3.5) and (3.6), respectively.

Proof. We proceed by induction on j. For $j = 0$, we have by (4.27) that $\lfloor x 2^m \rceil = k_m$, which verifies (4.28). Now, we show the forward direction of (4.29). Since k_m is odd by assumption, we have

$$k_m = \lfloor x 2^m \rceil \notin \{0, 2^{m-2}, 2^{m-1}, 3 \cdot 2^{m-2}, 2^m\},$$

so (4.27) implies that

$$\min\{x, |x - 1/4|, |x - 1/2|, |x - 3/4|, 1 - x\} > 2^{-(m+1)}. \tag{4.30}$$

Suppose $k_m \in S_m^n = ((n-1)2^{m-2}, n 2^{m-2})$. Then, by (4.27), we have

$$x \in \left(\frac{n-1}{4} - 2^{-(m+1)}, \frac{n}{4} + 2^{-(m+1)} \right),$$

but, by (4.30), we may not have $|x - (n-1)/4| < 2^{-(m+1)}$ nor $|x - n/4| < 2^{-(m+1)}$, so we are left with

$$x \in \left(\frac{n-1}{4}, \frac{n}{4} \right).$$

The reverse direction of (4.29) follows similarly.

Assume that (4.28), (4.29), and

$$K^j(x) = k_{m-j} 2^{-m+j} + y, \quad 0 < |y| < 2^{-(m+1)+j}$$

hold for some $0 \leq j < m-3$ and odd k_{m-j} with $1 \leq k_{m-j} < 2^{m-j}$. If $K^j(x) < 1/2$, then $k_{m-j} < 2^{m-1}$ and

$$K^{j+1}(x) = K(K^j(x)) = 2K^j(x) = k_{m-j}2^{-m+j+1} + 2y, \quad 0 < |2y| < 2^{-(m+1)+j+1}, \tag{4.31}$$

so

$$\lfloor K^{j+1}(x)2^{m-(j+1)} \rceil = k_{m-j} = k_{m-(j+1)}, \tag{4.32}$$

showing (4.28) when $x < 1/2$ for all $0 \leq j \leq m-3$. We can show that (4.32) holds for $x > 1/2$ similarly. Since $k_{m-(j+1)}$ is still odd, we again get that

$$\min\{K^{j+1}(x), |K^{j+1}x - 1/4|, |K^{j+1}(x) - 1/2|, |K^{j+1}(x) - 3/4|, 1 - K^{j+1}(x)\} > 2^{-(m+1)+j+1}$$

and so just as in our base case, we get that

$$k_{m-(j+1)} \in S^n_{m-(j+1)} \quad \text{ if and only if } \quad K^{j+1}(x) \in \left(\frac{n-1}{4}, \frac{n}{4}\right),$$

so we have shown (4.29) for all $0 \leq j \leq m-3$ and $1 \leq n \leq 4$, and we are done. □

Corollary 4.4.8. *Let $x \in [0,1]$ and $m \geq 3$ be such that*

$$x = k_m 2^{-m} + y, \quad 0 < |y| < 2^{-(m+1)}$$

for some odd k_m with $1 \leq k_m < 2^m$. Then, we have that

$$\frac{|C_m(\lfloor x2^m \rceil)|}{\lambda^{m-2}} = f_{m-2}(x)$$

for all $m \geq 2$.

Proof. By (4.28), we have that

$$C_m(\lfloor x2^m \rceil) = C_m(k_m).$$

By (4.29), we have that

$$T(K^j(x)) = \begin{cases} MB, & k_{m-j} \in S^1_{m-j} \\ M, & k_{m-j} \in S^2_{m-j} \\ AM, & k_{m-j} \in S^3_{m-j} \\ AMB, & k_{m-j} \in S^4_{m-j} \end{cases}.$$

Thus, the matrix products in the definition of $f_{m-2}(x)$ given in (4.14) and the definition of v_m given in (3.8) coincide. Note that k_m being odd is necessary to consider $v_m = v_m(k_m)$.

We conclude that

$$\frac{C_m(\lfloor x2^m \rceil)}{\lambda^{m-2}} = \frac{C_m(k_m)}{\lambda^{m-2}} = \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \frac{T(x)T(K(x))\cdots T(K^{m-2}(x))}{\lambda^{m-2}} A^{c_m} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right| = f_{m-2}(x).$$

□

Theorem 4.4.9. *For all $x \in (0,1]$, we have*

$$\lim_{m\to\infty} \frac{|C_m(\lfloor x2^m \rceil)|}{\lambda^{m-2}} = f(x).$$

Proof. Fix $x \in (0,1]$. If $x = k2^{-n}$ for some $n, k \in \mathbb{N}_0$, then Lemma 4.4.3 tells us that x does not eventually map to $2/3$ through K, so $f(x) = 0$ by Theorem 4.4.6. For sufficiently large m, we have $x2^m$ is even, so $C(m, \lfloor x2^m \rceil) = 0$. Thus, we are done in this case and now consider $x \neq k2^{-n}$ for any $n, k \in \mathbb{N} \cup \{0\}$.

Now, we may write

$$x = k_m 2^{-m} + y_m, \quad 0 < |y_m| < 2^{-(m+1)} \tag{4.33}$$

for any $m \geq 2$. There are two cases to consider. First, suppose that $K^n(x) = 2/3$ for some $n \in \mathbb{N}$. Then, by Lemma 4.4.3, we have that

$$x = \frac{\ell}{3 \cdot 2^{n-1}}$$

for some $1 \leq \ell < 3 \cdot 2^{n-1}$ with $3 \nmid \ell$. For $m \geq n$, we have by Lemma 4.4.7 that

$$k_m = \lfloor x2^m \rceil = \left\lfloor \frac{2^{m-n+1}\ell}{3} \right\rceil = \begin{cases} \frac{2^{m-n+1}\ell - 1}{3}, & 2^{m-n+1}\ell \equiv 1 \pmod 3 \\ \frac{2^{m-n+1}\ell + 1}{3}, & 2^{m-n+1}\ell \equiv 1 \pmod 3, \end{cases}$$

which is always odd. So, picking $m \geq n$ in (4.33) guarantees odd k_m, so we may use Corollary 4.4.8 to get that

$$\frac{|C_m(\lfloor x2^m \rceil)|}{\lambda^{m-2}} = f_{m-2}(x) \tag{4.34}$$

for arbitrary $m \geq n$. Thus, passing to the limit proves the claim in this case.

Now, suppose that $K^n(x) \neq 2/3$ for any $n \in \mathbb{N}$. If k_m in (4.33) is odd, then again Corollary 4.4.8 tells us that (4.34) holds. By Theorem 4.4.6, we have that $f(x) = 0$. So, if k_m in (4.33) is even, then $C(k_m) = C(\lfloor x2^m \rceil) = 0 = f(x)$. This concludes the proof. □

We now show that $x = 2/3$ gives maximal $f(x)$. We do so by splitting the product in (4.14) in ways that allow us to explicitly compute bounds for $f(x)$, much like (3.24). In

view of Theorem 4.4.9, this serves to motivate Conjecture 4.1.2, which states that the k_m^* with $1 < k_m^* < 2^m$ that gives maximal $|C_m(k_m)|$ should satisfy $\lim_{m\to\infty} k_m^*/2^m = 2/3$.

Theorem 4.4.10. *We have that $f(x) < f(2/3)$ for all $x \neq 2/3$.*

Proof. By Theorem 4.4.6, it suffices to consider x such that $K^n(x) = 2/3$ for some $n \in \mathbb{N}$. We first show that $f(1/3) < f(2/3)$. As shown in (4.21), we have

$$\lim_{k\to\infty} \left(\frac{MA}{\lambda}\right)^k \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = \mu \begin{bmatrix} -\lambda \\ 2-\lambda^2 \\ 1 \end{bmatrix} \tag{4.35}$$

and

$$f(2/3) = |\mu| \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -\lambda \\ 2-\lambda^2 \\ 1 \end{bmatrix} \right| = |\mu|\lambda,$$

again where $\mu = \frac{-2\mathrm{Re}(\nu)(2\mathrm{Re}(\nu)+|\nu|^2-1)}{\sqrt{-236}}$. Since $1/3 \in (1/4, 1/2]$, we have that $T(1/3) = M$ and so we use (4.35) and Lemma 4.4.4 to get

$$f(1/3) = |\mu| \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \frac{M}{\lambda} \begin{bmatrix} -\lambda \\ 2-\lambda^2 \\ 1 \end{bmatrix} \right| = |\mu| \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} \right| = |\mu| \frac{4-\lambda^2}{\lambda}.$$

Since $\lambda > \frac{4-\lambda^2}{\lambda}$, we have that $f(2/3) > f(1/3)$.

Now, we wish to show that $f(x) < f(2/3)$ for all $x \notin \{1/3, 2/3\}$. First, note how $K^{-1}(1/3) \in [0, 1/4) \cup (3/4, 1]$, meaning that $T(K^{-1}(1/3)) = \{MB, AMB\}$. We use (4.35) and the decomposition in Lemma 3.2.3 to get

$$\begin{aligned} f(x) &= \lim_{m\to\infty} \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \frac{A^\delta \left(\prod_{i=1}^n MA^{\delta_i}B^{1-\delta_i}\right)(MA)^{m+1}}{\lambda^{n+m+1}} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right| \\ &= |\mu| \left| \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \frac{A^\delta \left(\prod_{i=1}^n MA^{\delta_i}B^{1-\delta_i}\right)}{\lambda^n} \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} \right| \end{aligned}$$

for some $\delta, \delta_i \in \{0, 1\}$ and with $\delta_1 = 0$. In order to prove the claim, we will show that

$$\left\| \prod_{i=1}^n MA^{\delta_i}B^{1-\delta_i} \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} \right\|_\infty < \lambda,$$

which is a stronger statement than $f(x) < f(2/3)$, which depends only on the first component. We prove this by partitioning our n-factor product into smaller products of $(MA)^j(MB)^k$ and considering the L^∞ norm of these smaller products, similar to the proof of Theorem 3.1.1 but using the L^∞ norm in place of the L^2 norm. We aim to show that

$$\begin{aligned}\left\|\prod_{i=1}^{n}(MA)^{\alpha_i}(MB)^{\beta_i}\right\|_\infty &\leq \left\|\prod_{i=1}^{4k}(MA)^{\alpha_{i+3}}(MB)^{\beta_{i+3}}\right\|_\infty \cdot \left\|\prod_{i=1}^{3}(MA)^{\alpha_i}(MB)^{\beta_i}\begin{bmatrix}\frac{4-\lambda^2}{\lambda}\\ \lambda \\ -1\end{bmatrix}\right\|_\infty \\ &< \lambda \cdot \prod_{i=1}^{n}\lambda^{\alpha_i+\beta_i},\end{aligned} \tag{4.36}$$

where $\alpha_i \geq 0$, $\beta_i \geq 1$, and $4k$ is the largest multiple of 4 less than n. We achieve this by obtaining very specific bounds for the norms of shorter products of MA and MB. Again, we may assume without loss of generality that $1 \leq \beta_i \leq 2$ for all i.

We claim that

$$\frac{1}{\lambda^{\alpha+\beta}}\left\|(MA)^\alpha(MB)^\beta\right\|_\infty \leq 1.215 \tag{4.37}$$

for $\alpha \geq 0$ and $\beta \geq 1$. Obviously this is true if $\alpha = 0$. Using Lemma 3.2.5, we find that this is true if $\alpha \geq 17$. A computer check verifies the claim for $1 \leq \alpha \leq 16$ and $1 \leq \beta \leq 2$.

Using (4.37) along with the submultiplicativity of $\|\cdot\|_\infty$, we have that

$$\frac{1}{\prod_i \lambda^{\alpha_i+\beta_i}}\left\|\prod_{i=1}^{2}(MA)^{\alpha_i}(MB)^{\beta_i}\right\|_\infty \leq \frac{1.215}{\lambda^{\alpha_j+\beta_j}}\left\|(MA)^{\alpha_j}(MB)^{\beta_j}\right\|_\infty \tag{4.38}$$

for any $1 \leq j \leq 2$, and Lemma 3.2.5 get us that this quantity is less than or equal to 1.093 for $\alpha_j \geq 35$. We find that the same holds for when $\max\{\alpha_1, \alpha_2\} \leq 34$ by a computer check, so

$$\frac{1}{\prod_i \lambda^{\alpha_i+\beta_i}}\left\|\prod_{i=1}^{2}(MA)^{\alpha_i}(MB)^{\beta_i}\right\|_\infty \leq 1.093 \tag{4.39}$$

for all $\alpha_i \geq 0$ and $\beta_i \geq 1$.

Likewise, we find that (4.38) is less than 0.9148 when $\alpha_j \geq 94$ for any $1 \leq j \leq 2$.

$$\frac{1}{\prod_i \lambda^{\alpha_i+\beta_i}}\left\|\prod_{i=1}^{2}(MA)^{\alpha_i}(MB)^{\beta_i}\right\|_\infty \leq 0.9148 \tag{4.40}$$

for all α_i, β_i with either α_1 or α_2 greater than 4. We may use (4.39) and (4.40) along with submultiplicativity to get that $\left\|\frac{1}{\prod_i \lambda^{\alpha_i+\beta_i}}\prod_{i=1}^{4}(MA)^{\alpha_i}(MB)^{\beta_i}\right\|_\infty \leq 0.9148 \cdot 1.093 < 1$ when

$\max\{\alpha_i : 1 \le i \le 4\} \ge 5$. A computer check for the remaining cases concludes that

$$\frac{1}{\prod_i \lambda^{\alpha_i+\beta_i}} \left\| \prod_{i=1}^{4} (MA)^{\alpha_i} (MB)^{\beta_i} \right\|_\infty < 1 \tag{4.41}$$

for all $\alpha_i \ge 0$ and $\beta_i \ge 1$.

Now, we claim that

$$\left\| \frac{(MA)^\alpha (MB)^\beta}{\lambda^{\alpha+\beta}} \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} \right\|_\infty \le 0.8 \cdot \lambda \tag{4.42}$$

for $\alpha \ge 0$ and $\beta \ge 1$ with the exception of $(\alpha, \beta) = (2, 1)$. Obviously this is true if $\alpha = 0$. Using submultiplicativity of $\|\cdot\|_\infty$, we have

$$\left\| \frac{(MA)^\alpha (MB)^\beta}{\lambda^{\alpha+\beta}} \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} \right\|_\infty \le \left\| \frac{(MA)^\alpha (MB)^\beta}{\lambda^{\alpha+\beta}} \right\|_\infty \cdot \left\| \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} \right\|_\infty = \left\| \frac{(MA)^\alpha (MB)^\beta}{\lambda^{\alpha+\beta}} \right\|_\infty \cdot \lambda,$$

and by Lemma 3.2.5, we have that (4.42) is true if $\alpha \ge 51$, and a computer check furthers this to all $(\alpha, \beta) \notin \{(1,1), (2,1), (3,1), (4,1), (5,1), (6,1), (7,1), (9,1), (14,1)\}$. A check by hand verifies the claim for these exceptional cases with the exception of $(\alpha, \beta) = (2, 1)$.

Now, we consider the case $(\alpha, \beta) = (2, 1)$. We see that

$$\frac{(MA)^2 (MB)^1}{\lambda^3} \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} = \begin{bmatrix} \frac{8-3\lambda^2}{\lambda^4} \\ \frac{-8-\lambda^2}{\lambda^4} \\ \frac{8-3\lambda^2}{\lambda^4} \end{bmatrix}$$

and

$$\left\| \begin{bmatrix} \frac{8-3\lambda^2}{\lambda^4} \\ \frac{-8-\lambda^2}{\lambda^4} \\ \frac{8-3\lambda^2}{\lambda^4} \end{bmatrix} \right\|_\infty = \frac{8+\lambda^2}{\lambda^4} < \lambda. \tag{4.43}$$

We find that

$$\left\| \frac{(MA)^\alpha (MB)^\beta}{\lambda^{\alpha+\beta}} \begin{bmatrix} \frac{8-3\lambda^2}{\lambda^4} \\ \frac{-8-\lambda^2}{\lambda^4} \\ \frac{8-3\lambda^2}{\lambda^4} \end{bmatrix} \right\|_\infty \le 0.8 \cdot \lambda \tag{4.44}$$

for $\alpha \ge 0$ and $\beta \ge 1$ similarly to how we found (4.42). We have taken care of the norm of the matrix-vector product in (4.36). More specifically, by (4.37), (4.39), (4.42), (4.43), and

(4.44), we have that

$$\left\| \prod_{i=1}^{n} (MA)^{\alpha_i} (MB)^{\beta_i} \begin{bmatrix} \frac{4-\lambda^2}{\lambda} \\ \lambda \\ -1 \end{bmatrix} \right\|_\infty \leq 1.215 \cdot 0.8 \cdot \lambda < \lambda$$

for $1 \leq n \leq 3$, $\alpha_i \geq 0$, and $\beta_i \geq 1$. Combining this with (4.41) yields (4.36), so we are done. □

Remark 4.4.11. *In order to use this result to prove that the k that gives maximal $|C_m(k)|$ is asymptotically $\frac{2}{3} \cdot 2^m$, we need that the convergence given by Theorem 4.4.9 is uniform. However, to prove this, we encounter essentially the same problem as in dealing with Conjecture 4.3.10 – we need finer control on the convergence of $f_m(x)$ for x such that $T^n(x) \neq \frac{2}{3}$ for any n.*

Bibliography

[1] William W. Adams and Larry Joel Goldstein. *Introduction to Number Theory*. Prentice-Hall, Englewood Cliffs, NJ, 1973. 29

[2] Kathleen T. Alligood, Tim D. Sauer, and James A. Yorke. *Chaos: an introduction to dynamical systems*. Springer-Verlag New York, 1996. 92

[3] Jean-Paul Allouche. Finite automata and arithmetic. In *Sém. Lothar. Combin. [electronic only]*, volume 30, 1993. 55

[4] Jean-Paul Allouche, Stephen Choi, Alain Denise, Tamás Erdélyi, and Bahman Saffari. Bounds on autocorrelation coefficients of Rudin-Shapiro polynomials. *Anal. Math.*, 45:705–726, 2019. 55, 56, 62, 63, 71

[5] Jean-Paul Allouche and Jeffery Shallit. The ubiquitouis Prouhet-Thue-Morse sequence. In *Sequences and their applications (Singapore, 1998)*, Springer Ser. Discrete Math. Theor. Comput. Sci., pages 1–16. Springer, London, 1999. 52

[6] Alan Baker. *A concise introduction to the theory of numbers*. Cambridge University Press, 1984. 47

[7] Yuri Bilu and Robert Tichy. The diophantine equation $f(x) = g(y)$. *Acta Arith.*, 95:261–288, 2000. 7

[8] Vincent D. Blondel and John N. Tsitsiklis. The Lyapunov exponent and joint spectral radius of pairs of matrices are hard—when not impossible—to compute and to approximate. *Math. Control Signals Systems*, 10(1):31–40, 1997. 74

[9] Vincent D. Blondel and John N. Tsitsiklis. The boundedness of all products of a pair of matrices is undecidable. *Systems Control Lett.*, 41(2):135–140, 2000. 74

[10] Peter Borwein, Ron Ferguson, and Joshua Knauer. The merit factor problem. In *Number Theory and Polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 52–70. Cambridge University Press, 2008. 54

[11] Peter Borwein and Michael Mossinghoff. Rudin-Shapiro-like polynomials in L^4. *Math. Comp.*, 69(231):1157–1166, 2000. 54, 84

[12] Peter Borwein and Michael Mossinghoff. Barker sequences and flat polynomials. In *Number Theory and Polynomials*, pages 71–88. Cambridge University Press, 2008. 53

[13] Karen M. Brucks and Henk Bruin. *Topics from one-dimensional dynamics*, volume 62 of *London Math. Soc. Stud. Texts*. Cambridge University Press, 2004. 92

[14] Henk Bruin. For almost every tent map, the turning point is typical. *Fund. Math.*, 155(3):215–235, 1998. 92

[15] Jasbir S. Chahal and Nathan Priddis. Some congruence properties of Pell's equations. *Ann. Sci. Math. Québec*, 35(2):175–184, 2011. 28

[16] Tsz Ho Chan. Factors of a perfect square. *Acta Arith.*, 163(2):141–143, 2014. 2

[17] Tsz Ho Chan. Common factors among pairs of consecutive integers. *Int. J. Number Theory*, 14(3):871–880, 2018. 2, 4, 11

[18] Tsz Ho Chan, Stephen Choi, and Peter C.-H. Lam. Divisibility on the sequence of perfect squares minus one: The gap principle. *J. Number Theory*, 184:473–484, 2018. viii, 2, 4, 11

[19] Stephen Choi. Bounds on autocorrelation coefficients of Rudin–Shapiro polynomials II. *J. Approx. Theory*, 254:article 105390, 2020. 56, 63

[20] Stephen Choi, Peter C.-H. Lam, and Daniel Tarnu. Gap principle of divisibility of sequences of polynomials. *J. Number Theory*, 223:153–167, 2021. 1

[21] Stephen Choi and Daniel Tarnu. The order of the fundamental solution of $X^2-DY^2=1$ in $\mathbb{Z}[\sqrt{D}]/\langle D\rangle$. *Integers*, 22(A84), 2022. 25

[22] Stephen Choi and Daniel Tarnu. Limiting behavior of Rudin-Shapiro sequence autocorrelations. in preparation. 77

[23] Keith Conrad. Pell's equation, ii. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf. 29

[24] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons, Inc., 3rd edition, 2004. 16

[25] Tamás Erdélyi. Recent progress in the study of polynomials with constrained coefficients. In *Trigonometric Sums and Their Applications*, pages 29–69. Springer, Cham, 2020. 56

[26] Paul Erdős and Moshe Rosenfeld. The factor-difference set of integers. *Acta Arith.*, 79(4):353–359, 1997. 1

[27] Marcel J.E. Golay. Sieves for low autocorrelation binary sequences. *IEEE Trans. Inform. Theory*, IT-23(1):43–51, 1977. 53

[28] Nicola Guglielmi and Vladimir Yu. Protasov. Exact computation of joint spectral characteristics of linear operators. *Found. Comput. Math.*, 13(1):37–97, 2013. 57, 74, 76

[29] Nicola Guglielmi and Vladimir Yu. Protasov. Invariant polytopes of sets of matrices with applications to regularity of wavelets and subdivisions. *SIAM J. Matr. Anal. Appl.*, 37(1):18–52, 2016. 74, 75, 76

[30] Tom Høholdt. The merit factor problem for binary sequences. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 3857 of *Lecture Notes in Comput. Sci.*, pages 51–59. Springer, Berlin, 2006. 54

[31] Tom Høholdt and Helge Jensen. Determination of the merit factor of Legendre sequences. *IEEE Trans. Inform. Theory*, 4(1):161–164, 1988. 54

[32] Tom Høholdt, Helge Jensen, and Jørn Justesen. Aperiodic correlations and the merit factor of a class of binary sequences (corresp.). *IEEE Trans. Inform. Theory*, 31(4):549–552, 1985. 54, 55, 57, 58, 72, 79, 84

[33] Jonathan Jedwab. A survey of the merit factor problem for binary sequences. In *Sequences and their Applications — SETA 2004*, volume 3486 of *Lecture Notes in Comput. Sci.*, pages 30–55. Springer-Verlag, 2005. 54

[34] Jonathan Jedwab, Daniel J. Katz, and Kai-Uwe Schmidt. Advances in the merit factor problem for binary sequences. *J. Combin. Theory Ser. A*, 120(4):882–906, 2013. 53, 54

[35] Jonathan Jedwab, Daniel J. Katz, and Kai-Uwe Schmidt. Littlewood polynomials with small l^4 norm. *Adv. Math.*, 241:127–136, 2013. 54

[36] John E. Littlewood. Some problems in real and complex analysis. *Heath Mathematical Monographs, Lexington, Massachusetts*, 37, 1968. 54, 79, 84

[37] Raphael Jungers. *The joint spectral radius: Theory and applications*, volume 385 of *Lecture Notes in Control and Inform. Sci.* Springer, Berlin, 2009. 73, 74

[38] Daniel J. Katz and Courtney M. van der Linden. Peak sidelobe level and peak cross-correlation of Golay–Rudin–Shapiro sequences. *IEEE Trans. Inform. Theory*, 68:3455–3473, 2022. 55, 56

[39] Victor J. Katz. *A History of Mathematics: An Introduction.* Addison-Wesley, 3rd edition, 2009. 6

[40] Donald E. Knuth. *The Art of Computer Programming, Volume 4A: Combinatorial Algorithms, Part 1.*, volume 4A. Addison-Wesley Professional, 1st edition, 2014. 61

[41] Christian Mauduit. The Rudin-Shapiro sequence. In *Substitutions in Dynamics, Arithmetics and Combinatorics*, volume 1794 of *Lecture Notes in Math.*, pages 41–47. Springer, Berlin, 2002. 55

[42] R.A. Mollin and A. Srinivasan. Pell equations: Non-principal Lagrange criteria and central norms. *Canad. Math. Bull.*, 55(4):774–782, 2012. 31, 32

[43] Richard A. Mollin. *Fundamental Number Theory with Applications.* Chapman and Hall/CRC, 2nd edition, 2008. 32

[44] Richard A. Mollin and Anitha Srinivasan. A note on the negative Pell equation. *International Journal of Algebra*, 4(19):919–922, 2010. 32, 33

[45] Donald J. Newman and J.S. Byrnes. The L^4 norm of a polynomial with coefficients ± 1. *Amer. Math. Monthly*, 97:42–45, 1990. 54

[46] Oskar Perron. *Die Lehre von den Kettenbrüchen.* Teubner, Stuttgart, 1954. 32

[47] Gian-Carlo Rota and Gilbert Strang. A note on the joint spectral radius. *Indag. Math. (N.S.)*, 63:379–381, 1960. 57, 73

[48] Pierre Samuel. *Algebraic Theory of Numbers*. Hermann, Paris, 1970. 27

[49] Jörn Steuding. *Diophantine Analysis*. Discrete Mathematics and its Applications. CRC Press, 2005. 26, 27

[50] Daniel Tarnu. On maximal autocorrelations of Rudin-Shapiro sequences. *Journal of Approximation Theory*, 287:Article 105866, 2023. 51

[51] Jan Turk. Almost powers in short intervals. *Arch. Math.*, 43:157–166, 1984. 13

[52] Richard Turyn. Ambiguity functions of complementary sequences (corresp.). *IEEE Trans. Inform. Theory*, 9:46–47, 1963. 72

[53] George R. Welti. Quaternary codes for pulsed radar. *IRE Trans. Inform. Theory*, 6:400–408, 1960. 72

[54] Fabian Wirth. The generalized spectral radius and extremal norms. *Linear Algebra Appl.*, 342:17–40, 2000. 74

Appendix A

Code

All code required to verify the computations in this work can be found at: https://github.com/D-Tarnu/thesis.