PROPERTIES OF DIGITAL REPRESENTATIONS

BY

KATHERINE ALEXANDER ANDERS

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2014

Urbana, Illinois

Doctoral Committee:

Professor Iwan Duursma, Chair
Professor Bruce Reznick, Director of Research
Professor A.J. Hildebrand
Professor Alexander Yong

Abstract

Let $\mathcal{A}$ be a finite subset of $\mathbb{N}$ including 0 and $f_{\mathcal{A}}(n)$ be the number of ways to write $n = \sum_{i=0}^{\infty} \epsilon_i 2^i$, where $\epsilon_i \in \mathcal{A}$. The sequence $(f_{\mathcal{A}}(n)) \bmod 2$ is always periodic, and $f_{\mathcal{A}}(n)$ is typically more often even than odd. We give four families of sets $(\mathcal{A}_m)$ with $|\mathcal{A}_m| = 4$ such that the proportion of odd $f_{\mathcal{A}_m}(n)$'s goes to 1 as $m \to \infty$. We also consider asymptotics of the summatory function $s_{\mathcal{A}}(r, m) = \sum_{n=m2^r}^{m2^{r+1}-1} f_{\mathcal{A}}(n)$ and show that $s_{\mathcal{A}}(r, m) \approx c(\mathcal{A}, m) \, |\mathcal{A}|^r$ for some $c(\mathcal{A}, m) \in \mathbb{Q}$.

To my sanity. May you continue to endure.

Acknowledgements

The author acknowledges support from National Science Foundation grant DMS 08-38434 "EMSW21-MCTP: Research Experience for Graduate Students" and also from the Illinois Campus Research Board and the Illinois Campus Cluster Program.

The author expresses appreciation to Joshua Cooper, Dennis Eichhorn, and Kevin O'Bryant for permission to adapt several diagrams from their paper *Reciprocals of binary power series*, [3].

The author also wishes to thank Professor Bruce Reznick for his time, ideas, and encouragement.

Table of Contents

Chapter 1

Introduction

1.1 Binary Representations

Every non-negative integer n has a unique standard binary representation and can be written as a sum of powers of 2 in the form

$$n = \sum_{i=0}^{\infty} \epsilon_i 2^i, \quad \epsilon_i \in \{0, 1\}.$$

If we let $f_{\{0,1\}}(n)$ denote the number of ways to write n in this fashion, then $f_{\{0,1\}}(n) = 1$ for all $n \geq 0$, as shown by Euler [5, pages 277–8].

Now consider instead the coefficient set $\{0, 1, 2\}$ and let $f_{\{0,1,2\}}(n)$ denote the number of ways to write n as

$$n = \sum_{i=0}^{\infty} \epsilon_i 2^i, \quad \epsilon_i \in \{0, 1, 2\}.$$

First note that while it is still possible to represent every non-negative integer in this fashion, the representation is no longer unique. For example, there are three ways to write $n = 4$ as $\sum \epsilon_i 2^i$ with $\epsilon_i \in \{0, 1, 2\}$, and they are

$$4 = 2 \cdot 1 + 1 \cdot 2 = 0 \cdot 1 + 0 \cdot 2 + 1 \cdot 2^2 = 0 \cdot 1 + 2 \cdot 2.$$

Reznick showed in [10] that when taking coefficients from the set $\{0, 1, 2\}$, the number of representations of $n - 1$ corresponds to the n^{th} term of the Stern sequence, which is defined recursively by $s(2n) = s(n)$ and $s(2n + 1) = s(n) + s(n + 1)$ with initial values $s(0) = 0$ and $s(1) = 1$. The Stern sequence can also be viewed as a diatomic array in which each row is formed by inserting the sum of consecutive terms between the terms of the previous row. This diatomic array is symmetric and is like a Pascal's triangle with memory. The first few rows of this infinite array are shown in Table 1.1

To generalize these ideas, let $\mathcal{A} = \{0 = a_0 < a_1 < \cdots < a_j\}$ denote a finite subset of $\mathbb{N}$ containing 0. We must include 0 to avoid summing infinitely many powers of 2. Let $f_{\mathcal{A}}(n)$ denote the number of ways to

															1		1															
															1	2	1															
														1	3	2	3	1														
												1	4	3	5	2	5	3	4	1												
								1	5	4	7	3	8	5	7	2	7	5	8	3	7	4	5	1								
1	6	5	9	4	11	7	10	3	11	8	13	5	12	7	9	2	9	7	12	5	13	8	11	3	10	7	11	4	9	5	6	1
...	14	11	19	8	21	13	18	5	17	12	19	7	16	9	11	2	11	9	16	7	19	12	17	5	18	13	21	8	19	11	14	...

Table 1.1: Stern diatomic array

write n in the form

$$n = \sum_{i=0}^{\infty} \epsilon_i 2^i, \quad \epsilon_i \in \mathcal{A}.$$

We associate to $\mathcal{A}$ its characteristic function $\chi_{\mathcal{A}}(n)$. The generating function for $\chi_{\mathcal{A}}(n)$ is

$$\phi_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} \chi_{\mathcal{A}}(n) x^n = \sum_{a \in \mathcal{A}} x^a = 1 + x^{a_1} + \cdots + x^{a_j}.$$

Since $\mathcal{A}$ is a finite set, $\phi_{\mathcal{A}}(x)$ is a polynomial in $\mathbb{F}_2[x]$. For example, we return to the specific cases discussed earlier and see that $\phi_{\{0,1\}}(x) = 1 + x$ and $\phi_{\{0,1,2\}}(x) = 1 + x + x^2$.

Denote the generating function of $f_{\mathcal{A}}(n)$ by

$$F_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} f_{\mathcal{A}}(n) x^n.$$

Then

$$F_{\{0,1\}}(x) = \sum_{n=0}^{\infty} x^n = 1 + x + x^2 + \cdots .$$

If we view the number of ways to write n as a partition problem, we obtain a product representation for $F_{\mathcal{A}}(x)$ as

$$F_{\mathcal{A}}(x) = \prod_{k=0}^{\infty} \left(1 + x^{a_1 2^k} + \cdots + x^{a_j 2^k}\right) = \prod_{k=0}^{\infty} \phi_{\mathcal{A}}(x^{2^k}). \tag{1.1}$$

1.2 Polynomials in $\mathbb{F}_2[x]$

This section follows Section 3.1 in [8], but we are only concerned with polynomials in $\mathbb{F}_2[x]$ rather than polynomials over more general finite fields.

Theorem 1.1 ([8, 3.1]). *Let $f \in \mathbb{F}_2[x]$ with $f(0) \neq 0$ and $\deg(f) = n \geq 1$. Then there exists $D \in \mathbb{Z}$ with $1 \leq D \leq 2^n - 1$ such that $f(x) \mid 1 + x^D$.*

The proof follows by considering the $2^n - 1$ nonzero residue classes in the residue class ring $\mathbb{F}_2[x]/(f)$ and the 2^n nonzero residue classes $x^j + (f)$ for $0 \leq j \leq 2^n - 1$ and applying the Pigeonhole Principle.

Definition 1.2 ([8, 3.2]). The least D that satisfies the conditions of Theorem 1.1 is called the *order* of f and is denoted $\mathrm{ord}(f(x)) = \mathrm{ord}(f)$.

Theorem 1.3 ([8, 3.3]). *Let $f \in \mathbb{F}_2[x]$ be an irreducible polynomial over $\mathbb{F}_2$ with $\deg(f) = n$ and $f(0) \neq 0$. Then $\mathrm{ord}(f)$ is equal to the order of any root of f in the multiplicative group $\mathbb{F}_{2^n}^*$.*

Corollary 1.4 ([8, 3.4]). *Let $f \in \mathbb{F}_2[x]$ be an irreducible polynomial over $\mathbb{F}_2$ with $\deg(f) = n$. Then $\mathrm{ord}(f) \mid 2^n - 1$.*

Consider $\phi_{\{0,1,3\}}(x) = 1+x+x^3$, which is irreducible over $\mathbb{F}_2$. By Corollary 1.4, we know ord $\left(\phi_{\{0,1,3\}}(x)\right)$ divides 7, and since 7 is prime, ord $\left(\phi_{\{0,1,3\}}(x)\right) = 7$. Similarly, the polynomial $\phi_{\{0,2,3\}}(x) = 1 + x^2 + x^3$ is irreducible over $\mathbb{F}_2$ with ord $\left(\phi_{\{0,2,3\}}(x)\right) = 7$. In fact, $1+x^7$ factors over $\mathbb{F}_2$ as $(1+x)(1+x+x^3)(1+x^2+x^3)$.

Theorem 1.5 ([8, 3.6]). *Let $c \in \mathbb{Z}$ with $c > 0$ and $f \in \mathbb{F}_2[x]$ with $f(0) \neq 0$. Then $f(x) \mid 1 + x^c$ if and only if $\mathrm{ord}(f) \mid c$.*

Theorem 1.6 ([8, 3.7]). *Let e_1 and e_2 be positive integers and $d = \gcd(e_1, e_2)$. Then $\gcd(1 + x^{e_1}, 1 + x^{e_2})$ in $\mathbb{F}_2[x]$ is $1 + x^d$.*

Theorem 1.7 ([8, 3.8]). *Let $g \in \mathbb{F}_2[x]$ be irreducible over $\mathbb{F}_2$ with $g(0) \neq 0$ and $\mathrm{ord}(g) = D$, and let $f = g^b$ for a positive integer b. Let t be the smallest integer with $2^t \geq b$. Then $\mathrm{ord}(f) = D2^t$.*

Theorem 1.8 ([8, 3.9]). *Let $f = g_1 \cdots g_k$, where $0 \neq g_1, \ldots, g_k$ and the g_i's are pairwise relatively prime over $\mathbb{F}_2$. Then $\mathrm{ord}(f) = \mathrm{lcm}\,(\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_k))$.*

Theorem 1.9 ([1, 2.1]). *Suppose $f \in \mathbb{F}_2[x]$, $f(0) \neq 0$, and f can be factored over $\mathbb{F}_2[x]$ as*

$$f = \prod_{i=1}^{s} g_i^{e_i},$$

where the g_i are distinct irreducible polynomials with $\deg(g_i) = d_i$. *Choose* $k \in \mathbb{N}$ *such that* $2^k \geq e_i$ *for all* i. *Let*

$$M := M(f) = 2^k \operatorname{lcm}\left(2^{d_1} - 1, \ldots, 2^{d_s} - 1\right).$$

Then $f(x) \mid 1 + x^M$.

Example 1.1 ([1, 4.3])**.** Consider $f(x) = 1 + x + x^4 + x^9 = (1 + x)^4(1 + x + x^2)(1 + x^2 + x^3)$. Then $g_1 = 1+x, d_1 = 1$, and $e_1 = 4$, while $g_2 = 1+x+x^2, d_2 = 2, e_2 = 1$, and $g_3 = 1+x^2+x^3, d_3 = 3$, and $e_3 = 1$. Let $k = 2$ so that $2^k \geq e_i$ for all i. Then $M = 2^2 \operatorname{lcm}\left(2^1 - 1, 2^2 - 1, 2^3 - 1\right) = 4 \operatorname{lcm}(1, 3, 7) = 4(21) = 84$. Hence $f(x) \mid 1+x^{84}$ and by Theorem 1.5, $\operatorname{ord}(f) \mid 84$. We can check to see that $f(x) \nmid 1+x^D$ for any proper divisor D of 84, so 84 is in fact $\operatorname{ord}(f)$.

Definition 1.10. For a polynomial $f(x)$ of degree n, the *reciprocal polynomial* of $f(x)$ is $f_{(R)}(x) := x^n f(1/x)$.

Theorem 1.11 ([8, 3.13])**.** *If* $\operatorname{ord}(f(x)) = D$, *then* $\operatorname{ord}\left(f_{(R)}(x)\right) = D$.

Definition 1.12 ([8, 3.15])**.** Let $f \in \mathbb{F}_2[x]$ with $\deg(f) = n \geq 1$. If f is the minimal polynomial over $\mathbb{F}_2$ of a primitive element of $\mathbb{F}_{2^n}$, then f is a *primitive polynomial* over $\mathbb{F}_2$.

Theorem 1.13 ([8, 3.16])**.** *Let* $f \in \mathbb{F}_2[x]$ *with* $\deg(f) = n$. *Then* f *is a primitive polynomial over* $\mathbb{F}_2$ *if and only if* $f(0) \neq 0$, f *is monic, and* $\operatorname{ord}(f) = 2^n - 1$.

Definition 1.14. [2] A *Mersenne prime* is a prime of the form $2^r - 1$. A *Mersenne exponent* is the exponent r of a Mersenne prime $2^r - 1$.

In [2] Brent and Zimmermann discuss their search for primitive trinomials in $\mathbb{F}_2[x]$ of large degree. They note that if $2^r - 1$ is prime, then any irreducible polynomial of degree r must be primitive. Thus they consider in their search trinomials of degree r where r is a Mersenne exponent. They also note the importance of trinomials over $\mathbb{F}_2[x]$ in cryptography and random number generation. We will not pursue this direction, but note that the polynomials $\phi_{\{0,1,3\}}(x)$ and $\phi_{\{0,2,3\}}(x)$ are primitive.

1.3 Known Results

Recall that for $\mathcal{A} = \{0 = a_0 < a_1 < \cdots < a_j\}$ a finite subset of $\mathbb{N}$ containing 0, $f_{\mathcal{A}}(n)$ denotes the number of ways to write n in the form

$$n = \sum_{k=0}^{\infty} \epsilon_k 2^k, \quad \epsilon_k \in \mathcal{A}.$$

In [1], Anders, Dennison, Lansing, and Reznick studied the behavior of the sequence $(f_{\mathcal{A}}(n))$ mod 2. Also recall the definitions of

$$\phi_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} \chi_{\mathcal{A}}(n)x^n = \sum_{a\in\mathcal{A}} x^a = 1 + x^{a_1} + \cdots + x^{a_j}$$

and the generating function for $f_{\mathcal{A}}(n)$,

$$F_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} f_{\mathcal{A}}(n)x^n = \prod_{k=0}^{\infty} \phi_{\mathcal{A}}(x^{2^k}).$$

Lemma 1.15 ([8, 1.46])**.** *For $a, b \in \mathbb{F}_2$ and $n \in \mathbb{N}$, $(a+b)^{2^n} = a^{2^n} + b^{2^n}$.*

From this lemma and Fermat's Little Theorem, it follows that for any polynomial $f \in \mathbb{F}_2[x]$,

$$f(x)^2 = f(x^2). \tag{1.2}$$

Theorem 1.16 ([1, 1.1])**.** *As elements of the formal power series ring $\mathbb{F}_2[[x]]$,*

$$\phi_{\mathcal{A}}(x)F_{\mathcal{A}}(x) = 1.$$

Hence $F_{\mathcal{A}}(x) \in \mathbb{F}_2(x)$.

Proof. By repeated use of (1.1) and (1.2),

$$\phi_{\mathcal{A}}(x)F_{\mathcal{A}}^2(x) \equiv \phi_{\mathcal{A}}(x)F_{\mathcal{A}}(x^2) = \phi_{\mathcal{A}}(x)\prod_{k=0}^{\infty}\phi_{\mathcal{A}}\left(x^{2^{k+1}}\right) = F_{\mathcal{A}}(x). \qquad \square$$

Returning to the coefficient set $\{0,1,2\}$ with $\phi_{\{0,1,2\}}(x) = 1 + x + x^2$, we see by Theorem 1.16 that in $\mathbb{F}_2[[x]]$,

$$\begin{aligned} F_{\{0,1,2\}}(x) &= \frac{1}{1+x+x^2} \\ &= \frac{1+x}{1+x^3} \\ &= (1+x)(1+x^3+x^6+\cdots) \\ &= 1 + x + x^3 + x^4 + x^6 + x^7 + \cdots . \end{aligned}$$

Dennison observed in [4] that $f_{\{0,1,3\}}(n)$ is periodic with least period 7 and each period has four odd terms, which occur when $n \equiv 0, 1, 2, 4 \pmod 7$. Recall from the discussion immediately following Corollary

1.4 that ord $\left(\phi_{\{0,1,3\}}(x)\right) = 7$. Using Theorem 1.16, we find that in $\mathbb{F}_2[[x]]$,

$$F_{\{0,1,3\}}(x) = \frac{1}{1+x+x^3} = \frac{1+x+x^2+x^4}{1+x^7}.$$

Note that the denominator of the last fraction is of the form $1+x^D$ with D being the least period of the sequence $\left(f_{\{0,1,3\}}(n)\right)$ and the order of $\phi_{\{0,1,3\}}(x)$. Also, the digits of the numerator are precisely the n for which $f_{\{0,1,3\}}(n)$ is odd.

Similarly, Dennison noted in [4] that $f_{\{0,2,3\}}(n)$ is periodic with least period 7 and each period has 4 odd terms, which occur when $n \equiv 0, 2, 3, 4 \pmod 7$. Using Theorem 1.16, we see that in $\mathbb{F}_2[[x]]$,

$$F_{\{0,2,3\}}(x) = \frac{1}{1+x^2+x^3} = \frac{1+x^2+x^3+x^4}{1+x^7}.$$

Again, note that the denominator of the last fraction is of the form $1+x^D$ with D being the least period of the sequence $\left(f_{\{0,2,3\}}(n)\right)$ and the order of $\phi_{\{0,2,3\}}(x)$. Also, the digits of the numerator are precisely the n for which $f_{\{0,2,3\}}(n)$ is odd.

Since $\mathcal{A}$ is finite, $\phi_{\mathcal{A}}(x)$ is a polynomial in $\mathbb{F}_2[x]$. Also recall that the *order* of $\phi_{\mathcal{A}}$ is the smallest integer D such that $\phi_{\mathcal{A}}(x) \mid 1+x^D$. Define $q_{\mathcal{A}}(x)$ by

$$\phi_{\mathcal{A}}(x) q_{\mathcal{A}}(x) = 1 + x^D.$$

In coding theory, if $\deg(\phi_{\mathcal{A}}) = d$ and $D = 2^d - 1$, $\phi_{\mathcal{A}}(x)$ is called the *generator polynomial*, while $q_{\mathcal{A}}(x)$ is called the *parity-check polynomial*, [8, page 484]. We do not pursue these here.

Now we have in $\mathbb{F}_2[x]$,

$$F_{\mathcal{A}}(x) = \frac{1}{\phi_{\mathcal{A}}(x)} = \frac{q_{\mathcal{A}}(x)}{1+x^D}.$$

If $q_{\mathcal{A}}(x) = \sum_{i=0}^{r} x^{b_i}$, where $0 = b_0 < b_1 < \cdots < b_r = D - \max\{a_i\}$, then

$$f_{\mathcal{A}}(n) \equiv 1 \bmod 2 \iff n \equiv b_i \bmod D \text{ for some } i.$$

Definition 1.17. For a polynomial $f(x) \in \mathbb{F}_2[x]$, define the *length* of $f(x)$ to be the number of monomials in $f(x)$. This can also be viewed as the number of terms in $f(x)$ with coefficient 1 and is denoted by $\ell_1(f(x))$.

Definition 1.18. For a polynomial $f(x) \in \mathbb{F}_2[x]$, let $\ell_{0,N}(f(x))$ denote the number of terms in $f(x)$ with coefficient 0 when $f(x)$ is viewed as a polynomial of degree N. Note that N may exceed d, the usual degree of $f(x)$, if we take all terms of the form x^k, where $k > d$, to have coefficient 0.

In [3], Cooper, Eichhorn, and O'Bryant defined sets A and B of natural numbers to be *reciprocals* if the number of ways to write an integer n as $n = a + b$, for $a \in A$ and $b \in B$, is 1 when $n = 0$ and is even when $n > 0$, so $\sum_{a\in A} x^a \cdot \sum_{b\in B} x^b = 1$ in $\mathbb{F}_2[x]$. They denote this reciprocal relationship by $\overline{A} = B$ and $\overline{B} = A$. The authors develop typical properties of reciprocals and study reciprocals of special sets.

Theorem 1.1 of [1] and Lemma 2.2(ii) of [3] are the same, but the relation to digital representations is only developed in [1].

Using the notation of [3], for a given positive integer n, let P_n denote the polynomial in $\mathbb{F}_2[x]$ whose exponents are the powers of 2 in the binary representation of n. This enumerates $\mathbb{F}_2[x]$. For example, $11 = [1011]_2$, so $P_{11}(x) = x^3 + x + 1$. If n is odd and D is the order of P_n, P_n^* is defined in [3] to be the polynomial such that $P_n P_n^* = 1 + x^D$ in $\mathbb{F}_2[x]$. If $n = 2^{a_j} + 2^{a_{j-1}} + \cdots + 2^{a_0}$ is odd, this corresponds to letting $\mathcal{A} = \{a_0, a_1, \ldots, a_j\}, P_n(x) = \phi_{\mathcal{A}}(x)$, and $P_n^*(x) = F_{\mathcal{A}}(x)(1 + x^D) = q_{\mathcal{A}}(x)$.

Cooper, Eichhorn, and O'Bryant considered the fraction $\delta\left(\overline{P}\right)$, and in our notation, letting $D = \text{ord}(P)$, we have

$$\delta\left(\overline{P}\right) = \frac{\ell_1\left(P^*\right)}{D}. \tag{1.3}$$

We also considered the fraction $\ell_1(P^*)/D$ in [1], but here we instead consider the ordered pair

$$\beta(P_n) := (\ell_1(P_n^*), \ell_{0,D-1}(P_n^*)), \tag{1.4}$$

which gives more precise information than reduced fractions. In this pair, the first coordinate represents the number of times $f_{\mathcal{A}}(n)$ is odd in a minimal period D, and the second coordinate represents the number of times $f_{\mathcal{A}}(n)$ is even in a minimal period.

Definition 1.19. We call a polynomial $f(x)$ *robust* if the first coordinate of $\beta(f(x))$ exceeds the second coordinate by more than one, so $\ell_1(f^*(x)) > \ell_{0,D-1}(f^*(x)) + 1$, where D is the order of $f(x)$. This is equivalent to saying that $\ell_1(f^*(x)) > (D+1)/2$.

Remark 1.1. Suppose $f(x)$ is not robust. If $\beta(f(x)) = (1, 0)$, then $\frac{\ell_1(f^*(x))}{\text{order}(f(x))} = 1$. Otherwise, $\beta(f(x))$ is of the form (a, b), where $b \geq 1$ and $a \leq b + 1$. Let $\theta(x) = \frac{x}{x+1}$. Note that $\theta(x)$ is increasing for $x \geq 0$ and

$$\frac{a}{a+b} = \frac{\frac{a}{b}}{\frac{a}{b}+1} = \theta\left(\frac{a}{b}\right).$$

Since $\frac{a}{b} \leq \frac{b+1}{b} = 1 + \frac{1}{b} \leq 2$, it follows that

$$\frac{\ell_1(f^*(x))}{\text{order}(f(x))} = \frac{a}{a+b} = \theta\left(\frac{a}{b}\right) \leq \theta(2) = \frac{2}{3}.$$

n	ord(P_n)	$\delta\left(\overline{P}_n\right)$	n	ord(P_n)	$\delta\left(\overline{P}_n\right)$	n	ord(P_n)	$\delta\left(\overline{P}_n\right)$	n	ord(P_n)	$\delta\left(\overline{P}_n\right)$
1	1	1	65	6	1/6	129	7	1/7	193	127	64/127
3	1	1	67	63	32/63	131	127	64/127	195	12	1/2
5	2	1/2	69	14	2/7	133	93	46/93	197	63	31/63
7	3	2/3	71	31	15/31	135	60	1/2	199	105	52/105
9	3	1/3	73	9	2/9	137	127	64/127	201	62	1/2
11	7	4/7	75	28	1/2	139	15	1/3	203	127	64/127
13	7	4/7	77	31	15/31	141	62	1/2	205	93	46/93
15	4	1/2	79	15	2/5	143	127	64/127	207	14	3/7
17	4	1/4	81	14	2/7	145	127	64/127	209	15	1/3
19	15	8/15	83	21	11/21	147	62	1/2	211	127	64/127
21	6	1/3	85	8	1/4	149	63	31/63	213	127	64/127
23	7	3/7	87	21	8/21	151	42	10/21	215	62	1/2
25	15	8/15	89	31	15/31	153	24	1/2	217	35	18/35
27	6	1/2	91	63	32/63	155	35	18/35	219	9	1/3
29	7	3/7	93	15	2/5	157	127	64/127	221	28	13/28
31	5	2/5	95	30	1/2	159	21	3/7	223	93	46/93
33	5	1/5	97	63	32/63	161	93	46/93	225	60	1/2
35	21	10/21	99	10	1/2	163	63	31/63	227	105	52/105
37	31	16/31	101	21	11/21	165	20	1/2	229	127	64/127
39	14	1/2	103	63	32/63	167	127	64/127	231	15	7/15
41	31	16/31	105	28	1/2	169	63	31/63	233	42	10/21
43	15	7/15	107	12	1/2	171	127	64/127	235	62	1/2
45	12	1/2	109	63	32/63	173	105	52/105	237	63	31/63
47	31	16/31	111	31	15/31	175	42	1/2	239	127	64/127
49	21	10/21	113	31	15/31	177	62	1/2	241	127	64/127
51	8	1/2	115	63	32/63	179	93	46/93	243	14	3/7
53	15	7/15	117	21	8/21	181	105	52/105	245	42	1/2
55	31	16/31	119	12	5/12	183	63	31/63	247	127	64/127
57	14	1/2	121	15	2/5	185	127	64/127	249	21	3/7
59	31	16/31	123	31	15/31	187	28	13/28	251	93	46/93
61	31	16/31	125	30	1/2	189	12	1/3	253	127	64/127
63	6	1/3	127	7	2/7	191	127	64/127	255	8	1/4

Table 1.2: Properties of P_n for odd $n < 2^8$, modified from [3]

Hence if $\frac{\ell_1(f^*(x))}{\text{order}(f(x))} > 2/3$, then $f(x)$ is robust.

In section four of [3], the authors state, "The most interesting issued raised in this section, which remains unanswered, is to describe the set $\{\delta\left(\overline{P}\right) : P \text{ is a polynomial}\}$. For example, is there an n with $\delta\left(\overline{P_n}\right) = 3/4$?" They also computed $\delta\left(\overline{P_n}\right)$ for $n < 2^8$ and found that none of the P_n in this range are robust. Table 1.2, taken and adjusted from [3] with permission, records properties of P_n for odd $n < 256$.

Figures 1.1 and 1.2 were also taken from [3] with permission. Figure 1.1 gives a dot plot of all points of the form $\left(n, \delta\left(\overline{P}_n\right)\right)$ for n odd and less than 2^{12}. The points are tightly clustered around 1/2, but when they stray from 1/2, there is a strong propensity to be smaller than 1/2 rather than greater. Note the four points near the top represented by boxes. We will explain and generalize these robust polynomials in Chapter 3.

Figure 1.2 is a plot of the empirical distribution function of $\delta\left(\overline{P_n}\right)$. Cooper, Eichhorn, and O'Bryant

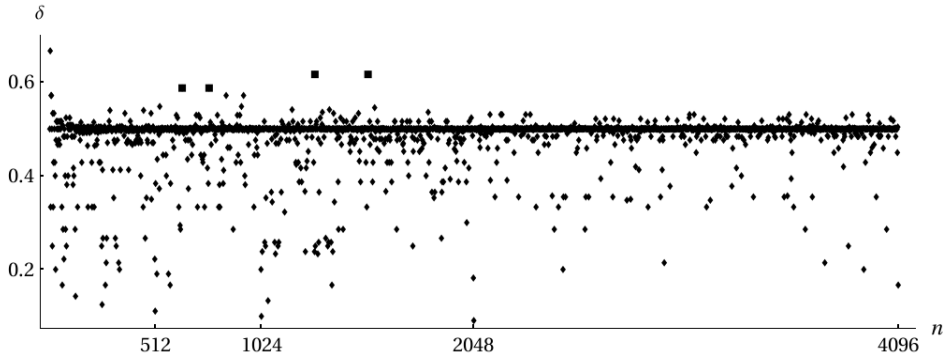

Figure 1.1: The points $\left(n, \delta\left(\overline{P}_n\right)\right)$ with n odd, except $(1,0)$ and $(3,1)$, taken from [3]

noted that the large discontinuities near $1/2$ mean that these densities occur with large frequency, and we can again see the tendency for $\delta\left(\overline{P}\right)$ to be smaller than $1/2$ rather than greater. The authors also point out that of the 2048 polynomials P_i with i odd and $1 \leq i \leq 4095$, there are 421 which have reciprocals with density exactly $1/2$.

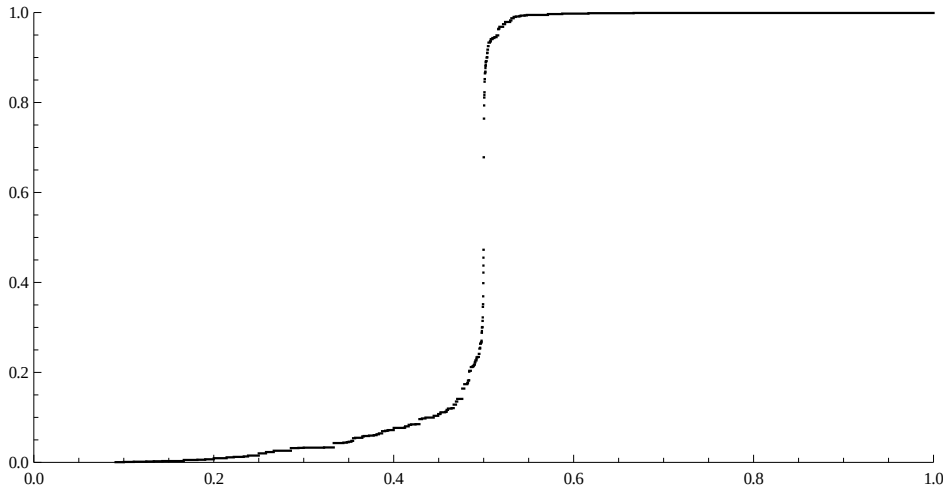

Figure 1.2: The distribution function $\Delta(x) := 2^{-11} \cdot \#\{n : 1 \leq n \leq 2^{12}, n \text{ odd}, \delta\left(\overline{P}_n\right) \leq x\}$, taken from [3]

Recall the aforementioned quote from [3], "The most interesting issued raised in this section, which remains unanswered, is to describe the set $\{\delta\left(\overline{P}\right) : P \text{ is a polynomial}\}$". Since $1 + x^D$ has order D and $\delta\left(\overline{1 + x^D}\right) = 1/D$, the lower bound of the set in question is 0. We shall exhibit in Chapter 3 four sequences $\{f_n\}$ of polynomials such that $\lim_{n\to\infty} \delta\left(\overline{f_n}\right) = 1$, thus establishing a least upper bound for the set.

First, however, we discuss in Chapter 2 background material on linear recurrence sequences over $\mathbb{F}_2$ and their relation to polynomials over $\mathbb{F}_2$. Section 2.1 establishes preliminary results on homogeneous k-th order linear recurring sequences in $\mathbb{F}_2$ and their generating functions. Section 2.2 introduces impulse response

sequences and characteristic polynomials of linear recurrence sequences. We explore the connections between the period of a sequence and the order of its characteristic polynomial, and these connections allow us to present an upper bound given in [8] for the difference in the coordinates of $\beta(f(x))$, the ordered pair defined in (1.4).

In Chapter 3 we present four sequences of robust polynomials and consider specific examples from those sequences. We also expound on the methods used to collect data in the search for robust polynomials.

Theorem. The polynomials $f_{r,1}(x) = 1 + x + x^{2^r-1} + x^{2^r+1}$ are robust with order dividing $4^r - 1$. If $h_{r,1}(x) = \left(1 + x^{4^r-1}\right)/f_{r,1}(x)$, then $\lim_{r\to\infty} \ell_1\left(h_{r,1}(x)\right)/\left(4^r-1\right) = 1$.

Corollary. The reciprocal polynomials $f_{(R),r,1}(x) = 1 + x^2 + x^{2^r} + x^{2^r+1}$ are robust with order dividing $4^r - 1$. If $h_{(R),r,1}(x) = \left(1 + x^{4^r-1}\right)/f_{(R),r,1}(x)$, then $\lim_{r\to\infty} \ell_1\left(h_{(R),r,1}(x)\right)/\left(4^r-1\right) = 1$.

Theorem. The reciprocal polynomials $f_{r,2}(x) = 1+x+x^{2^r}+x^{2^r+2}$ are robust with order dividing 4^r+2^r+1. If $h_{r,2}(x) = \left(1 + x^{4^r+2^r+1}\right)/f_{r,2}(x)$, then $\lim_{r\to\infty} \ell_1\left(h_{r,2}(x)\right)/\left(4^r+2^r+1\right) = 1$.

Corollary. The reciprocal polynomials $f_{(R),r,2}(x) = 1 + x^2 + x^{2^r+1} + x^{2^r+2}$ are robust with order dividing $4^r + 2^r + 1$. If $h_{(R),r,2}(x) = \left(1 + x^{4^r+2^r+1}\right)/f_{(R),r,2}(x)$, then $\lim_{r\to\infty} \ell_1\left(h_{(R),r,2}(x)\right)/\left(4^r+2^r+1\right) = 1$.

Chapter 4 develops asymptotics of the summatory function $s(\mathcal{A}, m) = \sum_{n=m2^r}^{m2^{r+1}-1} f_{\mathcal{A}}(n)$.

Theorem. Fix $\mathcal{A}, r$, and m. Then $s_{\mathcal{A}}(r, m) \approx c(\mathcal{A}, m)\,|\mathcal{A}|^r$ for some $c(\mathcal{A}, m) \in \mathbb{Q}$.

Chapter 5 is a discussion of open questions on these problems and areas for future work.

Appendix A contains samples of the Mathematica code used in determining $\beta(f(x))$ for all polynomials $f(x) \in \mathbb{F}_2[x]$ with $\mathrm{ord}(f(x)) \leq 83$ and tables with information on all robust polynomials in that range. Appendix B contains samples of the Mathematica code used in determining $\beta(f(x))$ for all quadrinomials $f(x) \in \mathbb{F}_2[x]$ with $\deg(f(x)) \leq 18$ and tables with information about robust quadrinomials.

Chapter 2

Linear Recurrence Sequences over $\mathbb{F}_2$

In this chapter, we explore the strong connections between polynomials over $\mathbb{F}_2$ and linear recurrence sequences.

2.1 Preliminaries

This section follows Section 8.1 of [8] with results again restricted to $\mathbb{F}_2$ rather than the general $\mathbb{F}_q$.

Let k be an integer and $a_0, \ldots, a_{k-1}$ elements of $\mathbb{F}_2$. If (s_n) is a sequence of elements of $\mathbb{F}_2$ such that

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n \tag{2.1}$$

for all $n \geq 0$, then (s_n) is a *homogeneous k-th order linear recurrence sequence* in $\mathbb{F}_2$. The sequence is uniquely determined by the *initial values* $s_0, s_1, \ldots, s_{k-1}$. The relation (2.1) is a *k-th order linear recurrence relation.*

We associate to (s_n) its generating function $S(x)$ defined by

$$S(x) = \sum_{n=0}^{\infty} s_n x^n.$$

Note that $S(x) \in \mathbb{F}_2[[x]]$. If there exists an M such that for all $n \geq M$, $s_n = 0$, then $S(x) \in \mathbb{F}_2[x]$.

A sequence (s_n) is *ultimately periodic* if there exist integers $N \geq 0$ and $T \geq 1$ such that for any $n \geq N$, $s_{n+T} = s_n$. Then T is called a *period* of the sequence, and the *least period* of an ultimately periodic sequence is the smallest such T. Additionally, N is the *preperiod* of the sequence (s_n), and if $N = 0$, the sequence is *periodic.* If (s_n) is an ultimately periodic sequence of elements in $\mathbb{F}_2$, then $\{n : s_n = 1\}$ is ultimately periodic. This is equivalent to $S(x)$ being a rational function [1, Lemma 2.3].

Consider the product

$$S(x)\left(1 + a_{k-1}x + \cdots + a_0 x^k\right). \tag{2.2}$$

The integer k is already fixed by the order of the recurrence relation. Now fix an integer $n \geq 0$. The term x^{n+k} will have coefficient

$$s_n a_0 + s_{n+1} a_1 + s_{n+2} a_2 + \cdots + s_{n+k-1} a_{k-1} + s_{n+k}.$$

By (2.1) this coefficient is equal to $2s_{n+k} \equiv 0$, so the product $S(x)\left(1 + a_{k-1}x + \cdots + a_0 x^k\right)$ is a polynomial in $\mathbb{F}_2[x]$ of degree less than k.

Lemma 2.1 ([8, 8.4])**.** *Let (s_n) be an ultimately periodic sequence with least period T. If R is a period of (s_n), then $T \mid R$.*

Theorem 2.2 ([8, 8.7])**.** *For a fixed positive integer k, every k-th order homogeneous linear recurrence sequence in $\mathbb{F}_2$ is ultimately periodic with least period $T \leq 2^k - 1$.*

Example 2.1. Consider the sequence (s_n) which has third order homogeneous linear recurrence relation

$$s_{n+3} = s_n + s_{n+1}$$

with initial conditions $s_0 = 1, s_1 = 0$, and $s_2 = 1$. Computing values, we see

$$(s_n) = (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, \ldots),$$

and the sequence is periodic with least period $7 = 2^3 - 1$. Other possible periods include $14, 21$, and 28.

Turning to the generating function,

$$\begin{aligned} S(x) &= \sum_{n=0}^{\infty} s_n x^n \\ &= 1 + x^2 + x^3 + x^4 + x^7 + x^9 + x^{10} + x^{11} + x^{14} + x^{16} + x^{17} + x^{18} + x^{21} + \cdots \\ &= \left(1 + x^2 + x^3 + x^4\right)\left(1 + x^7 + x^{14} + \cdots\right) \\ &= \frac{1 + x^2 + x^3 + x^4}{1 + x^7} \in \mathbb{F}_2[[x]]. \end{aligned} \tag{2.3}$$

Similarly, we can illustrate the period of 14 by writing

$$\begin{aligned} S(x) &= \left(1 + x^2 + x^3 + x^4 + x^7 + x^9 + x^{10} + x^{11}\right)\left(1 + x^{14} + x^{28} + \cdots\right) \\ &= \frac{1 + x^2 + x^3 + x^4 + x^7 + x^9 + x^{10} + x^{11}}{1 + x^{14}}. \end{aligned} \tag{2.4}$$

To highlight the connection between (2.3) and (2.4), note that (2.4) can be written as $\frac{(1+x^2+x^3+x^4)(1+x^7)}{(1+x^7)(1+x^7)}$.

Example 2.2. Consider the sequence (s_n) satisfying

$$s_{n+3} = s_{n+2}$$

with initial conditions $s_0 = 0, s_1 = 0$, and $s_2 = 1$. This sequence is $(s_n) = (0, 0, 1, 1, 1, \ldots)$ and is ultimately periodic but is not periodic. Here $S(x) = x^2 + x^3 + x^4 + \cdots = \frac{x^2}{1+x}$.

We will now see a condition under which a sequence must be periodic.

Theorem 2.3 ([8, 8.11])**.** *If (s_n) is a linear recurrence sequence in $\mathbb{F}_2$ satisfying* (2.1) *with the coefficient $a_0 = 1$, then (s_n) is a periodic sequence.*

Let (s_n) be a k-th order homogeneous linear recurrence sequence in $\mathbb{F}_2$ satisfying (2.1) for $n \geq 0$. We associate to this sequence the $k \times k$ matrix A over $\mathbb{F}_2$ given by

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-2} & a_{k-1} \end{pmatrix}. \tag{2.5}$$

If $k = 1$, we take A to be the 1×1 matrix (a_0). Note that A depends only on the recurrence relation of the sequence and not the initial values.

Definition 2.4. The *general linear group* $\mathrm{GL}(k, \mathbb{F}_2)$ is the group comprised of all $k \times k$ matrices with entries in $\mathbb{F}_2$ and nonzero determinant.

Definition 2.5. For a linear recurrence sequence satisfying (2.1), the column vector $\mathbf{s_n} = (s_n, s_{n+1}, \ldots, s_{n+k-1})$ is the *n-th state vector* of the linear recurrence sequence. The state vector $\mathbf{s_0} = (s_0, s_1, \ldots, s_{k-1})$ is the *initial state vector*.

For the third order linear recurrence relation in Example 2.1, $\mathbf{s_0} = (1, 0, 1)$ and $\mathbf{s_3} = (1, 1, 0)$.

Lemma 2.6 ([8, 8.12])**.** *Let (s_n) be a k-th order homogeneous linear recurrence sequence satisfying* (2.1) *with associated matrix A as in* (2.5)*. Then the state vectors of the sequence satisfy*

$$\mathbf{s_n} = A^n \mathbf{s_0} \quad \textit{for all } n \geq 0.$$

Theorem 2.7 ([8, 8.13]). *If (s_n) is a k-th order homogeneous linear recurrence sequence in $\mathbb{F}_2$ satisfying* (2.1) *with $a_0 = 1$ and associated matrix A as given in* (2.5)*, then the least period of (s_n) divides the order of A in the general linear group* $\mathrm{GL}(k, \mathbb{F}_2)$.

2.2 Orders

This section follows Sections 8.2, 8.3, and 8.4 of [8].

Given a k-th order homogeneous linear recurrence relation in $\mathbb{F}_2$, there are 2^k sequences (s_n) satisfying this relation, with each sequence uniquely determined by its initial values $s_0, s_1, \ldots, s_{k-1}$. Which of these sequences will have the maximal least period?

Definition 2.8 ([8, p.402]). Consider the sequence (d_n) which satisfies (2.1), so

$$d_{n+k} = a_{k-1}d_{n+k-1} + a_{k-2}d_{n+k-2} + \cdots + a_0 d_n, \tag{2.6}$$

and has initial values $d_0 = d_1 = \cdots = d_{k-2} = 0, d_{k-1} = 1$. This is called the *impulse response sequence* for the family of sequences satisfying (2.1).

We know from (2.2) and the discussion immediately following that for the generating function $D(x)$ of the sequence (d_n), $D(x)\left(1 + a_{k-1}x + \cdots + a_0 x^k\right)$ is a polynomial of degree less than k. Because of the initial conditions on the sequence, the only nonzero term with exponent less than k is x^{k-1}. Hence $D(x)$ is the rational function

$$D(x) = \frac{x^{k-1}}{1 + a_{k-1}x + \cdots + a_0 x^k}. \tag{2.7}$$

Example 2.3. Let (s_n) be a sequence in $\mathbb{F}_2$ satisfying

$$s_{n+3} = s_{n+2} + s_n \tag{2.8}$$

with initial values $s_0 = s_1 = 0$ and $s_2 = 1$. Then $(s_n) = (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, \ldots)$, has least period 7, and is the impulse response sequence (d_n) for the family of sequences satisfying (2.8).

The generating function is

$$\begin{aligned} S(x) &= x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} + x^{11} + x^{13} + x^{16} + x^{17} + x^{18} + x^{20} + x^{23} + \cdots \\ &= \left(1 + x + x^2 + x^4\right)\left(x^2 + x^9 + x^{16} + \cdots\right) \\ &= \left(1 + x + x^2 + x^4\right) x^2 \left(1 + x^7 + x^{14} + \cdots\right) \\ &= \frac{x^2\left(1 + x + x^2 + x^4\right)}{1 + x^7} \\ &= \frac{x^2}{1 + x + x^3}. \end{aligned}$$

Lemma 2.9 ([8, 8.15])**.** *Let (d_n) be the impulse response sequence satisfying* (2.6) *and A be the matrix in* (2.5)*. The state vectors $\mathbf{d_m}$ and $\mathbf{d_n}$ are equal if and only if $A^m = A^n$.*

Theorem 2.10 ([8, 8.16])**.** *Let (s_n) be a homogeneous linear recurrence sequence in $\mathbb{F}_2$ and (d_n) be the corresponding impulse response sequence. Then the least period of (s_n) divides the least period of (d_n).*

Example 2.4. Consider the fourth order homogeneous linear recurrence relation

$$s_{n+4} = s_{n+2} + s_n.$$

The sequence (s_n) that satisfies this relation and has initial values $s_0 = 0$, $s_1 = s_2 = 1$, and $s_3 = 0$ is $(s_n) = (0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots)$, which has least period 3. The corresponding impulse response sequence $(d_n) = (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, \ldots)$ has least period 6. Note that the least period of (s_n) divides the least period of (d_n).

Let $S(x)$ and $D(x)$ denote the generating functions of (s_n) and (d_n), respectively. Then

$$\begin{aligned} S(x) &= x + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + \cdots \\ &= x(1 + x) + x^4(1 + x) + x^7(1 + x) + x^{10}(1 + x) + \cdots \\ &= (1 + x)\left(x + x^4 + x^7 + x^{10} + \cdots\right) \\ &= \frac{x(1 + x)}{1 + x^3} \end{aligned}$$

and

$$\begin{aligned} D(x) &= x^3 + x^5 + x^9 + x^{11} + x^{15} + x^{17} + \cdots \\ &= x^3(1+x^2) + x^9(1+x^2) + x^{15}(1+x^2) + \cdots \\ &= (1+x^2)\left(x^3 + x^9 + x^{15} + \cdots\right) \\ &= \frac{x^3(1+x^2)}{1+x^6}. \end{aligned}$$

To highlight the connection between $S(x)$ and $D(x)$, note that $S(x) = \frac{x(1+x)(1+x^3)}{1+x^6}$.

Theorem 2.11 ([8, 8.17])**.** *Let (d_n) be the impulse response sequence in $\mathbb{F}_2$ satisfying (2.6) with $a_0 \neq 0$ and A the matrix in (2.5). Then the least period of (d_n) is equal to the order of A in the general linear group* $\mathrm{GL}(k, \mathbb{F}_2)$.

Example 2.5. Recall the fourth order impulse response sequence (d_n) of Example 2.4 which has least period 6. The corresponding matrix A is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

and the order of A in $\mathrm{GL}(4, \mathbb{F}_2)$ is 6.

We know that an impulse response sequence will have maximal least period. We will now see another condition under which a sequence has maximal least period.

Theorem 2.12 ([8, 8.19])**.** *Let (s_n) be a k-th order homogeneous linear recurrence sequence in $\mathbb{F}_2$ with preperiod n_0. If there exist k state vectors $\mathbf{s_{m_1}}, \mathbf{s_{m_2}}, \ldots, \mathbf{s_{m_k}}$ with $m_j \geq n_0$ for all $1 \leq j \leq k$, that are linearly independent over $\mathbb{F}_2$, then both (s_n) and its corresponding impulse response sequence (d_n) are periodic, and they have the same least period.*

Definition 2.13 ([8, p. 404])**.** Let (s_n) be a k-th order homogeneous linear recurrence sequence in $\mathbb{F}_2$ satisfying (2.1) with $a_j \in \mathbb{F}_2$ for $0 \leq j \leq k-1$. The *characteristic polynomial* of the sequence is

$$f(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0 \in \mathbb{F}_2[x]. \tag{2.9}$$

Note that the characteristic polynomial depends only on the recurrence relation and not on the initial conditions. Hence there are 2^k distinct sequences in $\mathbb{F}_2$ with the same characteristic polynomial.

Definition 2.14 ([8, p. 404])**.** Let A be the $k \times k$ matrix in (2.5) and I be the $k \times k$ identity matrix over $\mathbb{F}_2$. The *characteristic polynomial* of A is $f(x) = \det(xI - A)$. The matrix A is known as the *companion matrix* of $f(x)$.

The characteristic polynomial of the linear recurrence sequence and the characteristic polynomial of the corresponding matrix are the same.

Example 2.6. Consider the fourth order homogeneous recurrence relation $s_{n+4} = s_{n+2} + s_n$ from Examples 2.4 and 2.5. The characteristic polynomial of (s_n) is $f(x) = x^4 + x^2 + 1$, and the characteristic polynomial of the matrix A is also $f(x) = x^4 + x^2 + 1$.

Recall Definition 1.2, the definition of the order of a polynomial in $\mathbb{F}_2$. We will now state the connection between the order of the characteristic polynomial of a sequence and the order of the corresponding matrix.

Lemma 2.15 ([8, 8.26])**.** *Let $f(x)$ be as in Definition 2.13 with $k \geq 1$ and $a_0 = 1$ and A be the matrix in* (2.5)*. Then the order of $f(x)$ is equal to the order of A in the general linear group* $\mathrm{GL}(k, \mathbb{F}_2)$*.*

Recall the set-up of Examples 2.4 and 2.5. The order of $f(x)$ is 6, and the order of the matrix A is 6.

Now we explore the relationship between the least period of a sequence and the order of its characteristic polynomial.

Theorem 2.16 ([8, 8.27])**.** *Let (s_n) be a homogeneous linear recurrence sequence in $\mathbb{F}_2$ with characteristic polynomial $f(x) \in \mathbb{F}_2[x]$ and corresponding impulse response sequence (d_n). The least period of (s_n) divides the order of $f(x)$, and the least period of (d_n) equals the order of $f(x)$. If $a_0 = 1$, then both (s_n) and (d_n) are periodic.*

Consider generating functions in the case where $a_0 = 1$, so both (s_n) and (d_n) are periodic. Letting N and M denote the least periods of (s_n) and (d_n), respectively, there exist some $g(x), h(x)$ in $\mathbb{F}_2[x]$ such that

$$S(x) = \frac{g(x)}{1 + x^N} \qquad \text{and} \qquad D(x) = \frac{h(x)}{1 + x^M},$$

where $S(x)$ is the generating function of (s_n) and $D(x)$ is the generating function of (d_n).

By Theorem 2.10, $N \mid M$, so $1 + x^N \mid 1 + x^M \in \mathbb{F}_2[x]$. Hence there exists $j(x) \in \mathbb{F}_2[x]$ such that $\left(1 + x^N\right) j(x) = 1 + x^M$, and thus

$$D(x) = \frac{h(x)}{j(x)\left(1 + x^N\right)}.$$

Example 2.7. Recall that in Example 2.4, we considered the fourth order homogeneous linear recurrence relation $s_{n+4} = s_{n+2} + s_n$ and gave (s_n) initial values $s_0 = 0, s_1 = s_2 = 1$ and let (d_n) be the corresponding

impulse response sequence. The least period of (s_n) was 3, and the least period of (d_n) was 6. Since $\text{ord}(x^4 + x^2 + 1) = 6$, we see that indeed the least period of (s_n) divides $\text{ord}(f(x))$, and the least period of (d_n) equals $\text{ord}(f(x))$.

In Example 2.4 we had

$$S(x) = \frac{x(1+x)}{1+x^3} \qquad \text{and} \qquad D(x) = \frac{x^3(1+x^2)}{1+x^6}.$$

Note that we can rewrite $D(x)$ in $\mathbb{F}_2[x]$ as

$$D(x) = \frac{x^3(1+x^2)}{(1+x^3)(1+x^3)}.$$

Next we state a condition under which the least period of a sequence (s_n) is equal to the order of its characteristic polynomial.

Theorem 2.17 ([8, 8.28])**.** *Let (s_n) be a homogeneous linear recurrence sequence in $\mathbb{F}_2$ with $\mathbf{s}_0 \neq \mathbf{0}$. Suppose the characteristic polynomial $f(x)$ of (s_n) is irreducible over $\mathbb{F}_2$ with $f(0) \neq 0$. Then (s_n) is periodic, and the least period of (s_n) is equal to the order of $f(x)$.*

Example 2.8. Consider the third order homogeneous linear recurrence sequence in $\mathbb{F}_2$ given by $s_{n+3} = s_{n+1} + s_n$ with initial values $s_0 = 1, s_1 = 0$, and $s_2 = 1$. The least period of (s_n) is 7, and the characteristic polynomial $f(x) = x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and has order 7.

According to Theorem 2.2, the least period r of a k-th order homogeneous linear recurrence sequence satisfies $r \leq 2^k - 1$. Now we will consider sequences for which $r = 2^k - 1$.

Definition 2.18 ([8, 8.32])**.** Let (s_n) be a homogeneous linear recurrence sequence in $\mathbb{F}_2$ with characteristic polynomial $f(x)$. If $\mathbf{s}_0 \neq \mathbf{0}$ and $f(x)$ is a primitive polynomial over $\mathbb{F}_2$, then (s_n) is a *maximal period sequence* in $\mathbb{F}_2$.

Theorem 2.19 ([8, 8.33])**.** *Let (s_n) be a k-th order maximal period sequence in $\mathbb{F}_2$. Then (s_n) is periodic with least period r satisfying $r = 2^k - 1$.*

Any linear recurrence sequence satisfies multiple linear recurrence relations. Consider a sequence (s_n) which has least period r. Then, for all n sufficiently large, (s_n) satisfies $s_{n+r} = s_n$, but it also satisfies $s_{n+2r} = s_n$ and $s_{n+3r} = s_n$, and in fact, $s_{n+ir} = s_n$ for all $i \geq 0$. The next theorem illustrates the connection between different linear recurrence relations satisfied by the same sequence.

Theorem 2.20 ([8, 8.42]). *Let (s_n) be a homogeneous linear recurrence sequence in $\mathbb{F}_2$. Then there exists a uniquely determined monic polynomial $m(x) \in \mathbb{F}_2[x]$ such that a monic polynomial $f(x) \in \mathbb{F}_2[x]$ of positive degree is a characteristic polynomial of (s_n) if and only if $m(x)$ divides $f(x)$.*

Recall the definition of a reciprocal polynomial given in Definition 1.10. Suppose (s_n) satisfies (2.1) and let $f(x)$ denote the characteristic polynomial of this recurrence relation. We know from (2.2) that $S(x)$ is a rational function of the form

$$S(x) = \frac{p(x)}{1 + a_{k-1}x + \cdots + a_0x^k} = \frac{p(x)}{f_{(R)}(x)}$$

for some $p(x) \in \mathbb{F}_2[x]$. The sequence (s_n) satisfies another recurrence with characteristic polynomial $g(x)$ if and only if $S(x)g_{(R)}(x)$ is a polynomial.

The polynomial $m(x)$ of Theorem 2.20 is the *minimal polynomial* of the sequence (s_n). If (s_n) is the constant sequence all of whose terms are zero, $m(x) = 1$. Otherwise, the degree of $m(x)$ is positive, and $m(x)$ is the characteristic polynomial of the recurrence relation of least order satisfied by (s_n).

Theorem 2.21 ([8, 8.44]). *If (s_n) is a homogeneous linear recurrence sequence in $\mathbb{F}_2$ with least period r and minimal polynomial $m(x) \in \mathbb{F}_2[x]$, then $r = \mathrm{ord}(m(x))$.*

Theorem 2.22 ([8, 8.50]). *Let $f(x)$ be a monic polynomial in $\mathbb{F}_2[x]$ which is irreducible over $\mathbb{F}_2$. Let (s_n) be a homogeneous linear recurrence sequence in $\mathbb{F}_2$ which is not the constant sequence with all terms zero. If $f(x)$ is a characteristic polynomial of (s_n), then $f(x)$ is the minimal polynomial of (s_n).*

Theorem 2.23 ([8, 8.51]). *Let (s_n) be a sequence in $\mathbb{F}_2$ satisfying a k-th order homogeneous linear recurrence relation with characteristic polynomial $f(x) \in \mathbb{F}_2[x]$. Then $f(x)$ is the minimal polynomial of (s_n) if and only if the state vectors $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{k-1}$ are linearly independent over $\mathbb{F}_2$.*

Corollary 2.24 ([8, 8.52]). *Given a homogeneous linear recurrence relation in $\mathbb{F}_2$ with impulse response sequence (d_n), the minimal polynomial of (d_n) is the characteristic polynomial of the recurrence relation.*

Suppose (d_n) is a k-th order impulse response sequence satisfying (2.6) with generating function $D(x)$ and characteristic polynomial

$$f(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1x + a_0,$$

where $a_0 = 1$ so $f(0) \neq 0$. Let $M = \mathrm{ord}(f(x))$ so that $f(x)f^*(x) = 1 + x^M$. Then $f_{(R)}(x)f^*_{(R)}(x) = 1 + x^M$, and, in fact, $\left(f_{(R)}\right)^*(x) = (f^*)_{(R)}(x)$, as we will show in Lemma 3.5, so there is no ambiguity in writing $f^*_{(R)}(x)$.

Recall from Equation (2.7) that

$$D(x) = \frac{x^{k-1}}{1 + a_{k-1}x + \cdots + a_0 x^k} = \frac{x^{k-1}}{f_{(R)}(x)}.$$

Since $f_{(R)}(x) = \frac{1+x^M}{f^*_{(R)}(x)}$, we have

$$D(x) = \frac{x^{k-1} f^*_{(R)}(x)}{1 + x^M}. \tag{2.10}$$

Because (d_n) is an impulse response sequence and the constant term of $f(x)$ is 1, we know from Theorem 2.16 that (d_n) is periodic and with least period equal to M, the order of $f(x)$. Since $f_{(R)}(x) f^*_{(R)}(x) = 1 + x^M$ and $\deg\left(f_{(R)}(x)\right) = k$, we have $\deg\left(f^*_{(R)}(x)\right) = M - k$. Hence $\deg\left(x^{k-1} f^*_{(R)}(x)\right) = (k-1) + (M-k) = M - 1$. Because the numerator of (2.10) is of degree less than M, the number of 1's in a cycle of length M of (d_n) is equal to the number of terms with coefficient 1 in $x^{k-1} f^*_{(R)}(x)$, which is equal to the number of terms with coefficient 1 in $f^*(x)$. Recalling Definitions 1.17 and 1.18, we have

$$\#1\text{'s in a cycle of length } M \text{ of } (d_n) = \ell_1\left(f^*(x)\right) \tag{2.11}$$

and

$$\#0\text{'s in a cycle of length } M \text{ of } (d_n) = \ell_{0,M-1}\left(f^*(x)\right). \tag{2.12}$$

This fact allows us to use a theorem of [8] to establish an upper bound for $|\ell_1\left(f^*(x)\right) - \ell_{0,M-1}\left(f^*(x)\right)|$. First we supply some necessary definitions.

Definition 2.25 ([8, 2.22])**.** For $\alpha \in F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, the *trace* $\mathrm{Tr}_{F/K}(\alpha)$ of α over K is defined by

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

If K is the prime subfield of F, then $\mathrm{Tr}_{F/K}(\alpha)$ is called the *absolute trace* of α and simply denoted by $\mathrm{Tr}_F(\alpha)$.

Since we are working in $\mathbb{F}_2$, we have absolute traces $\mathrm{Tr}_{\mathbb{F}_2}(0) = 0$ and $\mathrm{Tr}_{\mathbb{F}_2}(1) = 1$.

Definition 2.26 ([8, p.190])**.** The *canonical additive character* of $\mathbb{F}_2$ is defined by

$$\chi(c) = e^{\pi i \,\mathrm{Tr}(c)} \quad \text{for all } c \in \mathbb{F}_2.$$

Thus the only nontrivial additive character of $\mathbb{F}_2$ has $\chi(0) = e^{\pi i 0} = 1$ and $\chi(1) = e^{\pi i} = -1$.

We return to (d_n), the k-th order impulse response sequence described above, which has characteristic polynomial $f(x)$ with $f(0) = 1$ and is periodic with least period M. Theorem 8.78 of [8] states that for χ the nontrivial additive character of $\mathbb{F}_2$,

$$\left| \sum_{n=u}^{u+M-1} \chi(d_n) \right| \leq 2^{k/2} \quad \text{for all } u \geq 0.$$

From the above discussion of the nontrivial additive character of $\mathbb{F}_2$ and Equations (2.11) and (2.12),

$$\begin{aligned} \left| \sum_{n=u}^{u+M-1} \chi(d_n) \right| &= |\text{difference between \#0's and \#1's in a cycle of length } M \text{ of } (d_n)| \\ &= |\ell_1(f^*(x)) - \ell_{0,M-1}(f^*(x))|. \end{aligned}$$

Hence $|\ell_1(f^*(x)) - \ell_{0,M-1}(f^*(x))| \leq 2^{k/2}$.

All polynomials we will discuss in Chapter 3 are of the form $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + 1$ with all $a_i \in \mathbb{F}_2$. Thus $f(x)$ can be viewed as the characteristic polynomial of the impulse response sequence (d_n) satisfying (2.6) with $a_0 = 1$. Hence $2^{k/2}$ is an upper bound for the difference in the coordinates of $\beta(f(x))$ for any $f(x)$ of degree k we will see in Chapter 3. We shall see in Chapter 5 that this is asymptotically much larger than the difference in coordinates for our most robust examples, suggesting that Theorem 8.78 of [8] might be sharpened for the $\mathbb{F}_2$ case.

Chapter 3

Families of Robust Polynomials

Recall Equation (1.3), which states that for a polynomial $f(x) \in \mathbb{F}_2[x]$,

$$\delta\left(\bar{f}\right) = \frac{\ell_1\left(f^*\right)}{\mathrm{ord}(f)}.$$

In this chapter, we present four sequences $\{f_n\}$ of polynomials such that $\lim_{n\to\infty} \delta\left(\bar{f_n}\right) = 1$, thereby establishing 1 as the least upper bound of the set $\{\delta\left(\bar{P}\right) : P \text{ is a polynomial}\}$. We then consider examples of elements of these sequences which correspond to the points represented by boxes in Figure 1.1. At the end of the chapter, we discuss the methods of data collection used in finding these and other examples of robust polynomials. All polynomials in this section are considered as elements of $\mathbb{F}_2[x]$.

Remark 3.1. Recall Equation (1.2), which states that for any polynomial $f(x) \in \mathbb{F}_2(x)$, $f(x^2) = (f(x))^2$, so $f(x^{2^m}) = f(x)^{2^m}$.

We restate Definitions 1.17 and 1.18 and, a bit later, Definition 1.10 for convenience.

Definition 3.1. For a polynomial $f(x) \in \mathbb{F}_2[x]$, define the *length* of $f(x)$ to be the number of monomials in $f(x)$. This can also be viewed as the number of terms in $f(x)$ with coefficient 1 and is denoted by $\ell_1(f(x))$.

Definition 3.2. For a polynomial $f(x) \in \mathbb{F}_2[x]$, let $\ell_{0,N}(f(x))$ denote the number of terms in $f(x)$ with coefficient 0 when $f(x)$ is viewed as a polynomial of degree N. Note that N may exceed d, the usual degree of $f(x)$, if we take all terms of the form x^k, where $k > d$, to have coefficient 0.

Also recall Equation (1.4), which defines $\beta(f(x)) = (\ell_1(f^*(x)), \ell_{0,D-1}(f^*(x)))$. We now define the more general ordered pair $\beta_N(f(x))$.

Definition 3.3. For $f(x) \in \mathbb{F}_2[x]$ and N a multiple of the order of $f(x)$ with $f^*(x) := (1 + x^N)/f(x)$, we define

$$\beta_N(f(x)) = \left(\ell_1(f^*(x), \ell_{0,N-1}(f^*(x))\right).$$

Definition 3.4. For a polynomial $f(x)$ of degree n, the *reciprocal polynomial* of $f(x)$ is $f_{(R)}(x) := x^n f(1/x)$.

Lemma 3.5. *In $\mathbb{F}_2[x]$, $\beta(f(x)) = \beta(f_R(x))$, and the robustness of $f(x)$ is equivalent to the robustness of $f_R(x)$.*

Proof. According to Theorem 1.11, if $\text{order}(f(x)) = D$, then $\text{order}(f_R(x)) = D$. Suppose $\deg(f(x)) = n$. Then we have

$$f(x)f^*(x) = 1 + x^D$$

and

$$f_{(R)}(x)\left(f_{(R)}\right)^*(x) = 1 + x^D,$$

where $\deg(f^*(x)) = \deg\left(\left(f_{(R)}\right)^*(x)\right) = D - n$.

Now

$$\begin{aligned}(f^*)_{(R)}(x) &= x^{D-n} f^*\left(\frac{1}{x}\right) = x^{D-n}\left(\frac{1+\left(\frac{1}{x}\right)^D}{f\left(\frac{1}{x}\right)}\right)\\ &= \frac{x^D\left(1+\frac{1}{x^D}\right)}{x^n f\left(\frac{1}{x}\right)} = \frac{1+x^D}{f_{(R)}(x)}\\ &= \left(f_{(R)}\right)^*(x).\end{aligned}$$

Thus there is no ambiguity in writing $f^*_{(R)}(x)$, and $\ell_1(f^*(x)) = \ell_1\left(f^*_{(R)}(x)\right)$, so we see that $\beta(f(x)) = \beta(f_R(x))$.

□

Lemma 3.6. *If $f(x), g(x), h(x) \in \mathbb{F}_2[x]$ satisfy $f(x)g(x) = 1 + x^N$ and $f(x)h(x) = 1 + x^M$, where $N < M$, then $\ell_1(g(x))/N = \ell_1(h(x))/M$. In particular, if $\ell_1(g(x))/N$ is in lowest terms, then N is the order of $f(x)$.*

Proof. From Theorem 1.5, we know that $N \mid M$, so $M = jN$. We can write

$$h(x) = \frac{1+x^M}{f(x)} = g(x)\cdot\frac{1+x^{jN}}{1+x^N} = g(x)(1 + x^N + \cdots + x^{(j-1)N}).$$

If $\ell_1(g(x)) = k$ and $\ell_{0,N-1}(g(x)) = N - k$, then $\ell_1(h(x)) = kM/N = jk$ and $\ell_{0,M-1}(h(x)) = (N-k)M/N = M - jk = j(N-k)$. This proves the assertion. □

Definition 3.7. For a non-negative integer k, let $b(k)$ denote the number of 1's in the standard binary representation of k.

Lemma 3.8. *For $r \geq 2$,*

$$\sum_{k=0}^{2^r-2} 2^{b(k)} = 3^r - 2^r.$$

Proof. Since $b(2^r-1)=r$ with r digits in the representation and no zeros, if $0 \leq n \leq 2^r-2$, then $b(n) \leq r-1$. Consider counting the value of $\sum_{k=0}^{2^r-2} 2^{b(k)}$ by first fixing the value of $b(k)$. Let $b(k)=j$, where $0 \leq j \leq r-1$. There are $\binom{r}{j}$ numbers n in the range of summation with $b(n)=j$. Hence the contribution to the sum from numbers with $b(k)=j$ is $\binom{r}{j}2^j$. Using this and the binomial formula, we obtain

$$\begin{aligned}\sum_{k=0}^{2^r-2} 2^{b(k)} &= \binom{r}{0}2^0 + \binom{r}{1}2^1 + \binom{r}{2}2^2 + \cdots + \binom{r}{r-1}2^{r-1} \\ &= (2+1)^r - 2^r \\ &= 3^r - 2^r.\end{aligned}$$

□

Lemma 3.9. *For $a, b \in \mathbb{N}$,*

$$(1+x^a+x^b)\prod_{j=0}^{m-1}\left(1+x^{2^j a}+x^{2^j b}\right) = 1+x^{2^m a}+x^{2^m b}.$$

Proof. Let $m=1$. Then the product is $(1+x^a+x^b)(1+x^a+x^b) = (1+x^{2a}+x^{2b})$ by Remark 3.1. Suppose the result holds for all $1 \leq m \leq n$. Then

$$\begin{aligned}(1+x^a+x^b)\prod_{j=0}^{n}\left(1+x^{2^j a}+x^{2^j b}\right) &= (1+x^{2^n a}+x^{2^n b})(1+x^{2^n a}+x^{2^n b}) \\ &= \left(1+(x^2)^{2^n a}+(x^2)^{2^n b}\right) \\ &= 1+x^{2^{n+1}a}+x^{2^{n+1}b},\end{aligned}$$

where we have again used Remark 3.1. Hence by induction the result holds for all m. □

Lemma 3.10. *For $1 \leq r \in \mathbb{N}$,*

$$\left(1+x^{2^r-1}+x^{2^r}\right)\left(\prod_{j=0}^{r-1}\left(1+x^{(2^r-1)2^j}+x^{2^r 2^j}\right)+x^{4^r-2^r}\right) = 1+x^{4^r-1}.$$

Proof. Using Lemma 3.9 with $a = 2^r - 1, b = 2^r$, and $m = r$,

$$\begin{aligned}\left(1 + x^{2^r-1} + x^{2^r}\right) &\left(\prod_{j=0}^{r-1}\left(1 + x^{(2^r-1)2^j} + x^{2^r 2^j}\right) + x^{4^r-2^r}\right) \\ &= 1 + x^{2^r(2^r-1)} + x^{2^r(2^r)} + \left(1 + x^{2^r-1} + x^{2^r}\right) x^{4^r-2^r} \\ &= 1 + x^{4^r-2^r} + x^{4^r} + x^{4^r-2^r} + x^{4^r-1} + x^{4^r} \\ &= 1 + x^{4^r-1}.\end{aligned}$$

□

Let $d_{r,1} = 3^r - 1$ and $c_{r,1} = (4^r - 1) - d_{r,1} = 4^r - 3^r$.

Theorem 3.11. *Fix $r \geq 3$.*

(i) *The order of $f_{r,1}(x) := 1 + x + x^{2^r-1} + x^{2^r+1}$ divides $4^r - 1$.*

(ii) *The polynomial $h_{r,1}(x) := (1 + x^{4^r-1})/f_{r,1}(x) = f^*_{r,1}$ has $\ell_1(h_{r,1}(x)) = c_{r,1}$.*

(iii) *Hence $\beta_{4^r-1}(f_{r,1}) = (c_{r,1}, d_{r,1})$ and $f_{r,1}(x)$ is robust.*

(iv) *Let $\mathcal{A}_r = \{0, 1, 2^r - 1, 2^r + 1\}$. Then $\phi_{\mathcal{A}_r}(x) = f_{r,1}(x)$ and the sequence $(f_{\mathcal{A}_r}(n)) \bmod 2$ is periodic with least period dividing $4^r - 1$. Among $4^r - 1$ consecutive terms of $(f_{\mathcal{A}_r}(n))$, $4^r - 3^r$ terms are odd and $3^r - 1$ terms are even.*

Proof. Define

$$g_{r,1}(x) = \prod_{j=0}^{r-1}\left(1 + x^{(2^r-1)2^j} + x^{2^r 2^j}\right) + x^{4^r-2^r}. \tag{3.1}$$

Then Lemma 3.10 gives

$$\left(1 + x^{2^r-1} + x^{2^r}\right) g_{r,1}(x) = 1 + x^{4^r-1}.$$

Since

$$g_{r,1}(1) = \prod_{j=0}^{r-1}(1 + 1 + 1) + 1 \equiv 0 \pmod 2,$$

we know $(1 + x) \mid g_{r,1}(x)$. Hence there exists $h_{r,1}(x) \in \mathbb{F}_2[x]$ such that $(1 + x)h_{r,1}(x) = g_{r,1}(x)$, so

$$\left(1 + x^{2^r-1} + x^{2^r}\right)(1 + x)h_{r,1}(x) = 1 + x^{4^r-1}.$$

Since $f_{r,1}(x) = 1 + x + x^{2^r-1} + x^{2^r+1} = (1 + x)\left(1 + x^{2^r-1} + x^{2^r}\right)$, we see that $f_{r,1}(x) \mid \left(1 + x^{4^r-1}\right)$. We have not shown that $4^r - 1$ is actually the order of $f_{r,1}(x)$, but we know by Lemma 3.6 that the exact order

is not necessary to determine robustness. We have checked by direct computation that for $r \leq 10$, $4^r - 1$ is the exact order of $f_{r,1}$.

Now we seek a nice expression for $h_{r,1}(x)$ to use in proving part (ii). We will do this by manipulating $g_{r,1}(x)$. Rewrite (3.1) to obtain

$$g_{r,1}(x) = \prod_{j=0}^{r-1} \left(1 + x^{(2^r-1)2^j}(1 + x^{2^j})\right) + x^{4^r-2^r}. \tag{3.2}$$

We next expand the product in (3.2) and use Remark 3.1, specifically $1+x^{2^j} = (1+x)^{2^j}$, to see that, with the exception of 1 and $x^{4^r-2^r}$, all summands in the expanded product are terms of the form $x^{(2^r-1)\sum 2^i}(1+x)^{\sum 2^i}$, where $\sum 2^i$ is a sum of some subset of $\{2^0, 2^1, \ldots, 2^{r-1}\}$. Considering all such $\sum 2^i$, we get all terms of the form $x^{(2^r-1)n}(1+x)^n$ for $1 \leq n \leq 2^r - 1$. Thus we can rewrite (3.2) as

$$\begin{aligned} g_{r,1}(x) &= 1 + x^{4^r-2^r} + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^n \\ &= (1+x)\left(\frac{1 + x^{4^r-2^r}}{1+x} + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}\right) \\ &= (1+x)\left(\sum_{j=0}^{4^r-2^r-1} x^j + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}\right). \end{aligned}$$

Hence by the definition of $h_{r,1}(x)$,

$$h_{r,1}(x) = \sum_{j=0}^{4^r-2^r-1} x^j + \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1}.$$

We shall use this representation of $h_{r,1}(x)$ to determine $\ell_1(h_{r,1}(x))$. We begin by focusing on

$$S_{r,1}(x) := \sum_{n=1}^{2^r-1} x^{(2^r-1)n}(1+x)^{n-1},$$

which is a polynomial of degree $4^r - 2^r - 1$. We note that the greatest exponent in a monomial when $n = k$ is $(2^r-1)k + (k-1) = 2^rk - 1$, and the least exponent in a monomial when $n = k+1$ is $(2^r-1)(k+1) = 2^rk + 2^r - (k+1)$. Since $k+1 \leq 2^r - 1$, it follows that $2^rk - 1 < 2^rk + 2^r - (k+1)$, so there is no cancellation of terms within $S_{r,1}(x)$. Glaisher's Theorem, see [7], states that the number of odd binomial coefficients of

the form $\binom{n}{j}$, $0 \leq j \leq n$, is equal to $2^{b(j)}$. Using this and Lemma 3.8, we see that

$$\ell_1(S_{r,1}(x)) = \sum_{j=1}^{2^r-1} 2^{b(j-1)} = \sum_{k=0}^{2^r-2} 2^{b(k)} = 3^r - 2^r.$$

Since $S_{r,1}(x)$ is a polynomial of degree $4^r - 2^r - 1$, $S_{r,1}(x)$ has $4^r - 2^r$ possible terms and $\ell_{0,4^r-2^r-1}(S_{r,1}(x)) = 4^r - 2^r - (3^r - 2^r) = 4^r - 3^r$. Then, to construct $h_{r,1}(x)$, we add $\sum_{j=0}^{4^r-2^r-1} x^j$. Note that the degree of this sum is equal to the degree of $S_{r,1}(x)$. This addition has the effect of reversing the 0's and 1's, so $\ell_1(h_{r,1}(x)) = 4^r - 3^r$ and $\ell_{0,4^r-2^r-1}(h_{r,1}(x)) = 3^r - 2^r$, completing the proof of part (ii). Because the order of $f_{r,1}(x)$ divides $4^r - 1$, we consider $h_{r,1}(x)$ as a polynomial of degree $4^r - 2$ with $4^r - 1$ possible terms. The $2^r - 1$ terms of degree $4^r - 2^r, \ldots, 4^r - 2$ have coefficient 0. Thus in total $\ell_1(h_{r,1}(x)) = 4^r - 3^r = c_{r,1}$ and $\ell_{0,4^r-2}(h_{r,1}(x)) = 3^r - 1 = d_{r,1}$.

Since $\gcd(c_{3,1}, d_{3,1}) = \gcd(37, 26) = 1$, we know $\ell_1(h_{3,1})/(4^3 - 1)$ is in lowest terms. By Lemma 3.6, the order of $f_{3,1}$ is indeed $4^3 - 1$, and the polynomial is robust. For $r \geq 4$, it is not necessarily the case that $\gcd(c_{r,1}, d_{r,1}) = 1$, but it is true that

$$\begin{aligned}\frac{c_{r,1}}{4^r - 1} = \frac{4^r - 3^r}{4^r - 1} &= 1 - \frac{3^r - 1}{4^r - 1} \\ &> 1 - \frac{3^r - (3/4)^r}{4^r - 1} = 1 - \left(\frac{3}{4}\right)^r > \frac{2}{3},\end{aligned}$$

so $f_{r,1}(x)$ is robust by Remark 1.1.

Part (iv) follows immediately. □

Example 3.1. Consider $f_{3,1}(x) = 1 + x + x^7 + x^9$. The order of $f_{3,1}(x)$ is $4^3 - 1 = 63$. The polynomial $f^*_{3,1}(x)$ has $\ell_1\left(f^*_{3,1}(x)\right) = 4^3 - 3^3 = 37$, and $\beta\left(f_{3,1}(x)\right) = (37, 26)$. Explicitly,

$$\begin{aligned}f^*_{3,1}(x) =& x^{54} + x^{52} + x^{50} + x^{48} + x^{45} + x^{44} + x^{41} + x^{40} + x^{38} + x^{37} + x^{36} + x^{34} \\ &+ x^{33} + x^{32} + x^{27} + x^{26} + x^{25} + x^{24} + x^{22} + x^{20} + x^{19} + x^{18} + x^{17} \\ &+ x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.\end{aligned}$$

Corollary 3.12. *The reciprocal polynomials $f_{(R),r,1} = 1 + x^2 + x^{2^r} + x^{2^r+1}$ are robust with order dividing $4^r - 1$.*

Proof. This follows immediately from Theorem 3.11 and Lemma 3.5. □

Example 3.2. Consider $f_{(R),3,1}(x) = 1 + x^2 + x^8 + x^9$. The order of $f_{(R),3,1}(x)$ is $4^3 - 1 = 63$. The polynomial $f^*_{(R),3,1}(x)$ has $\ell_1\left(f^*_{(R),3,1}(x)\right) = 4^3 - 3^3 = 37$, and $\beta\left(f_{(R),3,1}(x)\right) = (37, 26)$.

We now exhibit another family of robust polynomials.

Let $c_{r,2} = 4^r - 3^r + 2^r$ and $d_{r,2} = 3^r + 1$.

Theorem 3.13. *Fix $r \geq 3$.*

(i) *The order of $f_{r,2}(x) := 1 + x + x^{2^r} + x^{2^r+2}$ divides $4^r + 2^r + 1$.*

(ii) *The polynomial $h_{r,2}(x) := (1 + x^{4^r+2^r+1})/f_{r,2}(x) = f^*_{r,2}$ has $\ell_1(h_{r,2}(x)) = c_{r,2}$.*

(iii) *Hence $\beta_{4^r+2^r+1}(f_{r,2}(x)) = (c_{r,2}, d_{r,2})$ and $f_{r,2}(x)$ is robust.*

(iv) *Let $\mathcal{A}_r = \{0, 1, 2^r, 2^r + 2\}$. Then $\phi_{\mathcal{A}_r}(x) = f_{r,2}(x)$ and the sequence $(f_{\mathcal{A}_r}(n)) \bmod 2$ is periodic with least period dividing $4^r + 2^r + 1$. Among $4^r + 2^r + 1$ consecutive terms of $(f_{\mathcal{A}_r}(n))$, $4^r - 3^r + 2^r$ terms are odd and $3^r + 1$ terms are even.*

Proof. Let

$$g_{r,2}(x) = \prod_{j=0}^{r-1} \left(1 + x^{2^j 2^r} + x^{2^j(2^r+1)}\right). \tag{3.3}$$

By Lemma 3.9, we know that

$$\begin{aligned}\left(1 + x^{2^r} + x^{2^r+1}\right) g_{r,2}(x) &= 1 + x^{2^r 2^r} + x^{2^r(2^r+1)} \\ &= 1 + x^{4^r} + x^{4^r+2^r}.\end{aligned} \tag{3.4}$$

By factoring the terms in (3.3) we obtain

$$g_{r,2}(x) = \prod_{j=0}^{r-1} \left(1 + x^{2^j 2^r}\left(1 + x^{2^j}\right)\right).$$

Then by expanding the product and using Remark 3.1, we see that, with the exception of the term 1, all summands in the expanded product are terms of the form $x^{2^r \sum 2^i}(1+x)^{\sum 2^i}$, where $\sum 2^i$ is a sum of some subset of $\{2^0, 2^1, \ldots, 2^{r-1}\}$. Considering all such $\sum 2^i$, we get all terms of the form $x^{2^r n}(1+x)^n$ for all $1 \leq n \leq 2^r - 1$. Thus we can rewrite (3.3) as

$$\begin{aligned}g_{r,2}(x) &= \prod_{j=0}^{r-1} \left(1 + x^{2^j 2^r}\left(1 + x^{2^j}\right)\right) \\ &= 1 + \sum_{i=1}^{2^r-1} x^{2^r i}(1+x)^i.\end{aligned} \tag{3.5}$$

Using equations (3.4) and (3.5), we see that

$$\begin{aligned}\left(1+x^{2^r}+x^{2^r+1}\right)&\left(1+x^{4^r}+\sum_{i=1}^{2^r-1}x^{2^ri}(1+x)^i\right)\\&=\left(1+x^{2^r}+x^{2^r+1}\right)\left(x^{4^r}+g_{r,2}(x)\right)\\&=\left(1+x^{2^r}+x^{2^r+1}\right)x^{4^r}+1+x^{4^r}+x^{4^r+2^r}\\&=x^{4^r}+x^{4^r+2^r}+x^{4^r+2^r+1}+1+x^{4^r}+x^{4^r+2^r}\\&=1+x^{4^r+2^r+1}.\end{aligned}$$

Now observe that

$$\begin{aligned}\left(1+x^{2^r}+x^{2^r+1}\right)&\left(1+x\right)\left(\frac{1+x^{4^r}}{1+x}+\sum_{i=1}^{2^r-1}x^{2^ri}(1+x)^{i-1}\right)\\&=\left(1+x+x^{2^r}+x^{2^r+2}\right)\left(\frac{1+x^{4^r}}{1+x}+\sum_{i=1}^{2^r-1}x^{2^ri}(1+x)^{i-1}\right)\\&=f_{r,2}(x)\left(\frac{1+x^{4^r}}{1+x}+\sum_{i=1}^{2^r-1}x^{2^ri}(1+x)^{i-1}\right)\\&=1+x^{4^r+2^r+1}.\end{aligned}$$

Thus the order of $f_{r,2}(x)$ divides 4^r+2^r+1, completing the proof of part (i), and that suffices to determine if $f_{r,2}(x)$ is robust by Lemma 3.6. We have checked by direct computation that 4^r+2^r+1 is the exact order of $f_{r,2}(x)$ when $r \leq 10$.

Let

$$S_{r,2}(x) := \sum_{i=1}^{2^r-1} x^{2^ri}(1+x)^{i-1},$$

so $h_{r,2}(x) = \frac{1+x^{4^r}}{1+x} + S_{r,2}(x)$. We wish to determine $\ell_1(h_{r,2}(x))$ and will begin by determining $\ell_1(S_{r,2}(x))$. We first note that when $i=k$, the monomial of greatest degree is $x^{2^rk}x^{k-1} = x^{2^rk+k-1}$. When $i=k+1$, the monomial of lowest degree is $x^{2^r(k+1)} = x^{2^rk+2^r}$. Since $k < 2^r-1$, it follows that $2^rk+k-1 < 2^rk+2^r$, so there is no overlap of terms from $i=k$ and $i=k+1$.

Once again, we use Glaisher's Theorem, see [7], which states that the number of odd binomial coefficients of the form $\binom{n}{j}$, $0 \leq j \leq n$, is equal to $2^{b(j)}$, and Lemma 3.8 to see that

$$\ell_1(S_{r,2}(x)) = \sum_{j=1}^{2^r-1} 2^{b(j-1)} = \sum_{k=0}^{2^r-2} 2^{b(k)} = 3^r - 2^r.$$

Because $S_{r,2}(x)$ is a polynomial of degree $2^r(2^r-1)+2^r-2 = 4^r-2$, we have $\ell_{0,4^r-2}(S_{r,2}(x)) = 4^r-2+1-3^r+2^r = 4^r-3^r+2^r-1$. Adding in the $(1+x^{4^r})/(1+x) = 1+x+x^2+\cdots+x^{4^r-2}+x^{4^r-1}$ to construct $h_{r,2}(x)$ has the effect of reversing the 0's and 1's and adding an additional 1. Hence $\ell_1(h_{r,2}(x)) = 4^r-3^r+2^r$ and $\ell_{0,4^r-2}(h_{r,2}(x)) = 3^r-2^r$, and the proof of part (ii) is complete. We now consider $h_{r,2}(x)$ as a polynomial of degree 4^r+2^r, so the remaining $4^r+2^r-4^r+1 = 2^r+1$ terms have coefficient 0. Hence $\ell_1(h_{r,2}(x)) = 4^r-3^r+2^r = c_{r,2}$ and $\ell_{0,4^r+2^r}(h_{r,2}(x)) = 3^r+1 = d_{r,2}$.

It is not necessarily the case that $\gcd(c_{r,2}, d_{r,2}) = 1$, and when this fails we know only that the order of $f_{r,2}(x)$ divides 4^r+2^r+1, but this is still sufficient to determine if $f_{r,2}(x)$ is robust by Lemma 3.6. In fact, $\gcd(c_{6,2}, d_{6,2}) \neq 1$, but 4^r+2^r+1 is indeed the order of $f_{6,2}(x)$ and not just a divisor of the order. For $1 \leq r \leq 5$, $\gcd(c_{r,2}, d_{r,2}) = 1$, so the order of $f_{r,2}(x)$ is 4^r+2^r+1, and $\beta(f_{r,2}(x)) = (c_{r,2}, d_{r,2})$, making $f_{r,2}(x)$ robust. For $r \geq 6$,

$$\begin{aligned}\frac{c_{r,2}}{4^r+2^r+1} &= \frac{4^r-3^r+2^r}{4^r+2^r+1} = 1-\frac{3^r+1}{4^r+2^r+1} \\ &> 1-\frac{3^r+(3/2)^r+(3/4)^r}{4^r+2^r+1} = 1-\left(\frac{3}{4}\right)^r > \frac{2}{3},\end{aligned}$$

so $f_{r,2}(x)$ is robust by Remark 1.1. Part (iv) follows immediately. □

Example 3.3. Consider $f_{3,2}(x) = 1+x+x^8+x^{10}$. The order of $f_{3,2}(x)$ is $4^3+2^3+1 = 73$. The polynomial $f^*_{3,2}(x)$ has $\ell_1\left(f^*_{3,2}(x)\right) = 4^3-3^3+2^3 = 45$, and $\beta\left(f_{3,2}(x)\right) = (45, 28)$. Explicitly,

$$\begin{aligned}f^*_{3,2}(x) =& x^{63}+x^{61}+x^{59}+x^{57}+x^{55}+x^{54}+x^{51}+x^{50}+x^{47}+x^{46}+x^{45}+x^{43} \\ &+x^{42}+x^{41}+x^{39}+x^{38}+x^{37}+x^{36}+x^{31}+x^{30}+x^{29}+x^{28}+x^{27}+x^{25} \\ &+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11} \\ &+x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x^2+x+1.\end{aligned}$$

Corollary 3.14. *The reciprocal polynomials $f_{(R),r,2}(x) = 1+x^2+x^{2^r+1}+x^{2^r+2}$ are robust with order dividing 4^r+2^r+1.*

Proof. This follows immediately from Theorem 3.13 and Lemma 3.5. □

Example 3.4. Consider $f_{(R),3,2}(x) = 1+x^2+x^9+x^{10}$. The order of $f_{(R),3,2}(x) = 4^3+2^3+1 = 73$. The polynomial $f^*_{(R),3,2}(x)$ has $\ell_1\left(f^*_{(R),3,2}(x)\right) = 4^3-3^3+2^3 = 45$, and $\beta\left(f_{(R),3,2}\right) = (45, 28)$.

With Examples 3.1, 3.2, 3.3, and 3.4, we have accounted for all of the rectangular points in Figure 1.1.

In our search for robust polynomials, we have checked all polynomials of order less than or equal to 83, all quadrinomials of degree less than or equal to 18, all trinomials of degree less than or equal to 19, and all polynomials of degree less than or equal to 14. The families described above were the most interesting examples discovered in these searches, but we shall describe here the methods of searching and some of the results.

We found the four sequences of robust polynomials discussed in this chapter by using Mathematica to obtain large amounts of data. One tactic was to determine $\beta(f(x))$ for all polynomials $f(x) \in \mathbb{F}_2[x]$ with order less than or equal to 83. To accomplish this, we first fixed the value of m and then factored $1 + x^m$. The exact code used varies slightly depending on the number of distinct irreducible factors of $1 + x^m$ but does not depend on m in any other way. The next step was to build a table whose entries were all of the polynomial divisors of $1 + x^m$. We then used two nested for loops to calculate $\beta_m(g(x))$ for each polynomial divisor $g(x)$ of $1 + x^m$. Appendix A.1 contains the code used for $m = 6$, and Appendix A.2 contains the code used for $m = 7$. For some larger values of m in the range $1 \leq m \leq 83$ for which $1 + x^m$ has a high number of distinct irreducible factors, we also included an if statement in the nested for loops so that only the robust polynomial divisors $g(x)$ of $1 + x^m$ and their order pairs $\beta_m(g(x))$ would print. This is illustrated by the code in Appendix A.3. The tables in Appendix A.4 list all robust polynomials of order less than or equal to 83, which were obtained in the manner described above.

The robust polynomial $f_{3,1}(x) = 1 + x + x^7 + x^9$ of Example 3.1 was found using the method described above and appeared in the data for polynomials of order 63. Since $\beta\left(f_{3,1}(x)\right) = (37, 26)$ had such a high ratio of the first coordinate to the second coordinate, we began to check other polynomials $f_{r,1}(x)$ for small r and noticed that they, too, had $\beta\left(f_{r,1}(x)\right) = (4^r - 3^r, 3^r - 1)$. We hoped this would generalize to $f_{r,1}(x)$ for all values of r, and in time the proof of Theorem 3.11 was found. We later noticed among the Mathematica data on polynomials of order 63 the robust polynomial $f_{(R),3,1}$ of Example 3.2 and applied Lemma 3.5 to obtain Corollary 3.12. The tale of Theorem 3.13 and Corollary 3.14 is similar.

After finding these four sequences of robust polynomials, we continued our search and narrowed the focus to quadrinomials. We began to systemically consider all quadrinomials in $\mathbb{F}_2[x]$ by degree. We used Mathematica on a department office computer to obtain $\beta(f(x))$ for all quadrinomials $f(x)$ with degree less than or equal to 15. Appendix B.1 Figure B.1 contains the code used for quadrinomials of the form $1 + x + x^j + x^{12}$, where $2 \leq j \leq 11$, and Figure B.2 contains the code used for quadrinomials of the form $1 + x^2 + x^j + x^{12}$, where $3 \leq j \leq 11$. Nested for loops could have been used to create one piece of code that would generate data on all quadrinomials of degree 12, but it was more advantageous to break the problem into smaller pieces to avoid needing large chunks of consecutive run time on the office machine. After degree

15 the time required to run the code even when broken into smaller pieces became unreasonable. Jonathan Manton assisted us in learning to use the Illinois Campus Cluster Program. When using the secondary queue of Campus Cluster, we had access to all available nodes of the 512 in the Campus Cluster with a wall-clock limit of 4 hours per job. By breaking our overall job into sub-jobs, this allowed us to run many of our Mathematica calculations simultaneously. We used Campus Cluster to obtain $\beta(f(x))$ for all quadrinomials of degree 16, 17, and 18. While we did find robust polynomials in this search, we were unable to generalize any of them to sequences of polynomials. Appendix B.3 contains a complete list of all robust quadrinomials of degree less than or equal to 18.

Table V-1 of [6] contains information, including orders, on trinomials of degree less than or equal to 36. We used this information on orders to obtain $\beta(f(x))$ for all trinomials $f(x) \in \mathbb{F}_2[x]$ with degree less than or equal to 19. There were only 4 robust trinomials in this range, and they are given in Table 3.1. Calculations became difficult for trinomials of higher degree because of the large amounts of time needed to run the code.

$f(x)$	$\text{ord}(f(x))$	$\beta(f(x))$
$1 + x^3 + x^{14}$	5115	$(2600, 2515)$
$1 + x^{11} + x^{14}$	5115	$(2600, 2515)$
$1 + x^9 + x^{19}$	174251	$(87136, 87115)$
$1 + x^{10} + x^{19}$	174251	$(87136, 87115)$

Table 3.1: All robust trinomials of degree less than or equal to 19

We also determined $\beta(f(x))$ for all polynomials of degree less than or equal to 14. Of all the polynomials studied in these various methods, the most interesting ones remain the families described in this chapter, due to the large ratio of the first coordinate of $\beta(f(x))$ to the second coordinate and because those were the only cases in which we were able to take the specific examples we noticed in the data and generalize to entire families of robust polynomials.

Chapter 4

Asymptotics of the Summatory Function

We begin by reviewing some basic concepts of sequences introduced in Chapter 2 and include a matrix view of recurrence relations, following [9].

Consider a sequence $(b(n))$ such that

$$b(n) + c_{k-1}b(n-1) + c_{k-2}b(n-2) + \cdots + c_0 b(n-k) = 0 \tag{4.1}$$

for all $n \geq k$ and $c_i \in \mathbb{N}$. By shifting the sequence, we see that

$$b(n+k) + c_{k-1}b(n+k-1) + c_{k-2}b(n+k-2) + \cdots + c_0 b(n+k-k) = 0 \tag{4.2}$$

for $n \geq 0$. Recalling definitions from Chapter 2, (4.1) is a *homogeneous k-th order linear recurrence relation*, and $(b(n))$ is a *homogeneous k-th order linear recurrence sequence*. The coefficients $c_0, c_1, \ldots, c_{k-1}$ are the *initial values of the sequence*. For any sequence $(b(n))$ satisfying (4.1) we can define the *characteristic polynomial*

$$f(x) = x^k + c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_0. \tag{4.3}$$

We can also consider a recurrence relation from the point of view of a matrix system, considering k sequences indexed as $(b_i(n))$ for $1 \leq i \leq k$ which satisfy

$$b_i(n+1) = \sum_{j=1}^{k} m_{ij} b_j(n)$$

for $n \geq 0$ and $1 \leq i \leq k$. Then

$$\begin{pmatrix} b_1(n+1) \\ \vdots \\ b_k(n+1) \end{pmatrix} = \begin{pmatrix} m_{11} & \cdots & m_{1k} \\ \vdots & & \vdots \\ m_{k1} & \cdots & m_{kk} \end{pmatrix} \begin{pmatrix} b_1(n) \\ \vdots \\ b_k(n) \end{pmatrix}$$

for $n \geq 0$. To simplify the notation, if $M = [m_{ij}]$ and

$$\mathbf{B}(n) = \begin{pmatrix} b_1(n) \\ \vdots \\ b_k(n) \end{pmatrix},$$

then $\mathbf{B}(n+1) = M\mathbf{B}(n)$ for $n \geq 0$. Thus $\mathbf{B}(n) = M^n\mathbf{B}(0)$ for $n \geq 0$, where

$$\mathbf{B}(0) = \begin{pmatrix} b_1(0) \\ \vdots \\ b_k(0) \end{pmatrix}$$

is the vector of initial conditions.

In this matrix point of view, the *characteristic polynomial* of M is

$$g(\lambda) := \det(M - \lambda I_k).$$

By the Cayley-Hamilton Theorem, $g(M) = 0$, the $k \times k$ zero matrix.

If $g(x)$ is (4.3), then

$$0 = g(M) = M^k + c_{k-1}M^{k-1} + c_{k-2}M^{k-2} + \cdots + c_0 I_k.$$

Hence for any $n \geq 0$,

$$0 = M^{n+k} + c_{k-1}M^{n+k-1} + c_{k-2}M^{n+k-2} + \cdots + c_0 M^n$$

and thus

$$\begin{aligned} 0 &= \mathbf{B}(0)\left(M^{n+k} + c_{k-1}M^{n+k-1} + c_{k-2}M^{n+k-2} + \cdots + c_0 M^n\right) \\ &= \mathbf{B}(n+k) + c_{k-1}\mathbf{B}(n+k-1) + c_{k-2}\mathbf{B}(n+k-2) + \cdots + c_0\mathbf{B}(n). \end{aligned}$$

Thus each sequence $(b_j(n))$ satisfies the original linear recurrence (4.2).

As an additional connection between these two views of linear recurrence sequences, note that for a

sequence satisfying (4.1),

$$\begin{pmatrix} b(n+1) \\ b(n+2) \\ \vdots \\ b(n+k-1) \\ b(n+k) \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -c_0 & -c_1 & \cdots & -c_{k-2} & -c_{k-1} \end{pmatrix} \begin{pmatrix} b(n) \\ b(n+1) \\ \vdots \\ b(n+k-2) \\ b(n+k-1) \end{pmatrix},$$

where this matrix is the *companion matrix* to g and has characteristic polynomial $(-1)^k g$.

To apply these ideas, let $f_{\mathcal{A}}(n)$ denote the number of ways to write $n = \sum_{i=0}^{\infty} \epsilon_i 2^i$, where ϵ_i belongs to the set

$$\mathcal{A} := \{0 = a_0, a_1, \ldots, a_z\},$$

with $a_i \in \mathbb{N}$ and $a_i < a_{i+1}$ for all $0 \leq i \leq z-1$. Suppose that including 0 there are s even elements of $\mathcal{A}$. Call them $0 = 2b_1, 2b_2, \ldots, 2b_s$, with $0 = b_1 < b_2 < \cdots < b_s$. The remaining $(z+1) - s := t$ elements of $\mathcal{A}$ must be odd. Call them $2c_1 + 1, 2c_2 + 1, \ldots, 2c_t + 1$ with $0 \leq c_1 < c_2 < \ldots < c_t$. Then $\mathcal{A} = \{0 = 2b_1, 2b_2, \ldots, 2b_s, 2c_1 + 1, \ldots, 2c_t + 1\}$.

If n is even, then $\epsilon_0 = 0, 2b_2, 2b_3, \ldots$, or $2b_s$ and

$$f_{\mathcal{A}}(n) = f_{\mathcal{A}}(n/2) + f_{\mathcal{A}}((n-2b_2)/2) + f_{\mathcal{A}}((n-2b_3)/2) + \cdots + f_{\mathcal{A}}((n-2b_s)/2).$$

Writing $n = 2\ell$, we have

$$f_{\mathcal{A}}(2\ell) = f_{\mathcal{A}}(\ell) + f_{\mathcal{A}}(\ell - b_2) + f_{\mathcal{A}}(\ell - b_3) + \cdots + f_{\mathcal{A}}(\ell - b_s),$$

so for any even n, $f_{\mathcal{A}}(n)$ satisfies a homogeneous linear recurrence relation of order b_s. If n is odd, then $\epsilon_0 = 2c_1 + 1, 2c_2 + 1, \ldots$, or $2c_t + 1$, and

$$f_{\mathcal{A}}(n) = f_{\mathcal{A}}(n - (2c_1+1)/2) + f_{\mathcal{A}}((n - (2c_2+1)/2) + \cdots + f_{\mathcal{A}}((n - (2c_t+1))/2).$$

Writing $n = 2\ell + 1$, we have

$$f_{\mathcal{A}}(2\ell + 1) = f_{\mathcal{A}}(\ell - c_1) + f_{\mathcal{A}}(\ell - c_2) + \cdots + f_{\mathcal{A}}(\ell - c_t),$$

so for any odd n, $f_{\mathcal{A}}(n)$ satisfies a homogeneous linear recurrence relation of order c_t. This argument is

given for $f_{\mathcal{A},b}(n)$, the b-ary representation of n with coefficients from $\mathcal{A}$, using residue classes $\bmod b$ in [1].

Example 4.1. Let $\mathcal{A} = \{0, 1, 4, 9\}$. We can write $\mathcal{A} = \{2(0), 2(0)+1, 2(2), 2(4)+1\}$. Then

$$f_{\{0,1,4,9\}}(2\ell) = f_{\{0,1,4,9\}}(\ell) + f_{\{0,1,4,9\}}(\ell - 2)$$

and

$$f_{\{0,1,4,9\}}(2\ell + 1) = f_{\{0,1,4,9\}}(\ell) + f_{\{0,1,4,9\}}(\ell - 4).$$

In general, let

$$\omega_k(m) = \begin{pmatrix} f_{\mathcal{A}}(2^k m) \\ f_{\mathcal{A}}(2^k m - 1) \\ \vdots \\ f_{\mathcal{A}}(2^k m - a_z) \end{pmatrix}$$

and consider the fixed $(a_z + 1) \times (a_z + 1)$ matrix M such that for any $k \geq 0$,

$$\omega_{k+1} = M\omega_k.$$

Example 4.2. Let $\mathcal{A} = \{0, 1, 3, 4\}$. Then

$$f_{\mathcal{A}}(2\ell) = f_{\mathcal{A}}(\ell) + f_{\mathcal{A}}(\ell - 2)$$

and

$$f_{\mathcal{A}}(2\ell + 1) = f_{\mathcal{A}}(\ell) + f_{\mathcal{A}}(\ell - 1).$$

Now

$$\omega_{k+1}(m) = \begin{pmatrix} f_{\mathcal{A}}(2^{k+1}m) \\ f_{\mathcal{A}}(2^{k+1}m - 1) \\ f_{\mathcal{A}}(2^{k+1}m - 2) \\ f_{\mathcal{A}}(2^{k+1}m - 3) \\ f_{\mathcal{A}}(2^{k+1}m - 4) \end{pmatrix} = \begin{pmatrix} f_{\mathcal{A}}(2^k m) + f_{\mathcal{A}}(2^k m - 2) \\ f_{\mathcal{A}}(2^k m - 1) + f_{\mathcal{A}}(2^k m - 2) \\ f_{\mathcal{A}}(2^k m - 1) + f_{\mathcal{A}}(2^k m - 3) \\ f_{\mathcal{A}}(2^k m - 2) + f_{\mathcal{A}}(2^k m - 3) \\ f_{\mathcal{A}}(2^k m - 2) + f_{\mathcal{A}}(2^k m - 4) \end{pmatrix},$$

and $M = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ satisfies $\omega_{k+1}(m) = M\omega_k(m)$.

We will use these ideas to examine the asymptotic behavior of the summatory function $\sum_{n=m2^r}^{m2^{r+1}-1} f_{\mathcal{A}}(n)$, but we must first establish a lemma.

Lemma 4.1. *Let $M = [m_{ij}]$ be an $n \times n$ matrix with characteristic polynomial $g(\lambda)$ and eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_y$. Then*

$$\max_{1 \le i \le y} |\lambda_i| \le \max_{1 \le i \le n} \sum_{j=1}^{n} m_{ij}.$$

Theorem 4.2. *Let $\mathcal{A}, f_{\mathcal{A}}(n), M$, and $\omega_k(m)$ be as above, with the additional assumption that there exists some odd $a_i \in \mathcal{A}$. Define*

$$s_{\mathcal{A}}(r, m) = \sum_{n=m2^r}^{m2^{r+1}-1} f_{\mathcal{A}}(n).$$

Let $|\mathcal{A}|$ denote the number of elements in the set $\mathcal{A}$. Then for a fixed value of m,

$$\lim_{r \to \infty} \frac{s_{\mathcal{A}}(r, m)}{|\mathcal{A}|^r} = c(\mathcal{A}, m),$$

for some constant $c(\mathcal{A}, m) \in \mathbb{Q}$, so $s_{\mathcal{A}}(r, m) \approx c(\mathcal{A}, m)\,|\mathcal{A}|^r$.

Proof. Let $g(\lambda) := \det(M - \lambda I)$ be the characteristic polynomial of M with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_y$, where each λ_i has multiplicity e_i. We can write

$$g(\lambda) = \sum_{k=0}^{a_z+1} \alpha_k \lambda^k.$$

By Cayley-Hamilton, we know that $g(M) = 0$. Thus we have

$$0 = g(M) = \sum_{k=0}^{a_z+1} \alpha_k M^k$$

and hence, for all r,

$$0 = \left(\sum_{k=0}^{a_z+1} \alpha_k M^k \right) \omega_r(m) = \sum_{k=0}^{a_z+1} \alpha_k \omega_{r+k}(m).$$

Since

$$\omega_{r+k}(m) = \begin{pmatrix} f_{\mathcal{A}}(2^{r+k}m) \\ f_{\mathcal{A}}(2^{r+k}m-1) \\ \vdots \\ f_{\mathcal{A}}(2^{r+k}m-a_z) \end{pmatrix},$$

we have

$$\sum_{k=0}^{a_z+1} \alpha_k f(2^{r+k}m-j) = 0 \tag{4.4}$$

for all $0 \le j \le a_z$.

Let $I_r = \{2^r, 2^r+1, 2^r+2, \ldots, 2^{r+1}-1\}$. Then $I_r = 2I_{r-1} \cup (2I_{r-1}+1)$. Thus

$$\begin{aligned} s_{\mathcal{A}}(r,m) &= \sum_{n=m2^r}^{m2^{r+1}-1} f_{\mathcal{A}}(n) \\ &= \sum_{n=m2^{r-1}}^{m2^r-1} f_{\mathcal{A}}(2n) + f_{\mathcal{A}}(2n+1) \\ &= \sum_{n=m2^{r-1}}^{m2^r-1} f_{\mathcal{A}}(n) + f_{\mathcal{A}}(n-b_2) + \cdots + f_{\mathcal{A}}(n-b_s) + f_{\mathcal{A}}(n-c_1) + \cdots + f_{\mathcal{A}}(n-c_t). \end{aligned}$$

Since

$$\sum_{n=m2^{r-1}}^{m2^r-1} f_{\mathcal{A}}(n-k) = \sum_{n=m2^{r-1}}^{m2^r-1} f_{\mathcal{A}}(n) + \sum_{j=1}^{k} \left(f_{\mathcal{A}}(m2^{r-1}-j) - f_{\mathcal{A}}(m2^r-j) \right),$$

we deduce that

$$\begin{aligned} s_{\mathcal{A}}(r,m) &= |\mathcal{A}| \sum_{n=m2^{r-1}}^{m2^r-1} f_{\mathcal{A}}(n) + h(r) \\ &= |\mathcal{A}|\, s_{\mathcal{A}}(r-1,m) + h(r), \end{aligned}$$

where

$$h(r) = \sum_{i=2}^{s} \sum_{j=1}^{b_i} \left(f_{\mathcal{A}}(m2^{r-1}-j) - f_{\mathcal{A}}(m2^r-j) \right) + \sum_{i=1}^{t} \sum_{j=1}^{c_i} \left(f_{\mathcal{A}}(m2^{r-1}-j) - f_{\mathcal{A}}(m2^r-j) \right)$$

and

$$\sum_{k=0}^{a_z+1} \alpha_k h(r+k) = 0$$

by Equation (4.4).

Thus we have an inhomogeneous recurrence relation for $s_{\mathcal{A}}(r,m)$ and will first consider the corresponding

homogeneous recurrence relation $s_{\mathcal{A}}(r,m) = |\mathcal{A}|\, s_{\mathcal{A}}(r-1,m)$, which has solution $s_{\mathcal{A}}(r,m) = c_1\,|\mathcal{A}|^r$. Then the solution to our inhomogeneous recurrence relation is of the form

$$s_{\mathcal{A}}(r,m) = c_1\,|\mathcal{A}|^r + \sum_{i=1}^{y} p_i(\lambda_i, r),$$

where $p_i(\lambda_i, r) = \sum_{j=1}^{e_i} c_{ij} r^{j-1} \lambda_i^r$.

By Lemma 4.1, the maximum of the absolute values of the λ_i is bounded above by the maximum of the row sums of M, and any row sum of M is at most $|\mathcal{A}| - 1$ since all elements of M are either 0 or 1 and by assumption not all elements of $\mathcal{A}$ have the same parity. Hence the $c_1|\mathcal{A}|^r$ term dominates $s_{\mathcal{A}}(r,m)$ as $r \to \infty$, so

$$\lim_{r\to\infty} \frac{s_{\mathcal{A}}(r,m)}{|\mathcal{A}|^r} = c_1.$$

We can compute $\sum_{k=0}^{a_z+1} \alpha_k s_{\mathcal{A}}(r+k,m)$, and for sufficiently large r, we have

$$\sum_{k=0}^{a_z+1} \alpha_k s_{\mathcal{A}}(r+k,m) = c_1 \sum_{k=0}^{a_z+1} \alpha_k\,|\mathcal{A}|^{r+k} + 0 = c_1\,|\mathcal{A}|^r\, g\left(|\mathcal{A}|\right),$$

since

$$\sum_{k=0}^{a_z+1} \alpha_k \sum_{i=1}^{y} p_i\left(\lambda_i, r+k\right) = 0.$$

Then we can solve for c_1 to see that

$$c_1 = c(\mathcal{A},m) := \frac{\sum_{k=0}^{a_z+1} \alpha_k s_{\mathcal{A}}(r+k,m)}{|\mathcal{A}|^r\, g\left(|\mathcal{A}|\right)}. \tag{4.5}$$

□

Example 4.3. Let $\mathcal{A} = \{0,2,3\}$. Then

$$f_{\mathcal{A}}(2\ell) = f_{\mathcal{A}}(\ell) + f_{\mathcal{A}}(\ell-1) \tag{4.6}$$

and

$$f_{\mathcal{A}}(2\ell+1) = f_{\mathcal{A}}(\ell-1), \tag{4.7}$$

so

$$\begin{pmatrix} f_{\mathcal{A}}(2^{k+1}m) \\ f_{\mathcal{A}}(2^{k+1}m-1) \\ f_{\mathcal{A}}(2^{k+1}m-2) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} f_{\mathcal{A}}(2^{k}m) \\ f_{\mathcal{A}}(2^{k}m-1) \\ f_{\mathcal{A}}(2^{k}m-2) \end{pmatrix}.$$

Hence $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ satisfies $\omega_{k+1}(m) = M\omega_k(m)$. The characteristic polynomial of M is

$$g(x) = -(x-1)(x^2 - x - 1). \tag{4.8}$$

Let F_k denote the k-th Fibonacci number. Then

$$f_{\mathcal{A}}(2^k - 1) = F_{k-1} \tag{4.9}$$

for all $k \geq 1$. This can be shown by using induction and Equations (4.6) and (4.7) to prove that $f_{\mathcal{A}}(2^k - 2) = F_k$ for all $k \geq 2$ and observing that Equation (4.7) gives $f_{\mathcal{A}}(2^k - 1) = f_{\mathcal{A}}(2^{k-1} - 2)$.

Considering the summatory function with $m = 1$ and using Equations (4.6),(4.7), and (4.9), we see that

$$\begin{aligned}
s_{\mathcal{A}}(r,1) &= \sum_{n=2^r}^{2^{r+1}-1} f_{\mathcal{A}}(n) \\
&= \sum_{n=2^{r-1}}^{2^r-1} (f_{\mathcal{A}}(2n) + f_{\mathcal{A}}(2n+1)) \\
&= \sum_{n=2^{r-1}}^{2^r-1} (f_{\mathcal{A}}(n) + f_{\mathcal{A}}(n-1) + f_{\mathcal{A}}(n-1)) \\
&= s_{\mathcal{A}}(r-1,1) + 2\sum_{n=2^{r-1}}^{2^r-1} f_{\mathcal{A}}(n-1) \\
&= s_{\mathcal{A}}(r-1,1) + 2\sum_{n=2^{r-1}}^{2^r-1} f_{\mathcal{A}}(n) + 2f_{\mathcal{A}}(2^{r-1}-1) - 2f_{\mathcal{A}}(2^r - 1) \\
&= 3s_{\mathcal{A}}(r-1,1) + 2f_{\mathcal{A}}(2^{r-1}-1) - 2f_{\mathcal{A}}(2^r-1) \\
&= 3s_{\mathcal{A}}(r-1,1) + 2F_{r-2} - 2F_{r-1} \\
&= 3s_{\mathcal{A}}(r-1,1) - 2F_{r-3}.
\end{aligned}$$

This is an inhomogeneous recurrence relation for $s_{\mathcal{A}}(r,1)$. We first consider the corresponding homogeneous recurrence relation $s_{\mathcal{A}}(r,1) = 3s_{\mathcal{A}}(r-1,1)$, which has solution

$$s_{\mathcal{A}}(r,1) = c_1 3^r,$$

for some c_1 in $\mathbb{Q}$. Recall that the characteristic polynomial $g(x)$ of M has roots $1, \phi$, and $\bar{\phi}$, each with

multiplicity 1. Hence the solution to the inhomogeneous recurrence relation is

$$s_{\mathcal{A}}(r,1) = c_1 3^r + c_2\phi^r + c_3\bar{\phi}^r + c_4(1)^r, \tag{4.10}$$

where $c_2, c_3, c_4 \in \mathbb{Q}$. Observe that the $c_1 3^r$ summand will dominate as $r \to \infty$, so

$$\lim_{r\to\infty} \frac{s_{\mathcal{A}}(r,1)}{3^r} = c_1$$

and $s_{\mathcal{A}}(r,1) \approx c_1 3^r$.

Using Equations (4.8) and (4.10), we can compute c_1 as

$$\begin{aligned} s_{\mathcal{A}}(r+2,1) - s_{\mathcal{A}}(r+1,1) - s_{\mathcal{A}}(r,1) &= c_1 3^r(3^2 - 3 - 1) + c_2\phi^r(\phi^2 - \phi - 1) \\ &\quad + c_3\bar{\phi}^r(\bar{\phi}^2 - \bar{\phi} - 1) + c_4(1^2 - 1 - 1) \\ &= c_1 3^r \cdot 5 - c_4. \end{aligned}$$

Plugging in $r = 1$ and $r = 0$ and computing sums, we see that $c_1 = 2/5$. Hence

$$\lim_{r\to\infty} \frac{s_{\mathcal{A}}(r,1)}{3^r} = \frac{2}{5}$$

and $s_{\mathcal{A}}(r,1) \approx \frac{2}{5}(3)^r$.

Given a set $\mathcal{A} = \{0, a_1, \ldots, a_z\}$, let $\tilde{\mathcal{A}}$ be

$$\tilde{\mathcal{A}} := \{0, a_z - a_{z-1}, \ldots, a_z - a_1, a_z\}.$$

The following chart displays the value $c(\mathcal{A},1)$ for various sets $\mathcal{A}$ and their corresponding sets $\tilde{\mathcal{A}}$, where $s_{\mathcal{A}}(r,1) \approx c(\mathcal{A},1)|\mathcal{A}|^r$. Note that in all cases the denominator of $c(\mathcal{A},1)$ is the same as that of $c(\tilde{\mathcal{A}},1)$. The following theorem will show that this holds for all $\mathcal{A}$.

$\mathcal{A}$	$c(\mathcal{A},1)$	$\mathrm{N}(c(\mathcal{A},1))$	$\tilde{\mathcal{A}}$	$c(\tilde{\mathcal{A}},1)$	$\mathrm{N}(c(\tilde{\mathcal{A}},1))$
$\{0,1,2,4\}$	$\frac{7}{11}$	0.636	$\{0,2,3,4\}$	$\frac{3}{11}$	0.273
$\{0,2,3,6\}$	$\frac{2531}{9536}$	0.265	$\{0,3,4,6\}$	$\frac{1344}{9536}$	0.141
$\{0,1,6,9\}$	$\frac{3401207}{16513920}$	0.206	$\{0,3,8,9\}$	$\frac{1156032}{16513920}$	0.070
$\{0,1,7,9\}$	$\frac{132416}{655040}$	0.202	$\{0,2,8,9\}$	$\frac{51145}{655040}$	0.078
$\{0,4,5,6,9\}$	$\frac{4044}{83753}$	0.048	$\{0,3,4,5,9\}$	$\frac{6716}{83753}$	0.080

Table 4.1: $c(\mathcal{A},1)$ for various sets $\mathcal{A}$ and $\tilde{\mathcal{A}}$

Theorem 4.3. *Let $\mathcal{A}, f_{\mathcal{A}}(n), M = [m_{\alpha,\beta}]$, and $\tilde{\mathcal{A}}$ be as above, with $0 \le \alpha, \beta \le a_z$. Let $N = [n_{\alpha,\beta}]$ be the $(a_z+1)\times(a_z+1)$ matrix such that*

$$\begin{pmatrix} f_{\tilde{\mathcal{A}}}(2n) \\ f_{\tilde{\mathcal{A}}}(2n-1) \\ \vdots \\ f_{\tilde{\mathcal{A}}}(2n-a_z) \end{pmatrix} = N \begin{pmatrix} f_{\tilde{\mathcal{A}}}(n) \\ f_{\tilde{\mathcal{A}}}(n-1) \\ \vdots \\ f_{\tilde{\mathcal{A}}}(n-a_z) \end{pmatrix}.$$

Then $m_{\alpha,\beta} = n_{a_z-\alpha,a_z-\beta}$.

Proof. Recall that we can write

$$\mathcal{A} := \{0, 2b_1, \ldots, 2b_s, 2c_1+1, \ldots, 2c_t+1\},$$

so that

$$f_{\mathcal{A}}(2n-2j) = f_{\mathcal{A}}(n-j) + f_{\mathcal{A}}(n-j-b_1) + \cdots + f_{\mathcal{A}}(n-j-b_s)$$

and

$$f_{\mathcal{A}}(2n-2j-1) = f_{\mathcal{A}}(n-j-c_1-1) + \cdots + f_{\mathcal{A}}(n-j-c_t-1)$$

for j sufficiently large.

Then $m_{\alpha,\beta} = 1$ if and only if $f_{\mathcal{A}}(n-\beta)$ is a summand in the recursive sum that expresses $f_{\mathcal{A}}(2n-\alpha)$, which happens if and only if $2n-\alpha = 2(n-\beta)+K$, where $K \in \mathcal{A}$, and this is equivalent to $2\beta-\alpha$ belonging to $\mathcal{A}$.

Now $n_{a_z-\alpha,a_z-\beta} = 1$ if and only if $f_{\tilde{\mathcal{A}}}(n-(a_z-\beta))$ is a summand in the recursive sum that expresses $f_{\tilde{\mathcal{A}}}(2n-(a_z-\alpha))$, which happens if and only if $2n-(a_z-\alpha) = 2(n-(a_z-\beta))+\tilde{K}$, where $\tilde{K} \in \tilde{\mathcal{A}}$. This means that $a_z+\alpha-2\beta = \tilde{K}$, which gives $2\beta-\alpha \in \mathcal{A}$. □

Thus $M = A^{-1}NA$, where

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

so M and N have the same characteristic polynomial. By taking $n = 2^r m$, we see that $c(\mathcal{A}, m)$ and $c\left(\tilde{\mathcal{A}}, m\right)$ have the same denominator.

Chapter 5

Open Questions

In this chapter, we discuss open questions relating to the problems, theorems, and examples in Chapters 3 and 4.

The original statement by Cooper, Eichhorn, and O'Bryant in [3] was, "The most interesting issued raised in this section, which remains unanswered, is to describe the set $\{\delta\left(\overline{P}\right) : P \text{ is a polynomial}\}$. For example, is there an n with $\delta\left(\overline{P_n}\right) = 3/4$?" It is trivial that the infimum of the set is 0, and we saw in Chapter 3 that the supremum of the set is 1. The cluster points of the set remain to be determined, as does whether or not $3/4$ belongs to the set.

We would like to show that $4^r - 1$ is in fact the order of the robust polynomials $f_{r,1}$ of Theorem 3.11 and their reciprocals $f_{(R),r,1}$ of Corollary 3.12 rather than a multiple of the order, which is the result we now have. Similarly, we hope to show that $4^r + 2^r + 1$ is the exact order of the robust polynomials $f_{r,2}$ and $f_{(R),r,2}$ of Theorem 3.13 and Corollary 3.14.

A nicer formula for $c(\mathcal{A}, m)$ than that given in Equation (4.5) is desired and seems likely. To that end, we have computed values of $c(\mathcal{A})$ for a variety of sets $\mathcal{A}$ but have not been able to detect any patterns. Table 5.1 shows $c(\mathcal{A}, 1)$ for all sets of the form $\mathcal{A} = \{0, 1, k\}$, where $2 \leq k \leq 15$. We have also computed $c(\mathcal{A}, 1)$ for some sets with $|\mathcal{A}| = 4$ and $|\mathcal{A}| = 5$, and that data is contained in Table 4.1. Larger sets have not been considered because computations become increasingly tedious as the cardinality of $\mathcal{A}$ grows.

We would like to find more families of robust polynomials. It seems that the best way to do this would be to proceed as before, collecting large amounts of data and working to generalize the specific robust polynomials found in that data. More efficient computing and coding will be needed, however, to obtain more data. Coding in Sage or PARI/GP would likely be beneficial, as would continuing to utilize Campus Cluster and other available high-performance computing systems.

Another open problem is to consider properties of $f_{\mathcal{A}}(n)$ in bases other than 2. Calculations of sequences $(f_{\mathcal{A}}(n)) \bmod 3$ for $\mathcal{A} = \{0, 1, 3\}, \{0, 2, 3\}, \{0, 1, 4, 9\}, \{0, 1, 5, 9, 10\}, \{0, 2, 3, 4\}, \{0, 1, 2, \ldots, 2^j\}$ for $2 \leq j \leq 6$, and $\{0, 1, 3, \ldots, 3^j\}$ for $2 \leq j \leq 4$ showed no immediately obvious periodicity properties. We also considered the sequence $\left(f_{\{0,2,8,9\}}(n)\right) \bmod 3, 4, 5, 6, 7$, and 8 but noticed no periodicities.

$\mathcal{A}$	$c(\mathcal{A},1)$	$\mathrm{N}(c(\mathcal{A},1))$	$\mathcal{A}$	$c(\mathcal{A},1)$	$\mathrm{N}(c(\mathcal{A},1))$
$\{0,1,2\}$	1	1.000	$\{0,1,3\}$	$\frac{4}{5}$	0.800
$\{0,1,4\}$	$\frac{5}{8}$	0.625	$\{0,1,5\}$	$\frac{14}{25}$	0.560
$\{0,1,6\}$	$\frac{425}{852}$	0.499	$\{0,1,7\}$	$\frac{176}{391}$	0.450
$\{0,1,8\}$	$\frac{137}{338}$	0.405	$\{0,1,9\}$	$\frac{1448}{3775}$	0.384
$\{0,1,10\}$	$\frac{1990}{5527}$	0.360	$\{0,1,11\}$	$\frac{3223}{9476}$	0.340
$\{0,1,12\}$	$\frac{2020}{6283}$	0.322	$\{0,1,13\}$	$\frac{47228}{154123}$	0.306
$\{0,1,14\}$	$\frac{35624}{122411}$	0.291	$\{0,1,15\}$	$\frac{699224}{2501653}$	0.280

Table 5.1: $c(\mathcal{A},1)$ for all sets of the form $\mathcal{A}=\{0,1,k\}$, where $2\leq k\leq 15$

.

Recall the upper bound from [8, 8.78] of $2^{k/2}$ for $|\ell_1(f^*(x))-\ell_{0,M-1}(f^*(x))|$ for a polynomial $f(x)$ of degree k and order M discussed at the end of Chapter 2. The most extreme robust examples found thus far are those given in Examples 3.1, 3.2, 3.3, and 3.4. Recall $\beta(f_{3,1}(x))=\beta\left(f_{(R),3,1}(x)\right)=(37,26)$ and $\deg(f_{3,1}(x))=\deg\left(f_{(R),3,1}(x)\right)=9$. Additionally, $\beta(f_{3,2}(x))=\beta\left(f_{(R),3,2}(x)\right)=(45,28)$ and $\deg(f_{3,2}(x))=\deg\left(f_{(R),3,2}(x)\right)=10$. Using the bound from [8], we have

$$\left|\ell_1\left(f^*_{3,1}(x)\right)-\ell_{0,62}\left(f^*_{3,1}(x)\right)\right|=\left|\ell_1\left(f^*_{(R),3,1}(x)\right)-\ell_{0,62}\left(f^*_{(R),3,1}(x)\right)\right|=37-26=11\leq 2^{9/2}\approx 22.6$$

and

$$\left|\ell_1\left(f^*_{3,2}(x)\right)-\ell_{0,72}\left(f^*_{3,2}(x)\right)\right|=\left|\ell_1\left(f^*_{(R),3,2}(x)\right)-\ell_{0,72}\left(f^*_{(R),3,2}(x)\right)\right|=45-28=17\leq 2^{10/2}=32.$$

For any $r\geq 3$, if we assume that 4^r-1 and 4^r+2^r+1 are the exact orders of $f_{r,1}$ and $f_{r,2}$, respectively, we have

$$\begin{aligned}\left|\ell_1\left(f^*_{r,1}(x)\right)-\ell_{0,4^r-2}\left(f^*_{r,1}(x)\right)\right|&=\left|\ell_1\left(f^*_{(R),r,1}(x)\right)-\ell_{0,4^r-2}\left(f^*_{(R),r,1}(x)\right)\right|\\&=4^r-3^r-(3^r-1)\\&=4^r-2\cdot 3^r+1\\&\ll 2^{\frac{1}{2}(2^r+1)}\\&=4^{2^{r-2}+\frac{1}{4}}\end{aligned}$$

and

$$\begin{aligned}\left|\ell_1\left(f^*_{r,2}(x)\right) - \ell_{0,4^r+2^r}\left(f^*_{r,2}(x)\right)\right| &= \left|\ell_1\left(f^*_{(R),r,2}(x)\right) - \ell_{0,4^r+2^r}\left(f^*_{(R),r,2}(x)\right)\right| \\ &= 4^r - 3^r + 2^r - (3^r + 1) \\ &= 4^r - 2 \cdot 3^r + 2^r - 1 \\ &\ll 2^{\frac{1}{2}(2^r+2)} \\ &= 4^{2^{r-2}+\frac{1}{2}},\end{aligned}$$

where the penultimate expressions in both displayed equations come from the upper bound in [8].

Since these are the most extreme examples but do not push the upper bound, we suspect that the bound of $2^{k/2}$ could be improved in the $\mathbb{F}_2$ case.

Appendix A

Searching for Robust Polynomials by Order

This appendix contains samples of the Mathematica code used in determining $\beta(f(x))$ for all polynomials $f(x) \in \mathbb{F}_2[x]$ with order less than or equal to 83. It also contains tables with information on all robust polynomials in that range.

A.1

```
k := 6
Factor[1 + x^k, Modulus → 2]
(1 + x)^2 (1 + x + x^2)^2
m = FactorList[1 + x^k, Modulus → 2]
{{1, 1}, {1 + x, 2}, {1 + x + x^2, 2}}
A = Append[Table[m[[2, 1]]^i, {i, m[[2, 2]]}], 1]
{1 + x, (1 + x)^2, 1}
B = Append[Table[m[[3, 1]]^i, {i, m[[3, 2]]}], 1]
{1 + x + x^2, (1 + x + x^2)^2, 1}
Q = Outer[Times, A, B]
{{(1 + x) (1 + x + x^2), (1 + x) (1 + x + x^2)^2, 1 + x},
 {(1 + x)^2 (1 + x + x^2), (1 + x)^2 (1 + x + x^2)^2, (1 + x)^2}, {1 + x + x^2, (1 + x + x^2)^2, 1}}
r = Dimensions[Q]
{3, 3}
r[[1]]
3
```

Figure A.1: Mathematica code for determining $\beta_6(g(x))$ for all polynomial divisors of $1 + x^6$

```
For[j = 1, j < r[[1]] + 1, j++,
 For[i = 1, i < Length[Q[[j]]] + 1, i++, Print[Q[[j, i]]]; p[x_] := Q[[j, i]]; a := Max[Reap[For[n = 1,
      n < 1000, n++, If[PolynomialRemainder[1 + x^n, p[x], x, Modulus → 2] == 0, Break[]]]; Sow[n]]];
  q[x_] := PolynomialQuotient[1 + x^a, p[x], x, Modulus → 2]; c := q[x] /. x → 1;
  Print[q[x]]; Print[Row[{c, a}, s]]]]
```

$(1+x)\left(1+x+x^2\right)$

1

1 s 3

$(1+x)\left(1+x+x^2\right)^2$

$1+x$

2 s 6

$1+x$

1

1 s 1

$(1+x)^2\left(1+x+x^2\right)$

$1+x+x^2$

3 s 6

$(1+x)^2\left(1+x+x^2\right)^2$

1

1 s 6

$(1+x)^2$

1

1 s 2

$1+x+x^2$

$1+x$

2 s 3

$\left(1+x+x^2\right)^2$

$1+x^2$

2 s 6

1

$1+x$

2 s 1

Figure A.2: Mathematica code for determining $\beta_6(g(x))$ for all polynomial divisors of $1+x^6$. Each polynomial divisor $g(x)$ is listed, followed by the polynomial $g^*(x) := (1+x^6)/g(x)$, and then $\ell_1(g^*(x))$ s $\mathrm{ord}(g(x))$.

A.2

```
k := 7

Factor[1 + x^k, Modulus → 2]

(1 + x) (1 + x + x^3) (1 + x^2 + x^3)

m = FactorList[1 + x^k, Modulus → 2]

{{1, 1}, {1 + x, 1}, {1 + x + x^3, 1}, {1 + x^2 + x^3, 1}}

A = Append[Table[m[[2, 1]]^i, {i, m[[2, 2]]}], 1]

{1 + x, 1}

B = Append[Table[m[[3, 1]]^i, {i, m[[3, 2]]}], 1]

{1 + x + x^3, 1}

F = Append[Table[m[[4, 1]]^i, {i, m[[4, 2]]}], 1]

{1 + x^2 + x^3, 1}

Q = Outer[Times, A, B]

{{(1 + x) (1 + x + x^3), 1 + x}, {1 + x + x^3, 1}}

T = Flatten[Q]

{(1 + x) (1 + x + x^3), 1 + x, 1 + x + x^3, 1}

S = Outer[Times, T, F]

{{(1 + x) (1 + x + x^3) (1 + x^2 + x^3), (1 + x) (1 + x + x^3)},
 {(1 + x) (1 + x^2 + x^3), 1 + x}, {(1 + x + x^3) (1 + x^2 + x^3), 1 + x + x^3}, {1 + x^2 + x^3, 1}}

r = Dimensions[S]

{4, 2}

r[[1]]

4

r[[2]]

2
```

Figure A.3: Mathematica code for determining $\beta(g(x))$ for all polynomial divisors of $1 + x^7$

```
For[j = 1, j < r[[1]] + 1, j++,
 For[i = 1, i < Length[S[[j]]] + 1, i++, Print[S[[j, i]]]; p[x_] := S[[j, i]]; a := Max[Reap[For[n = 1,
      n < 1000, n++, If[PolynomialRemainder[1 + x^n, p[x], x, Modulus → 2] == 0, Break[]]]; Sow[n]]];
  q[x_] := PolynomialQuotient[1 + x^a, p[x], x, Modulus → 2]; c := q[x] /. x → 1;
  Print[q[x]]; Print[Row[{c, a}, s]]]]
```

$(1+x)\left(1+x+x^3\right)\left(1+x^2+x^3\right)$

1

1 s 7

$(1+x)\left(1+x+x^3\right)$

$1+x^2+x^3$

3 s 7

$(1+x)\left(1+x^2+x^3\right)$

$1+x+x^3$

3 s 7

$1+x$

1

1 s 1

$\left(1+x+x^3\right)\left(1+x^2+x^3\right)$

$1+x$

2 s 7

$1+x+x^3$

$1+x+x^2+x^4$

4 s 7

$1+x^2+x^3$

$1+x^2+x^3+x^4$

4 s 7

1

$1+x$

2 s 1

Figure A.4: Mathematica code for determining $\beta(g(x))$ for all polynomial divisors of $1+x^7$. Each polynomial divisor $g(x)$ is listed, followed by the polynomial $g^*(x)$, and then $\ell_1(g^*(x))$ s $\mathrm{ord}(g(x))$.

A.3

```
For[j = 1, j < r[[1]] + 1, j++,
 For[i = 1, i < Length[u[[j]]] + 1, i++, p[x_] := u[[j, i]]; a := Max[Reap[For[n = 1, n < 1000,
      n++, If[PolynomialRemainder[1 + x^n, p[x], x, Modulus → 2] == 0, Break[]]]; Sow[n]]];
  q[x_] := PolynomialQuotient[1 + x^a, p[x], x, Modulus → 2]; c := q[x] /. x → 1;
  If[2 * c > a + 1, Print[u[[j, i]]]; Print[q[x]]; Print[Row[{c, a}, s]],]]]
```

$(1+x)\left(1+x+x^9\right)$

$$1+x^2+x^4+x^6+x^8+x^9+x^{12}+x^{13}+x^{16}+x^{17}+x^{18}+x^{20}+x^{21}+x^{22}+$$
$$x^{24}+x^{25}+x^{26}+x^{27}+x^{32}+x^{33}+x^{34}+x^{35}+x^{36}+x^{38}+x^{40}+x^{41}+x^{42}+x^{43}+x^{44}+$$
$$x^{45}+x^{48}+x^{49}+x^{50}+x^{51}+x^{52}+x^{53}+x^{54}+x^{56}+x^{57}+x^{58}+x^{59}+x^{60}+x^{61}+x^{62}+x^{63}$$

45 s 73

$(1+x)\left(1+x^8+x^9\right)$

$$1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+$$
$$x^{18}+x^{19}+x^{20}+x^{21}+x^{22}+x^{23}+x^{25}+x^{27}+x^{28}+x^{29}+x^{30}+x^{31}+x^{36}+x^{37}+x^{38}+$$
$$x^{39}+x^{41}+x^{42}+x^{43}+x^{45}+x^{46}+x^{47}+x^{50}+x^{51}+x^{54}+x^{55}+x^{57}+x^{59}+x^{61}+x^{63}$$

45 s 73

$1+x+x^2+x^4+x^9$

$$1+x+x^3+x^7+x^8+x^9+x^{10}+x^{11}+x^{14}+x^{17}+x^{18}+x^{19}+x^{20}+x^{21}+x^{22}+x^{25}+x^{26}+x^{27}+x^{28}+x^{30}+x^{31}+$$
$$x^{32}+x^{34}+x^{35}+x^{38}+x^{39}+x^{40}+x^{41}+x^{42}+x^{44}+x^{47}+x^{48}+x^{49}+x^{50}+x^{54}+x^{55}+x^{56}+x^{57}+x^{59}+x^{64}$$

40 s 73

$1+x^5+x^7+x^8+x^9$

$$1+x^5+x^7+x^8+x^9+x^{10}+x^{14}+x^{15}+x^{16}+x^{17}+x^{20}+x^{22}+x^{23}+x^{24}+x^{25}+x^{26}+x^{29}+x^{30}+x^{32}+x^{33}+x^{34}+$$
$$x^{36}+x^{37}+x^{38}+x^{39}+x^{42}+x^{43}+x^{44}+x^{45}+x^{46}+x^{47}+x^{50}+x^{53}+x^{54}+x^{55}+x^{56}+x^{57}+x^{61}+x^{63}+x^{64}$$

40 s 73

1

$1+x$

2 s 1

Figure A.5: Mathematica code for determining $\beta(g(x))$ for all polynomial divisors of $1+x^{73}$. The u referred to in the code is a 256 by 2 table containing all polynomial divisors of $1+x^{73}$. Each robust polynomial divisor $g(x)$ is listed, followed by the polynomial $g^*(x)$, and then $\ell_1(g^*(x))$ s $\mathrm{ord}(g(x))$.

A.4

$f(x)$	$\mathrm{ord}(f(x))$	$\beta(f(x))$
$(1+x+x^2)^2(1+x+x^4)$	30	$(16,14)$
$(1+x+x^2)^2(1+x^3+x^4)$	30	$(16,14)$
$(1+x)(1+x+x^2)^2(1+x+x^3)^2$	30	$(16,14)$
$(1+x)(1+x+x^2)^2(1+x^2+x^3)^2$	30	$(16,14)$
$1+x+x^5+x^9+x^{10}$	33	$(18,15)$
$(1+x)(1+x+x^2)(1+x+x^3)^2$	42	$(22,20)$
$(1+x)(1+x+x^2)(1+x^2+x^3)^2$	42	$(22,20)$
$(1+x)(1+x+x^3+x^4+x^8)$	51	$(27,24)$
$(1+x)(1+x^4+x^5+x^7+x^8)$	51	$(27,24)$
$(1+x)(1+x+x^2)(1+x+x^2+x^4+x^6+x^7+x^8)$	51	$(27,24)$
$(1+x+x^2)(1+x^2+x^3+x^4+x^9+x^{14}+x^{15}+x^{16}+x^{18})$	57	$(30,27)$
$(1+x)^4(1+x+x^4)$	60	$(31,29)$
$(1+x)^4(1+x^3+x^4)$	60	$(31,29)$
$(1+x)^4(1+x+x^2)(1+x+x^2+x^3+x^4)$	60	$(31,29)$
$(1+x^2+x^5)^2(1+x+x^2+x^3+x^5)$	62	$(32,30)$
$(1+x^3+x^5)^2(1+x^2+x^3+x^4+x^5)$	62	$(32,30)$
$(1+x^2+x^5)^2(1+x^2+x^3+x^4+x^5)$	62	$(32,30)$
$(1+x^3+x^5)^2(1+x+x^2+x^3+x^5)$	62	$(32,30)$
$(1+x+x^2+x^3+x^4)(1+x^2+x^5+x^6+x^7+x^{10}+x^{12})$	65	$(34,31)$
$1+x^2+x^5+x^6+x^7+x^{10}+x^{12}$	65	$(34,31)$
$(1+x)(1+x+x^2)^2(1+x^3+x^5+x^7+x^{10})$	66	$(34,32)$
$(1+x)^4(1+x+x^2+x^4+x^6+x^7+x^8)$	68	$(35,33)$

Table A.1: All robust polynomials of order less than or equal to 83 except those of order 63 and 73

$f(x)$	$\mathrm{ord}(f(x))$	$\beta(f(x))$
$(1+x)(1+x+x^2)(1+x+x^6)(1+x^2+x^4+x^5+x^6)$	63	$(33, 30)$
$(1+x)(1+x+x^2)(1+x^5+x^6)(1+x+x^2+x^4+x^6)$	63	$(33, 30)$
$(1+x)(1+x+x^3)(1+x+x^6)(1+x^3+x^6)$	63	$(33, 30)$
$(1+x)(1+x^2+x^3)(1+x^5+x^6)(1+x^3+x^6)$	63	$(33, 30)$
$(1+x)(1+x+x^3)(1+x^3+x^6)(1+x+x^2+x^4+x^6)$	63	$(33, 30)$
$(1+x)(1+x^2+x^3)(1+x^3+x^6)(1+x^2+x^4+x^5+x^6)$	63	$(33, 30)$
$(1+x)(1+x^3+x^6)(1+x+x^2+x^4+x^6)$	63	$(33, 30)$
$(1+x)(1+x^3+x^6)(1+x^2+x^4+x^5+x^6)$	63	$(33, 30)$
$(1+x+x^2)(1+x+x^6)$	63	$(34, 29)$
$(1+x+x^2)(1+x^5+x^6)$	63	$(34, 29)$
$(1+x+x^6)(1+x^5+x^6)(1+x+x^2+x^5+x^6)(1+x+x^4+x^5+x^6)$	63	$(34, 29)$
$(1+x)(1+x+x^3)(1+x^2+x^3)(1+x+x^2+x^5+x^6)$	63	$(35, 28)$
$(1+x)(1+x+x^3)(1+x^2+x^3)(1+x+x^4+x^5+x^6)$	63	$(35, 28)$
$(1+x+x^3)(1+x+x^2+x^4+x^6)(1+x+x^2+x^5+x^6)$	63	$(36, 27)$
$(1+x^2+x^3)(1+x+x^4+x^5+x^6)(1+x^2+x^4+x^5+x^6)$	63	$(36, 27)$
$(1+x+x^3)(1+x^5+x^6)$	63	$(36, 27)$
$(1+x^2+x^3)(1+x+x^6)$	63	$(36, 27)$
$(1+x+x^2+x^4+x^6)(1+x^2+x^3+x^5+x^6)$	63	$(36, 27)$
$(1+x+x^3+x^4+x^6)(1+x^2+x^4+x^5+x^6)$	63	$(36, 27)$
$(1+x)(1+x+x^2)(1+x^2+x^3+x^5+x^6)$	63	$(37, 26)$
$(1+x)(1+x+x^2)(1+x+x^3+x^4+x^6)$	63	$(37, 26)$
$(1+x+x^6)(1+x^5+x^6)$	63	$(38, 25)$
$1+x+x^2+x^4+x^9$	73	$(40, 33)$
$1+x^5+x^7+x^8+x^9$	73	$(40, 33)$
$(1+x)(1+x+x^9)$	73	$(45, 28)$
$(1+x)(1+x^8+x^9)$	73	$(45, 28)$

Table A.2: All robust polynomials of order 63 and 73

Appendix B

Searching for Robust Quadrinomials by Degree

This appendix contains samples of the Mathematica code used in determining $\beta(f(x))$ for all quadrinomials $f(x) \in \mathbb{F}_2[x]$ of degree less than or equal to 18. Sections B.1 and B.2 contain code and data for quadrinomials of the form $1 + x + x^j + x^{12}$ and $1 + x^2 + x^j + x^{12}$, respectively. Section B.3 contains tables of information about robust quadrinomials of degree less than or equal to 18.

B.1

```
For[j = 1, j < 10, j++,
 For[i = 2, j < i < 12, i++, p[x_] := 1 + x^j + x^i + x^12; a := Max[Reap[For[n = 1, n < 10 000,
      n++, If[PolynomialRemainder[1 + x^n, p[x], x, Modulus → 2] == 0, Break[]]]; Sow[n]]];
  q[x_] := PolynomialQuotient[1 + x^a, p[x], x, Modulus → 2]; c := q[b] /. b → 1;
  Print[p[x]]; Print[a]; Print[Row[{c, a - c}, s]]]]
```

$1 + x + x^2 + x^{12}$

595

303 s 292

$1 + x + x^3 + x^{12}$

2046

1023 s 1023

$1 + x + x^4 + x^{12}$

219

101 s 118

$1 + x + x^5 + x^{12}$

1016

508 s 508

$1 + x + x^6 + x^{12}$

1905

953 s 952

$1 + x + x^7 + x^{12}$

126

61 s 65

$1 + x + x^8 + x^{12}$

651

323 s 328

$1 + x + x^9 + x^{12}$

868

433 s 435

$1 + x + x^{10} + x^{12}$

1533

767 s 766

$1 + x + x^{11} + x^{12}$

22

11 s 11

Figure B.1: Mathematica code for determining $\beta(f(x))$ for all quadrinomials of the form $1 + x + x^j + x^{12}$. For each $2 \leq j \leq 11$, the quadrinomial $f_j(x) = 1 + x + x^j + x^{12}$ is given, followed by $\mathrm{ord}(f_j(x))$, and then $\beta(f_j(x))$ given as $\ell_1(f_j^*(x))$ s $\ell_{0,\mathrm{ord}(f_j(x))-1}(f_j^*(x))$.

B.2

```
For[j = 2, j < 10, j++,
 For[i = 3, j < i < 12, i++, p[x_] := 1 + x^j + x^i + x^12; a := Max[Reap[For[n = 1, n < 10 000,
      n++, If[PolynomialRemainder[1 + x^n, p[x], x, Modulus → 2] == 0, Break[]]]; Sow[n]]];
  q[x_] := PolynomialQuotient[1 + x^a, p[x], x, Modulus → 2]; c := q[b] /. b → 1;
  Print[p[x]]; Print[a]; Print[Row[{c, a - c}, s]]]]
```

$1 + x^2 + x^3 + x^{12}$

89

33 s 56

$1 + x^2 + x^4 + x^{12}$

62

15 s 47

$1 + x^2 + x^5 + x^{12}$

465

231 s 234

$1 + x^2 + x^6 + x^{12}$

56

14 s 42

$1 + x^2 + x^7 + x^{12}$

2047

1023 s 1024

$1 + x^2 + x^8 + x^{12}$

42

11 s 31

$1 + x^2 + x^9 + x^{12}$

1905

953 s 952

$1 + x^2 + x^{10} + x^{12}$

20

5 s 15

$1 + x^2 + x^{11} + x^{12}$

1533

767 s 766

Figure B.2: Mathematica code for determining $\beta(f(x))$ for all quadrinomials of the form $1 + x^2 + x^j + x^{12}$. For each $3 \leq j \leq 11$, the quadrinomial $f_j(x) = 1 + x^2 + x^j + x^{12}$ is given, followed by $\mathrm{ord}(f_j(x))$, and then $\beta(f_j(x))$ given as $\ell_1(f_j^*(x))$ s $\ell_{0,\mathrm{ord}(f_j(x))-1}(f_j^*(x))$.

B.3

$f(x)$	$\mathrm{ord}(f(x))$	$\beta(f(x))$
$1+x+x^5+x^8$	60	$(31,29)$
$1+x^3+x^7+x^8$	60	$(31,29)$
$1+x^2+x^8+x^9$	63	$(37,26)$
$1+x+x^7+x^9$	63	$(37,26)$
$1+x^2+x^7+x^{10}$	155	$(79,76)$
$1+x^3+x^8+x^{10}$	155	$(79,76)$
$1+x+x^8+x^{10}$	73	$(45,28)$
$1+x^2+x^9+x^{10}$	73	$(45,28)$
$1+x+x^5+x^{11}$	315	$(159,156)$
$1+x^6+x^{10}+x^{11}$	315	$(159,156)$
$1+x+x^7+x^{11}$	341	$(181,160)$
$1+x^4+x^{10}+x^{11}$	341	$(181,160)$
$1+x^3+x^4+x^{11}$	508	$(255,253)$
$1+x^7+x^8+x^{11}$	508	$(255,253)$
$1+x^3+x^7+x^{11}$	341	$(181,160)$
$1+x^4+x^8+x^{11}$	341	$(181,160)$
$1+x+x^2+x^{12}$	595	$(303,292)$
$1+x^{10}+x^{11}+x^{12}$	595	$(303,292)$
$1+x+x^6+x^{13}$	762	$(383,379)$
$1+x^7+x^{12}+x^{13}$	762	$(383,379)$
$1+x+x^8+x^{13}$	2044	$(1023,1021)$
$1+x^5+x^{12}+x^{13}$	2044	$(1023,1021)$
$1+x^2+x^8+x^{13}$	819	$(435,384)$
$1+x^5+x^{11}+x^{13}$	819	$(435,384)$
$1+x^3+x^7+x^{13}$	1023	$(533,490)$
$1+x^6+x^{10}+x^{13}$	1023	$(533,490)$
$1+x^4+x^5+x^{13}$	2044	$(1023,1021)$
$1+x^8+x^9+x^{13}$	2044	$(1023,1021)$

Table B.1: All robust quadrinomials of degree less than or equal to 13

$f(x)$	$\mathrm{ord}(f(x))$	$\beta(f(x))$
$1+x+x^8+x^{14}$	889	$(447, 442)$
$1+x^6+x^{13}+x^{14}$	889	$(447, 442)$
$1+x^3+x^{10}+x^{14}$	889	$(447, 442)$
$1+x^4+x^{11}+x^{14}$	889	$(447, 442)$
$1+x^4+x^5+x^{14}$	2555	$(1279, 1276)$
$1+x^9+x^{10}+x^{14}$	2555	$(1279, 1276)$
$1+x^6+x^7+x^{14}$	1581	$(797, 784)$
$1+x^7+x^8+x^{14}$	1581	$(797, 784)$
$1+x+x^5+x^{15}$	5461	$(2773, 2688)$
$1+x^{10}+x^{14}+x^{15}$	5461	$(2773, 2688)$
$1+x+x^9+x^{15}$	5461	$(2773, 2688)$
$1+x^6+x^{14}+x^{15}$	5461	$(2773, 2688)$
$1+x^2+x^4+x^{15}$	1953	$(985, 968)$
$1+x^{11}+x^{13}+x^{15}$	1953	$(985, 968)$
$1+x^2+x^6+x^{15}$	5461	$(2773, 2688)$
$1+x^9+x^{13}+x^{15}$	5461	$(2773, 2688)$
$1+x^3+x^8+x^{15}$	2540	$(1271, 1269)$
$1+x^7+x^{12}+x^{15}$	2540	$(1271, 1269)$
$1+x+x^{10}+x^{16}$	10235	$(5119, 5116)$
$1+x^6+x^{15}+x^{16}$	10235	$(5119, 5116)$
$1+x^2+x^9+x^{16}$	4599	$(2327, 2272)$
$1+x^7+x^{14}+x^{16}$	4599	$(2327, 2272)$
$1+x^3+x^4+x^{16}$	7161	$(3591, 3570)$
$1+x^{12}+x^{13}+x^{16}$	7161	$(3591, 3570)$
$1+x^4+x^9+x^{16}$	7905	$(3963, 3942)$
$1+x^7+x^{12}+x^{16}$	7905	$(3963, 3942)$

Table B.2: All robust quadrinomials of degree $14, 15$, and 16

$f(x)$	$\mathrm{ord}(f(x))$	$\beta(f(x))$
$1+x+x^4+x^{17}$	10540	$(5275, 5265)$
$1+x^{13}+x^{16}+x^{17}$	10540	$(5275, 5265)$
$1+x+x^{15}+x^{17}$	255	$(175, 80)$
$1+x^2+x^{16}+x^{17}$	255	$(175, 80)$
$1+x^2+x^6+x^{17}$	16383	$(8277, 8106)$
$1+x^{11}+x^{15}+x^{17}$	16383	$(8277, 8106)$
$1+x^2+x^{12}+x^{17}$	16383	$(8277, 8106)$
$1+x^5+x^{15}+x^{17}$	16383	$(8277, 8106)$
$1+x^3+x^7+x^{17}$	7161	$(3583, 3578)$
$1+x^{10}+x^{14}+x^{17}$	7161	$(3583, 3578)$
$1+x^5+x^9+x^{17}$	16383	$(8277, 8106)$
$1+x^8+x^{12}+x^{17}$	16383	$(8277, 8106)$
$1+x+x^4+x^{18}$	32385	$(16203, 16182)$
$1+x^{14}+x^{17}+x^{18}$	32385	$(16203, 16182)$
$1+x+x^{13}+x^{18}$	3066	$(1551, 1515)$
$1+x^5+x^{17}+x^{18}$	3066	$(1551, 1515)$
$1+x+x^{16}+x^{18}$	273	$(191, 82)$
$1+x^2+x^{17}+x^{18}$	273	$(191, 82)$
$1+x^2+x^3+x^{18}$	15841	$(7941, 7900)$
$1+x^{15}+x^{16}+x^{18}$	15841	$(7941, 7900)$
$1+x^2+x^{11}+x^{18}$	1395	$(699, 696)$
$1+x^7+x^{16}+x^{18}$	1395	$(699, 696)$
$1+x^2+x^{13}+x^{18}$	40005	$(20013, 19992)$
$1+x^5+x^{16}+x^{18}$	40005	$(20013, 19992)$
$1+x^3+x^4+x^{18}$	14105	$(7081, 7024)$
$1+x^{14}+x^{15}+x^{18}$	14105	$(7081, 7024)$
$1+x^3+x^{10}+x^{18}$	40955	$(20479, 20476)$
$1+x^8+x^{15}+x^{18}$	40955	$(20479, 20476)$
$1+x^4+x^{13}+x^{18}$	4599	$(2303, 2296)$
$1+x^5+x^{14}+x^{18}$	4599	$(2303, 2296)$
$1+x^5+x^{12}+x^{18}$	7905	$(3961, 3944)$
$1+x^6+x^{13}+x^{18}$	7905	$(3961, 3944)$

Table B.3: All robust quadrinomials of degree 17 and 18

References

[1] Anders, K., M. Dennison, J. Lansing, and B. Reznick, *Congruence properties of binary partition functions*, Ann. Comb. **17** (2013), no.1, 15–26. MR3027571

[2] Brent, R. and P. Zimmermann, *The great trinomial hunt*, Notices Amer. Math. Soc. **58** (2011), no. 2, 233–239. MR2768116

[3] Cooper, J., D. Eichhorn, and K. O'Bryant, *Reciprocals of binary power series*, Int. J. Number Theory **2** (2006), no. 4, 499–522. MR2281861 (2007h:11015)

[4] Dennison, M. *A sequence related to the Stern sequence*, Ph.D. dissertation, University of Illinois at Urbana-Champaign, 2010.

[5] Euler, L., *Introduction to analysis of the infinite. Book I.* Translated from the Latin and with an introduction by John D. Blanton. Springer-Verlag, New York, 1988. MR0961255 (89g:01067)

[6] Golomb, S., *Shift register sequences*, with portions co-authored by L. Welch, R. Goldstein, and A. Hales. Holden-Day, Inc., San Francisco, Calif.-Cambridge-Amsterdam, 1967. MR0242575 (39 #3906)

[7] Granville, A. *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle*, Amer. Math. Monthly **99** (1992), no. 4, 318–331. MR1157222 (93a:05008)

[8] Lidl, R. and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and Its Applications 20. Cambridge Univ. Press, Cambridge, 1997. MR1429394 (97i:11115)

[9] Reznick, B., *A Stern introduction to combinatorial number theory*, Class notes, Math 595, UIUC, Spring 2012.

[10] Reznick, B., *Some binary partition functions*, Analytic Number Theory (Proc. Conference in honor of Paul Bateman), Birkhäuser, Boston, 1990, 451–457. MR1084197 (91k:11092)