Autocorrelation and Flatness of Height One Polynomials

by

Idris David Mercer

B.Sc. (Honours), University of Victoria, 1995

M.Sc., University of Toronto, 1997

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Summer 2005

APPROVAL

Name: Idris David Mercer

Degree: Doctor of Philosophy

Title of thesis: Autocorrelation and Flatness of Height One Polynomials

Examining Committee: Dr. Imin Chen
Chair

Dr. Peter Borwein, Senior Supervisor

Dr. Stephen Choi, Supervisory Committee

Dr. Petr Lisoněk, Supervisory Committee

Dr. Luis Goddyn
External to Supervisory Committee

Dr. Michael Filaseta
University of South Carolina
External to University

Date Approved: April 25, 2005

SIMON FRASER UNIVERSITY

PARTIAL COPYRIGHT LICENCE

Abstract

This thesis is concerned with two classes of polynomials whose **height** (meaning the largest absolute value of a coefficient) is 1: **Littlewood polynomials**, whose coefficients are $+1$ or -1, and **zero-one polynomials**, whose coefficients are 0 or 1. We are interested in the behaviour of these polynomials on the unit circle in the complex plane. Roughly speaking, there is a tendency for a polynomial to be 'flat' on the unit circle if its **autocorrelations** are 'near zero', where the 'autocorrelations' can be regarded as dot products that measure the 'periodicity' of the coefficient sequence of the polynomial.

In Chapter 1, we provide some illustrative conjectures as well as establishing some probabilistic language that is useful for studying the flatness or autocorrelations of 'typical' Littlewood polynomials or zero-one polynomials.

In Chapter 2, we use properties of cosine sums to prove results about roots on the unit circle of Littlewood polynomials possessing certain kinds of symmetries. In particular, we prove that a type of Littlewood polynomial called a **skewsymmetric** Littlewood polynomial cannot have any roots on the unit circle.

In Chapter 3, we show how one can compute all **moments** (meaning average values of powers) of autocorrelations of Littlewood polynomials, and we give an improved upper bound on the function that measures the minimum maximum autocorrelation (in absolute value) of a Littlewood polynomial.

In Chapter 4, we give explicit formulae for the average fourth power of the four-norm of a zero-one polynomial, and show that this yields a surprising new proof of a known result about Sidon sets.

Acknowledgments

The author would like to thank Simon Fraser University, as well as its Mathematics Department, for financial support and for being a pleasant place to work. He would also like to thank Peter Borwein for research assistantships and for asking the right questions. The helpful suggestions and feedback of numerous other faculty members, postdoctoral fellows, and graduate students was also appreciated.

The author would also like to thank the following individuals for their timely and personable assistance with authorship and copyright matters:

- Emo Philips and the OmniPop Talent Agency
- Lynne Okin Sheridan from the Licensing Department of the Bob Dylan Music Company

Dedication

To my parents, for all their years of encouragement,
to Jamie, for turning stressful times into happy times,
to my favourite dog, Kayley (31-Aug-1989—11-Mar-2005),
to all of the regulars and staff at SFU's Highland Pub, and
to everyone I ever drank beer with during the entire time I was at Simon Fraser.
I couldn't have done it without you.

'And malt does more than Milton can
To justify God's ways to man.'
—A.E. Housman, *A Shropshire Lad* (first published 1896)

Contents

Approval ii
Abstract iii
Acknowledgments iv
Dedication v
Contents vi
1 Introduction 1
1.1 The 'spaces' $\mathcal{L}_n$ and $\mathcal{A}_n$ 1
1.2 Autocorrelation 4
1.3 Flat Littlewood polynomials 8
1.4 Sidon sets 12
1.5 Some probabilistic language 14
2 Special Littlewood Polynomials 21
2.1 Self-reciprocals and skewsymmetrics 21
2.2 Relevant facts about cosine sums 26
2.3 Unimodular roots of special Littlewoods 36
3 Autocorrelation in $\mathcal{L}_n$ 40
3.1 Average of c_k^r over $\mathcal{L}_n$ 40
3.2 Bounds on Turyn's b function 47
4 Autocorrelation in $\mathcal{A}_n$ 52
4.1 Average of c_k^2 over $\mathcal{A}_n$, $\mathcal{B}_n$, and $\mathcal{A}_{n,m}$ 52
4.2 Ubiquity of Sidon sets 60
Bibliography 63

Chapter 1

Introduction

All the people we used to know
They're an illusion to me now
Some are mathematicians
Some are carpenters' wives
Don't know how it all got started
I don't know what they do with their lives
—'Tangled Up In Blue', Bob Dylan (by permission)

1.1 The 'spaces' $\mathcal{L}_n$ and $\mathcal{A}_n$

We begin by defining the main objects of study of this thesis, or in other words, by specifying the underlying 'spaces' we consider.

Definition 1.1 *We let $\mathcal{L}_n$ denote the set of all 2^n polynomials of the form*

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \quad \textit{where } a_j \in \{-1, +1\} \textit{ for all } j,$$

and we let $\mathcal{A}_n$ denote the set of all 2^n polynomials of the form

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \quad \textit{where } a_j \in \{0, 1\} \textit{ for all } j.$$

We call the elements of $\mathcal{L}_n$ **Littlewood polynomials**, *and we call the elements of $\mathcal{A}_n$* **zero-one polynomials**.

We will sometimes refer to the elements of $\mathcal{L}_n$ as the Littlewood polynomials of **length** n, which is consistent with the common convention of defining the 'length' of a polynomial to be the sum of the absolute values of its coefficients. Both $\mathcal{L}_n$ and $\mathcal{A}_n$ are examples of sets of **height one** polynomials, where (as is common elsewhere) the 'height' of a polynomial means the largest absolute value of the coefficients. We now single out two more examples of collections of height one polynomials as being worthy of special labels.

Definition 1.2 *We let* $\mathcal{A}_{n,m}$ *denote the set*

$$\{\alpha(z) = a_0 + \cdots + a_{n-1}z^{n-1} \in \mathcal{A}_n : \alpha(1) = m\}$$
$$= \{a_0 + \cdots + a_{n-1}z^{n-1} \in \mathcal{A}_n : a_j = 1 \text{ for precisely } m \text{ values of } j\}$$

and we let $\mathcal{B}_n$ *denote* $\mathcal{A}_{n+1} \setminus \mathcal{A}_n$.

Thus $\mathcal{A}_{n,m}$ has $\binom{n}{m}$ elements, and the 2^n elements of $\mathcal{B}_n$ are simply the zero-one polynomials of degree exactly n.

There is a rich literature on the theme of making a polynomial 'flat' on a compact set, subject to some restriction on its coefficients (such as the restrictions defining $\mathcal{L}_n$, $\mathcal{A}_n$, or $\mathcal{A}_{n,m}$). For instance, one could ask for the minimum supnorm of a polynomial on an interval $[a, b] \subset \mathbb{R}$ subject to the restriction that its coefficients be integers; this is the 'integer Chebyshev problem' (see Chapter 10 of [3]), which we do not discuss further in this thesis. Rather than considering an interval in $\mathbb{R}$, we are interested in the behaviour of height one polynomials on another 'canonical' one-dimensional compact set.

Definition 1.3 *We let* $\mathbb{S}$ *denote the set*

$$\{z \in \mathbb{C} : |z| = 1\};$$

that is, $\mathbb{S}$ *denotes the unit circle in the complex plane.*

Intuitively, $\mathbb{S}$, unlike an interval in $\mathbb{R}$, is 'homogeneous' in the sense that all of its points are the 'same'. Much study has been made of features of the modulus of Littlewood polynomials on $\mathbb{S}$, such as the usual L_p norms (see Chapters 4 and 15 of [3] for a

good starting point). This is discussed in more detail in Section 1.3, but to give a taste of things to come, we now state two illustrative open conjectures. The first is credited to Littlewood and appears in problem collections compiled by Erdős [12] and Littlewood [30]. The second is credited to Erdős and appears in [8] and [13].

Conjecture 1.4 (Two-sided conjecture, strong version) *For all n, there exists $\alpha \in \mathcal{L}_n$ satisfying*

$$K_1\sqrt{n} \leq |\alpha(z)| \leq K_2\sqrt{n} \quad \text{for all } z \in \mathbb{S},$$

where K_1 and K_2 are positive constants (i.e., they are independent of n).

Conjecture 1.5 *For all $n > 1$ and all $\alpha \in \mathcal{L}_n$, we have*

$$|\alpha(z)| \geq (1+K)\sqrt{n} \quad \text{for some } z \in \mathbb{S},$$

where K is a positive constant.

Informally, Conjecture 1.5 says that the constant in the upper bound in the two-sided conjecture is bounded away from 1.

Given a positive integer n and a polynomial

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1}z^{n-1} \in \mathbb{R}[z],$$

we define the **coefficient sequence** of α to be the n-tuple

$$(a_0, a_1, \ldots, a_{n-1}).$$

Thus there is a natural bijection between $\mathcal{L}_n$ and the collection of n-tuples with entries in $\{-1, +1\}$, and also between $\mathcal{A}_n$ and the collection of n-tuples with entries in $\{0, 1\}$.

If we define $[n] := \{0, 1, \ldots, n-1\}$ (we use this notation throughout the rest of this thesis), then there is also a natural bijection φ from $\mathcal{A}_n$ to the collection of all subsets of $[n]$, defined by

$$\varphi(a_0 + a_1 z + \cdots + a_{n-1}z^{n-1}) = \{j \in [n] : a_j = 1\}.$$

We refer to $\varphi(\alpha)$ as the subset of $[n]$ that **corresponds** to α.

If α is a Littlewood polynomial or zero-one polynomial, then there is a relationship between the 'flatness' of α on $\mathbb{S}$ and certain combinatorial properties of the coefficient sequence of α. This is explained more precisely in the rest of Chapter 1.

1.2 Autocorrelation

If α is any polynomial in $\mathbb{R}[z]$, say

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \quad \text{where } a_j \in \mathbb{R},$$

then for $z \in \mathbb{S}$, we have

$$\begin{aligned} |\alpha(z)|^2 = \alpha(z)\overline{\alpha(z)} &= \left(a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}\right)\left(a_0 + a_1 \frac{1}{z} + \cdots + a_{n-1} \frac{1}{z^{n-1}}\right) \\ &= c_{n-1} \frac{1}{z^{n-1}} + \cdots + c_1 \frac{1}{z} + c_0 + c_1 z + \cdots + c_{n-1} z^{n-1} \end{aligned} \tag{1.1}$$

where the c_k are the so-called (acyclic or aperiodic) **autocorrelations** of α.

Definition 1.6 *If $\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \in \mathbb{R}[z]$, the* **autocorrelations** *of α are defined for $0 \leq k \leq n-1$ by*

$$c_k := \sum_{j=0}^{n-k-1} a_j a_{j+k} = \sum_{j \in [n-k]} a_j a_{j+k}.$$

If A denotes the coefficient sequence of α, then we can regard the autocorrelation c_k as the dot product of a vector consisting of the first $n-k$ entries of A and a vector consisting of the last $n-k$ entries of A.

a_0	$\cdots$	a_{k-1}	a_k	$\cdots$	a_{n-1}			
			a_0	$\cdots$	a_{n-k-1}	a_{n-k}	$\cdots$	a_{n-1}

$$c_k = a_0 a_k + \cdots + a_{n-k-1} a_{n-1}$$

In particular, c_0 is just $a_0^2 + \cdots + a_{n-1}^2$, so $c_0 = n$ for all $\alpha \in \mathcal{L}_n$ and $c_0 = m$ for all $\alpha \in \mathcal{A}_{n,m}$. We find it convenient to group together $c_1, \ldots, c_{n-1}$ as the 'nontrivial' or 'off-peak' autocorrelations.

Definition 1.7 *Given $n > 1$ and a polynomial*

$$\alpha = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \in \mathbb{R}[z],$$

we define the **autocorrelation vector** *of α to be the $(n-1)$-tuple*

$$C := (c_1, c_2, \ldots, c_{n-1}).$$

Suppose for the moment that $\alpha \in \mathcal{L}_n$. Then c_k is a sum of $n-k$ terms that are each ± 1, implying the following.

Proposition 1.8 *If $\alpha \in \mathcal{L}_n$, then*

$$c_k \equiv n - k \pmod 2.$$

For $\alpha \in \mathcal{L}_n$, each $j \in [n-k]$ satisfying $a_j = a_{j+k}$ makes a contribution of $+1$ to c_k, whereas each $j \in [n-k]$ satisfying $a_j \neq a_{j+k}$ makes a contribution of -1 to c_k. Hence, if c_k is 'near zero' for some $\alpha \in \mathcal{L}_n$, it means that the coefficient sequence A is 'uncorrelated' with a version of itself that has been acyclically shifted by k positions, in the sense that a_j and a_{j+k} agree about as often as they disagree.

In signal processing [15] and statistical physics [33], one sometimes seeks n-tuples of $+1$'s and -1's whose autocorrelations are as 'near zero' as possible. In view of Proposition 1.8, the following condition represents the 'closest to zero' that we could ask the autocorrelations of a Littlewood polynomial to be.

Definition 1.9 *We call a polynomial*

$$\alpha = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \in \mathcal{L}_n$$

a **Barker polynomial** *(and call its coefficient sequence a* **Barker sequence***) if $|c_k| \leq 1$ for all $k \neq 0$ (i.e. if all entries of C lie in $\{-1, 0, +1\}$).*

There exist Barker sequences of lengths 2, 3, 4, 5, 7, 11, 13, of no odd lengths greater than 13, and of no lengths between 14 and $4 \cdot 10^{12}$. See [48] and [44]. Proving there are no Barker polynomials of length greater than 13 is considered to be a difficult open problem, but one can still ask: How close to zero can we make the autocorrelations of a Littlewood polynomial?

Definition 1.10 (Turyn, 1968) *If $n > 1$ is a positive integer, we define*

$$b(n) := \min_{\alpha \in \mathcal{L}_n} \max_{1 \leq k < n} |c_k|,$$

which we can think of as the 'minimum maximum autocorrelation' among polynomials in $\mathcal{L}_n$.

The asymptotic growth rate of $b(n)$ is unknown, but exact values of $b(n)$ can be found for modest values of n by exhaustive search. Computations in [9] and [10] reveal that we have $b(n) \leq 2$ for all $n \leq 21$, $b(n) \leq 3$ for all $n \leq 48$, and $b(n) \leq 4$ for all $n \leq 69$. The best currently known upper bound on $b(n)$ appears to be the following result.

Proposition 1.11 (Moon & Moser, 1968) *For every $\varepsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that*

$$b(n) \leq (2+\varepsilon)\sqrt{n \log n} \tag{1.2}$$

for $n \geq N$.

In Section 3.2, we improve (1.2) to $b(n) \leq (\sqrt{2}+\varepsilon)\sqrt{n \log n}$ by refining Moon and Moser's technique.

We now shift our attention from Littlewood polynomials to zero-one polynomials. In general, if

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \in \mathcal{A}_n,$$

we will define

$$m := \alpha(1) = \text{the number of coefficients of } \alpha(z) \text{ that are } 1,$$

so that $\alpha(z) \in \mathcal{A}_{n,m}$, and we also write

$$\alpha(z) = z^{\beta_1} + z^{\beta_2} + \cdots + z^{\beta_m}$$

where $\beta_1 < \beta_2 < \cdots < \beta_m$. That is, $\{\beta_1, \ldots, \beta_m\}$ is the subset of $[n]$ corresponding to $\alpha(z)$.

For $\alpha \in \mathcal{A}_n$, we can still regard c_k as a dot product, but it is no longer true that each 'agreement' contributes $+1$ and each 'disagreement' contributes -1. Instead, we have

$$\begin{aligned} c_k &= \text{the number of } j \text{ such that } a_j \text{ and } a_{j+k} \text{ are both } 1 \\ &= \text{the number of times } k \text{ appears as a difference } \beta_i - \beta_j. \end{aligned}$$

Since there are $\binom{m}{2}$ pairs $\{\beta_i, \beta_j\}$, we get

$$c_1 + \cdots + c_{n-1} = \binom{m}{2} \quad \text{for all } \alpha \in \mathcal{A}_{n,m}.$$

So, whether considering Littlewood polynomials or zero-one polynomials, we could ask for the autocorrelations to be 'close to zero'. For $\mathcal{L}_n$, we have the restriction that Proposition 1.8 must hold, and for $\mathcal{A}_n$, we have the restriction that the c_k are nonnegative integers whose sum is $\binom{m}{2}$. In either case, discussing the 'closeness to zero' of the autocorrelations motivates the introduction of the usual ℓ_p norms of the autocorrelation vector.

Definition 1.12 *Let* $(c_1, c_2, \ldots, c_{n-1}) \in \mathbb{R}^{n-1}$. *For* $p \in \mathbb{R}$, $p \geq 1$, *we define*

$$|C|_p := \left(|c_1|^p + |c_2|^p + \cdots + |c_{n-1}|^p \right)^{1/p},$$

which we call the ℓ_p **norm** *of* C. *We also define*

$$|C|_\infty := \max_{1 \leq k \leq n-1} |c_k|,$$

which we call the **supnorm** *or* ℓ_∞ **norm** *of* C.

We recall the following without proof.

Proposition 1.13 (Monotonicity of ℓ_p norms) *For* $C \in \mathbb{R}^{n-1}$, *we have*

$$\lim_{p \to \infty} |C|_p = |C|_\infty .$$

Furthermore, if $p \leq q$, *we have* $|C|_p \geq |C|_q$.

In order to say a bit more about the tendency for autocorrelations 'near zero' to yield a 'flat' polynomial, we introduce the usual L_p norms of a polynomial on $\mathbb{S}$.

Definition 1.14 *Let* $\alpha : \mathbb{S} \to \mathbb{C}$ *be continuous. For* $p \in \mathbb{R}$, $p \geq 1$, *we define*

$$\|\alpha\|_p := \left(\frac{1}{2\pi} \int_0^{2\pi} \left| \alpha(e^{i\theta}) \right|^p d\theta \right)^{1/p},$$

which we call the L_p **norm** *of* α. *We also define*

$$\|\alpha\|_\infty := \max_{z \in \mathbb{S}} |\alpha(z)| ,$$

which we call the **supnorm** *or* L_∞ **norm** *of* α.

We recall the following without proof. Note that the monotonicity inequality for the L_p norms 'points the other way' as the one for the ℓ_p norms.

Proposition 1.15 (Monotonicity of L_p norms) *If $\alpha : \mathbb{S} \to \mathbb{C}$ is continuous, we have*

$$\lim_{p\to\infty} \|\alpha\|_p = \|\alpha\|_\infty .$$

Furthermore, if $p \leq q$, we have $\|\alpha\|_p \leq \|\alpha\|_q$.

We now use (1.1), together with the general fact that

$$\frac{1}{2\pi}\int_0^{2\pi} \Big(b_{-r}\frac{1}{z^r} + \cdots + b_{-1}\frac{1}{z} + b_0 + b_1 z + \cdots + b_r z^r\Big)d\theta = b_0 \quad (z = e^{i\theta})$$

to observe that any polynomial $\alpha = a_0 + \cdots + a_{n-1}z^{n-1} \in \mathbb{R}[z]$ satisfies

$$\begin{aligned}\|\alpha\|_2^2 &= \frac{1}{2\pi}\int_0^{2\pi} \Big(c_{n-1}\frac{1}{z^{n-1}} + \cdots + c_1\frac{1}{z} + c_0 + c_1 z + \cdots + c_{n-1}z^{n-1}\Big)d\theta \quad (z = e^{i\theta}) \\ &= c_0\end{aligned}$$

and also satisfies

$$\begin{aligned}\|\alpha\|_4^4 &= \frac{1}{2\pi}\int_0^{2\pi} \Big(c_{n-1}\frac{1}{z^{n-1}} + \cdots + c_1\frac{1}{z} + c_0 + c_1 z + \cdots + c_{n-1}z^{n-1}\Big)^2 d\theta \quad (z = e^{i\theta}) \\ &= c_{n-1}^2 + \cdots + c_1^2 + c_0^2 + c_1^2 + \cdots + c_{n-1}^2 = c_0^2 + 2\,|C|_2^2 .\end{aligned}$$

Hence $\|\alpha\|_2$ has the same value for all $\alpha \in \mathcal{L}_n$, and similarly for $\mathcal{A}_{n,m}$. Notice also that for either of the sets $\mathcal{L}_n$ or $\mathcal{A}_{n,m}$, minimizing $\|\alpha\|_4$ and minimizing $|C|_2$ are the same problem.

1.3 Flat Littlewood polynomials

We have observed that every $\alpha \in \mathcal{L}_n$ satisfies

$$\begin{aligned}\|\alpha\|_2 &= \sqrt{n} \quad \text{and} \\ \|\alpha\|_4 &= (n^2 + 2\,|C|_2^2)^{1/4}.\end{aligned}$$

Notice that $\|\alpha\|_4 \geq \|\alpha\|_2$, as is consistent with Proposition 1.15. We could ask for $\|\alpha\|_4$ to be 'only slightly larger' than $\|\alpha\|_2$, which would mean we would want $|C|_2^2$ to be as small as possible.

Definition 1.16 *For $\alpha \in \mathcal{L}_n$, we define*

$$|C|_2^2 = c_1^2 + \cdots + c_{n-1}^2 = \frac{1}{2}(\|\alpha\|_4^4 - \|\alpha\|_2^4)$$

to be the **energy** *of α.*

The use of the term 'energy' comes from statistical physics [33]. Proposition 1.8 implies that the smallest conceivable energy of a Littlewood polynomial is $|C|_2^2 = \lceil (n-1)/2 \rceil$, which occurs if and only if α is a Barker polynomial.

Definition 1.17 *For any integer $n > 1$, we define*

$$E_{\min}(n) := \min_{\alpha \in \mathcal{L}_n} |C|_2^2,$$

which is hence the **minimum energy** *of a polynomial in $\mathcal{L}_n$.*

As with Turyn's b function (Definition 1.10), the asymptotic growth rate of $E_{\min}(n)$ is unknown. It has been shown through 'branch and bound' search (see [33] and [34]) that we have

$$\frac{1}{18}n^2 \leq E_{\min}(n) \leq \frac{1}{14}n^2 \quad \text{whenever } 30 \leq n \leq 60,$$

and the following conjecture is credited to Golay [19].

Conjecture 1.18 ('Merit factor' conjecture) *For all $n > 1$, we have*

$$E_{\min}(n) \geq Kn^2,$$

where K is a positive constant.

Conjecture 1.18 says that for all $n > 1$ and all $\alpha \in \mathcal{L}_n$, we have $|C|_2^2 \geq Kn^2$. It would follow that

$$\|\alpha\|_\infty \geq \|\alpha\|_4 = (n^2 + 2\,|C|_2^2)^{1/4} \geq (1 + 2K)^{1/4}\sqrt{n};$$

that is, Conjecture 1.18 implies Conjecture 1.5.

Conjecture 1.18 also implies that there are only finitely many Barker sequences, since an infinite family of Barker polynomials would have energy growing like $n/2$.

In the same article that introduced his b function [47], Turyn made the following conjecture in passing.

Conjecture 1.19 (Turyn, 1968) *We have*

$$b(n) \sim K \log n$$

for some positive constant K.

Conjecture 1.19 may seem plausible when one observes that the modest list of known exact values of $b(n)$ appears to be 'growing slowly'. However, any result of the form $b(n) = o(\sqrt{n})$ would violate Conjecture 1.18. If $b(n) = o(\sqrt{n})$, then for every $n > 1$, there exists $\alpha \in \mathcal{L}_n$ satisfying

$$|C|_2^2 = \sum_{k=1}^{n-1} c_k^2 \leq \sum_{k=1}^{n-1} \big(b(n)\big)^2 \leq n\big(b(n)\big)^2 = o(n^2).$$

The following weaker version of Conjecture 1.19 is also unproved, but some known results (including some of the results of this thesis) are tantalizingly close to it.

Conjecture 1.20 *We have*

$$b(n) \leq K\sqrt{n}$$

for some positive constant K (perhaps $K \leq 1$).

Littlewood's 'two-sided' conjecture (Conjecture 1.4) has a 'weak' version.

Conjecture 1.21 (Two-sided conjecture, weak version) *For infinitely many n, there exists $\alpha \in \mathcal{L}_n$ satisfying*

$$K_1\sqrt{n} \leq |\alpha(z)| \leq K_2\sqrt{n} \quad \text{for all } z \in \mathbb{S}, \tag{1.3}$$

where K_1 and K_2 are positive constants.

Although (as previously mentioned) it is strongly suspected that no infinite family of Barker polynomials exists, it has been observed [43] that such a family of polynomials would satisfy Conjecture 1.21.

An infinite family of Littlewood polynomials satisfying just the upper bound in (1.3) is given by the Rudin–Shapiro polynomials (see, e.g., Chapter 4 of [3]), which exist for all lengths n that are a power of 2. The Rudin–Shapiro polynomials satisfy $|\alpha(z)| \leq \sqrt{2} \cdot \sqrt{n}$ on $\mathbb{S}$. Furthermore, Spencer [46] used probabilistic methods to show that for sufficiently large fixed K, the number of polynomials $\alpha \in \mathcal{L}_n$ satisfying $|\alpha(z)| \leq K\sqrt{n}$ (for $z \in \mathbb{S}$) is eventually bounded below by an exponential function of n (so there are 'many' Littlewood polynomials whose modulus on $\mathbb{S}$ is at most $K\sqrt{n}$).

Nobody has shown the existence of an infinite family of Littlewood polynomials satisfying just the lower bound in (1.3). That is, the following conjecture, which appears in [8] where it is credited to Erdős, remains open.

Conjecture 1.22 (High minimum modulus conjecture) *For all $n \in \mathbb{Z}^+$, there exists $\alpha \in \mathcal{L}_n$ satisfying*

$$|\alpha(z)| \geq K\sqrt{n} \quad \textit{for all } z \in \mathbb{S}, \tag{1.4}$$

where K is a positive constant. (Perhaps $K = 1/2$ suffices.)

Analogously to the two-sided conjecture, Conjecture 1.22 has a weak version as well as a strong version.

Computations in [41] reveal that for all n in $\{11, 12, \ldots, 25\} \cup \{27, 29, \ldots, 65\}$, there exists $\alpha \in \mathcal{L}_n$ satisfying $|\alpha(z)| \geq 0.56\sqrt{n}$ for all $z \in \mathbb{S}$. It would be interesting to extend this to an infinite family of Littlewood polynomials, but the known infinite family that comes closest to satisfying (1.4) is a family of polynomials that exist for lengths of the form $n = 13^r$ and have modulus bounded below by $n^{0.4308}$ on $\mathbb{S}$. This family is constructed from the Barker sequence of length 13 (see [7], or Problem C1 in Chapter 4 of [3]).

It has been observed that Littlewood polynomials with particularly high minimum modulus on $\mathbb{S}$ often tend to be 'skewsymmetric' (this term is defined in Section 2.1). In Section 2.3, we establish a kind of 'converse' of this tendency by proving that skewsymmetric Littlewood polynomials have no zeros on $\mathbb{S}$.

1.4 Sidon sets

Let n be a positive integer and let $\alpha \in \mathcal{A}_n$. As mentioned in Section 1.2, we have $\alpha \in \mathcal{A}_{n,m}$ where $m := \alpha(1)$, and we can write

$$\alpha(z) = z^{\beta_1} + z^{\beta_2} + \cdots + z^{\beta_m} \quad (\beta_1 < \beta_2 < \cdots < \beta_m)$$

where $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is the subset of $[n]$ that corresponds to α.

Just as we did with $\alpha \in \mathcal{L}_n$, we can enquire whether there exists $\alpha \in \mathcal{A}_{n,m}$ satisfying $|C|_\infty \leq 1$; that is, satisfying $|c_k| \leq 1$ whenever $1 \leq k \leq n-1$. Recalling from Section 1.2 that c_k is the number of times k appears as a difference $\beta_i - \beta_j$, we see that the condition that $\alpha \in \mathcal{A}_{n,m}$ satisfies $|C|_\infty \leq 1$ is equivalent to the condition that $\{\beta_1, \ldots, \beta_m\}$ satisfies the following.

Definition 1.23 *Let $A = \{\beta_1, \beta_2, \ldots, \beta_m\} \subseteq [n]$ with $\beta_1 < \beta_2 < \cdots < \beta_m$. We call A a* **Sidon set** *if the $\binom{m}{2}$ positive differences*

$$\beta_j - \beta_i \quad (i < j)$$

are all distinct.

The condition that $\{\beta_1, \ldots, \beta_m\}$ is a Sidon set is equivalent to the implication

$$\big(\beta_i - \beta_j = \beta_k - \beta_\ell\big) \Longrightarrow \big((i = j \text{ and } k = \ell) \text{ or } (i = k \text{ and } j = \ell)\big)$$

which may also be written in the form

$$\big(\beta_i + \beta_\ell = \beta_k + \beta_j\big) \Longrightarrow \big((i = j \text{ and } k = \ell) \text{ or } (i = k \text{ and } j = \ell)\big).$$

This gives the following.

Proposition 1.24 *The set $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is Sidon if and only if the $\binom{m+1}{2}$ sums*

$$\beta_i + \beta_j \quad (i \leq j)$$

are all distinct.

Sidon sets are also called $B_2[1]$ sets, or more briefly, B_2 sets. (Some authors use the term '$B_h[g]$ set' to refer to a set A of nonnegative integers with the property that each $n \in \mathbb{Z}$ can be expressed in at most g ways as a sum of h (not necessarily distinct) elements of A.) For a good introduction to the topic of Sidon sets or B_2 sets, see Problem C9 in [21] or Section II.3 of [23].

One can ask for necessary or sufficient conditions on m and n for the existence of a Sidon set of size m in $[n]$. Lindström [29] showed the following by elementary methods, which improved an earlier result of Erdős and Turán [14].

Proposition 1.25 *The condition*

$$m \leq n^{1/2} + n^{1/4} + 1$$

is necessary for the existence of a Sidon set of size m in $[n]$.

There is also the following result, which appears in Problem C9 of [21], and follows from a result of Singer [45] (on so-called 'planar difference sets' obtained from finite projective planes) and from classical results on the distribution of primes.

Proposition 1.26 *Let ε be a positive real number less than 1. Then there exists $N \in \mathbb{Z}$ such that for all $n \geq N$, the condition*

$$m \leq (1 - \varepsilon)n^{1/2}$$

is sufficient to guarantee the existence of a Sidon set of size m in $[n]$.

So roughly speaking, a value of m just below $\sqrt{n}$ is small enough to guarantee that there is a Sidon set of size m in $[n]$, whereas a value of m much bigger than $\sqrt{n}$ is large enough to make it impossible to have a Sidon set of size m in $[n]$. One might then suspect that a smaller value of m would make Sidon sets more 'numerous'. In Section 4.2, as a consequence of finding the average L_4 norm of polynomials in $\mathcal{A}_{n,m}$, we give a new proof of the following known result [18, 37]: If $m = o(n^{1/4})$ and $B(n,m)$ denotes the number of Sidon sets of size m in $[n]$, then 'almost all' subsets of $[n]$ of size m are Sidon, in the sense that

$$\lim_{n\to\infty} \frac{B(n,m)}{\binom{n}{m}} = 1.$$

1.5 Some probabilistic language

If Ω denotes one of the four spaces $\mathcal{L}_n$, $\mathcal{A}_n$, $\mathcal{A}_{n,m}$, or $\mathcal{B}_n$ defined in Section 1.1, then we can turn Ω into a probability space by endowing it with a probability mass function. Then Ω is a finite set, which means that technically, we can heed the following remarks of Bollobás [2]: 'It should be noted that we never use more than the convenient *language* of probability theory, since all the probabilistic arguments we need can be replaced by *counting* the number of objects in various sets.'

However, although it may be true that all our probabilistic-sounding statements can be proved by counting arguments, it is perhaps fair to say that many of the counting arguments we use would not have been discovered had they not been phrased in probabilistic language. In any case, we devote the rest of Chapter 1 to some known results and techniques from discrete probability that have been assembled here for ease of exposition.

Definition 1.27 *A* **finite probability space** *is a pair (Ω, p) where Ω is a finite set, called the* **sample space**, *and p is a function from Ω to $[0,1]$ that satisfies*

$$\sum_{\alpha \in \Omega} p(\alpha) = 1.$$

The elements of Ω are called **sample points** *or* **atoms**, *and p is called a probability* **mass function**.

Generally, we will write our sample space as

$$\Omega = \{\alpha_1, \alpha_2, \ldots, \alpha_N\}.$$

By an **event**, we mean any subset of Ω. Thus there are precisely 2^N different events. The **complement** of an event A, which we denote by $\overline{A}$, is the set $\Omega \setminus A$. An event of the form $\{\alpha_i\}$ is called an **atomic event**; any event can therefore be written uniquely as a (possibly empty) finite union of atomic events.

Definition 1.28 *The* **probability** *of an event $A \subset \Omega$ is defined by*

$$\mathbf{Pr}[A] := \sum_{\alpha \in A} p(\alpha);$$

that is, the probability of A is just the sum of the masses associated with the sample points in A.

We thus have $\mathbf{Pr}[\Omega] = 1$ and $\mathbf{Pr}[\emptyset] = 0$. We call our probability space **nondegenerate** if the only event having zero probability is the empty event, or equivalently, if all atomic events have nonzero probability.

One technical notion we need to define is that of **mutual independence** of a collection of events. This is a stronger condition than pairwise independence (see, for instance, Example 2.23 in [16]) and is harder to define than it would seem at first glance. Our treatment of independence may appear nonstandard, but our definitions will be equivalent to the standard ones (such as those appearing in [16] and [35]).

Definition 1.29 *If A and B are events, we define the* **conditional probability** $\mathbf{Pr}[A|B]$, *called the 'probability of A given B', by*

$$\mathbf{Pr}[A|B] = \begin{cases} \mathbf{Pr}[A \cap B]/\mathbf{Pr}[B] & \text{if } \mathbf{Pr}[B] \neq 0, \\ \mathbf{Pr}[A] & \text{if } \mathbf{Pr}[B] = 0. \end{cases}$$

We say A is **independent** *of B if* $\mathbf{Pr}[A|B] = \mathbf{Pr}[A]$.

The following is an easy exercise.

Proposition 1.30 *Let A, B, C be any events.*

1. *Event A is independent of event B if and only if* $\mathbf{Pr}[A \cap B] = \mathbf{Pr}[A]\mathbf{Pr}[B]$.
2. *Suppose A is independent of B, A is independent of C, and B and C are disjoint. Then A is independent of $B \cup C$.*

In view of fact 1 above, we can simply refer to two events as being **independent**. In order to extend the notion of independence to collections of more than two events, we introduce some auxiliary definitions.

Definition 1.31 *Let $(A_1, \ldots, A_k)$ be a list of events. The* **subworlds** *determined by $(A_1, \ldots, A_k)$ are the 2^k events of the form*

$$E_1 \cap E_2 \cap \cdots \cap E_k$$

where for each $i \in \{1, \ldots, k\}$, the event E_i is either A_i or $\overline{A_i}$. (Note that some of the subworlds may be empty.) A **Boolean combination** *of $(A_1, \ldots, A_k)$ is any event of the form*

$$E_1 \cap E_2 \cap \cdots \cap E_k$$

where for each $i \in \{1, \ldots, k\}$, the event E_i is either A_i, $\overline{A_i}$, or Ω.

Intuitively, the difference between subworlds and Boolean combinations is as follows. Specifying a subworld means that for each $i \in \{1, \ldots, k\}$, we specify whether or not event A_i happens. Specifying a Boolean combination means that for some of the $i \in \{1, \ldots, k\}$, we specify whether or not event A_i happens.

The next proposition follows easily from Definition 1.31.

Proposition 1.32 *Let $A_1, \ldots, A_k$ be any events.*

1. *The 2^k subworlds determined by $(A_1, \ldots, A_k)$ are disjoint.*
2. *Any Boolean combination of $(A_1, \ldots, A_k)$ can be written as a union of some of the subworlds determined by $(A_1, \ldots, A_k)$.*

We are now in a position to define mutual independence of a collection of more than two events.

Definition 1.33 *Let $(A_1, \ldots, A_k)$ be a list of events. We say that $A_1, \ldots, A_k$ are* **independent** *if every event A_i is independent of each of the subworlds determined by $(A_1, \ldots, A_{i-1}, A_{i+1}, \ldots, A_k)$.*

The following is an easy consequence of Definition 1.33, Proposition 1.32, and part 2 of Proposition 1.30.

Proposition 1.34 *Let $A_1, \ldots, A_k$ be any events. Then $A_1, \ldots, A_k$ are independent if and only if for each $i \in \{1, \ldots, k\}$, the event A_i is independent of any Boolean combination of $(A_1, \ldots, A_{i-1}, A_{i+1}, \ldots, A_k)$.*

Informally, when we say that a collection of events is mutually independent, we mean that any partial information about whether or not some of the events occur does not affect the probability that one of the remaining events occurs.

The next result has an easy proof by induction.

Proposition 1.35 *If $A_1, \ldots, A_k$ are independent events, then*

$$\mathbf{Pr}[A_1 \cap A_2 \cap \cdots \cap A_k] = \mathbf{Pr}[A_1]\mathbf{Pr}[A_2] \cdots \mathbf{Pr}[A_k].$$

The above is sometimes taken as the definition of mutual independence of events. By contrast, our definition of 'random variable' agrees with the standard one.

Definition 1.36 *If (Ω, p) is a finite probability space, then a (real)* **random variable** *on (Ω, p) is any function X from Ω to $\mathbb{R}$. The* **range** *of X is the set*

$$\text{Range}(X) := \{X(\alpha) : \alpha \in \Omega\} = \{X(\alpha_1), \ldots, X(\alpha_N)\}$$

where $\{\alpha_1, \ldots, \alpha_N\}$ is an enumeration of Ω.

Any random variable on a finite probability space is a **finite random variable**, which simply means that its range is a finite set. We can always express the range of such a random variable as

$$\text{Range}(X) = \{x_1, x_2, \ldots, x_r\}$$

where $x_1 < x_2 < \ldots < x_r$ and $r \leq N$. The function $f : \text{Range}(X) \to [0, 1]$ defined by

$$f(x_i) := \mathbf{Pr}[X = x_i]$$

is called the **probability distribution** function of X.

Definition 1.37 *The* **expected value** *of a finite random variable X is*

$$\mathbf{E}(X) := \sum_{i=1}^{r} x_i \cdot f(x_i) = \sum_{i=1}^{N} X(\alpha_i) \cdot p(\alpha_i)$$

where f and $x_1, \ldots, x_r$ are as defined above.

Note that any function of a finite random variable is itself a finite random variable, so notations such as $\mathbf{E}\big(g(X)\big)$ make sense.

The next proposition is easy, and does not require mutual independence of the random variables involved (a concept which will be defined shortly).

Proposition 1.38 (Linearity of expectation) *Suppose $(X_1, \ldots, X_k)$ is a list of (finite) random variables defined on a finite probability space. We then have*

$$\mathbf{E}(X_1 + \cdots + X_k) = \mathbf{E}(X_1) + \cdots + \mathbf{E}(X_k).$$

The following result also has an easy short proof, which we include. It turns out to be convenient to have two slightly different versions of Markov's inequality.

Proposition 1.39 (Markov's inequality) *Let X be a random variable defined on a finite probability space. Suppose X is nonnegative (which just means each value in the range of X is nonnegative). Then for each nonnegative real number a, we have $\mathbf{Pr}[X > a] < \mathbf{E}(X)/a$ and $\mathbf{Pr}[X \geq a] \leq \mathbf{E}(X)/a$.*

Proof. As before, let $\text{Range}(X) = \{x_1, \ldots, x_r\}$ where $x_1 < \ldots < x_r$, and let f be the probability distribution of X. We have

$$\begin{aligned}\mathbf{E}(X) &= \sum_{i=1}^{r} x_i \cdot f(x_i) \geq \sum_{x_i > a} x_i \cdot f(x_i) \\ &> \sum_{x_i > a} a \cdot f(x_i) = a \sum_{x_i > a} f(x_i) = a \cdot \mathbf{Pr}[X > a]\end{aligned}$$

and also

$$\begin{aligned}\mathbf{E}(X) &= \sum_{i=1}^{r} x_i \cdot f(x_i) \geq \sum_{x_i \geq a} x_i \cdot f(x_i) \\ &\geq \sum_{x_i \geq a} a \cdot f(x_i) = a \sum_{x_i \geq a} f(x_i) = a \cdot \mathbf{Pr}[X \geq a]. \blacksquare\end{aligned}$$

In order to define the notion of mutual independence of random variables, we now introduce some auxiliary definitions similar to the ones we needed to define mutual independence of events.

Definition 1.40 *Suppose $X_1, \ldots, X_k$ are (finite) random variables defined on a finite probability space. For each $i \in \{1, \ldots, k\}$, define $r_i := |\text{Range}(X_i)|$. The* **basic subworlds** *determined by $(X_1, \ldots, X_k)$ are the $r_1 r_2 \cdots r_k$ events of the form*

$$X_1 = x_1 \text{ and } X_2 = x_2 \text{ and } \ldots \text{ and } X_k = x_k$$

where for each $i \in \{1, \ldots, k\}$, x_i *is one of the* r_i *values in* Range(X_i). *The* **complex subworlds** *determined by* $(X_1, \ldots, X_k)$ *are the events of the form*

$$X_1 \in A_1 \text{ and } X_2 \in A_2 \text{ and } \ldots \text{ and } X_k \in A_k$$

where for each $i \in \{1, \ldots, k\}$, *the set* A_i *is either all of* Range(X_i) *or a subset of* Range(X_i) *of size* 1.

Clearly, the basic subworlds determined by $(X_1, \ldots, X_k)$ are disjoint sets whose union is Ω, and each complex subworld is a union of some of the basic subworlds. Intuitively, the basic subworlds are events that specify the value of each of the variables X_i, whereas the complex subworlds are events that specify the values of some of the variables X_i.

We can now define mutual independence of a collection of random variables.

Definition 1.41 *Let* $(X_1, \ldots, X_k)$ *be a list of (finite) random variables defined on a finite probability space. We say* $X_1, \ldots, X_k$ *are* **independent** *if for each* $i \in \{1, \ldots, k\}$ *and for each* $x \in$ Range(X_i), *the event* $X_i = x$ *is independent of each of the basic subworlds determined by* $(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_k)$.

The next result can be proved in a similar way to Proposition 1.34 by using part 2 of Proposition 1.30.

Proposition 1.42 *Let* $(X_1, \ldots, X_k)$ *be a list of (finite) random variables defined on a finite probability space. Then* $X_1, \ldots, X_k$ *are independent if and only if for each* $i \in \{1, \ldots, k\}$ *and for each* $x \in$ Range(X_i), *the event* $X_i = x$ *is independent of each of the complex subworlds determined by* $(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_k)$.

It follows that we can prove mutual independence of a collection of random variables by the 'almost intuitive' method of showing, roughly speaking, that the probability distribution of one of the variables is not affected by specifying the values of some of the remaining variables.

Mutually independent random variables satisfy the following condition, whose proof we omit.

Proposition 1.43 *Suppose $X_1, \ldots, X_k$ are independent random variables (on a finite probability space). Then*

$$\mathbf{E}(X_1 X_2 \cdots X_k) = \mathbf{E}(X_1)\mathbf{E}(X_2)\cdots\mathbf{E}(X_k).$$

The last technical term we define in this section is the **moment-generating function** of a random variable.

Definition 1.44 *Suppose X is a (finite) random variable on a finite probability space. The* **moment-generating function**, *or* **MGF**, *of X is defined by*

$$M_X(t) := \mathbf{E}(e^{tX})$$

where t is a formal variable.

Note that if $x_1, \ldots, x_r$ and f are as defined previously, then $M_X(t)$ is just the finite weighted sum

$$f(x_1) \cdot e^{x_1 t} + f(x_2) \cdot e^{x_2 t} + \cdots + f(x_r) \cdot e^{x_r t}$$

of exponential functions of t. The following result is straightforward.

Proposition 1.45 *Suppose X is a (finite) random variable on a finite probability space. Then for each nonnegative integer m, we have*

$$\frac{d^m}{dt^m} M_X(t)\bigg|_{t=0} = \mathbf{E}(X^m).$$

Equivalently, we have

$$M_X(t) = 1 + \mathbf{E}(X)\frac{t}{1!} + \mathbf{E}(X^2)\frac{t^2}{2!} + \cdots.$$

We close this section with the following result that follows easily from Proposition 1.43.

Proposition 1.46 *Suppose $X_1, \ldots, X_k$ are independent random variables (defined on a finite probability space), and let Y be the random variable $X_1 + \cdots + X_k$. Then*

$$M_Y(t) = M_{X_1}(t) M_{X_2}(t) \cdots M_{X_k}(t).$$

Chapter 2

Special Littlewood Polynomials

I concentrate on
the concentric rings
produced by my pen
in the ink.
The thing that distinguishes
thoughts from things
is that thoughts are harder
to think.
—Piet Hein, 'Thoughts And Things', *Grooks 3*, 1970

2.1 Self-reciprocals and skewsymmetrics

If we are interested in the behaviour of Littlewood polynomials on the unit circle, it turns out to be useful to single out two classes of Littlewood polynomials as deserving of special names.

Definition 2.1 *Suppose* $\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \in \mathcal{L}_n$. *We call* α **self-reciprocal** *if* $\alpha(z) = z^{n-1}\alpha(1/z)$ *(informally, if the coefficient sequence of* α *is palindromic). If* n *is odd, say* $n = 2m + 1$, *then we call* α **skewsymmetric** *if* $a_{m+j} = (-1)^j a_{m-j}$ *for* $1 \leq j \leq m$ *(equivalently, for* $0 \leq j \leq m$*).*

Littlewood [30] describes skewsymmetric polynomials as having 'a central term and two stretches of $n/2$ terms on either side, the end one having the coefficients of the front one written backwards, but affected with signs alternately $-$ and $+$' (however, note that his n is our $n-1$).

It was shown some time ago that a skewsymmetric Littlewood polynomial has the 'flatness' property that 'half' of its autocorrelations are zero (so it satisfies 'half' the conditions of being a Barker polynomial). More precisely, we have the following straightforward result.

Proposition 2.2 *Suppose that $\alpha(z) = a_0 + a_1 z + \cdots + a_{2m} z^{2m}$ is a polynomial that satisfies $a_{m+j} = (-1)^j a_{m-j}$ for $0 \le j \le m$. Then the autocorrelations c_k of α (defined as in Definition 1.6) have the property that $c_k = 0$ whenever k is odd.*

Since proofs of this fact are difficult to find in the literature, we supply two proofs below. The first is more elementary, but uses notation that is somewhat unwieldy.

First proof of Proposition 2.2. The autocorrelation c_k is

$$c_k = \sum_{j=0}^{2m-k} a_j a_{j+k}$$

which is a sum of $2m-k+1$ terms. We have $c_k = R + S + T$, where

$$R := \sum_{j=0}^{m-k} a_j a_{j+k}, \tag{2.1}$$

$$S := \sum_{j=m-k+1}^{m-1} a_j a_{j+k}, \tag{2.2}$$

$$T := \sum_{j=m}^{2m-k} a_j a_{j+k}. \tag{2.3}$$

Observe that R, S, and T are sums of $m-k+1$ terms, $k-1$ terms, and $m-k+1$ terms respectively. (Note that $k-1$ could be 0.)

In the sum S, we have $j+k \ge m+1$, so $j+k$ is of the form $m+j'$ for some $j' \ge 1$, and we can use the relation $a_{m+j'} = (-1)^{j'} a_{m-j'}$. That is, in S, we have

$$a_{j+k} = a_{m+(j+k-m)} = (-1)^{j+k-m} a_{m-(j+k-m)} = (-1)^{j+k-m} a_{2m-j-k}. \tag{2.4}$$

Similarly, in the sum T, both j and $j+k$ are of the form $m+j'$ for some $j' \geq 0$, so we can again use $a_{m+j'} = (-1)^{j'} a_{m-j'}$. This means that in T, we have

$$a_j = a_{m+(j-m)} = (-1)^{j-m} a_{m-(j-m)} = (-1)^{j-m} a_{2m-j}, \tag{2.5}$$

$$a_{j+k} = a_{m+(j+k-m)} = (-1)^{j+k-m} a_{m-(j+k-m)} = (-1)^{j+k-m} a_{2m-j-k}. \tag{2.6}$$

If we now combine (2.3), (2.5), and (2.6), we get

$$T = \sum_{j=m}^{2m-k} (-1)^{j-m} a_{2m-j} (-1)^{j+k-m} a_{2m-j-k} = (-1)^k \sum_{j=m}^{2m-k} a_{2m-j} a_{2m-j-k}$$

which, when k is odd, is equal to

$$-\sum_{j=m}^{2m-k} a_{2m-j} a_{2m-j-k}. \tag{2.7}$$

The sum (2.7), upon defining $j' := 2m-k-j$, becomes

$$T = -\sum_{j'=0}^{m-k} a_{j'+k} a_{j'}$$

which, with (2.1), implies that $R+T=0$.

It now remains to show that $S=0$ if k is an odd integer greater than 1. Let $k = 2\ell+1$ where $\ell \geq 1$, and observe that substituting (2.4) into (2.2) gives us

$$S = \sum_{j=m-2\ell}^{m-1} (-1)^{j+2\ell-m+1} a_j a_{2m-j-2\ell-1} = \sum_{j=m-2\ell}^{m-1} (-1)^{j-m+1} a_j a_{2m-j-2\ell-1}$$

which is a sum of 2ℓ terms. We have $S = S_1 + S_2$ where

$$S_1 := \sum_{j=m-2\ell}^{m-\ell-1} (-1)^{j-m+1} a_j a_{2m-j-2\ell-1}, \tag{2.8}$$

$$S_2 := \sum_{j=m-\ell}^{m-1} (-1)^{j-m+1} a_j a_{2m-j-2\ell-1}, \tag{2.9}$$

so each of S_1 and S_2 is a sum of ℓ terms. The sum (2.9), upon defining $j' := 2m - 2\ell - 1 - j$, becomes

$$\begin{aligned} S_2 &= \sum_{j'=m-2\ell}^{m-\ell-1} (-1)^{m-2\ell-j'} a_{2m-j'-2\ell-1} a_{j'} \\ &= \sum_{j'=m-2\ell}^{m-\ell-1} (-1)^{m-j'} a_{2m-j'-2\ell-1} a_{j'} \\ &= \sum_{j=m-2\ell}^{m-\ell-1} (-1)^{m-j} a_{2m-j-2\ell-1} a_j. \end{aligned} \tag{2.10}$$

Adding (2.8) and (2.10) gives 0 as required, because

$$(-1)^{j-m+1} + (-1)^{m-j} = 0$$

since $j - m + 1$ and $m - j$ are integers of opposite parity. ∎

A shorter proof can be obtained by noticing that the skewsymmetry condition implies something about the function $\alpha(z)/z^m$.

Second proof of Proposition 2.2. Let $n := 2m+1$. Recall that from (1.1), we know that for $z \in \mathbb{S}$, we have

$$|\alpha(z)|^2 = c_{n-1}\frac{1}{z^{n-1}} + \cdots + c_1\frac{1}{z} + c_0 + c_1 z + \cdots + c_{n-1}z^{n-1}.$$

We wish to show this is an even function of z, implying that the coefficients of the odd powers of z are zero. That is, we wish to show $|\alpha(z)|^2 = |\alpha(-z)|^2$.

We define

$$f(z) := \frac{\alpha(z)}{z^m} = \frac{a_0}{z^m} + \cdots + \frac{a_{m-1}}{z} + a_m + a_{m+1}z + \cdots + a_{2m}z^m,$$

implying that

$$f\left(\frac{1}{z}\right) = z^m \alpha\left(\frac{1}{z}\right) = a_0 z^m + \cdots + a_{m-1}z + a_m + \frac{a_{m+1}}{z} + \cdots + \frac{a_{2m}}{z^m}$$

and also

$$f(-z) = \frac{\alpha(-z)}{(-z)^m} = \frac{a_0}{(-z)^m} + \cdots + \frac{a_{m-1}}{-z} + a_m + a_{m+1}(-z) + \cdots + a_{2m}(-z)^m.$$

We then observe that the fact that α is skewsymmetric implies that $f(1/z) = f(-z)$, or equivalently, that

$$z^m \alpha\Big(\frac{1}{z}\Big) = \frac{\alpha(-z)}{(-z)^m} \tag{2.11}$$

which (substituting $-z$ for z) implies that we also have

$$(-z)^m \alpha\Big(-\frac{1}{z}\Big) = \frac{\alpha(z)}{z^m}. \tag{2.12}$$

We then conclude that

$$\big(\text{LHS of (2.11)}\big) \times \big(\text{RHS of (2.12)}\big) = \big(\text{RHS of (2.11)}\big) \times \big(\text{LHS of (2.12)}\big)$$

or equivalently, that $\alpha(z)\alpha(1/z) = \alpha(-z)\alpha(-1/z)$, which for $z \in \mathbb{S}$ is equivalent to the desired conclusion that $|\alpha(z)|^2 = |\alpha(-z)|^2$. ∎

So skewsymmetric Littlewood polynomials are 'halfway' to being Barker. As a sort of 'converse', all known odd length Barker polynomials are skewsymmetric. In fact, one can show (although we omit the proof) that any odd length Barker polynomial must be skewsymmetric; this is essentially contained in [48] where they prove the stronger result that there are no odd length Barker polynomials of length greater than 13.

Skewsymmetric Littlewood polynomials enjoy another 'flatness' property: as we mentioned at the end of Section 1.3, they tend to have particularly high minimum modulus on $\mathbb{S}$. Exhaustive searches of $\mathcal{L}_n$ by Robinson [41] reveal that for each $n \in \{11, 13, \ldots, 25\}$, the polynomial with highest minimum modulus on $\mathbb{S}$ among all 2^n polynomials in $\mathcal{L}_n$ turns out to be skewsymmetric. It is not known if this pattern continues for larger values of n, but searches over just the skewsymmetric polynomials in $\mathcal{L}_n$ have yielded further examples of polynomials with high minimum modulus. In Section 2.3, we prove the author's result [31] that all skewsymmetric Littlewood polynomials satisfy the further 'flatness' condition of never attaining a modulus of zero on $\mathbb{S}$.

Self-reciprocal Littlewood polynomials, by contrast, are 'far' from having high minimum modulus on $\mathbb{S}$, in the sense that they always have at least one zero on the unit circle. This is already known [11], but we prove it in a new way by deriving it as a corollary of Theorem 2.6 of the next section.

To prove our results about the behaviour of special Littlewood polynomials on $\mathbb{S}$, we find it useful to assemble some facts about cosine sums and Chebyshev polynomials.

2.2 Relevant facts about cosine sums

Let θ be a real variable and let $c := \cos\theta$. For nonnegative integers n, each of the expressions

$$T_n := \cos(n\theta),$$
$$U_n := \frac{\sin\big((n+1)\theta\big)}{\sin\theta}$$

is a polynomial in c of degree n, called the **Chebyshev polynomials** of the first and second kind respectively. It is easy to check that

$$T_0 = 1, \qquad U_0 = 1,$$
$$T_1 = c, \qquad U_1 = 2c,$$

and one can use well-known trigonometric identities to show that for $n \geq 1$, we have

$$T_{n+1} = 2cT_n - T_{n-1},$$
$$U_{n+1} = 2cU_n - U_{n-1}.$$

This makes it a routine matter to list the first few Chebyshev polynomials of both kinds, which we do below for illustrative purposes.

$$T_0 = 1, \qquad U_0 = 1,$$
$$T_1 = c, \qquad U_1 = 2c,$$
$$T_2 = 2c^2 - 1, \qquad U_2 = 4c^2 - 1,$$
$$T_3 = 4c^3 - 3c, \qquad U_3 = 8c^3 - 4c,$$
$$T_4 = 8c^4 - 8c^2 + 1, \qquad U_4 = 16c^4 - 12c^2 + 1.$$

Some facts about Chebyshev polynomials are easy to prove by induction. For instance:

- Both T_n and U_n are odd when n is odd, and even when n is even. (An 'odd polynomial' is one containing only odd powers of the variable; 'even polynomial' is defined analogously.)
- For $n \geq 1$, the leading term of T_n is $2^{n-1}c^n$. For $n \geq 0$, the leading term of U_n is $2^n c^n$.

Since T_n has degree n, any polynomial in c of degree n can be written uniquely as a linear combination of $T_0, T_1, \ldots, T_n$. In particular, it is natural to ask how to write U_n as a linear combination of $T_0, T_1, \ldots, T_n$. This is answered by the following result, which has a straightforward inductive proof and which can be found, for example, as part of Problem 16 in Part VI of [40].

Proposition 2.3 *Let T_n and U_n be as previously defined. We then have*

$$U_{2m} = T_0 + \sum_{k=1}^{m} 2T_{2k}, \tag{2.13}$$

$$U_{2m+1} = \sum_{k=0}^{m} 2T_{2k+1} \tag{2.14}$$

for all $m \geq 0$.

We now define the new variable $x := 2c$. Then trivially, T_n and U_n can be regarded as polynomials in x rather than polynomials in c. It is easy to show by induction that U_n and $2T_n$ have integer coefficients when regarded as polynomials in x, since we have

$$2T_{n+1} = 4cT_n - 2T_{n-1} = x \cdot 2T_n - 2T_{n-1},$$
$$U_{n+1} = 2cU_n - U_{n-1} = xU_n - U_{n-1}.$$

Therefore $T_0, 2T_1, 2T_2, \ldots$ and $U_0, U_1, U_2, \ldots$ belong to $\mathbb{Z}[x]$, where as usual, $\mathbb{Z}[x]$ means the ring of polynomials in x with integer coefficients. For illustration, we now give

the first few polynomials in each of those lists.

$$\begin{aligned} T_0 &= 1, & U_0 &= 1, \\ 2T_1 &= x, & U_1 &= x, \\ 2T_2 &= x^2 - 2, & U_2 &= x^2 - 1, \\ 2T_3 &= x^3 - 3x, & U_3 &= x^3 - 2x, \\ 2T_4 &= x^4 - 4x^2 + 2, & U_4 &= x^4 - 3x^2 + 1. \end{aligned}$$

It is easy to see that when U_n is regarded as a polynomial in $\mathbb{Z}[x]$, its leading term is x^n. The same is true of $2T_n$ if $n \geq 1$. From now on, we will write U_n and $2T_n$ as $\overline{U_n}$ and $\overline{2T_n}$ respectively, if regarding them as polynomials in x, in order to avoid possible ambiguity.

To prove that skewsymmetric Littlewood polynomials have no roots on $\mathbb{S}$, the crucial ingredient turns out to be the following observation. Roughly speaking, two polynomials in $\mathbb{Z}[x]$ that have the same pattern of odd and even coefficients as $\overline{U_n}$ and $\overline{U_{n+1}}$ cannot have any common roots.

We define $\mathbb{Z}_2 := \mathbb{Z}/(2\mathbb{Z})$ (the integers mod 2). Let φ be the natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_2$, and let Φ be the homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}_2[x]$ defined by

$$\Phi(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$$

(that is, Φ simply reduces all coefficients mod 2). We then have the following.

Lemma 2.4 *Let n be a nonnegative integer, and let $A(x), B(x)$ be two polynomials in $\mathbb{Z}[x]$ satisfying*

- $\Phi\big(A(x)\big) = \Phi\big(\overline{U_{n+1}}\big)$,
- $\Phi\big(B(x)\big) = \Phi\big(\overline{U_n}\big)$,
- *one of $A(x), B(x)$ is odd and the other is even.*

Then no complex number is a root of both $A(x)$ and $B(x)$.

Proof. If $n = 0$, the hypotheses of the lemma say $B(x)$ is an odd nonzero constant and hence has no roots whatsoever. Assume the result is true for n, and let $A(x), B(x) \in \mathbb{Z}[x]$ satisfy

- $\Phi\big(A(x)\big) = \Phi\big(\overline{U_{n+2}}\big)$,
- $\Phi\big(B(x)\big) = \Phi\big(\overline{U_{n+1}}\big)$,
- one of $A(x), B(x)$ is odd and the other is even.

We wish to show $A(x)$ and $B(x)$ have no common roots. The hypotheses imply that the leading term of $A(x)$ is ax^{n+2} where a is odd, and that the leading term of $B(x)$ is bx^{n+1} where b is odd. Define $r := \operatorname{lcm}(a, b)$, $s := r/a$, and $t := r/b$, so r, s, t are odd integers. Then $C(x) := sA(x) - txB(x)$ is a linear combination of $A(x)$ and $B(x)$ where the x^{n+2} term has been 'killed'. Notice that $C(x)$ is odd if $A(x)$ is odd, and is even if $A(x)$ is even. Thus $\deg C(x) \leq n$. Furthermore, any common root of $A(x)$ and $B(x)$ is also a root of $C(x)$. We now observe that

$$\begin{aligned}
\Phi\big(C(x)\big) &= \Phi\big(sA(x) - txB(x)\big) \\
&= \Phi(s)\Phi\big(A(x)\big) + \Phi(-tx)\Phi\big(B(x)\big) \\
&= \Phi(1)\Phi\big(\overline{U_{n+2}}\big) + \Phi(-x)\Phi\big(\overline{U_{n+1}}\big) \\
&= \Phi\big(\overline{U_{n+2}} - x\overline{U_{n+1}}\big) \\
&= \Phi\big(\overline{-U_n}\big) = \Phi\big(\overline{U_n}\big).
\end{aligned}$$

This means that $B(x)$ and $C(x)$ satisfy the induction hypothesis, so $B(x)$ and $C(x)$ have no common roots. This implies $A(x)$ and $B(x)$ have no common roots, as required. ∎

In order to state and prove some more results about trigonometric sums, we now make the following definition, following [17].

Definition 2.5 *A* **zero-mean cosine polynomial** *is any function of the form*

$$f(\theta) = a_n \cos\big(n\theta\big) + a_{n-1} \cos\big((n-1)\theta\big) + \cdots + a_1 \cos\big(\theta\big),$$

and a **monic zero-mean cosine polynomial** *is any function of the form*

$$f(\theta) = \cos\big(n\theta\big) + a_{n-1}\cos\big((n-1)\theta\big) + \cdots + a_1\cos\big(\theta\big).$$

Here, a_1 through a_n are real numbers.

Note that any monic zero-mean cosine polynomial f can of course be rewritten as

$$f = T_n + a_{n-1}T_{n-1} + \cdots + a_1 T_1. \tag{2.15}$$

If $c := \cos\theta$ as before, then (2.15) is a polynomial in c of degree n whose leading coefficient is the same as that of T_n. If we then recall the well-known fact (see, e.g., Exercise E2 in Chapter 7 of [3], or Section 8.3 of [6]) that Chebyshev polynomials of the first kind have minimum supnorm on $[-1,1]$ among polynomials of prescribed degree and prescribed leading coefficient, we can conclude

$$\max_{-\pi\le\theta\le\pi}|f| = \max_{0\le\theta\le\pi}|f| = \max_{-1\le c\le 1}|f| \ge \max_{-1\le c\le 1}|T_n| = \max_{0\le\theta\le\pi}|\cos(n\theta)| = 1,$$

so we have either $f \ge +1$ somewhere or $f \le -1$ somewhere. By continuity and the fact that the average value of (2.15) is 0, we conclude that either $f(\theta) = +1$ for some $\theta \in [0,\pi]$ or $f(\theta) = -1$ for some $\theta \in [0,\pi]$. The following result shows that we can make the stronger statement that both of these possibilities must occur. This does not seem to follow immediately from basic properties of Chebyshev polynomials, but it does have a short proof using complex analysis which is essentially due to the referee of the first submitted version of [31].

Theorem 2.6 *If f is a monic zero-mean cosine polynomial, then $f(\theta) = +1$ for some $\theta \in [0,\pi]$, and $f(\theta) = -1$ for some $\theta \in [0,\pi]$.*

Before proving the theorem, we digress to recall some facts from complex analysis that we will need. These facts may be found, for example, in Sections 4.4 and 5.1 of [28].

If $p : \mathbb{C} \to \mathbb{C}$ is any continuous function, we can think of p as a 'transformation' from one copy of the complex plane (the z-plane) to another copy of the complex plane (the w-plane). The image under p of the unit circle $\mathbb{S}$ in the z-plane is a closed

curve, which we call Γ, in the w-plane. That is, Γ is the closed curve formed by $p(e^{i\theta})$ as θ increases from 0 to 2π.

If ξ is a point in the w-plane, and $\xi \notin \Gamma$, then we define the **winding number** of Γ around ξ (also called the 'index' of Γ with respect to ξ), which is an integer denoted $\mathrm{Ind}_\Gamma(\xi)$. Geometrically, $\mathrm{Ind}_\Gamma(\xi)$ can be regarded as the number of times the curve Γ goes counterclockwise around ξ as θ increases from 0 to 2π. It also has the integral formulation

$$\mathrm{Ind}_\Gamma(\xi) = \frac{1}{2\pi i} \oint_\Gamma \frac{1}{w-\xi}\, dw. \tag{2.16}$$

We are interested only in the case $\xi = 0$.

Suppose now that p is analytic on all of $\mathbb{C}$. (In fact, we care only about the case when p is a polynomial.) Then p has no poles. Suppose further that p has no zeros on $\mathbb{S}$. Then the curve Γ, being the image of $\mathbb{S}$ under p, does not go through the point 0 in the w-plane, so $\mathrm{Ind}_\Gamma(0)$ is defined. It is a theorem, which we will call the **argument principle**, that under these conditions, the sum of the orders of all zeros of p inside $\mathbb{S}$ is equal to

$$\frac{1}{2\pi i} \oint_{\mathbb{S}} \frac{p'(z)}{p(z)}\, dz. \tag{2.17}$$

Using the substitution $w = p(z)$, we see that the integrals in (2.16) and (2.17) are equal. Thus, the argument principle may be rephrased as: Under the conditions described above, the sum of the orders of all zeros of p inside $\mathbb{S}$ is equal to the number of times the image curve Γ goes around the origin.

Proof of Theorem 2.6. Note that $f(\theta) \pm 1 = \mathrm{Re}\big(p(e^{i\theta})\big)$, where

$$p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z \pm 1.$$

Since the product of all roots of p is ± 1, we conclude p has at least one root inside or on the unit circle. Let Γ denote the closed curve formed by $p(e^{i\theta})$ for $\theta \in [0, 2\pi]$. If p has a root on the unit circle, then certainly Γ passes through the origin and thus intersects the line $\mathrm{Re}\, z = 0$. If p has no roots on the unit circle, then p has at least one root inside the unit circle. By the Argument Principle, we then conclude Γ goes around the origin at least once and thus intersects the line $\mathrm{Re}\, z = 0$. In either case, $f(\theta) \pm 1 = \mathrm{Re}\big(p(e^{i\theta})\big)$ must have at least one real zero. ∎

The author's original submitted version of [31] contained an alternate proof of Theorem 2.6 that, although longer, provided a new way of deriving some results of [17] as corollaries. We therefore now give this longer alternate proof of Theorem 2.6.

Alternate proof of Theorem 2.6. We define

$$g(\theta) = a_{n-1}\cos\big((n-1)\theta\big) + \cdots + a_1\cos\big(\theta\big), \tag{2.18}$$

so we have $f(\theta) = \cos(n\theta) + g(\theta)$. Observe that since f has average value 0 on $[0,\pi]$, it suffices to show that $f(\theta) \geq +1$ for some θ and that $f(\theta) \leq -1$ for some θ. We now consider two cases.

Case 1. Suppose n is even; say $n = 2m$. Then $\cos(n\theta) = +1$ at each of the $m+1$ points

$$\theta = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \pi$$

and $\cos(n\theta) = -1$ at each of the m points

$$\theta = \frac{\pi}{n}, \frac{3\pi}{n}, \frac{5\pi}{n}, \ldots, \frac{(n-1)\pi}{n}.$$

We show that the $m+1$ values

$$g(0), g\Big(\frac{2\pi}{n}\Big), g\Big(\frac{4\pi}{n}\Big), \ldots, g(\pi)$$

cannot all be negative by showing they cannot all have the same sign, and we show that the m values

$$g\Big(\frac{\pi}{n}\Big), g\Big(\frac{3\pi}{n}\Big), g\Big(\frac{5\pi}{n}\Big), \ldots, g\Big(\frac{(n-1)\pi}{n}\Big)$$

cannot all be positive by showing they cannot all have the same sign. This will follow if we can prove that the identities

$$g(0) + 2g\Big(\frac{2\pi}{n}\Big) + 2g\Big(\frac{4\pi}{n}\Big) + \cdots + 2g\Big(\frac{(n-2)\pi}{n}\Big) + g(\pi) = 0 \tag{2.19}$$

and

$$g\Big(\frac{\pi}{n}\Big) + g\Big(\frac{3\pi}{n}\Big) + g\Big(\frac{5\pi}{n}\Big) + \cdots + g\Big(\frac{(n-1)\pi}{n}\Big) = 0 \tag{2.20}$$

are true independently of the values of $a_1, \ldots, a_{n-1}$.

To verify that (2.19) holds, we note that the left-hand side of (2.19) is

$$g(0)+g(\pi)+2\sum_{j=1}^{m-1} g\Big(\frac{2j\pi}{n}\Big) = \sum_{k=1}^{n-1} a_k\cos 0 + \sum_{k=1}^{n-1} a_k\cos k\pi + 2\sum_{j=1}^{m-1}\sum_{k=1}^{n-1} a_k\cos\frac{2jk\pi}{n}$$
$$= \sum_{k=1}^{n-1} a_k\Big(\cos 0+\cos k\pi + 2\sum_{j=1}^{m-1}\cos\frac{2jk\pi}{n}\Big).$$

Thus it suffices to show that for fixed k satisfying $1\le k\le n-1$, we have

$$\cos 0+\cos k\pi + 2\sum_{j=1}^{m-1}\cos\frac{2jk\pi}{n} = 0. \tag{2.21}$$

For such k, the complex number $\zeta := e^{i2\pi k/n}$ is an nth root of unity other than 1, so

$$\sum_{j=0}^{n-1}\zeta^j = 0 \implies 0 = \sum_{j=0}^{n-1}\operatorname{Re}\,\zeta^j = \sum_{j=0}^{n-1}\cos\frac{2jk\pi}{n} = \sum_{j=0}^{2m-1}\cos\frac{2jk\pi}{n}$$
$$= \cos 0 + \sum_{j=1}^{m-1}\cos\frac{2jk\pi}{n} + \cos k\pi + \sum_{j=m+1}^{2m-1}\cos\frac{2jk\pi}{n}. \tag{2.22}$$

The rightmost sum in (2.22) is (using the transformation $j' := n-j = 2m-j$)

$$\sum_{j=m+1}^{2m-1}\cos\frac{2jk\pi}{n} = \sum_{j'=1}^{m-1}\cos\frac{2(2m-j')k\pi}{n} = \sum_{j'=1}^{m-1}\cos\Big(2k\pi-\frac{2j'k\pi}{n}\Big) = \sum_{j'=1}^{m-1}\cos\frac{2j'k\pi}{n}.$$

This proves (2.21) and hence completes the verification of (2.19).

To verify that (2.20) holds, we note that the left-hand side of (2.20) is

$$\sum_{j=1}^{m} g\Big(\frac{(2j-1)\pi}{n}\Big) = \sum_{j=1}^{m}\sum_{k=1}^{n-1} a_k\cos\frac{(2j-1)k\pi}{n}$$
$$= \sum_{k=1}^{n-1} a_k\Big(\sum_{j=1}^{m}\cos\frac{(2j-1)k\pi}{n}\Big).$$

Thus it suffices to show that for fixed k satisfying $1\le k\le n-1$, we have

$$\sum_{j=1}^{m}\cos\frac{(2j-1)k\pi}{n} = 0. \tag{2.23}$$

But this is precisely Lemma 2(i) of [17] (and also follows immediately from Problem 16 in Part VI of [40]). This proves (2.23) and hence completes the verification of (2.20). Thus we are finished with Case 1.

Case 2. Suppose n is odd; say $n = 2m - 1$. Then $\cos(n\theta) = +1$ at each of the m points

$$\theta = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{(n-1)\pi}{n}$$

and $\cos(n\theta) = -1$ at each of the m points

$$\theta = \frac{\pi}{n}, \frac{3\pi}{n}, \frac{5\pi}{n}, \ldots, \pi.$$

Analogously to Case 1, we show that the m values

$$g(0), g\Big(\frac{2\pi}{n}\Big), g\Big(\frac{4\pi}{n}\Big), \ldots, g\Big(\frac{(n-1)\pi}{n}\Big)$$

cannot all be negative by showing they cannot all have the same sign, and we show that the m values

$$g\Big(\frac{\pi}{n}\Big), g\Big(\frac{3\pi}{n}\Big), g\Big(\frac{5\pi}{n}\Big), \ldots, g(\pi)$$

cannot all be positive by showing they cannot all have the same sign. This will follow if we can prove that the identities

$$g(0) + 2g\Big(\frac{2\pi}{n}\Big) + 2g\Big(\frac{4\pi}{n}\Big) + \cdots + 2g\Big(\frac{(n-1)\pi}{n}\Big) = 0 \tag{2.24}$$

and

$$2g\Big(\frac{\pi}{n}\Big) + 2g\Big(\frac{3\pi}{n}\Big) + \cdots + 2g\Big(\frac{(n-2)\pi}{n}\Big) + g(\pi) = 0 \tag{2.25}$$

are true independently of the values of $a_1, \ldots, a_{n-1}$.

To verify that (2.24) holds, we note that the left-hand side of (2.24) is

$$\begin{aligned} g(0) + 2\sum_{j=1}^{m-1} g\Big(\frac{2j\pi}{n}\Big) &= \sum_{k=1}^{n-1} a_k \cos 0 + 2\sum_{j=1}^{m-1}\sum_{k=1}^{n-1} a_k \cos\frac{2jk\pi}{n} \\ &= \sum_{k=1}^{n-1} a_k \Big(\cos 0 + 2\sum_{j=1}^{m-1} \cos\frac{2jk\pi}{n} \Big). \end{aligned}$$

Thus it suffices to show that for fixed k satisfying $1 \le k \le n-1$, we have

$$\cos 0 + 2\sum_{j=1}^{m-1} \cos \frac{2jk\pi}{n} = 0. \tag{2.26}$$

For such k, the complex number $\zeta := e^{i2\pi k/n}$ is an nth root of unity other than 1, so

$$\begin{aligned}\sum_{j=0}^{n-1} \zeta^j = 0 \implies 0 = \sum_{j=0}^{n-1} \operatorname{Re} \zeta^j = \sum_{j=0}^{n-1} \cos \frac{2jk\pi}{n} = \sum_{j=0}^{2m-2} \cos \frac{2jk\pi}{n} \\ = \cos 0 + \sum_{j=1}^{m-1} \cos \frac{2jk\pi}{n} + \sum_{j=m}^{2m-2} \cos \frac{2jk\pi}{n}. \end{aligned} \tag{2.27}$$

The rightmost sum in (2.27) is (using the transformation $j' := n-j = (2m-1)-j$)

$$\sum_{j=m}^{2m-2} \cos \frac{2jk\pi}{n} = \sum_{j'=1}^{m-1} \cos \frac{2(n-j')k\pi}{n} = \sum_{j'=1}^{m-1} \cos \left(2k\pi - \frac{2j'k\pi}{n}\right) = \sum_{j'=1}^{m-1} \cos \frac{2j'k\pi}{n}.$$

This proves (2.26) and hence completes the verification of (2.24).

To verify that (2.25) holds, we note that the left-hand side of (2.25) is

$$\begin{aligned} g(\pi) + 2\sum_{j=1}^{m-1} g\Big(\frac{(2j-1)\pi}{n}\Big) = \sum_{k=1}^{n-1} a_k \cos k\pi + 2\sum_{j=1}^{m-1}\sum_{k=1}^{n-1} a_k \cos \frac{(2j-1)k\pi}{n} \\ = \sum_{k=1}^{n-1} a_k \Big(\cos k\pi + 2\sum_{j=1}^{m-1} \cos \frac{(2j-1)k\pi}{n} \Big). \end{aligned}$$

Thus it suffices to show that for fixed k satisfying $1 \le k \le n-1$, we have

$$\cos k\pi + 2\sum_{j=1}^{m-1} \cos \frac{(2j-1)k\pi}{n} = 0. \tag{2.28}$$

But this is precisely Lemma 2(ii) of [17]. (It can also be proved by a very similar argument to our proofs of (2.21) and (2.26).) This proves (2.28) and hence completes the verification of (2.25). Thus we are finished with Case 2, and the alternate proof of Theorem 2.6 is complete. ∎

Note that the following is a consequence of the alternate proof of Theorem 2.6, as opposed to a corollary of the statement of Theorem 2.6.

Proposition 2.7 *Suppose g is of the form (2.18) (where n may be even or odd). Then g cannot maintain the same sign throughout the interval $[0, (n-1)\pi/n]$, and g cannot maintain the same sign throughout the interval $[\pi/n, \pi]$.*

Proposition 2.7 constitutes the nonexistence portion of Corollaries 1 and 3 of [17]. It is further shown in [17] that the intervals in Proposition 2.7 are best possible.

2.3 Unimodular roots of special Littlewoods

The following theorem is the main original result of Chapter 2. The crucial ingredient in the proof is Lemma 2.4 of the previous section.

Theorem 2.8 *A skewsymmetric Littlewood polynomial has no zeros on the unit circle (in other words, no roots of unit modulus, or 'unimodular roots').*

Proof. Let $\alpha(z)$ be a skewsymmetric Littlewood polynomial. Hence $\alpha(z)$ has even degree, so say

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{2m} z^{2m} \quad (a_j = \pm 1)$$

where $a_{m+j} = (-1)^j a_{m-j}$ for $j \in \{1, 2, \ldots, m\}$. We then have

$$\begin{aligned} \frac{\alpha(z)}{z^m} &= a_0 \frac{1}{z^m} + \cdots + a_{m-1} \frac{1}{z} + a_m + a_{m+1} z + \cdots + a_{2m} z^m \\ &= a_m + \sum_{j=1}^{m} \left(a_{m+j} z^j + a_{m-j} \frac{1}{z^j} \right) \\ &= a_m + \sum_{j=1}^{m} a_{m+j} \left(z^j + (-1)^j \frac{1}{z^j} \right) =: f(z). \end{aligned}$$

Showing $\alpha(z)$ has no zeros on $\mathbb{S}$ is equivalent to showing $f(z)$ has no zeros on $\mathbb{S}$, which in turn is equivalent to showing $f(iz)$ has no zeros on $\mathbb{S}$. Observe that

$$\begin{aligned} f(iz) &= a_m + \sum_{j=1}^{m} a_{m+j}\Big((iz)^j + (-1)^j \frac{1}{(iz)^j}\Big) \\ &= a_m + \sum_{j=1}^{m} a_{m+j}\Big(i^j z^j + \Big(\frac{-1}{i}\Big)^j \frac{1}{z^j}\Big) \\ &= a_m + \sum_{j=1}^{m} a_{m+j} i^j \Big(z^j + \frac{1}{z^j}\Big) \\ &= a_m + \sum_{j=1}^{m} a_{m+j} i^j \cdot 2\cos(j\theta) \qquad (\text{where } z = e^{i\theta}). \end{aligned}$$

To show $f(iz)$ is never 0 on $\mathbb{S}$, it suffices to show that $\mathrm{Re} f(iz)$ and $\mathrm{Im} f(iz)$ cannot both be 0. Recalling that each a_j is ± 1, and defining $r := \lfloor m/2 \rfloor$, we see that

$$\begin{aligned} \mathrm{Re} f(iz) &= \pm 1 \pm 2\cos(2\theta) \pm 2\cos(4\theta) \pm \cdots \pm 2\cos(2r\theta), \\ \mathrm{Im} f(iz) &= \pm 2\cos\big(\theta\big) \pm 2\cos\big(3\theta\big) \pm 2\cos\big(5\theta\big) \pm \cdots \pm 2\cos\big((2r\pm 1)\theta\big). \end{aligned}$$

which, using the notation defined in Section 2.2, can be rewritten as

$$\begin{aligned} \mathrm{Re} f(iz) &= \pm 1 \pm 2T_2 \pm 2T_4 \pm \cdots \pm 2T_{2r}, \\ \mathrm{Im} f(iz) &= \pm 2T_1 \pm 2T_3 \pm 2T_5 \pm \cdots \pm 2T_{2r\pm 1}. \end{aligned}$$

Now let $A := \mathrm{Re} f(iz)$ and let $B := \mathrm{Im} f(iz)$. Both A and B can be regarded as polynomials in x with integer coefficients, where as before, $x := 2c := 2\cos\theta$. Notice that one of A, B is odd and the other is even, and that $\deg A$ and $\deg B$ differ by 1. We now observe that

$$\begin{aligned} \Phi(A) &= \Phi\big(\pm 1 \pm \overline{2T_2} \pm \overline{2T_4} \pm \cdots \pm \overline{2T_{2r}}\big) \\ &= \Phi\big(\pm 1\big) + \Phi\big(\pm \overline{2T_2}\big) + \Phi\big(\pm \overline{2T_4}\big) + \cdots + \Phi\big(\pm \overline{T_{2r}}\big) \\ &= \Phi\big(1\big) + \Phi\big(\overline{2T_2}\big) + \Phi\big(\overline{2T_4}\big) + \cdots + \Phi\big(\overline{T_{2r}}\big) \\ &= \Phi\big(1 + \overline{2T_2} + \overline{2T_4} + \cdots + \overline{2T_{2r}}\big) \\ &= \Phi\big(\overline{U_{2r}}\big) \quad \text{by (2.13)} \end{aligned}$$

and similarly,

$$\begin{aligned}\Phi(B) &= \Phi\big(\pm\overline{2T_1}\pm\overline{2T_3}\pm\cdots\pm\overline{2T_{2r\pm1}}\big)\\ &= \Phi\big(\pm\overline{2T_1}\big)+\Phi\big(\pm\overline{2T_3}\big)+\cdots+\Phi\big(\pm\overline{2T_{2r\pm1}}\big)\\ &= \Phi\big(\overline{2T_1}\big)+\Phi\big(\overline{2T_3}\big)+\cdots+\Phi\big(\overline{2T_{2r\pm1}}\big)\\ &= \Phi\big(\overline{2T_1}+\overline{2T_3}+\cdots+\overline{2T_{2r\pm1}}\big)\\ &= \Phi\big(\overline{U_{2r\pm1}}\big)\quad\text{by (2.14).}\end{aligned}$$

Thus A and B, in some order, satisfy the hypotheses of Lemma 2.4, and the theorem is proved. ∎

We now shift our attention to self-reciprocal polynomials. There are two known results about self-reciprocal polynomials that have new proofs as immediate corollaries of Theorem 2.6. The first appears as Corollary 2 in [27].

Corollary 2.9 *Suppose $\alpha(z)$ is a self-reciprocal polynomial of even degree, say*

$$\alpha(z) = a_0+\cdots+a_{m-1}z^{m-1}+a_mz^m+a_{m-1}z^{m+1}+\cdots+a_0z^{2m}$$

where $a_0,\ldots,a_m$ are real. Suppose $|a_m|\le 2\,|a_0|$ (informally, the middle coefficient is no more than twice as big as the end coefficients). Then $\alpha(z)$ has at least one root on the unit circle.

Proof. For $\alpha(z)$ as above and $z=e^{i\theta}\in\mathbb{S}$, we have

$$\begin{aligned}\frac{\alpha(z)}{z^m} &= a_0\frac{1}{z^m}+\cdots+a_{m-1}\frac{1}{z}+a_m+a_{m-1}z+\cdots+a_0z^m\\ &= a_m+2\Big(a_{m-1}\operatorname{Re}z+\cdots+a_0\operatorname{Re}z^m\Big)\\ &= a_m+2\Big(a_{m-1}\cos(\theta)+\cdots+a_0\cos(m\theta)\Big).\end{aligned}\tag{2.29}$$

By Theorem 2.6, the expression (2.29) attains both of the values a_m+2a_0 and a_m-2a_0 on the interval $[0,\pi]$. Suppose $a_0\ge 0$ (the other case is similar). Then the condition $|a_m|\le 2\,|a_0|$ gives us

$$-2a_0\le a_m\le+2a_0,$$

which implies that the interval $[a_m - 2a_0,\ a_m + 2a_0]$ contains 0. By continuity, and the fact that (2.29) is real-valued, we conclude that $\alpha(z)/z^m$ and hence also $\alpha(z)$ is equal to 0 for some $z \in \mathbb{S}$. ∎

Corollary 2.9, restricted to the Littlewood case, gives a new proof of the following (which also appears as Theorem 2.8 in [11]).

Corollary 2.10 *A self-reciprocal polynomial whose coefficients are* ± 1 *has at least one zero on* $\mathbb{S}$.

Proof. Let α be a self-reciprocal polynomial whose coefficients are ± 1. If the degree of α is odd, it is straightforward to show that -1 is a root of α. If the degree of α is even, then the condition $|a_m| \leq 2\,|a_0|$ in Corollary 2.9 is satisfied, so α has a root on $\mathbb{S}$. ∎

Chapter 3

Autocorrelation in $\mathcal{L}_n$

> When I was a kid, I used to pray every night for a new bicycle. Then I realized that the Lord, in his wisdom, doesn't work that way. So I just stole one and asked him to forgive me.
> —Emo Philips (by permission)

3.1 Average of c_k^r over $\mathcal{L}_n$

As mentioned in Section 1.5, we turn $\mathcal{L}_n$ into a finite probability space by defining a probability mass function p that assigns a weight to each of the 2^n polynomials in $\mathcal{L}_n$. We give each polynomial equal weight by defining $p(\alpha) = 1/2^n$ for all $\alpha \in \mathcal{L}_n$. It is easy to see that this means the n coefficients $a_0, a_1, \ldots, a_{n-1}$ are independent random variables.

Suppose now that n and k are fixed positive integers with $k < n$, and define $Y_k := c_{n-k}$, so Y_k is the autocorrelation which is a sum of k terms. (Here we are reverting to the common convention of using capital letters to denote random variables.) We also define $X_j := a_j a_{j+n-k}$ for $0 \leq j \leq k-1$, so we have

$$\begin{aligned} Y_k &= a_0 a_{n-k} + a_1 a_{n-k+1} + \cdots + a_{k-1} a_{n-1} \\ &= X_0 + X_1 + \cdots + X_{k-1}. \end{aligned}$$

The following is the crucial observation that allows us to prove the results of Chapter 3.

Proposition 3.1 *The X_j are mutually independent.*

Proposition 3.1 is not difficult and has undoubtedly been discovered previously (the referee of the first submitted version of [32] claimed it was known to the French harmonic analysts of the 1960s) but since proofs are surprisingly hard to find in the literature given the relative simplicity of the proposition, we include a short proof below.

Proof of Proposition 3.1. By Proposition 1.42, we just need to show that if the values of some of the X_j are specified, then any one of the remaining X_j is equally likely to be $+1$ or -1. So suppose $0 \le i_1 < i_2 < \cdots < i_m \le k-1$ and $j \notin \{i_1, i_2, \ldots, i_m\}$, and suppose we are given that

$$X_{i_\ell} = s_\ell \quad \text{for } 1 \le \ell \le m, \tag{3.1}$$

where each s_ℓ is either $+1$ or -1. We must show that among the polynomials in $\mathcal{L}_n$ that satisfy (3.1), half of them satisfy $X_j = +1$ and half satisfy $X_j = -1$.

Consider a graph G whose vertices are the a_j and whose edges are precisely the pairs of the form (a_j, a_{j+n-k}), so the edges correspond to the X_j. Note that the components of G are paths. Let G' be the graph obtained from G by deleting all edges except $X_{i_1}, \ldots, X_{i_m}$. Using the fact that the components of G' are paths, it is straightforward to see that the number of polynomials in $\mathcal{L}_n$ satisfying (3.1) is equal to 2^λ where λ is the number of components of G'. Observing that the endvertices of edge X_j lie in different components of G', we see that the 'conditional distribution' of X_j is as claimed. ∎

The mutual independence of the X_j has several immediate consequences. First, it is obvious by symmetry that $\mathbf{E}(Y_k^r) = 0$ if r is odd. We also see that for general r, $\mathbf{E}(Y_k^r)$ is given by the non-closed-form expression

$$P(k) := \sum_{j=0}^{k} \frac{\binom{k}{j}}{2^k} (k-2j)^r. \tag{3.2}$$

It is not immediately apparent that for fixed even r, the sum $P(k)$ is a polynomial in k of degree $r/2$.

One way to see that $P(k)$ is a polynomial in k, if one fixes a specific (even) value of r, is to apply Zeilberger's 'creative telescoping' algorithm, which can be found in Chapter 6 of [39]. This algorithm, when given the summand in (3.2) as input, outputs a recurrence satisfied by the function $P(k)$. That recurrence turns out to be of the form

$$a(k)P(k+1) + b(k)P(k) = 0, \tag{3.3}$$

where $a(k)$ and $b(k)$ are polynomials that happen to satisfy $b(k) = -a(k+1)$, in which case the recurrence (3.3) clearly has $P(k) = a(k)$ as a solution. So in summary, if one fixes an even value of r, then Zeilberger's algorithm can tell us that $\mathbf{E}(Y_k^r)$ is a polynomial in k.

It is also worth mentioning that an immediate consequence of Proposition 3.1 is that Y_k is a linearly transformed binomial random variable. More specifically, we have

$$Y_k = 2\Big(U - \frac{k}{2}\Big) = 2\big(U - \mathbf{E}(U)\big) \tag{3.4}$$

where U is binomial with parameters k and $1/2$. Thus, evaluating $\mathbf{E}(Y_k^r)$ reduces to evaluating the central moments of a binomial random variable, but as there is no simple closed-form expression for those central moments, this does not seem to make the evaluation of $\mathbf{E}(Y_k^r)$ trivial.

A 1923 recurrence due to Romanovsky [42], which also appears in Chapter 3 of [26], shows that if U is binomial with parameters k and p, then the rth central moment of U, considered as a polynomial in k, has degree at most $\lfloor r/2 \rfloor$. Romanovsky's recurrence, however, involves differentiation with respect to p, and if we care only about the special case $p = 1/2$, then a variant of Romanovsky's technique yields a more efficient way to generate the expected values of Y_k^r. This is the content of the following result.

Theorem 3.2 *As described previously, let $\mathcal{L}_n$ be regarded as a finite probability space by weighting each polynomial equally. If the autocorrelations c_k and the autocorrelation vector C are as defined in Section 1.2, then for $k < n$, $\mathbf{E}(c_{n-k}^{2m})$ is a polynomial in k of degree m, implying that $\mathbf{E}(|C|_{2m}^{2m})$ is a polynomial in n of degree $m+1$. If we define*

$$P_m(k) := \mathbf{E}(Y_k^{2m}) := \mathbf{E}(c_{n-k}^{2m}),$$

then we can generate the polynomials P_m recursively via

$$P_{m+1}(k) = k^2 P_m(k) - k(k-1)P_m(k-2).$$

Because of (3.4), this recurrence can also be viewed as generating the central moments of a binomial random variable that satisfies $p = 1/2$. More precisely, if U is binomial with parameters k and $1/2$, then the $(2m)$th central moment of U is

$$2^{-2m}\mathbf{E}(Y_k^{2m}) = 2^{-2m}P_m(k).$$

Proof of Theorem 3.2. By Proposition 3.1, we know that Y_k is a sum of k mutually independent random variables that are each equally likely to be $+1$ or -1. Then by Proposition 1.46, we know that the moment-generating function of Y_k is

$$M(t) := \left(\frac{e^{+t} + e^{-t}}{2}\right)^k = \cosh^k t = 1 + \mathbf{E}(Y_k^2)\frac{t^2}{2!} + \mathbf{E}(Y_k^4)\frac{t^4}{4!} + \cdots$$

(note that this function contains only even powers of t).

We now observe that

$$\begin{aligned}
\frac{d^2}{dt^2}M(t) &= \frac{d}{dt}\left(k\cosh^{k-1} t \sinh t\right) \\
&= k(k-1)\cosh^{k-2} t \sinh^2 t + k\cosh^k t \\
&= k(k-1)\cosh^{k-2} t(\cosh^2 t - 1) + k\cosh^k t \\
&= k^2\cosh^k t - k(k-1)\cosh^{k-2} t, \qquad (3.5)
\end{aligned}$$

but also

$$\begin{aligned}
\frac{d^2}{dt^2}M(t) &= \frac{d^2}{dt^2}\left(1 + \mathbf{E}(Y_k^2)\frac{t^2}{2!} + \mathbf{E}(Y_k^4)\frac{t^4}{4!} + \cdots\right) \\
&= \mathbf{E}(Y_k^2) + \mathbf{E}(Y_k^4)\frac{t^2}{2!} + \mathbf{E}(Y_k^6)\frac{t^4}{4!} + \cdots. \qquad (3.6)
\end{aligned}$$

If we now equate the coefficient of $t^{2m}/(2m)!$ in (3.6) and the coefficient of $t^{2m}/(2m)!$ in (3.5), we get

$$\mathbf{E}(Y_k^{2m+2}) = k^2\mathbf{E}(Y_k^{2m}) - k(k-1)\mathbf{E}(Y_{k-2}^{2m}),$$

or equivalently,

$$P_{m+1}(k) = k^2 P_m(k) - k(k-1)P_m(k-2),$$

establishing the theorem. ∎

For illustration, we now give the first few polynomials in the list $(P_1, P_2, P_3, \ldots)$:

$$\begin{aligned}
P_1(k) &= \mathbf{E}(Y_k^2) = k, \\
P_2(k) &= \mathbf{E}(Y_k^4) = 3k^2 - 2k, \\
P_3(k) &= \mathbf{E}(Y_k^6) = 15k^3 - 30k^2 + 16k, \\
P_4(k) &= \mathbf{E}(Y_k^8) = 105k^4 - 420k^3 + 588k^2 - 272k, \\
P_5(k) &= \mathbf{E}(Y_k^{10}) = 945k^5 - 6300k^4 + 16380k^3 - 18960k^2 + 7936k.
\end{aligned}$$

This permits us to list $\mathbf{E}(|C|_{2m}^{2m})$ for the first few values of m:

$$\begin{aligned}
\mathbf{E}(|C|_2^2) &= \sum_{k=1}^{n-1} \mathbf{E}(Y_k^2) = \sum_{k=1}^{n-1} P_1(k) \\
&= \frac{1}{2}n^2 - \frac{1}{2}n, \\
\mathbf{E}(|C|_4^4) &= \sum_{k=1}^{n-1} \mathbf{E}(Y_k^4) = \sum_{k=1}^{n-1} P_2(k) \\
&= n^3 - \frac{5}{2}n^2 + \frac{3}{2}n, \\
\mathbf{E}(|C|_6^6) &= \sum_{k=1}^{n-1} \mathbf{E}(Y_k^6) = \sum_{k=1}^{n-1} P_3(k) \\
&= \frac{15}{4}n^4 - \frac{35}{2}n^3 + \frac{107}{4}n^2 - 13n, \\
\mathbf{E}(|C|_8^8) &= \sum_{k=1}^{n-1} \mathbf{E}(Y_k^8) = \sum_{k=1}^{n-1} P_4(k) \\
&= 21n^5 - \frac{315}{2}n^4 + 441n^3 - 535n^2 + \frac{461}{2}n, \\
\mathbf{E}(|C|_{10}^{10}) &= \sum_{k=1}^{n-1} \mathbf{E}(Y_k^{10}) = \sum_{k=1}^{n-1} P_5(k) \\
&= \frac{315}{2}n^6 - \frac{3465}{2}n^5 + \frac{30555}{4}n^4 - 16610n^3 + \frac{69857}{4}n^2 - 6918n. \qquad (3.7)
\end{aligned}$$

By using Proposition 1.13, together with the trivial fact that a random variable cannot always exceed its expected value, we can obtain upper bounds on Turyn's b function

(Definition 1.10) that, loosely speaking, are 'slightly greater' than $\sqrt{n}$. For instance, a computation reveals that (3.7) is less than $(315/2)n^6$ for all $n \geq 1$. It follows that for $n \geq 1$, there is always at least one Littlewood polynomial in $\mathcal{L}_n$ that satisfies

$$|C|_\infty \leq |C|_{10} \leq \left(\frac{315}{2}n^6\right)^{1/10} \approx 1.658n^{6/10}.$$

We thus get an upper bound on $b(n)$ that is worse than Proposition 1.11 in a big O sense, but better than Proposition 1.11 in the sense that it holds for all n.

Looking at the polynomials $P_m(k)$ that we have listed so far, one might guess that in general, we have

$$P_m(k) = (2m-1)!!\, k^m + O(k^{m-1}),$$

where the notation $(2m-1)!!$ means $(2m-1)(2m-3)\cdots 3 \cdot 1$. This fact does not seem to follow immediately from the recurrence in Theorem 3.2, but it can be proved by a separate counting argument which we now digress to include.

Theorem 3.3 *As before, suppose our probability space is $\mathcal{L}_n$, and let Y_k and $P_m(k)$ be as previously defined. We then have*

$$P_m(k) = \mathbf{E}(Y_k^{2m}) = (2m-1)!!\, k^m + O(k^{m-1}).$$

Proof. We have

$$Y_k = \sum_{j \in [k]} X_j$$

where the X_j are as defined at the beginning of this chapter. We remember from Proposition 3.1 that the X_j are mutually independent ± 1 random variables. Now

$$\mathbf{E}(Y_k^r) = \sum_{(j_1,\ldots,j_r) \in [k]^r} \mathbf{E}(X_{j_1} \cdots X_{j_r}) \tag{3.8}$$

by linearity of expectation (Proposition 1.38). Here, we are using the convention that $[k]^r$ means the set of all r-tuples with entries from $[k]$. Let us now adopt some terminology that will assist us in our exposition. We will refer to any of the k^r elements of $[k]^r$ as a **word** consisting of r **spaces**, where each space is filled with one of the k **symbols** 0 through $k-1$.

Now since each X_{j_i} is ± 1, each expression of the form

$$X_{j_1} X_{j_2} \cdots X_{j_r}$$

can be rewritten as

$$X_0^{e_0} X_1^{e_1} \cdots X_{k-1}^{e_{k-1}} \tag{3.9}$$

where each e_i is 0 or 1. Specifically, e_i is either 0 or 1 depending on whether the symbol i appears an even or an odd number of times in the word $(j_1, j_2, \ldots, j_r)$. Now it follows easily from the mutual independence of the X_i that an expression of the form (3.9) has expected value 0, **unless** each e_i is 0, in which case its expected value is 1. It then follows from (3.8) that $\mathbf{E}(Y_k^r)$ is equal to the number of words in $[k]^r$ with the property that each symbol in the word appears an **even** number of times (possibly 0 times). For brevity, we will refer to such a word as a **pairful** word.

Certainly there are no pairful words in $[k]^r$ if r is odd, so suppose $r = 2m$. If we define $\psi(m, j)$ to be the number of ways of partitioning $[2m]$ into j disjoint nonempty parts each containing an even number of elements, then the number of pairful words in $[k]^{2m}$ is

$$\psi(m,m)k^{[m]} + \psi(m,m-1)k^{[m-1]} + \cdots + \psi(m,1)k^{[1]} \tag{3.10}$$

where we are using the notation $k^{[j]} := k(k-1)\cdots(k-j+1)$. (The same notation is used in Chapter 4.) To obtain (3.10), note that we can count the number of pairful words in $[k]^{2m}$ by first partitioning the $2m$ spaces into precisely j nonempty even-sized parts, where $1 \leq j \leq m$, such that spaces belonging to the same part are filled with the same symbol. We can then choose one of k symbols for the spaces in the first part, one of $k-1$ symbols for the spaces in the second part, and so on.

To the best of the author's knowledge, detailed study of the function ψ has not been done. However, to complete the proof of the theorem, we need only to observe that $\psi(m,m) = (2m-1)!!$ since counting partitions of $[2m]$ into m nonempty even-sized parts (necessarily parts of size 2) is equivalent to counting perfect matchings in the complete graph on $2m$ vertices. ∎

Suppose now that we care only about an upper bound for $\mathbf{E}(Y_k^{2m})$, as opposed to exact or asymptotic expressions for the polynomials $P_m(k)$. It was pointed out by the

referee of the first submitted version of [32] that we can prove

$$\mathbf{E}(Y_k^{2m}) \leq (2m-1)!!\, k^m \tag{3.11}$$

using some known results from probability. Specifically, we rely upon the following version of the Khinchin inequalities, due to Haagerup [22].

Proposition 3.4 *Let $X_0, \ldots, X_{k-1}$ be independent random variables, each equally likely to be $+1$ or -1, and let $r_0, \ldots, r_{k-1}$ be real constants. For positive real p, we have*

$$A_p\Big(\sum_{j=0}^{k-1} r_j^2\Big)^{1/2} \leq \Big[\mathbf{E}\Big(\Big|\sum_{j=0}^{k-1} r_j X_j\Big|^p\Big)\Big]^{1/p} \leq B_p\Big(\sum_{j=0}^{k-1} r_j^2\Big)^{1/2} \tag{3.12}$$

where A_p and B_p are constants depending only on p. If $p > 2$, we can take $A_p = 1$ and

$$B_p = 2^{1/2}\Big(\frac{\Gamma(\frac{p+1}{2})}{\sqrt{\pi}}\Big)^{1/p}$$

where Γ denotes the usual gamma function of Euler.

If we apply Proposition 3.4 to the case where $p = 2m$ for some $m \in \mathbb{Z}^+$ and $r_j = 1$ for all j, then the rightmost inequality in (3.12) gives

$$\mathbf{E}(Y_k^{2m}) = \mathbf{E}\Big(\Big|\sum_{j=0}^{k-1} X_j\Big|^{2m}\Big) \leq B_{2m}^{2m}\Big(\sum_{j=0}^{k-1} 1\Big)^m = B_{2m}^{2m} k^m,$$

and we then observe that

$$B_{2m}^{2m} = 2^m \frac{\Gamma(\frac{2m+1}{2})}{\sqrt{\pi}} = 2^m \frac{\frac{(2m-1)!!}{2^m}\sqrt{\pi}}{\sqrt{\pi}} = (2m-1)!!$$

which establishes that (3.11) holds as claimed.

3.2 Bounds on Turyn's b function

We pointed out in the previous section that one upper bound for Turyn's b function, valid for all $n \geq 1$, is

$$b(n) \leq \Big(\frac{315}{2}\Big)^{1/10} n^{6/10}.$$

Somewhat messy computations using the polynomials $P_m(k)$ for $m > 5$ can of course yield similar results with smaller exponents than 6/10, but any such result fails to improve upon Proposition 1.11 in an asymptotic or big O sense.

In this section, as mentioned in Section 1.2, we use some known techniques to provide a refinement of Proposition 1.11. To the best of the author's knowledge, this refinement constitutes the best asymptotic upper bound on $b(n)$ appearing in the available literature.

We begin by pointing out that Proposition 3.1 allows us to use Chernoff-type bounds for 'tails' of sums of independent ± 1 random variables. One such bound is given by the following result.

Proposition 3.5 *If $Y_k = X_0 + X_1 + \cdots + X_{k-1}$, where the X_j are independent random variables equally likely to be $+1$ or -1, then for any $\lambda > 0$, we have*

$$\mathbf{Pr}\big[\,|Y_k| > \lambda\big] < 2\exp(-\lambda^2/2k).$$

Proposition 3.5 appears as Theorem A.1.1 in Appendix A of [1], where it is credited to Chernoff. Despite its age, we include a proof, as it involves a particularly clever use of generating functions and Markov's inequality.

Proof of Proposition 3.5. Assume the hypotheses of the proposition, and observe that by symmetry, we have

$$\mathbf{Pr}\big[\,|Y_k| > \lambda\big] = 2 \cdot \mathbf{Pr}\big[Y_k > \lambda\big]. \tag{3.13}$$

Then note that for any positive number t, the event $Y_k > \lambda$ is equivalent to $tY_k > t\lambda$, which in turn is equivalent to $e^{tY_k} > e^{t\lambda}$. Now since e^{tY_k} is a nonnegative random variable, Markov's inequality (Proposition 1.39) gives

$$\mathbf{Pr}\big[e^{tY_k} > e^{t\lambda}\big] < \frac{\mathbf{E}(e^{tY_k})}{e^{\lambda t}}.$$

That is, we have shown that for all $t > 0$, we have

$$\mathbf{Pr}[Y_k > \lambda] < \frac{M_Y(t)}{e^{\lambda t}} \tag{3.14}$$

where $M_Y(t)$ is the moment-generating function of Y_k as defined in Definition 1.44. As observed in the proof of Theorem 3.2, we have

$$M_Y(t) = (\cosh t)^k.$$

We now observe that since

$$\cosh t = 1 + \frac{t^2}{1 \cdot 2} + \frac{t^4}{1 \cdot 2 \cdot 3 \cdot 4} + \frac{t^6}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} + \cdots$$

and also

$$\begin{aligned} \exp(t^2/2) &= 1 + \frac{t^2}{2} + \frac{1}{2!}\left(\frac{t^2}{2}\right)^2 + \frac{1}{3!}\left(\frac{t^2}{2}\right)^3 + \cdots \\ &= 1 + \frac{t^2}{2} + \frac{t^4}{2 \cdot 4} + \frac{t^6}{2 \cdot 4 \cdot 6} + \cdots, \end{aligned}$$

we have $\cosh t < \exp(t^2/2)$ for all $t > 0$, implying $(\cosh t)^k < \exp(kt^2/2)$. Together with (3.14), this gives us

$$\mathbf{Pr}[Y_k > \lambda] < \frac{e^{kt^2/2}}{e^{\lambda t}} = \exp\left(\frac{kt^2}{2} - \lambda t\right). \tag{3.15}$$

for all positive t. We now notice, using elementary calculus, that the positive t that minimizes the right side of (3.15) is $t = \lambda/k$. Substituting this value of t into (3.15) gives us

$$\mathbf{Pr}[Y_k > \lambda] < \exp\left(\frac{-\lambda^2}{2k}\right)$$

which, together with (3.13), completes the proof of the proposition. ∎

It is now a simple matter to establish the following refinement of Proposition 1.11.

Theorem 3.6 *For all $\varepsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that if $n > N$, then there exists a Littlewood polynomial in $\mathcal{L}_n$ that satisfies*

$$|c_k| \leq (\sqrt{2} + \varepsilon)\sqrt{n \log n} \tag{3.16}$$

for all $k \in \{1, 2, \ldots, n-1\}$.

Proof. Suppose $\varepsilon > 0$, and define

$$\lambda := (\sqrt{2} + \varepsilon)\sqrt{n \log n}.$$

A crude overestimate for the probability that $|c_k| > \lambda$ for some $k \in \{1, 2, \ldots, n-1\}$ is given by

$$\sum_{k=1}^{n-1} \mathbf{Pr}\big[\,|c_{n-k}| > \lambda\big] = \sum_{k=1}^{n-1} \mathbf{Pr}\big[\,|Y_k| > \lambda\big]$$

which, by Proposition 3.5, is bounded above by

$$\begin{aligned}
&\sum_{k=1}^{n-1} 2\exp(-\lambda^2/2k) \\
&< \sum_{k=1}^{n-1} 2\exp(-\lambda^2/2n) \\
&< 2n\exp(-\lambda^2/2n) \\
&= 2n\exp\big(-(2+\varepsilon')(n\log n)/2n\big) \\
&= 2n\exp\big(-(1+\varepsilon'')\log n\big) \\
&= 2/n^{\varepsilon''}
\end{aligned}$$

which is certainly less than 1 for n large enough. It follows that there exists $N \in \mathbb{Z}^+$ such that for all $n > N$, at least one Littlewood polynomial in $\mathcal{L}_n$ satisfies (3.16) for all $k \in \{1, 2, \ldots, n-1\}$, completing the proof of the theorem. ∎

We thus have more than one result giving upper bounds on Turyn's b function that, roughly speaking, are 'slightly greater' than $\sqrt{n}$. We close this section with some elaborations on the idea that we are 'close' to proving Conjecture 1.20 that $b(n) = O(\sqrt{n})$, and some informal reasons for the author's belief that someone will prove $b(n) = O(\sqrt{n})$ in the near future by using more subtle or sophisticated probabilistic techniques.

We observed that for all positive integers n, there exists a polynomial in $\mathcal{L}_n$ whose nontrivial autocorrelations are all bounded (in absolute value) by a multiple of $n^{6/10}$ (and remarked that similar bounds are possible with smaller exponents). Note that we showed the existence of such a polynomial by showing, essentially, that it suffices to choose any Littlewood polynomial such that the ℓ_{10} norm of the autocorrelation vector is merely 'better than average'. This suggests such polynomials are not 'rare' and that more sophisticated methods should be able to find ones that are 'even better'.

Notice also that in the proof of Theorem 3.6, we used the trivial fact that the probability of a union of events is bounded above by the sum of the probabilities of the events. This is typically a gross overestimate, unless the events in question are disjoint. In the case under consideration, the events are of the form $|c_k| > \lambda$, which are not disjoint. In fact, some authors such as Golay [20] have pointed out that one expects the autocorrelations c_k to enjoy some sort of 'near-independence' property. Turning this observation into precise mathematics may lead to further insight into the true growth rate of the functions $b(n)$ or $E_{\min}(n)$.

Chapter 4

Autocorrelation in $\mathcal{A}_n$

> The mathematician Simon Sidon was famed for his reclusive nature. One afternoon, Paul Erdős and another mathematician named Turán showed up on Sidon's doorstep unannounced. Sidon opened the door a crack and greeted his visitors with these words: 'Please visit another time—and especially another person.'
>
> `http://www.anecdotage.com` (original source unknown)

4.1 Average of c_k^2 over $\mathcal{A}_n$, $\mathcal{B}_n$, and $\mathcal{A}_{n,m}$

In this chapter, we are interested in norms of 'typical' zero-one polynomials. More precisely, we consider the average, or expected value, of the fourth power of the L_4 norm on $\mathbb{S}$ of a polynomial in $\mathcal{A}_n$, $\mathcal{B}_n$, or $\mathcal{A}_{n,m}$. Because of the relationship

$$\|\alpha\|_4^4 = c_0^2 + 2\,|C|_2^2 \tag{4.1}$$

indicated at the end of Section 1.2, this is more or less the same problem as finding the average or expected value of $|C|_2^2$ over the sets $\mathcal{A}_n$, $\mathcal{B}_n$, and $\mathcal{A}_{n,m}$.

As one might expect, we turn each of the three sets $\mathcal{A}_n$, $\mathcal{B}_n$, and $\mathcal{A}_{n,m}$ into (finite) probability spaces in much the same way as we did with $\mathcal{L}_n$ in Chapter 3: by using a probability mass function that assigns the same weight to each polynomial in the set.

That is, throughout this chapter our probability space will be (Ω, p), where either

$$\Omega = \mathcal{A}_n \text{ and } p(\alpha) = \frac{1}{2^n} \text{ for all } \alpha \in \Omega,$$
$$\Omega = \mathcal{B}_n \text{ and } p(\alpha) = \frac{1}{2^n} \text{ for all } \alpha \in \Omega, \text{ or}$$
$$\Omega = \mathcal{A}_{n,m} \text{ and } p(\alpha) = \frac{1}{\binom{n}{m}} \text{ for all } \alpha \in \Omega.$$

When considering the expected value of some random variable defined on one of these three spaces, we will sometimes use the notation $\mathbf{E}_{\mathcal{A}_n}$, $\mathbf{E}_{\mathcal{B}_n}$, or $\mathbf{E}_{\mathcal{A}_{n,m}}$ as appropriate, in order to make explicit which of the three sets of polynomials we are averaging over.

Recalling that $\mathcal{A}_n$ consists of all 2^n polynomials of the form

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}, \quad a_j \in \{0, 1\} \text{ for } 0 \leq j \leq n-1, \tag{4.2}$$

one can see that assigning equal weight to each such polynomial implies that the coefficients $a_0, \ldots, a_{n-1}$ form a collection of (mutually) independent random variables, as was the case with $\mathcal{L}_n$ in Chapter 3. This time, of course, the n coefficients are independent random variables equally likely to be 0 or 1. Similarly, we see that since $\mathcal{B}_n$ consists of the 2^n polynomials of the form

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} + z^n, \quad a_j \in \{0, 1\} \text{ for } 0 \leq j \leq n-1,$$

it follows that a_0 through a_{n-1} are independent random variables in that space as well. By contrast, since $\mathcal{A}_{n,m}$ consists of those polynomials of the form (4.2) such that precisely m of the a_j are 1, it follows that the a_j are not mutually independent in that probability space. (Informally, knowing one of the coefficients is 1 decreases the probability that any other coefficient is 1.)

Another subtlety worth mentioning at this point is that the autocorrelation c_0 has the same value m for all polynomials in $\mathcal{A}_{n,m}$, but has different values for different polynomials in $\mathcal{A}_n$ or $\mathcal{B}_n$.

The main result of this section, which also appears in the joint publication [5], is that one can find explicit expressions for $\mathbf{E}_\Omega(\|\alpha\|_4^4)$ if Ω is any of the three spaces $\mathcal{A}_n$, $\mathcal{B}_n$, or $\mathcal{A}_{n,m}$ equipped with the probability mass functions described above. To be

specific, if $m \le n$, we have

$$\mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) = \frac{4n^3+42n^2-4n+3-3(-1)^n}{96},$$
$$\mathbf{E}_{\mathcal{B}_n}(\|\alpha\|_4^4) = \frac{4n^3+66n^2+188n+87+9(-1)^n}{96}, \text{ and}$$
$$\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) = 2m^2-m+\frac{2m^{[4]}}{3(n-3)}+\frac{m^{[3]}(n-m)(2n^2-4n+1-(-1)^n)}{2n^{[4]}},$$

where the notation $x^{[k]}$ is shorthand for $x(x-1)\cdots(x-k+1)$. This complements results of Newman and Byrnes [38], who found the average of $\|\alpha\|_4^4$ over $\mathcal{L}_n$, and Borwein and Choi [4], who found (among other things) the average of $\|\alpha\|_6^6$ and $\|\alpha\|_8^8$ over $\mathcal{L}_n$, as well as the average of $\|\alpha\|_2^2$, $\|\alpha\|_4^4$, and $\|\alpha\|_6^6$ over the 3^n polynomials of the form

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1}z^{n-1}, \quad a_j \in \{+1, 0, -1\} \text{ for } 0 \le j \le n-1.$$

Because we have $\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) = \mathbf{E}_{\mathcal{A}_{n,m}}(c_0^2 + 2\,|C|_2^2) = m^2 + 2\mathbf{E}_{\mathcal{A}_{n,m}}(|C|_2^2)$, and because the autocorrelations of a polynomial in $\mathcal{A}_{n,m}$ have a combinatorial interpretation as mentioned in Section 1.2, it turns out that our expression for $\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4)$ leads to a surprising new proof of a known result about Sidon sets. This is explained in Section 4.2.

To obtain the results of this section, we begin by observing some facts about the squared autocorrelations of a polynomial $\alpha = \sum a_j z^j \in \mathcal{A}_n$. We have

$$\begin{aligned} c_k^2 &= \Big(\sum_{j=0}^{n-k-1} a_j a_{j+k}\Big)^2 \\ &= \sum_{i=0}^{n-k-1} a_i a_{i+k} \cdot \sum_{j=0}^{n-k-1} a_j a_{j+k} \\ &= \sum_{i=0}^{n-k-1}\sum_{j=0}^{n-k-1} a_i a_j a_{i+k} a_{j+k} \\ &= \sum_{i=0}^{n-k-1}\sum_{j=0}^{n-k-1} f(i,j) \quad \text{say.} \end{aligned}$$

Noting that $f(i,j) := a_i a_j a_{i+k} a_{j+k}$ satisfies $f(i,j) = f(j,i)$, we then have

$$\begin{aligned} c_k^2 &= \sum_{i=0}^{n-k-1} \sum_{j=0}^{n-k-1} f(i,j) \\ &= \sum_{i=0}^{n-k-1} f(i,i) + 2 \sum_{0 \le i < j \le n-k-1} f(i,j) \\ &= \sum_{i=0}^{n-k-1} a_i^2 a_{i+k}^2 + 2 \sum_{0 \le i < j \le n-k-1} a_i a_j a_{i+k} a_{j+k}. \end{aligned} \tag{4.3}$$

Now define $m := \alpha(1)$. Then $\alpha \in \mathcal{A}_{n,m}$, and we can write $\alpha = z^{\beta_1} + \cdots + z^{\beta_m}$ where $\beta_1 < \cdots < \beta_m$. Recalling from Section 1.2 that the c_k are nonnegative integers whose sum is $\binom{m}{2}$, we conclude that

$$c_1^2 + \cdots + c_{n-1}^2 \ge c_1 + \cdots + c_{n-1} = \frac{m(m-1)}{2}$$

with equality if and only if $c_k \in \{0,1\}$ for $1 \le k \le n-1$. Recalling that c_k is the number of times k appears as a difference $\beta_j - \beta_i$, we conclude that

$$|C|_2^2 - \binom{m}{2} = c_1^2 + \cdots + c_{n-1}^2 - \frac{m(m-1)}{2}$$

is a nonnegative integer, and is zero if and only if $\{\beta_1, \ldots, \beta_m\}$ is a Sidon set.

Now, suppose j_1, j_2, j_3, j_4 are distinct integers. Our next step is to calculate some averages of products of a_{j_i} that we will need later. First, if our probability space is $\mathcal{A}_n$, we have

$$\begin{aligned} \mathbf{E}_{\mathcal{A}_n}(a_{j_1} a_{j_2}) &= \frac{1}{2^n}(\text{number of } \alpha \in \mathcal{A}_n \text{ such that } a_{j_1} = a_{j_2} = 1) \\ &= \frac{2^{n-2}}{2^n} = \frac{1}{4}, \end{aligned} \tag{4.4}$$

and then by similar reasoning, we have

$$\left.\begin{aligned} \mathbf{E}_{\mathcal{A}_n}(a_{j_1} a_{j_2} a_{j_3}) &= 1/8, \\ \mathbf{E}_{\mathcal{A}_n}(a_{j_1} a_{j_2} a_{j_3} a_{j_4}) &= 1/16. \end{aligned}\right\} \tag{4.5}$$

On the other hand, if our probability space is $\mathcal{A}_{n,m}$, we have

$$\begin{aligned}\mathbf{E}_{\mathcal{A}_{n,m}}(a_{j_1}a_{j_2}) &= \frac{1}{\binom{n}{m}}(\text{number of } \alpha \in \mathcal{A}_{n,m} \text{ such that } a_{j_1} = a_{j_2} = 1) \\ &= \frac{\binom{n-2}{m-2}}{\binom{n}{m}} = \frac{m(m-1)}{n(n-1)} = \frac{m^{[2]}}{n^{[2]}},\end{aligned} \tag{4.6}$$

and then by similar reasoning, we have

$$\left.\begin{aligned}\mathbf{E}_{\mathcal{A}_{n,m}}(a_{j_1}a_{j_2}a_{j_3}) &= m^{[3]}/n^{[3]}, \\ \mathbf{E}_{\mathcal{A}_{n,m}}(a_{j_1}a_{j_2}a_{j_3}a_{j_4}) &= m^{[4]}/n^{[4]}.\end{aligned}\right\} \tag{4.7}$$

Now, whether Ω is $\mathcal{A}_n$ or $\mathcal{A}_{n,m}$, we have $a_j^2 = a_j$ for all j, so (4.3) implies

$$c_k^2 = \sum_{i=0}^{n-k-1} a_i a_{i+k} + 2 \sum_{0 \le i < j \le n-k-1} a_i a_{i+k} a_j a_{j+k}. \tag{4.8}$$

We define $\lambda := n - k$ and also define

$$S := \sum_{i=0}^{\lambda-1} a_i a_{i+k}, \tag{4.9}$$

$$T := \sum_{0 \le i < j \le \lambda-1} a_i a_j a_{i+k} a_{j+k}, \tag{4.10}$$

which of course implies

$$c_k^2 = S + 2T. \tag{4.11}$$

If $k = 0$, then $c_k^2 = m^2$. So if $\Omega = \mathcal{A}_{n,m}$, we have simply $\mathbf{E}(c_0^2) = m^2$, whereas if $\Omega = \mathcal{A}_n$, we have

$$\mathbf{E}(c_0^2) = \sum_{m=0}^{n} \frac{\binom{n}{m}}{2^n} m^2. \tag{4.12}$$

It is a short exercise to see that the right side of (4.12) evaluates to $(n^2 + n)/4$. Alternatively, we may observe that c_0 has a binomial distribution with parameters n and $1/2$, which implies

$$\mathbf{E}(c_0^2) = \mathbf{Var}(c_0) + \mathbf{E}(c_0)^2 = n \cdot \frac{1}{2} \cdot \frac{1}{2} + \left(n \cdot \frac{1}{2}\right)^2 = \frac{n^2 + n}{4}. \tag{4.13}$$

Having found $\mathbf{E}(c_0^2)$ for $\Omega = \mathcal{A}_{n,m}$ and for $\Omega = \mathcal{A}_n$, we now shift our attention to $\mathbf{E}(c_k^2)$ for $k \neq 0$.

Assume $k \neq 0$, and observe that equations (4.8) through (4.11) (and linearity of expectation) give us

$$\mathbf{E}(c_k^2) = \mathbf{E}(S) + 2\mathbf{E}(T) = \sum_{i=0}^{\lambda-1} \mathbf{E}(a_i a_{i+k}) + 2 \sum_{0 \leq i < j \leq \lambda-1} \mathbf{E}(a_i a_j a_{i+k} a_{j+k}). \tag{4.14}$$

Since $k \neq 0$, each of the λ terms in the sum $\mathbf{E}(S)$ is of the form $\mathbf{E}(a_{j_1} a_{j_2})$ where $j_1 \neq j_2$. We thus have

$$\mathbf{E}(S) = \begin{cases} \lambda/4 & \text{if } \Omega = \mathcal{A}_n, \\ \lambda m^{[2]}/n^{[2]} & \text{if } \Omega = \mathcal{A}_{n,m}. \end{cases} \tag{4.15}$$

by (4.4) and (4.6).

As for the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$, each term is of the form $\mathbf{E}(a_i a_j a_{i+k} a_{j+k})$. Since $k \neq 0$ and $i < j$, the four subscripts $i, j, i+k, j+k$ constitute either three distinct integers (if $j = i+k$) or four distinct integers (if $j \neq i+k$). If $\{i, j, i+k, j+k\}$ consists of three distinct integers j_1, j_2, j_3 where j_3 is the one that is 'repeated', then, since $a_j \in \{0, 1\}$ for all j, we have $\mathbf{E}(a_i a_j a_{i+k} a_{j+k}) = \mathbf{E}(a_{j_1} a_{j_2} a_{j_3}^2) = \mathbf{E}(a_{j_1} a_{j_2} a_{j_3})$, whereas of course if $\{i, j, i+k, j+k\}$ consists of four distinct integers, then $\mathbf{E}(a_i a_j a_{i+k} a_{j+k})$ is of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4})$. Therefore, we now ask the question: For which of the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$ does the set $\{i, j, i+k, j+k\}$ consist of only three distinct integers?

For some $i \in \{0, 1, \ldots, \lambda - 1\}$, there is exactly one j satisfying both $i < j \leq \lambda - 1$ and $j = i + k$, and for other values of i, there is no such j. We will say that i is of 'type I' if the former criterion holds, and is of 'type II' if the latter criterion holds. An integer i is of type I if and only if $i + k < \lambda$, or equivalently, $i < \lambda - k = n - 2k$. If $n - 2k \leq 0$ (i.e. if $k \geq \lceil n/2 \rceil$), then $i < n - 2k$ never happens, i.e. no i is of type I and so all of the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$ are of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4})$. On the other hand, if $n - 2k > 0$ (i.e. if $k < \lceil n/2 \rceil$), then $i < n - 2k = \lambda - k$ sometimes happens; namely, it happens if and only if i is one of the $\lambda - k$ integers $0, 1, \ldots, \lambda - k - 1$. In that case, each of those $\lambda - k$ values of i is of type I. This implies that precisely $\lambda - k$ of the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$ are of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3})$ and the remaining terms are of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4})$.

It follows that we have

$$\mathbf{E}(T) = \begin{cases} \binom{\lambda}{2}\mathbf{E}(a_{j_1}a_{j_2}a_{j_3}a_{j_4}) & \text{if } k \geq \lceil n/2 \rceil, \\ \binom{\lambda}{2}\mathbf{E}(a_{j_1}a_{j_2}a_{j_3}a_{j_4}) + (\lambda - k)\big[\mathbf{E}(a_{j_1}a_{j_2}a_{j_3}) - \mathbf{E}(a_{j_1}a_{j_2}a_{j_3}a_{j_4})\big] & \text{if } k < \lceil n/2 \rceil. \end{cases}$$

Thus, for $\Omega = \mathcal{A}_n$ we have

$$\mathbf{E}_{\mathcal{A}_n}(T) = \begin{cases} \binom{\lambda}{2}/16 & \text{if } k \geq \lceil n/2 \rceil, \\ \binom{\lambda}{2}/16 + (\lambda - k)/16 & \text{if } k < \lceil n/2 \rceil, \end{cases}$$

and hence, using (4.14) and (4.15), we get

$$\mathbf{E}_{\mathcal{A}_n}(c_k^2) = \begin{cases} \lambda/4 + \lambda(\lambda - 1)/16 & \text{if } k \geq \lceil n/2 \rceil, \\ \lambda/4 + \lambda(\lambda - 1)/16 + 2(\lambda - k)/16 & \text{if } k < \lceil n/2 \rceil. \end{cases}$$

On the other hand, for $\Omega = \mathcal{A}_{n,m}$ we have

$$\mathbf{E}_{\mathcal{A}_{n,m}}(T) = \begin{cases} \binom{\lambda}{2} m^{[4]}/n^{[4]} & \text{if } k \geq \lceil n/2 \rceil, \\ \binom{\lambda}{2} m^{[4]}/n^{[4]} + (\lambda - k)[m^{[3]}/n^{[3]} - m^{[4]}/n^{[4]}] & \text{if } k < \lceil n/2 \rceil, \end{cases}$$

and hence, using (4.14) and (4.15), we get

$$\mathbf{E}_{\mathcal{A}_{n,m}}(c_k^2) = \begin{cases} \lambda \frac{m^{[2]}}{n^{[2]}} + \lambda(\lambda - 1)\frac{m^{[4]}}{n^{[4]}} & \text{if } k \geq \lceil n/2 \rceil, \\ \lambda \frac{m^{[2]}}{n^{[2]}} + \lambda(\lambda - 1)\frac{m^{[4]}}{n^{[4]}} + 2(\lambda - k)\Big[\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\Big] & \text{if } k < \lceil n/2 \rceil. \end{cases}$$

As for the average of $|C|_2^2 = c_1^2 + \cdots + c_{n-1}^2$ over $\mathcal{A}_n$ or $\mathcal{A}_{n,m}$, we then have

$$\mathbf{E}_{\mathcal{A}_n}(|C|_2^2) = \sum_{k=1}^{n-1}\Big(\frac{\lambda}{4}\Big) + \sum_{k=1}^{n-1}\Big(\frac{\lambda(\lambda-1)}{16}\Big) + \sum_{k=1}^{\lceil n/2\rceil - 1}\Big(\frac{2(\lambda-k)}{16}\Big) \tag{4.16}$$

and

$$\mathbf{E}_{\mathcal{A}_{n,m}}(|C|_2^2) = \sum_{k=1}^{n-1}\Big(\lambda\frac{m^{[2]}}{n^{[2]}}\Big) + \sum_{k=1}^{n-1}\Big(\lambda(\lambda-1)\frac{m^{[4]}}{n^{[4]}}\Big) + \sum_{k=1}^{\lceil n/2\rceil - 1}\Big(2(\lambda-k)\Big[\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\Big]\Big). \tag{4.17}$$

Recalling that λ is simply shorthand for $n - k$, it is straightforward to verify that

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

$$\sum_{k=1}^{n-1}(\lambda^2 - \lambda) = \frac{n(n-1)(n-2)}{3},$$

and that

$$\sum_{k=1}^{\lceil n/2 \rceil - 1} 2(\lambda - k) = \begin{cases} n(n-2)/2 & n \text{ even}, \\ (n-1)^2/2 & n \text{ odd}. \end{cases}$$

This means that from (4.16), we get $\mathbf{E}_{\mathcal{A}_n}(|C|_2^2)$

$$= \begin{cases} \frac{1}{4} \cdot \frac{n(n-1)}{2} + \frac{1}{16} \cdot \frac{n(n-1)(n-2)}{3} + \frac{1}{16} \cdot \frac{n(n-2)}{2} & n \text{ even}, \\ \frac{1}{4} \cdot \frac{n(n-1)}{2} + \frac{1}{16} \cdot \frac{n(n-1)(n-2)}{3} + \frac{1}{16} \cdot \frac{(n-1)^2}{2} & n \text{ odd}, \end{cases}$$

$$= \begin{cases} (2n^3 + 9n^2 - 14n)/96 & n \text{ even}, \\ (2n^3 + 9n^2 - 14n + 3)/96 & n \text{ odd}, \end{cases}$$

which, using (4.1) and (4.13), implies

$$\mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) = \begin{cases} \frac{n^2+n}{4} + \frac{2n^3+9n^2-14n}{48} = \frac{2n^3+21n^2-2n}{48} & n \text{ even}, \\ \frac{n^2+n}{4} + \frac{2n^3+9n^2-14n+3}{48} = \frac{2n^3+21n^2-2n+3}{48} & n \text{ odd}, \end{cases}$$

or equivalently,

$$\mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) = \frac{4n^3 + 42n^2 - 4n + 3 - 3(-1)^n}{96}. \tag{4.18}$$

On the other hand, from (4.17), we get $\mathbf{E}_{\mathcal{A}_{n,m}}(|C|_2^2)$

$$= \begin{cases} \frac{m^{[2]}}{n^{[2]}} \cdot \frac{n(n-1)}{2} + \frac{m^{[4]}}{n^{[4]}} \cdot \frac{n(n-1)(n-2)}{3} + \left(\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\right) \cdot \frac{n(n-2)}{2} & n \text{ even}, \\ \frac{m^{[2]}}{n^{[2]}} \cdot \frac{n(n-1)}{2} + \frac{m^{[4]}}{n^{[4]}} \cdot \frac{n(n-1)(n-2)}{3} + \left(\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\right) \cdot \frac{(n-1)^2}{2} & n \text{ odd}, \end{cases}$$

$$= \left\{ \begin{array}{ll} \binom{m}{2} + m^{[4]}/(3(n-3)) + m^{[3]}(n-m)(n^2-2n)/(2n^{[4]}) & n \text{ even}, \\ \binom{m}{2} + m^{[4]}/(3(n-3)) + m^{[3]}(n-m)(n^2-2n+1)/(2n^{[4]}) & n \text{ odd}, \end{array} \right\} \tag{4.19}$$

which, using (4.1), implies

$$\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) = \begin{cases} 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n)}{n^{[4]}} & n \text{ even}, \\ 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n+1)}{n^{[4]}} & n \text{ odd}, \end{cases}$$

or equivalently,

$$\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) = 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(2n^2-4n+1-(-1)^n)}{2n^{[4]}}. \tag{4.20}$$

Note that if we fix m and let n approach infinity, $\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4)$ approaches $2m^2 - m$, or equivalently, $\mathbf{E}_{\mathcal{A}_{n,m}}(|C|_2^2)$ approaches $m(m-1)/2$. Informally paraphrased, this

says that for fixed m and large n, we 'expect' a random $\alpha \in \mathcal{A}_{n,m}$ to correspond to a Sidon set, as is consistent with intuition.

If $\Omega = \mathcal{B}_n$, then since $\mathcal{B}_n := \mathcal{A}_{n+1} \setminus \mathcal{A}_n$, we get

$$\begin{aligned}\mathbf{E}_{\mathcal{B}_n}(\|\alpha\|_4^4) &= \frac{1}{2^n}\sum_{\alpha\in\mathcal{B}_n}\|\alpha\|_4^4 \\ &= 2\mathbf{E}_{\mathcal{A}_{n+1}}(\|\alpha\|_4^4) - \mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) \\ &= \frac{4n^3+66n^2+188n+87+9(-1)^n}{96}\end{aligned}$$

by (4.18). This completes the proof of the following.

Theorem 4.1 *For $m \le n$, we have*

$$\begin{aligned}\mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) &= \frac{4n^3+42n^2-4n+3-3(-1)^n}{96}, \\ \mathbf{E}_{\mathcal{B}_n}(\|\alpha\|_4^4) &= \frac{4n^3+66n^2+188n+87+9(-1)^n}{96}, \text{ and} \\ \mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) &= 2m^2-m+\frac{2m^{[4]}}{3(n-3)}+\frac{m^{[3]}(n-m)(2n^2-4n+1-(-1)^n)}{2n^{[4]}}.\end{aligned}$$

4.2 Ubiquity of Sidon sets

In the last section of this thesis, we show that our expression for $\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4)$, or equivalently, our expression for $\mathbf{E}_{\mathcal{A}_{n,m}}(|C|_2^2)$, yields a surprising new proof of a result that appears in articles by Godbole et al. [18] and Nathanson [37].

Suppose that $\Omega = \mathcal{A}_{n,m}$, and as before, denote a typical element of $\mathcal{A}_{n,m}$ by

$$\alpha(z) = z^{\beta_1} + z^{\beta_2} + \cdots + z^{\beta_m}.$$

Recall from the previous section that

$$X := |C|_2^2 - \binom{m}{2} = c_1^2 + \cdots + c_{n-1}^2 - \frac{m(m-1)}{2}$$

is a nonnegative integer-valued random variable on Ω, and attains the value 0 if and only if $\{\beta_1, \ldots, \beta_m\}$ is a Sidon set.

We have, using (4.19),

$$\begin{aligned}
\mathbf{E}_{\mathcal{A}_{n,m}}(X) &= \mathbf{E}_{\mathcal{A}_{n,m}}(|C|_2^2) - \binom{m}{2} \\
&= \begin{cases} \frac{m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n)}{2n^{[4]}} & \text{if } n \text{ is even,} \\ \frac{m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n+1)}{2n^{[4]}} & \text{if } n \text{ is odd.} \end{cases} \\
&\leq \frac{m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n-1)^2}{2n^{[4]}} \\
&= \frac{m(m-1)(m-2)(2mn-3n-m)}{6n(n-2)} \\
&\leq \frac{m(m-1)(m-2)(2mn-3m-m)}{6n(n-2)} \\
&= \frac{m(m-1)(m-2)2m(n-2)}{6n(n-2)} \\
&\leq \frac{m^4}{3n}
\end{aligned}$$

if $m \leq n$. Then, using Markov's inequality (Proposition 1.39), we have

$$\mathbf{Pr}[X \geq 1] \leq \frac{\mathbf{E}(X)}{1} \leq \frac{m^4}{3n},$$

which implies that

$$\mathbf{Pr}\big[\{\beta_1, \ldots, \beta_m\} \text{ is Sidon}\big] > 1 - \frac{m^4}{3n}.$$

If m is a function of n growing 'faster' than $n^{1/4}$, then this has the uninteresting consequence that a probability is bounded below by a negative number. However, if $m = o(n^{1/4})$, we get the following.

Corollary 4.2 *If $m = o(n^{1/4})$, then as n approaches infinity, the probability that a randomly chosen m-subset of $[n]$ is Sidon approaches* 1.

Here we are using the common convention that 'm-subset' just means 'subset of size m'.

Recall from Section 1.4 that a $B_h[g]$ set is a set A of nonnegative integers such that each $n \in \mathbb{Z}$ can be expressed in at most g ways as a sum of h (not necessarily distinct) elements of A, and hence a Sidon set is the same thing as a $B_2[1]$ set. Nathanson [37]

showed that if $m = o(n^{g/(2g+2)})$, then the probability that a randomly chosen m-subset of $[n]$ is a $B_2[g]$ set approaches 1 as n approaches infinity. (The present author got the idea to use the term 'ubiquity' from Nathanson's paper.) Godbole et al. [18] showed that if $m = o(n^{1/2h})$, then the probability that a randomly chosen m-subset of $[n]$ is a $B_h[1]$ set approaches 1 as n approaches infinity. They further showed that $m = o(n^{1/2h})$ is a 'sharp threshold' in the sense that if $m \gg n^{1/2h}$, then the probability that a randomly chosen m-subset of $[n]$ is a $B_h[1]$ set approaches 0 as n approaches infinity.

Thus Corollary 4.2 is known, but it is perhaps surprising that we get to deduce it for 'free' as a consequence of finding the 'typical' L_4 norm on $\mathbb{S}$ of a zero-one polynomial.

Bibliography

[1] N. Alon & J. H. Spencer, *The Probabilistic Method* (2nd edition), Wiley, New York, 2000.

[2] B. Bollobás, *Graph Theory*, Springer-Verlag, New York, 1979.

[3] P. B. Borwein, *Computational Excursions in Analysis and Number Theory*, Springer-Verlag, New York, 2002.

[4] P. B. Borwein & K.-K. S. Choi, *The average norm of polynomials of fixed height*, to appear in Trans. Amer. Math. Soc.

[5] P. B. Borwein, K.-K. S. Choi & I. D. Mercer, *Expected norms of zero-one polynomials*, submitted to Math. Proc. Cambridge Philos. Soc.

[6] R. L. Burden & J. D. Faires, *Numerical Analysis* (5th edition), PWS-Kent, Boston, 1993.

[7] F. W. Carroll, D. Eustice & T. Figiel, *The minimum modulus of polynomials with coefficients of modulus one*, J. London Math. Soc. **16** (1977), 76–82.

[8] J. Clunie, *The minimum modulus of a polynomial on the unit circle*, Quart. J. Math. Oxford Ser. 2, **10** (1959), 95–98.

[9] M. N. Cohen, M. R. Fox & J. M. Baden, *Minimum peak sidelobe compression codes*, in *IEEE International Radar Conference* (IEEE, 1990), 633–638.

[10] G. E. Coxson, A. Hirschel & M. N. Cohen, *New results on minimum-PSL binary codes*, in *IEEE Radar Conference* (IEEE, 2001), 153–156.

[11] T. Erdélyi, *On the zeros of polynomials with Littlewood-type coefficient constraints*, Michigan Math. J. **49** (2001), 97–111.

[12] P. Erdős, *Some unsolved problems*, Michigan Math. J. **4** (1957), 291–300.

[13] P. Erdős, *An inequality for the maximum of trigonometric polynomials*, Ann. Polon. Math. **12** (1962), 151–154.

[14] P. Erdős & P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215.

[15] P. Fan & M. Darnell, *Sequence Design for Communications Applications*, Research Studies Press, Taunton, UK, 1996.

[16] J. E. Freund, *Mathematical Statistics* (5th edition), Prentice Hall, Englewood Cliffs, NJ, 1992.

[17] A. D. Gilbert & C. J. Smyth, *Zero-mean cosine polynomials which are non-negative for as long as possible*, J. London Math. Soc. (2) **62** (2000), 489–504.

[18] A. P. Godbole, S. Janson, N. W. Locantore Jr. & R. Rapoport, *Random Sidon sequences*, J. Number Theory **75** (1999), 7–22.

[19] M. J. Golay, *A class of finite binary sequences with alternate autocorrelation values equal to zero*, IEEE Trans. Inform. Theory **18** (1972), 449–450.

[20] M. J. Golay, *Sieves for low autocorrelation binary sequences*, IEEE Trans. Inform. Theory **23** (1977), 43–51.

[21] R. K. Guy, *Unsolved Problems in Number Theory* (2nd edition), Springer-Verlag, New York, 1994.

[22] U. Haagerup, *The best constants in the Khintchine inequality*, Studia Math. **70** (1981), 231–283.

[23] H. Halberstam & K. F. Roth, *Sequences* (2nd edition), Springer-Verlag, New York, 1983.

[24] P. Hein, *Grooks 3*, Doubleday, Garden City, NY, 1970.

[25] A. E. Housman, *A Shropshire Lad*, Richards Press, London, 1956.

[26] N. L. Johnson, S. Kotz & A. W. Kemp, *Univariate Discrete Distributions*, Wiley, New York, 1992.

[27] J. Konvalina & V. Matache, *Palindrome-polynomials with roots on the unit circle*, C. R. Math. Acad. Sci. Soc. R. Can. **26** (2004), 39–44.

[28] S. G. Krantz, *Handbook of Complex Variables*, Birkhäuser, Boston, 1999.

[29] B. Lindström, *An inequality for B_2-sequences*, J. Combinatorial Theory **6** (1969), 211–212.

[30] J. E. Littlewood, *Some Problems in Real and Complex Analysis*, D. C. Heath & Co., Lexington, MA, 1968.

[31] I. D. Mercer, *Unimodular roots of special Littlewood polynomials*, to appear in Canad. Math. Bull.

[32] I. D. Mercer, *Autocorrelations of random binary sequences*, submitted to Combin. Probab. Comput.

[33] S. Mertens, *Exhaustive search for low-autocorrelation binary sequences*, J. Phys. A **29** (1996), L473–L481.

[34] S. Mertens, WWW research page on low autocorrelated binary sequences, `http://wase.urz.uni-magdeburg.de/mertens/research` [March 2005]

[35] M. Molloy & B. Reed, *Graph Colouring and the Probabilistic Method*, Springer-Verlag, Berlin, 2002.

[36] J. W. Moon & L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), 340–343.

[37] M. B. Nathanson, *On the ubiquity of Sidon sets*, in *Number Theory: New York Seminar 2003*, ed. D. Chudnovsky et al. (Springer-Verlag, New York, 2004), 263–272.

[38] D. J. Newman & J. S. Byrnes, *The L_4 norm of a polynomial with coefficients ± 1*, Amer. Math. Monthly **97** (1990), 42–45.

[39] M. Petkovšek, H. S. Wilf & D. Zeilberger, *$A=B$*, A. K. Peters, Wellesley, MA, 1996.

[40] G. Pólya & G. Szegö, *Problems and Theorems in Analysis*, Volume II, Springer-Verlag, New York, 1976.

[41] L. Robinson, *Polynomials with plus or minus one coefficients: Growth properties on the unit circle*, M.Sc. thesis, Simon Fraser University, 1997.

[42] V. Romanovsky, *Note on the moments of a binomial $(p+q)^n$ about its mean*, Biometrika **15** (1923), 410–412.

[43] B. Saffari, *Barker sequences and Littlewood's "two-sided" conjectures on polynomials with ± 1 coefficients*, in *Séminaire d'Analyse Harmonique, Année 1989/90* (Univ. Paris XI, Orsay, 1990), 139–151.

[44] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), 929–952.

[45] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.

[46] J. Spencer, *Six standard deviations suffice*, Trans. Amer. Math. Soc. **289** (1985), 679–706.

[47] R. J. Turyn, *Sequences with small correlation*, in *Error Correcting Codes: Proceedings of a Symposium*, ed. H. B. Mann (Wiley, New York, 1968), 195–228.

[48] R. J. Turyn & J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.