Preface

This book is designed for a topics course in computational number theory. It is based around a number of difficult old problems that live at the interface of analysis and number theory. Some of these problems are the following:

The Integer Chebyshev Problem. *Find a nonzero polynomial of degree n with integer coefficients that has smallest possible supremum norm on the unit interval.*

Littlewood's Problem. *Find a polynomial of degree n with coefficients in the set $\{+1, -1\}$ that has smallest possible supremum norm on the unit disk.*

The Prouhet–Tarry–Escott Problem. *Find a polynomial with integer coefficients that is divisible by $(z-1)^n$ and has smallest possible l_1 norm. (That is, the sum of the absolute values of the coefficients is minimal.)*

Lehmer's Problem. *Show that any monic polynomial p, $p(0) \neq 0$, with integer coefficients that is irreducible and that is not a cyclotomic polynomial has Mahler measure at least* $1.1762\ldots$.

All of the above problems are at least forty years old; all are presumably very hard, certainly none are completely solved; and all lend themselves to extensive computational explorations.

The techniques for tackling these problems are various and include probabilistic methods, combinatorial methods, "the circle method," and Diophantine and analytic techniques. Computationally, the main tool is the LLL algorithm for finding small vectors in a lattice.

The book is intended as an introduction to a diverse collection of techniques. For all chapters we have suggested related research papers where additional details may be pursued. There are many exercises and open research problems included. Indeed, the primary aim of the book is to tempt the able reader into the rich open possibilities for research in this area.

I would particularly like to thank Stephen Choi for Appendix C, Kevin Hare for Chapter 16, and Alan Meichsner for Appendix B as well as many general comments. I would also like to thank Ron Ferguson, Jonathan Jedwab, Vishaal Kapoor, Samantha McCollum, Idris Mercer, and Chris Smyth for their generous assistance.

Contents

Chapter 1

Introduction

This book focuses on a variety of old problems in number theory and analysis. The problems concern polynomials with integer coefficients and typically ask something about the size of the polynomial with an appropriate measure of size and often with some restriction on the height and the degree.

So, for example, we might seek to minimize the supremum norm of a polynomial with integer coefficients of degree n on the unit interval. Or we might try to minimize the supremum norm on the unit disk of a polynomial all of whose coefficients are either 1 or -1. Both of these are "old plums." The first is due to Hilbert, and the second is due to Littlewood. Both problems arise in various contexts. The first gives easy Chebyshev estimates on the density of primes. (See E3.) The second arises in signal processing.

As is typical of these and the other problems we consider, the objects of study are very familiar. The problems are, by and large, easy to formulate, and while none have been completely solved, all have had significant progress made on them.

The tools of attack are diverse and include Diophantine, analytic, and probabilistic methods. The problems lend themselves to extensive computational exploration, and this is one of the unifying threads of this work.

No attempt is made to discuss the material in great generality; indeed, some effort is made to choose accessible special cases. Another unifying theme is that all the problems can be reformulated as problems about polynomials with integer coefficients, even though they often arise in other contexts.

Notation

The principal classes of polynomials we consider are $\mathcal{Z}_n$, $\mathcal{F}_n$, and $\mathcal{L}_n$ which we now define.

Let

$$\mathcal{Z}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \mathbb{Z} \right\}$$

denote the set of algebraic polynomials of degree at most n with integer coefficients and let $\mathcal{Z}$ denote the union over n of all such polynomials. Throughout this book polynomials will be assumed to be in $\mathcal{Z}$ unless otherwise specified. The set $\mathcal{Z}$ is more usually denoted by $\mathbb{Z}[z]$. However, $\mathbb{Z}_p[z]$ (the polynomials with integer coefficients modulo p) is not the same as $\mathcal{Z}_p$ (where p is the degree), and thus the notational distinction.

Let

$$\mathcal{F}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \{-1, 0, 1\} \right\}$$

denote the set of polynomials of degree at most n with coefficients from the set $\{-1, 0, 1\}$. These are the polynomials of height 1 and degree at most n. Here and throughout the book, the *height* of a polynomial p is the magnitude of the largest coefficient and is often denoted by $H(p)$. Consistent with the above notation, $\mathcal{F}$ is the set of all height 1 polynomials.

Let

$$\mathcal{L}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \{-1, 1\} \right\}$$

denote the set of polynomials of degree exactly n with coefficients from $\{-1, 1\}$. In general, we will call polynomials with coefficients in $\{-1, 1\}$ *Littlewood polynomials* and denote the set of all such polynomials by $\mathcal{L}$.

Occasionally we will also consider

$$\mathcal{A}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \{0, 1\} \right\},$$

the set of polynomials of degree at most n with coefficients from $\{0, 1\}$, and will denote by $\mathcal{A}$ the union of all the $\mathcal{A}_n$.

Finally, let

$$\mathcal{P}_n^c := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \mathbb{C} \right\}$$

denote the set of polynomials of degree at most n with complex coefficients and let

$$\mathcal{P}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \mathbb{R} \right\}$$

denote the set of polynomials of degree at most n with real coefficients.

So obviously,

$$\mathcal{L}_n, \mathcal{A}_n \subset \mathcal{F}_n \subset \mathcal{Z}_n \subset \mathcal{P}_n \subset \mathcal{P}_n^c.$$

The open unit disk in the complex plane is denoted by D. A general open disk with radius r and centre z_0 is denoted by $D(z_0, r)$.

We now define the norms that we consider. The definitions are given for polynomials but hold generally for appropriately integrable or measurable functions. The *supremum norm*, or L_∞ norm, of a polynomial p on a set A is denoted by $\|\cdot\|_A$. It is defined as

$$\|p\|_A := \sup_{z\in A} |p(z)|.$$

For positive α, the L_α norm on the boundary of the unit disk is defined by

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

For a polynomial $p(z) := a_n z^n + \cdots + a_1 z + a_0$, the L_2 norm on D is also given by

$$\|p\|_2 = \sqrt{|a_n|^2 + \cdots + |a_1|^2 + |a_0|^2}.$$

This is a consequence of the fact that the Fourier transform is an isometry on the boundary of D, though for a polynomial it is also just a direct calculation.

In the two interesting limiting cases we get

$$\lim_{\alpha\to\infty} \|p\|_\alpha = \|p\|_D =: \|p\|_\infty$$

and

$$\lim_{\alpha\to 0} \|p\|_\alpha = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left|p\left(e^{i\theta}\right)\right| d\theta\right) =: \|p\|_0.$$

This latter quantity is called the *Mahler measure* and is denoted by $M(p)$. For a polynomial

$$p_n(z) := a(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)$$

it is, by Jensen's theorem, the product of all the roots of p that have modulus at least 1 multiplied by the leading coefficient. That is,

$$M(p_n) = |a| \prod_{|\alpha_i|\geq 1} |\alpha_i|.$$

Observe that the Mahler measure is multiplicative: $M(pq) = M(p)M(q)$. The Mahler measure of an algebraic number α, denoted by $M(\alpha)$, is, by convention, the Mahler measure of the minimal polynomial for α.

Note that L_α is a true norm only for $\alpha \geq 1$ (for $\alpha < 1$ the triangle inequality fails).

It is useful to define two other quantities associated with polynomials. As above, the *height* of a polynomial p, denoted by $H(p)$, is just the size of the largest coefficient of p. The *length* is denoted by $L(p)$ and is just the sum of the absolute values of the coefficients of p. If $p(z) := a_n z^n + \cdots + a_1 z + a_0$, then

$$L(p) := |a_n| + \cdots + |a_1| + |a_0|$$

and

$$H(p) := \max\{|a_n|, \ldots, |a_1|, |a_0|\}.$$

The length is also the l_1 norm: $L(p) = \|p\|_{l_1}$.

Some Results from Real and Complex Analysis

The following standard results about norms are useful. (See also Appendix A.) The $\|\cdot\|_\alpha$ norms are monotonic in α. For $0 \le \alpha \le \beta$,

$$\|f\|_\alpha \le \|f\|_\beta.$$

In fact, the norm $\|f\|_\alpha$ is a convex function of α. If $0 < r < s < t$, then

$$\|f\|_s^s \le (\|f\|_r^r)^{\frac{t-s}{t-r}} (\|f\|_t^t)^{\frac{s-r}{t-r}}.$$

We also have *Hölder's inequality*: if $1 \le \alpha < \beta \le \infty$ and $\alpha^{-1} + \beta^{-1} = 1$, then

$$\|fg\|_1 \le \|f\|_\alpha \|g\|_\beta.$$

For completeness we also state Cauchy's integral formula, Rouché's theorem, and Jensen's theorem. These are the principal tools from complex analysis that we need.

Cauchy's Integral Formula. *Let γ be a simple closed curve in the complex plane. Suppose f is analytic in the interior of the region bounded by γ and continuous on γ. Then for z interior to γ,*

$$0 = \int_\gamma f(t)\, dt,$$

$$f(z) = \frac{1}{2\pi i} \int_\gamma \frac{f(t)}{t-z}\, dt,$$

and

$$f^{(n)}(z) = \frac{n!}{2\pi i} \int_\gamma \frac{f(t)}{(t-z)^{n+1}}\, dt.$$

Unless otherwise specified, the integration on a simple closed curve is taken anticlockwise. In most of our applications γ is a circle.

Rouché's Theorem. *Suppose f and g are analytic inside and on a simple closed curve γ. If*

$$|f(z) - g(z)| < |f(z)|$$

for every $z \in \gamma$, then f and g have the same number of zeros inside γ (counting multiplicities).

Jensen's Theorem. *Suppose h is a nonnegative integer and*

$$f(z) = \sum_{k=h}^{\infty} c_k (z - z_0)^k, \quad c_h \neq 0,$$

is analytic on the closure of the disk $D(z_0, r)$. Suppose that the zeros of f in $D(z_0, r) \setminus \{z_0\}$ are $a_1, a_2, \dots, a_m$, where each zero is listed according to its multiplicity. Then

$$\log |c_h| + h \log r + \sum_{k=1}^{m} \log \frac{r}{|a_k - z_0|} = \frac{1}{2\pi} \int_0^{2\pi} \log \left| f\left(z_0 + re^{i\theta}\right)\right| \, d\theta.$$

The results of this section may all be found in Rudin [1987].

The Main Open Problems

We now state the principal problems we consider in later chapters, where we give a more motivated discussion of how each problem arises. Where possible, the problems are stated as "norm problems" whether or not this is how they naturally arise. Most of these problems have resisted solution for at least fifty years.

P1. The Integer Chebyshev Problem. *Find a nonzero polynomial in $\mathcal{Z}_n$ that has smallest possible supremum norm on the unit interval. Analyze the asymptotic behaviour as n tends to infinity.*

P2. The Prouhet–Tarry–Escott Problem. *Find a polynomial with integer coefficients that is divisible by $(z-1)^n$ and has smallest possible length. (That is, minimize the sum of the absolute values of the coefficients.)*

P3. The Erdős–Szekeres Problem. *For each n, minimize*

$$\|(1 - z^{\alpha_1})(1 - z^{\alpha_2}) \cdots (1 - z^{\alpha_n})\|_\infty ,$$

where the α_i are positive integers. In particular, show that these minima grow faster than n^β for any positive constant β.

P4. Littlewood's Problem in L_∞. *Find a polynomial in $\mathcal{L}_n$ that has smallest possible supremum norm on the unit disk. Show that there exist positive constants c_1 and c_2 such that for any n it is possible to find $p_n \in \mathcal{L}_n$ with*

$$c_1 \sqrt{n+1} \leq |p_n(z)| \leq c_2 \sqrt{n+1}$$

for all complex z with $|z| = 1$.

P5. Erdős's Problem in L_∞. *Show that there exists a positive constant c_3 such that for all sufficiently large n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \ge (1+c_3)\sqrt{n+1}$.*

P6. Erdős's Problem in L_∞ for Reciprocal Polynomials. *Show that there exists a positive constant c_3' such that for all sufficiently large n and all reciprocal polynomials $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \ge \left(\sqrt{2}+c_3'\right)\sqrt{n+1}$.*

P7. The Merit Factor Problem of Golay. *Find a polynomial in $\mathcal{L}_n$ that has smallest possible L_4 norm on the unit disk. Show that there exists a positive constant c_4 such that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_4 \ge (1+c_4)\sqrt{n+1}$.*

P8. The Barker Polynomial Problem. *For n sufficiently large ($n > 12$ may suffice) and $p_n \in \mathcal{L}_n$, show that*

$$\|p_n\|_4 > \left((n+1)^2 + n + 1\right)^{1/4}.$$

Equivalently, show that no polynomial in $\mathcal{L}_n$ of degree greater than 12 can have all acyclic autocorrelation coefficients of size at most 1.

P9. Lehmer's Problem. *Show that any monic polynomial p, $p(0) \neq 0$, with integer coefficients that is irreducible and is not a cyclotomic polynomial has Mahler measure at least $1.1762\ldots$. (This latter constant is the Mahler measure of $1+z-z^3-z^4-z^5-z^6-z^7+z^9+z^{10}$.)*

P10. Mahler's Problem. *For each n, find the polynomials in $\mathcal{L}_n$ that have largest possible Mahler measure. Analyze the asymptotic behaviour as n tends to infinity.*

P11. Conjecture of Schinzel and Zassenhaus. *There is a constant $c > 0$ such that any monic polynomial p_n of degree n with integer coefficients either has Mahler measure 1 or has at least one root of modulus at least $1 + c/n$.*

P12. Closure of Measures Conjecture of Boyd. *The set of all possible values of the Mahler measure of polynomials with integer coefficients in any number of variables is a closed set.*

P13. Multiplicity of Zeros of Height One Polynomials. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{F}_n$?*

P14. Multiplicity of Zeros in $\mathcal{L}_n$. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{L}_n$?*

P15. Another Erdős Problem. *Establish whether there is a positive constant c such that if*

$$V_n := \left(1+z^{b_1}\right)\left(1+z^{b_2}\right)\cdots\left(1+z^{b_n}\right)$$

is in $\mathcal{A}$, then

$$\max\{b_i\} > c\,2^n.$$

P16. A Montgomery Question. *Show that the minimal s arising as in Lemma 1 of Chapter 10 does not give the right value for $\Omega[0,1]$. Does $\Omega[0,1]$ have a closed form?*

P17. The Schur–Siegel–Smyth Trace Problem. *Fix $\epsilon > 0$. Suppose*

$$p_n(z) := z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathcal{Z}_n$$

has all real, positive roots and is irreducible. Show that, independently of n, except for finitely many explicitly computable exceptions,

$$|a_{n-1}| \geq (2-\epsilon)n.$$

Introductory Exercises

E1. Show, for $p_n \in \mathcal{L}_n$, that

$$\|p_n\|_2 = \sqrt{n+1}.$$

Show, for $\alpha \geq 2$, that

$$\sqrt{n+1} \leq \|p_n\|_\alpha \leq n+1$$

while, for $0 \leq \alpha \leq 2$,

$$1 \leq \|p_n\|_\alpha \leq \sqrt{n+1}.$$

When is equality possible in the above inequalities?

E2. For each positive even integer m and each positive integer n show that

$$\max\{\|p\|_m : p \in \mathcal{L}_n\}$$

is attained by the polynomial $1+z+z^2+\cdots+z^n$. Observe that this is not the unique extremal polynomial.

Klemeš [2001] proves this for $2 < m < 4$ ($m \in \mathbb{R}$) and also that the above polynomials are extremals for $\min\{\|p\|_m : p \in \mathcal{L}_n\}$ for $0 < m < 2$.

E3. Find a nontrivial upper bound ($< \frac{1}{2}$) in P1. Derive a nontrivial lower bound in P1 as follows. If $0 \neq p_n \in \mathcal{Z}_n$, then for some integer $m \neq 0$,

$$\|p_n\|_{[0,1]}^2 \geq \int_0^1 p_n^2(x)\,dx = \frac{m}{\operatorname{lcm}(1,2,\ldots,2n+1)} \neq 0,$$

where lcm denotes the least common multiple. By the prime number theorem, $\bigl(\operatorname{lcm}(1,2,\ldots,n)\bigr)^{1/n} \sim e$.

E4. Symmetric Polynomials. Let

$$(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n) = z^n - c_1 z^{n-1} + c_2 z^{n-2} - \cdots + (-1)^n c_n.$$

The coefficients c_k are, by definition, the *elementary symmetric functions* in the variables $\alpha_1, \ldots, \alpha_n$. For positive integers k, let

$$s_k := \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k.$$

Derive the *Newton identities*

$$s_k = (-1)^{k+1} k c_k + (-1)^k \sum_{j=1}^{k-1} (-1)^j c_{k-j} s_j, \quad k \leq n,$$

and

$$s_k = (-1)^{k+1} \sum_{j=k-n}^{k-1} (-1)^j c_{k-j} s_j, \quad k > n.$$

A *symmetric polynomial of n variables* is a polynomial of n variables that is invariant under any permutation of the variables.

One can show (by induction) that any symmetric polynomial in n variables (with integer coefficients) may be written uniquely as a polynomial (with integer coefficients) in the elementary symmetric functions.

We need the following consequence of this. Suppose that $p(z)$ is a monic polynomial with integer coefficients and with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. Show that if q is any polynomial with integer coefficients, then

$$q(\alpha_1) q(\alpha_2) \cdots q(\alpha_n)$$

is an integer.

E5. Show that P7 (the second part) implies P5. Show that P6 implies P5 for sufficiently large n. What other implications are there among the above problems?

Computational Problems

Experimentation on the computational problems in this book is most easily done in a symbolic algebra package such as Maple.

C1. Write a computer program to compute the L_p norms of polynomials on the boundary of D. Why is this easy if p is an even integer? Why is this hard otherwise?

C2. Write a computer program to search the class $\mathcal{L}_n$. Solve P4, P7, P13, and P14 for modest-sized n. (Gray codes are one way to implement this with some efficiency. See Knuth [1981].)

C3. Plot all the zeros of all Littlewood polynomials of degree at most 20. Similarly, plot all zeros of all polynomials in $\mathcal{A}_n$ for n at most 20.

Research Problems

R1. Solve P1 through P17 of this chapter (and skip the rest of the book).

Selected References

The basic analysis needed in this book may be found in the first and fifth references below. Littlewood's charming monograph discusses some of the problems (he also speculates in the introduction that the Riemann hypothesis is false).

1. P. Borwein and T. Erdélyi, *Polynomials and Polynomial Inequalities*, Springer-Verlag, New York, 1995.

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

3. M. Mignotte, *Mathematics for Computer Algebra*, Springer-Verlag, New York, 1992.

4. M. Mignotte and D. Ştefănescu, *Polynomials. An Algorithmic Approach*, Springer-Verlag Singapore, Singapore, 1999.

5. W. Rudin, *Real and Complex Analysis*, third edition, McGraw-Hill, New York, 1987.

Chapter 2

LLL and PSLQ

The single most useful algorithm of computational number theory is the LLL lattice basis reduction algorithm of Lenstra, Lenstra, and Lovász [1982]. It finds a relatively short vector in an integer lattice. In this chapter we give some examples of how LLL can be used to approach some of the central problems of the book. Appendix B deals, in detail, with the LLL algorithm and the closely related PSLQ algorithm for finding integer relations. In many of our applications LLL can be treated as a "black box"—why it works doesn't matter. One inputs a lattice and receives as output a candidate short vector that can be verified to have the requisite properties for the particular problem under consideration.

A lattice is defined as follows.

Definition. *The lattice L spanned by the n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ is the set of vectors $L := \{\sum_{i=1}^{n} n_i \mathbf{b}_i : n_i \in \mathbb{Z}\}$. We say that the vectors $\mathbf{b}_i$ form a basis for L.*

Many problems in number theory are solved by finding short (or shortest) vectors in a particular lattice. "Short" means with respect to a norm given by an inner product. Often the norm we use is the Euclidean or l_2 norm; namely, for a vector

$$\mathbf{a} := [\alpha_1, \alpha_2, \ldots, \alpha_n]$$

the norm is

$$l_2(\mathbf{a}) := |\mathbf{a}| := \sqrt{|\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_n|^2}.$$

The problem of finding the smallest vector in a lattice is computationally difficult and it is believed that no polynomial-time algorithm exists for solving this problem in general. (In the language of complexity theory, it is provably NP-hard under randomized reductions. See Ajtai [1997].)

What LLL actually does is to take a lattice basis (a maximally independent set of vectors, as above) and return a new basis that is reduced in a precise sense. This reduced basis consists of relatively short vectors. The smallest reduced basis vector $\mathbf{a}$ that LLL returns is small in the sense that $|\mathbf{a}| \leq 2^{(n-1)/2}|\mathbf{x}|$, where $\mathbf{x}$ is any other nonzero vector in the lattice and n is the dimension of the lattice. LLL finds this reduced basis in polynomial time and, in practice, often finds vectors very much smaller than the guaranteed bound.

A typical example for us is the following. Consider the Prouhet–Tarry–Escott problem of the last chapter for a fixed size n. We want to find a polynomial $q(z) := a_d z^d + \cdots + a_1 z + a_0$ with minimal l_1 norm that is divisible by $(1-z)^n$. (While minimizing the l_1 norm and the l_2 norm is not the same, it is the same if the minimizing polynomial has coefficients of size 1 and will be a good first approximation if the minimizing polynomial is of low height.) The lattice of dimension $m+1$ we now construct has basis

$$[(1-z)^n, z(1-z)^n, \ldots, z^m(1-z)^n].$$

(We identify the polynomial with the vector of coefficients, adding leading zeros as needed.) Note that any integer linear combination of this basis is divisible by $(1-z)^n$. LLL will return a small vector with respect to the l_2 norm, and this is what we are looking for (see also the exercises).

Now suppose we want to find a Littlewood polynomial of degree m divisible by $(1-z)^n$. How do we try to force LLL to return a polynomial with coefficients that are just -1 and 1? One strategy is the following. Find a monic polynomial p of degree m divisible by $(1-z)^n$ that has only odd coefficients. (This will be possible for all n and some m. For example, $(1-z)^{2^n-1}$ has odd coefficients.) Now consider the basis

$$\left[p(z), 2(1-z)^n, 2z(1-z)^n, \ldots, 2z^{m-n}(1-z)^n\right]$$

reduced by LLL. This reduced basis must have at least one member with just odd coefficients in order to have the same span. With a little luck this will be the desired element of relatively small norm. There is no guarantee that this will work, but often it does.

Another problem that can be attacked using LLL is the integer Chebyshev problem. Here we wish to find a polynomial of a given degree that has small supremum norm on, say, $[\alpha, \beta]$. One approach is to take the lattice $\mathcal{Z}_n$ and use the inner product associated with the norm

$$\|p\|_{L_2[\alpha,\beta]} := \left(\int_\alpha^\beta |p(x)|^2\, dx\right)^{1/2}.$$

This is discussed further in Chapter 10.

PSLQ is a relative of LLL that solves the problem of finding integer relations. Finding minimal polynomials is an example of such a problem. Given an algebraic α, one is looking for integers a_i with

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

Remarkably, LLL and PSLQ both solve this problem in polynomial time. This is detailed in Appendix B.

Computational Problems

C1. Implement LLL and PSLQ . (See Appendix B.)

C2. Use LLL to look for solutions of the Prouhet–Tarry–Escott problem (P2) for $n \leq 20$. (For each n the minimum possible l_1 norm is $2n$. See Chapter 11.)

C3. Which of P1 through P17 can be explored with LLL? How?

Research Problems

R1. Is it possible to approach the merit factor problem (P7) using LLL? For which other norms is there an analogue of LLL that gives polynomial-time algorithms for finding short vectors with respect to that norm?

R2. Are there polynomial-time algorithms for any of P1 through P17? (To make sense of this, one has to decide how to measure the size of an instance of the problem.) Note that it isn't clear that P2 is even algorithmic, and indeed, this is an open problem.

Selected References

Algorithms for LLL and PSLQ and variants are given in Appendix B. LLL is well presented in the original paper of Lenstra, Lenstra, and Lovász [1982]. There are now many variants and improvements on this algorithm. See, for example, Cohen [1993].

1. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.

2. A.K. Lenstra, H.W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

Chapter 3

Pisot and Salem Numbers

There are two very special classes of algebraic integers that arise repeatedly and naturally in this area of study. Recall that an *algebraic integer* is any root of any monic polynomial with integer coefficients. A real algebraic integer α is a *Pisot number* if all its conjugate roots have modulus strictly less than 1. A real algebraic integer α is a *Salem number* if all its conjugate roots have modulus at most 1, and at least one (and hence (see E2) all but one) of the conjugate roots has modulus exactly 1. As is traditional, though somewhat confusing, we denote the class of all Pisot numbers by S and the class of all Salem numbers by T.

One of the remarkable properties of these sets is that S is closed (in the sense that it contains all its limit points). Furthermore, every point of S is a two-sided limit of points of T. The reader is referred to Salem [1963] for additional material on this. See also the exercises.

We will denote *the nth cyclotomic polynomial* by Φ_n. This is the minimal polynomial of a primitive nth root of unity (e.g., $\exp(2\pi i/n)$). The cyclotomic polynomials are just the irreducible monic polynomials in $\mathcal{Z}$ of Mahler measure 1. The Φ_n are given by

$$\Phi_n(z) = \prod_{\substack{1 \le j \le n \\ \gcd(j,n)=1}} \bigl(z - \exp(j2\pi i/n)\bigr),$$

so for p a prime,

$$\Phi_p(z) = \frac{z^p - 1}{z - 1}.$$

Cyclotomic polynomials are discussed in more detail in Chapter 6.

Kronecker's theorem characterizes the monic polynomials of measure 1. A proof is outlined in E4 of Chapter 6.

Kronecker's Theorem. *If $p \in \mathcal{Z}$ is monic and irreducible and has all its roots in the set $\{0 < |z| \le 1\}$, then all the roots of p are roots of unity and p is a cyclotomic polynomial.*

The extent to which Kronecker's theorem extends to characterize monic polynomials of measure $c > 1$ is a principal topic of this section.

The smallest Pisot number is the largest root of $z^3 - z - 1$ and is approximately $1.3247\ldots$. This is also the smallest possible Mahler measure of a nonreciprocal polynomial that doesn't vanish at 0 or 1. This result is due to Smyth [1971]. A polynomial p of degree d is *reciprocal* if $p(z) = p^*(z)$. Recall that if

$$p(z) := a_0 + a_1 z + \cdots + a_d z^d$$

then

$$p^*(z) := \overline{a_0} z^d + \overline{a_1} z^{d-1} + \cdots + \overline{a_d} = z^d \, \overline{p(1/\overline{z})}.$$

Sometimes reciprocal polynomials are called *symmetric* or *self-inversive*. A polynomial p of degree d is *negative reciprocal* if $p(z) = -p^*(z)$. Note that if $p(z)$ is negative reciprocal and of odd degree, then $p(-z)$ is reciprocal.

The smallest Salem number is conjectured to be the largest root of $1 + z - z^3 - z^4 - z^5 - z^6 - z^7 + z^9 + z^{10}$. This polynomial is called Lehmer's polynomial. Its largest root is approximately $1.17628\ldots$. This is also conjectured to be the smallest possible Mahler measure of an irreducible noncyclotomic polynomial (excluding z).

The best results in the direction of the above conjecture are as follows. Louboutin [1983], improving constants of Dobrowolski [1979], shows that for any positive ϵ, an irreducible noncyclotomic polynomial p of large enough degree d satisfies

$$M(p) > 1 + \left(\frac{9-\epsilon}{4}\right)\left(\frac{\log\log d}{\log d}\right)^3.$$

(Voutier [1996] shows that for all $d \geq 2$, the above holds with $\epsilon = 8$.) In a slightly different vein, Dobrowolski [1991] shows that a monic polynomial p with k nonzero coefficients that is not a product of cyclotomic polynomials and does not vanish at 0 (i.e., not of measure 1) satisfies

$$M(p) > 1 + \frac{1}{a \exp(bk^k)},$$

where $a \leq 13911$ and $b \leq 2.27$ are absolute constants. See Schinzel [2000] for a discussion of these results.

The smallest limit point of measures (as in P12) is believed to be approximately $1.255433\ldots$. This limit point arises from the polynomial

$$q(x,y) := 1 + x + y + xy + xy^2 + x^2y + x^2y^2.$$

The natural generalization to two variables of Mahler's measure is via the integral

$$\exp\left(\frac{1}{4\pi^2}\int_0^{2\pi}\int_0^{2\pi} \log\left|q\left(e^{i\theta_1}, e^{i\theta_2}\right)\right| \, d\theta_1 \, d\theta_2\right).$$

(The Mahler measure of a polynomial in n variables is defined in the obvious way as an n-fold integral as above.) The limit point $(1.255433\ldots)$ is the value of the above integral. It is the limit of the measures of the single-variable polynomials $\{q(x, x^n)\}$. Multivariate Mahler measures arise as special values of L series in quite remarkable ways. See Boyd [1998].

Interestingly, the above q is a knot-invariant polynomial (see Ghate and Hironaka [2001]). Tables of information on this problem due to Mossinghoff are available at http://www.math.ucla.edu/~mjm/lc/lc.html.

We now restate Lehmer's problem, which arises in Lehmer [1933].

P9. Lehmer's Problem. *Show that any monic polynomial p, $p(0) \neq 0$, with integer coefficients that is irreducible and is not a cyclotomic polynomial has Mahler measure at least $1.1762\ldots$. (This latter constant is the Mahler measure of $1 + z - z^3 - z^4 - z^5 - z^6 - z^7 + z^9 + z^{10}$.)*

The best partial result, as observed above, is due to Smyth.

***Theorem* (Smyth).** *If $p \in \mathcal{Z}$ is irreducible and not reciprocal, and $p(0)p(1) \neq 0$, then*

$$M(p) \geq \theta := 1.3247\ldots,$$

where θ is the largest real root of $z^3 - z - 1 = 0$.

We will prove only a weaker form of Smyth's result where the constant $\theta := 1.3247\ldots$ is replaced by $\sqrt{5}/2 = 1.1180\ldots$. We will need the following standard result from complex analysis.

Parseval's Formula. *Suppose that ϕ is an analytic function in an open region containing the closed unit disk with Taylor expansion*

$$\phi(z) := e_0 + e_1 z + \cdots.$$

Then

$$\int_0^1 \left|\phi\left(e^{2\pi i\theta}\right)\right|^2 d\theta = \sum_{i=0}^{\infty} |e_i|^2.$$

Proof of Smyth's Theorem. We assume that the measure of p is less than 2, so we may also assume p monic. Thus, since p is irreducible, we may further assume that $|p(0)| = 1$.

Write

$$p^*(z) := d_0 + d_1 z + \cdots + d_n z^n,$$

where $d_0 = 1$ and $d_n = \pm 1$. Further, write

$$\frac{1}{p^*(z)} := e_0 + e_1 z + \cdots$$

and notice that

$$1 = (d_0 + d_1 z + \cdots + d_n z^n)(e_0 + e_1 z + \cdots) = \sum_{j=0}^{\infty} \sum_{i=0}^{j} d_{j-i} e_i z^j.$$

Thus $e_0 = d_0 = 1$ and

$$d_0 e_j = -\sum_{i=0}^{j-1} d_{j-i} e_i,$$

and since $d_0 = 1$, we have that each e_j is an integer. So

$$\frac{1}{p^*(z)} = e_0 + e_1 z + \cdots$$

with each $e_i \in \mathbb{Z}$.

Define G, h, and g by

$$\begin{aligned} G(z) &:= \frac{p(0)p(z)}{p^*(z)} = \frac{p(0)\prod(z-\alpha_i)}{\prod(1-z\alpha_i)} = \frac{p(0)\prod(z-\alpha_i)}{\prod(1-z\bar{\alpha}_i)} \\ &= \frac{p(0)\prod_{|\alpha_i|>1}(z-\alpha_i)\prod_{|\alpha_i|<1}(z-\alpha_i)}{\prod_{|\alpha_i|>1}(1-z\bar{\alpha}_i)\prod_{|\alpha_i|<1}(1-z\bar{\alpha}_i)} \\ &= \frac{p(0)\prod_{|\alpha_i|<1}\frac{(z-\alpha_i)}{(1-z\bar{\alpha}_i)}}{\prod_{|\alpha_i|>1}\frac{(1-z\bar{\alpha}_i)}{(z-\alpha_i)}} =: \frac{h(z)}{g(z)}. \end{aligned}$$

Observe that terms with roots of modulus 1 cancel out so both of the functions h and g are analytic on an open set containing the unit disk.

Consider a typical factor $(z-\alpha_i)/(1-\bar{\alpha}_i z)$ of $h(z)$ with z on the unit circle, $|z| = 1$:

$$\begin{aligned} \left(\frac{z-\alpha_i}{1-\bar{\alpha}_i z}\right)\overline{\left(\frac{z-\alpha_i}{1-\bar{\alpha}_i z}\right)} &= \left(\frac{z-\alpha_i}{1-\bar{\alpha}_i z}\right)\left(\frac{\bar{z}-\bar{\alpha}_i}{1-\alpha_i \bar{z}}\right) \\ = \left(\frac{z-\alpha_i}{1-\bar{\alpha}_i z}\right)\left(\frac{1-\bar{\alpha}_i z}{z-\alpha_i}\right) &= 1. \end{aligned}$$

Thus $|h(z)| = 1$ on $|z| = 1$, and similarly, $|g(z)| = 1$ on $|z| = 1$.

Now write

$$\begin{aligned} h(z) &:= b + b_1 z + \cdots, \\ g(z) &:= c + c_1 z + \cdots, \end{aligned}$$

and

$$G(z) := 1 + a_k z^k + \cdots, \quad a_k \neq 0.$$

Then, since $G(z) = h(z)/g(z)$,

$$\begin{aligned} 1 + a_k z^k + \cdots &= \frac{b + b_1 z + \cdots}{c + c_1 z + \cdots}, \\ (c + c_1 z + \cdots)(1 + a_k z^k + \cdots) &= b + b_1 z + \cdots, \end{aligned}$$

and

$$c + c_1 z + \cdots + c_{k-1} z^{k-1} + (ca_k + c_k) z^k + \cdots = b + b_1 z + \cdots .$$

From this, we compute that

$$\begin{aligned} c &= b, \\ c_1 &= b_1, \\ &\vdots \\ c_{k-1} &= b_{k-1}, \\ c_k + a_k c &= b_k. \end{aligned}$$

If $|c| > 2\max(|b_k|, |c_k|)$, then we see that

$$|a_k c| \le |b_k - c_k| \le |b_k| + |c_k| \le 2\max(|b_k|, |c_k|) < |c|,$$

which is a contradiction. Hence $|c| \le 2\max(|b_k|, |c_k|)$.

Without loss of generality, assume that $|b_k| \ge |b/2|$ (otherwise, the same argument applies to $|c_k|$). Then we have

$$\int_0^1 \left| h\left(e^{2\pi i\theta}\right)\right|^2 \, d\theta = \int_0^1 1 \, d\theta = 1 = \left|b^2\right| + \left|b_1^2\right| + \cdots + \left|b_k^2\right| + \cdots .$$

Thus

$$b^2 + |b_k|^2 \le 1$$

and

$$b^2 + \frac{b^2}{4} \le 1,$$

so

$$|b| \le \frac{2}{\sqrt{5}}.$$

But

$$|b| = |h(0)| = |p(0)| \prod_{|\alpha_i|<1} \frac{|0 - \alpha_i|}{|1 - 0\alpha_i|} = \frac{1}{M(p)}.$$

□

Schinzel [1973] gave the following sharp result for the measure of polynomials whose roots are all real.

***Theorem* (Schinzel).** *If $p \in \mathcal{Z}_d \setminus \mathcal{Z}_{d-1}$ has all real roots, is monic, and satisfies $p(-1)p(1) \neq 0$ and $|p(0)| = 1$, then $M(p) \ge \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}$.*

Proof. We use the following inequality for real $\beta_i > 1$:

$$(\beta_1 - 1)(\beta_2 - 1)\cdots(\beta_d - 1) \le \left((\beta_1\beta_2\cdots\beta_d)^{1/d} - 1\right)^d,$$

which follows from the convexity of $\log(e^x - 1)$ for $x > 0$. Now suppose $p(z) := \prod_{i=1}^d (z - \alpha_i)$. Then

$$\begin{aligned} 1 &\le \frac{\prod_{|\alpha_i|<1}(\alpha_i^{-2} - 1)\prod_{|\alpha_i|>1}(\alpha_i^2 - 1)}{M(p)^2} \le \frac{\left(M(p)^{4/d} - 1\right)^d}{M(p)^2} \\ &= \left(M(p)^{2/d} - M(p)^{-2/d}\right)^d, \end{aligned}$$

and the result follows. □

The above theorem holds more generally for all $p \in \mathcal{Z}_d$ that have all real roots and satisfy the condition $p(-1)p(1)p(0) \neq 0$. The proof follows the above outline and is left as an exercise. Note that the above theorem is sharp for $p(z) := \left(z^2 - z - 1\right)^n$.

A conjecture of similar flavour to Lehmer's problem is the following.

P11. Conjecture of Schinzel and Zassenhaus. *There is a constant $c > 0$ such that any monic polynomial p_n of degree n with integer coefficients either has Mahler measure 1 or has at least one root of modulus at least $1 + c/n$.*

This conjecture is made in Schinzel and Zassenhaus [1965]. It is easy to see that P9 implies P11. The best partial result is due to Smyth [1971]. If p is a nonreciprocal monic irreducible polynomial of degree $n > 1$, then at least one root ρ satisfies

$$\rho \ge 1 + \frac{\log \phi}{n},$$

where $\phi = 1.3247\ldots$ is the smallest Pisot number, namely, the real root of $z^3 - z - 1$. (The right constant in P11 may well be $\frac{3}{2}\log\phi$.) Boyd [1985] establishes P11 for polynomials of degree at most 11 and conjectures that the extremals are never reciprocal. He also conjectures that for degree $3k$ an extremal is $z^{3k} + z^{2k} - 1$.

There is a stronger, and perhaps more natural, conjecture of Boyd [1981] that implies P9 and P11 (up to the exact constants).

P12. Closure of Measures Conjecture of Boyd. *The set of all possible values of the Mahler measure of polynomials with integer coefficients in any number of variables is a closed set.*

Another problem, due to Mahler [1963], is to determine the maximum possible Mahler measure over the Littlewood polynomials. This also appears to be a difficult question. It relates to the questions of Chapter 15.

P10. Mahler's problem. *For each n, find the polynomials in $\mathcal{L}_n$ that have largest possible Mahler measure. Analyze the asymptotic behaviour as n tends to infinity.*

The most interesting question is whether or not this is asymptotic to $\sqrt{n}$.

Introductory Exercises

E1. Show that if α is a Pisot number and $p \in \mathcal{Z}$ is a polynomial of height h that does not have α as a root, then

$$|p(\alpha)| > c(\alpha, h),$$

where the positive constant $c(\alpha, h)$ depends only on α and h.

Hint: If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the complete set of roots of the minimal polynomial for α then

$$|p(\alpha_1)p(\alpha_2)\cdots p(\alpha_n)| \geq 1.$$

□

E2. Suppose that α is a Salem number. Show that the minimal polynomial is reciprocal. Show that the other roots of the minimal polynomial of α have modulus 1 except for a single root of modulus $|1/\alpha|$.

E3. Suppose that α is a Pisot number and denote by $d(\alpha)$ the least distance from α to an integer. Show that $d(\alpha^n) \to 0$ as $n \to \infty$.

This characterizes Pisot numbers if we add the assumption that α is an algebraic number. It is believed to characterize Pisot numbers generally, but the best that has been proved is that

$$\sum_{n=1}^{\infty} d(\alpha^n)^2$$

converges iff α is a Pisot number. This is due to Salem [1963].

For any positive α define $d^*(\alpha)$ to be the fractional part of α. (So $d(\alpha) = \min\{d^*(\alpha), d^*(1-\alpha)\}$.) When α is a Salem number, it can be shown that $\{d^*(\alpha^n)\}_{n=1}^{\infty}$ is dense, but not uniformly distributed, in the unit interval. In general, questions concerning the behaviour of $\{d^*(\alpha^n)\}_{n=1}^{\infty}$ are hard. It is still open as to whether $\left\{d^*\left(\left(\frac{3}{2}\right)^n\right)\right\}_{n=1}^{\infty}$ is infinitely often in the interval $[\frac{1}{2}, 1]$.

Show that if τ is a fourth-degree Salem number (with conjugates $1/\tau, \theta, \bar{\theta}$) and β is any number in $(0,1)$, then there exists a subsequence $\{n_i\}$ of the positive integers such that

$$d(\tau^{n_i}) \to \beta.$$

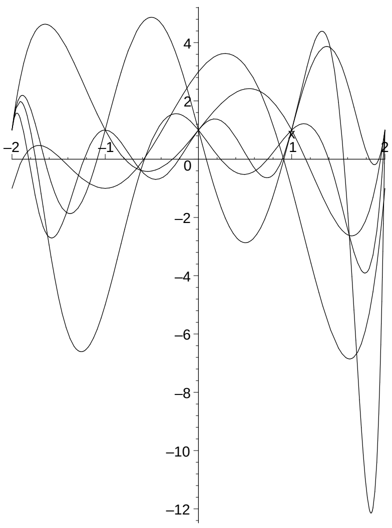
Hint: Note that if γ is an irrational number, then $\cos(2\pi\gamma n)$ comes arbitrarily close to any value in $[-1, 1]$ for an infinite number of n. □

E4. Suppose that p is a real reciprocal polynomial and suppose $p(-1)p(1) \neq 0$. Show that p has even degree $2n$ and there exists a polynomial q of degree n such that $z^{-n}p(z) = q(z + 1/z)$. Furthermore, if p has integer coefficients, so does q. (Note that $z + 1/z$ maps the boundary of the unit disc to the interval $[-2, 2]$.) Conclude that $z^{-n}p(z)$ is real-valued for complex z of modulus 1.

Suppose p has even degree $2n$ and $z^{-n}p(z)$ is real-valued for complex z of modulus 1. Show that $p(z)$ is reciprocal.

What is the analogous result for *negative reciprocal* p, that is, polynomials with real coefficients that satisfy $p(z) = -z^d p(1/z)$?

The smallest known Salem polynomials mapped, as in E4, to $[-2, 2]$.



E5. Show that for each d there is a positive constant c_d such that $M(p) > 1 + c_d$ for polynomials in $\mathcal{Z}_d$ of degree at most d that do not vanish at 0 and do not have measure 1.

E6. Suppose that ϕ is a Pisot number with minimal polynomial p of degree at least 3. Show that ϕ is a two-sided limit point of Salem numbers that are roots of the polynomials $z^m p(z) \pm p^*(z)$ as m varies.

Show that for any polynomial p, as $m \to \infty$,

$$M\big(z^m p(z) + p^*(z)\big) \to M\big(p(z)\big).$$

Hint: This result is due to Salem [1963]. Use Rouché's theorem to show that $(1+\epsilon)z^m p(z) + p^*(z)$ and $z^m p(z)$ have the same number of roots inside the unit disk. Note that $|p(z)| = |p^*(z)|$ for $|z| = 1$. So with $\epsilon = 0$, $z^m p(z) + p^*(z)$ has all but one zero in the closed unit disk. Now show that the extra zero is of modulus strictly greater than 1 for m large enough. For this last part consider the graph of $z^m p(z) + p^*(z)$ around ϕ.

Consider also $\big(z^m p(z) - p^*(z)\big)/(z-1)$ to see the two-sided property of the limit. □

E7. Show that the golden mean (the larger root of $z^2 - z - 1$) is a limit point of Mahler measures of Littlewood polynomials.

E8. Prove that if $p \in \mathcal{Z}$ has Mahler measure less than $h+1$, where h is an integer, then p divides some polynomial $q \in \mathcal{Z}$ of height at most h.

Hint: We will consider the case $h = 1$. Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ is the complete set of roots of p and $M(p) < 2$. Suppose r is a monic polynomial of degree n and height 1 and that p is not a factor of r (if it is, we are done). Then

$$1 \le |r(\alpha_1) r(\alpha_2) \cdots r(\alpha_d)|,$$

and since

$$|r(\alpha_k)| \le (n+1) \max\{1, |\alpha_k^n|\},$$

we have

$$|r(\alpha_2) r(\alpha_3) \cdots r(\alpha_d)| \le (n+1)^{d-1} M(p)^n.$$

So

$$|r(\alpha_1)| \ge \frac{1}{(n+1)^{d-1} M(p)^n}.$$

This is the key.

The rest of the argument is a Dirichlet box argument. Note that p has at least one root, say α_1, of modulus at most 1 and that any $s \in \mathcal{A}_n$ will satisfy $|s(\alpha_1)| \le n+1$. There are $2^{n+1} - 1$ nonzero polynomials in $\mathcal{A}_n$. So for n large enough, two of them must agree at α_1, and their difference is the required polynomial.

For a Salem number, or any number where α_1 may be chosen real, any n large enough such that

$$\frac{(n+1)^d M(p)^n}{2^{n+1} - 1} < 1$$

suffices. □

E9. Suppose α and β are algebraic numbers of degrees m and n respectively. Show that

$$M(\alpha + \beta) \le 2^{mn} M(\alpha)^n M(\beta)^m$$

and

$$M(\alpha\beta) \le M(\alpha)^n M(\beta)^m.$$

E10. Some Inequalities. Suppose that $p(z) := a_n z^n + \cdots + a_1 z + a_0$ is a polynomial of degree n with complex coefficients. Show that

$$|a_j| \le \binom{n}{j} M(p),$$
$$L(p) \le 2^n M(p),$$

and

$$L(p) \le nH(p).$$

If $p(z) := a_n z^n + \cdots + a_1 z + a_0$, then the following inequality of Gonçalves holds:

$$M(p)^2 + |a_0 a_n|^2 M(p)^{-2} \le \|p\|_2^2.$$

Also, for any $\alpha \ge 0$,

$$M(p) = \inf \|p\,q\|_2 = \inf \|p\,q\|_\alpha,$$

where the infimum is over all monic polynomials q with complex coefficients. The latter two inequalities may be found in Mignotte [1992]. See Appendix A.

E11. Show that P12 implies P9 (up to the exact constant) and that P9 implies P11.

E12. An algebraic integer is a *Perron number* if its modulus is strictly greater than the modulus of each of its conjugates. Suppose $\alpha > 1$ is the Mahler measure of a monic polynomial with integer coefficients. Show that α is a Perron number.

E13. Show that if p is a reciprocal polynomial, then the only zeros of p' of modulus 1 are the multiple zeros of p of modulus 1.

Hint: See Inequality 13 of Appendix A. Alternatively, it suffices to prove this at 1. Consider

$$\frac{p'(1)}{p(1)} = \sum_{i=1}^{n} \frac{1}{1-\zeta_i}.$$

Transform $\{|z| = 1\}$ to $\left\{\mathrm{Re}(z) = \frac{1}{2}\right\}$ by the transformation $w = (1+z)^{-1}$ and observe, by symmetry, that $\sum_{i=1}^{n} w_j \ne 0$. $\square$

E14. Suppose that p is a real reciprocal polynomial and that p has exactly k roots of modulus greater than 1. Show that p' also has exactly k roots of modulus greater than 1.

Hint: See Bonsall and Marden [1952]. Let n be the degree of p and let $\epsilon > 0$. Since $p(z) = z^n p(1/z)$, we have that

$$zp'(z) + z^{n-1}p'(1/z) = np(z),$$

or

$$zp'(z) + (p')^*(z) = np(z).$$

As in E6, and with E13, we have that $(1+\epsilon)zp'(z) + (p')^*(z)$ and $zp'(z)$ have the same number of zeros in the region $\{|z| > 1\}$. □

Computational Problems

C1. Find the 10 smallest possible Mahler measures (other than 1) of Littlewood polynomials of degree at most 50. Make a plausible conjecture about the smallest limit point of these measures.

C2. A natural approach to looking for polynomials with small Mahler measure (> 1) is to take products of cyclotomic polynomials and then perturb some of the coefficients symmetrically to construct noncyclotomic reciprocal polynomials that are, in some sense, close to products of cyclotomics. (See Mossinghoff, Pinner, and Vaaler [1998].) Explore this method computationally.

Research Problems

R1. Verify Lehmer's problem up to, say, degree 100. (Currently it has been checked exhaustively by Rhin and Qiang up to degree 40.)

R2. Solve Lehmer's problem for some interesting classes of reciprocal polynomials; for example, the class of reciprocal Littlewood polynomials.

R3. In E8 above, is it possible to make p divide a height h polynomial with the same measure as p? (That is, can the factor q/p be chosen to be a product of cyclotomic polynomials?)

R4. Show that the minimum Mahler measure (> 1) of a monic polynomial in $\mathcal{Z}$ is attained by a Salem polynomial.

Selected References

There is a lovely algorithm due to Boyd (reference 3 below) for computing Pisot numbers in a given interval.

1. M.-J. Bertin et al., *Pisot and Salem numbers*, Birkhäuser, Basel, 1992.
2. D. Boyd, *Variations on a theme of Kronecker*, Canad. Math. Bull. **21** (1978), 129–133.

3. D. Boyd, *Pisot and Salem numbers in intervals of the real line*, Math. Comp. **32** (1978), 1244–1260.

4. G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer-Verlag, London, 1999.

5. R. Salem, *Algebraic Numbers and Fourier Analysis*, D.C. Heath and Co., Boston, MA, 1963.

6. A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge University Press, Cambridge, 2000.

Chapter 4

Rudin–Shapiro Polynomials

Littlewood's problem asks how small a polynomial with coefficients from the set $\{+1, -1\}$ can be on the unit disk.

P4. Littlewood's Problem in L_∞. *Find a polynomial in $\mathcal{L}_n$ that has smallest possible supremum norm on the unit disk. Show that there exist positive constants c_1 and c_2 such that for any n it is possible to find $p_n \in \mathcal{L}_n$ with*

$$c_1\sqrt{n+1} \le |p_n(z)| \le c_2\sqrt{n+1}$$

for all complex z with $|z| = 1$.

As we will discuss in Chapter 15, the lower bound part of this conjecture, by itself, seems hard, and no sequence is known that satisfies just the lower bound. A sequence of Littlewood polynomials that satisfies just the upper bound is given by the Rudin–Shapiro polynomials. The Rudin–Shapiro polynomials appear in Harold Shapiro's 1951 thesis at MIT and are sometimes called just Shapiro polynomials. They also arise independently in Golay [1951]. They are remarkably simple to construct and are a rich source of counterexamples to possible conjectures.

The Rudin–Shapiro polynomials are defined by

$$P_0(z) := 1, \quad Q_0(z) := 1,$$

and

$$P_{n+1}(z) := P_n(z) + z^{2^n} Q_n(z),$$
$$Q_{n+1}(z) := P_n(z) - z^{2^n} Q_n(z).$$

These have all coefficients ± 1, and P_n and Q_n both have degree $2^n - 1$. If $|z| = 1$, then

$$|P_{n+1}|^2 + |Q_{n+1}|^2 = 2\left(|P_n|^2 + |Q_n|^2\right),$$

and it is easy to deduce that

$$|P_n(z)| \le \sqrt{2^{n+1}} = \sqrt{2}\sqrt{\text{degree}(P_n) + 1}$$

and

$$|Q_n(z)| \le \sqrt{2^{n+1}} = \sqrt{2}\sqrt{\text{degree}(Q_n) + 1}$$

for all z of modulus 1.

Iteration 1. *Let $p_0(z)$ be a polynomial of degree d_0 with coefficients in a set A of real numbers, and suppose that $p_0(0) \neq 0$. Let*

$$p_{n+1}(z) = p_n(z) + z^{d_n+1} p_n^*(-z),$$

where d_n is the degree of p_n. Then p_n is a polynomial of degree $d_n = 2^n d_0 - 1$ with all coefficients in $A \cup -A$. Furthermore, if

$$R_n := p_n(z) \quad \textit{and} \quad S_n := p_n^*(-z),$$

then

$$R_{n+1} = R_n + z^{d_n+1} S_n$$

and

$$S_{n+1} = (-1)^{d_n} \left(R_n - z^{d_n+1} S_n\right).$$

Proof. Most of this is simple calculation. Observe that

$$p_{n+1}(z) = p_n(z) + (-1)^{d_n} z^{2d_n+1} p_n(-1/z),$$

so

$$p_{n+1}(-1/z) = p_n(-1/z) - (-1)^{d_n} z^{-2d_n-1} p_n(z),$$

and multiplying this equation by $-z^{2d_n+1}$ yields the second form of the iteration. □

Lemma 1. *In the notation of Iteration 1,*

$$|R_n(z)|^2 + |S_n(z)|^2 = 2^n \left(|p_0(z)|^2 + |p_0^*(-z)|^2\right),$$

provided that $|z| = 1$. Furthermore,

$$\frac{|R_n(z)|^2}{\|R_n\|_2^2} + \frac{|S_n(z)|^2}{\|S_n\|_2^2} = \frac{|p_0(z)|^2}{\|p_0\|_2^2} + \frac{|p_0^*(-z)|^2}{\|p_0\|_2^2}.$$

Proof. The first statement follows from the parallelogram law for complex numbers:

$$\begin{aligned} |R_{n+1}(z)|^2 + |S_{n+1}(z)|^2 &= |R_n(z) + z^{d_n+1} S_n(z)|^2 + |R_n(z) - z^{d_n+1} S_n(z)|^2 \\ &= 2\left(|R_n(z)|^2 + |S_n(z)|^2\right). \end{aligned}$$

The second statement follows on observing that

$$\|R_{n+1}\|_2^2 = 2\|R_n\|_2^2$$

and

$$\|S_{n+1}\|_2^2 = 2\|S_n\|_2^2.$$

□

We wish to compute the L_4 norm of p_n. For this, we follow Littlewood [1968].

Theorem 1. *In the notation of Iteration 1, let $y_n := \|p_n\|_4^4/\|p_n\|_2^4$ for $n \geq 0$, and let*

$$\gamma := \frac{\|p_0\|_4^4 + \|p_0(z)p_0^*(-z)\|_2^2}{2\|p_0\|_2^4}.$$

Then

$$y_n = \frac{4\gamma}{3} + \left(y_0 - \frac{4\gamma}{3}\right)\left(-\frac{1}{2}\right)^n.$$

For the Rudin–Shapiro polynomials, this gives the following corollary.

Corollary 1. *The L_4 norm of the Rudin–Shapiro polynomials satisfies*

$$\frac{\|P_n\|_4^4}{4^n} = \frac{\|Q_n\|_4^4}{4^n} = \frac{4}{3} - \left(\frac{1}{3}\right)\left(-\frac{1}{2}\right)^n \to \frac{4}{3}.$$

Proof of Theorem 1. With R_n and S_n as in Iteration 1, let

$$x_n := \|R_n\|_4^4 = \|S_n\|_4^4$$

and

$$w_n := \|R_n S_n\|_2^2.$$

Then, with $z := e^{i\theta}$ and $d_n := \text{degree}(R_n)$,

$$\begin{aligned} 2x_{n+1} &= \|R_{n+1}\|_4^4 + \|S_{n+1}\|_4^4 \\ &= \frac{1}{2\pi}\int_0^{2\pi} \left(|R_n(z) + z^{d_n+1}S_n(z)|^4 + |R_n(z) - z^{d_n+1}S_n(z)|^4\right) d\theta. \end{aligned}$$

If we use the identity for complex numbers

$$|u+v|^4 + |u-v|^4 = 2(|u|^4 + |v|^4) + 4\big(\text{Re}(u\overline{v})\big)^2 - 4\big(\text{Im}(u\overline{v})\big)^2 + 8|uv|^2$$

with $u := R_n(z)$ and $v := z^{d_n+1}S_n(z)$, we deduce that

$$\begin{aligned} 2x_{n+1} = 4x_n + 8w_n &+ \frac{4}{2\pi}\int_0^{2\pi} \left(\text{Re}\big(R_n(z)\overline{z^{d_n+1}S_n(z)}\big)\right)^2 d\theta \\ &- \frac{4}{2\pi}\int_0^{2\pi} \left(\text{Im}\big(R_n(z)\overline{z^{d_n+1}S_n(z)}\big)\right)^2 d\theta. \end{aligned}$$

Now, if P is a polynomial with real coefficients and zero constant term, then

$$\frac{1}{2\pi}\int_0^{2\pi}\Big(\mathrm{Re}\big(P(z)\big)\Big)^2\,d\theta = \frac{1}{2\pi}\int_0^{2\pi}\Big(\mathrm{Im}\big(P(z)\big)\Big)^2\,d\theta = \frac{1}{2}\|P\|_2^2,$$

and it follows that the two integrals above cancel. Thus

$$x_{n+1} = 2x_n + 4w_n. \tag{1}$$

We now observe that with Lemma 1,

$$\begin{aligned}
2x_n + 2w_n &= \frac{1}{2\pi}\int_0^{2\pi}\left(|R_n(z)|^2 + |S_n(z)|^2\right)^2 d\theta \\
&= \frac{2^{2n}}{2\pi}\int_0^{2\pi}\left(|p_0(z)|^2 + |p_0^*(-z)|^2\right)^2 d\theta \\
&= \frac{2^{2n+2}}{2\pi}\int_0^{2\pi}\frac{|p_0(z)|^4 + |p_0(z)p_0^*(-z)|^2}{2}\,d\theta \\
&= 2^{2n+2}\left(\frac{\|p_0\|_4^4 + \|p_0(z)p_0^*(-z)\|_2^2}{2}\right).
\end{aligned}$$

From this and (1) we deduce that

$$x_{n+1} = -2x_n + 2^{2n+3}\left(\frac{\|p_0\|_4^4 + \|p_0(z)p_0^*(-z)\|_2^2}{2}\right).$$

Since $\|p_{n+1}\|_2^4 = 4\|p_n\|_2^4$, this yields

$$y_{n+1} = -\frac{y_n}{2} + 2\gamma,$$

which solves to give the result. □

An immediate consequence of this is the following.

Corollary 2. *The sequence $p_n(z)$ generated by Iteration 1 satisfies*

$$\lim_{n\to\infty}\frac{\|p_n\|_4}{\|p_n\|_2} = \left(\frac{4\gamma}{3}\right)^{1/4},$$

where

$$\gamma = \frac{\|p_0\|_4^4 + \|p_0(z)p_0^*(-z)\|_2^2}{2\|p_0\|_2^4} \geq 1.$$

Proof. The only part needing proof is that $\gamma \geq 1$. Note that with $z := e^{i\theta}$,

$$\begin{aligned}
\|p\|_4^4 + \|p(z)p^*(-z)\|_2^2 &= \frac{2}{2\pi}\int_0^{2\pi}\left(\frac{|p(z)|^2 + |p^*(-z)|^2}{2}\right)^2 d\theta \\
&\geq 2\left(\frac{1}{2\pi}\int_0^{2\pi}\frac{|p(z)|^2 + |p^*(-z)|^2}{2}\,d\theta\right)^2 \\
&= 2\|p\|_2^4.
\end{aligned}$$

Here we have used the fact that $L_2(q) \geq L_1(q)$. □

The question of when $\gamma = 1$ is discussed further in Chapter 14. This relates to the existence of Golay complementary pairs.

It is easy to check that the same results hold for the iteration

$$p_{n+1}(z) = p_n(z) - z^{d_n+1} p_n^*(-z).$$

Define

$$\gamma(p) = \frac{\|p\|_4^4 + \|p(z)p^*(-z)\|_2^2}{2\|p\|_2^4}$$

and let

$$T_\pm(p) = p(z) \pm z^{d_n+1} p^*(-z).$$

A direct computation, as in the proof of Theorem 1, shows that $\gamma\big(T_\pm(p)\big) = \gamma(p)$. Thus, by an obvious analogue of Corollary 1, if $\{q_n\}$ is a sequence of polynomials generated by $q_{n+1} = T_\pm(q_n)$ for any choice of signs, then

$$\lim_{n\to\infty} \frac{\|q_n\|_4}{\|q_n\|_2} = \left(\frac{4\gamma(q_0)}{3}\right)^{1/4}.$$

We remark that the usual Rudin–Shapiro polynomials satisfy the recurrence

$$P_{n+1}(z) = P_n(z) - (-1)^n z^{2^n} P_n^*(-z)$$

and

$$Q_{n+1}(z) = P_n(z) + (-1)^n z^{2^n} P_n^*(-z).$$

So for $n \ge 1$, we have

$$\{P_{n+1}, Q_{n+1}\} = \{T_+(P_n), T_-(P_n)\}.$$

Introductory Exercises

E1. The Rudin–Shapiro polynomials satisfy the upper bound in P4 on a subsequence with a constant $c_2 := \sqrt{2}$. Show how to find a sequence that satisfies the upper bound with a constant c for all n. (In fact, $c = 2$ is possible. See Saffari [1990].)

E2. Show that the Rudin–Shapiro polynomials satisfy

(a) $P_{n+1}(z) = P_n\left(z^2\right) + zP_n\left(-z^2\right)$.

(b) $Q_{n+1}(z) = Q_n\left(z^2\right) + zQ_n\left(-z^2\right)$.

(c) $P_n(z)P_n(1/z) + Q_n(z)Q_n(1/z) = 2^{n+1}$.

(d) $P_{n+m+1}(z) = P_m(z)P_n\left(z^{2m+1}\right) + z^{2m}Q_m(z)P_n\left(-z^{2m+1}\right)$.

(e) $P_n(1) = 2^{[(n+1)/2]}$.

(f) $P_n(-1) = \frac{1}{2}\big(1 + (-1)^n\big)2^{[n/2]}$.

Here $[\cdot]$ denotes the integer part. These and more may be found in Brillhart, Lomont, and Morton [1976].

E3. Consider the following four-term variant of the Rudin–Shapiro polynomials: Let $P_0 := Q_0 := R_0 := S_0 := 1$ and

$$\begin{aligned}
P_n &:= P_{n-1} + z^{4^{n-1}} Q_{n-1} + z^{2\cdot 4^{n-1}} R_{n-1} + z^{3\cdot 4^{n-1}} S_{n-1},\\
Q_n &:= P_{n-1} + iz^{4^{n-1}} Q_{n-1} - z^{2\cdot 4^{n-1}} R_{n-1} + -iz^{3\cdot 4^{n-1}} S_{n-1},\\
R_n &:= P_{n-1} - z^{4^{n-1}} Q_{n-1} + z^{2\cdot 4^{n-1}} R_{n-1} - z^{3\cdot 4^{n-1}} S_{n-1},\\
S_n &:= S_{n-1} + -iz^{4^{n-1}} Q_{n-1} - z^{2\cdot 4^{n-1}} R_{n-1} + iz^{3\cdot 4^{n-1}} S_{n-1}.
\end{aligned}$$

Show that if $|z| = 1$, then

$$|P_n(z)|^2 + |Q_n(z)|^2 + |R_n(z)|^2 + |S_n(z)|^2 = 4^{n+1}.$$

In general, let $P_{0,j} = \omega^{j-1}$ for $j := 1, \ldots, N$, where ω is a primitive Nth root of unity, and for each integer $h > 0$ let

$$P_{h,j}(z) := \sum_{k=1}^{N} \omega^{(k-1)(j-1)} z^{(k-1)N^{h-1}} P_{h-1,k}(z), \quad j = 1, \ldots, N.$$

Then, for $|z| = 1$,

$$\sum_{k=1}^{N} |P_{n,k}(z)|^2 = N^{n+1}.$$

E4. The Average Norm of Littlewood Polynomials. Show that if $p \in \mathcal{L}_n$, then

$$\|zp(z) + 1\|_4^4 + \|zp(z) - 1\|_4^4 = 2\|p(z)\|_4^4 + 8n + 10.$$

Deduce from this that the average value of $\|p(z)\|_4^4$ for $p \in \mathcal{L}_n$ is

$$2n^2 + 3n + 1.$$

See Newman and Byrnes [1990]. (For any fixed p, this is also the average over the set of all polynomials of degree n whose coefficients are all pth roots of unity.) This result is extended in Borwein and Choi [to appear] where it is shown that the average value of $\|p(z)\|_6^6$ for $p \in \mathcal{L}_n$ is

$$6n^3 + 9n^2 + 4n + 1,$$

and the average value of $\|p(z)\|_8^8$ for $p \in \mathcal{L}_n$ is

$$24n^4 + 30n^3 + 4n^2 + 5n + 4 - 3(-1)^n.$$

E5. Show that if p is of degree n, then

$$\|p(z) + z^{n+1}p^*(z)\|_4^4 + \|p(z) - z^{n+1}p^*(z)\|_4^4 = 12\|p(z)\|_4^4.$$

Deduce that the average value of $\|p(z)\|_4^4$ over the reciprocal and negative reciprocal $p \in \mathcal{L}_n$, for odd n, is

$$3n^2 + 3n.$$

Show that the above is also the average over just the set of reciprocal $p \in \mathcal{L}_n$ when n is odd. When n is even the average is $3n^2 + 3n + 1$.

E6. A polynomial is *skewsymmetric* if $p(z) = \pm z^d p(-1/z)$, where d is the degree of p. Observe that for real polynomials this is equivalent to $p(iz) = \pm p^*(iz)$.

Show that if n is odd and p is of degree n, then

$$p(z) \pm z^{n+1} + z^{2n+2}p^*(-1/z)$$

are both skewsymmetric. Show that if n is even and p is of degree n, then

$$p(z) \pm z^{n+1} - z^{2n+2}p^*(-1/z)$$

are both skewsymmetric.

Show that all skewsymmetric Littlewood polynomials are as above.

E7. Show that the average value of $\|p(z)\|_4^4$ over the skewsymmetric $p \in \mathcal{L}_n$, for even n, is

$$2n^2 + n + 1.$$

E8. The Average Norm of Height One Polynomials. Show that the average value of $\|p(z)\|_2^2$ over all height 1 polynomials of degree n is

$$\frac{2}{3}n + \frac{2}{3}.$$

Show that the average value of $\|p(z)\|_4^4$ over all height 1 polynomials of degree n is

$$\frac{8}{9}n^2 + \frac{14}{9}n + \frac{2}{3}$$

and the average value of $\|p(z)\|_4^4$ over all height 1 polynomials of degree n with leading coefficient 1 is

$$\frac{8}{9}n^2 + \frac{22}{9}n + 1.$$

Show that the average value of $\|p(z)\|_6^6$ over all height 1 polynomials of degree n is

$$\frac{16}{9}n^3 + 4n^2 + \frac{26}{9}n + \frac{2}{3}.$$

This is proved in Borwein and Choi [to appear], as is the following. Let $n \geq 0$ and $H \geq 1$ be integers and let

$$\mathcal{F}_n(H) := \left\{ \sum_{i=0}^{n} a_i z^i : |a_i| \leq H, a_i \in \mathbb{Z} \right\}$$

be the set of all the polynomials of height at most H and degree $\leq n$. Let

$$\beta_n(m, H) := \frac{1}{(2H+1)^{n+1}} \sum_{P \in \mathcal{F}_n(H)} \|P\|_m^m.$$

Theorem 2. *For $n \geq 0$ and $H \geq 1$, we have*

$$\begin{aligned}
\beta_n(2,H) &= \frac{1}{3}H(H+1)(n+1),\\
\beta_n(4,H) &= \frac{2}{9}H^2(H+1)^2n^2 + \frac{1}{45}H(H+1)\left(19H^2+19H-3\right)n\\
&\quad + \frac{1}{15}H(H+1)\left(3H^2+3H-1\right),
\end{aligned}$$

and

$$\begin{aligned}
\beta_n(6,H) = &\frac{2}{9}H^3(H+1)^3n^3 + \frac{1}{5}H^2(H+1)^2(3H^2+3H-1)n^2\\
&+ \frac{1}{315}H(H+1)\left(164H^4+328H^3+56H^2-108H+15\right)n\\
&+ \frac{1}{21}H(H+1)\left(3H^4+6H^3-3H+1\right).
\end{aligned}$$

Computational Problems

C1. Compute the maximum and minimum of the Rudin–Shapiro polynomials on the circle $\{|z|=1\}$ for as many n as possible. Show that the Rudin–Shapiro polynomials of odd index vanish at -1.

Observe that the Rudin–Shapiro polynomial P_4,

$$-z^{15}+z^{14}-z^{13}-z^{12}-z^{11}+z^{10}+z^9+z^8+z^7-z^6+z^5+z^4-z^3+z^2+z+1,$$

has $\min\{|p(z)| : |z|=1\} > 1.185$. Use this to construct an infinite sequence of polynomials $p_n \in \mathcal{L}_n$ with

$$\min\{|p_n(z)| : |z|=1\} \gg (n+1)^\rho$$

for some $\rho > 0$.

Use the Barker polynomial

$$z^{12}+z^{11}+z^{10}+z^9+z^8-z^7-z^6+z^5+z^4-z^3+z^2-x+1$$

to get a bound of $\rho > 0.43$.

Research Problems

R1. There are many ways to extend the Rudin–Shapiro construction. One can consider iterations of three or more terms, for example (see E3 above). Is it possible to extend the construction to get good lower bounds in P4?

R2. Extend the formulae of the exercises for the average of $\|p(z)\|_n^n$. So, for example, extend the formulae of Theorem 2 for $\beta_n(m, H)$ for all even n.

Selected References

The results in this section, for the most part, follow the second reference below.

1. P. Borwein and S. Choi, *The average norm of polynomials of fixed height* (to appear).

2. P. Borwein and M. Mossinghoff, *Rudin–Shapiro-like polynomials in L_4*, Math. Comp. **69** (2000), 1157–1166.

3. J. Brillhart, J.S. Lomont, and P. Morton, *Cyclotomic properties of the Rudin–Shapiro polynomials*, J. Reine Angew. Math. **288** (1976), 37–65.

4. H. Shapiro, *Extremal problems for polynomials and power series*, M.Sc. thesis, MIT, 1951.

Chapter 5

Fekete Polynomials

The *Fekete polynomials* are defined, for prime p, by

$$f_p(z) := \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) z^k,$$

where $(\frac{\cdot}{p})$ is the Legendre symbol. Recall that the Legendre symbol $(\frac{k}{p})$ is defined as follows:

$$\left(\frac{k}{p}\right) := \begin{cases} 1 & \text{if } x^2 \equiv k \pmod{p} \text{ has a nonzero solution,} \\ 0 & \text{if } p \text{ divides } k, \\ -1 & \text{otherwise.} \end{cases}$$

The Legendre symbol is a character mod p, i.e., a function χ that maps the nonzero integers modulo p into the complex numbers of modulus 1 and satisfies $\chi(ab) = \chi(a)\chi(b)$. It is also called the *quadratic character* mod p.

The Fekete polynomials are (except for the constant coefficient) Littlewood polynomials, though their primary existence is as Gauss sums. They, like the Rudin–Shapiro polynomials of the last chapter, provide a rich source of examples and counterexamples. See Appendix C.

Recall that the L_2 norm of $f_p(z)$ is $\sqrt{p-1}$ and that the supremum norm is bounded below by the L_2 norm. The modulus of f_p at any primitive pth root of unity is $\sqrt{p}$. This is proved in the following lemma.

***Lemma 1* (Gauss).** *If p is an odd prime,* $\gcd(k,p) = 1$*, and ζ_p is a primitive pth root of unity, then*

$$f_p\left(\zeta_p^k\right) = \pm\sqrt{\left(\frac{-1}{p}\right) p}$$

and

$$f_p(1) = 0.$$

Proof. Let χ be the quadratic character mod p (the Legendre symbol) and let b be the least positive residue of $ak \pmod p$. Then

$$\sum_{a=1}^{p-1} \chi(a)\zeta_p^{ak} = \sum_{b=1}^{p-1} \chi\left(bk^{-1}\right)\zeta_p^b = \bar{\chi}(k)\sum_{b=1}^{p-1}\chi(b)\zeta_p^b.$$

It follows that

$$f_p(\zeta_p^k) = \left(\frac{k}{p}\right) f_p(\zeta_p).$$

Also, since exactly $(p-1)/2$ of the reduced residues a modulo p satisfy

$$\left(\frac{a}{p}\right) = 1,$$

we see that

$$f_p(1) = 0.$$

We now see that

$$\begin{aligned}(p-1) f_p\left(\zeta_p^k\right)^2 &= \sum_{j=0}^{p-1} f_p(\zeta_p^j)^2 = \sum_{j=0}^{p-1}\sum_{a,b=0}^{p-1}\left(\frac{ab}{p}\right)\zeta_p^{(a+b)j} \\ &= \sum_{a,b=1}^{p-1}\left(\frac{ab}{p}\right)\sum_{j=0}^{p-1}\zeta_p^{(a+b)j} = p\sum_{\substack{a=1\\ b=p-a}}^{p-1}\left(\frac{ab}{p}\right) = p\left(\frac{-1}{p}\right)(p-1),\end{aligned}$$

and we are done. $\square$

The choice of root in the above lemma is more subtle. This is also a result of Gauss (see Hua [1982]).

***Theorem 1* (Gauss).** *For p an odd prime, let*

$$\epsilon_p := \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ i & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Then if $\gcd(k,p) = 1$,

$$f_p\left(\zeta_p^k\right) = \epsilon_p\sqrt{p}\left(\frac{k}{p}\right).$$

Since $f_p(z)$ is of constant modulus $\sqrt{p}$ at the primitive pth roots of unity, it is a natural candidate for an extremal polynomial in the supremum norm. However, Montgomery [1980] shows that the supremum norm of $f_p(z)$ on D grows at least like $\sqrt{p}\log\log p$. (See R1.) The extent to which $f_p(z)$ is an extremal at the roots of unity is the content of the following theorem.

Theorem 2. *Let $p(z) := a_1 z + a_2 z^2 + \cdots + a_{N-1}z^{N-1}$ with N odd and each $a_n = \pm 1$. Then we have*

$$\sum_{k=0}^{N-1} |p(\zeta^k)|^4 \geq N^2(N-1)$$

and

$$\max\left\{\left|p\left(\zeta^k\right)\right| : 0 \le k \le N-1\right\} \ge \sqrt{N}.$$

The above inequalities are sharp. Equality holds in the second inequality if and only if N is an odd prime and $p(z)$ is $\pm f_N(z)$. Here $\zeta := e^{2\pi i/N}$.

The proof of this may be found in Borwein, Choi, and Yazdani [2001]. We prove only the following lemma, which includes the first part of the above theorem.

Lemma 2. *Let $p(z) := a_1 z + a_2 z^2 + \cdots + a_{N-1} z^{N-1}$ with N odd and each $a_n = \pm 1$. We have*

$$\sum_{k=0}^{N-1} \left|p\left(\zeta^k\right)\right|^2 = N(N-1)$$

and

$$\sum_{k=0}^{N-1} \left|p\left(\zeta^k\right)\right|^4 \ge N^2(N-1).$$

Proof. Since $a_n = \pm 1$, we have

$$\sum_{k=0}^{N-1} \left|p\left(\zeta^k\right)\right|^2 = \sum_{n,m=1}^{N-1} a_n a_m \sum_{k=0}^{N-1} \zeta^{k(n-m)} = N(N-1),$$

which is the first equality. For the second inequality,

$$\begin{aligned}
\sum_{k=0}^{N-1} \left|p\left(\zeta^k\right)\right|^4 &= \sum_{k=0}^{N-1} \left|p\left(\zeta^k\right)^2\right|^2 = \sum_{k=0}^{N-1} \left|p\left(\zeta^k\right) p\left(\zeta^{-k}\right)\right|^2 \\
&= \sum_{k=0}^{N-1} \left|\sum_{l=0}^{N-1} \left\{ \sum_{n-m\equiv l \pmod N} a_n a_m \right\} \zeta^{kl}\right|^2 \\
&= N \sum_{l=0}^{N-1} \left\{ \sum_{n-m\equiv l \ (\mathrm{mod})N} a_n a_m \right\}^2 \\
&= N \left\{ (N-1)^2 + \sum_{l=1}^{N-1} \left\{ \sum_{n-m\equiv l \pmod N} a_n a_m \right\}^2 \right\} \\
&\ge N((N-1)^2 + (N-1)) = N^2(N-1),
\end{aligned}$$

because

$$\sum_{n-m\equiv l \pmod N} a_n a_m \equiv N-2 \equiv 1 \pmod 2$$

for $1 \le l \le N-1$. □

There is an interesting connection that Dirichlet observed between the Fekete polynomials and the L series

$$L\left(s, \left(\frac{\cdot}{p}\right)\right) := \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n^s}.$$

Because the gamma function satisfies

$$\Gamma(s) = n^s \int_0^1 (-\log t)^{s-1} t^{n-1}\, dt,$$

it follows that

$$\begin{aligned}\Gamma(s) L\left(s, \left(\frac{\cdot}{p}\right)\right) &= \Gamma(s) \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n^s} = \int_0^1 (-\log t)^{s-1} \sum_{n=1}^{\infty} \left(\frac{n}{p}\right) t^{n-1}\, dt \\ &= \int_0^1 \frac{(-\log t)^{s-1}}{t} \frac{f_p(t)}{1-t^p}\, dt,\end{aligned}$$

since $f_p(x)/(1-x^p) = \sum_{n=1}^{\infty} \left(\frac{n}{p}\right) x^n$.

This leads to the analytic continuation of the L series and also allows one approach to the so-called Siegel zeros of L. A Siegel zero is a real zero of the L series in the interval $(0,1)$. (They are conjectured not to exist.) Observe, as Fekete did, that if $f_p(x)$ has no real zeros in $(0,1)$, then $L\big(s, \left(\frac{\cdot}{p}\right)\big)$ has no real zeros on the positive real axis. However, the Fekete polynomials tend to have real zeros, and the approach fails. See Conrey et al. [2000].

Introductory Exercises

E1. For p an odd prime, the *shifted Fekete polynomials* are defined as

$$f_p^t(z) := \sum_{k=0}^{p-1} \left(\frac{k+t}{p}\right) z^k.$$

They also satisfy

$$\left| f_p\left(\zeta_p^k\right)\right| = \sqrt{p}$$

for $1 \le k \le p-1$. Prove this.

In Chapter 15 and Appendix C we will see that the L_4 norms of some of these shifted Fekete polynomials are explicitly computable in terms of the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. This leads to infinite sequences of Littlewood polynomials with the smallest known asymptotic L_4 norm.

Computational Problems

C1. Gauss's *quadratic reciprocity theorem* states that for p and q odd primes

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Also,

$$\left(\frac{-1}{q}\right) := \begin{cases} 1 & \text{if} \quad q \equiv 1 \pmod 4, \\ -1 & \text{if} \quad q \equiv 3 \pmod 4, \end{cases}$$

and

$$\left(\frac{2}{q}\right) := \begin{cases} 1 & \text{if} \quad q \equiv 1, 7 \pmod 8, \\ -1 & \text{if} \quad q \equiv 3, 5 \pmod 8. \end{cases}$$

Use this to write a program to compute quadratic residues. If the aim is to compute all the residues mod p or, equivalently, to compute the Fekete polynomial f_p, how else might one proceed?

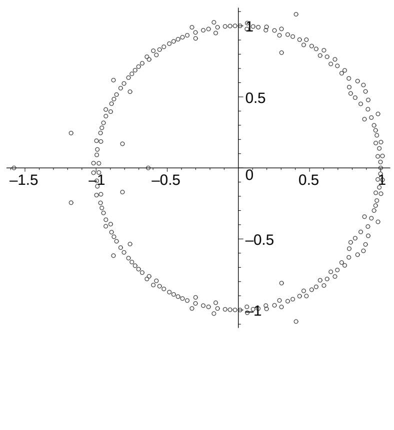
C2. Explore the zeros of the Fekete polynomials and the shifted Fekete polynomials. Formulate some reasonable conjectures.

Consider $z^{-p/2} f_p(z)$ and observe that this function changes sign between consecutive roots of unity ζ_p^k and ζ_p^{k+1} if

$$\left(\frac{k}{p}\right)\left(\frac{k+1}{p}\right) = -1.$$

So the number of zeros of $f_p(z)$ on the unit circle is bounded below by the number of sign changes in the sequence $\{(\frac{k}{p})\}$. Conrey et al. [2000] show that the number of zeros of $f_p(z)$ on the unit circle is asymptotic to κp where κ is between 0.500668 and 0.500813.

Zeros of $f_{199}(z)$.



Research Problems

R1. It is natural to ask about the growth of the Fekete polynomials on the disk D. Montgomery [1980] shows that

$$\|f_p(z)\|_D \gg \sqrt{p}\log\log p$$

and that

$$\|f_p(z)\|_D \ll \sqrt{p}\log p.$$

Which is the correct rate of growth? Extend the above result to the shifted Fekete polynomials of E1.

Selected References

1. P. Borwein and S. Choi, *Explicit merit factor formulae for Fekete and Turyn polynomials*, Trans. Amer. Math. Soc. **354** (2002), 219–234.

2. P. Borwein, S. Choi, and S. Yazdani, *An extremal property of Fekete polynomials*, Proc. Amer. Math. Soc. **129** (2001), 19–27.

3. B. Conrey, A. Granville, B. Poonen, and K. Soundararajan, *Zeros of Fekete polynomials*, Ann. Inst. Fourier (Grenoble) **50** (2000), 865–889.

4. H.L. Montgomery, *An exponential polynomial formed with the Legendre symbol*, Acta Arith. **37** (1980), 375–380.

Chapter 6

Products of Cyclotomic Polynomials

As in Chapter 3, the *nth cyclotomic polynomial* Φ_n is the minimal polynomial of a primitive nth root of unity. Recall that Φ_n is given by

$$\Phi_n(z) = \prod_{\substack{1 \le j \le n \\ \gcd(j,n)=1}} \bigl(z - \exp(j2\pi i/n)\bigr).$$

The first six cyclotomic polynomials are

$$z-1, z+1, z^2+z+1, z^2+1, z^4+z^3+z^2+z+1, z^2-z+1.$$

Products of cyclotomic polynomials (and powers of z) are precisely the class of monic polynomials in $\mathcal{Z}$ with Mahler measure 1. Equivalently, they are exactly the monic polynomials in $\mathcal{Z}$ that have all their roots of modulus at most 1. This follows from Kronecker's theorem (see E4). So products of cyclotomic polynomials are exactly the subset of $\mathcal{Z}$ of polynomials that do not vanish at 0 and have minimal Mahler measure. One aim of this section is to characterize those polynomials with odd coefficients that have Mahler measure 1 and to explore a conjecture that characterizes when Littlewood polynomials have measure 1. All such polynomials are built from a very natural construction.

There are very few cases where we can determine the class of extremal polynomials within the Littlewood polynomials with respect to either the maximum or minimum L_p norms, though in every case this is an interesting question. The following conjecture is proved in Borwein and Choi [1999] for N odd. Some further evidence for it is presented at the end of the chapter.

Conjecture. *A Littlewood polynomial $P(z)$ of degree $N-1$ has Mahler measure 1 if and only if P can be written in the form*

$$P(z) = \pm\Phi_{p_1}(\pm z)\Phi_{p_2}(\pm z^{p_1}) \cdots \Phi_{p_r}(\pm z^{p_1 p_2 \cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct.

We now characterize the monic polynomials with measure 1 and all coefficients odd. This is the first part of establishing the above conjecture for odd N. So, for example, we show that if N is odd, then any polynomial $P(z)$ with odd coefficients of even degree $N-1$ has Mahler measure 1 if and only if

$$P(z) = \prod_{d|N, d>1} \Phi_d(\pm z).$$

The approach is via Graeffe's root powering method. Define the operator T_p for prime p as the operator on the monic polynomials that takes a polynomial P to a polynomial whose roots are the pth powers of the roots of P:

$$T_p[P(z)] := \prod_{i=1}^{N} (z - \alpha_i^p)$$

for every $P(z) := \prod_{i=1}^{N}(z-\alpha_i)$ in $\mathcal{Z}$. Note that if P is in $\mathcal{Z}$, then so is $T_p(P)$.

To discuss the factorization of polynomials with measure 1 with odd coefficients as a product of irreducible cyclotomic polynomials, we first consider the factorization over $\mathbb{Z}_p[z]$ where p is a prime number. The most useful case is $p = 2$ because every Littlewood polynomial reduces to the Dirichlet kernel $1 + z + \cdots + z^{N-1}$ in $\mathbb{Z}_2[z]$. In $\mathbb{Z}_p[z]$, $\Phi_n(z)$ is no longer irreducible in general, but $\Phi_n(z)$ and $\Phi_m(z)$ are still relatively prime to each other.

Lemma 1. *Suppose n and m are distinct positive integers relatively prime to a prime p. Then $\Phi_n(z)$ and $\Phi_m(z)$ are relatively prime in $\mathbb{Z}_p[z]$.*

Proof. Suppose e and f are the smallest positive integers such that

$$p^e \equiv 1 \pmod{n} \qquad \text{and} \qquad p^f \equiv 1 \pmod{m}.$$

Let F_{p^k} be the field of order p^k. Then F_{p^e} contains exactly $\phi(n)$ elements of order n, and over $\mathbb{Z}_p$, $\Phi_n(z)$ is a product of $\phi(n)/e$ irreducible factors of degree e, and each irreducible factor is a minimal polynomial for an element in F_{p^e} of order n over $\mathbb{Z}_p$. (See Lidl and Niederreiter [1983] and E1.) So $\Phi_n(z)$ and $\Phi_m(z)$ cannot have a common factor in $\mathbb{Z}_p[z]$, since their irreducible factors are minimal polynomials of different orders. This proves our lemma. $\square$

The following lemma tells which $\Phi_m(z)$ can possibly be factors of polynomials with odd coefficients.

Lemma 2. *Suppose $P(z)$ is a polynomial with odd coefficients of degree $N-1$. If $\Phi_m(z)$ divides $P(z)$, then m divides $2N$.*

Proof. If $\Phi_m(z)$ divides $P(z)$, then $\Phi_m(z)$ also divides $P(z)$ in $\mathbb{Z}_2[z]$. However, in $\mathbb{Z}_2[z]$, $P(z)$ equals $1 + z + \cdots + z^{N-1}$ and can be factored as

$$P(z) = \Phi_1^{-1}(z) \prod_{d \mid M} \Phi_d^{2^t}(z), \tag{1}$$

where $N = 2^t M$, $t \geq 0$, and M is odd. In view of Lemma 1, $\Phi_{d_1}(z)$ and $\Phi_{d_2}(z)$ are relatively prime in $\mathbb{Z}_2[z]$ if d_1 and d_2 are distinct odd integers. So if m is odd, then $\Phi_m(z)$ is a factor in the right-hand side of (1), and hence $m = d$ for some $d \mid M$. On the other hand, if m is even and $m = 2^l m'$ where $l \geq 1$ and m' is odd, then

$$\Phi_m(z) = \Phi_{2m'}(z^{2^{l-1}}) = \Phi_{m'}(z^{2^{l-1}}) = \Phi_{m'}^{2^{l-1}}(z)$$

in $\mathbb{Z}_2[z]$. Thus in view of (1), we must have $m' = d$ for $d \mid M$ and $l \leq t + 1$. Hence in both cases, we have m divides $2N$. □

In view of Lemma 2, every product of cyclotomic polynomials $P(z)$ with odd coefficients of degree $N - 1$ and with lead coefficient 1 can be written as

$$P(z) = \prod_{d \mid 2N} \Phi_d^{e(d)}(z), \tag{2}$$

where the $e(d)$ are nonnegative integers.

As above, for each prime p the operator T_p is defined by

$$T_p[P(z)] := \prod_{i=1}^{N} (z - \alpha_i^p)$$

for every $P(z) := \prod_{i=1}^{N} (z - \alpha_i)$ in $\mathcal{Z}$. Now $T_p[P(z)]$ is also a monic polynomial in $\mathcal{Z}$. We extend T_p to be defined over the quotient of two monic polynomials in $\mathcal{Z}$ by $T_p[(P/Q)(z)] := T_p[P(z)]/T_p[Q(z)]$. This operator obviously takes a polynomial to the polynomial whose roots are the pth powers of the roots of P. Also, we let M_p be the natural projection from $\mathcal{Z}$ onto $\mathbb{Z}_p[z]$. So,

$$M_p[P(z)] = P(z) \pmod{p}.$$

Lemma 3. *Let n be a positive integer relatively prime to p, and let i be an integer greater than 2. Then*

(a) $T_p\left[\Phi_n(z)\right] = \Phi_n(z)$,

(b) $T_p\left[\Phi_{pn}(z)\right] = \Phi_n^{p-1}(z)$,

(c) $T_p\left[\Phi_{p^i n}(z)\right] = \Phi_{p^{i-1}n}^p(z)$.

Proof. The proof of (a) is trivial because if $\gcd(n,p)=1$, then T_p just permutes the roots of $\Phi_n(z)$. To prove (b) and (c), we consider

$$T_p[P(z^p)] = T_p\left[\prod_{j=1}^{N}(z^p-\alpha_i)\right] = T_p\left[\prod_{j=1}^{N}\prod_{l=1}^{p}\left(z-e^{2\pi il/p}\alpha_i^{1/p}\right)\right]$$
$$= \prod_{j=1}^{N}\prod_{l=1}^{p}(z-\alpha_i) = P(z)^p.$$

Thus (b) and (c) follow from (a), $\Phi_{pn}(z) = \Phi_n(z^p)/\Phi_n(z)$, and $\Phi_{p^in}(z) = \Phi_{p^{i-1}n}(z^p)$ (see E1). $\square$

When $P(z)$ is a product of cyclotomic polynomials, the iterates $T_p^n[P(z)]$ converge in a finite number of steps to a fixed point of T_p, and we define this to be the fixed point of $P(z)$ with respect to T_p.

Lemma 4. *If $P(z)$ is a product of monic cyclotomic polynomials in $\mathcal{Z}$, then*

$$M_p\big[T_p[P(z)]\big] = M_p[P(z)], \tag{3}$$

in $\mathbb{Z}_p[z]$, where $M_p[P(z)] = P(z) \pmod p$ is the above natural projection.

Proof. Since both T_p and M_p are multiplicative, it suffices to consider the primitive cyclotomic polynomials $\Phi_n(z)$. Let n be an integer relatively prime to p. Then (3) is true for $P(z)=\Phi_n(z)$ by (i) of Lemma 3. For $P(z)=\Phi_{pn}(z)$, we have

$$M_p\big[T_p\left[\Phi_{pn}(z)\right]\big] = M_p\left[\Phi_n^{p-1}(z)\right] = M_p\left[\Phi_n(z)\right]^{p-1}$$

by (ii) of Lemma 3. However,

$$M_p\left[\Phi_{pn}(z)\right] = \frac{M_p\left[\Phi_n(z^p)\right]}{M_p\left[\Phi_n(z)\right]} = \frac{M_p\left[\Phi_n\right](z^p)}{M_p\left[\Phi_n(z)\right]} = M_p\left[\Phi_n(z)\right]^{p-1},$$

in $\mathbb{Z}_p[z]$. This proves that (3) is also true for $P(z)=\Phi_{pn}(z)$. Finally, if $P(z) = \Phi_{p^in}(z)$, then

$$M_p\big[T_p\left[\Phi_{p^in}(z)\right]\big] = M_p\left[\Phi_{p^{i-1}n}(z)^p\right] = M_p\left[\Phi_{p^{i-1}n}(z^p)\right] = M_p\left[\Phi_{p^in}(z)\right]$$

by (iii) of Lemma 3. This completes the proof of our lemma. $\square$

Lemma 4 shows that if $T_p[P(z)] = T_p[Q(z)]$, then $M_p[P(z)] = M_p[Q(z)]$. The next result shows that the converse is also true.

Theorem 1. *Suppose $P(0)\neq 0$. Then $P(z)$ and $Q(z)$ are monic polynomials in $\mathcal{Z}$ of Mahler measure 1, and $M_p[P(z)] = M_p[Q(z)]$ in $\mathbb{Z}_p[z]$ if and only if both $P(z)$ and $Q(z)$ have the same fixed point with respect to iteration of T_p.*

Proof. Suppose

$$P(z) = \prod_{d \in \mathcal{D}} \Phi_d^{e(d)}(z) \Phi_{pd}^{e(pd)}(z) \cdots \Phi_{p^t d}^{e(p^t d)}(z)$$

and

$$Q(z) = \prod_{d \in \mathcal{D}} \Phi_d^{e(d)'}(z) \Phi_{pd}^{e(pd)'}(z) \cdots \Phi_{p^t d}^{e(p^t d)'}(z),$$

where $t, e(j), e(j)' \geq 0$ and $\mathcal{D}$ is a set of positive integers relatively prime to p. Then using (i)–(iii) of Lemma 3, we have for $l \geq t$,

$$T_p^l[P(z)] = \prod_{d \in \mathcal{D}} \Phi_d^{f(d)}(z) \qquad \text{and} \qquad T_p^l[Q(z)] = \prod_{d \in \mathcal{D}} \Phi_d^{f(d)'}(z), \tag{4}$$

where

$$f(d) = e(d) + (p-1) \sum_{j=1}^{t} p^{j-1} e(p^j d)$$

and

$$f(d)' = e(d)' + (p-1) \sum_{j=1}^{t} p^{j-1} e(p^j d)'.$$

From Lemma 4, we have

$$M_p\left[T_p^l[P(z)]\right] = M_p[P(z)] = M_p[Q(z)] = M_p\left[T_p^l[Q(z)]\right],$$

for any $l \geq t$. From this and (4),

$$\prod_{d \in \mathcal{D}} M_p\left[\Phi_d(z)\right]^{f(d)} = \prod_{d \in \mathcal{D}} M_p\left[\Phi_d(z)\right]^{f(d)'}.$$

By Lemma 1, $M_p[\Phi_d(z)]$ and $M_p[\Phi_{d'}(z)]$ are relatively prime if $d \neq d'$. So we must have $f(d) = f(d)'$ for all $d \in \mathcal{D}$, and hence from (4), $P(z)$ and $Q(z)$ have the same fixed point with respect to T_p. $\square$

From Theorem 1, we can characterize the polynomials of Mahler measure 1 by their images in $\mathbb{Z}_p[z]$ under the projection M_p. They all have the same fixed point under T_p. In particular, when $p = 2$ we have the following.

Corollary 1. *All products of monic cyclotomic polynomials with odd coefficients of degree $N-1$ have the same fixed point under iteration of T_2. Specifically, if $N = 2^t M$ where $t \geq 0$ and $\gcd(2, M) = 1$, then the fixed point occurs at the $(t+1)$th step of the iteration and equals*

$$\left(z^M - 1\right)^{2^t} (z-1)^{-1}.$$

Proof. The first part follows directly from Theorem 1 and the fact that

$$M_2[P(z)] = 1 + z + \cdots + z^{N-1}$$

in $\mathbb{Z}_2[z]$ if $P(z)$ is a monic polynomial of degree $N-1$ with odd coefficients. If $N = 2^t M$, then from (2),

$$P(z) = \prod_{d \mid M} \Phi_d^{e(d)}(z)\Phi_{2d}^{e(2d)}(z) \cdots \Phi_{2^{t+1}d}^{e(2^{t+1}d)}(z).$$

Over $\mathbb{Z}_2[z]$,

$$1 + z + \cdots + z^{N-1} = \Phi_1(z)^{-1} \prod_{d \mid M} \Phi_d^{2^t}(z),$$

so

$$f(d) = e(d) + \sum_{i=1}^{t+1} 2^{i-1} e(2^i d) = \begin{cases} 2^t & \text{for } d \mid M, d > 1, \\ 2^t - 1 & \text{for } d = 1. \end{cases} \tag{5}$$

From (5) and Lemma 3,

$$T_2^{t+1}[P(z)] = \prod_{d \mid M} \Phi_d^{f(d)}(z) = \Phi_1(z)^{-1} \prod_{d \mid M} \Phi_d^{2^t}(z) = \left(z^M - 1\right)^{2^t} (z-1)^{-1}.$$

□

Corollary 1, when N is odd ($t = 0$), shows that $T_2[P(z)]$ equals $1 + z + \cdots + z^{N-1}$ for all polynomials of Mahler measure 1 with odd coefficients and, from (2) and (5), we have the following characterization of products of cyclotomic polynomials with odd coefficients.

Corollary 2. *Let $N = 2^t M$ with $t \geq 0$ and $\gcd(2, M) = 1$. A polynomial $P(z)$ with odd coefficients of degree $N-1$ has Mahler measure 1 if and only if*

$$P(z) = \prod_{d \mid M} \Phi_d^{e(d)}(z)\Phi_{2d}^{e(2d)}(z) \cdots \Phi_{2^{t+1}d}^{e(2^{t+1}d)}(z)$$

and the $e(d)$ satisfy condition (5).

Furthermore, if N is odd, then any polynomial $P(z)$ of even degree $N-1$ with odd coefficients has Mahler measure 1 if and only if

$$P(z) = \prod_{d \mid N,\ d>1} \Phi_d(\pm z).$$

We now compute the number of measure 1 polynomials with odd coefficients. Let $B(n)$ be the number of partitions of n into a sum of terms of the sequence $\{1, 1, 2, 4, 8, 16, \ldots\}$. Then $B(n)$ has generating function

$$F(z) = (1-z)^{-1} \prod_{k=0}^{\infty} \left(1 - z^{2^k}\right)^{-1}.$$

The next corollary follows from (5) and Corollary 2.

Corollary 3. *Let $N = 2^t M$ with $t \geq 0$ and $\gcd(2, M) = 1$. The number of polynomials of degree $N-1$ with odd coefficients that are a product of cyclotomic polynomials is*

$$C(N) = B(2^t)^{d(M)-1} \cdot B\left(2^t - 1\right), \tag{6}$$

where $d(M)$ denotes the number of divisors of M. Furthermore,

$$\log C(N) \sim \left(\frac{t^2}{2}\log 2\right)(d(M)-1) + \frac{\left(\log\left(2^t-1\right)\right)^2}{\log 4}. \tag{7}$$

Proof. Formula (6) follows from (5) and Corollary 2. To prove (7), we use the asymptotic estimation for $B(n)$ in de Bruijn [1948]:

$$B(n) \sim \exp\left(\frac{(\log n)^2}{\log 4}\right).$$

Now (7) follows from this and (6). □

The following conjecture, as observed at the beginning of this chapter, is true when N is odd. It also holds when N is a power of 2.

Conjecture. *A Littlewood polynomial $P(z)$ of degree $N-1$ has Mahler measure 1 if and only if P can be written in the form*

$$P(z) = \pm\Phi_{p_1}(\pm z)\Phi_{p_2}\left(\pm z^{p_1}\right)\cdots\Phi_{p_r}\left(\pm z^{p_1 p_2 \cdots p_{r-1}}\right),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct.

This holds up to degree 190. The computation is based on computing all products of cyclotomic polynomials with odd coefficients of a given degree, checking which ones are actually Littlewood polynomials, and then seeing that this set matches the set generated by the conjecture. For example, for $N-1 = 143$ there are 6773464 polynomials with odd coefficients that are products of cyclotomic polynomials, and of these 416 are Littlewood. For $N-1 = 191$ there are 697392380 polynomials with odd coefficients that are products of cyclotomic polynomials (which was too big for our program).

We can generate all the measure 1 polynomials with odd coefficients of a fixed degree from Corollary 2 quite easily, so the bulk of the work is involved in checking which ones have height 1. The set in the conjecture can be computed very easily recursively.

Introductory Exercises

E1. Basic Properties of Cyclotomic Polynomials. A *primitive nth root of unity* is a complex number ω that satisfies $\omega^n = 1$ and $\omega^k \neq 1$ for any positive $k < n$. Let $\zeta_n := \exp(2\pi i/n)$; then ζ_n is a primitive nth root of unity. The $\phi(n)$ primitive nth roots of unity are $\{\zeta_n^m : \gcd(m, n) = 1\}$.

The nth cyclotomic polynomial Φ_n is the minimal polynomial of any primitive nth root of unity. This is an irreducible polynomial of degree $\phi(n)$ given by

$$\Phi_n(z) = \prod_{\substack{1 \leq j \leq n \\ \gcd(j,n)=1}} \big(z - \exp(j2\pi i/n)\big).$$

Show that

$$z^n - 1 = \prod_{d|n} \Phi_n(z).$$

Show that

$$\Phi_{p^n}(z) = \Phi_p\left(z^{p^{n-1}}\right),$$

and more generally, if every prime that divides m also divides n, then

$$\Phi_{mn}(z) = \Phi_n(z^m).$$

Show that for odd n,

$$\Phi_n(-z) = \Phi_{2n}(z).$$

Show that if p is a prime not dividing an integer n, then

$$\Phi_{pn}(z) = \Phi_n(z^p)/\Phi_n(z).$$

Show, with μ defined as in E2, that

$$\Phi_n(z) = \prod_{d|n} (z^d - 1)^{\mu(n/d)}.$$

Show that

$$\Phi_{p^k}(1) = p$$

if p is a prime and that $\Phi_n(1) = 1$ if n is not a power of a prime. Also show that

$$\Phi_{2p^k}(-1) = p$$

if p is a prime, $\Phi_1(-1) = -2$, $\Phi_2(-1) = 0$, and that $\Phi_n(-1) = 1$ otherwise.

If p is a prime not dividing n, then Φ_n factors in $\mathbb{Z}_p[z]$ into $\phi(n)/d$ irreducible factors, each of degree d, where d is the smallest positive integer solution of $p^d \equiv 1 \pmod{n}$. See Lidl and Niederreiter [1983].

E2. The Möbius μ Function and the Euler ϕ Function. The Möbius μ function is defined by

$$\begin{cases} \mu(1) = 1, & \\ \mu(n) = 0 & \text{if } p^2 \text{ divides } n \text{ for some prime } p, \\ \mu(n) = (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes.} \end{cases}$$

Show that μ is *multiplicative;* that is, $\mu(ab) = \mu(a)\mu(b)$ if $\gcd(a, b) = 1$.

The Euler ϕ function counts the number of integers less than or equal to n that are relatively prime to n. So $\phi(n) := |\{1 \le m \le n : \gcd(m, n) = 1\}|$. Show that ϕ is multiplicative and that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right),$$

where $p_1, p_2, \ldots, p_k$ are the distinct prime factors of n.

Show that

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

E3. Norm and Trace. Recall that the *norm* of an algebraic number α is just the product of all the roots of the minimal polynomial, while the *trace* is the sum of all the roots. Denote the norm of α by $N(\alpha)$ and the trace by $T(\alpha)$. For an algebraic integer, the norm is just the constant term of the minimal polynomial multiplied by $(-1)^d$, where d is the degree of the minimal polynomial. The trace is -1 times the coefficient of the term of degree $d - 1$.

As in E1, let $\zeta_n := \exp(2\pi i/n)$. Show that if p is an odd prime, then $N(\zeta_{p^k}) = 1$ and $N(\zeta_p - 1) = p$.

E4. Prove *Kronecker's theorem:* If $p \in \mathcal{Z}$ is monic, $p(0) \neq 0$, and p has all its roots in the set $\{|z| \le 1\}$, then all the roots of p are roots of unity.

Hint: First prove that there are at most $n(2H + 1)^n$ algebraic numbers of height H and degree n. (The height of an algebraic number is the height of its minimal polynomial.) Let α be any root of p and suppose p is of degree n and height H. Note that α^m is of degree at most n and height at most $2^n H$ by E10 of Chapter 3. Conclude that $\alpha^m = \alpha^k$ for some m and k and hence that α is a root of unity. $\square$

E5. Prove that every $p \in \mathcal{L}_{100}$ is irreducible. Prove that if $n + 1$ is not prime, then some $p \in \mathcal{L}_n$ is reducible. (Can you find a condition on $n + 1$ such that every $p \in \mathcal{L}_n$ is irreducible?)

Computational Problems

C1. Design an efficient algorithm to compute $\Phi_n(z)$ using the formulae of E1.

C2. Find the first n for which $\Phi_n(z)$ has height 2 and the first n for which $\Phi_n(z)$ has height 3.

The growth of the coefficients of $\Phi_n(z)$ is interesting. The situation for small n is misleading. Erdős proved that for every k, $H(\Phi_n) > n^k$ for infinitely many n, and Maier [1996] showed that this holds for a set of positive density.

C3. Write an efficient algorithm based on Graeffe's method to determine whether a polynomial is a product of cyclotomic factors.

C4. Implement an algorithm that inverts Graeffe's root squaring method (in the sense that it determines the set of polynomials in $\mathcal{Z}$ that map to a given p in $\mathcal{Z}$ under root squaring).

Use this in conjunction with Corollary 2 to compute all polynomials of a given degree of measure 1 with all odd coefficients. Similarly, use it to compute all Littlewood polynomials of measure 1 of a given degree.

C5. Assume the conjecture of this section. Based on it, implement an algorithm to compute all Littlewood polynomials of degree less than 200 that are products of cyclotomic polynomials.

Research Problems

R1. Prove the conjecture of this section for N even.

R2. Is there a characterization of all measure 1 polynomials with coefficients just 0 and 1?

Selected References

1. P. Borwein and S. Choi, *On cyclotomic polynomials with* ± 1 *coefficients*, Experiment. Math. **8** (1999), 399–407.

2. R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

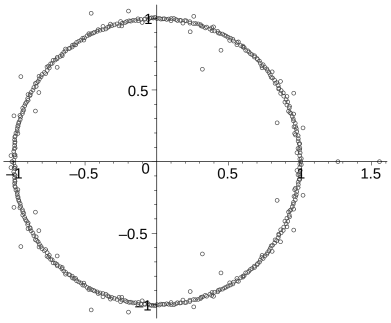
3. M. Mignotte and D. Ştefănescu, *Polynomials. An Algorithmic Approach*, Springer-Verlag Singapore, Singapore, 1999.

Chapter 7

Location of Zeros

We are interested in the zeros of polynomials with restricted coefficients. A typical restriction is that the first coefficient dominates the other coefficients—as is the case in $\mathcal{F}_n$, $\mathcal{L}_n$, and $\mathcal{A}_n$. However, none of the results of this section are about polynomials with integer coefficients specifically.

Zeros of a typical element of $\mathcal{L}_{500}$.



As is apparent from the graphic above, the zeros of a typical Littlewood polynomial are far from randomly distributed ("typical" in this case means that the choice of sign of the coefficients is random). This chapter and the next two chapters discuss various aspects of this phenomenon.

The following result of Schur (rediscovered with a shorter proof by Erdős and Turán [1950]) is a prototype for the results we have in mind. In general, it is a sharp result. However, in the cases we are most interested in, there is an extra logarithm that is dealt with in Theorem 5.

***Theorem* (Schur).** *If $p(z) := \sum_{j=0}^{n} a_j z^j$ has m positive real zeros, then*

$$m^2 \le 2n \log \left(\frac{|a_0| + |a_1| + \cdots + |a_n|}{\sqrt{|a_0 a_n|}} \right).$$

In this same paper, Erdős and Turán discuss the angular distribution of the zeros of polynomials in terms of the size of the coefficients. Informally, the results they prove say that "if the middle coefficients of a polynomial are not too large compared with the extreme ones," then the angular distribution of the zeros is uniform. See also Theorem 2 below.

In the first two references for this section we prove a variety of sharpenings of Schur's result and the results of Erdős and Turán. We now state some of these results. The first result shows that the bulk of the zeros of low-height polynomials are close to the unit circle and gives precise quantitative estimates.

Theorem 1. *Every polynomial p of the form*

$$p(z) = \sum_{j=0}^{n} a_j z^j, \quad |a_0| = 1, \quad |a_j| \le 1, \quad a_j \in \mathbb{C},$$

has at most $c\sqrt{n}$ zeros inside any polygon with vertices on the unit circle, where the constant c depends only on the polygon.

A version of this theorem is proved as Theorem 5 of this section. The next two theorems tell us something about the distribution of the zeros.

Theorem 2. *There is an absolute constant c such that*

$$p(z) = \sum_{j=0}^{n} a_j z^j, \quad |a_0| = |a_n| = 1, \quad |a_j| \le 1, \quad a_j \in \mathbb{C},$$

has at most $c(n\alpha + \sqrt{n})$ zeros in the strip

$$\{z \in \mathbb{C} : |\operatorname{Im}(z)| \le \alpha\},$$

and at most $c(n\alpha + \sqrt{n})$ zeros in the sector

$$\{z \in \mathbb{C} : |\arg(z)| \le \alpha\}.$$

Theorem 3. *Let $\alpha \in (0,1)$. Every polynomial p of the form*

$$p(z) = \sum_{j=0}^{n} a_j z^j, \quad |a_0| = 1, \quad |a_j| \le 1, \quad a_j \in \mathbb{C},$$

has at most c/α zeros inside any polygon with vertices on the circle

$$\{z \in \mathbb{C} : |z| = 1 - \alpha\},$$

where the constant c depends only on the number of the vertices of the polygon.

The sharpness of Theorem 1 is given in the following result.

Theorem 4. *For every $n \in \mathbb{N}$, there exists a polynomial p_n of the form given in Theorem 1 with real coefficients such that p_n has a zero at 1 with multiplicity at least $\lfloor\sqrt{n}\rfloor - 1$.*

Theorem 5. *Every polynomial p of the form*

$$p(z) = \sum_{j=0}^{n} a_j z^j, \quad |a_0| = 1, \quad |a_j| \le 1, \quad a_j \in \mathbb{C},$$

has at most $\lfloor \frac{16}{7}\sqrt{n} \rfloor + 5$ zeros at 1.

The key to the proof of Theorem 5 is the following lemma.

Lemma 1. *For every positive integer n, there exists a $q \in \mathcal{P}_m$ with*

$$m \le \lfloor \tfrac{16}{7}\sqrt{n} \rfloor + 4$$

such that

$$q(0) > |q(1)| + |q(2)| + \cdots + |q(n)|.$$

Proof. Let

$$k := \lfloor \tfrac{4}{7}\sqrt{n} \rfloor + 1$$

and

$$g(z) := \frac{1}{2}T_0(z) + T_1(z) + T_2(z) + \cdots + T_k(z),$$

where as usual, T_i denotes the Chebyshev polynomial of degree i. (See the exercises.) We have $g(1) = k + \frac{1}{2}$, and for $0 < t \le \pi$,

$$g(\cos t) = \frac{1}{2} + \cos t + \cos 2t + \cdots + \cos kt = \frac{\sin\left(k+\frac{1}{2}\right)t}{2\sin\frac{t}{2}} = \frac{\sin\left(k+\frac{1}{2}\right)t}{\sqrt{2(1-\cos t)}}$$

and

$$|g(z)| \le \frac{1}{\sqrt{2(1-z)}}, \quad z \in [-1, 1).$$

Let

$$q(z) := \left(g\left(1 - \tfrac{2}{n}z\right)\right)^4.$$

Then $q \in \mathcal{P}_m$ with $m = 4k \le \lfloor \frac{16}{7}\sqrt{n} \rfloor + 4$ and

$$|q(1)| + |q(2)| + \cdots + |q(n)| \le \sum_{j=1}^{n} \left(\frac{4j}{n}\right)^{-2} = \frac{n^2}{16}\sum_{j=1}^{n}\frac{1}{j^2} < \frac{\pi^2}{96}n^2 < k^4 < q(0),$$

and the proof is finished. □

Proof of Theorem 5. If p has a zero at 1 of multiplicity m, then for every polynomial $q \in \mathcal{P}_{m-1}^c$, we have

$$a_0 q(0) + a_1 q(1) + \cdots + a_n q(n) = 0. \tag{1}$$

(This is proved by considering the cases $q(z) := z^i$ for $i = 0, 1, \dots, m-1$.) Lemma 1 constructs a polynomial q of degree at most

$$m \le \lfloor \tfrac{16}{7}\sqrt{n} \rfloor + 4$$

for which

$$q(0) > |q(1)| + |q(2)| + \cdots + |q(n)|.$$

Equality (1) cannot hold with this q, so the multiplicity of the zero of p at 1 is at most one more than the degree of q. □

Introductory Exercises

E1. The *Chebyshev polynomials* are defined, for $x \in [-1, 1]$, by

$$T_n(x) := \cos(n \arccos x).$$

(a) Show, for complex z, that

$$\begin{aligned} T_n(z) &:= \frac{1}{2}\left(\left(z + \sqrt{z^2-1}\right)^n + \left(z - \sqrt{z^2-1}\right)^n\right) \\ &= \frac{n}{2}\sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{(n-k-1)!}{k!\,(n-2k)!}(2z)^{n-2k}. \end{aligned}$$

(b) The nth Chebyshev polynomial has the following equioscillation property. At the $n+1$ points $\lambda_j := \cos(j\pi/n)$ in $[-1, 1]$,

$$T_n(\lambda_j) = (-1)^{n-j}\|T_n\|_{[-1,1]} = (-1)^{n-j}, \quad j = 0, 1, \dots, n.$$

Observe that the zeros of T_n are precisely the points

$$x_k = \cos\tfrac{(2k-1)\pi}{2n}, \quad k = 1, 2, \dots, n.$$

(c) Show that

$$T_{nm}(z) = T_n\big(T_m(z)\big)$$

and that T_n satisfies the three-term recursion

$$T_n(z) = 2zT_{n-1}(z) - T_{n-2}(z), \quad n = 2, 3, \dots.$$

(d) Verify that $T_0(z) = 1$, $T_1(z) = z$, $T_2(z) = 2z^2 - 1$, $T_3(z) = 4z^3 - 3z$, $T_4(z) = 8z^4 - 8z^2 + 1$, and $T_5(z) = 16z^5 - 20z^3 + 5z$.

The *Chebyshev polynomials of the second kind* are defined by

$$U_{n-1}(z) := \frac{1}{n}T_n'(z) = \frac{\sin n\theta}{\sin\theta}, \quad z = \cos\theta.$$

(e) Show that

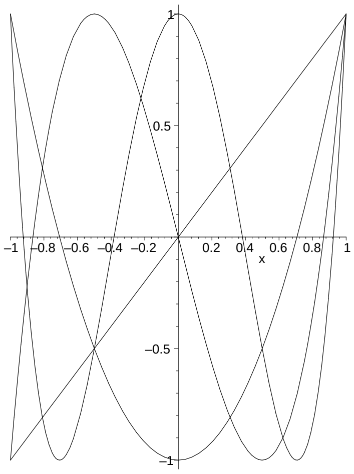
$$U_0(z) = 1, \quad U_1(z) = 2z, \quad U_n(z) = 2zU_{n-1}(z) - U_{n-2}(z), \quad n = 2, 3, \dots.$$

E2. Show that the Chebyshev polynomial T_n satisfies the following extremal property:

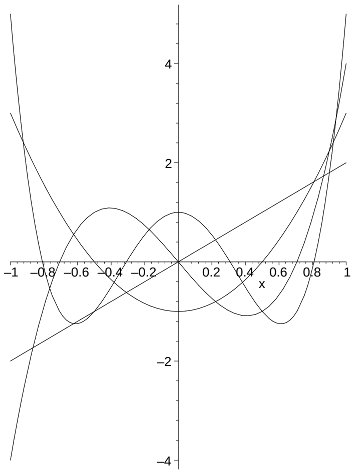
$$\min_{p \in \mathcal{P}^c_{n-1}} \|x^n - p(x)\|_{[-1,1]} = \|2^{1-n}T_n\|_{[-1,1]} = 2^{1-n},$$

where the minimum is uniquely attained by $p(x) = x^n - 2^{1-n}T_n(x)$.

The first four Chebyshev polynomials of the first kind.



The first four Chebyshev polynomials of the second kind.



E3. What is the closure of the set of all zeros of all polynomials of the form

$$p(z) = \sum_{j=0}^{n} a_j z^j, \quad |a_0| = 1, \quad |a_j| \le 1, \quad a_j \in \mathbb{C}?$$

Research Problems

The following conjecture is in Erdélyi [2001a].

R1. Establish whether every polynomial $p \in \mathcal{L}_n$ has at least one zero in the annulus

$$\left\{1 - \frac{c}{n} < |z| < 1 + \frac{c}{n}\right\},$$

where $c > 0$ is an absolute constant.

Selected References

1. P. Borwein and T. Erdélyi, *On the zeros of polynomials with restricted coefficients*, Illinois J. Math. **41** (1997), 667–675.

2. P. Borwein, T. Erdélyi, and G. Kós, *Littlewood-type problems on* $[0, 1]$, Proc. London Math. Soc. (3) **79** (1999), 22–46.

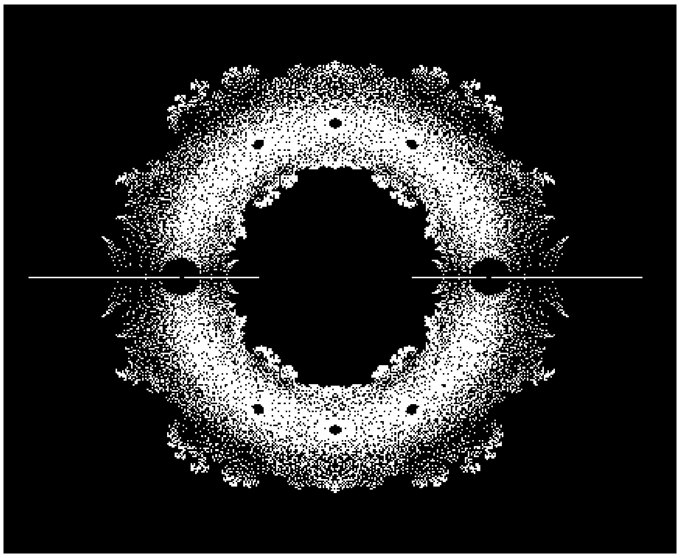
3. P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Ann. of Math. (2) **51** (1950), 105–119.

Chapter 8

Maximal Vanishing

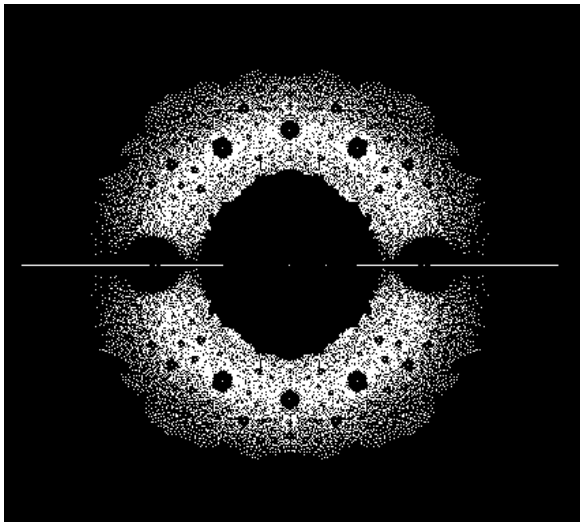
The location of the zeros of Littlewood polynomials and related classes of low-height polynomials is subtle and interesting. The zeros cluster heavily around the unit circle and appear to form a set with fractal boundary.

The zeros of all degree 12 polynomials with $\{+1, -1\}$ coefficients.



This graphic suggests various questions. What is the nature of the boundary? This is discussed further in the exercises. What is the structure of the "holes"?

Zeros of all polynomials with $\{0, +1, -1\}$ coefficients of degree 8.



In this chapter we are interested in possible repeated zeros of polynomials in the classes $\mathcal{A}_n$, $\mathcal{L}_n$, and $\mathcal{F}_n$, and we address the problem for each of these classes. Specifically, we address P13 and P14 and ask what is the minimal degree of a polynomial in each of the above classes with high-order vanishing at ± 1. In the next chapter we examine the size of the holes.

We first address the problem of maximal vanishing in $\mathcal{L}_n$.

P14. Multiplicity of Zeros in $\mathcal{L}_n$. *What is the maximum multiplicity of the vanishing at* 1 *of a polynomial in* $\mathcal{L}_n$*?*

Boyd [1997] shows that there is an absolute constant c such that every $p \in \mathcal{L}_n$ can have at most $c \log^2 n / \log\log n$ zeros at 1. See E6 and E7. Since

$$(1-z)\left(1-z^2\right)\left(1-z^4\right)\cdots\left(1-z^{2^{d-1}}\right)$$

is in $\mathcal{L}_{2^d-1}$, there are examples in $\mathcal{L}_n$ where the vanishing is $O(\log n)$. It would be of interest to know what the right order of maximal vanishing is. One key technique is to look at the polynomials in $\mathcal{L}_n$ taken modulo 2. Then every element of $\mathcal{L}_{n-1} \pmod 2$ is just $d_n(z) := 1 + z + \cdots + z^{n-1}$. The factorization of $d_n \pmod 2$ is known. If $n = 2^t M$ where $t \geq 0$ and $\gcd(2, M) = 1$, then

$$d_n(z) = \left(z^M - 1\right)^{2^t} (z-1)^{-1} \pmod 2.$$

It is now reasonable to search for the maximal vanishing of a $p \in \mathcal{L}_{n-1}$ where n is divisible by a large power of 2. It had been incorrectly conjectured that for each n,

$$(1-z)\left(1-z^2\right)\left(1-z^4\right)\cdots\left(1-z^{2^{n-1}}\right)$$

is the Littlewood polynomial of smallest degree with a zero of order n at 1. Boyd [1997] shows that this is true for n up to 6 but fails for $n = 6$ and therefore fails for all higher n. He gives an example of degree 47 ($n + 1 = 3 \cdot 2^4$) with a zero of order 6 at 1.

The next lemma is central to understanding why polynomials in $\mathcal{F}$ with high vanishing at 1 must have many cyclotomic factors.

Lemma 1. *If $(z-1)^m \mid f(z)$ and p is a prime number satisfying*

$$\frac{\log p}{p-1} > \frac{\log L(f)}{m},$$

then $\Phi_p(z) \mid f(z)$.

Proof. Let $\zeta_p = \exp(2\pi i/p)$, and let $N(\alpha)$ denote the norm of the algebraic number α. (Recall that the norm of an algebraic number is just the product of all the roots of the minimal polynomial; for an algebraic integer the norm is, up to sign, just the constant term of the minimal polynomial. See E3 of Chapter 6.) Since $N(\zeta_p - 1) = p$, we have that $p^m \mid N\big(f(\zeta_p)\big)$, so if $f(\zeta_p) \neq 0$, then $\big|N\big(f(\zeta_p)\big)\big| \geq p^m$. By the triangle inequality, $\big|N\big(f(\zeta_p)\big)\big| \leq L(f)^{p-1}$, so $f(\zeta_p) \neq 0$ implies that $\log(p)/(p-1) \leq \log\big(L(f)\big)/m$. This proves the theorem. $\square$

This can be refined to the following result.

Theorem 1. *Suppose $f(z)$ is a polynomial having degree d, height 1, and a zero of order m at $z = 1$. Let $p \leq m+1$ be an odd prime number, and let $q = \lfloor m/(p-1) \rfloor$.*

If $q = 1$ and $d \leq (p^2-5)/2$, then $\Phi_p(z) \mid f(z)$.

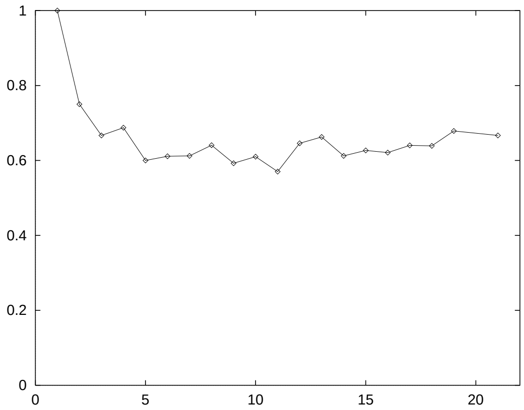
If $q > 1$ and $d \leq p(p^q+1)/2 - 2$, then $\Phi_p(z) \mid f(z)$.

This is in Borwein and Mossinghoff [2000a], which is a computational exploration of P13 (the problem of determining the maximal vanishing at 1 of a polynomial in $\mathcal{F}_n$).

P13. Multiplicity of Zeros of Height One Polynomials. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{F}_n$?*

This is solved exactly up to and including vanishing of order 12, and good examples are found up to order 21. The following is a plot of d/m^2 versus d, where d is the degree of the smallest example we could find with a zero of order m at 1.

Plot of d/m^2 versus d for smallest known d where $(1-z)^m$ divides some $p \in \mathcal{F}_d$.



It is known that the optimal examples satisfy

$$1 \ll d/m^2 \ll \log m.$$

The lower bound is Theorem 5 of the last chapter. The upper bound is a box principle argument and is left as E5. This leaves a small but very interesting amount of ambiguity in what is best possible in P13. The flatness of the plot is intriguing. This problem is related both to the Erdős–Szekeres problem of Chapter 13 and the Prouhet–Tarry–Escott problem of Chapter 11. From the point of view of Chapter 13, it is interesting to note that all the minimal examples of Borwein and Mossinghoff [2000a] factor as products of the form

$$(1 - z^{\alpha_1})(1 - z^{\alpha_2}) \cdots (1 - z^{\alpha_d}).$$

It would be very surprising if this were always true, but this too is not known.

Also of interest is the possible vanishing of height 1 polynomials within the unit disk. Is it possible for such a polynomial to have a zero of arbitrarily high multiplicity in the unit disk? See R2 below. A negative answer to the above question, for the most part, resolves Lehmer's conjecture (P9) on Mahler's measure. See E2. It seems quite likely that such high-order zeros can exist, but this is open.

In $\mathcal{L}_n$ and $\mathcal{F}_n$ the possible vanishing at 1 and -1 is the same, but in $\mathcal{A}_n$, where there can be no vanishing at 1, the right question to address is the vanishing at -1. It is easy to prove that a polynomial $p \in \mathcal{A}_n$ can have at most $\log_2 n$ zeros at -1. This is left as an exercise. Since the polynomial

$$(1+z)\left(1+z^3\right)\left(1+z^7\right)\cdots\left(1+z^{2^n-1}\right)$$

has a zero of order n at -1, the cognate question for polynomials in $\mathcal{A}_n$ is, at least up to order of growth, answered. A better example than the one above is discussed in E1.

Introductory Exercises

E1. Show that if $p \in \mathcal{A}_n$ has a zero of multiplicity m at -1, then 2^m divides $L(p)$. So a polynomial $p \in \mathcal{A}_n$ can have at most $\log_2 n$ zeros at -1.

Recursively define a sequence $\{a_i\}$ of odd integers by $a_1 := 1$ and let a_{k+1} be the smallest odd integer greater than $a_1 + a_2 + \cdots + a_k$. This is the sequence $\{1, 3, 5, 11, 21, \ldots\}$. Show that

$$U_n := (1 + z^{a_1})(1 + z^{a_2}) \cdots (1 + z^{a_n})$$

is in $\mathcal{A}$ and has a zero of order n at -1 and that the degree of U_n is less than 2^{n+1}. Show that if d_n is the degree of U_n, then $d_n/2^n \to \frac{4}{3}$ from below.

The best asymptotic known for the degrees of polynomials in $\mathcal{A}$ with zeros of multiplicity n at -1 is currently $(103/96)2^n$.

For $n \leq 5$ the polynomials U_n are polynomials of minimal degree in $\mathcal{A}$ with a zero of multiplicity n at -1, though for $n = 5$ the example is not unique. For $n = 6$ the polynomial

$$\left(1+z^1\right)\left(1+z^3\right)\left(1+z^5\right)\left(1+z^7\right)\left(1+z^{13}\right)\left(1+z^{17}\right)\, h(z),$$

where

$$\begin{aligned} h(z) := {} & z^{30} - z^{27} + z^{26} - z^{25} + z^{24} - z^{23} + z^{22} - z^{21} + 2z^{20} \\ & - z^{19} + z^{18} - 2z^{17} + z^{16} - z^{15} + z^{14} - 2z^{13} + z^{12} \\ & - z^{11} + 2z^{10} - z^9 + z^8 - z^7 + z^6 - z^5 + z^4 - z^3 + 1, \end{aligned}$$

is in $\mathcal{A}_{76}$ and has a zero of order 6 at -1. Note that U_6 is of degree 84. Thus for all $n \geq 6$ the polynomials U_n are not minimal-degree elements of $\mathcal{A}$ with a zero of multiplicity n at -1. See Borwein and Mossinghoff [to appear] where a sequence with degree asymptotic to $(103/96)2^n$ (as above) is given.

E2. Prove that if a polynomial p of height 1 has Mahler measure less than $2^{1/n}$ and a zero at α, then there exists a height 1 polynomial with a zero of order n at α. (Use E8 of Chapter 3.)

E3. Show that the zeros of all Littlewood polynomials are dense in a neighbourhood of 1. (So some of the holes in the first and second figures of this chapter get filled in eventually.) This kind of result is explored in Odlyzko and Poonen [1993]. By their methods one can show that the set of all zeros is dense in some neighbourhood of each point where $|z| = 1$.

E4. Suppose that $p \in \mathcal{A}_n$ for some n and $p(2)$ is prime. Show that p is irreducible.

Hint: To do this, first prove the following result of Pólya and Szegő. Suppose p is a polynomial in $\mathcal{Z}$ and suppose, for some positive integer m, that $p(m) = q$, where q is prime, and $p(m-1) \neq 0$. If all the roots of p have real part less than $m - \frac{1}{2}$, then p is irreducible. See Brillhart, Filaseta, and Odlyzko [1981]. □

E5. Show that there is a constant c such that for each m there is a polynomial in $\mathcal{F}_d$ that has a zero of order m at 1 and satisfies

$$d < cm^2 \log m.$$

Hint: Suppose p and q are both in $\mathcal{A}_d$ and satisfy $p^{(i)}(1) = q^{(i)}(1)$ for $i = 0, 1, \ldots, h$. Then $p-q \in \mathcal{F}_d$ has a zero of order $h+1$ at 1. Now do a box principle argument. Count the number of different vectors $\{p(1), p^{(2)}(1), \ldots, p^{(h)}(1)\}$ and choose d such that $2^{d+1} - 1$ (the size of $\mathcal{A}_d$) is larger than this estimate. □

The next two exercises follow Boyd [1997].

E6. Show that if $p \in \mathcal{L}_n$ and $q \in \mathcal{L}_m$ and $q(z)$ divides $p(z)$, then m divides n.

Hint: Suppose $n = am + b$, with $0 \le b < m$. Let

$$d_n(z) := 1 + z + \cdots + z^{n-1}.$$

So

$$d_n(z) = d_m(z) d_a(z^m) + d_b(z).$$

Since $p(z) \equiv d_n(z)$ and $q(z) \equiv d_m(z)$ modulo 2,

$$p(z) \equiv q(z) d_a(z^m) + d_b(z) \pmod 2.$$

So if $q(z)$ divides $p(z)$, then $q(z)$ must divide $p(z)$ over $\mathbb{Z}_2[z]$. But $d_b(z)$ vanishes over $\mathbb{Z}_2[z]$ only when $b = 0$. □

E7. Show that there is an absolute constant c such that every $p \in \mathcal{L}_n$ can have at most $c \log^2 n / \log\log n$ zeros at 1.

Hint: Use E6 and Lemma 1. □

E8. There is a question of Erdős dating from 1931 with a \$500 prize attached to it. See Guy [1981] and Elkies [1986]. It is related to E1. It may be formulated as a question about polynomials as follows.

P15. Another Erdős Problem. Establish whether there is a positive constant c such that if

$$V_n := \left(1 + z^{b_1}\right)\left(1 + z^{b_2}\right) \cdots \left(1 + z^{b_n}\right)$$

is in $\mathcal{A}$, then

$$\max\{b_i\} > c\, 2^n.$$

Note that $V_n \in \mathcal{A}$ is equivalent to all the sums of distinct elements from $\{b_1, b_2, \ldots, b_n\}$ being distinct.

Show that in the notation of P15,

$$\max\{b_i\} > \frac{c\,2^n}{n}.$$

It is known that it is possible to replace $c\,2^n/n$ by $c\,2^n/\sqrt{n}$ in the above inequality.

Computational Problems

C1. Find polynomials of height 1 with zeros of multiplicity 2 and 3 and, if possible, 4 at some points in $(1,2)$. (See E2.) It is open as to whether this is possible for multiplicity greater than 4.

C2. For each m, find the smallest d such that each of $\mathcal{F}_d$, $\mathcal{L}_d$, and $\mathcal{A}_d$ has an element that is divisible by $(1+z)^m$. In each case, do this for as many m as possible. Do the same calculations looking for reciprocal p in each of $\mathcal{F}_d$, $\mathcal{L}_d$, and $\mathcal{A}_d$ divisible by $(1+z)^m$. (It seems likely that extremals should be reciprocal, but this is not known.)

Research Problems

Odlyzko raised the next question after observing computationally that there is no $p \in \mathcal{A}_n$ with $n \le 25$ that has a repeated root of modulus greater than 1.

R1. Prove or disprove that a polynomial $p \in \mathcal{A}_n$ has all its repeated zeros at 0 or on the unit circle.

R2. Can the multiplicity of a zero of a height 1 polynomial in $\{z \in \mathbb{C} : 0 < |z| < 1\}$ be arbitrarily large?

R3. Is it true that there is an absolute constant $c > 0$ such that every $p \in \mathcal{A}_n$ with $p(0) = 1$ has at most $c \log n$ *real* zeros? If not, what is the best possible upper bound for the number of *real* zeros of polynomials $p \in \mathcal{A}_n$? What is the best possible upper bound for the number of *distinct real* zeros of polynomials $p \in \mathcal{A}_n$?

The above three problems are all raised in Borwein and Erdélyi [1996b].

Selected References

1. P. Borwein and M. Mossinghoff, *Polynomials with height* 1 *and prescribed vanishing at* 1, Experiment. Math. **9** (2000), 425–433.

2. P. Borwein and M. Mossinghoff, *Newman polynomials with prescribed vanishing and integer sets with distinct subset sums*, Math. Comp. (to appear).

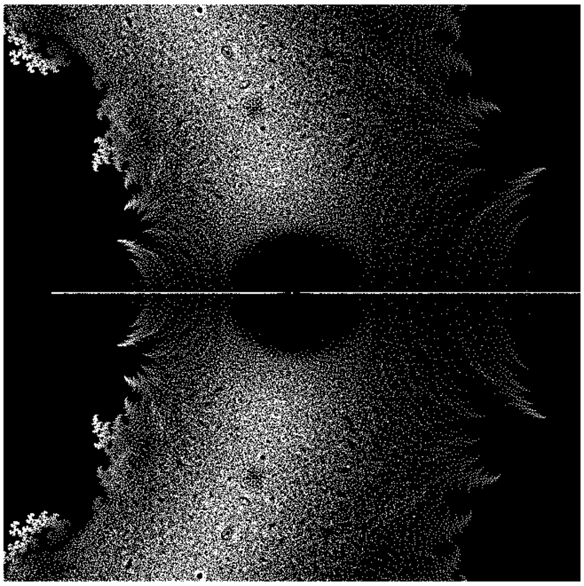
3. D. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comp. **66** (1997), 1697–1703.

4. A. Odlyzko and B. Poonen, *Zeros of polynomials with* 0, 1 *coefficients*, Enseign. Math. (2) **39** (1993), 317–348.

Chapter 9

Diophantine Approximation of Zeros

Detail around 1 of zeros of all degree 15 polynomials with $\{+1,-1\}$ coefficients.



We are concerned with how closely we can approximate an algebraic number by zeros of height 1 polynomials. This, at least in part, will tell us the size of the holes in graphics like the one above. For Pisot numbers and roots of unity, we can give quite precise answers. The main theorem of this section, taken from Borwein and Pinner [1997], gives good Diophantine estimates from below. With it, we get results like the following.

Let $\mathcal{B}_N$ denote the set of roots of all $\{0, +1, -1\}$ polynomials of degree at most N and let $\mathcal{B}_N(\alpha, k)$ denote the set of roots of those polynomials that have a zero of order at most k at α. For a Pisot number α in $(1, 2]$,

$$\min_{\beta \in \mathcal{B}_N \setminus \{\alpha\}} |\alpha - \beta| \asymp \frac{1}{\alpha^N},$$

and for α a dth root of unity,

$$\min_{\beta \in \mathcal{B}_N(\alpha,k) \setminus \{\alpha\}} |\alpha - \beta| \asymp \frac{1}{N^{(k+1)\lceil \frac{1}{2}\phi(d) \rceil + 1}}.$$

Here ϕ is the usual Euler ϕ function, and $a_n \asymp b_n$ means that a_n/b_n is bounded above and below by positive constants.

When $\alpha = 1$ and the multiplicity k of the root at 1 is restricted to 0 or 1, we can be very precise:

$$\min_{\beta \in \mathcal{B}_N(1,0) \setminus \{1\}} |1 - \beta| \sim \frac{4}{N^2}, \qquad \min_{\beta \in \mathcal{B}_N(1,1) \setminus \{1\}} |1 - \beta| \sim \frac{32}{N^3}.$$

(See E3.)

The main theorem concerns approximation by zeros of elements of $\mathcal{F}$, the height 1 polynomials.

Theorem 1. *Let α be a fixed algebraic number. Let F be a height 1 polynomial of degree N with a root of order $k \geq 0$ at α and any m (not necessarily distinct) roots $\beta_1, \ldots, \beta_m$ not equal to α. (Note that $k = 0$ is possible, in which case α is not a root of F.)*

Then, for fixed α, k, and m, there is a positive constant $c_1 = c_1(m, k, \alpha)$ such that

$$|\alpha - \beta_1| \cdots |\alpha - \beta_m| \geq \frac{c_1}{M(\alpha)^{\delta N} (N+1)^{c_2 + m\epsilon}}.$$

Here $\delta := 1$ if α is real, and $\delta := \frac{1}{2}$ otherwise.

Also, $\epsilon := 0$ if $|\alpha| \neq 1$ and $\epsilon := 1$ if $|\alpha| = 1$. Furthermore,

$$c_2 = c_2(k, \alpha) := \delta(k+1) d_1,$$

where d_1 denotes the number of conjugates of α (including α) that lie on the unit circle.

When α is an nth root of unity,

$$c_1(m, k, \alpha) = (k!)^{\lceil \frac{1}{2}\phi(n) \rceil} e^{-m},$$

where ϕ is the Euler ϕ function.

The case $m = 1$ in the above theorem is often the most interesting. Note that by Theorem 3 of Chapter 7, if F is a height 1 polynomial of degree N with a root of order $k \geq 0$ at α where $|\alpha| \neq 1$, then the multiplicity of α is bounded independently of N, while if $|\alpha| = 1$, then by Theorem 5 of Chapter 7, the multiplicity of α is bounded by $c\sqrt{n}$. The following corollary is now immediate.

Corollary 1. *For a fixed algebraic number α, any root $\beta \neq \alpha$ of a height 1 polynomial of degree N satisfies*

$$|\alpha - \beta| > \exp(-c(\alpha)N + O(\log N)), \qquad c(\alpha) := \delta \log M(\alpha),$$

if α is not a root of unity ($\delta := 1$ if α is real and $\delta := \frac{1}{2}$ if α is not real). Otherwise,

$$|\alpha - \beta| > \exp\left(-c(\alpha)\sqrt{N}\log N + O(\sqrt{N})\right), \qquad c(\alpha) := \frac{8}{7}\left\lceil \frac{1}{2}\phi(n)\right\rceil,$$

if α is an nth root of unity.

In the other direction we have the following result.

Theorem 2. *If α is a fixed real number in $(1, 2]$, then there exists a positive constant $c(\alpha)$ such that for each N, there is a height 1 polynomial of degree N with a real root $\beta \neq \alpha$ such that*

$$|\alpha - \beta| \leq \frac{c(\alpha)}{\alpha^N}.$$

The proof of Theorem 2 is sketched in E4.

Proof of Theorem 1 Suppose that $F(z) := \sum_{i=0}^{N} a_i z^i$ is a height 1 polynomial with a kth order root at α and other roots $\beta_1, \ldots, \beta_m$. We set

$$G(z) := \frac{F(z)}{(z - \beta_1)\cdots(z - \beta_m)},$$

so that

$$|\alpha - \beta_1|\cdots|\alpha - \beta_m| = \left|\frac{F^k(\alpha)/k!}{G^k(\alpha)/k!}\right|.$$

Here $F^j(z)$ denotes the jth derivative of $F(z)$. Suppose that $a_d \prod_{i=1}^{d}(z - \alpha_i)$ is the minimal polynomial of α. Then, by integrality,

$$|a_d|^{N-k} \prod_{i=1}^{d} \left|\frac{F^k(\alpha_i)}{k!}\right| \geq 1,$$

where if α is complex with $\alpha = \alpha_1 = \overline{\alpha_2}$,

$$\left|\frac{F^k(\alpha)}{k!}\right| = \left(\left|\frac{F^k(\alpha_1)}{k!}\right| \left|\frac{F^k(\alpha_2)}{k!}\right|\right)^{1/2}.$$

Hence, if $\delta := 1$ if α is real and $\delta := \frac{1}{2}$ if α is not real, and $\mu := 2$ if α is real and $\mu := 3$ if α is not real, we have

$$|\alpha - \beta_1| \cdots |\alpha - \beta_m| \geq \left(|a_d|^{\delta(N-k)} \left| \frac{G^k(\alpha)}{k!} \right| \prod_{i=\mu}^{d} \left| \frac{F^k(\alpha_i)}{k!} \right|^{\delta} \right)^{-1}.$$

For $|\alpha_i| \leq 1$ we use the following trivial bounds. If $|\alpha_i| = 1$,

$$\left| \frac{F^k(\alpha_i)}{k!} \right| \leq \frac{(N+1)^{k+1}}{k!},$$

and if $|\alpha_i| < 1$,

$$\left| \frac{F^k(\alpha_i)}{k!} \right| \leq (1 - |\alpha_i|)^{-(k+1)}.$$

For $|\alpha_i| > 1$ we make use of the vanishing of F at α_i. Let

$$H(z) := \frac{F(z)}{\big(1 - (z/\alpha_i)\big)^k},$$

so that

$$|\alpha_i|^k \left| \frac{F^k(\alpha_i)}{k!} \right| = |H(\alpha_i)|.$$

Now the coefficients of $H(z) = \sum_{j=0}^{N-k} h_j z^j$ satisfy

$$|h_l| = \left| \sum_{j=0}^{l} \binom{j+k-1}{k-1} \alpha_i^{-j} a_{l-j} \right| \leq \left(1 - |\alpha_i|^{-1}\right)^{-k},$$

and

$$\left| \frac{F^k(\alpha_i)}{k!} \right| \leq \frac{|\alpha_i|^{-k}}{(1 - |\alpha_i|^{-1})^k} \sum_{j=0}^{N-k} |\alpha_i|^j \leq \frac{|\alpha_i|^{N-k+1}}{(|\alpha_i| - 1)^{k+1}}.$$

It remains to estimate $G^k(\alpha)/k!$. Set

$$K(z) := \frac{G(z)}{(z-\alpha)^k} = \frac{F(z)}{(z-\alpha)^k (z-\beta_1) \cdots (z-\beta_m)},$$

so that $G^k(\alpha)/k! = K(\alpha)$. Notice that if

$$\frac{1}{1 - z/u} \sum r_i z^i = \sum s_i z^i,$$

then for any u,

$$|s_i| = \left| \sum_{j=0}^{i} r_{i-j} u^{-j} \right| \leq \max_{0 \leq j \leq i} |r_j| (i+1) \max\left\{1, |u|^{-1}\right\}^i,$$

while if $|u| > 1$,

$$|s_i| = \left|\sum_{j=0}^{i} r_{i-j} u^{-j}\right| \le \max_{0\le j\le i} |r_j| \left(1 - |u|^{-1}\right)^{-1}.$$

Now if $|\alpha| > 1$, we can assume that $|\beta_i| > 1$ for all i (otherwise, $|\alpha - \beta_i|$ is greater than a constant, and we can omit those β_i and adjust the constant accordingly). Hence the coefficients of $K(z) = \sum_{j=0}^{N-m-k} k_j z^j$ satisfy

$$k_j \le |\alpha|^{-k} \left(1 - |\alpha|^{-1}\right)^{-k} \prod_{i=1}^{m} |\beta_i|^{-1} \left(1 - |\beta_i|^{-1}\right)^{-1},$$

and

$$\begin{aligned}\left|\frac{G^k(\alpha)}{k!}\right| &\le (|\alpha| - 1)^{-k} \prod_{i=1}^{m} (|\beta_i| - 1)^{-1} \sum_{j=0}^{N-m-k} |\alpha|^j \\ &\le |\alpha|^{N-m-k+1} (|\alpha| - 1)^{-(k+1)} \prod_{i=1}^{m} (|\beta_i| - 1)^{-1}.\end{aligned}$$

Hence, when $|\alpha| > 1$ and $|\beta_i| > 1$ for each i, we obtain

$$|\alpha - \beta_1| \cdots |\alpha - \beta_m| \ge \frac{C_1(\alpha, m, k, \beta)}{M(\alpha)^{\delta N} (N+1)^{\delta(k+1)d_1}},$$

where

$$C_1(\alpha, m, k, \beta) := B_1(\alpha, k) |\alpha|^m \prod_{i=1}^{m} \big||\beta_i| - 1\big|,$$

with

$$B_1(\alpha, k) := |a_d|^\delta M(\alpha)^{\delta(k-1)} (k!)^{\delta d_1} \prod_{|\alpha_i| \ne 1} \big||\alpha_i| - 1\big|^{\delta(k+1)}.$$

The result follows, since we can assume $|\beta_i| - 1 > \frac{1}{2}(|\alpha| - 1)$ (or else we can omit that term from the product). The result for $|\alpha| < 1$ follows by working with α^{-1} and β_i^{-1}.

If $|\alpha| = 1$, we similarly see that the coefficients of $G(z) = \sum_{j=0}^{N-m} g_j z^j$ satisfy

$$|g_j| \le (j+1)^m \prod_{i=1}^{m} \max\left\{1, |\beta_i|^{-1}\right\}^j,$$

and hence

$$\left|\frac{G^k(\alpha)}{k!}\right| \le \prod_{i=1}^{m} \max\left\{1, |\beta_i|^{-1}\right\}^{N-m} \frac{(N-m)^k}{k!} \sum_{j=0}^{N-m} (j+1)^m.$$

So

$$\left|\frac{G^k(\alpha)}{k!}\right| \le \prod_{i=1}^{m} \max\left\{1, |\beta_i|^{-1}\right\}^{N-m} \frac{N^{k+m+1}}{k!},$$

and in this case

$$|\alpha - \beta_1| \cdots |\alpha - \beta_m| \ge \frac{C_1(\alpha, m, k, \beta)}{M(\alpha)^{\delta N}(N+1)^{\delta(k+1)d_1+m}},$$

where

$$C_1(\alpha, m, k, \beta) := B_1(\alpha, k) \prod_{i=1}^{m} \min\{1, |\beta_i|\}^{N-m}$$

with $B_1(\alpha, k)$ as above.

The result follows, since we can assume that $|\beta_i| > 1-(N+1)^{-1}$ (otherwise, $|\alpha-\beta_i| > 1/(N+1)$, and the result follows by simply omitting the term $|\alpha-\beta_i|$ from the product). □

Introductory Exercises

E1. Prove that the set of all zeros of $\mathcal{F}$ is dense in $[-2, -\frac{1}{2}] \cup [\frac{1}{2}, 2]$.

E2. Prove that the set of all zeros of $\mathcal{A}$ is dense in $\left[-\left(1+\sqrt{5}\right)/2, \left(1-\sqrt{5}\right)/2\right]$.

E3. Let $F(z; N)$ denote a polynomial of degree N in $\mathcal{F}$ that does not vanish at 1 and has a real root in $(0,1)$ that is as close to 1 as possible.

Show that for $N \ge 2$ the extremal polynomials $F(z; N)$ take the form

$$\begin{aligned} &\pm\frac{\left(z^{2m+1} - 2z^m + 1\right)}{(1-z)}, &&\text{if } N = 2m, \\ &\pm\frac{\left(z^{2m+2} - z^{m+1} - z^m + 1\right)}{(1-z)}, &&\text{if } N = 2m+1. \end{aligned}$$

E4. Beta Expansions and the Proof of Theorem 2. Prove Theorem 2 as follows. The *beta expansion* $\{c_n\}$ of 1 for α is given by

$$\gamma_0 := 1, \quad c_n := \lfloor \alpha\gamma_{n-1} \rfloor, \quad \gamma_n := \alpha\gamma_{n-1} - c_n.$$

Note that for α in $(1,2)$, all the c_i are 0 or 1 and

$$1 = \sum_{i=1}^{\infty} c_i \alpha^{-i}.$$

Write

$$F(z) := 1 - \sum_{i=1}^{\infty} c_i z^i,$$

so that $F(\alpha^{-1}) = 0$, and note that by Descartes's rule of signs, α^{-1} is a simple root of F (the only real root in $(0,1)$).

If the sequence $\{c_i\}$ terminates in zeros, which is possible (that is, α is a simple beta number), then α^{-1} is a simple root of the $\{0,+1,-1\}$ polynomial F. (In this case, modify the expansion to a nonterminating expansion by adding in F shifted by high powers of z.)

Now write

$$F_N(z) := 1 - \sum_{i=1}^{N} c_i z^i$$

for the Nth truncation of F and observe that

$$\left| \frac{F_N^j(\alpha^{-1})}{j!} \right| \le \left(1 - |\alpha|^{-1}\right)^{-(j+1)}$$

and

$$F_N^j\left(\alpha^{-1}\right) = F^j\left(\alpha^{-1}\right) + O\left(N^j \alpha^{-N}\left(1 - |\alpha|^{-1}\right)^{-(j+1)}\right).$$

The result now follows with the β (as in Theorem 2) denoting the reciprocals of appropriate roots of F_N and estimating how rapidly these roots approach $1/\alpha$. □

Computational Problems

C1. Recompute the first figure of the last section. Do this for the zeros of all Littlewood polynomials of degree n for various n. Identify as many of the "holes" as possible as roots of unity or Pisot or Salem numbers.

Research Problems

R1. Consider the set of all zeros of all Littlewood polynomials (as in E3 of the previous chapter) and denote this set by Ω. Show that the boundary of Ω is a fractal set and compute its Hausdorff dimension. Show that Ω is path connected. (Odlyzko and Poonen [1993] prove that the set of all zeros of all polynomials with coefficients in the set $\{0,1\}$ is path connected.) Determine whether Ω contains holes. Equivalently, does the complement of Ω have more than two components?

These questions should also be addressed for the polynomials of height 1.

Selected References

1. P. Borwein and C. Pinner, *Polynomials with* $\{0, +1, -1\}$ *coefficients and a root close to a given point*, Canad. J. Math. **49** (1997), 887–915.

2. A. Odlyzko and B. Poonen, *Zeros of polynomials with* $0, 1$ *coefficients*, Enseign. Math. (2) **39** (1993), 317–348.

Chapter 10

The Integer Chebyshev Problem

The main problem of this chapter is to find a polynomial in $\mathcal{Z}_n$ of minimal supremum norm on an interval. This is P1, and it is of a slightly different flavour than most of the other problems in this book, in that there is no restriction on the size of the coefficients. We now state P1 with greater precision.

P1. (Elaborated). *For any interval* $[a, b]$ *find*

$$\Omega[a, b] := \lim_{n \to \infty} \Omega_n[a, b],$$

where

$$\Omega_n[a, b] := \min_{p_n \neq 0, p_n \in \mathcal{Z}_n} \|p_n(z)\|_{[a,b]}^{1/n}.$$

As before, $\|\cdot\|_{[a,b]}$ denotes the supremum norm on $[a, b]$. From

$$(\Omega_{n+m}[a, b])^{n+m} \leq (\Omega_n[a, b])^n \big(\Omega_m[a, b]\big)^m, \tag{1}$$

it is fairly easy to deduce that $\Omega[a, b]$ exists. This quantity is called the *integer Chebyshev constant* or the *integer transfinite diameter* for the interval $[a, b]$.

When the coefficients are not restricted to being integers, the minimization problem in P1 is straightforward. Chebyshev polynomials, suitably normalized, are the polynomials of minimal supremum norm on an interval (see E2 of Chapter 7). Note that on $[-2, 2]$, the usual Chebyshev polynomials, normalized to have leading coefficient 1, have integer coefficients and supremum norm 2.

One can vary the problem to demand that the minimizing polynomial be monic of exact degree n. This is a quite different problem and is discussed in E3.

On intervals of length greater than or equal to 4, it follows from E2 of Chapter 7 that the minimum is given by the polynomial that is identically 1. There are no intervals of length less than 4 where the explicit value is known. However, on intervals of length less than 4, the integer Chebyshev constant is always less than 1.

For $b - a < 4$, Fekete [1923] showed that

$$(\Omega_n[a,b])^n \le 2^{1-2^{-n-1}}(n-1)\left(\frac{b-a}{4}\right)^{n/2},$$

so

$$\Omega[a,b] \le \left(\frac{b-a}{4}\right)^{1/2}.$$

See also Hilbert [1894] and Kashin [1991].

From (1) above one deduces that

$$\Omega[a,b] \le \Omega_n[a,b]$$

for any particular n. So, upper bounds can be derived computationally from the computation of any specific $\Omega_n[a,b]$. For example, if we let

$$\begin{aligned}
p_0(z) &:= z,\\
p_1(z) &:= 1 - z,\\
p_2(z) &:= 2z - 1,\\
p_3(z) &:= 5z^2 - 5z + 1,\\
p_4(z) &:= 13z^3 - 19z^2 + 8z - 1,\\
p_5(z) &:= 13z^3 - 20z^2 + 9z - 1 = -p_4(1-z),\\
p_6(z) &:= 29z^4 - 58z^3 + 40z^2 - 11z + 1,\\
p_7(z) &:= 31z^4 - 61z^3 + 41z^2 - 11z + 1,\\
p_8(z) &:= 31z^4 - 63z^3 + 44z^2 - 12z + 1 = p_7(1-z),\\
p_9(z) &:= 941z^8 - 3764z^7 + 6349z^6 - 5873z^5 + 3243z^4\\
&\qquad - 1089z^3 + 216z^2 - 23z + 1,
\end{aligned}$$

then we can show the following.

Theorem 1. *Let*

$$P_{210} := p_0^{67} \cdot p_1^{67} \cdot p_2^{24} \cdot p_3^{9} \cdot p_4 \cdot p_5 \cdot p_6^{3} \cdot p_7 \cdot p_8 \cdot p_9;$$

then

$$\Omega[0,1] \le \left(\|P_{210}\|_{[0,1]}\right)^{1/210} = \frac{1}{2.3543\ldots}.$$

Proof. This is a computation. The difficulty is in finding the approximation. While in principle, this is the almost pure LLL problem of minimizing the L_2 norm on $[0,1]$ over the lattice of integer polynomials of a fixed degree, in practice this alone does not generate particularly good estimates. See C2. □

Refinements on the method in Borwein and Erdélyi [1996a], based on optimizing the exponents of the factors of P_{210}, give

$$\Omega[0,1] \leq \frac{1}{2.3605\ldots}.$$

This has been further improved in Habsieger and Salvy [1997] to

$$\Omega[0,1] \leq \frac{1}{2.3612\ldots}.$$

Of course, when the coefficients of the polynomials above are not required to be integers, this reduces to the usual problem of constructing Chebyshev polynomials, and the limit (provided the polynomials are normalized to be monic) gives the usual transfinite diameter. From this unrestricted case, we have the obvious inequality

$$\Omega_n[0,1] \geq \frac{2^{1/n}}{4}.$$

However, inspection of the above example shows that an integer Chebyshev polynomial (a polynomial that achieves the value $\Omega_n[a,b]$, as in P1) doesn't look anything like a usual Chebyshev polynomial. In particular, it has many multiple roots, and indeed this must be the case since we have the following lemma.

Lemma 1. *Suppose $p_n \in \mathcal{Z}_n$ (the polynomials of degree at most n with integer coefficients) and suppose $q_k(z) := a_k z^k + \cdots + a_0 \in \mathcal{Z}_k$ has all its roots in $[a,b]$. If p_n and q_k do not have common factors, then*

$$\left(\|p_n\|_{[a,b]}\right)^{1/n} \geq |a_k|^{-1/k}.$$

Proof. Let $\beta_1, \beta_2, \ldots, \beta_k$ be the roots of q_k. Then

$$|a_k|^n p_n(\beta_1) p_n(\beta_2) \cdots p_n(\beta_k)$$

is a nonzero integer, and the result follows. □

From this lemma and the above-mentioned bound, we see that all of p_1 through p_9 must occur as high-order factors of integer Chebyshev polynomials on $[0,1]$ for all sufficiently large n. The divisibility to high order follows from Markov's inequality (Appendix A) which gives, for $p \in \mathcal{P}_n$,

$$\|p'\|_{[0,1]} \leq 2n^2 \|p\|_{[0,1]}.$$

There is a sequence of polynomials, called the Gorshkov–Wirsing polynomials, as in Montgomery [1994], that arise from iterating the rational function

$$u(z) := \frac{z(1-z)}{1-3z(1-z)}.$$

These are defined inductively by

$$q_0(z) := 2z - 1, \quad q_1(z) := 5z^2 - 5z + 1,$$

and

$$q_{n+1} := q_n^2 + q_n q_{n-1}^2 - q_{n-1}^4.$$

It transpires, on iterating u, that

$$u^{(n)} = \frac{q_{n-1}^2 - q_n}{2q_{n-1}^2 - q_n}.$$

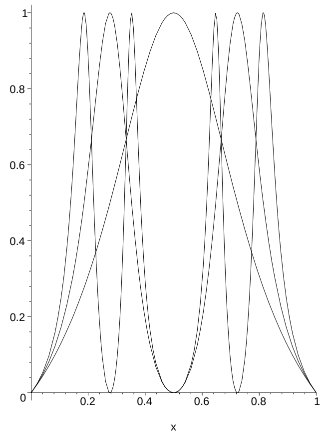
Each q_k is a polynomial of degree 2^k with simple zeros, all in $(0,1)$, and if b_k is the leading coefficient of q_k, then

$$\lim b_k^{1/2^k} = 2.3768417062\ldots.$$

Wirsing has proved that these polynomials are all irreducible. It follows now from Lemma 1 that

$$\Omega[0,1] \geq \frac{1}{2.3768417062\ldots}.$$

The first three iterates of $u(z)$.



It is conjectured by Montgomery [1994, p. 201] that if s is the least limit point of $|a_k|^{-1/k}$ (as in in Lemma 1) over polynomials with all their roots in $[0,1]$, then $\Omega[0,1] = s$. This was also conjectured by Chudnovsky [1983], who further conjectured that the minimal s arises from the Gorshkov–Wirsing polynomials, in which case s would equal $(2.3768417062\ldots)^{-1}$. In Borwein and Erdélyi [1996a] it is shown that

$$\Omega[0,1] \geq \frac{1}{2.3768417062\ldots} + \epsilon$$

for some positive ϵ. This shows that either Montgomery's conjecture is false or that the Gorshkov–Wirsing polynomials do not give rise to the minimal s. (The above lower bound is improved somewhat in Pritsker [preprint], where it is shown that the integer Chebyshev polynomials must have infinitely many distinct factors.) This leads us to ask the following question.

P16. A Montgomery Question. *Show that the minimal s arising as in Lemma 1 does not give the right value for $\Omega[0,1]$. Does $\Omega[0,1]$ have a closed form?*

Do all the integer Chebyshev polynomials on $[0,1]$ have all their roots in $[0,1]$? Habsieger and Salvy [1997] show that this can fail, with the first not totally real factor occurring for $n = 70$. A polynomial whose roots are all real is called *totally real*, and a polynomial whose roots are all real and nonnegative is called *totally positive*.

This same paper computes extrema up to degree 75. This is a nontrivial computation and is quite likely NP hard. Nonetheless, one suspects that there is a close relationship between $\Omega[0,1]$ and polynomials with integer coefficients whose roots are all in $[0,1]$. Sorting out this relationship would be of interest.

There is a somewhat related problem that we have called the Schur–Siegel–Smyth trace problem.

P17. Schur–Siegel–Smyth Trace Problem. Fix $\epsilon > 0$. Suppose

$$p_n(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathcal{Z}_n$$

has all real, positive roots and is irreducible. Show that, except for finitely many exceptions,

$$|a_{n-1}| \geq (2-\epsilon)n.$$

There are some partial results. In the notation of P17, except for finitely many (explicit) exceptions, $a_{n-1} \geq (1.771\ldots)n$. This is due to Smyth [1984b]. Previously, in 1918, Schur had shown that $a_{n-1} \geq e^{1/2}n$, and in 1943 Siegel had shown that $a_{n-1} \geq (1.733\ldots)n$ except for finitely many (explicit) exceptions.

A relationship between this and the integer Chebyshev problem is given by the following lemma.

Lemma 2. *Suppose m is a positive integer and*

$$\Omega\left[0, \frac{1}{m}\right] < (m+\delta)^{-1}.$$

Then, with at most finitely many exceptions,

$$\frac{\alpha_1 + \alpha_2 + \cdots + \alpha_d}{d} \geq \delta$$

for every totally positive algebraic integer α_1 *of degree* $d > 1$ *with conjugates* $\alpha_2, \ldots, \alpha_d$.

Proof. Suppose p is the minimal polynomial for α_1 and

$$p(z) := z^d - a_{d-1}z^{d-1} + \cdots + a_0;$$

then $\alpha_1 + m, \alpha_2 + m, \ldots, \alpha_d + m$ are conjugate roots of $q \in \mathcal{Z}_d$ defined by

$$q(z) := z^d - (a_{d-1} + md)z^{d-1} + \cdots + b_0.$$

Now,

$$b_0^{1/d} = ((\alpha_1 + m)(\alpha_1 + m) \cdots ((\alpha_d + m))^{1/d},$$

so by the arithmetic–geometric mean inequality,

$$b_0^{1/d} \leq \frac{\alpha_1 + \alpha_2 + \cdots + \alpha_d + dm}{d} = \frac{a_{d-1}}{d} + m.$$

We apply Lemma 1 to

$$q^*(z) := z^d q(1/z),$$

which has all its roots in $(0, 1/m)$ and is irreducible, to conclude that either

$$\frac{a_{d-1}}{d} + m > m + \delta$$

(which is the conclusion we want) or $q^*(z)$ is a factor of all nth degree integer Chebyshev polynomials on $[0, 1/m]$, provided n is large enough. $\square$

This reduces the search for better bounds in the Schur–Siegel–Smyth trace problem to computations on short intervals. From an example on $[0, 1/100]$, we derive the following result.

Corollary 1. *Suppose*

$$p_n(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathcal{Z}_n$$

has all real, positive roots and is irreducible. Then, except for finitely many exceptions,

$$|a_{n-1}| \geq (1.744)n.$$

Smyth [1999] has shown that this method can never give the full result of P17, but it would be interesting to see how far it can be taken.

Introductory Exercises

E1. Gorshkov–Wirsing Polynomials on $[0,1]$**.** Let

$$u(z) := \frac{z(1-z)}{1-3z(1-z)}$$

and let $u^{(n)}$ denote the nth iterate of u with itself ($u^{(0)} := u$).

(a) Show, by induction, that

$$u^{(n)} = \frac{q_{n-1}^2 - q_n}{2q_{n-1}^2 - q_n},$$

where

$$q_0(z) := 2z-1, \quad q_1(z) := 5z^2 - 5z + 1,$$

and

$$q_{n+1} := q_n^2 + q_n q_{n-1}^2 - q_{n-1}^4.$$

(b) Show that

$$q_{n+1}(z) = \left(-1+3z-3z^2\right)^{2^n} q_n\big(u(z)\big).$$

(c) Show that q_k is a polynomial of degree 2^k with all simple zeros in $(0,1)$. The main observation for this is that u maps the interval $[0,1]$ twice onto the interval $[0,1]$.

(d) Show that $\|q_k\|_{[0,1]} = 1$.

E2. Gorshkov–Wirsing Polynomials on $[0,\infty)$**.** Let

$$v(z) := z - \frac{1}{z}$$

and let $v^{(n)}$ denote the nth iterate of v with itself.

(a) Show, by induction, that

$$v^{(n)} = \frac{g_{n-1}(z^2)}{zh_{n-1}(z^2)},$$

where $g_0(z) = z-1$, $g_1(z) = z^2-3z+1$, $g_2(z) = z^4 - 7z^3 + 13z^2 - 7z + 1$, and

$$g_{n+1} := g_n^2 + g_n g_{n-1}^2 - g_{n-1}^4.$$

Further, $h_n(z) = \prod_{j=1}^{n-1} g_j(z)$.

(b) Show that with q_n as in the previous exercise,

$$q_n(z) = (1-z)^{2^n} g_n\left(\frac{z}{1-z}\right).$$

(c) Show that
$$g_n(z) = z^{2^{n-1}} g_{n-1}\left(z + \frac{1}{z} - 2\right).$$

(d) Show that each g_n is a monic polynomial with all its roots in $[0, \infty)$ and that
$$g_k = z^{2^n} - (2^{n+1} - 1)z^{2^n - 1} + \cdots.$$
So the trace is 1 less than twice the degree.

(e) Show that the trace of $U_n(z/2 - 2)$, the Chebyshev polynomial of the first kind shifted to the interval $[0, 4]$, is $2n - 1$. (See E1 of Chapter 7.)

E3. Monic Integer Chebyshev Polynomials. Show that for any n, z^n is the monic polynomial in $\mathcal{Z}_n$ of smallest supremum norm on any interval $[0, 1/m]$, where m is any integer greater than 1.

Show that $z^n(1 - z)^n$ is the monic polynomial in $\mathcal{Z}_{2n}$ of smallest supremum norm on $[0, 1]$.

In general, let $\mathcal{M}_n$ denote the monic polynomials of degree n with integer coefficients. Let E be an arbitrary compact set. A *monic integer Chebyshev polynomial* $v_n \in \mathcal{M}_n$ satisfies
$$\|v_n\|_E = \inf_{p_n \in \mathcal{M}_n} \|p_n\|_E,$$
and the *monic integer Chebyshev constant* is then defined by
$$\Omega^*(E) := \lim_{n\to\infty} \|v_n\|_E^{1/n}.$$
This is the obvious analogue of the more usual integer Chebyshev constant.

Show that
$$\Omega^*\left(\left\{\frac{m}{n}\right\}\right) = \frac{1}{n}$$
if $\gcd(m, n) = 1$ and $n > 1$, and if a is irrational or an integer, then
$$\Omega^*(\{a\}) = 0.$$

The following conjecture is made in Borwein, Pinner, and Pritsker [to appear] where it is verified for denominators up to 23.

Conjecture. *Suppose $[a_2/b_2, a_1/b_1]$ is an interval whose endpoints are consecutive nonintegral Farey fractions. This is characterized by $(a_1b_2 - a_2b_1) = 1$. Then*
$$\Omega^*\left(\left[\frac{a_2}{b_2}, \frac{a_1}{b_1}\right]\right) = \max\left(\frac{1}{b_1}, \frac{1}{b_2}\right).$$

Computational Problems

C1. Solve the integer Chebyshev problem (P1) up to degree 20 (or as far as you can go).

C2. Use LLL to try to compute polynomials in $\mathcal{Z}$ that have small supremum norm on $[0, 1]$. A reasonable strategy is to use LLL to find required divisors as in Lemma 1 and then to use a basis where each element is divisible by these required divisors to find additional required divisors.

C3. Verify the conjecture of E3 as far as possible (at least for all denominators less than 20). This can be done by using LLL to find examples that give the exact bounds. It is useful to have a version of LLL implemented with respect to the norm

$$\left(\int_a^b |p(x)|^2\, dx\right)^{1/2}.$$

C4. Compute the exceptions in Corollary 1.

Research Problems

R1. Compute $\Omega[\alpha, \beta]$ exactly on any interval of length less than 4.

R2. It is very natural to explore the integer Chebyshev question in many variables, say polynomials in two variables on triangles or on squares. See Chudnovsky [1983].

The following two theorems are proved in Borwein, Erdélyi, and Kós [1999]. They relate to how small one can make polynomials in $\mathcal{F}_n$ and $\mathcal{A}_n$.

Theorem 2. *There are absolute constants $c_1 > 0$ and $c_2 > 0$ such that*

$$\exp\left(-c_1\sqrt{n}\right) \le \inf_{0 \ne p \in \mathcal{F}_n} \|p\|_{[0,1]} \le \exp\left(-c_2\sqrt{n}\right).$$

The left side of the above inequality in fact holds over the polynomials p of the form

$$p(z) = \sum_{j=0}^{n} a_j z^j, \quad |a_0| = 1, \quad |a_j| \le 1, \quad a_j \in \mathbb{C}.$$

Theorem 3. *There are absolute constants $c_1 > 0$ and $c_2 > 0$ such that*

$$\exp\bigl(-c_1 \log^2(n+1)\bigr) \le \inf_{0 \ne p \in \mathcal{A}_n} \|p(-z)\|_{[0,1]} \le \exp\bigl(-c_2 \log^2(n+1)\bigr).$$

In the light of the above two theorems, it is natural to ask the following questions, which are the height 1 analogues of the integer Chebyshev problem.

R3. Does

$$\lim_{n\to\infty} \frac{\log\left(\inf_{0\neq p\in\mathcal{F}_n} \|p\|_{[0,1]}\right)}{\sqrt{n}}$$

exist? If it does, what is it?

R4. Does

$$\lim_{n\to\infty} \frac{\log\left(\inf_{0\neq p\in\mathcal{A}_n} \|p(-z)\|_{[0,1]}\right)}{\log^2(n+1)}$$

exist? If it does, what is it?

Selected References

The papers by Aparicio in the references and Montgomery's monograph below are good entry points to this subject matter. Flammang, Rhin, and Smyth [1997] substantially generalize the methods of this section to arbitrary intervals.

1. P. Borwein and T. Erdélyi, *The integer Chebyshev problem*, Math. Comp. **65** (1996), 661–681.

2. P. Borwein, C. Pinner, and I. Pritsker, *The monic integer Chebyshev problem*, Math. Comp. (to appear).

3. V. Flammang, G. Rhin, and C.J. Smyth, *The integer transfinite diameter of intervals and totally real algebraic integers*, J. Théor. Nombres Bordeaux **9** (1997), 137–168.

4. L. Habsieger and B. Salvy, *On integer Chebyshev polynomials*, Math. Comp. **66** (1997), 763–770.

5. H.L. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, CBMS, Vol. 84, Amer. Math. Soc., Providence, RI, 1994.

6. I. Pritsker, *Small polynomials with integer coefficients*, preprint.

Chapter 11

The Prouhet–Tarry–Escott Problem

A classical problem in Diophantine equations that occurs in many guises is the Prouhet–Tarry–Escott problem. This is the problem of finding two distinct lists (repeats are allowed) of integers $[\alpha_1, \ldots, \alpha_n]$ and $[\beta_1, \ldots, \beta_n]$ such that

$$\begin{aligned} \alpha_1 + \cdots + \alpha_n &= \beta_1 + \cdots + \beta_n \\ \alpha_1^2 + \cdots + \alpha_n^2 &= \beta_1^2 + \cdots + \beta_n^2 \\ \vdots \quad & \vdots \quad \vdots \\ \alpha_1^k + \cdots + \alpha_n^k &= \beta_1^k + \cdots + \beta_n^k. \end{aligned}$$

We will call this the Prouhet–Tarry–Escott Problem. We call n the size of the solution and k the degree. We abbreviate the above system by writing $[\alpha_i] =_k [\beta_i]$.

This problem has a long history and is, in some form, over 200 years old. In 1750–1751 Euler and Goldbach noted that

$$[a, b, c, a+b+c] =_2 [a+b, a+c, b+c].$$

A general solution of the problem for all degrees, but large sizes, came a century later, in 1851, when Prouhet found that there are n^{k+1} numbers separable into n sets such that each pair of sets forms a solution of degree k and size n^k. (See Theorem 1 of Chapter 12.) Prouhet's result, while the first general solution of the problem, was not properly noticed until Wright [1959] took exception to the problem being called the Tarry–Escott problem and drew attention to Prouhet's contribution in a paper called "Prouhet's 1851 solution of the Tarry–Escott problem of 1910." More of the early history of the problem can be found in Dickson [1952], where he refers to it as the problem of "equal sums of like powers."

The Diophantine equation above can be reformulated as a question about polynomials in two ways.

Theorem 1. *The following are equivalent:*

(a) $$\sum_{i=1}^{n} \alpha_i^j = \sum_{i=1}^{n} \beta_i^j \text{ for } j = 1, \ldots, k-1.$$

(b) $$\deg\Big(\prod_{i=1}^{n}(z-\alpha_i) - \prod_{i=1}^{n}(z-\beta_i)\Big) \le n-k.$$

(c) $$(z-1)^k \,\Big|\, \sum_{i=1}^{n} z^{\alpha_i} - \sum_{i=1}^{n} z^{\beta_i}.$$

It is the third form above that rephrases the Prouhet–Tarry–Escott problem as a question on the vanishing of low-height polynomials.

An *ideal solution* is one where the degree is 1 less than the size, which is the maximum possible. An *even ideal symmetric solution* of size n is of the form

$$[\pm\alpha_1, \ldots, \pm\alpha_{n/2}] =_{n-1} [\pm\beta_1, \ldots, \pm\beta_{n/2}]$$

and satisfies any of the following equivalent statements:

(a) $$\sum_{i=1}^{n/2} \alpha_i^{2j} = \sum_{i=1}^{n/2} \beta_i^{2j} \text{ for } j = 1, \ldots, \frac{n-2}{2}.$$

(b) $$\prod_{i=1}^{n/2}\left(z^2-\alpha_i^2\right) - \prod_{i=1}^{n/2}\left(z^2-\beta_i^2\right) = C \text{ for some constant } C.$$

(c) $$(1-z)^n \,\Big|\, \sum_{i=1}^{n/2}\left(z^{\alpha_i}+z^{-\alpha_i}\right) - \sum_{i=1}^{n/2}\left(z^{\beta_i}+z^{-\beta_i}\right).$$

Note that the third form of an even symmetric solution gives rise to a real (cosine) polynomial on the boundary of the unit disk.

An *odd ideal symmetric solution* of size n and even degree $n-1$ is of the form

$$[\alpha_1, \ldots, \alpha_n] =_{n-1} [-\alpha_1, \ldots, -\alpha_n]$$

and satisfies any of the following equivalent statements:

(a) $$\sum_{i=1}^{n} \alpha_i^j = 0 \text{ for } j = 1, 3, 5, \ldots, n-2.$$

(b) $$\prod_{i=1}^{n}(z-\alpha_i) - \prod_{i=1}^{n}(z+\alpha_i) = C \text{ for some constant } C.$$

(c) $$(1-z)^n \,\Big|\, \sum_{i=1}^{n} z^{\alpha_i} - \sum_{i=1}^{n} z^{-\alpha_i}.$$

In the third form above, an odd symmetric solution gives rise, on multiplication by i, to a real (sine) polynomial on the boundary of the unit disk.

There is a trivial transformation on solutions. Any linear transformation of a solution is a solution ($\alpha_i \mapsto A\alpha_i + B$ with A and B integers). Two such solutions are called *equivalent*.

The following is a list of ideal solutions for sizes 2 through 12, excluding 11 where no solution is known. For each size it includes the smallest known solution. Except for the case of size 4, the solutions are all symmetric. Exactly two inequivalent solutions of size 9 are known, and exactly one inequivalent solution of size 12 is known. For the rest of the known cases there are infinite parametric families of inequivalent solutions.

$$
\begin{aligned}
[\pm 2] &=_1 [\pm 1],\\
[-2, -1, 3] &=_2 [2, 1, -3],\\
[-5, -1, 2, 6] &=_3 [-4, -2, 4, 5],\\
[-8, -7, 1, 5, 9] &=_4 [8, 7, -1, -5, -9],\\
[\pm 1, \pm 11, \pm 12] &=_5 [\pm 4, \pm 9, \pm 13],\\
[-50, -38, -13, -7, 24, 33, 51] &=_6 [50, 38, 13, 7, -24, -33, -51],\\
[\pm 5, \pm 14, \pm 23, \pm 24] &=_7 [\pm 2, \pm 16, \pm 21, \pm 25],\\
&\hspace{-7em}[-98, -82, -58, -34, 13, 16, 69, 75, 99]\\
&=_8 [98, 82, 58, 34, -13, -16, -69, -75, -99],\\
&\hspace{-7em}[174, 148, 132, 50, 8, -63, -119, -161, -169]\\
&=_8 [-174, -148, -132, -50, -8, 63, 119, 161, 169],\\
[\pm 99, \pm 100, \pm 188, \pm 301, \pm 313] &=_9 [\pm 71, \pm 131, \pm 180, \pm 307, \pm 308],\\
[\pm 103, \pm 189, \pm 366, \pm 452, \pm 515] &=_9 [\pm 18, \pm 245, \pm 331, \pm 471, \pm 508],\\
[\pm 151, \pm 140, \pm 127, \pm 86, \pm 61, \pm 22] &=_{11} [\pm 148, \pm 146, \pm 121, \pm 94, \pm 47, \pm 35].
\end{aligned}
$$

The main problem of this section is the question of the size of minimal solutions of the Prouhet–Tarry–Escott problem and specifically whether or not ideal solutions exist:

P2. The Prouhet–Tarry–Escott Problem. *Find a polynomial with integer coefficients that is divisible by $(z-1)^n$ and has smallest possible length. (That is, minimize the sum of the absolute values of the coefficients.)*

Wright [1934] specifically conjectures that it is always possible to find ideal solutions. This has interesting consequences for the so-called easier Waring problem that is discussed in the next section. Heuristic arguments suggest that Wright's conjecture should be false. Counting arguments, as in the next section, give solutions of degree n and size $O(n^2)$, and it is tempting to speculate that this is essentially best possible. It is, however, intriguing that ideal solutions exist for as many n as they do.

Parametric Solutions

We now present parametric solutions of size 5, 6, 7, 8, and 10. The families of solutions of size 6, 8, and 10 are all symmetric, and immediately (on replacing t^2 by t) give infinite families of solutions of size 3, 4, and 5 where all the α_i are squares.

Size 5. The following is a one-parameter example of size 5:

$$\begin{aligned} F_5 := {} & \left(t+2m^2\right)(t-1)\left(t+2m^2-1\right)\left(t-2m^2+1-m\right)\left(t-2m^2+m+1\right) \\ & -\left(t-2m^2\right)(t+1)\left(t-2m^2+1\right)\left(t+2m^2-1+m\right)\left(t+2m^2-m-1\right). \end{aligned}$$

This expands to

$$F_5 := -4m^2(m-1)(2m+1)(2m-1)(m+1)\left(2m^2-1\right).$$

The fact that the expansion is independent of t proves, by the second criterion of Theorem 1 (with $z=t$), that the example is correct.

Size 6. The following is a simple two-parameter example of size 6:

$$\begin{aligned} F_6 := {} & \left(t^2-(2n+2m)^2\right)\left(t^2-(nm+n+m-3)^2\right)\left(t^2-(nm-n-m-3)^2\right) \\ & -\left(t^2-(2n-2m)^2\right)\left(t^2-(n-nm-m-3)^2\right)\left(t^2-(m-nm-n-3)^2\right). \end{aligned}$$

On expansion, one sees that

$$F_6 := -16nm(m-1)(m+3)(m-3)(m+1)(n-1)(n+3)(n-3)(n+1).$$

It is possible to solve for symmetric solutions of size 6. (See C3.) This gives the following three-parameter solution of size 6 (in nonsymmetric form):

$$\begin{aligned} & \left[\frac{2}{3}\frac{a_3^2-b_1^2-b_2^2-b_2b_1}{-b_1+a_3-b_2}, \frac{a_3b_1+a_3b_2-b_2b_1-b_2^2-b_1^2}{-b_1+a_3-b_2}, a_3, \frac{2}{3}\frac{a_3^2-b_1^2-b_2^2-b_2b_1}{-b_1+a_3-b_2}-a_3,\right. \\ & \qquad \left.\frac{2}{3}\frac{a_3^2-b_1^2-b_2^2-b_2b_1}{-b_1+a_3-b_2}-\frac{a_3b_1+a_3b_2-b_2b_1-b_2^2-b_1^2}{-b_1+a_3-b_2}, 0\right] \\ =_5 & \left[b_1, b_2, \frac{a_3^2+b_2b_1-a_3b_2-a_3b_1}{-b_1+a_3-b_2}, \frac{2}{3}\frac{a_3^2-b_1^2-b_2^2-b_2b_1}{-b_1+a_3-b_2}-\frac{a_3^2+b_2b_1-a_3b_2-a_3b_1}{-b_1+a_3-b_2},\right. \\ & \qquad \left.\frac{2}{3}\frac{a_3^2-b_1^2-b_2^2-b_2b_1}{-b_1+a_3-b_2}-b_2, \frac{2}{3}\frac{a_3^2-b_1^2-b_2^2-b_2b_1}{-b_1+a_3-b_2}-b_1\right]. \end{aligned}$$

Size 7. The following gives a parametric solution of size 7. This is homogeneous in j and k, so it is really a one-parameter solution. This is a much simplified version of a result of Gloden [1944]. He gives a four-parameter solution, but two of the parameters are extraneous. Chernick [1937] also gives such a family. Let

$$\begin{aligned} F_7 := {} & (t-R_1)(t-R_2)(t-R_3)(t-R_4)(t-R_5)(t-R_6)(t-R_7) \\ & -(t+R_1)(t+R_2)(t+R_3)(t+R_4)(t+R_5)(t+R_6)(t+R_7), \end{aligned}$$

where

$$\begin{aligned}
R_1 &:= -\left(-3j^2k+k^3+j^3\right)\left(j^2-kj+k^2\right),\\
R_2 &:= (j+k)(j-k)\left(j^2-3kj+k^2\right)j,\\
R_3 &:= (j-2k)\left(j^2+kj-k^2\right)kj,\\
R_4 &:= -(j-k)\left(j^2-kj-k^2\right)(-k+2j)k,\\
R_5 &:= -(j-k)\left(-2kj^3+j^4-j^2k^2+k^4\right),\\
R_6 &:= \left(j^4-4kj^3+j^2k^2+2k^3j-k^4\right)k,\\
R_7 &:= \left(j^4-4kj^3+5j^2k^2-k^4\right)j.
\end{aligned}$$

On expansion,

$$\begin{aligned}
F_7 = 2j^3k^3&(-k+2j)(j-2k)(j+k)\\
&\times\left(j^2+kj-k^2\right)\left(j^2-kj-k^2\right)\left(j^2-3kj+k^2\right)\\
&\times\left(-3j^2k+k^3+j^3\right)\left(j^4-4kj^3+5j^2k^2-k^4\right)\\
&\times\left(-2kj^3+j^4-j^2k^2+k^4\right)\left(j^4-4kj^3+j^2k^2+2k^3j-k^4\right)\\
&\times\left(j^2-kj+k^2\right)(j-k)^3,
\end{aligned}$$

which is independent of t. If we take $j := 2$ and $k := 3$, for example, then

$$\begin{aligned}
F_7 = &(t-7)(t-50)(t+24)(t+33)(t-13)(t+51)(t-38)\\
&-(t+7)(t+50)(t-24)(t-33)(t+13)(t-51)(t+38),
\end{aligned}$$

which expands to

$$F_7 = 13967553600.$$

Size 8. The following is a (homogeneous) size 8 solution due to Chernick [1937]:

$$\begin{aligned}
F_8 := &\left(t^2-R_1^2\right)\left(t^2-R_2^2\right)\left(t^2-R_3^2\right)\left(t^2-R_4^2\right)\\
&-\left(t^2-R_5^2\right)\left(t^2-R_6^2\right)\left(t^2-R_7^2\right)\left(t^2-R_8^2\right),
\end{aligned}$$

where

$$\begin{aligned}
R_1 &:= 5m^2+9mn+10n^2,\\
R_2 &:= m^2-13mn-6n^2,\\
R_3 &:= 7m^2-5mn-8n^2,\\
R_4 &:= 9m^2+7mn-4n^2,\\
R_5 &:= 9m^2+5mn+4n^2,\\
R_6 &:= m^2+15mn+8n^2,\\
R_7 &:= 5m^2-7mn-10n^2,\\
R_8 &:= 7m^2+5mn-6n^2.
\end{aligned}$$

On expansion,

$$\begin{aligned}F_8 = &-10752mn(2n+m)(n+m)(2n+3m)\\ &\times(n+2m)(4n-m)(5n+4m)(n-2m)(3n+m)\\ &\times(n-m)(n+5m)\left(3n^2+2mn-2m^2\right)\left(n^2+mn+m^2\right).\end{aligned}$$

Size 9. We know no parametric solution of size 9. Indeed, only two inequivalent solutions are known. Both are symmetric, and they are the following:

$$\begin{aligned}&[-98,-82,-58,-34,13,16,69,75,99]\\ &\quad =_8 [98,82,58,34,-13,-16,-69,-75,-99]\end{aligned}$$

and

$$\begin{aligned}&[174,148,132,50,8,-63,-119,-161,-169]\\ &\quad =_8 [-174,-148,-132,-50,-8,63,119,161,169].\end{aligned}$$

There are no other symmetric size 9 solutions of height less than 2000. (The height is the entry of largest modulus.)

Size 10. There are two small size 10 solutions known. They are

$$[\pm 99,\pm 100,\pm 188,\pm 301,\pm 313] =_9 [\pm 71,\pm 131,\pm 180,\pm 307,\pm 308]$$

and

$$[\pm 103,\pm 189,\pm 366,\pm 452,\pm 515] =_9 [\pm 18,\pm 245,\pm 331,\pm 471,\pm 508].$$

Otherwise, no symmetric examples of height less than 1500 exist.

The following size 10 example is originally due to Letac and is much simplified in Smyth [1991]. It constructs an infinite family of inequivalent ideal size 10 solutions based on rational solutions of an elliptic curve.

Let

$$\begin{aligned}F_{10} := &\left(t^2-R_1^2\right)\left(t^2-R_2^2\right)\left(t^2-R_3^2\right)\left(t^2-R_4^2\right)\left(t^2-R_5^2\right)\\ &-\left(t^2-R_6^2\right)\left(t^2-R_7^2\right)\left(t^2-R_8^2\right)\left(t^2-R_9^2\right)\left(t^2-R_{10}^2\right),\end{aligned}$$

where

$$\begin{aligned}R_1 &:= (4n+4m), & R_2 &:= (mn+n+m-11),\\ R_3 &:= (mn-n-m-11), & R_4 &:= (mn+3n-3m+11),\\ R_5 &:= (mn-3n+3m+11), & R_6 &:= (4n-4m),\\ R_7 &:= (-mn+n-m-11), & R_8 &:= (-mn-n+m-11),\\ R_9 &:= (-mn+3n+3m+11), & R_{10} &:= (-mn-3n-3m+11).\end{aligned}$$

On expansion of F_{10}, the constant coefficient is a polynomial in n and m alone. The rest of the expansion is divisible by the factor

$$m^2n^2 - 13n^2 + 121 - 13m^2.$$

Thus, any solution of the above biquadratic gives a size 10 solution. One such solution is given by $n = 153/61$ and $m = 191/79$. A second solution is given by $n = -296313/249661$ and $m = -1264969/424999$. The first of these gives the following solution:

$$\begin{aligned}&[\pm 12, \pm 11881, \pm 20231, \pm 20885, \pm 23738]\\&\qquad =_9 [\pm 436, \pm 11857, \pm 20449, \pm 20667, \pm 23750].\end{aligned}$$

The above biquadratic is equivalent to the elliptic curve

$$y^2 = (x - 435)(x - 426)(x + 861)$$

and gives rise to infinitely many inequivalent solutions. See Smyth [1991].

Size 11. No solutions are known, and no ideal symmetric solutions with all entries of modulus less than 2000 exist. See Borwein, Lisoněk, and Percival [to appear] and the last section of this chapter.

Size 12. The only known size 12 solution, found by Nuutti Kuosa and Chen Shuwen, is

$$[\pm 151, \pm 140, \pm 127, \pm 86, \pm 61, \pm 22] =_{11} [\pm 148, \pm 146, \pm 121, \pm 94, \pm 47, \pm 35].$$

There are no other symmetric solutions with all entries of modulus less than 1000.

Searching for Solutions

At present there are no known methods for finding ideal symmetric solutions of size 11 or higher to the Prouhet–Tarry–Escott problem other than massive searches. Nevertheless, the required searches can be made significantly less massive than the naive approach. (See Borwein, Lisoněk, and Percival [to appear].)

To begin with, ideal symmetric solutions of size $2n$ and $2n+1$ are defined uniquely by $n+1$ elements. In the case of a solution of even size, given $\alpha_1, \ldots, \alpha_{n+1-k}$ and $\beta_1, \ldots, \beta_k$, we note that as

$$\begin{aligned}\prod_{i=1}^{n}(z^2 - \alpha_i^2) - \prod_{i=1}^{n}(z^2 - \beta_i^2) &= C,\\ \prod_{i=1}^{n}(\beta_j^2 - \alpha_i^2) - 0 &= C \text{ for } j = 1, \ldots, n,\end{aligned}$$

and so

$$\frac{1}{C}\prod_{i=n-k+2}^{n}\left(\beta_j^2-\alpha_i^2\right)=\prod_{i=1}^{n-k+1}\left(\beta_j^2-\alpha_i^2\right)^{-1}\text{ for } j=1,\dots,k,$$

which gives us k evaluations of the unique degree $k-1$ polynomial with leading coefficient $1/C$ and roots $\alpha_{n-k+2},\dots,\alpha_n$. These points can thus be interpolated, and the resulting polynomial solved to yield the unspecified α_i. The remaining β_i can be computed similarly. This reduces the dimension of the problem in the even case from $2n$ to $n+1$.

In an analogous manner, given $\alpha_1,\dots,\alpha_{n+1}$ of an ideal symmetric size $2n+1$ solution to the Prouhet–Tarry–Escott problem, we note that as

$$\prod_{i=1}^{2n+1}(z+\alpha_i)-\prod_{i=1}^{2n+1}(z-\alpha_i)=C,$$

$$\prod_{i=1}^{2n+1}(\alpha_j+\alpha_i)=C\text{ for } j=1,\dots,n+1,$$

and so

$$\frac{1}{C}\prod_{i=n+2}^{2n+1}(\alpha_j+\alpha_i)=\prod_{i=1}^{n+1}(\alpha_j+\alpha_i)^{-1}\text{ for } j=1,\dots,n+1,$$

which again uniquely specifies a polynomial that can be interpolated and solved to give the unknown α_i. This reduces the dimension of the problem in the odd case from $2n+1$ to $n+1$.

In addition to reducing the search space from $2n$ or $2n+1$ dimensions to $n+1$ dimensions, we can reduce the search space further by considering the modular properties of solutions. Each size of solution has associated with it a set of primes that must divide the constant C (see C1). For odd sizes, if a prime p divides C, then (subject to reordering of the α_i) we must have $\alpha_1\equiv 0 \pmod p$ and $\alpha_{2k}+\alpha_{2k+1}\equiv 0 \pmod p$, while for even sizes the equivalent requirement is that $\alpha_k^2\equiv\beta_k^2 \pmod p$.

The best known approach to finding ideal symmetric solutions to the PTE problem is thus to find all $(n+1)$-tuples satisfying the divisibility criteria (for the appropriate size), and test whether they extend to solutions of size $2n$ or $2n+1$.

The following searches were done using the method described above and approximately 10^{17} floating-point operations on 100 relatively fast PCs (by 2001 standards a large computation). The method lends itself to trivial parallelization with essentially no communication needed between processors.

Size	Search limit	Result
9	2000	one (inequivalent) solution found
10	1500	two (inequivalent) solutions found
11	2000	no solutions found
12	1000	one (inequivalent) solutions found

Introductory Exercises

E1. Prove Theorem 1.

E2. Show that if $[\alpha_1, \ldots, \alpha_n]$ and $[\beta_1, \ldots, \beta_n]$ is an ideal solution and is ordered such that $\alpha_1 \le \alpha_2 \le \cdots \le \alpha_n$ and $\beta_1 \le \beta_2 \le \cdots \le \beta_n$, then $\alpha_i \ne \beta_j$ for any i and j and

$$\alpha_1 < \beta_1 \le \beta_2 < \alpha_2 \le \alpha_3 < \beta_3 \le \beta_4 < \alpha_4 \cdots$$

(where without loss of generality we assume that $\alpha_1 < \beta_1$).

Conclude that an ideal solution of the Prouhet–Tarry–Escott problem (in the third equivalent form) is a polynomial of height at most 2. Conclude also that $k = n - 1$ is best possible in the first theorem of this chapter.

E3. Show that for each prime p, the Prouhet–Tarry–Escott problem of size p has nontrivial solutions mod p.

E4. Show that the parametric solutions of this section give rise to infinitely many inequivalent solutions.

E5. There are various results concerning the divisibility of

$$C_n := \prod_{i=1}^{n} (z - \alpha_i) - \prod_{i=1}^{n} (z - \beta_i),$$

where $[\alpha_i] =_{n-1} [\beta_i]$ is an ideal solution. Prove the following lemma.

Lemma. *If $[\alpha_i] =_{n-1} [\beta_i]$ is an ideal solution with C_n defined as above, then*

$$|C_n| = \left|\prod_{i=1}^{n}(\beta_j - \alpha_i)\right| = \left|\prod_{i=1}^{n}(\alpha_j - \beta_i)\right| = \left|\prod_{i=1}^{n}\alpha_i - \prod_{i=1}^{n}\beta_i\right| = \left|\frac{\sum_{i=1}^{n}\alpha_i^n - \sum_{i=1}^{n}\beta_i^n}{n}\right|$$

for all j.

E6. Suppose

$$f(z) := \sum_{i=1}^{n} z^{\alpha_i} - \sum_{i=1}^{n} z^{\beta_i}$$

is divisible by

$$\prod_{i=1}^{k} (1 - z^{n_i}).$$

Show that

$$k! \prod_{i=1}^{k} n_i \;\Big|\; \sum_{i=1}^{n} \alpha_i^k - \sum_{i=1}^{n} \beta_i^k.$$

Computational Problems

C1. For fixed p, find ideal solutions of the Prouhet–Tarry–Escott problem mod p. Show that the constant C in the second equivalent form of the problem is divisible by a set of primes that depends only on p. For example, for $p = 11$, the constant C is divisible by 2, 3, 5, 7, 11, 13, and 17. For $p = 13$, the constant C would have to be divisible by all primes up to 31. (See Borwein, Lisoněk, and Percival [to appear] and Rees and Smyth [1990].)

C2. Find all symmetric solutions of sizes 1 through 5 in parametric form.

C3. Verify that it is possible to solve the even symmetric problem of size 6 in Maple (or equivalent). The following simple Maple code finds a parametric solution to the even symmetric problem of size 6. (Actually, it is a translated solution with $a_6 = 0$.)

```
PTE:=proc(n)
   local i,j,k,S;
   S:={seq(a[j]=a[1]-a[n+1-j],j=n/2+1..n),
       seq(b[j]=a[1]-b[n+1-j],j=n/2+1..n)};
subs(S,{seq(sum(a[i]^k,i=1..n)-sum(b[i]^k,i=1..n),k=1..n-1)});
end;
```

The command `solve(PTE(6))` gives the following as rational solutions of size 6:

$$\Big\{a_2 = a_2, b_1 = b_1, b_3 = b_3, b_2 = \frac{a_2^2 - a_2 b_3 + b_1 b_3 - a_2 b_1}{-b_1 - b_3 + a_2},$$
$$a_1 = \frac{2}{3}\frac{a_2^2 - b_3^2 - b_1^2 - b_1 b_3}{-b_1 - b_3 + a_2}, a_3 = \frac{-b_1^2 - b_1 b_3 + a_2 b_1 + a_2 b_3 - b_3^2}{-b_1 - b_3 + a_2}\Big\}.$$

Show that the three-parameter solution of size 6 of this chapter (in nonsymmetric form) is just a reworking of the above output.

Research Problems

R1. Find infinite families of ideal solutions of the Prouhet–Tarry–Escott problem of size 9 and size 12 or show they can't exist.

R2. Find an ideal solution of size 11 or any size greater than 12.

R3. Show for some n that no ideal solutions of the Prouhet–Tarry–Escott problem exist.

Selected References

1. P. Borwein and C. Ingalls, *The Prouhet–Tarry–Escott problem revisited*, Enseign. Math. (2) **40** (1994), 3–27.

2. P. Borwein, P. Lisoněk and C. Percival, *Computational investigations of the Prouhet–Tarry–Escott problem* (to appear).

3. W.H.J. Fuchs and E.M. Wright, *The 'easier' Waring problem*, Quart. J. Math. Oxford Ser. **10** (1939), 190–209.

4. E. Rees and C.J. Smyth, *On the constant in the Tarry–Escott problem*, in *Cinquante Ans de Polynômes*, Springer-Verlag, Berlin, 1990.

5. E.M. Wright, *Prouhet's 1851 solution of the Tarry–Escott problem of 1910*, Amer. Math. Monthly **66** (1959), 199–201.

Chapter 12

The Easier Waring Problem

Wright [1934] stated, and probably misnamed, the following variation of the well-known Waring problem concerning writing integers as sums of kth powers. The problem is to find the least n such that for all m there are natural numbers $[\alpha_1, \ldots, \alpha_n]$ with

$$\pm\alpha_1^k \pm \cdots \pm \alpha_n^k = m$$

for some choice of signs. We denote the least such n by $v(k)$. Recall that the usual Waring problem requires all positive signs. For arbitrary k the best known bounds for $v(k)$ derive from the bounds for the usual Waring problem. This gives the bound $v(k) \ll k\log(k)$ (though it is believed that the "right" bound in both the usual Waring problem and the easier Waring problem is $O(k)$). So to date, the "easier" Waring problem is not easier than the Waring problem. However, the best bounds for small k are derived in an elementary manner from solutions to the Prouhet–Tarry–Escott problem. This is discussed later in this chapter.

We define $N(k)$ to be the least n such that the Prouhet–Tarry–Escott problem of degree k has a solution of size n, as in the first theorem of the last chapter. So an ideal solution corresponds to $N(k) = k+1$. We further define $N^*(k)$ to be the least n such that the Prouhet–Tarry–Escott problem of degree k has a solution of size n that is not also a solution of degree $k+1$. It transpires that bounding $N(k)$ is significantly easier than bounding $N^*(k)$.

Theorem 1.

$$N(k) \leq \frac{1}{2}k(k+1) + 1.$$

Proof. Let $n > s^k s!$ and

$$A = \{[\alpha_1, \ldots, \alpha_s] : \alpha_i \in \mathbb{Z}, 1 \leq \alpha_i \leq n \text{ for } i = 1, \ldots, s\}.$$

There are n^s members of A. Consider the relation $\sim$ defined on A by $\mathbf{a} \sim \mathbf{b}$ if $\mathbf{a} := [\alpha_1, \ldots, \alpha_s]$ is a permutation of $\mathbf{b} := [\beta_1, \ldots, \beta_s]$. There are at least

$n^s/s!$ distinct equivalence classes in $A/\sim$, since each $[\alpha_1, \ldots, \alpha_s]$ has at most $s!$ different permutations. Let

$$s_j(\mathbf{a}) := \alpha_1^j + \cdots + \alpha_s^j \text{ for } j = 1, \ldots, k.$$

Note that

$$s \leq s_j(\mathbf{a}) \leq sn^j,$$

so there are at most

$$\prod_{j=1}^{k} \left(sn^j - s + 1\right) < s^k n^{k(k+1)/2}$$

distinct $[s_1(\mathbf{a}), \ldots, s_k(\mathbf{a})]$. We may now choose $s = \frac{1}{2}k(k+1) + 1$, and we have

$$s^k n^{k(k+1)/2} = s^k n^{s-1} < \frac{n^s}{s!},$$

since $n > s^k s!$. So the number of possible $[s_1(\mathbf{a}), \ldots, s_k(\mathbf{a})]$ is less than the number of distinct $\mathbf{a}$, and we may conclude that two distinct sequences $[\alpha_1, \ldots, \alpha_s]$ and $[\beta_1, \ldots, \beta_s]$ form a solution of degree k. $\square$

Slightly stronger upper bounds are discussed in Wright [1935] and Melzak [1961], but they are more difficult to establish and only improve the estimates to

$$N(k) \leq \frac{1}{2}\left(k^2 - 3\right), \ k \text{ odd}$$

and

$$N(k) \leq \frac{1}{2}\left(k^2 - 4\right), \ k \text{ even.}$$

The estimate for solutions of exact degree k are considerably harder. Hua [1982] shows that

$$N^*(k) \leq (k+1)\left(\frac{\log \frac{1}{2}(k+2)}{\log(1+\frac{1}{k})} + 1\right) \sim k^2 \log k.$$

The connection to the easier Waring problem can now be made.

Theorem 2. *Suppose* $[\alpha_1, \ldots, \alpha_n] =_{k-2} [\beta_1, \ldots, \beta_n]$. *Then*

$$\sum_{i=1}^{n}(z+\alpha_i)^k - \sum_{i=1}^{n}(z+\beta_i)^k = Cz + D,$$

where

$$C = k\left(\sum_{i=1}^{n} \alpha_i^{k-1} - \sum_{i=1}^{n} \beta_i^{k-1}\right)$$

and

$$D = \sum_{i=1}^{n} \alpha_i^k - \sum_{i=1}^{n} \beta_i^k.$$

This follows easily from Theorem 1 of the last chapter. Note that $k = n + 1$ corresponds to an ideal solution of the Prouhet–Tarry–Escott problem.

We define $\Delta(k, C)$ to be the smallest s such that every residue mod C is represented as a sum of s positive and negative kth powers. Define

$$\Delta(k) := \max_{C} \Delta(k, C).$$

Lemma 1. *If*

$$\sum_{i=1}^{n} (z + \alpha_i)^k - \sum_{i=1}^{n} (z + \beta_i)^k = Cz + D,$$

where $C \neq 0$, then

$$\Delta(k) \leq v(k) \leq 2n + \Delta(k, C) \leq 2n + \Delta(k).$$

Proof. This follows directly from the above definitions. □

Wright [1934] and Fuchs and Wright [1939] show how to calculate $\Delta(k, C)$ and $\Delta(k)$. They prove the following.

Theorem 3. *For all k,*

$$\Delta(k) \leq 2k.$$

(a) *If $k = 2^n$, then*

$$\Delta(k) = 2^{n+1} = 2k.$$

(b) *If $k = p^n(p-1)/2$ for some prime p, and k is not a power of 2, then*

$$\Delta(k) = (p^{n+1} - 1)/2 \geq k + 1.$$

(c) *If $k = (p-1)/2$ and $k \neq p^n(p-1)/2$ for some prime p, then*

$$\Delta(k) = (p-1)/2 = k.$$

(d) *In all other cases*

$$\Delta(k) \leq k.$$

The next theorem shows that

$$v(k) \ll k^2 \log k.$$

Theorem 4. *For all k,*

$$v(k) \leq 2N^*(k-2) + \Delta(k) \leq 2(k-1)\left(\frac{\log \frac{1}{2}(k)}{\log(1 + \frac{1}{k-2})} + 1\right) + 2k.$$

Proof. This follows from Lemma 1, the fact that

$$\Delta(k) \leq 2k$$

(as in Theorem 3), and Hua's bound for $N^*(k)$. Note that we must use $N^*(k)$ and not $N(k)$, since we require exact solutions, which implies that $C \neq 0$. □

Introductory Exercises

E1. Show that $v(2) = 3$. Exact values of $v(k)$ are not known for any other k.

E2. Use the identity

$$(z+1)^3 + (z-1)^3 - 2z^3 = 6z$$

to show that $v(3) \leq 5$. Show, on considering the problem mod 9, that $v(3) \geq 4$.

E3. Use the identity

$$\begin{aligned}(z+8)^7 + (z-8)^7 + (z+5)^7 + (z-5)^7 + (z-3)^7 \\ + (z+3)^7 - 2z^7 - 2(z-7)^7 - 2(z+7)^7 = 604800z\end{aligned}$$

to show that $v(7) \leq 14$.

One knows the following: $v(2) = 2$, $4 \leq v(3) \leq 5$, $8 \leq v(4) \leq 12$, $5 \leq v(5) \leq 10$, $5 \leq v(5) \leq 10$, $6 \leq v(6) \leq 14$, and $7 \leq v(7) \leq 14$. More values may be found in Fuchs and Wright [1939].

The best bounds that follow from the usual Waring problem are not as good. Define $G(k)$ to be the smallest integer n such that every sufficiently large integer is a sum of positive kth powers. Then $G(2) = 4$ and $G(4) = 16$. No other exact values are known. Linnik showed that $4 \leq G(3) \leq 7$, and Vaughan and Wooley [1995] showed that $6 \leq G(5) \leq 17$.

See http://www.mathsoft.com/asolve/pwrs32/waring.html for more numbers.

Computational Problems

C1. Use LLL to find reasonable values for $N(k)$ for k up to 20.

C2. Use Lemma 1 to find reasonable values for $v(k)$ for k up to 20.

Good bounds for small k are derived from Lemma 1 using specific solutions of the Prouhet–Tarry–Escott problem and careful computation of $\Delta(k, C)$ as above.

Research Problems

R1. Show that $N^*(k) \ll k^2$.

R2. Is it true that $N^*(k) = o(k \log k)$? This would be a significant result, since it would give better bounds for the easier Waring problem than those that follow from the current bounds for the usual Waring problem.

Selected References

1. W.H.J. Fuchs and E.M. Wright, *The 'easier' Waring problem*, Quart. J. Math. Oxford Ser. **10** (1939), 190–209.
2. L.K. Hua, *Introduction to Number Theory*, Springer-Verlag, New York–Berlin, 1982.
3. R.C. Vaughan and T.D. Wooley, *Further improvements in Waring's problem*, Acta Math. **174** (1995), 147–240.
4. E.M. Wright, *An easier Waring's problem*, J. London Math. Soc. **9** (1934), 267–272.

Chapter 13

The Erdős–Szekeres Problem

One approach to the Prouhet–Tarry–Escott problem is to construct products of the form

$$p(z) := \prod_{k=1}^{N} (1 - z^{\alpha_i}).$$

This product has a zero of order N at 1, and the idea is to try to minimize the length (the l_1 norm) of p. We denote by E_N^* the minimum possible l_1 norm of any N-term product of the above form. The l_1 norm is just the sum of the absolute values of the coefficients of the polynomial p when it is expanded, and an ideal solution of the Prouhet–Tarry–Escott problem arises when $E_N^* = 2N$ (as in Theorem 1(c) of Chapter 11).

The following conjecture of Erdős and Szekeres implies that the above approach will be quite far from giving ideal solutions for large N. Note that the conjecture is stated in terms of the supremum norm, but this is equivalent to an l_1 formulation of the problem. (See E1.)

P3. The Erdős–Szekeres Problem. *For each N, minimize*

$$\|(1 - z^{\alpha_1})(1 - z^{\alpha_2}) \cdots (1 - z^{\alpha_N})\|_\infty$$

where the α_i are positive integers. In particular, show that these minima grow faster than N^β for any positive constant β.

The following table shows what is known for N up to 13.

N	$\|p\|_{l_1}$	$[\alpha_1, \ldots, \alpha_N]$
1	2	$[1]$
2	4	$[1,2]$
3	6	$[1,2,3]$
4	8	$[1,2,3,4]$
5	10	$[1,2,3,5,7]$
6	12	$[1,1,2,3,4,5]$
7	16	$[1,2,3,4,5,7,11]$
8	16	$[1,2,3,5,7,8,11,13]$
9	20	$[1,2,3,4,5,7,9,11,13]$
10	24	$[1,2,3,4,5,7,9,11,13,17]$
11	28	$[1,2,3,5,7,8,9,11,13,17,19]$
12	36	$[1,\ldots,9,11,13,17]$
13	44	$[1,\ldots,5,7,9,11,13,16,17,19,23]$

(For $N = 14$ and $N = 15$ the best known examples have $\|p\|_{l_1} = 52$.) Note that for $N \in \{1,2,3,4,5,6,8\}$ this provides an ideal solution of the Prouhet–Tarry–Escott problem, and indeed, the first known solutions were mostly of this form. Maltby [1996] shows, for $N \in \{7,9,10,11\}$, that these kinds of products cannot solve the Prouhet–Tarry–Escott problem, and in fact, for $N \in \{7,9,10\}$ the above examples are provably optimal. This leads to the following conjecture.

Conjecture. *Except for $N \in \{1,2,3,4,5,6,8\}$,*

$$E_N^* \geq 2N + 2.$$

Currently, the only lower bounds known (except for Maltby's results for $N \in \{7,9,10,11\}$) are the trivial lower bounds $E_N^* \geq 2N$ of the Prouhet–Tarry–Escott problem.

Currently the best subexponential upper bounds in this problem of the form

$$\log(E_N^*) \ll \log^4(N)$$

are due to Belov and Konyagin [1996].

The following result, due to Atkinson [1961], gives an easy subexponential bound.

Theorem 1. *Let β_i be the sequence formed by taking the elements of the set*

$$\{2^n - 2^m : n > m \geq 0\}$$

in increasing order. Then for infinitely many N,

$$\left\| \prod_{i=1}^{N} \left(1 - z^{\beta_i}\right) \right\|_\infty \leq (2N)^{\sqrt{N/8}}.$$

The above theorem is an immediate consequence of the next lemma.

Lemma 1. *Let* $1 \le \beta_1 < \beta_2 < \cdots$ *and let*

$$V_n(z) := \prod_{1 \le i < j \le n} \left(1 - z^{\beta_j - \beta_i}\right).$$

Then

$$\|V_n(z)\|_\infty \le n^{n/2}.$$

Proof. We can explicitly evaluate the Vandermonde determinant

$$D_n := \prod_{1 \le i < j \le n} \left(z^{\beta_j} - z^{\beta_i}\right) = \begin{vmatrix} 1 & z^{\beta_1} & \dots & z^{(n-1)\beta_1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z^{\beta_n} & \dots & z^{(n-1)\beta_n} \end{vmatrix}.$$

By Hadamard's inequality, since each entry of the matrix has modulus at most 1 in the unit disk,

$$\|D_n\|_\infty \le n^{n/2}.$$

Thus

$$\left\| \prod_{1 \le i < j \le n} \left(1 - z^{\beta_j - \beta_i}\right) \right\|_\infty = \left\| \prod_{1 \le i < j \le n} \left(z^{\beta_j} - z^{\beta_i}\right) \right\|_\infty \le n^{n/2}.$$

□

The question of the norms of specific families of products is interesting. The following result occurs in Borwein [1993]. A proof of the first part is indicated in E3.

Theorem 2. *If* $\gcd(p, \alpha_i) = 1$ *and* p *is prime, then*

$$\left\| \prod_{i=1}^{N} \left(1 - z^{\alpha_i}\right) \right\|_\infty \ge p^{N/(p-1)}.$$

This is best possible for $p \in \{2, 3, 5, 7, 11, 13\}$, *with extremal examples given by the partial products of*

$$\prod_{\substack{n=1 \\ \gcd(p,n)=1}}^{\infty} \left(1 - z^n\right).$$

In Bell, Borwein, and Richmond [1998] it is shown that if α is an integer greater than 1, then we have

$$\left\| \prod_{i=1}^{N} (1 - z^{i^\alpha}) \right\|_\infty \gg C^N$$

for some $C > 1$. This is, essentially, a circle method argument.

Introductory Exercises

E1. Show that

$$\|(1-z^{\alpha_1})(1-z^{\alpha_2})\cdots(1-z^{\alpha_N})\|_\infty \le \|(1-z^{\alpha_1})(1-z^{\alpha_2})\cdots(1-z^{\alpha_N})\|_{l_1}$$

and

$$\|(1-z^{\alpha_1})(1-z^{\alpha_2})\cdots(1-z^{\alpha_N})\|_{l_1} \le K\,\|(1-z^{\alpha_1})(1-z^{\alpha_2})\cdots(1-z^{\alpha_N})\|_\infty\,,$$

where K is the number of nonzero terms in the expansion of the product. So if the conjecture in the Erdős–Szekeres problem is correct, it is independent of which of the above norms is chosen.

E2. Euler's pentagonal number theorem states that

$$\prod_{k=1}^{\infty}\left(1-z^k\right) = \sum_{m=-\infty}^{\infty}(-1)^m z^{(3m^2+m)/2}.$$

This makes it natural to look at

$$W_N := \prod_{k=1}^{N}\left(1-z^k\right).$$

Show that

$$\|W_N(z)\|_\infty \gg c^N$$

for some constant $c > 1$. (In fact, $c := 1.219\ldots$ is the right order of growth. See Sudler [1964].)

E3. Show that if $\gcd(p,\alpha_i) = 1$ and p is prime, then

$$\left\|\prod_{i=1}^{N}(1-z^{\alpha_i})\right\|_\infty \ge p^{N/(p-1)}.$$

Hint: Evaluate the product at each of a complete set of primitive pth roots of unity. Multiply all of these evaluations together. □

Computational Problems

C1. Design an algorithm to compute E_n^* and use it to compute E_n^* for as many n as possible.

This is, in fact, possible. The key is to observe that it is possible to write this as a collection of integer relations on the exponents. This is elaborated in Maltby [1996]. Maltby (with an improvement by Cipu [preprint]) shows that a minimal solution for E_n^* can be chosen such that all exponents are no greater than $(n-1)^{(n-1)/2}$.

Research Problems

R1. There is an amusing problem, related to Theorem 2, whose solution would let one compute the exact l_1 norm in the case $p = 3$.

Problem. *For each n, write*

$$(1-z)\left(1-z^2\right)\left(1-z^4\right)\left(1-z^5\right)\cdots\left(1-z^{3n+1}\right)\left(1-z^{3n+2}\right)=\sum a_i z^i.$$

Show that $a_i \geq 0$ if and only if 3 divides i.

A similar result should hold for $p = 5$. See Andrews [1995].

R2. Prove the conjecture that except for $N \in \{1,2,3,4,5,6,8\}$,

$$E_N^* \geq 2N+2.$$

Selected References

1. J. Bell, P. Borwein, and B. Richmond, *Growth of the product* $\prod_{j=1}^{n}(1-x^{a_j})$, Acta Arith. **86** (1998), 115–130.

2. A.S. Belov and S.V. Konyagin, *An estimate for the free term of a nonnegative trigonometric polynomial with integral coefficients*, Mat. Zametki **59** (1996), 627–629.

3. P. Borwein and C. Ingalls, *The Prouhet–Tarry–Escott problem revisited*, Enseign. Math. (2) **40** (1994), 3–27.

4. P. Erdős and G. Szekeres, *On the product* $\prod_{k=1}^{n}(1-z^{a_k})$, Acad. Serbe Sci. Publ. Inst. Math. **13** (1959), 29–34.

5. R. Maltby, *Pure product polynomials and the Prouhet–Tarry–Escott problem*, Math. Comp. **66** (1997), 1323–1340.

Chapter 14

Barker Polynomials and Golay Pairs

Both Barker polynomials (which probably exist only for a few small degrees) and Golay complementary pairs are combinatorial objects that, as discussed later, have certain optimal properties in signal processing and signal recovery. They also provide, when they exist, extremal examples for various problems we are considering in this book.

For any polynomial

$$p(z) := \sum_{k=0}^{n} a_k z^k,$$

the kth *acyclic autocorrelation coefficient* is defined, for $-n \le k \le n$, by

$$c_k := \sum_{j=0}^{n-k} a_j a_{j+k} \quad \text{and} \quad c_{-k} := c_k.$$

So

$$\|p(z)\|_4^4 = \left\| p(z) p\left(\frac{1}{z}\right) \right\|_2^2 = \left\| \sum_{k=-n}^{n} c_k z^k \right\|_2^2 = \sum_{k=-n}^{n} c_k^2.$$

A *Barker polynomial*

$$p(z) := \sum_{k=0}^{n} a_k z^k,$$

with each $a_k \in \{+1, -1\}$, is a polynomial where each acyclic autocorrelation coefficient satisfies

$$|c_j| \le 1, \quad j = 1, 2, \ldots, n.$$

Thus,

$$c_0 = n + 1,$$

and by parity

$$c_k = 0, \quad n-k \text{ odd}$$

and

$$|c_k| = 1, \quad n-k \text{ even}.$$

Since

$$\|p(z)\|_4^4 = \sum_{k=-n}^{n} c_k^2$$

we have that if $p(z)$ is a Barker polynomial of even degree n then

$$\|p\|_4 = \left((n+1)^2 + n\right)^{1/4},$$

while if $p(z)$ is a Barker polynomial of odd degree n then

$$\|p\|_4 = \left((n+1)^2 + n + 1\right)^{1/4}.$$

Thus, when a Barker polynomial of degree n exists, it mimimizes the L_4 norm (and maximizes the merit factor—see the next chapter) of polynomials from the class $\mathcal{L}_n$.

It is widely believed that no Barker polynomials exist of degree greater than 12. This is discussed further in the exercises, where all known Barker polynomials are listed.

The following conjecture implies that the largest nontrivial acyclic autocorrelation coefficients must tend to infinity with the degree.

P7. The Merit Factor Problem of Golay. *Find the polynomial in $\mathcal{L}_n$ that has smallest possible L_4 norm on the unit disk. Show that there exists a positive constant c such that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_4 \geq (1+c)\sqrt{n+1}$.*

Even the following much weaker problem is open.

P8. The Barker Polynomial Problem. *For n sufficiently large ($n > 12$ may suffice) and $p_n \in \mathcal{L}_n$, show that*

$$\|p_n\|_4 > \left((n+1)^2 + n + 1\right)^{1/4}.$$

This would imply the nonexistence of Barker polynomials for n sufficiently large. Note that P8 would follow from the estimate $\|p_n\|_4 > \sqrt{n+1} + 1$.

Golay Pairs

A *Golay complementary pair* is a pair of polynomials

$$q(z) := \sum_{k=0}^{n} a_k z^k$$

and

$$r(z) := \sum_{k=0}^{n} b_k z^k,$$

with each $a_k, b_k \in \{+1, -1\}$, where if $c_k(q)$ and $c_k(r)$ are the acyclic autocorrelation coefficients of q and r respectively, then

$$c_k(q) + c_k(r) = 0, \quad k \neq 0,$$

and

$$c_0(q) + c_0(r) = 2n + 2.$$

So it is obvious that both polynomials of a Golay pair have the same L_4 norm. Being a Golay pair is equivalent to

$$|q(z)|^2 + |r(z)|^2 = 2n + 2 \quad \text{for } |z| = 1,$$

and is also equivalent to

$$|p(z)|^2 + |p(-z)|^2 = 2(2n + 2) \quad \text{for } |z| = 1,$$

where $p(z) := q(z^2) + zr(z^2)$. Note that $p \in \mathcal{L}_{2n+1}$ will satisfy the above if and only if all the even acyclic autocorrelation coefficients of p are zeros, and in this case $p(z)$ and $p(-z)$ also form a Golay pair.

Theorem 1. *Let $p \in \mathcal{L}$ and*

$$\gamma := \frac{\|p\|_4^4 + \|p(z)p^*(-z)\|_2^2}{2\|p\|_2^4}.$$

Then $\gamma = 1$ if and only if

$$p(z) := q\left(z^2\right) + zr\left(z^2\right)$$

and q and r are a Golay complementary pair.

Proof. Note that $|p(z)p^*(-z)| = |p(z)p(-z)|$ if p has real coefficients, so with $z = e^{i\theta}$,

$$\begin{aligned}
\|p\|_4^4 + \|p(z)p^*(-z)\|_2^2 &= \frac{2}{2\pi} \int_0^{2\pi} \left(\frac{|p(z)|^2 + |p^*(-z)|^2}{2} \right)^2 d\theta \\
&= \frac{2}{2\pi} \int_0^{2\pi} \left(\frac{|p(z)|^2 + |p(-z)|^2}{2} \right)^2 d\theta \\
&\geq 2 \left(\frac{1}{2\pi} \int_0^{2\pi} \frac{|p(z)|^2 + |p(-z)|^2}{2} \, d\theta \right)^2 \\
&= 2\|p\|_2^4.
\end{aligned}$$

The "if" part now follows from the observation above that if

$$p(z) := q\left(z^2\right) + zr\left(z^2\right)$$

and q and r are a Golay complementary pair, then

$$|p(z)|^2 + |p(-z)|^2 = 2(2n+2) \quad \text{for } |z| = 1.$$

The "only if" part follows because the inequality above is an equality only for constant functions. $\square$

Theorem 2. *If $n = 2^a 10^b 26^c - 1$ (for nonnegative integers a, b, c) then there exists a Golay complementary pair of degree n.*

A guided proof is given in the exercises. The usual Rudin–Shapiro polynomials of Chapter 4 provide Golay pairs of degrees $n = 2^a - 1$ for each a. It may be that Theorem 2 gives all possible degrees for Golay complementary pairs. This is confirmed up to degree 100 in Borwein and Ferguson [to appear]. The next section outlines the computational methods that make this check possible.

Searching for Golay Pairs

An often effective step in analyzing autocorrelation equations for polynomials in $\mathcal{L}$ involves reductions modulo a power of 2. For example, when $a, b \in \{+1, -1\}$, we have

$$ab \equiv a + b - 1 \pmod 4, \tag{1}$$

which converts multiplication to a linear operation. This leads to the following result derived from Golay [1961].

Theorem 3. *For a Golay pair $q(z) := \sum_{k=0}^{n} a_k z^k$ and $r(z) := \sum_{k=0}^{n} b_k z^k$,*

$$a_k b_k + a_{n-k} b_{n-k} = 0$$

for $0 \le k \le n$. Furthermore, n is odd.

Proof. We apply reduction modulo 4 to the n equations

$$c_k(q) + c_k(r) = 0$$

for $1 \le k \le n$, and transform these using reduction (1) above to obtain the set of equations

$$a_k + b_k + a_{n-k} + b_{n-k} + 2 \equiv 0 \pmod 4.$$

These, in turn, are equivalent to

$$a_k b_k + a_{n-k} b_{n-k} = 0$$

for $0 \le k \le n$.

On considering the central term if n is even, we may conclude that $n+1$ must be even. So $m := (n+1)/2$ is an integer. $\square$

Following Andres and Stanton [1977], we now focus on *quads*, or quadruples of coefficients from a pair, defined by

$$X_k := \begin{bmatrix} a_k & a_{n-k} \\ b_k & b_{n-k} \end{bmatrix},$$

forming a sequence $X_0, X_1, \ldots, X_{m-1}$. Here $m-1 = (n-1)/2$ is essentially half the length of the pair. By Theorem 3, one of the entries in a quad is of opposite sign to the other three. We completely describe this sequence in terms of three binary vectors relating to the position of this "odd" entry and the dominant sign for each term. Namely:

(1) The *horizontal orientation vector* $H := [h_0, h_1, \ldots, h_{m-1}]$, where h_i is 0 if the odd term in X_i is on the right and is 1 otherwise.

(2) The *vertical orientation vector* $V := [v_0, v_1, \ldots, v_{m-1}]$, where v_i is 0 if the odd term in X_i is on the top and is 1 otherwise.

(3) The *sign vector* $S := [s_0, s_1, \ldots, s_{m-1}]$, where $s_i = 1$ or -1 to match the dominant sign of X_i. An equivalent formulation is as a binary vector $B_s = [b_0, b_1, \ldots, b_{m-1}]$, where $b_i = \frac{1}{2}(s_i + 1)$.

Multiplication of quads is defined by

$$XY = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} = \frac{1}{4}\left(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4\right),$$

with divisibility by 4 following from Theorem 3. Note that this is not usual matrix multiplication.

The condition

$$a_0a_n + b_0b_n = 0$$

is satisfied by the quad X_0. The next condition,

$$a_0a_{n-1} + a_1a_n + b_0b_{n-1} + b_1b_n = 0,$$

can be written as $X_0X_1^* = 0$, where the superscript * signifies the interchange of columns in a quad. With this interpretation, the autocorrelation conditions become

$$\begin{aligned}
X_0X_1^* &= 0,\\
X_0X_2^* &= 0,\\
X_0X_3^* + X_1X_2^* &= 0,\\
X_0X_4^* + X_1X_3^* &= 0,\\
X_0X_5^* + X_1X_4^* + X_2X_3^* &= 0,\\
X_0X_6^* + X_1X_5^* + X_2X_4^* &= 0,\\
&\vdots\\
X_0X_{n-2}^* + X_1X_{n-3}^* + X_2X_{n-4}^* + \cdots + X_{m-2}X_{m-1}^* &= 0,\\
X_0X_{n-1}^* + X_1X_{n-2}^* + X_2X_{n-3}^* + \cdots + X_{m-2}X_m^* &= 0.
\end{aligned}$$

It is also useful to think of quads as being of two types, P and Q, according to their vertical orientation, where

$$P := \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad Q := \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

The eight possible quads are then $P, -P, P^*, -P^*$ and $Q, -Q, Q^*, -Q^*$. They have the following multiplication table:

	P	P^*	Q	Q^*
P	1	0	0	0
P^*	0	1	0	0
Q	0	0	1	0
Q^*	0	0	0	1

which is extended by $(-X)Y = X(-Y) = -XY$ and $(-X)(-Y) = XY$.

Searching for Golay pairs may now be conducted by solving the following two linear systems modulo 2:

(1) *Reduction modulo* 2: For quads, on reducing modulo 2, we derive the following:

$$\begin{aligned} X_iX_j &\equiv (1 + v_i + v_j)(1 + h_i + h_j) \pmod 2, \\ X_iX_j^* &\equiv (1 + v_i + v_j)(h_i + h_j) \pmod 2. \end{aligned}$$

After specifying the value of either the H or V vector, the autocorrelation equations become linear in the coordinates of the other orientation vector by reducing modulo 2. (This is an order $2^{n/2}$ search.)

(2) *Reduction modulo* 4 (again): We note now that

$$X_iX_j = s_is_j\big(X_iX_j \pmod 2\big).$$

A solution is completely determined by the values of the H, V, and S vectors. We are now left with checking that the given H and V from step (1) generate an S that gives a solution. Substituting the values of H and V leaves us with a quadratic system in the components of S. Reducing modulo 4 converts this to a linear system. If we switch to components of B_s, we are able to divide each equation by 2, obtaining a linear system modulo 2.

The final check is to verify any solutions from step (2). This is no more than exponential in the number of free variables of this system.

Some Additional Context

We consider binary sequences $A := (a_0, a_1, \ldots, a_n)$ and $B := (b_0, b_1, \ldots, b_n)$ of length $n + 1$, where each $a_i, b_i \in \{+1, -1\}$. We have been viewing these as coefficients of polynomials, but it is common to view them just as sequences.

Define the *aperiodic correlation function* $A * B$ of A and B by

$$(A * B)_k := \sum_{j=0}^{n-k} a_j b_{j+k}$$

for $0 \le k \le n$, and $(A * B)_{-k} := (B * A)_k$. Write $(A * A)_k$ as $c_k(A)$, which, as before, is the *aperiodic autocorrelation function* of the sequence A (at shift k).

The information represented by the binary sequence A can be communicated over space; for example, by using the successive values a_i to modulate a carrier signal such as $\sin(\omega t)$ at predefined time intervals. The signal energy of the modulated sequence is given by c_0^2, whereas the wasted sidelobe energy is given by $\{c_k^2 : k \neq 0\}$.

The most efficient transmission is given by sequences having the largest ratio of signal energy to wasted energy. Such sequences are desirable in many signal processing applications such as spread-spectrum communication or position determination. Therefore we would like ideally to find a binary sequence having $c_k = 0$ for all $k \neq 0$. However, this is impossible because $c_k \equiv n-k+1 \pmod 2$. The next best thing would be to have $|c_k| = 0$ or 1 for all $k \neq 0$, which defines a Barker sequence, but unfortunately the longest known Barker sequence has $n = 12$. This motivates the definition of the *merit factor* $F := c_0^2 / \sum_{k \neq 0} c_k^2$ as a measure of how well suited a binary sequence is to signal transmission. This is usually written in the equivalent form $F = (n+1)^2 / \left(2 \sum_{k>0} c_k^2\right)$. (Note that in the sequence literature it is more usual to take the sequence length to be $N := n+1$ and so the merit factor would be written $N^2 / \left(2 \sum_{k>0} c_k^2\right)$.)

The behaviour of the optimal value of F as n varies is a study in its own right which we shall consider in more detail in the next chapter. For now, we note that there are applications for which even binary sequences with optimal merit factor, including the Barker sequences, waste too much signal energy. An alternative strategy is to define, as before, a *Golay complementary pair* of sequences A, B as satisfying the equation $c_k(A) + c_k(B) = 0$ for all $k \neq 0$. These sequence pairs were introduced by Golay [1949], [1951] to solve a problem in infrared multislit spectrometry, and have since found application in fields such as optical time domain reflectometry (Nazarathy et al. [1989]) and acoustic surface-wave encoding (Tseng [1971]).

As an example, we describe the system devised by Nazarathy et al. [1989], for which the wasted energy is proportional to the vanishing terms $c_k(A) + c_k(B)$. Define the *convolution function* $A \times B$ of A and B by $(A \times B)_k := \sum_{j=0}^{n-k} a_j b_{k-j}$ for $0 \le k \le n$, and $(A \times B)_{-k} := (B \times A)_k$. An *optical time domain reflectometer* is a measuring instrument for characterizing optical fibres. The instrument sends a probe signal X into the fibre and measures the return signal $X \times h$, where h is a discrete sampled version of the *impulse response function*. By determining h accurately, the instrument can infer the amount and location of the signal losses occurring in the fibre due to splices, connectors, and defects. The signal energy is spread over time using a binary sequence A to code a $(+1, -1)$ pulse train for X. Now suppose A and B are a Golay complementary pair. By probing first with A and then with B, we might seek to obtain the response functions $A \times h$ and $B \times h$. We could then proceed by calculating $A * (A \times h) + B * (B \times h)$, which, by an associative law, can be rewritten as $(A * A + B * B) \times h$. By the Golay complementary pair property, this equals $2n\delta \times h$, where

$$\delta_k := \begin{cases} 1 \text{ for } k = 0, \\ 0 \text{ for } k \neq 0. \end{cases}$$

We therefore recover $2nh$; in other words, a linear multiple of h. This method would work well for an acoustic application using an amplitude detector, but is unsuitable for a low-cost portable optical time domain reflectometer using an intensity detector (which measures the square of the amplitude and so cannot distinguish values in the response functions $A \times h$ and $B \times h$ having the same magnitude but different sign).

The simple ingenious solution of Nazarathy et al., which gave the best performance of any practical instrument when introduced, is to probe the fibre not with $(+1, -1)$ signals A and B but with $(0, 1)$ signals $(1 + A)/2$, $(1 - A)/2$, $(1 + B)/2$, and $(1 - B)/2$. The optical responses to the first two signals are $((1 + A)/2) \times h$ and $((1 - A)/2) \times h$, which can be measured by an intensity detector and subtracted to yield $A \times h$. Similarly, the responses to the second two signals can be used to produce $B \times h$. The instrument can then recover h as already described.

Introductory Exercises

E1. Suppose p is a Barker polynomial of odd degree $2n + 1$. Show

$$p(z) := q\left(z^2\right) + zr\left(z^2\right)$$

where q and r are polynomials of degree n that form a Golay pair.

For even degree $2n$, show that $a_k a_{n-k} + a_{k+1} a_{n-k-1} = 0$ for $0 \leq k \leq n + 1$, which then simplifies to $a_k a_{n-k} = (-1)^{k+n}$.

It is conjectured that no Barker polynomials exist for $n > 12$. See Saffari [1990] for more on Barker polynomials and a proof of the nonexistence of self-inversive Barker polynomials. In Turyn and Storer [1961] it is shown, as above, that no even-degree Barker polynomials exist for $n > 12$ (and indeed, as in Schmidt [1999] and subsequent work, none exist for any degree between 12 and 10^{20}). It can also be shown (see Turyn [1965]) that any odd-degree Barker polynomial of degree greater than 12 must have degree of the form $4s^2 - 1$, where s is an odd composite number.

E2. Suppose q and r are a Golay pair of degree n. Show that $n + 1 = a^2 + b^2$ for some integers a and b.

More generally, it is proved in Eliahou, Kervaire, and Saffari [1990] that if a Golay pair exists of degree n (and length $N := n + 1$), then N is even and has no prime factor congruent to 3 mod 4.

E3. Sketch of proof of Theorem 2 This is due to Turyn [1974]. Suppose A and B are a Golay complementary pair of degree m, and X and Y are a Golay complementary pair of degree n. Then U and V are a Golay complementary pair of degree $(m+1)(n+1)-1$, where

$$U(z) := \frac{A\left(z^{n+1}\right)\left(X(z)+Y(z)\right) - B^*\left(z^{n+1}\right)\left(X(z)-Y(z)\right)}{2}$$

and

$$V(z) := \frac{B\left(z^{n+1}\right)\left(X(z)+Y(z)\right) + A^*\left(z^{n+1}\right)\left(X(z)-Y(z)\right)}{2}.$$

Check that $1-z$ and $1+z$ are a Golay complementary pair, and check that

$$1 - z - z^2 + z^3 - z^4 + z^5 - z^6 - z^7 - z^8 + z^9$$

and

$$1 - z - z^2 - z^3 - z^4 - z^5 - z^6 + z^7 + z^8 - z^9$$

are a Golay complementary pair. Check also that

$$\begin{aligned} &- z^{25} + z^{24} - z^{23} + z^{22} + z^{21} + z^{20} - z^{19} - z^{18} + z^{17} + z^{16} + z^{15} + z^{14} - z^{13} \\ &\quad + z^{12} - z^{11} + z^{10} + z^9 + z^8 + z^7 - z^6 + z^5 + z^4 - z^3 - z^2 + z - 1 \end{aligned}$$

and

$$\begin{aligned} &- z^{25} + z^{24} - z^{23} + z^{22} + z^{21} + z^{20} - z^{19} - z^{18} + z^{17} + z^{16} + z^{15} + z^{14} + z^{13} \\ &\quad + z^{12} + z^{11} - z^{10} - z^9 - z^8 - z^7 + z^6 - z^5 - z^4 + z^3 + z^2 - z + 1 \end{aligned}$$

are a Golay complementary pair.

Observe that if $n = 2^a 10^b 26^c - 1$, then there exists a Golay complementary pair of degree n.

E4. The six operations $(q(z), r(z)) \mapsto$ (i) $(r(z), q(z))$, (ii) $(q(z), -r(z))$, (iii) $(-q(z), r(z))$, (iv) $(q^*(z), r(z))$, (v) $(q(z), r^*(z))$, (vi) $(q(-z), r(-z))$ map Golay pairs to Golay pairs. Show that the vertical orientation vector either remains the same or is complemented (mod 2) under each of these operations.

A more difficult exercise is to show that together, these generate a group of order 64 (see Djoković [1998]). Golay pairs in the same group orbit are *conjugates*. Show that for degree greater than 1, each pair has either 32 or 64 conjugates. Describe a method for normalizing pairs, i.e., finding a canonical representative from each conjugacy class.

E5. Express each of the four entries in a quad X_k in terms of components h_k, v_k, and s_k. Show that

$$X_iX_j = s_1s_2\,(1 - v_i - v_j + 2v_iv_j)\,(1 - h_i - h_j + 2h_ih_j)$$

and

$$X_iX_j^* = s_1s_2\,(1 - v_i - v_j + 2v_iv_j)\,(h_i + h_j - 2h_ih_j)\,.$$

Show that

$$s_is_j \equiv 2b_i + 2b_j + 1 \pmod 4,$$

for the sign vectors S and B_s.

Computational Problems

C1. Check that the following is a complete set of Barker polynomials of degree 20 or less. These are normalized to have the two leading coefficients positive and are all the known Barker polynomials:

$$z + 1,$$

$$z^2 + z - 1,$$

$$z^3 + z^2 - z + 1,$$

$$z^3 + z^2 + z - 1,$$

$$z^4 + z^3 + z^2 - z + 1,$$

$$z^6 + z^5 + z^4 - z^3 - z^2 + z - 1,$$

$$z^{10} + z^9 + z^8 - z^7 - z^6 - z^5 + z^4 - z^3 - z^2 + z - 1,$$

$$z^{12} + z^{11} + z^{10} + z^9 + z^8 - z^7 - z^6 + z^5 + z^4 - z^3 + z^2 - z + 1.$$

C2. Check that there are 128 Golay pairs of degree 9, 64 of degree 25, but none of degree 33, 49, or 57.

Research Problems

R1. Show that no Barker polynomials exist for $n > 12$.

R2. Are there any *primitive* Golay pairs for $n \geq 100$? (See Borwein and Ferguson [to appear].)

R3. If

$$p(z) := \sum_{k=0}^{n} a_k z^k,$$

where the a_k are complex numbers, then the kth *acyclic autocorrelation coefficient* is defined by

$$c_k := \sum_{j=0}^{n-k} \overline{a_j} a_{j+k} \quad \text{and} \quad c_{-k} := \overline{c_k}.$$

Then

$$\|p(z)\|_4^4 = \left\| p(z)\overline{p(z)} \right\|_2^2 = \sum_{k=-n}^{n} |c_k|^2.$$

A natural generalization of a Barker polynomial would be a polynomial whose coefficients are all complex numbers of modulus 1 that satisfies $|c_k| \leq 1$ for $k \neq 0$.

Do generalized Barker polynomials exist for all n?

Selected References

See Pott [1995] for how Barker sequences and Golay pairs fit into coding theory.

1. T. Andres and R. Stanton, *Golay sequences*, Combinatorial mathematics, V (Proc. Fifth Austral. Conf., Roy. Melbourne Inst. Tech., Melbourne, 1976), Lecture Notes in Math., Vol. 622, Springer, Berlin, (1977), 44–54.

2. P. Borwein and R. Ferguson, *A complete description of Golay pairs for lengths up to* 100, (to appear).

3. J.A. Davis and J. Jedwab, *Peak-to-mean power control in OFDM, Golay complementary sequences and Reed–Muller codes*, IEEE Trans. Inform. Theory **45** (1999), 2397–2417.

4. M.J. Golay, *Complementary series*, IRE Trans. **IT-7** (1961), 82–87.

5. A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, 1601, Springer-Verlag, Berlin, 1995.

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

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

8. R.J. Turyn, *Hadamard matrices, Baumert–Hall units, four-symbol sequences, pulse compression, and surface wave encodings*, J. Combinatorial Theory Ser. A **16** (1974), 313–333.

Chapter 15

The Littlewood Problem

The Littlewood problem concerns the size of the L_p norm on the boundary of D of Littlewood polynomials. When $p > 2$ it asks how small the L_p norm can be, and when $p < 2$ it asks how large the L_p norm can be. In both cases we are interested in how close these norms can be to the L_2 norm. Recall that the L_2 norm of a Littlewood polynomial of degree n is $\sqrt{n+1}$. That the behaviour changes at $p = 2$ is expected from *Hölder's inequality*, which gives, for $1 \le \alpha < \beta \le \infty$ and $\alpha^{-1} + \beta^{-1} = 1$, that

$$\|P\|_2^2 \le \|P\|_\alpha \|P\|_\beta.$$

The Littlewood Problem in L_p

The primary question of this section is how small the L_4 norm of a Littlewood polynomial can be. The L_4 norm is, after the L_2 norm, the most computationally tractable L_p norm to work with, since it can be computed algebraically from the coefficients. As in Chapter 14, if

$$p(z) := \sum_{k=0}^{n} a_k z^k$$

is a polynomial with real coefficients, then

$$p(z)p\left(\frac{1}{z}\right) = \sum_{k=-n}^{n} c_k z^k,$$

where, if $0 \le k \le n$, the autocorrelation coefficients are defined by

$$c_k := \sum_{j=0}^{n-k} a_j a_{j+k} \quad \text{and} \quad c_{-k} := c_k,$$

and
$$\|p(z)\|_4^4 = \left\| p(z)p\left(\frac{1}{z}\right) \right\|_2^2 = \sum_{k=-n}^{n} c_k^2.$$

The *merit factor* is defined, as in the previous chapter, by
$$F := \frac{c_0^2}{\sum_{k\neq 0} c_k^2} = \frac{\|p\|_2^4}{\|p\|_4^4 - \|p\|_2^4}.$$
The merit factor is a useful normalization. It tends to give interesting sequences integer limits, and "typically" the merit factor is around 1 for a polynomial with ± 1 coefficients (corresponding to an expected value of $2n^2 + 3n + 1$ for the fourth power of the L_4 norm). As we saw in Corollary 1 of Chapter 4, the Rudin–Shapiro polynomials have merit factors that tend to 3.

For polynomials with real coefficients of modulus 1 (that is, coefficients ± 1) it is conjectured that the merit factor is bounded above. This is equivalent to the next problem.

P7. The Merit Factor Problem of Golay. *Find the polynomial in $\mathcal{L}_n$ that has smallest possible L_4 norm on the unit disk. Show that there exists a positive constant c such that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_4 \geq (1+c)\sqrt{n+1}$.*

The best asymptotic bound known is 6, which is approached, for q prime, by the merit factors of
$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q}\right) z^k,$$
where $[\cdot]$ denotes the nearest integer. Here $(\frac{\cdot}{q})$ denotes the Legendre symbol. This is an old observation of Turyn's that was proved first in Høholdt and Jensen [1988]. Proofs are given in Appendix C. It follows from Theorem 2 below in a very precise fashion.

The asymptotic bound of 6 (and various other values) has been conjectured to be best possible, though not, in the author's opinion, for any compelling reason. The largest known merit factor belongs to the Barker polynomial of degree 12:
$$z^{12} + z^{11} + z^{10} + z^9 + z^8 - z^7 - z^6 + z^5 + z^4 - z^3 + z^2 - z + 1$$
which has merit factor 14.0833.... The second largest merit factor belongs to the Barker polynomial of degree 10 and is 12.1. No other merit factor greater than 10 is known. For all even degrees between 30 and 160, Littlewood polynomials are known with merit factor greater than 7. Mertens [1996], in the context of computing minima of the energy in the so-called Bernasconi Model, finds the largest merit factors for degree up to 47. (This has been extended now to 57.) The algorithm is a "branch and bound" algorithm with an apparent

running time of approximately 1.85^n. His data suggest that perhaps the limit of the largest merit factors might be around 9. Golay [1982] gives a heuristic argument based on something he calls "the ergodicity postulate" which suggests that the asymptotic limit is approximately 12.32.

A polynomial is *skewsymmetric* if $p(z) = \pm z^d p(-1/z)$, where d is the degree of p. Often, though by no means always, the extremals in the merit factor problem of even degree (and in Littlewood's problem) are skewsymmetric. This suggests searching over the skewsymmetric polynomials, where a search of roughly twice the degree possible for general Littlewood polynomials is reasonable. Note that if p is a skewsymmetric Littlewood polynomial, then it is of even degree, every other autocorrelation coefficient is zero, and $p(iz)$ is reciprocal or negative reciprocal.

Reciprocal Littlewood polynomials are shown to have bounded merit factors in Littlewood [1966]. See also Borwein and Erdélyi [to appear].

The merit factor of various shifted Fekete polynomials is explicitly given in terms of the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\alpha})$. For any odd prime d a formula for the class number is

$$h(-d) = \lambda_d \sum_{k=1}^{(d-1)/2} \left(\frac{k}{d}\right)(-1)^k,$$

where

$$\lambda_d := \begin{cases} 1 & \text{if } d \equiv 1, 7 \pmod 8, \\ \frac{1}{3} & \text{if } d \equiv 3 \pmod 8, \\ -1 & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

The following theorems are proved in Appendix C.

Theorem 1. *For q an odd prime, the Fekete polynomial*

$$f_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

satisfies

$$\|f_q\|_4^4 = \frac{5q^2}{3} - 3q + \frac{4}{3} - \gamma_q,$$

where

$$\gamma_q := \begin{cases} 0 & \textit{if } q \equiv 1 \pmod 4, \\ 12(h(-q))^2 & \textit{if } q \equiv 3 \pmod 4. \end{cases}$$

This shows that the merit factors of the Fekete polynomials approach $\frac{3}{2}$ as q tends to infinity.

Theorem 2. *For q an odd prime, the Turyn-type polynomials*

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q}\right) z^k,$$

where $[\cdot]$ *denotes the nearest integer, satisfy*

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

where

$$\gamma_q := \begin{cases} h(-q)\big(h(-q)-4\big) & \textit{if } q \equiv 1,5 \pmod 8, \\ 12\big(h(-q)\big)^2 & \textit{if } q \equiv 3 \pmod 8, \\ 0 & \textit{if } q \equiv 7 \pmod 8). \end{cases}$$

Thus these polynomials have merit factors asymptotic to 6. Golay, Høholdt and Jensen, and Turyn (and others) show that the merit factors of cyclically permuted character polynomials associated with nonprincipal real characters (the Legendre symbol) vary asymptotically between $\frac{3}{2}$ and 6. This is also made precise in Appendix C as follows. The L_4 norm of the shifted Fekete polynomial

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k+t}{q}\right) z^k$$

is given by

$$\|f_q^t\|_4^4 = \frac{1}{3}\left(5q^2+3q+4\right) + 8t^2 - 4qt - 8t - \frac{8}{q^2}\left(1 - \frac{1}{2}\left(\frac{-1}{q}\right)\right)\left|\sum_{n=1}^{q-1} n\left(\frac{n+t}{q}\right)\right|^2$$

if $t \le (q+1)/2$ is a positive integer.

Other L_p Norms

As in E5 of Chapter 1, for each positive even integer m (including infinity) and each positive integer n,

$$\max\{\|p\|_m : p \in \mathcal{L}_n\}$$

is attained by the polynomial $1 + z + z^2 + \cdots + z^n$. Klemeš [2001] proves that this extends for $2 < m < 4$ ($m \in \mathbb{R}$) and also that the above polynomials are extremals for $\min\{\|p\|_m : p \in \mathcal{L}_n\}$ for $0 < m < 2$. It seems likely that this should be true for $m > 4$ also.

For $m = 0$, the Littlewood polynomials that are products of cyclotomic polynomials are the unique minimizing polynomials in the L_0 norm (the Mahler measure).

In all other cases, characterizing either the minimum or maximum is open.

Littlewood's well-known conjecture of around 1948 asks for the minimum L_1 norm of polynomials of the form

$$p(z) := \sum_{j=0}^{n} a_j z^{k_j},$$

where the coefficients a_j are complex numbers of modulus at least 1 and the exponents k_j are distinct nonnegative integers. It states that such polynomials have L_1 norms on the unit circle that grow at least like $c \log n$ with an absolute constant $c > 0$. This was proved by Konyagin [1981] and independently by McGehee, Pigno, and Smith [1981]. It is believed that the minimum, for polynomials of degree n with complex coefficients of modulus at least 1, is attained by $1 + z + z^2 + \cdots + z^n$, but this too is open.

For polynomials with complex coefficients of modulus 1, it is possible to have asymptotically unbounded merit factors, as the following example (mostly due to Littlewood [1961]) shows. Let

$$W_n(z) := \sum_{k=0}^{n-1} e^{k(k+1)\pi i/n} z^k.$$

Then

$$\|W_n\|_4^4 = n^2 + \frac{2n^{3/2}}{\pi} + \delta_n \frac{n^{1/2}}{3} + O\left(n^{-1/2}\right),$$

where

$$\delta_n := \begin{cases} -2 & \text{if } n \equiv 0, 1 \pmod 4, \\ 1 & \text{if } n \equiv 2, 3 \pmod 4. \end{cases}$$

Littlewood shows, for odd n, that

$$\frac{|W_n(z)|}{\sqrt{n}} \to 1$$

uniformly for all z of modulus 1 except in a neighbourhood of 1. He also shows that

$$\frac{|W_n(z)|}{\sqrt{n}} \le 1.35$$

for all z of modulus 1. From this, one sees that for each $p \ge 0$,

$$\frac{\|W_n\|_p}{\sqrt{n}} \to 1.$$

Actually, Littlewood shows that on $|z| = 1$,

$$\frac{|W_n(z)|}{\sqrt{n}} = 1 + O\left(n^{-1/2+\delta}\right)$$

except in a neighbourhood of 1 of radius $n^{-\delta}$.

One can compute the expected L_p norms of random Littlewood polynomials $q_n \in \mathcal{L}_n$ and their derivatives. Specifically, in Borwein and Lockhart [2001] it is shown that

$$\frac{\mathrm{E}(\|q_n\|_p)}{n^{1/2}} \to \left(\Gamma\left(1 + \frac{p}{2}\right)\right)^{1/p},$$

so for example, the expected normalized L_4 norm of a Littlewood polynomial of degree n tends to $2^{1/4}$. (See also E4 of Chapter 4, where the exact value is derived.) For derivatives,

$$\frac{\mathrm{E}(\|q_n^{(r)}\|_p)}{n^{(2r+1)/2}} \to (2r+1)^{-1/2}\left(\Gamma\left(1+\frac{p}{2}\right)\right)^{1/p}.$$

From this and the inequality

$$\frac{\|q_n'\|_p}{n\|q_n\|_p} \le 1$$

one can also deduce an expected Bernstein inequality for Littlewood polynomials, namely,

$$\mathrm{E}\left(\frac{\|q_n'\|_p}{n\|q_n\|_p}\right) \to \frac{1}{\sqrt{3}}.$$

This should be compared to interesting results of Nazarov and of Queffélec and Saffari [1996], which say that

$$\max_{q_n \in \mathcal{L}_n} \frac{\|q_n'\|_p}{n\|q_n\|_p} \to 1$$

for all $p > 1$, except $p = 2$ where the lim sup is $1/\sqrt{3}$.

The Littlewood Problem in L_∞

The principal problem of this section is due to Littlewood, probably from sometime in the 1950s. It is discussed in some detail in Littlewood [1968].

P4. Littlewood's Problem in L_∞. *Show that there exist positive constants c_1 and c_2 such that for any n (or at least for infinitely many n) it is possible to find $p_n \in \mathcal{L}_n$ with*

$$c_1\sqrt{n+1} \le |p_n(z)| \le c_2\sqrt{n+1}$$

for all complex z with $|z| = 1$.

Such polynomials are often called "flat." Because the L_2 norm of a polynomial from $\mathcal{L}_n$ is exactly $\sqrt{n+1}$, the constants must satisfy $c_1 < 1$ and $c_2 > 1$. Littlewood partly based his conjecture on computations of all such polynomials up to degree 20. Odlyzko has now done extensive computations that tend to confirm the conjecture. However, it is still the case that no sequence is known that satisfies just the lower bound, although computations in Robinson [1997] tend to suggest that the lower bound can be satisfied with a constant $c_1 > 0.6$. As we have seen in Chapter 4, a sequence of Littlewood polynomials that satisfies just the upper bound is given by the Rudin–Shapiro polynomials.

The best known lower bounds in Littlewood's problem arise as in C1 of Chapter 4. Suppose $p \in \mathcal{L}_n$ satisfies

$$|p(z)| \ge (n+1)^{\alpha}$$

for all z of modulus 1. Then $q(z) := p(z^{n+1})p(z)$ is in $\mathcal{L}_d$, where the degree is $d = (n+1)^2 - 1$, and

$$|q(z)| \geq (d+1)^\alpha$$

for all z of modulus 1. So any particular example that gives rise to an α as above gives an infinite sequence of examples. The best α known that arises in this fashion is $0.4308\ldots$. It comes from the Barker polynomial of degree 12.

The conjecture P4 is refined by a conjecture of Erdős [1962].

P5. Erdős's Problem in L_∞. *Show that there exists a positive constant c_3 such that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \geq (1+c_3)\sqrt{n+1}$.*

This is also still open, though a remarkable result due to Kahane [1980] shows that if the polynomials are allowed to have complex coefficients of modulus 1, then "flat" polynomials exist, and indeed, that it is possible to make c_1 and c_2 asymptotically arbitrarily close to 1. Another striking result, due to Beck [1991b], proves that "flat" polynomials exist from the class of polynomials of degree n whose coefficients are 1200th roots of unity.

The merit factor problem of the last chapter conjectures, for $p \in \mathcal{L}_n$ and n sufficiently large, that $\|p\|_4^4 \geq (1+\delta)(n+1)^2$. This, of course, implies Erdős's conjecture above.

Littlewood [1961] gives a proof of Erdős's problem for real trigonometric polynomials. We offer the following easy resolution of P5 for reciprocal Littlewood polynomials.

Theorem 3. *Let P be a reciprocal Littlewood polynomial of degree n. Then*

$$\|P(z)\|_\infty \geq \sqrt{\frac{4}{3}}\sqrt{n+1}.$$

Proof. Let P be a reciprocal Littlewood polynomial of degree n. Observe that Inequality 10 of Appendix A gives

$$\|P'(z)\|_\infty \leq \frac{n}{2}\|P(z)\|_\infty.$$

So with Parseval's formula, we have

$$\begin{aligned} 2\pi\,\frac{(n+1)n^2}{3} &\leq 2\pi\,\frac{n(n+1)(2n+1)}{6} \\ &= \frac{1}{2\pi}\int_0^{2\pi} |P'(e^{i\theta})|^2\,d\theta \\ &\leq 2\pi\left(\frac{n}{2}\right)^2 \|P(z)\|_\infty^2, \end{aligned}$$

and

$$\|P(z)\|_\infty \geq \sqrt{\frac{4}{3}}\sqrt{n+1}$$

follows. □

Konyagin [1997] conjectures the following for polynomials in $\mathcal{A}$: for any *fixed* set $E \subset \partial D$ (the boundary of the unit disk) of positive measure there exists a constant $c(E) > 0$ (depending only on E) such that for any distinct positive integers k_j and any integer n,

$$\int_E \left| \sum_{j=0}^{n} z^{k_j} \right| |dz| \geq c(E).$$

In the same paper he shows that for each positive ϵ, there exists a set $E_\epsilon \subset \partial D$ of measure π and a choice of exponents k_j such that

$$\int_{E_\epsilon} \left| \sum_{j=0}^{n} z^{k_j} \right| |dz| < \epsilon.$$

However, if his conjecture is correct, E_ϵ must vary with ϵ.

Konyagin's conjecture is proved for subarcs. Borwein and Erdélyi [1997b] show that Littlewood polynomials (and many other related polynomials) cannot be arbitrarily small on any fixed subarc of the unit circle, and as a consequence, the following holds.

Theorem 4. *Let A be a fixed subarc of the unit circle. If $\{p_k\}$ is a sequence of monic polynomials that tends to 0 in $L_1(A)$, then the sequence $H(p_k)$ of heights tends to ∞.*

Introductory Exercises

E1. Show that if p is in $\mathcal{L}_n$, then

$$\|p\|_4 \geq \left((n+1)^2 + n\right)^{1/4}$$

with equality only if p is a Barker polynomial of even degree.

There is no better lower bound known.

E2. Let

$$W_n(z) := \sum_{k=0}^{n-1} e^{k(k+1)\pi i/n} z^k.$$

Show that

$$\|W_n\|_4^4 = n^2 + O\left(n^{3/2}\right).$$

Show that

$$W_n(-\zeta_n z) = zW_n(z) + \left(1 + (-z)^n\right),$$

where $\zeta_n := \exp(2\pi i/n)$. Deduce that W_n is of constant modulus at nth roots of unity when n is odd.

E3. Show that a reciprocal Littlewood polynomial of sufficiently large degree has at least one zero of modulus 1.

E4. Show that if $\{p_n\}$ is a sequence of Littlewood polynomials (with $p_n \in \mathcal{L}_n$) and $0 < \alpha < \beta$, then

$$\frac{\|p_n\|_\beta}{\sqrt{n+1}} \to 1$$

implies

$$\frac{\|p_n\|_\alpha}{\sqrt{n+1}} \to 1.$$

E5. Show that if $\{p_n\}$ is a sequence of Littlewood polynomials (with $p_n \in \mathcal{L}_n$), then

$$\frac{\|p_n\|_4}{\sqrt{n+1}} \to 1$$

implies

$$\frac{|p_n(z)|}{\sqrt{n+1}} \to 1$$

for almost every z of modulus 1.

Hint:

$$\frac{\|p_n\|_4^4}{(n+1)^2} - 1 = \frac{1}{2\pi}\int_0^{2\pi} \left(\frac{|p_n(e^{i\theta})|^2}{(n+1)^2} - 1\right)^2 d\theta.$$

□

E6. Golomb Rulers. Consider polynomials of the form

$$p(z) = z^{\alpha_1} + z^{\alpha_2} + \cdots + z^{\alpha_k},$$

where $0 \le \alpha_1 < \alpha_2 < \cdots < \alpha_k$. Let $\mathcal{G}_k$ denote the collection of all such polynomials.

Show that $p(z) \in \mathcal{G}_k$ satisfies

$$\|p(z)\|_4 \ge \left(2k^2 - k\right)^{1/4}$$

with equality iff all differences of pairs of elements of $A := \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ are distinct.

The problem of finding the *minimum* value of α_k for which there exists a set $\{0 = \alpha_1 < \alpha_2 < \cdots < \alpha_k\}$ of integers such that the differences $\alpha_j - \alpha_i$ are all distinct is sometimes called the Golomb ruler problem.

Show that this minimum exists for all k, and find the minimum for $k \le 10$.

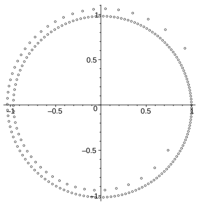
Computational Problems

C1. Find the maximal merit factors of Littlewood polynomials for degrees up to 40. Do the same calculation for symmetric and skewsymmetric Littlewood polynomials for degrees up to 80.

C2. Golay and Harris [1990] suggest a heuristic for finding Littlewood polynomials of degree $2n$ with large merit factors. The idea is to find skewsymmetric Littlewood polynomials for which the even part and odd part both have a relatively large merit factor. Explore this heuristic.

C3. Examine the zeros of the polynomials W_n.

The zeros of W_{200}.



C4. Construct a program to find the optimal polynomials in Littlewood's conjecture, and run it up to degree at least 20.

As before, a polynomial is skewsymmetric if $p(z) = \pm z^d p(-1/z)$, where d is the degree of p.

Extend the above search as far as reasonable for skewsymmetric polynomials.

Research Problems

R1. Find the maximal merit factors of Littlewood polynomials for degrees up to 100.

R2. Prove that the merit factor of Littlewood polynomials is bounded above independently of the degree.

R3. Prove the conjecture of Konyagin [1997]: for any *fixed* set $E \subset \partial D$ (the boundary of the unit disk) of positive measure there exists a constant $c(E) > 0$ (depending only on E) such that for any distinct positive integers k_j and any integer n,

$$\int_E \left| \sum_{j=0}^{n} z^{k_j} \right| |dz| \geq c(E).$$

R4. What is the minimum number of zeros of modulus 1 of a real-valued Littlewood polynomial of degree n?

Littlewood [1966, problem 22] poses the following research problem, which appears to still be open: "If the n_m are integral and all different, what is the lower bound on the number of real zeros of $\sum_{m=1}^{N} \cos(n_m \theta)$? Possibly $N-1$, or not much less."

R5. Erdős's Problem in L_∞ for Reciprocal Polynomials. *Show that there exists a positive constant c such that for all sufficiently large n and all reciprocal polynomials $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \geq \left(\sqrt{2}+c\right)\sqrt{n+1}$.*

This implies Erdős's problem (P5). It is supported by computational evidence up to degree 50 or so. "Sufficiently large" in this case may well mean $n > 8$.

Selected References

1. J. Beck, *Flat polynomials on the unit circle—note on a problem of Littlewood*, Bull. London Math. Soc. **23** (1991), 269–277.

2. P. Borwein and S. Choi, *Explicit merit factor formulae for Fekete and Turyn polynomials*, Trans. Amer. Math. Soc. **354** (2002), 219–234.

3. P. Borwein and T. Erdélyi, *Littlewood-type problems on subarcs of the unit circle*, Indiana Univ. Math. J. **46** (1997), 1323–1346.

4. M.J. Golay and D.B. Harris, *A new search for skewsymmetric binary sequences with optimal merit factors*, IEEE Trans. Inform. Theory **36** (1990), 1163–1167.

5. J. Jensen, H. Jensen, and T. Høholdt, *The merit factor of binary sequences related to difference sets*, IEEE Trans. Inform. Theory **37** (1991), 617–626.

6. J.-P. Kahane, *Sur les polynômes à coefficients unimodulaires*, Bull. London Math. Soc. **12** (1980), 321–342.

7. J.-P. Kahane, *Some Random Series of Functions*, Cambridge Studies in Advanced Mathematics, Cambridge, 1985.

8. S. Konyagin, *On a question of Pichorides*, C. R. Acad. Sci. Paris Sér. I Math. **324** (1997), 385–388.

9. J.E. Littlewood, *On the mean values of certain trigonometric polynomials*, J. London Math. Soc. **36** (1961), 307–334.

10. J.E. Littlewood, *On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$*, J. London Math. Soc. **41** (1966), 367–376.

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

Chapter 16

Spectra

In this chapter, we examine *spectra*, the sets of values which result when various classes of polynomials are evaluated at a fixed number q. When this class is $\mathcal{F}$ and q is a Pisot number, the *spectrum*

$$\{p(q) : p \in \mathcal{F}\}$$

is, quite surprisingly, discrete. Indeed, from E1 of Chapter 3, we have that for q a Pisot number and $p \in \mathcal{Z}$ of height h with q not a root of p,

$$|p(q)| \geq c(q, h),$$

where the positive constant $c(q, h)$ depends only on q and h. This suggests the question of establishing the exact value for $c(q, h)$. Specifically, we search for the minimum positive value in the spectrum of height h polynomials evaluated at a number q, where q is between 1 and 2.

Erdős, Joó, and Komornik [1990] look at spectra with respect to the class of polynomials $\mathcal{A}$ in the following way. Consider

$$Y(q) := \{p(q) : p \in \mathcal{A}\} = \left\{0, 1, q, q+1, q^2, q^2+1, q^2+q, \dots\right\},$$

ordered as $0 = y_0 < y_1 < y_2 < y_3 < \cdots$. They show that for $q > \tau$ (where τ is the golden ratio), there exist infinitely many k where $y_{k+1} - y_k = 1$. They also show that if $q < \tau$ and q is a Pisot number, then $y_{k+1} - y_k \not\to 0$.

Erdős, Joó, and Joó [1992] show further that $y_{k+1} - y_k \leq 1$ for all k, and if q is the Pisot number which is a root of $z^n - z^{n-1} - \cdots - 1 = 0$, then

$$\liminf(y_{k+1} - y_k) = 1/q.$$

(To see that $\liminf(y_{k+1} - y_k) \leq 1/q$, see E8.) They ask which other q make this infimum strictly greater than 0. We denote this infimum by

$$l(q) := \liminf(y_{k+1} - y_k).$$

We define wider classes of spectra by

$$Y^m(q) := \{p(q) : p(z) := \epsilon_n z^n + \cdots + \epsilon_0, \epsilon_i \in \{0, \ldots m\}\}$$

which we order as $y_0^m = 0 < y_1^m < y_2^m < y_3^m < \cdots$. We extend the definition of $l(q)$ in the obvious way to

$$l^m(q) := \liminf \left(y_{k+1}^m - y_k^m\right).$$

It is clear that

$$l(q) = l^1(q) \geq l^2(q) \geq l^3(q) \geq \cdots \geq 0.$$

Bugeaud [1996] proves the following result.

Theorem 1. *If $q \in (1,2)$, then $l^k(q) > 0$ for all k if and only if q is a Pisot number.*

He also studies the related problem of $\limsup(y_{k+1} - y_k)$. Define

$$L^m(q) := \limsup \left(y_{k+1}^m - y_k^m\right).$$

Clearly, $L^1(q) \geq L^2(q) \geq \cdots \geq 0$ and $L^m(q) \geq l^m(q)$.

Bugeaud shows that $L^1(q) < 1$ for all $q < \tau$, and $L^2(q) < 1$ for all $\tau \leq q < 2$. He also shows that if q is not a root of a polynomial of height 1, then $l(q) = 0$ by a pigeonhole argument (see E4).

A good overview of these problems is found in Joó and Schnitzer [1996]. They list a number of problems, all of which are still open at the time of the printing of this book. These include:

1. For $q \in (1,2)$, is $l(q) > 0$ if and only if q is a Pisot number?
2. For $1 < q < \tau$, does $l(q) = 0$ imply $L^1(q) = 0$?
3. If $1 < q < q_1$ (where q_1 is the smallest Pisot number), is $l(q) = 0$?

In the study of $l^m(q)$, we wish to find the minimal positive value in $Y^m(q) - Y^m(q)$. Since $Y^m(q) - Y^m(q)$ is the set of all height m polynomials evaluated at q, we are led to the definitions

$$\Lambda(q) := \{p(q) : p \in \mathcal{F}\}$$

and

$$\Lambda^m(q) := \{p(q) : p \in \mathcal{Z}, H(p) \leq m\}.$$

We can equivalently define $l(q)$ and $l^m(q)$ as

$$l(q) := \inf\{|y| : y \in \Lambda(q), y \neq 0\}$$

and

$$l^m(q) := \inf\{|y| : y \in \Lambda^m(q), y \neq 0\}$$

(see E2 for this equivalence).

There are a variety of further results by Erdős and Komornik [1998], including the following.

Theorem 2.

(a) *If q is not a Pisot number and $m \geq q - q^{-1}$, then $\Lambda^m(q)$ has a finite accumulation point.*

(b) *If $q \in (1,2)$ is not a Pisot number, then $l^m(q) = 0$ for all $m \geq \lceil q - q^{-1} \rceil + \lceil q - 1 \rceil$.*

(c) *If $1 < q \leq 2^{1/4}$ and if q^2 is not the first or second Pisot number, then $l^m(q) = 0$ for all m.*

Komornik, Loreti, and Pedicini [2000] show that if q is the Pisot number which is a root of $z^3 - z^2 - 1$, then $l(q) = q^2 - 2$. For general m, and q the golden ratio, they give a complete description for $l^m(q)$. If F_k is the kth Fibonacci number ($F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$), and $q^{k-2} < m \leq q^{k-1}$, then $l^m(q) = |F_k q - F_{k+1}|$.

These results are extended to all unit quadratic Pisot numbers by Borwein and Hare [to appear] in the following way. (*Unit quadratic* Pisot numbers are Pisot numbers that satisfy polynomials of the form $z^2 - az \pm 1$.)

Theorem 3. *Let q be a unit quadratic Pisot number with conjugate r. If q has continued fraction approximations $\{C_n/D_n\}$, and k is the greatest integer such that*

$$|D_k r - C_k| \leq m \frac{1}{1 - |r|},$$

then

$$l^m(q) = |D_k q - C_k|.$$

Another spectrum that is studied is the class of ± 1 polynomials evaluated at q, defined by

$$A(q) := \{p(q) : p \in \mathcal{L}\}$$

with the minimal value $a(q)$ defined by

$$a(q) := \inf\{|y| : y \in A(q), y \neq 0\}.$$

Determining which $q \in (1,2)$ make $A(q)$ discrete is of interest. A spectrum Λ is *discrete* if for any finite interval $[a,b]$ of the real line, $\Lambda \cap [a,b]$ has only a finite number of elements. A spectrum is *uniformly discrete* if there exists an ϵ greater than zero such that any two distinct values in the spectrum are at least ϵ apart. A spectrum is *nonuniformly discrete* if it is discrete but not uniformly discrete. Peres and Solomyak [2000] show that if q is a Pisot number, then $A(q)$ is uniformly discrete. However, examples of q where $A(q)$ is nonuniformly discrete are given in Borwein and Hare [to appear] and in the exercises.

It is clear that $A(q) \subset \Lambda(q)$. Peres and Solomyak prove the next result.

Theorem 4. *$A(q)$ is dense in $\mathbb{R}$ for almost every $q \in (\sqrt{2}, 2)$. Also, if $q \in (1, \sqrt{2})$ and q^2 is not the root of a height 1 polynomial, then $A(q)$ is dense.*

An Algorithm for Computing Spectra

There are good algorithms that allow for a computational exploration of various spectra. An algorithm to determine $\Lambda(q) \cap [-1/(q-1), 1/(q-1)]$ is given by Lau [1993]. This algorithm is extended by Borwein and Hare [to appear] as follows. Let S be a finite set of integers with s_l the smallest and s_u the largest. Let p be a polynomial with coefficients in S, and let $q > 1$. Set $\alpha_l := -s_u/(q-1)$ and $\alpha_u := -s_l/(q-1)$. If $p(q) \notin [\alpha_l, \alpha_u]$, then $q\,p(q) + s \notin [\alpha_l, \alpha_u]$ for all $s \in S$ (see E3). Thus, if $p(q) \notin [\alpha_l, \alpha_u]$, it follows that if $p_s(z)$ is a polynomial with coefficients in S whose leading terms are equal to $z^k p(z)$ for some k, then $p_s(q) \notin [\alpha_l, \alpha_u]$, and thus $p_s(z)$ can be ignored in a search for spectral values in $[\alpha_l, \alpha_u]$. Further, if $\alpha_l^* \le \alpha_l$ and $\alpha_u^* \ge \alpha_u$, then the same result follows for the range $[\alpha_l^*, \alpha_u^*]$. The fact that $\Lambda^m(q)$ is uniformly discrete for q Pisot gives that $|\Lambda^m(q) \cap [a, b]|$ is finite. This guarantees that the algorithm terminates.

The algorithm below takes as input an algebraic number q and a set of integers S which are the coefficients of the polynomials considered for the spectrum. It returns the spectrum in $[\alpha_l, \alpha_u]$.

```
Spec(S, q)
  α_u := -min(s:s∈S) / (q-1);
  α_l := -max(s:s∈S) / (q-1);
  L_0 := S;
  d := 0;
  repeat
    L_{d+1} := L_d;
    for p ∈ L_d, s ∈ S do
      if q * p + s ∈ [α_l, α_u] then
        L_{d+1} = L_{d+1} union {qp + s}
      end if
    end do
    d := d + 1;
  until L_{d+1} = L_d;
  RETURN(L_d);
end;
```

It is often an advantage to compute exactly using the minimal polynomials of q, so as to avoid floating-point errors.

This algorithm allows us to compute various spectra. For example, for $\Lambda_m(q)$ we use $S = \{-m, \dots, m\}$, and for $A(q)$ we use $S = \{\pm 1\}$. It performs surprisingly well. Many of the exercises are based on these explorations. A small example of how this algorithm works is given below.

Let us compute $\Lambda(q)\cap[-1/(q-1), 1/(q-1)]$ for q satisfying q^3-2q^2+q-1. So we have (to nine decimal places) $q = 1.754877666$ and $1/(q-1) = 1.324717958$. Printed below are the various values of L_d.

$$
\begin{aligned}
L_0 &= [-1, 0, 1],\\
L_1 &= [-1, -0.754877666, 0, 0.754877666, 1],\\
L_2 &= [-1.324717957, -1, -0.754877666, -0.324717957, 0, 0.324717957,\\
&\quad 0.754877666, 1, 1.324717957],\\
L_3 &= [-1.324717957, -1, -0.754877666, -0.569840291, -0.430159709,\\
&\quad -0.324717957, 0, 0.324717957, 0.430159709, 0.569840291, 0.754877666,\\
&\quad 1, 1.324717957],\\
L_4 &= [-1.324717957, -1, -0.754877666, -0.569840291, -0.430159709,\\
&\quad -0.324717957, -0.245122334, 0, 0.245122334, 0.324717957,\\
&\quad 0.430159709, 0.569840291, 0.754877666, 1, 1.324717957],\\
L_5 &= [-1.324717957, -1, -0.754877666, -0.569840291, -0.430159709,\\
&\quad -0.324717957, -0.245122334, 0, 0.245122334, 0.324717957,\\
&\quad 0.430159709, 0.569840291, 0.754877666, 1, 1.324717957].
\end{aligned}
$$

Since $L_5 = L_4$, we see that the algorithm has terminated. From this we see that the minimal element in the spectrum is $l(q) = 0.245122334$.

Introductory Exercises

E1. Show that $l^m(q) > 0$ for all m and for all Pisot numbers q.

Hint: See E1 of Chapter 3. □

E2. Show that $\Lambda(q) = Y(q) - Y(q)$. (Hence the two definitions for $l(q)$ are equivalent.)

E3. Let S be a finite set of integers with s_l the smallest and s_u the largest. Let p be a polynomial with coefficients in S, and let $q > 1$. Set $\alpha_u := -s_l/(q-1)$ and $\alpha_l := -s_u/(q-1)$. Show that if $p(q) \notin [\alpha_l, \alpha_u]$, then $q\,p(q) + s \notin [\alpha_l, \alpha_u]$ for all $s \in S$.

E4. Show that if q is not a root of a height 1 polynomial, then $l(q) = 0$.

Hint: Find the average distance between $y_{k+1} - y_k$ if $Y(q)$ is restricted to polynomials of degree n. □

E5. Show that if q is not a root of a polynomial of the form

$$\epsilon_n z^n + \cdots + \epsilon_m z^m + \beta_{m-1} z^{m-1} + \cdots + \beta_0,$$

where $\epsilon_i \in \{\pm 1\}$ and $\beta_i \in \{\pm 2, 0\}$, then $A(q)$ is not discrete. (As a corollary, notice that all Pisot numbers in $(1,2)$ must be a root of a polynomial of this form.)

Hint: Consider the sequence $P_0 = 1$, $P_n = 1 - q\,P_{n-1}$ if $q\,P_{n-1} < 1$ and $P_n = q\,P_{n-1} - 1$ if $q\,P_{n-1} > 1$. □

E6. Show that if $l(q) = 0$, then $A(q)$ is not uniformly discrete, and if $A(q)$ is not uniformly discrete, then $l^2(q) = 0$.

Hint: Show that $2\Lambda(q) \subseteq A(q) - A(q) \subseteq \Lambda^2(q)$. □

E7. Show that if $1 < q$ is a root of the polynomial $z^n - z^{n-1} - z^{n-2} - \cdots - z^2 - z + 1$, then $A(q)$ is discrete. (This q is a Salem number, as follows from E6 of Chapter 3.)

Hint: Consider the algorithm of this chapter, and show that at each step the number of polynomials added to the spectrum is bounded, and that it eventually terminates. □

E8. Show that if q is the Pisot number which is a root of $z^n - z^{n-1} - \cdots - 1$, then $l(q) \leq 1/q$.

Hint: Find a $p \in \mathcal{F}$ such that $p(q) = 1/q$. □

Computational Problems

C1. Write programs to compute $a(q)$ and $l^m(q)$.

C2. Compute $a(q)$, where q is the Pisot number which is a root of $z^3 - 2z - 2$, to show that $a(q) > 0$. Notice by E3 that $l(q) = 0$ in this case. Thus by E6, $A(q)$ is nonuniformly discrete.

C3. Duplicate the results of Komornik, Loreti, and Pedicini [2000] by computing $l(q)$, where q is the Pisot number which is a root of $z^3 - z^2 - 1$.

C4. Compute $l^m(q)$, where q is the Pisot number which is a root of $z^3 - z - 1$, for various m. Compute $1/q^k$ for various k.

C5. Compute the spectrum of $A(q)$, where q is the Pisot number which is a root of $z^6 - z^5 - 2z^4 + z^2 - z - 1$, and show that $0 \notin A(q)$. Find other Pisot numbers with this property.

Research Problems

R1. Let $q \in (1,2)$. Show that $l(q) > 0$ if and only if q is a Pisot number.

R2. Find an algorithm that computes $L^1(q)$.

Selected References

1. P. Borwein and K.G. Hare, *Some computations on the spectra of Pisot and Salem numbers*, Math. Comp. (to appear).

2. P. Borwein and K.G. Hare, *General forms for minimal spectral values for a class of quadratic Pisot numbers*, J. London Math. Soc. (to appear).

3. P. Erdős, I. Joó, and V. Komornik, *Characterization of the unique expansions $1 = \sum_{i=1}^{\infty} q^{-n_i}$ and related problems*, Bull. Soc. Math. France **118** (1990), 377–390.

4. I. Joó and F.J. Schnitzer, *On some problems concerning expansions by noninteger bases*, Anz. Österreich. Akad. Wiss. Math.-Natur. Kl. **133** (1996), 3–10.

5. Y. Peres and B. Solomyak, *Approximation by polynomials with coefficients* ± 1, J. Number Theory **84** (2000), 185–198.

Appendix A

A Compendium of Inequalities

We collect a compendium of the most useful inequalities for polynomials on the unit disk. Most of the inequalities in this section may be found in either Borwein and Erdélyi [1995] or Milovanović, Mitrinović, and Rassias [1994].

We first reintroduce the standard notation. As before, let

$$D := \{z \in \mathbb{C} : |z| < 1\} \qquad \text{and} \qquad K := \mathbb{R} \pmod{2\pi}.$$

We let $\mathcal{P}_n^c$ (resp. $\mathcal{P}_n$) denote the set of algebraic polynomials of degree at most n with complex (resp. real) coefficients, and denote the set of trigonometric polynomials of degree at most n by $\mathcal{T}_n$. More precisely,

$$\mathcal{T}_n := \left\{ t : t(z) = a_0 + \sum_{k=1}^{n} (a_k \cos kz + b_k \sin kz), \quad a_k, b_k \in \mathbb{R} \right\}.$$

The *supremum norm*, or L_∞ norm, on a set A is denoted by $\|\cdot\|_A$. For positive α, the L_α norm on the boundary of the unit disk is defined by

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

For a polynomial

$$p(z) := a_n z^n + \cdots + a_1 z + a_0 = a_n(z - z_1)(z - z_2) \cdots (z - z_n),$$

the L_2 norm on D is also given by

$$\|p\|_2 = \sqrt{|a_n|^2 + \cdots + |a_1|^2 + |a_0|^2}.$$

In the two limiting cases,

$$\lim_{\alpha \to \infty} \|p\|_\alpha = \|p\|_D := \|p\|_\infty$$

and
$$\lim_{\alpha\to 0} \|p\|_\alpha = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log(|p(e^{i\theta})|)\,d\theta\right) =: \|p\|_0.$$
This latter quantity is the *Mahler measure* and is denoted by $M(p)$. It has the alternative form
$$M(p_n) = |a_n| \prod_{|z_i|\geq 1} |z_i|.$$
For $0 \leq \alpha \leq \beta$,
$$\|f\|_\alpha \leq \|f\|_\beta,$$
and for $0 < r < s < t$,
$$\|f\|_s^s \leq (\|f\|_r^r)^{\frac{t-s}{t-r}} (\|f\|_t^t)^{\frac{s-r}{t-r}}.$$
If $1 \leq \alpha < \beta \leq \infty$ and $\alpha^{-1} + \beta^{-1} = 1$, then *Hölder's inequality* states that
$$\|f\,g\|_1 \leq \|f\|_\alpha \|g\|_\beta.$$

The *height* of a polynomial p, denoted by $H(p)$, is just the size of the largest coefficient of p. The *length* is denoted by $L(p)$ and is just the sum of the absolute values of the coefficients of p. If $p(z) := a_n z^n + \cdots + a_1 z + a_0$, then
$$L(p) := l_1(p) := |a_n| + \cdots + |a_1| + |a_0|$$
and
$$H(p) := \max\{|a_n|, \ldots, |a_1|, |a_0|\}.$$
The length is also the l_1 norm, where generally,
$$l_\alpha(p) := \left(|a_n|^\alpha + \cdots + |a_1|^\alpha + |a_0|^\alpha\right)^{1/\alpha}.$$

Norm Inequalities

1. Bernstein's Inequality for Trigonometric Polynomials. For $t \in \mathcal{T}_n$ and $\theta \in \mathbb{R}$,
$$|t'(\theta)| \leq n\|t\|_K.$$

2. An Inequality of Bernstein. For $p \in \mathcal{P}_n^c$ and $|z| \geq 1$,
$$|p(z)| \leq |z|^n \|p\|_D.$$

3. Bernstein's Inequality on the Disk. For $p \in \mathcal{P}_n^c$ and $|z| \geq 1$,
$$|p'(z)| \leq n|z|^{n-1} \|p\|_D.$$

4. Bernstein-Type Inequality in L_α. For $t \in \mathcal{T}_n$ and $\alpha \geq 0$,

$$\int_0^{2\pi} |t'(\theta)|^\alpha \, d\theta \leq n^\alpha \int_0^{2\pi} |t(\theta)|^\alpha \, d\theta.$$

Equivalently, for $\in \mathcal{P}_n^c$ and $\alpha \geq 0$,

$$\|p'(z)\|_\alpha \leq n\|p(z)\|_\alpha.$$

For $\alpha \geq 1$, this is due to Zygmund. The extension for $\alpha \geq 0$ is due to Nevai. Von Golitschek and Lorentz [1989] give a simpler proof of this. For $\alpha = 0$, the result is due to Mahler; a proof of this case may be found in Everest and Ward [1999].

If p has no zeros in D, then de Bruijn shows, for $\alpha \geq 1$, that

$$\|p'(z)\|_\alpha \leq c_\alpha n\|p(z)\|_\alpha,$$

where

$$c_\alpha^\alpha = \frac{\sqrt{\pi}\,\Gamma\left(\frac{\alpha}{2}+1\right)}{2^\alpha \Gamma\left(\frac{\alpha}{2}+\frac{1}{2}\right)}.$$

5. An Inequality of Szegő. If $p \in \mathcal{P}_n^c$ and $z_1, z_2, \ldots, z_{2n}$ are any equally spaced points on the unit circle ∂D, then

$$\|p'\|_D \leq n \max_{1 \leq k \leq 2n} |p(z_k)|.$$

Proof. See Frappier, Rahman, and Ruscheweyh [1985]. □

6. Markov's Inequality. For $p \in \mathcal{P}_n$,

$$\|p'\|_{[-1,1]} \leq n^2 \|p\|_{[-1,1]}.$$

7. Chebyshev's Inequality. For $p \in \mathcal{P}_n$ and $x \in \mathbb{R} \setminus [-1,1]$,

$$|p(x)| \leq |T_n(x)| \, \|p\|_{[-1,1]},$$

where T_n is the Chebyshev polynomial of degree n as defined in Chapter 7.

8. Riesz's Identity. There are real numbers a_i with $\sum_{i=1}^{2n} |a_i| = n$ such that for $t \in \mathcal{T}_n$ and $\theta \in \mathbb{R}$,

$$t'(\theta) = \sum_{i=1}^{2n} a_i t(\theta + \theta_i),$$

where

$$\theta_i := \frac{2i-1}{2n}\pi, \qquad i = 1, 2, \ldots, 2n,$$

and

$$a_i = \frac{(-1)^{i+1}}{4n\sin^2\left(\frac{\theta_i}{2}\right)}, \qquad i = 1, 2, \ldots, 2n.$$

(This is, apart from the explicit determination of the numbers a_i, an identity discovered by M. Riesz.)

9. A Nikolskii-Type Inequality of Arestov. For $p \in \mathcal{P}_n^c$ and $\alpha > 0$,

$$\|p(z)\|_\alpha \le c_n(\alpha)\|p(z)\|_0,$$

where

$$c_n(\alpha) := 2^n \left(\frac{\Gamma\left(\frac{n\alpha+1}{2}\right)}{\sqrt{\pi}\,\Gamma\left(\frac{n\alpha+2}{2}\right)}\right)^{1/\alpha}.$$

Proof. See Milovanović, Mitrinović, and Rassias [1994, p. 449]. □

The above inequalities are, for the most part, discussed in Appendix 3 of Borwein and Erdélyi [1995], where the treatment is through an interpolation theorem of Shapiro. This gives something of a unified treatment of these results.

Norm Inequalities with Restrictions

10. Lax's Inequality. We have

$$\|p'\|_D \le \frac{n}{2}\,\|p\|_D$$

for all $p \in \mathcal{P}_n^c$ that have no zeros in the open unit disk.

Proof. This is in Lax [1944]. It also follows from Inequality 12 below. □

11. An Extension. Associated with

$$p(z) = c\prod_{j=1}^{n}(z - z_j), \quad c \ne 0,$$

let

$$p^*(z) := \overline{c}\prod_{j=1}^{n}(1 - z\overline{z}_j) = z^n\overline{p\left(1/\overline{z}\right)}.$$

Then

$$\max_{z\in\partial D}\left(|p'(z)| + |p^{*\prime}(z)|\right) = n\|p\|_D$$

for every $0 \ne p \in \mathcal{P}_n^c$.

Proof. See Malik [1969]. □

12. An Observation of Kroó. Suppose $p \in \mathcal{P}_n^c$ satisfies that if $p(z) = 0$ for some $z \in D$, then $p(1/\overline{z}) = 0$ (there is no restriction for the zeros of p outside D). Then

$$\|p'\|_D \le \frac{n}{2}\, \|p\|_D \,.$$

Proof. If $p \in \mathcal{P}_n^c$ satisfies the assumption, then $|p'(z)| \le |p^{*\prime}(z)|$ for every $z \in \partial D$. The proof now follows from the preceding inequality. □

13. An Inequality for Reciprocal Polynomials. Suppose that $p \in \mathcal{P}_n^c$ satisfies $p(z) = z^n \overline{p(1/\bar{z})}$. Then for $|z| = 1$,

$$n\,|p(z)| \le 2\,|p'(z)|,$$

and for each $\alpha \ge 0$,

$$\frac{n}{2}\,\|p\|_\alpha \le \|p'\|_\alpha.$$

14. An Inequality of Ankeny and Rivlin. Let $r \ge 1$. The inequality

$$\max_{|z|=r} |p(z)| \le \frac{r^n + 1}{2} \max_{|z|=1} |p(z)|$$

holds for all $p \in \mathcal{P}_n^c$ that have no zeros in the open unit disk.

Proof. See Ankeny and Rivlin [1955]. □

15. Let

$$p(z) := c \prod_{k=1}^{n} (z - z_k) \in \mathcal{P}_n^c, \qquad c \ne 0,$$

be reciprocal. Then

$$\|p'\|_D = \left(\sum_{k=1}^{n} \frac{1}{1 + |z_k|} \right) \|p\|_D \,.$$

Proof. This follows from Inequality 11 above and the fact that

$$\frac{1}{1+|z|} + \frac{1}{1+|z|^{-1}} = 1.$$

□

16. Let $r \in (0,1]$. The inequality

$$\|p'\|_D \geq \frac{n}{1+r}\,\|p\|_D$$

holds for all $p \in \mathcal{P}_n^c$ that have all their zeros in the disk $\{z \in \mathbb{C} : |z| \leq r\}$.

Proof. Consider $p'(z)/p(z)$. □

17. An Inequality of Govil. Let $r > 1$. The inequality

$$\|p'\|_D \geq \frac{n}{1+r^n}\,\|p\|_D$$

holds for all $p \in \mathcal{P}_n^c$ that have no zeros in the disk $\{z \in \mathbb{C} : |z| \leq r\}$.

Proof. See Govil [1973]. □

Derivatives of Rational Functions

Let ∂D denote the boundary of the unit disk D. The following two inequalities are proved in Borwein and Erdélyi [1995].

18. Bernstein-Type Inequality for Rational Functions. Define the Bernstein factor B_n, for $\{z_k\}_{k=1}^n \subset \mathbb{C} \setminus \partial D$, by

$$B_n(z) := \max\left\{B_n^+(z), B_n^-(z)\right\}$$

with

$$B_n^+(z) := \sum_{\substack{k=1\\|z_k|>1}}^n \frac{|z_k|^2-1}{|z_k-z|^2} \qquad \text{and} \qquad B_n^-(z) := \sum_{\substack{k=1\\|z_k|<1}}^n \frac{1-|z_k|^2}{|z_k-z|^2}\,.$$

Then

$$|f'(z)| \leq B_n(z)\|f\|_{\partial D}\,, \qquad z \in \partial D,$$

for every

$$f \in \left\{\frac{p(z)}{\prod_{k=1}^n (z-z_k)} : p \in \mathcal{P}_n^c\right\}.$$

19. A Lax-Type Inequality. Given $\{z_k\}_{k=1}^n \subset \mathbb{C} \setminus \overline{D}$, let the Bernstein factor C_n be defined by

$$C_n(z) := \sum_{k=1}^{n} \frac{|z_k|^2 - 1}{|z_k - z|^2}.$$

Then

$$|h'(z)| \le \tfrac{1}{2} C_n(z) \|h\|_{\partial D}, \qquad z \in \partial D,$$

for every

$$h \in \left\{ \frac{p(z)}{\prod_{k=1}^n (z - z_k)} : p \in \mathcal{P}_n^c \right\}$$

having all its zeros in $\mathbb{C} \setminus D$.

Inequalities Involving Coefficients

20. Visser's Inequality. Let $p(z) := a_n z^n + \cdots + a_1 z + a_0 \in \mathcal{P}_n^c$ and suppose $\|p(z)\|_D \le 1$. Then

$$|a_0| + |a_n| \le 1.$$

21. Malik's Refinement. Let $p(z) := a_n z^n + \cdots + a_1 z + a_0 \in \mathcal{P}_n^c$ be reciprocal and suppose $\|p(z)\|_D \le 1$. Then

$$|a_0| \le \frac{1}{2},$$

and for $1 \le k \le n-1$,

$$|a_0| + \binom{n}{k}^{-1} |a_k| \le \frac{1}{2}.$$

22. Szász's Inequality. Let $p(z) := a_n z^n + \cdots + a_1 z + a_0$ and suppose $\|p(z)\|_D \le 1$. Then, for $0 \le i < j \le n$,

$$|a_i| + |a_j| \le \sum_{k=0}^{\lfloor j/(j-i) \rfloor} \binom{1/2}{k}^2 \le \frac{4}{\pi}.$$

See Milovanović, Mitrinović, and Rassias [1994, pp. 123–135] for proofs of these inequalities.

Inequalities for Length, Height, and Measure

23. The Measure of the Sum and Product of Numbers. Suppose α and β are algebraic numbers of degree m and n respectively. Then

$$M(\alpha+\beta) \le 2^{mn} M(\alpha)^n M(\beta)^m$$

and

$$M(\alpha\beta) \le M(\alpha)^n M(\beta)^m .$$

24. The Measure of the Sum of Polynomials. Suppose p and q are polynomials of degree n. Then

$$M(p \pm q) \le L(p \pm q) \le L(p) + L(q) \le 2^n (M(p) + M(q)).$$

25. Some Inequalities. Suppose that $p(z) := a_n z^n + \cdots + a_1 z + a_0$ is a polynomial of degree n with complex coefficients. Then

$$|a_j| \le \binom{n}{j} M(p),$$

$$L(p) \le 2^n M(p) \le 2^n L(p),$$

and

$$L(p) \le nH(p).$$

26. Gonçalves's Inequality. If

$$p(z) := a_n z^n + \cdots + a_1 z + a_0 = a_n (z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n) \in \mathcal{P}_n^c,$$

then

$$M(p)^2 + |a_0 a_n|^2 M(p)^{-2} \le \|p\|_2^2,$$

and more generally, for any $1 \le m \le n$ and $\lambda \ge 2$, if p is monic, then

$$|\alpha_1 \cdots \alpha_m|^\lambda + |\alpha_{m+1} \cdots \alpha_n|^\lambda \le \left(1 + \sum_{i=1}^n |a_i|^2\right)^{\lambda/2} .$$

These inequalities may be found in Mignotte [1992].

Inequalities for Zeros

27. Eneström–Kakeya Theorem. If

$$p(z) := a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0, a_i \in \mathbb{R},$$

with

$$a_0 \ge a_1 \ge \cdots \ge a_n > 0\,,$$

then all the zeros of p lie outside the open unit disk.

28. Suppose $\alpha, \beta > 1$ and $\alpha^{-1} + \beta^{-1} = 1$. Then the polynomial $p \in \mathcal{P}_n^c$ of the form

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0 \,, \qquad a_n \neq 0,$$

has all its zeros in the disk $\{|z| \le r\}$, where

$$r := \left\{ 1 + \left(\sum_{j=0}^{n-1} \frac{|a_j|^\alpha}{|a_n|^\alpha} \right)^{\beta/\alpha} \right\}^{1/\beta} .$$

29. Pellet's Theorem. Suppose $a_p \neq 0$, $|a_{p+1}| + \cdots + |a_n| > 0$, and

$$g(x) := |a_0| + |a_1|x + \cdots + |a_{p-1}|x^{p-1} - |a_p|x^p + |a_{p+1}|x^{p+1} + \cdots + |a_n|x^n$$

has exactly two positive zeros $s_1 < s_2$. Then

$$f(z) := a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0 \in \mathcal{P}_n^c$$

has exactly p zeros in the disk $\{z \in \mathbb{C} : |z| \le s_1\}$ and no zeros in the annulus $\{z \in \mathbb{C} : s_1 < |z| < s_2\}$.

30. An Inequality of Schur. Suppose

$$p(z) := \sum_{j=0}^{n} a_j z^j \in \mathcal{P}_n^c$$

has m positive real roots. Then

$$m^2 \le 2n \log \left(\frac{|a_0| + |a_1| + \cdots + |a_n|}{\sqrt{|a_0 a_n|}} \right) .$$

See also Chapter 7.

31. A Theorem of Szegő. Suppose $f, g, h \in \mathcal{P}_n^c$, where

$$f(z) := \sum_{k=0}^{n} a_k \binom{n}{k} z^k \,, \qquad a_n \neq 0,$$

$$g(z) := \sum_{k=0}^{n} b_k \binom{n}{k} z^k \,, \qquad b_n \neq 0,$$

and

$$h(z) := \sum_{k=0}^{n} a_k b_k \binom{n}{k} z^k \,.$$

Suppose f has all its zeros in a closed disk F, and g has zeros $\beta_1, \ldots, \beta_n$. Then all the zeros of h are of the form $-\beta_i \gamma_i$ with $\gamma_i \in F$.

32. A Theorem of Fejér. Let

$$p(z) := \sum_{k=0}^{n} a_k z^{\lambda_k}\,, \qquad a_k \in \mathbb{C}, \quad a_0 a_1 \neq 0$$

where $0 \le \lambda_1 < \lambda_2 < \ldots < \lambda_n$. Then p has at least one zero $z_0 \in \mathbb{C}$ such that

$$|z_0| \le \left(\frac{\lambda_2 \lambda_3 \cdots \lambda_n}{(\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1) \cdots (\lambda_n - \lambda_1)} \right)^{1/\lambda_1} \left| \frac{a_0}{a_1} \right|^{1/\lambda_1}.$$

33. Lucas's Theorem. Let $p \in \mathcal{P}_n^c$. All the zeros of p' are contained in the closed convex hull of the set of zeros of p.

34. Walsh's Two-Circle Theorem. Suppose $p \in \mathcal{P}_n^c$ has all its n zeros in the disk D_1 with centre c_1 and radius r_1, and suppose $q \in \mathcal{P}_m^c$ has all its m zeros in the disk D_2 with centre c_2 and radius r_2. Then:

(a) All the zeros of $(pq)'$ lie in $D_1 \cup D_2 \cup D_3$, where D_3 is the disk with centre c_3 and radius r_3 given by

$$c_3 := \frac{nc_2 + mc_1}{n+m}\,, \qquad r_3 := \frac{nr_2 + mr_1}{n+m}\,.$$

(b) Suppose $n \neq m$. Then all the zeros of $(p/q)'$ lie in $D_1 \cup D_2 \cup D_3$, where D_3 is the disk with centre c_3 and radius r_3 given by

$$c_3 := \frac{nc_2 - mc_1}{n-m}\,, \qquad r_3 := \frac{nr_2 + mr_1}{|n-m|}\,.$$

All of the above inequalities are in Chapter 1 of Borwein and Erdélyi [1995].

Inequalities for Factors

35. An Inequality of Kneser. Suppose that $p = qr$, where $q \in \mathcal{P}_m^c$ and $r \in \mathcal{P}_{n-m}^c$. Then

$$\|q\|_{[-1,1]} \|r\|_{[-1,1]} \le \tfrac{1}{2} C_{n,m} C_{n,n-m} \|p\|_{[-1,1]}\,,$$

where

$$C_{n,m} := 2^m \prod_{k=1}^{m} \left(1 + \cos \tfrac{(2k-1)\pi}{2n}\right).$$

Furthermore, for any n and any $m \le n$, the inequality is sharp in the case that p is the Chebyshev polynomial T_n of degree n and the factor $q \in \mathcal{P}_m^c$ is chosen to make q vanish at the m zeros of p closest to -1.

36. The Norm of a Single Factor of a $p \in \mathcal{P}_n^c$ on the Unit Disk. Let $p \in \mathcal{P}_n^c$ be monic and suppose $p = qr$, where $q \in \mathcal{P}_m^c$ and $r \in \mathcal{P}_{n-m}^c$. Then

$$|r(0)|^{1/2}\|q\|_D \le \left(\tfrac{1}{2}C_{n,m}\right)^{1/2}\|t\|_D\,,$$

where $C_{n,m}$ is the same as in Inequality 35. This bound is attained when m and n are even, $p(z) = z^n + 1$, and $q \in \mathcal{P}_m^c$ vanishes at m adjacent zeros of p on the unit circle.

Also,

$$\|q\|_D \le \beta^n \|p\|_D\,,$$

where $\beta := M(1 + x + y) = 1.3813\ldots$.

37. The Norm of the Factors of a $p \in \mathcal{P}_n$ on the Unit Disk. Suppose $p = qr$, where $q \in \mathcal{P}_m$ and $r \in \mathcal{P}_{n-m}$. Then

$$\|q\|_D\|r\|_D \le \left(\tfrac{1}{2}C_{n,m}C_{n,n-m}\right)^{1/2}\|p\|_D\,,$$

where $C_{n,m}$ is the same as in Inequality 35 and

$$(C_{n,m}C_{n,n-m})^{1/(2n)} \le \delta := M(1 + x + y - xy) = 1.7916\ldots .$$

This bound is attained when m and n are even, $p(z) = z^n + 1$, and $q \in \mathcal{P}_m^c$ vanishes at the m zeros of p closest to 1 and $r \in \mathcal{P}_{n-m}$ vanishes at the $n - m$ zeros of p closest to -1.

Let $p = qr$, where $q \in \mathcal{P}_m^c$ and $r \in \mathcal{P}_{n-m}^c$. Then

$$\|q\|_D\|r\|_D \le \delta^n\|p\|_D.$$

The unrestricted cases of Inequalities 36 and 37 are due to Boyd [1992].

38. Bombieri's Norm. For $Q(z) := \sum_{k=0}^n a_k z^k$ the *Bombieri p norm* is defined by

$$[Q]_p := \left(\sum_{k=0}^n \binom{n}{k}^{1-p}|a_k|^p\right)^{1/p}.$$

Note that this is a norm on $\mathcal{P}_n^c$ for every $p \in [1,\infty)$, but it varies with n. The following remarkable inequality holds (see Beauzamy et al. [1990]). If $Q = RS$ with $Q \in \mathcal{P}_n^c$, $R \in \mathcal{P}_m^c$, and $S \in \mathcal{P}_{n-m}^c$, then

$$[R]_2[S]_2 \le \binom{n}{m}^{1/2}[Q]_2,$$

and this is sharp.

The inequalities of this final section are all in Borwein and Erdélyi [1995].

Appendix B

Lattice Basis Reduction and Integer Relations

Lattice basis reduction algorithms and *integer relation algorithms* are central tools in the field of computational number theory. In this section we present LLL (without proof of termination) and discuss in detail the integer relation algorithm PSLQ. These both rely on constructing an appropriate sequence of bases for a given lattice. This treatment follows Meichsner [2001].

Definition 1. (Integer Relation). *We say that there exists an integer relation among the numbers $x_1, x_2, \ldots, x_n$ if there exist integers $a_1, a_2, \ldots, a_n$, not all zero, such that $\sum_{i=1}^{n} a_i x_i = 0$. For the vector $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$, the nonzero vector $\mathbf{a} \in \mathbb{Z}^n$ is an integer relation for $\mathbf{x}$ if $\mathbf{a} \cdot \mathbf{x} = 0$.*

Definition 2. (Lattice). *The lattice L spanned by the n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ is the set of vectors $L = \{\sum_{i=1}^{n} r_i \mathbf{b}_i : r_i \in \mathbb{Z}\}$. We say that the vectors $\mathbf{b}_i$ form a basis for L.*

Although the Euclidean and continued fraction algorithms solve the problem of finding integer relations for the vector $[x_1, x_2, \ldots, x_n]^T$ when $n = 2$, until recently there were no known polynomial-time algorithms that solved the problem for $n \geq 3$, and it is likely that no algorithm exists in general. A breakthrough was made in 1977 with the *generalized Euclidean algorithm* of Ferguson and Forcade [1979], a recursive algorithm that is guaranteed to find an integer relation when one exists. Following this, a number of nonrecursive algorithms were developed, including the PSLQ algorithm, the HJLS algorithm, and a method based on the LLL algorithm.

The LLL Algorithm

It is often desirable to find a basis for a lattice L that is in some sense reduced. The obvious choice for a reduced basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ is to let $\mathbf{b}_i$ be the shortest vector in L that is independent of the vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}$. Although Gaussian reduction finds such a basis for $n = 2$ (Cohen [1993, p. 23]) and a method due to Vallée [1986] finds such a basis for $n = 3$, currently there is no known algorithm that will construct such a basis in a reasonable amount of time for $n > 3$. The following alternative definition of a reduced basis, due to Lenstra, Lenstra, and Lovász [1982], is useful since there is a polynomial-time algorithm (LLL) for finding such a reduced basis.

Definition 3. (LLL Reduced Basis). *Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be a basis for the lattice L and let $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*$ where $\mu_{i,j} = (\mathbf{b}_i \cdot \mathbf{b}_j^*)/\|\mathbf{b}_j^*\|^2$. (This is the Gram–Schmidt orthogonalization process.) We call the vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$* LLL reduced *if:*

(1) $|\mu_{i,j}| \le \frac{1}{2}$ *for* $1 \le j < i \le n$.

(2) $\|\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*\|^2 \ge \frac{3}{4}\|\mathbf{b}_{i-1}^*\|^2$ *for* $1 < i \le n$.

Condition (1) states that the vectors $\mathbf{b}_i$ must be close to orthogonal. Condition (2), along with (1), allows us to bound the values $\|\mathbf{b}_j\|$ in terms of the norms of the shortest vectors in the lattice L.

Theorem 1. *Suppose $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ form an LLL reduced basis for a lattice L. Then for every nonzero vector $\mathbf{x} \in L$, we have $\|\mathbf{b}_1\| \le 2^{(n-1)/2}\|\mathbf{x}\|$. In particular, $\|\mathbf{b}_1\|$ is no larger than $2^{(n-1)/2}$ times the norm of a shortest nonzero vector in L.*

Proof. Since the vectors $\mathbf{b}_i^*$ and $\mathbf{b}_{i-1}^*$ are orthogonal, Condition (2) tells us that

$$(\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*) \cdot (\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*) = \|\mathbf{b}_i^*\|^2 + |\mu_{i,i-1}|^2 \|\mathbf{b}_{i-1}^*\|^2 \ge \frac{3}{4}\|\mathbf{b}_{i-1}^*\|^2.$$

By Condition (1), this implies $\|\mathbf{b}_i^*\|^2 \ge \frac{1}{2}\|\mathbf{b}_{i-1}^*\|^2$, and so by induction,

$$\|\mathbf{b}_i^*\|^2 \ge \frac{1}{2^{i-j}}\|\mathbf{b}_j^*\|^2.$$

Now for any nonzero vector $\mathbf{x} \in L$, we can write $\mathbf{x}$ as $\mathbf{x} := \sum_{i=1}^{k} a_i \mathbf{b}_i$ with $1 \le k \le n$, $a_k \ne 0$, and each $a_i \in \mathbb{Z}$. Replacing $\mathbf{b}_i$ with $\mathbf{b}_i = \mathbf{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$ allows us to write $\mathbf{x} = \sum_{i=1}^{k} s_i \mathbf{b}_i^*$ with each $s_i \in \mathbb{R}$ and $s_k = a_k \in \mathbb{Z}$. This gives

$$\begin{aligned}\|\mathbf{x}\|^2 = \sum_{i=1}^{k} |s_i|^2 \|\mathbf{b}_i^*\|^2 &\ge |a_k|^2 \|\mathbf{b}_k^*\|^2 \ge \|\mathbf{b}_k^*\|^2 \\ &\ge \|\mathbf{b}_1^*\|^2 2^{1-k} \ge \|\mathbf{b}_1^*\|^2 2^{1-n} = \|\mathbf{b}_1\|^2 2^{1-n},\end{aligned}$$

or equivalently,

$$\|\mathbf{b}_1\| \le 2^{(n-1)/2}\|\mathbf{x}\|$$

for every $\mathbf{x} \in L$. □

As shown in Lenstra, Lenstra, and Lovász [1982], one can prove that for an LLL reduced basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ and for any set of t linearly independent vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_t \in L$, we have the inequality

$$\|\mathbf{b}_j\| \le 2^{(n-1)/2} \max(\|\mathbf{x}_1\|, \|\mathbf{x}_2\|, \ldots, \|\mathbf{x}_t\|) \text{ for } 1 \le j \le t.$$

The details of the algorithm used to construct an LLL reduced basis from an arbitrary basis for L are presented in Figure B.1.

Referring to Figure B.1, we see that the body of the main loop first ensures that Condition (1) in the definition of an LLL reduced basis is satisfied for the vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ and then checks to see whether Condition (2) holds. Note that at the beginning of the main loop, the vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}$ form an LLL reduced basis for the lattice that they span. For proof of termination and improvements on the basic algorithm, one is referred to Lenstra, Lenstra, and Lovász [1982] and Cohen [1993]. For example, the bound of $2^{(n-1)/2}$ in Theorem 1 may be improved to $(\frac{4}{3} + \epsilon)^{(n-1)/2}$ at the expense of increasing the running time of the algorithm. The complexity of LLL is as follows. Let $C > 1$ be greater than the maximum of the norms of the vectors in a basis for the lattice. Then LLL will find a reduced basis using

$$O\left(n^4 \log C\right)$$

exact arithmetic operations. These operations can be performed on integers of size

$$O\left(n \log C\right)$$

if the lattice is in $\mathbb{Z}^n$.

Finding Integer Relations with LLL

One use of the LLL algorithm is to find small integer relations among nonzero values $x_1, x_2, \ldots, x_n$. To use the LLL algorithm to find an integer relation for $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$, define the $(n+1) \times n$ lower trapezoidal matrix B as

$$B = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ Nx_1 & Nx_2 & \cdots & \cdots & Nx_n \end{bmatrix}$$

The LLL Algorithm

This algorithm takes an arbitrary basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ for the lattice L as input and uses it to construct an LLL reduced basis.

Step 1 Initialization
  Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be a basis for L.
  for i to n do
    set $\mathbf{b}_i^* := \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*$
    calculate $\|\mathbf{b}_i^*\|^2$ and $\mu_{j,i}$ for $i+1 \leq j \leq n$ $(\mu_{j,i} := (\mathbf{b}_j \cdot \mathbf{b}_i^*)/\|\mathbf{b}_i^*\|^2)$
  end do
  set $k := 2$

Step 2 Main Loop
  Repeat
   for j from $(k-1)$ downto 1 do
    $q := \lfloor \mu_{k,j} \rceil$ (nearest integer, with either choice at $\frac{1}{2}$)
    $\mathbf{b}_k := \mathbf{b}_k - q\mathbf{b}_j$
    for i to j do $\mu_{k,i} := \mu_{k,i} - q\mu_{j,i}$ end do
   end do
   If $\|\mathbf{b}_k^*\|^2 \geq (\frac{3}{4} - \mu_{k,k-1}^2)\|\mathbf{b}_{k-1}^*\|^2$
    then set $k := k+1$
    else interchange $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$.
     Update $\mathbf{b}_k^*$, $\mathbf{b}_{k-1}^*$, $\|\mathbf{b}_k^*\|^2$, $\|\mathbf{b}_{k-1}^*\|^2$ and the $\mu_{i,j}$'s as follows:
     set $\mathbf{b}_{k-1}^*{}' := \mathbf{b}_k^* + \mu_{k,k-1}\mathbf{b}_{k-1}^*$
      $\|\mathbf{b}_{k-1}^*{}'\|^2 := \|\mathbf{b}_k^*\|^2 + (\mu_{k,k-1})^2\|\mathbf{b}_{k-1}^*\|^2$
      $m := \mu_{k,k-1}\|\mathbf{b}_{k-1}^*\|^2/\|\mathbf{b}_{k-1}^*{}'\|^2$
      $\mathbf{b}_k^*{}' := \mathbf{b}_k^* - m\mathbf{b}_{k-1}^*{}' = \frac{\|\mathbf{b}_k^*\|^2}{\|\mathbf{b}_{k-1}^*{}'\|^2}\mathbf{b}_{k-1}^* - m\mathbf{b}_k^*$
      $\|\mathbf{b}_k^*{}'\|^2 := \frac{\|\mathbf{b}_k^*\|^4}{\|\mathbf{b}_{k-1}^*{}'\|^4}\|\mathbf{b}_{k-1}^*\|^2 + m^2\|\mathbf{b}_k^*\|^2$
        $= \|\mathbf{b}_k^*\|^2\|\mathbf{b}_{k-1}^*\|^2/\|\mathbf{b}_{k-1}^*{}'\|^2$
     interchange $\mu_{k,i}$ with $\mu_{k-1,i}$ for $1 \leq i \leq k-2$
     for i from $k+1$ to n do
      $t := \mu_{i,k}$, $\mu_{i,k} := \mu_{i,k-1} - \mu_{k,k-1}\mu_{i,k}$, $\mu_{i,k-1} := t + m\mu_{i,k}$
     end do
     set $\mu_{k,k-1} := m$
     set $\mathbf{b}_k^* := \mathbf{b}_k^*{}'$, $\|\mathbf{b}_k^*\|^2 := \|\mathbf{b}_k^*{}'\|^2$,
       $\mathbf{b}_{k-1}^* := \mathbf{b}_{k-1}^*{}'$, $\|\mathbf{b}_{k-1}^*\|^2 := \|\mathbf{b}_{k-1}^*{}'\|^2$.
     set $k := \max(2, k-1)$
   end if
  until $k = n+1$

At this point the vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ form an LLL reduced basis for the lattice L.

Figure B.1: **Pseudocode implementation of the LLL algorithm** (where N is a large number) and let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be the column vectors of B. If we now consider the vectors in the lattice L spanned by $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$, we see they are of the form

$$\mathbf{m}' = \sum_{i=1}^{n} m_i \mathbf{b}_i = \left[m_1, m_2, \ldots, m_n, N \sum_{i=1}^{n} m_i x_i \right]^T.$$

We may view the last term in $\mathbf{m}'$, $N \sum m_i x_i$, as a penalty term. If the vector $\mathbf{m} = [m_1, m_2, \ldots, m_n]^T$ is an integer relation for $\mathbf{x}$, then this term will be zero. However, if $\mathbf{m}$ is not an integer relation for $\mathbf{x}$, then this term will be large, provided that N is large enough. The penalty for not being an integer relation depends on the choice of N. If N is taken large enough and $\mathbf{m}$ is a short integer relation for $\mathbf{x}$, then $\mathbf{m}'$ will be one of the shortest vectors in L. With this in mind, to find an integer relation for $\mathbf{x}$ we choose a suitably large value of N and run the LLL algorithm on the vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$. The first vector, $\mathbf{b}_1'$, in the returned basis will be one of the smallest vectors in L. (Note that $\mathbf{b}_1'$ is not necessarily the shortest vector in the returned basis. We may also wish to consider the other $\mathbf{b}_i'$ as well.) If N is large enough and if an integer relation exists, then LLL will succeed.

Lemma 1. *Suppose there are integer relations for $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$. Then the method presented above will find one, provided that N is large enough.*

Proof. Let M be the norm of a smallest integer relation for $\mathbf{x}$ and consider the finite set of vectors $\left\{\mathbf{y} \in \mathbb{Z}^n : \|\mathbf{y}\| < 2^{n/2}M, (\mathbf{y} \cdot \mathbf{x}) \neq 0\right\}$. From this nonempty set, choose a vector $\mathbf{y}$ with the property that $|\mathbf{y} \cdot \mathbf{x}| = |\sum y_i x_i|$ is minimal. For this $\mathbf{y}$, choose N so that $N|\sum y_i x_i| > 2^{n/2}M$. Now for any $\mathbf{m}' \in L$, if $\sum_{i=1}^{n} m_i x_i \neq 0$ then $\|\mathbf{m}'\| > 2^{n/2}M$. If $\mathbf{m} = [m_1, m_2, \ldots, m_n]^T$ is not an integer relation for $\mathbf{x}$, then the norm of the vector $\mathbf{m}' = [m_1, m_2, \ldots, m_n, N \sum m_i x_i]^T$ is greater than $2^{((n+1)-1)/2}$ times the norm of a shortest nonzero vector in L and hence cannot be the first vector in an LLL reduced basis (by Theorem 1). $\square$

Although this shows that an integer relation will be found if one exists and N is large enough, we do not know beforehand how large N must be.

The PSLQ Algorithm

Following the *generalized Euclidean algorithm* of Ferguson and Forcade [1979], Ferguson and others developed a sequence of nonrecursive integer relation algorithms (Ferguson [1987]; Bailey and Ferguson [1989]; Ferguson, Bailey, and Arno [1999]), each an improvement on the previous ones. In this section we cover the latest incarnation of these, a simplified statement of the PSLQ algorithm. We follow the general outline of Ferguson, Bailey, and Arno [1999].

As before, suppose we wish to find a small integer relation among the nonzero values $x_1, x_2, \ldots, x_n$. Rather than using the method of the previous section (based upon the LLL algorithm), here we attempt to construct a sequence of bases for the lattice $\mathbb{Z}^n$ that converge to the line $\mathbb{R}\mathbf{x}$ by examining the projections of these basis vectors onto $\mathbf{x}^\perp$.

Let $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$ and suppose we have a set of n linearly independent vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n \in \mathbb{Z}^n$ such that the projection of each $\mathbf{a}_i$ onto $\mathbf{x}^\perp$ is small (we say each vector $\mathbf{a}_i$ is close to $\mathbf{x}$). If we define A to be the matrix such that the ith row of A is $\mathbf{a}_i^T$, then A is invertible. Let $B = A^{-1}$ and let $\mathbf{b}_j$ be the jth column vector of B. Now, since $(\mathbf{a}_i \cdot \mathbf{b}_j) = 0$ for $i \neq j$ and each $\mathbf{a}_i$ is close to $\mathbf{x}$, we would expect that each $\mathbf{b}_j$ lies close to $\mathbf{x}^\perp$. The idea behind the PSLQ algorithm is to start with the standard basis for the lattice $\mathbb{Z}^n$, and with each iteration construct a new basis $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ for $\mathbb{Z}^n$ in which the $\mathbf{a}_i$ are closer to $\mathbf{x}$. In doing so, we hope to force the vectors $\mathbf{b}_j$ closer to $\mathbf{x}^\perp$. We will see that as an upper bound on the values $\left\|\operatorname{proj}_{\mathbf{x}^\perp} \mathbf{a}_i\right\|$ decreases, a lower bound on the size of any possible integer relation for $\mathbf{x}$ increases. Throughout the PSLQ algorithm we work with the following matrices:

A**:** An $n \times n$ invertible matrix. The column vectors $\mathbf{a}_i$ of A^T form a basis for the lattice $\mathbb{Z}^n$.

H**:** An $n \times (n-1)$ matrix with column vectors $\mathbf{h}_j$ that form an orthonormal basis for $\mathbf{x}^\perp$.

H'**:** The matrix AH. Each entry $h'_{i,j}$ in H' is the inner product of $\mathbf{a}_i$ with $\mathbf{h}_j$. Note that the projection of $\mathbf{a}_i$ onto $\mathbf{x}^\perp$ is $\sum_{j=1}^{n-1}(\mathbf{a}_i \cdot \mathbf{h}_j)\mathbf{h}_j$. Each time we begin the main iteration of the algorithm, H' will be lower trapezoidal (see Definition 4 below) and we will have $\left|h'_{i,j}\right| \leq \frac{1}{2}\left|h'_{j,j}\right|$ for $1 \leq i < j$. This will give

$$\left\|\operatorname{proj}_{\mathbf{x}^\perp} \mathbf{a}_i\right\|^2 \leq \frac{1}{4}\sum_{j=1}^{i-1}\left|h'_{j,j}\right|^2 + \left|h'_{i,i}\right|^2 \leq \sum_{j=1}^{i}\left|h'_{j,j}\right|^2.$$

By reducing the $\left|h'_{i,i}\right|$, we will reduce an upper bound on $\left\|\operatorname{proj}_{\mathbf{x}^\perp} \mathbf{a}_i\right\|$ for each i.

B**:** $B = A^{-1}$. The column vectors $\mathbf{b}_j$ of B will be forced closer to $\mathbf{x}^\perp$ by forcing the vectors $\mathbf{a}_i$ closer to $\mathbf{x}$.

Definition 4. (Lower Trapezoidal). *The $m \times n$ matrix C is lower trapezoidal if $m > n$, and each entry $c_{i,j}$ of C equals zero if $j > i$.*

Although forcing the vectors $\mathbf{a}_i$ closer to $\mathbf{x}$ is not sufficient to guarantee that one of the $\mathbf{b}_j$ will eventually lie in $\mathbf{x}^\perp$, termination of the algorithm and a bound on the size of the relation found will follow from Theorem 2. From this we will see that reducing the values $\left|h'_{i,i}\right|$ also increases a lower bound on the norm of the smallest possible integer relation for $\mathbf{x}$.

Theorem 2. *Let A be an invertible $n \times n$ matrix with integer coefficients, $\mathbf{x}$ a vector in $\mathbb{R}^n$, and H an $n \times (n-1)$ matrix with column vectors that form an orthonormal basis for $\mathbf{x}^\perp$. If $H' = AH$ is lower trapezoidal with each diagonal entry $h'_{i,i}$ nonzero, then*

$$\frac{1}{\max\left|h'_{i,i}\right|} \leq \|\mathbf{m}\| \quad \text{for any integer relation } \mathbf{m} \text{ of } \mathbf{x}.$$

Proof. For any integer relation $\mathbf{m}$, $HH^T\mathbf{m} = \mathbf{m}$, since HH^T is the projection matrix onto $\mathbf{x}^\perp$. Thus $A\mathbf{m} = H'(H^T\mathbf{m})$. Let $\mathbf{a}_i^T$ be the ith row vector of A, $\mathbf{h}_i^T$ the ith row vector of H^T, and $h'_{j,j}$ the jth diagonal element of H'. Since A is invertible, $A\mathbf{m} \neq \mathbf{0}$. Let j be the least integer such that $\mathbf{a}_j^T\mathbf{m} \neq 0$. Then $\mathbf{a}_k^T\mathbf{m} = 0$ for $1 \leq k < j$, and so by recursion and the fact that H' is lower trapezoidal with nonzero diagonal elements, $\mathbf{h}_k^T\mathbf{m} = 0$ for $1 \leq k < j$ and $\mathbf{a}_j^T\mathbf{m} = h'_{j,j}(\mathbf{h}_j^T\mathbf{m})$. Since $\mathbf{a}_j^T\mathbf{m}$ is a nonzero integer,

$$1 \leq \left|h'_{j,j}\right| \left|\mathbf{h}_j^T\mathbf{m}\right| \leq \left|h'_{j,j}\right| \|\mathbf{m}\|.$$

The last inequality comes from the fact that the norm of the projection of $\mathbf{m}$ onto the unit vector $\mathbf{h}_j$ cannot be larger than the norm of $\mathbf{m}$. The result now follows. $\square$

The details of the PSLQ algorithm are presented in Figure B.2. Although one can implement the algorithm in such a way that requires only the matrices B and H', the matrices A and H are included since they make it easier to follow the reasoning behind the various steps. While the version presented here is valid only for real vectors $\mathbf{x}$, it can easily be extended to work with complex vectors as well (Ferguson, Bailey, and Arno [1999]).

Note that in Step 1, partial sums of squares of the x_i are used to construct the matrix H. It can be seen that the column vectors $\mathbf{h}_i$ of H form an orthonormal basis for $\mathbf{x}^\perp$ by considering $(\mathbf{x}\cdot\mathbf{h}_i)$ and $(\mathbf{h}_i\cdot\mathbf{h}_j)$ for $1 \leq i, j \leq n-1$. By examining the definitions of the h_i and s_i in Step 1 of the algorithm, we see the following:

For $1 \leq i \leq n-1$,

$$\begin{aligned}(\mathbf{x}\cdot\mathbf{h}_i) &= x_i h_{i,i} + \sum_{k=i+1}^{n} x_k h_{k,i} = x_i \frac{s_{i+1}}{s_i} + \sum_{k=i+1}^{n} x_k \frac{-x_k x_i}{s_i s_{i+1}} \\ &= \frac{x_i s_{i+1}}{s_i} - \frac{x_i}{s_i s_{i+1}} \sum_{k=i+1}^{n} x_k^2 = \frac{x_i s_{i+1}}{s_i} - \frac{x_i s_{i+1}^2}{s_i s_{i+1}} = 0.\end{aligned}$$

The PSLQ Algorithm

This algorithm takes a vector $\mathbf{x}^T = [x_1, x_2, \ldots, x_n]$ and a constant $T \geq 1$ as input. It either returns an integer relation for $\mathbf{x}$ along with a lower bound on the norm of the shortest integer relation or it returns a lower bound ($\geq T$) on the norm of any possible relation for $\mathbf{x}$.

Step 1: Initialization

Fix the constant $\gamma > \sqrt{\frac{4}{3}}$.

Let $A = B = I$, $\mathbf{a}_i^T$ be the ith row of A, $\mathbf{b}_j$ be the jth column of B.

Let H and H' be the $n \times (n-1)$ lower trapezoidal matrices with entries

$$h'_{i,j} = h_{i,j} = \begin{cases} 0 & 1 \leq i < j \leq n-1 \\ s_{i+1}/s_i & 1 \leq i = j \leq n-1 \\ -x_i x_j / s_j s_{j+1} & 1 \leq j < i \leq n \end{cases} \quad \text{where } s_j^2 = \sum_{k=j}^{n} x_k^2.$$

Let $\mathbf{h}'_i$ be the ith row vector of H' and $\mathbf{h}_i$ be the ith column vector of H.

Step 2: Size Reduce H'

for i from 2 to n do, for j from $i-1$ down to 1 do

set $t = \lfloor h'_{i,j}/h'_{j,j} \rceil$

replace $\mathbf{a}_i$ with $\mathbf{a}_i - t\mathbf{a}_j$, $\mathbf{b}_j$ with $\mathbf{b}_j + t\mathbf{b}_i$, and $\mathbf{h}'_i$ with $\mathbf{h}'_i - t\mathbf{h}'_j$

end do, end do

Step 3: The Main Iteration

Choose r such that $\gamma^i \left|h'_{i,i}\right|$ is maximal when $i = r$.

Repeat the following until either $1/\max\left|h'_{i,i}\right| \geq T$ or both $h'_{n,n-1} = 0$ and $r = n-1$:

1. Let $\alpha = h'_{r,r}$, $\beta = h'_{r+1,r}$, and $\lambda = h'_{r+1,r+1}$.
   Then interchange rows $\mathbf{a}_r^T$ and $\mathbf{a}_{r+1}^T$ of A, columns $\mathbf{b}_r$ and $\mathbf{b}_{r+1}$ of B, and rows $\mathbf{h}'_r$ and $\mathbf{h}'_{r+1}$ of H'.
2. If $r = n-1$, then H' is still lower trapezoidal. In this case, the value of $|h_{n-1,n-1}|$ was reduced by at least a factor of 2.
   If $r < n-1$, then H' is no longer trapezoidal. Remedy this by modifying the basis for $\mathbf{x}^\perp$. Rotate $\mathbf{h}_r$ and $\mathbf{h}_{r+1}$ in the plane they define so that the projection of $\mathbf{a}_r$ onto $\mathbf{h}_{r+1}$ is 0. This is done by replacing H by HQ and H' by $H'Q$, where Q is the $(n-1) \times (n-1)$ unitary matrix defined as follows:
   Set $Q = I_{n-1}$ and let $\delta = \sqrt{\beta^2 + \lambda^2}$. Then set $q_{r,r} = \beta/\delta$, $q_{r+1,r} = \lambda/\delta$, $q_{r,r+1} = -\lambda/\delta$, and $q_{r+1,r+1} = \beta/\delta$.
   In addition to setting $h'_{r,r+1}$ to 0, this also sets $h'_{r,r} = \delta$ and $h'_{r+1,r+1} = -\alpha\lambda/\delta$.
3. Size reduce H' as in Step 2.
4. Choose r such that $\gamma^i \left|h'_{i,i}\right|$ is maximal as above.

Step 4: Return $1/\max\left|h'_{i,i}\right|$ as a lower bound on the norm of any integer relation for $\mathbf{x}$. If $r = n-1$ and $h'_{n,n-1} = 0$, then return $\mathbf{b}_{n-1}$ as an integer relation for $\mathbf{x}$.

Figure B.2: **Pseudocode implementation of the PSLQ algorithm**

For $1 \le i < j \le n-1$,

$$\begin{aligned}(\mathbf{h}_i \cdot \mathbf{h}_j) &= h_{j,i}h_{j,j} + \sum_{k=j+1}^{n} h_{k,i}h_{k,j} = \frac{-x_j x_i}{s_i s_{i+1}} \frac{s_{j+1}}{s_j} + \sum_{k=j+1}^{n} \frac{-x_k x_i}{s_i s_{i+1}} \frac{-x_k x_j}{s_j s_{j+1}} \\ &= \frac{-x_i x_j s_{j+1}}{s_i s_{i+1} s_j} + \frac{x_i x_j}{s_i s_{i+1} s_j s_{j+1}} \sum_{k=j+1}^{n} x_k^2 \\ &= \frac{-x_i x_j s_{j+1}}{s_i s_{i+1} s_j} + \frac{x_i x_j s_{j+1}^2}{s_i s_{i+1} s_j s_{j+1}} = 0.\end{aligned}$$

For $1 \le i \le n-1$,

$$\begin{aligned}(\mathbf{h}_i \cdot \mathbf{h}_i) &= h_{i,i}^2 + \sum_{k=i+1}^{n} h_{k,i}^2 = \left(\frac{s_{i+1}}{s_i}\right)^2 + \sum_{k=i+1}^{n} \left(\frac{-x_k x_i}{s_i s_{i+1}}\right)^2 \\ &= \frac{s_{i+1}^2}{s_i^2} + \frac{x_i^2}{s_i^2 s_{i+1}^2} \sum_{k=i+1}^{n} x_k^2 = \frac{s_i^2 - x_i^2}{s_i^2} + \frac{x_i^2}{s_i^2 s_{i+1}^2} s_{i+1}^2 = 1.\end{aligned}$$

The matrix H we start with has the desired property; its columns form an orthonormal basis for $\mathbf{x}^{\perp}$.

At the beginning of Step 1 of the algorithm we set the constant $\gamma > \sqrt{\frac{4}{3}}$. This requires an explanation. As stated above, if we reduce the values $\left|h'_{i,i}\right|$ for each i, then we reduce an upper bound on the values $\left\|\mathrm{proj}_{\mathbf{x}^{\perp}} \mathbf{a_i}\right\|$ and increase a lower bound on the size of the smallest possible norm for any integer relation of $\mathbf{x}$. Now, since r is chosen such that $\gamma^r \left|h'_{r,r}\right|$ is as large as possible, if $r < n-1$ then $\left|h'_{r+1,r+1}\right| \le \frac{1}{\gamma}\left|h'_{r,r}\right|$. In this case we let $\alpha = h'_{r,r}$, $\beta = h'_{r+1,r}$, $\lambda = h'_{r+1,r+1}$, and set $\delta = \sqrt{\beta^2 + \lambda^2}$. We then replace $h'_{r,r}$ with δ. From the reduction of H' we have that $\left|h'_{r+1,r}\right| \le \frac{1}{2}\left|h'_{r,r}\right|$, which then gives

$$\delta = \sqrt{\beta^2 + \lambda^2} < \sqrt{\frac{\alpha^2}{4} + \frac{\alpha^2}{\gamma^2}} = |\alpha| \sqrt{\frac{1}{4} + \frac{1}{\gamma^2}}. \tag{B.1}$$

Thus $\left|h'_{r,r}\right|$ is reduced as long as $\sqrt{\frac{1}{4} + \frac{1}{\gamma^2}} < 1$ or $\gamma > \sqrt{\frac{4}{3}}$. Although this also increases $\left|h'_{r+1,r+1}\right|$ (since $h'_{r+1,r+1}$ is replaced with $-\alpha\lambda/\delta$ and $\left|h'_{r,r}h'_{r+1,r+1}\right| = |\delta \cdot \alpha\lambda/\delta| = |\alpha\lambda|$ remains unchanged, we see that $\left|h'_{r+1,r+1}\right|$ increases), this is not a significant problem. At each step we are forcing the larger diagonal elements of H' toward $h'_{n-1,n-1}$, where their size can be reduced by at least a factor of 2 when $r = n-1$.

Even though we strive to reduce the diagonal entries of H', none will ever equal zero. From the fact that $h'_{i,i} \neq 0$ initially for any i, and since $h'_{r,r}$ and $h'_{r+1,r+1}$ are replaced with nonzero values when $r < n-1$, the only way a value $h'_{i,i}$ may become zero is if we interchange rows h'_{n-1} and h'_n of H' when

$h_{n,n-1} = 0$. However, we would exit the algorithm before this interchange occurred, and we need not concern ourselves about division by zero when computing $\lfloor h'_{i,j}/h'_{j,j} \rceil$ during the reductions of H'.

Now, in the event that the algorithm terminates with $h_{n,n-1} = 0$, the column vector $\mathbf{b}_{n-1}$ of B is an integer relation for $\mathbf{x}$. To see this, recall that $\mathbf{x}^T H = \mathbf{0}, BA = I, AH = H'$, and $h'_{n-1,n-1} \neq 0$. This gives $\mathbf{0} = \mathbf{x}^T BH' = \left[\mathbf{x}^T B\mathbf{h}'_1, \mathbf{x}^T B\mathbf{h}'_2, \ldots, \mathbf{x}^T B\mathbf{h}'_{n-1}\right]$ where $\mathbf{h}'_i$ is the ith column vector of H'. Since the only nonzero entry in $\mathbf{h}'_{n-1}$ is $h'_{n-1,n-1}$, we have $0 = \mathbf{x}^T\mathbf{b}_{n-1}h_{n-1,n-1}$, which yields $\mathbf{x}^T\mathbf{b}_{n-1} = 0$. The $(n-1)$th column vector of B is an integer relation for $\mathbf{x}$.

A Bound on the Relation Found by PSLQ

We have just shown that if the PSLQ algorithm terminates with $h'_{n,n-1} = 0$, then the column vector $\mathbf{b}_{n-1}$ of B is an integer relation for $\mathbf{x}$. Since we are looking for a small integer relation, we would like to show that the relation found is not much larger than the smallest possible integer relation for $\mathbf{x}$. To do this, we need the following lemma.

Lemma 2. *If the PSLQ algorithm terminates with $h'_{n,n-1}$ equaling zero, then the norm of $\mathbf{b}_{n-1}$, the integer relation found, is*

$$\|\mathbf{b_{n-1}}\| = \frac{1}{|h'_{n-1,n-1}|}.$$

Proof. Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ be the standard orthonormal basis for $\mathbb{R}^n$ and let $\mathbf{e}'_1, \mathbf{e}'_2, \ldots, \mathbf{e}'_{n-1}$ be the standard orthonormal basis for $\mathbb{R}^{n-1}$. As $\mathbf{b}_{n-1}$ is an integer relation for $\mathbf{x}$, $(HH^T)\mathbf{b}_{n-1} = \mathbf{b}_{n-1}$. Using the facts that $AH = H'$ and $\mathbf{b}_{n-1}$ is the $(n-1)$th column of $B = A^{-1}$, we see that

$$H'H^T\mathbf{b}_{n-1} = AHH^T\mathbf{b}_{n-1} = A\mathbf{b}_{n-1} = \mathbf{e}_{n-1} = [0, 0, \ldots, 1, 0]^T$$

or

$$H^T\mathbf{b}_{n-1} = (H')^\dagger\mathbf{e}_{n-1}$$

where $(H')^\dagger$ is the left inverse of H'. We know that H' has a left inverse because the row vectors of the lower trapezoidal matrix H' span $\mathbb{R}^{n-1}$. However, since the only nonzero element in the last column of H' is $h'_{n-1,n-1}$, the $(n-1)$th column of the $(n-1) \times n$ matrix $(H')^\dagger$ must be equal to $1/h'_{n-1,n-1}\mathbf{e}'_{n-1} = \left[0, 0, \ldots, 0, 1/h'_{n-1,n-1}\right]^T$. The linear combination of the rows of H' required to construct $\mathbf{e}'^T_i$ cannot use the $(n-1)$th row of H' when $i \neq n-1$ and must have a multiple of $1/h'_{n-1,n-1}$ times the $(n-1)$th row when $i = n-1$. It follows that

$$\left\|H^T\mathbf{b}_{n-1}\right\| = \left\|H'^\dagger\mathbf{e}_{n-1}\right\| = \left\|\left[0, 0, \ldots, 0, \frac{1}{h'_{n-1,n-1}}\right]^T\right\| = \frac{1}{|h'_{n-1,n-1}|}.$$

Now, since $\mathbf{b}_{n-1}$ lies in $\mathbf{x}^\perp$ and the rows of H^T form an orthonormal basis for $\mathbf{x}^\perp$, we see that $\|H^T\mathbf{b_{n-1}}\| = \|\mathbf{b_{n-1}}\|$ which gives the result we are after:

$$\|\mathbf{b}_{n-1}\| = \frac{1}{\left|h'_{n-1,n-1}\right|}.$$

□

Armed with this lemma, it becomes a simple matter to find a bound on the size of an integer relation found by the PSLQ algorithm.

Theorem 3. *Let M be the norm of the smallest integer relation for $\mathbf{x}$. If the PSLQ algorithm terminates because $h'_{n,n-1} = 0$ and $r = n-1$, then*

$$\|\mathbf{b}_{n-1}\| \leq \gamma^{n-2} M.$$

Proof. By Lemma 2, we know that $\|\mathbf{b}_{n-1}\| = 1/\left|h'_{n-1,n-1}\right|$. Since $r = n-1$, we have $\gamma^{n-1}\left|h'_{n-1,n-1}\right| \geq \gamma^i \left|h'_{i,i}\right|$ for $1 \leq i \leq n-1$. From Theorem 2, since none of the diagonal elements of H' are zero, $M \geq 1/\left|h'_{j,j}\right|$ for some j, and so

$$M\gamma^{n-1} \geq \frac{\gamma^{n-1}}{\left|h'_{j,j}\right|} \geq \frac{\gamma^j}{\left|h'_{n-1,n-1}\right|} \geq \frac{\gamma}{\left|h'_{n-1,n-1}\right|} = \gamma\|\mathbf{b}_{n-1}\|,$$

or

$$\|\mathbf{b}_{n-1}\| \leq \gamma^{n-2} M.$$

□

We cannot guarantee that the PSLQ algorithm will return a smallest integer relation for $\mathbf{x}$. However, if we have $\max\left|h'_{i,i}\right| = \left|h'_{n-1,n-1}\right|$ upon termination, then we have found an integer relation for $\mathbf{x}$ of smallest possible norm. It should be noted that if we stop the algorithm when $h'_{n,n-1} = 0$ but before $r = n-1$, then the above bound does not apply. Although $\mathbf{b}_{n-1}$ will still be an integer relation for $\mathbf{x}$ with norm equal to $1/\left|h'_{n-1,n-1}\right|$, this norm may not be as small as we can make it. If we continue until $r = n-1$, then we may increase the value $|h_{n-1,n-1}|$ (it will not decrease) and hence decrease the norm of $\mathbf{b}_{n-1}$.

Termination of the Algorithm

We first consider the case when the vector $\mathbf{x}$ has integer relations. In this case, termination of the algorithm rests upon Theorem 2 and the method used to reduce the diagonal elements of H'. To begin, define τ so that

$$\frac{1}{\tau} = \sqrt{\frac{1}{4} + \frac{1}{\gamma^2}}.$$

In Step 1 of the algorithm, γ was chosen so that $\gamma > \sqrt{\frac{4}{3}}$, and thus we see that $\tau > 1$. To show that the algorithm terminates, we show that $\Pi(k)$, a function of the diagonal elements of H', is bounded and increases with each iteration.

Definition 5. *Let $h'_{i,i}(k)$ be the ith diagonal element of H' at the end of the kth iteration for $k \geq 1$, and let $h'_{i,i}(0)$ be the ith diagonal element of H' at the beginning of the first iteration. Let γ be as chosen in Step 1 and let M be the norm of a smallest integer relation for the n-dimensional vector $\mathbf{x}$. Then define $\Pi(k)$ to be*

$$\Pi(k) := \prod_{i=1}^{n-1}\left[\min\left(\gamma^{n-1}M, \frac{1}{\left|h'_{i,i}(k)\right|}\right)\right]^{n-i}.$$

The following lemma shows that the function $\Pi(k)$ is bounded.

Lemma 3. *At the end of the kth iteration ($k \geq 0$) we have that*

$$1 \leq \Pi(k) \leq (\gamma^{n-1}M)^{\binom{n}{2}}.$$

Proof. From Step 1 of the algorithm we see that

$$\left|h'_{i,i}(0)\right| = \left|\frac{s_{i+1}}{s_i}\right| < 1 \text{ for } 1 \leq i \leq n-1.$$

Now suppose that at the beginning of the kth iteration, $\left|h'_{i,i}(k)\right| \leq 1$ for each i. Then if $r = n-1$, only $\left|h'_{n-1,n-1}(k)\right|$ changes, and is reduced by at least a factor of 2. If $r < n-1$, then only $\left|h'_{r,r}(k)\right|$ and $\left|h'_{r+1,r+1}(k)\right|$ change. As was shown previously in equation B.1, $\left|h'_{r,r}(k)\right|$ is replaced with the smaller value $|\delta|$, and $\left|h'_{r+1,r+1}(k)\right|$ is replaced with $\left|\frac{\alpha\lambda}{\delta}\right| < |\alpha| = \left|h'_{r,r}(k)\right| \leq 1$. Thus $\left|h'_{i,i}(k+1)\right| \leq 1$ for $1 \leq i \leq n-1$. We see that for each i and $k \geq 0$, $\left|h'_{i,i}(k)\right| \leq 1$. Since both γ and M are larger than 1, it follows that for any $k \geq 0$, $\min\left(\gamma^{n-1}M, 1/\left|h'_{i,i}(k)\right|\right) \geq 1$ for $1 \leq i \leq n-1$. This establishes one of the desired inequalities, $1 \leq \Pi(k)$ for each $k \geq 0$.

For the second inequality, note that

$$\gamma^{n-1}M \geq \min\left(\gamma^{n-1}M, \frac{1}{\left|h'_{i,i}(k)\right|}\right)$$

and so

$$\Pi(k) \leq \prod_{i=1}^{n-1}\left(\gamma^{n-1}M\right)^{n-i} = \left(\gamma^{n-1}M\right)^{\sum_{i=1}^{n-1} i}.$$

Since $\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2} = \binom{n}{2}$, we have the required result. ◻

Before showing that $\Pi(k)$ increases by at least a factor of τ with each iteration, we need the following lemma.

Lemma 4. *Suppose the positive constants a, b, and t satisfy the following inequalities:*

$$a \geq b, \quad a \geq t, \quad \text{and} \quad 1 \geq t.$$

Then

$$\frac{\min(a,1)\min(b,t)}{\min(a,t)\min(b,1)} \geq 1.$$

Proof. The proof is a simple verification. If one lists all 24 possible orderings of a, b, 1, and t and then crosses off those orderings where it is possible to have $a < b$, $a < t$, or $1 < t$, then only the following 5 orderings remain:

$$\begin{gathered} a \geq b \geq 1 \geq t, \\ a \geq 1 \geq b \geq t, \\ a \geq 1 \geq t \geq b, \\ 1 \geq a \geq b \geq t, \\ 1 \geq a \geq t \geq b. \end{gathered}$$

With these remaining orderings, one easily checks that the inequality holds. □

Lemma 5. *For any $k \geq 0$, $\Pi(k+1) \geq \tau\Pi(k)$.*

Proof. We will show that the quotient $\Pi(k+1)/\Pi(k)$ is greater than or equal to τ. When $r < n-1$, the 2×2 submatrix of H'

$$\begin{bmatrix} h'_{r,r}(k) & 0 \\ h'_{r+1,r}(k) & h'_{r+1,r+1}(k) \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ \beta & \lambda \end{bmatrix} \quad \text{becomes} \quad \begin{bmatrix} \delta & 0 \\ \alpha\beta/\delta & -\alpha\lambda/\delta \end{bmatrix},$$

where $\delta = \sqrt{\beta^2 + \lambda^2}$. All other diagonal elements of H' remain unchanged. It follows that in this case,

$$\frac{\Pi(k+1)}{\Pi(k)} = \frac{\min\left(\gamma^{n-1}M, 1/\left|\delta\right|\right)^{n-r} \cdot \min\left(\gamma^{n-1}M, \left|\delta/(\alpha\lambda)\right|\right)^{n-r-1}}{\min\left(\gamma^{n-1}M, 1/\left|\alpha\right|\right)^{n-r} \cdot \min\left(\gamma^{n-1}M, 1/\left|\lambda\right|\right)^{n-r-1}}.$$

If we make the substitutions $a = \gamma^{n-1}M\,|\delta|$ and $b = \gamma^{n-1}M\,|\lambda|$, then we have

$$\frac{\Pi(k+1)}{\Pi(k)} = \frac{\min(a,1)}{\min(a,|\delta/\alpha|)} \left(\frac{\min(a,1)}{\min(a,|\delta/\alpha|)}\frac{\min(b,|\delta/\alpha|)}{\min(b,1)}\right)^{n-r-1}.$$

Now, since $\delta = \sqrt{\beta^2 + \lambda^2} \geq |\lambda|$, we have $a \geq b$, and since $\gamma > \sqrt{\frac{4}{3}}$, equation B.1 shows that $|\delta/\alpha| < 1$. By Theorem 2 and the choice of r, we also have that

$M \geq 1/\left|h'_{j,j}\right|$ for some j and $\gamma^r |\alpha| \geq \gamma^i \left|h'_{i,i}\right|$ for $1 \leq i \leq n-1$. Since $\gamma > 1$, this implies that

$$M\gamma^{n-1} \geq \frac{\gamma^r}{\left|h'_{j,j}\right|} \geq \frac{\gamma^j}{|\alpha|} \geq \frac{\gamma}{|\alpha|} \geq \frac{1}{|\alpha|}, \tag{B.2}$$

or equivalently, that

$$a = M\gamma^{n-1}\delta \geq \frac{\delta}{|\alpha|}.$$

Since the conditions of Lemma 4 are satisfied, we see that

$$\frac{\Pi(k+1)}{\Pi(k)} \geq \frac{\min(a,1)}{\min(a,|\delta/\alpha|)}.$$

If $a \geq 1$, then

$$\frac{\min(a,1)}{\min(a,|\delta/\alpha|)} = \left|\frac{\alpha}{\delta}\right| \geq \frac{|\alpha|}{\sqrt{\frac{\alpha^2}{4}+\frac{\alpha^2}{\gamma^2}}} = \frac{1}{\sqrt{\frac{1}{4}+\frac{1}{\gamma^2}}} = \tau.$$

Otherwise, we have $1 > a \geq |\delta/\alpha|$, and so

$$\frac{\min(a,1)}{\min(a,|\delta/\alpha|)} = M\gamma^{n-1}|\alpha| \geq \gamma$$

from equation B.2 above. From the definition of τ we see that $1/\tau^2 > 1/\gamma^2$, or that $\gamma > \tau$. Thus if $r < n-1$, then

$$\Pi(k+1) \geq \tau\Pi(k).$$

If $r = n-1$, then the only diagonal entry of H' that changes is $\left|h'_{n-1,n-1}\right| = |\alpha|$. In this case we have $\left|h'_{n-1,n-1}(k+1)\right| \leq |\alpha|/2$, and so

$$\frac{\Pi(k+1)}{\Pi(k)} \geq \frac{\min(\gamma^{n-1}M, 2/|\alpha|)}{\min(\gamma^{n-1}M, 1/|\alpha|)} = \frac{\min(\gamma^{n-1}M|\alpha|, 2)}{\min(\gamma^{n-1}M|\alpha|, 1)}.$$

Again, from equation B.2 we have $\gamma^{n-1}M|\alpha| \geq \gamma \geq 1$. Now, since $\frac{1}{\tau^2} = \frac{1}{4}+\frac{1}{\gamma^2} > \frac{1}{4}$, we have $2 > \tau$, and so if $\gamma^{n-1}M|\alpha| \geq 2$, then

$$\frac{\Pi(k+1)}{\Pi(k)} = 2 > \tau.$$

On the other hand, if $2 > \gamma^{n-1}M|\alpha| \geq 1$, we have

$$\frac{\Pi(k+1)}{\Pi(k)} = \gamma^{n-1}M|\alpha| \geq \gamma > \tau.$$

So, if $r = n-1$, we also have

$$\Pi(k+1) \geq \tau\Pi(k).$$

□

We are now in a position to give bounds on both the number of iterations required to find an integer relation for $\mathbf{x}$ and the number of exact arithmetic operations required to find this relation.

Theorem 4. *If the vector* $\mathbf{x}$ *has integer relations, then the PSLQ algorithm will find one in less than*

$$\binom{n}{2}\frac{\log(\gamma^{n-1}M)}{\log\tau}$$

iterations, where M *is the norm of a shortest relation for* $\mathbf{x}$*,* γ *is as chosen in Step 1 of the algorithm, and* $\tau > 1$ *is defined by* $\frac{1}{\tau^2} = \frac{1}{4} + \frac{1}{\gamma^2}$*.*

Proof. Suppose we have completed k iterations of the algorithm and have not yet found an integer relation for $\mathbf{x}$. Then from Lemma 5 we see that

$$\Pi(k) \geq \tau\Pi(k-1) \geq \cdots \geq \tau^k\Pi(0).$$

From Lemma 3, it follows that

$$\left(\gamma^{n-1}M\right)^{\binom{n}{2}} > \Pi(k) \geq \tau^k.$$

Now, since $\tau > 1$, we have

$$\frac{\binom{n}{2}\log(\gamma^{n-1}M)}{\log\tau} > k.$$

$\square$

Corollary 1. *If* $\mathbf{x}$ *has integer relations, then the PSLQ algorithm can be made to find one using*

$$O\left(n^4 + n^3\log M\right)$$

exact arithmetic operations.

Proof. From the above theorem, we see that the PSLQ algorithm takes fewer than

$$\frac{n^2+n}{2}\,\frac{((n-1)\log\gamma + \log M)}{\log\tau}$$

iterations, which is $O\left(n^3 + n^2\log M\right)$. Examining the algorithm, we see that Parts 1, 2, and 4 of the main iteration can be completed using $O(n)$ exact arithmetic operations, and Part 3, the size reduction of H', requires $O(n^3)$. Thus the algorithm as given requires $O(n^6 + n^5\log M)$ exact arithmetic operations. However, if we examine the proof of Lemma 5, we see that the full reduction of the matrix H' is not necessary. All that is required for this proof to go through is that $\left|h'_{i+1,i}\right| \leq \frac{1}{2}\left|h'_{i,i}\right|$ for $1 \leq i \leq n-1$. If we make this change to the algorithm, then Part 3 can be completed in $O(n)$ exact arithmetic operations as well. Thus, if $\mathbf{x}$ has integer relations, then the PSLQ algorithm can be made to find one in $O(n^4 + n^3 \log M)$ exact arithmetic operations. $\square$

Although we can modify Part 3 of the main iteration so that it requires only $O(n)$ exact arithmetic operations, this was not done, since our final goal is to implement the PSLQ algorithm using inexact arithmetic. If we do not do a full reduction of the matrix H', but instead do only a partial reduction, then the algorithm becomes unstable. More is said on this matter when we discuss the HJLS algorithm and its relation to PSLQ.

The proof of termination of the algorithm when $\mathbf{x}$ has no integer relations of norm less than T is very similar and requires only cosmetic changes. In this case, we define a new function $\Pi^*(k)$ as

$$\Pi^*(k) = \prod_{i=1}^{n-1}\left[\min\left(\gamma^{n-1}T, \frac{1}{\left|h'_{i,i}(k)\right|}\right)\right]^{n-i}.$$

Exactly as in Lemma 3, we have that

$$1 \leq \Pi^*(k) \leq (\gamma^{n-1}T)^{\binom{n}{2}}.$$

Now, rather than using Theorem 2 in Lemma 5, we instead use the fact that if the algorithm has not terminated after the kth iteration, then there is at least one j such that

$$\left|\frac{1}{h'_{j,j}}\right| < T.$$

If we redefine a and b so that

$$a = \gamma^{n-1}T\delta \quad \text{and} \quad b = \gamma^{n-1}T\left|\lambda\right|,$$

then equation B.2 becomes

$$T\gamma^{n-1} \geq \frac{\gamma^r}{\left|h'_{j,j}\right|} \geq \frac{\gamma^j}{|\alpha|} \geq \frac{\gamma}{|\alpha|} \geq \frac{1}{|\alpha|},$$

or equivalently,

$$a = T\gamma^{n-1}\delta \geq \frac{\delta}{|\alpha|}.$$

Everything carries through as before. We see that

$$\Pi^*(k+1) \geq \tau\Pi^*(k).$$

The results of this section are summarized in the following theorem:

Theorem 5. *Let $\mu = \min(M, T)$, where T is the bound passed to the PSLQ algorithm and M is the norm of a smallest integer relation for* $\mathbf{x}$ *(if* $\mathbf{x}$ *has no integer relations, then $M = \infty$). Then the PSLQ algorithm will terminate in fewer than*

$$\binom{n}{2} \frac{\log\left(\gamma^{n-1}\mu\right)}{\log \tau}$$

iterations. Upon termination, the algorithm will either return an integer relation for $\mathbf{x}$ *of norm no larger than $\gamma^{n-2}M$ or return a lower bound $\geq T$ on the norm of any integer relation for* $\mathbf{x}$.

The fact that the PSLQ algorithm can return a lower bound on the size of an integer relation for $\mathbf{x}$ is very useful. For instance, Bailey and Plouffe [1997] use this to show that if Euler's constant satisfies an integer polynomial of degree 50 or less, then the Euclidean norm of the coefficients must exceed $7 \cdot 10^{17}$.

The HJLS Algorithm

Initially given the preferable name of the *small integer relation algorithm*, HJLS is an integer relation algorithm which was developed by Håstad, Just, Lagarias, and Schnorr [1989]. As with the PSLQ algorithm, it is based on work stemming from Ferguson and Forcade's generalized Euclidean algorithm. The idea behind HJLS is again to construct a sequence of bases for the lattice $\mathbb{Z}^n$ in such a way that a lower bound on the size of any possible integer relation for $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$ increases. We present the details of the algorithm in Figure B.3. The proof of termination and a bound on the number of iterations required is essentially the same as that given for the PSLQ algorithm and will be omitted.

Theorem 6. *The HJLS algorithm correctly returns either an integer relation for* $\mathbf{x}$ *or the value 2^k as a lower bound on the norm of any possible relation. If an integer relation is found, it is no more than $\sqrt{2}^{\,n-2}$ times as large as the smallest possible relation for* $\mathbf{x}$.

Note that there is nothing special that requires having a power of 2 for the lower bound found by HJLS. This lower bound on the norm of any possible integer relation for $\mathbf{x}$ is only a consequence of the termination condition, which can be modified.

As in the proof of termination for the PSLQ algorithm, the HJLS algorithm will terminate, provided that we always have $|\mu_{r+1,r}| \leq \frac{1}{2}$ before exchanging $\mathbf{a}_r$ and $\mathbf{a}_{r+1}$. Due to this fact, the authors claim that having $|\mu_{i,j}| \leq \frac{1}{2}$ for all $i > j$ is unnecessary in the real number model of computation, and so implement their algorithm with only a partial reduction done at each step. This is unfortunate,

The HJLS Algorithm

This algorithm takes a vector $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ and a constant k as input. It either returns an integer relation for $\mathbf{x}$ or shows that $\mathbf{x}$ has no integer relations of norm less than 2^k.

Step 1 Initialization

Set $A = B = I_n$.

Let $\mathbf{a}_i^T$ be the ith row vector of A and $\mathbf{b}_i$ be the ith column vector of B

Set $\mathbf{a}_0^* = \mathbf{x}$ and $\mathbf{a}_i^* = \mathbf{a}_i - \sum_{j=0}^{i-1} \mu_{i,j}\mathbf{a}_j^*$ for $i = 1, \dots, n$,

$$\text{where } \mu_{i,j} = \begin{cases} \frac{\mathbf{a}_i \cdot \mathbf{a}_j^*}{\|\mathbf{a}_j^*\|^2}, & \|\mathbf{a}_j^*\| \neq 0, \\ 0, & \|\mathbf{a}_j^*\| = 0. \end{cases}$$

The vectors $\mathbf{a}_1^*, \mathbf{a}_2^*, \dots, \mathbf{a}_n^*$ span $\mathbf{x}^\perp$.

If $\|\mathbf{a}_n^*\| = 0$, then return $\mathbf{b}_n$ as an integer relation for $\mathbf{x}$.

Step 2

Repeat

Choose the value r that maximizes $2^r\|\mathbf{a}_r^*\|^2$ for $1 \leq r \leq n$.

Partial Reduction: (Ensure $|\mu_{r+1,r}| \leq \frac{1}{2}$)

Set $\mathbf{a}_{r+1} = \mathbf{a}_{r+1} - \lceil \mu_{r+1,r} \rfloor \mathbf{a}_r$

Set $\mathbf{b}_{r+1} = \mathbf{b}_{r+1} + \lceil \mu_{r+1,r} \rfloor \mathbf{b}_r$ to maintain $B = A^{-1}$

Update the values $\mu_{r+1,i}, 1 \leq i \leq r$

Exchange and Update:

Exchange rows $\mathbf{a}_r^T$ and $\mathbf{a}_{r+1}^T$ of A.

Exchange columns $\mathbf{b}_r$ and $\mathbf{b}_{r+1}$ of B.

Update $\mathbf{a}_r^*, \|\mathbf{a}_r^*\|, \mathbf{a}_{r+1}^*, \|\mathbf{a}_{r+1}^*\|, \mu_{r+1,r}$,

and the values $\mu_{i,r}$ and $\mu_{i,r+1}$ for $r+2 \leq i \leq n$.

Until $\|\mathbf{a}_n^*\| \neq 0$ or $\|\mathbf{a}_i^*\| \leq 2^{-k}$ for all i with $1 \leq i \leq n$.

If $\|\mathbf{a}_n^*\| \neq 0$, then return $\mathbf{b}_n$ as an integer relation for $\mathbf{x}$. Otherwise, return 2^k as a lower bound on the norm of any possible integer relation for $\mathbf{x}$.

Figure B.3: **Pseudocode implementation of the HJLS algorithm** since it leads to numerical instability in the algorithm when implemented with inexact arithmetic operations. If we implement HJLS with full reductions, which actually forces the projections of the basis vectors to tend to zero, then we simply have another implementation of the PSLQ algorithm. The equivalence of PSLQ and HJLS is treated in Meichsner [2001], where it is shown that HJLS with full reductions is equivalent to PSLQ with $\gamma = \sqrt{2}$. Specifically, we have the following.

Theorem 7. *For each iteration, the matrix A from the HJLS algorithm with full reductions and the matrix A from the PSLQ algorithm are the same, and (up to sign) the column vectors of the matrix H from PSLQ are the same as the first $n-1$ column vectors of the matrix H from HJLS.*

Practical Implementations of PSLQ

Given a set of values $x'_1, x'_2, \ldots, x'_n$ in symbolic form, it is often far too costly to find an integer relation using exact arithmetic operations. Instead, we would like to let the values $x_1, x_2, \ldots, x_n$ be good rational approximations of $x'_1, x'_2, \ldots, x'_n$ and attempt to find an integer relation for $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$ using inexact arithmetic. As stated in Bailey and Broadhurst [2001], a simple information theory argument gives a lower bound on the number of digits of precision that must be used. If we wish to recover a relation $\mathbf{a} \in \mathbb{Z}^n$ with coefficients of at most d digits in size, then the coefficients of $\mathbf{x}$ must be given to at least nd digits. Although this simple lower bound is often too low, the PSLQ algorithm usually recovers a given relation using only about 15% more digits than this bound suggests are necessary. Now, in the event that we do recover a suspected relation $\mathbf{a} \in \mathbb{Z}^n$ using inexact arithmetic, there is no guarantee that it is a true integer relation for $\mathbf{x}'$. If the values $x'_1, x'_2, \ldots, x'_n$ are computed to twice the precision and $\mathbf{a}$ still appears to be an integer relation, then this gives us evidence that it probably is one. While this cannot prove that $\mathbf{a}$ is an integer relation for $\mathbf{x}'$, it suggests that it may be worthwhile to search for a rigorous proof.

In what follows, we present implementations of PSLQ using inexact arithmetic.

The Basic Algorithm

We begin with the basic implementation of the PSLQ algorithm, similar to that given in Ferguson, Bailey, and Arno [1999], Bailey and Plouffe [1997], and Bailey and Broadhurst [2001]. The details are presented in Figure B.5. Note that the only significant differences between this implementation and the algorithm given in Figure B.2 are that here the matrices A and H have been omitted and the termination condition has been modified. Rather than waiting until $r = n-1$ and $h'_{n,n-1} = 0$, termination occurs as soon as $\mathbf{x} \cdot \mathbf{b}_j = 0$ for some column vector $\mathbf{b}_j$ of B. Although any returned relations tend to be small in practice,

The HJLS Algorithm with Full Reductions

This algorithm takes a vector $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$ and a constant T as input. It either returns an integer relation for $\mathbf{x}$ along with a lower bound on the norm of a shortest integer relation or shows that $\mathbf{x}$ has no integer relations of norm less than T.

Step 1 Initialization

Set $A = B = H = I_n$.
Let $\mathbf{a}_i$ be the ith column vector of A^T
and let $\mathbf{b}_i$ be the ith column vector of B.
Set $\mathbf{h}_0 = \mathbf{x}/\|\mathbf{x}\|$, entry $h_{n,n}$ of H to 0,
and let $\mathbf{h}_i$ be the ith column vector of H.

For j from 1 to $n-1$ do (Gram–Schmidt)
set $\mathbf{h}_j = \mathbf{h}_j - \sum_{k=0}^{j-1}(\mathbf{h}_j \cdot \mathbf{h}_k)\mathbf{h}_k$
set $\mathbf{h}_j = \mathbf{h}_j/\|\mathbf{h}_j\|$
end do.

Set $M = AH = H$ as $A = I_n$
Let $\mathbf{m}_i$ be the ith row vector of M and $m_{i,j}$ the (i,j) entry of M

Step 2 Size Reduction of M

for i from 2 to n do, for j from $i-1$ to 1 do
set $t = \lfloor m_{i,j}/m_{j,j}\rceil$
replace $\mathbf{a}_i$ with $\mathbf{a}_i - t\mathbf{a}_j$, $\mathbf{b}_j$ with $\mathbf{b}_j + t\mathbf{b}_i$, and $\mathbf{m}_j$ with $\mathbf{m}_i - t\mathbf{m}_j$
end do, end do

Step 3: The Main Iteration

Choose r such that $\sqrt{2}^i m_{i,i}$ is maximal when $i = r$.
Repeat the following until either $1/\max(m_{i,i}) \geq T$ or both $m_{n,n-1} = 0$ and $r = n-1$

1. Let $\alpha = m_{r,r}$, $\beta = m_{r+1,r}$, $\lambda = m_{r+1,r+1}$, $\delta = \sqrt{\beta^2 + \lambda^2}$, and let $S = I_{n-1}$.
   Set $s_{r,r} = \beta/\delta$, $s_{r+1,r} = \lambda/\delta$, $s_{r,r+1} = \lambda/\delta$, and $s_{r+1,r+1} = -\beta/\delta$.
2. interchange rows $\mathbf{a}_r^T$ and $\mathbf{a}_{r+1}^T$ of A, columns $\mathbf{b}_r$ and $\mathbf{b}_{r+1}$ of B, and rows $\mathbf{m}_r$ and $\mathbf{m}_{r+1}$ of M.
3. Replace H with HS and M with MS
4. Size reduce M as in Step 2.
5. Choose r such that $\sqrt{2}^i m_{i,i}$ is maximal as above.

Step 4: Return $1/\max(m_{i,i})$ as a lower bound on the norm of any integer relation for $\mathbf{x}$. If $m_{n,n-1} = 0$, then return $\mathbf{b}_{n-1}$ as an integer relation for $\mathbf{x}$.

Figure B.4: **Pseudocode implementation of the HJLS algorithm with full reductions**

The Basic PSLQ Algorithm

This algorithm takes a vector $\mathbf{x}^T = [x_1, x_2, \dots, x_n]$ and a constant $T \geq 1$ as input. It either returns a suspected integer relation for $\mathbf{x}$ or a lower bound ($\geq T$) on the norm of any possible relation for $\mathbf{x}$.

Step 1: Initialization

Fix the constant $\gamma > \sqrt{\frac{4}{3}}$.

Let $B = I$ and let $\mathbf{b}_j$ be the jth column vector of B.

Let $\mathbf{h}'_\mathbf{i}$ be the ith row vector of H', where the entries of H' are defined as follows:

$$h'_{i,j} = \begin{cases} 0 & 1 \leq i < j \leq n-1, \\ s_{i+1}/s_i & 1 \leq i = j \leq n-1, \\ -x_i x_j / s_j s_{j+1} & 1 \leq j < i \leq n, \end{cases} \quad \text{where } s_j^2 = \sum_{k=j}^{n} x_k^2.$$

Set $\mathbf{y} = \mathbf{x}/\|\mathbf{x}\|$ and let y_i be the ith component of $\mathbf{y}$.

Step 2: Size Reduce H'

for i from 2 to n do, for j from $i-1$ downto 1 do

set $t = \lfloor h'_{i,j}/h'_{j,j} \rceil$

Replace $\mathbf{b}_j$ with $\mathbf{b}_j + t\mathbf{b}_i$, $\mathbf{h}'_i$ with $\mathbf{h}'_i - t\mathbf{h}'_j$, and y_j with $y_j + ty_i$

end do, end do

Step 3: The Main Iteration

Repeat the following until either $1/\max\left|h'_{i,i}\right| \geq T$ or $\min y_j/\|\mathbf{b}_j\| < \epsilon$:

1. Choose r such that $\gamma^i \left|h'_{i,i}\right|$ is maximal when $i = r$. Then interchange columns $\mathbf{b}_r$ and $\mathbf{b}_{r+1}$ of B, rows $\mathbf{h}'_r$ and $\mathbf{h}'_{r+1}$ of H', and entries y_r and y_{r+1} of $\mathbf{y}$.
2. If $r < n-1$, then

   set $\alpha = h'_{r+1,r}$, $\beta = h'_{r,r}$, $\gamma = h'_{r,r+1}$, and $\delta = \sqrt{\beta^2 + \lambda^2}$

   for i from r to n do

   set $t = h'_{i,r}$, $h'_{i,r} = \frac{\beta}{\delta} h'_{i,r} + \frac{\lambda}{\delta} h'_{i,r+1}$, and $h'_{i,r+1} = -\frac{\lambda}{\delta} t + \frac{\beta}{\delta} h'_{i,r+1}$

   end do
3. Size reduce H'

   For i from $r+1$ to n do, for j from $\min(i-1, r+1)$ downto 1 do

   set $t = \lfloor h'_{i,j}/h'_{j,j} \rceil$

   Replace $\mathbf{b}_j$ with $\mathbf{b}_j + t\mathbf{b}_i$, $\mathbf{h}'_i$ with $\mathbf{h}'_i - t\mathbf{h}'_j$, and y_j with $y_j + ty_i$

   end do, end do

Step 4: If $\min\{y_j/\|\mathbf{b}_j\|\} < \epsilon$, then return the corresponding $\mathbf{b}_j$ as an integer relation for $\mathbf{x}$; otherwise, return $1/\max\left|h'_{i,i}\right|$ as a lower bound on the norm of any relation for $\mathbf{x}$.

Figure B.5: **Pseudocode implementation of the basic PSLQ algorithm** this modified termination condition causes us to lose the ability to claim that they have norm no larger than $\gamma^{n-2}M$ where M is the norm of a smallest integer relation for $\mathbf{x}$.

Some care must be taken when checking to see whether $\mathbf{x} \cdot \mathbf{b}_j = 0$. We shall claim that $\mathbf{x} \cdot \mathbf{b}_j = 0$ when $\frac{\mathbf{x}}{\|\mathbf{x}\|} \cdot \frac{\mathbf{b}_j}{\|\mathbf{b}_j\|} < \epsilon$, where ϵ depends on the level of precision being used. If we look only at the values $y_j = \mathbf{b}_j \cdot \frac{\mathbf{x}}{\|\mathbf{x}\|}$, then we may miss a relation. If $\|\mathbf{b}_j\|$ is large enough, then $\mathbf{b}_j \cdot \frac{\mathbf{x}}{\|\mathbf{x}\|}$ may be larger than the given value of ϵ. Since it is undesirable to require the calculation of the values $\|\mathbf{b}_j\|$ for $1 \leq j \leq n$ with each iteration, it is noted that in practice the values y_j tend to stay within a few orders of magnitude of each other and gradually decrease until one of the $\mathbf{b}_j$ is an integer relation for $\mathbf{x}$. As one would expect, when $\mathbf{b}_j \cdot \mathbf{x} = 0$ the corresponding value y_j suddenly decreases. Rather than checking all the values $y_j/\|\mathbf{b}_j\|$ to see whether one is less than ϵ, we can select the value j such that y_j is minimal and look only at the corresponding value of $y_j/\|\mathbf{b}_j\|$.

Periodic Reductions and the Multipair Algorithm

For a first improvement to the basic algorithm, we note that the full reductions of the matrix H' are a bottleneck. As the standard HJLS algorithm shows, we cannot omit the full reductions altogether, since this causes severe numerical instability. We can, however, perform them periodically and still achieve good results. Rather than fully reducing the matrix H' at each step, we will perform a full reduction only when $r = n-1$. If $r < n-1$, then we will perform a partial reduction prior to exchanging $\mathbf{h}_r$ and $\mathbf{h}_{r+1}$ to ensure that $\left|h'_{r+1,r}\right| \leq \left|h'_{r,r}\right|/2$. The details of the PSLQ algorithm with periodic reductions are presented in Figure B.6.

On a similar note, but with an eye towards a parallel implementation, Bailey and Broadhurst [2001] have introduced a variant of PSLQ that they call the multipair algorithm. The idea behind this variant is to first select a number of disjoint pairs $(r_i, r_i + 1)$ and then perform the normal operations of PSLQ on each pair with $r = r_i$. One can easily do this in such a way that the operations from one pair do not affect the operations of another, since the pairs are disjoint. In addition, they have also reordered the steps in which the full reduction of the matrix H' are performed. Even though it has been designed for a parallel implementation, when run on a single processor the multipair algorithm offers an improvement to the basic algorithm. However, in this case it amounts to little more than the PSLQ algorithm with periodic reductions and a poor selection procedure. The selection procedure used in the algorithm is as follows:

1. Sort the entries of the length $(n-1)$ vector $\left[\gamma^i \left|h'_{i,i}\right|\right]$ in decreasing order, producing the sort indices.

2. Beginning at the sort index r_1 corresponding to the largest $\gamma^i \left|h'_{i,i}\right|$, select pairs of indices $(r_i, r_i + 1)$, where r_i is the sort index. If at any step

The PSLQ Algorithm with Periodic Reductions

This algorithm takes a vector $\mathbf{x}^T = [x_1, x_2, \ldots, x_n]$ and a constant $T \geq 1$ as input. It either returns a suspected integer relation for $\mathbf{x}$ or a lower bound ($\geq T$) on the norm of any possible relation for $\mathbf{x}$.

Step 1: Initialization (see Figure B.5)

Step 2: Size Reduce H' (see Figure B.5)

Step 3: The Main Iteration
Repeat the following until either $1/\max\left|h'_{i,i}\right| \geq T$ or $\min y_j/\|\mathbf{b}_j\| < \epsilon$:

1. set doFullReduction = false
   while doFullReduction = false do
   Choose r such that $\gamma^i \left|h'_{i,i}\right|$ is maximal when $i = r$.
   Set $t = \lfloor h'_{r+1,r}/h'_{r,r} \rceil$
   and let $\mathbf{b}_r = \mathbf{b}_r + t\mathbf{b}_{r+1}$, $\mathbf{h}'_{r+1} = \mathbf{h}'_{r+1} - t\mathbf{h}'_r$, and $y_r = y_r + ty_{r+1}$.
   Interchange columns $\mathbf{b}_r$ and $\mathbf{b}_{r+1}$ of B, rows $\mathbf{h}'_r$ and $\mathbf{h}'_{r+1}$ of H', and entries y_r and y_{r+1} of $\mathbf{y}$.
   If $r < n-1$, then
   set $\alpha = h'_{r+1,r}$, $\beta = h'_{r,r}$, $\gamma = h'_{r,r+1}$, and $\delta = \sqrt{\beta^2 + \lambda^2}$
   for i from r to n do
   set $t = h'_{i,r}$, $\quad h'_{i,r} = \frac{\beta}{\delta} h'_{i,r} + \frac{\lambda}{\delta} h'_{i,r+1}$,
   and let $h'_{i,r+1} = -\frac{\lambda}{\delta} t + \frac{\beta}{\delta} h'_{i,r+1}$
   end do
   else
   doFullReduction = true
   end if
   end do
2. Size reduce H' as in Step 2 above

Step 4: If $\min y_j/\|\mathbf{b}_j\| < \epsilon$, then return the corresponding $\mathbf{b}_j$ as an integer relation for $\mathbf{x}$; otherwise, return $1/\max\left|h'_{i,i}\right|$ as a lower bound on the norm of any relation for $\mathbf{x}$.

Figure B.6: **Pseudocode implementation of the PSLQ algorithm with periodic full reductions** either r_i or $r_i + 1$ has already been selected, pass to the next index in the list. Continue until either the maximum number of pairs desired has been selected, or the list is exhausted.

It has been reported that for certain problems, the multipair algorithm falls into a cycle. Examining the selection criterion, we see that although we pass to the next index in the list if either r_i or $r_i + 1$ has already been selected, we do allow pairs $(r_i, r_i + 1)$ where $r_i + 1$ has already been passed over. We allow pairs $(r_i, r_i + 1)$ where $\left|h'_{r_i,r_i}\right| \le \gamma \left|h'_{r_i+1,r_i+1}\right|$. If we restrict ourselves to pairs where either $r_i = n - 1$ or $\left|h'_{r_i,r_i}\right| > \gamma \left|h'_{r_i+1,r_i+1}\right|$, then we cannot fall into a cycle. This can be shown by considering the product $\mathbf{P} = \prod_{i=1}^{n-1} \left|h'_{i,i}\right|^{n-i}$.

First, consider the pair $(r_i, r_i + 1)$, where $r_i < n - 1$. Let $\alpha = h'_{r_i,r_i}$, $\beta = h'_{r_i+1,r_i}$, $\lambda = h'_{r_i+1,r_i+1}$, and let $\delta = \sqrt{\beta^2 + \lambda^2}$. Then since $\beta^2 \le \alpha^2/4$, $\lambda^2 < \alpha^2/\gamma^2$, and $1/\gamma^2 < 3/4$ we have

$$\frac{|\delta|^{n-r_i} \left|\alpha\lambda/\delta\right|^{n-r_i-1}}{|\alpha|^{n-r_i} |\lambda|^{n-r_i-1}} = \frac{|\delta|}{|\alpha|} = \frac{\sqrt{\beta^2+\lambda^2}}{|\alpha|} < \frac{\sqrt{\alpha^2/4+\alpha^2/\gamma^2}}{|\alpha|} = \sqrt{\frac{1}{4}+\frac{1}{\gamma^2}} < 1.$$

Since the algorithm replaces $h'_{r_i,r_i} = \alpha$ and $h'_{r_i+1,r_i+1} = \lambda$ with the values δ and $-\alpha\lambda/\delta$, at the end of the iteration the term $\left|h'_{r_i,r_i}\right|^{n-r_i} \left|h'_{r_i+1,r_i+1}\right|^{n-r_i-1}$ in the product $\mathbf{P}$ has been decreased.
In the case when $r_i = n-1$, the algorithm simply exchanges rows $\mathbf{h'}_n$ and $\mathbf{h'}_{n-1}$ of H', resulting in a decrease of the value $\left|h'_{n-1,n-1}\right|$ by at least a factor of 2. Here, the term $\left|h'_{n-1,n-1}\right|$ of the product $\mathbf{P}$ decreases as well.

This shows that $\mathbf{P} = \prod_{i=1}^{n-1} |h'_i|^{n-i}$ decreases with each iteration of the multipair algorithm, provided that we add the restriction $\left|h'_{r_i,r_i}\right| > \gamma \left|h'_{r_i+1,r_i+1}\right|$ to our selection procedure. Since the product $\mathbf{P}$ strictly decreases with each iteration, we cannot fall into a cycle.

A Multilevel Implementation

Although using periodic full reductions can reduce the time required to execute the PSLQ algorithm, run times can still be excessively long for large problems. As a further improvement we consider a multilevel implementation (Bailey and Broadhurst [2001]), an implementation in which the majority of the calculations are done using low-precision arithmetic. Even though this introduces a significant amount of additional overhead, it drastically reduces the time spent within the main iteration and results in an overall savings.

To apply such a scheme, we first perform the usual initialization and reduction steps to produce the full precision versions of B, H', and $\mathbf{y}$. We then let $\overline{H'}$ be the double-precision equivalent of $H'/\max\left|h'_{i,j}\right|$, let $\overline{\mathbf{y}}$ be the double-precision equivalent of $\mathbf{y}/\min|y_i|\,a$, and repeat the following until either a relation is found or the desired bound on the norm of any possible integer relation is achieved:

1. Using only double-precision arithmetic, set both $\overline{A}$ and $\overline{B}$ equal to I and repeat the main iteration of PSLQ with periodic full reductions on the matrices $\overline{B}$, $\overline{H'}$, $\overline{A}$, and the vector $\overline{\mathbf{y}}$. Note that to maintain $\overline{A} = (\overline{B})^{-1}$, when we interchange columns $\overline{\mathbf{b}}_r$ and $\overline{\mathbf{b}}_{r+1}$ of $\overline{B}$, we must interchange rows $\overline{\mathbf{a}}_r^T$ and $\overline{\mathbf{a}}_{r+1}^T$ of $\overline{A}$, and when we set $\overline{\mathbf{b}}_j = \overline{\mathbf{b}}_j + t\overline{\mathbf{b}}_i$ we must set $\overline{\mathbf{a}}_i = \overline{\mathbf{a}}_i - t\overline{\mathbf{a}}_j$. Stop when either a relation is found, $\min|\overline{y}_i| < \overline{\epsilon}$, or $\max|\overline{a}_{i,j}| > \overline{\mu}$, where good choices for the values $\overline{\epsilon}$ and $\overline{\mu}$ are 10^{-12} and 10^{12}. The reason for requiring a bound on the integral entries of $\overline{A}$ is that if they become too large, then they can no longer be accurately stored.

2. Returning to full-precision arithmetic, let $B = B\overline{B}$, $H' = \overline{A}H'$, and $\mathbf{y} = \mathbf{x}B$. Then let $\overline{\mathbf{y}}$ be the double-precision equivalent of $\mathbf{y}/\min|y_i|$ and let $\overline{H'}$ be the double-precision equivalent of $H'/\max\left|h'_{i,j}\right|$. Using double-precision, perform an LQ factorization of the matrix $\overline{H'}$ and set $\overline{H'}$ equal to L.

For full details of the multilevel PSLQ algorithm, see Meichsner [2001]. A three-level scheme is also outlined in Bailey and Broadhurst [2001].

It is of interest to note that the code is in some sense self-correcting. Even if some errors are introduced within the double-precision loop, causing incorrect choices of t and r, we may recover from this. As long as the matrices $\overline{A}$ and $\overline{B}$ have integral entries and LQ factorization of $\overline{A}H'$ produces a matrix L for which the maximum diagonal entry has decreased, then we have increased a lower bound on the norm of any possible integer relation for $\mathbf{x}$ and have everything we need to proceed. Even with small errors at the double-precision level, we may still move forward and recover an integer relation or an appropriate lower bound.

A Selection of Timings for the Various Algorithms

To give a brief idea of the relative efficiency of the algorithms considered, we present a small selection of timings. Although we have covered only the basic LLL algorithm, timings are also presented for Maple's `lin_dep` routine, a routine based on the integral LLL algorithm.

For the timings, the four algebraic numbers $\alpha_1 = 3^{1/4} - 2^{1/4}$, $\alpha_2 = -3^{1/5} + 2^{1/5}$, $\alpha_3 = 3^{1/5} + 2^{1/6}$ and $\alpha_4 = 3^{1/6} - 2^{1/6}$ were considered. As the minimal polynomials of these numbers are

$$
\begin{aligned}
p_1(x) &= x^{16} - 20x^{12} - 666x^8 - 3860x^4 + 1, \\
p_2(x) &= x^{25} + 5x^{20} + 3760x^{15} - 11240x^{10} + 116255x^5 + 1, \\
p_3(x) &= x^{30} - 18x^{25} - 10x^{24} + 135x^{20} - 7380x^{19} + 40x^{18} - 540x^{15} \\
&\quad - 135540x^{14} - 56160x^{13} - 80x^{12} + 1215x^{10} - 336420x^9 \\
&\quad + 538380x^8 - 43920x^7 + 80x^6 - 1458x^5 - 102060x^4 \\
&\quad - 98280x^3 - 20520x^2 - 1440x + 697,
\end{aligned}
$$

and

$$p_4(x) = x^{36} - 30x^{30} - 16221x^{24} - 618280x^{18} + 3137919x^{12} - 4281690x^6 + 1,$$

we see that there exist integer relations for the vectors $\mathbf{x}_i = [1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{n_i}]^T$ where $n_1 = 16$, $n_2 = 25$, $n_3 = 30$, and $n_4 = 36$. Both the time and number of digits required to recover these relations are presented in Table B.1. These were found by successively reducing the number of digits in increments of 5 until an incorrect relation was returned. The time and number of digits used in the last correct run appear in the table. All algorithms were implemented in Maple V, Release 5, and run on a machine with a 600 MHz Pentium III processor.

	$\alpha_1 = 3^{1/4} - 2^{1/4}$		$\alpha_2 = -3^{1/5} + 2^{1/5}$	
Algorithm	*Digits*	*Time*	*Digits*	*Time*
LLL				
The Basic Algorithm	60	10.8 s	130	94.9 s
Maple's `lin_dep` routine	60	3.1 s	140	34.5 s
HJLS				
With full reductions	80	21.6 s	180	347.3 s
PSLQ ($\gamma = \sqrt{2}$)				
The Basic Algorithm	80	13.5 s	175	212.3 s
Periodic Full Reductions	80	5.8 s	175	73.1 s
Multilevel scheme	80	2.2 s	180	34.4 s
PSLQ ($\gamma = \sqrt{4/3}$)				
The Basic Algorithm	70	15.3 s	150	184.2 s
Periodic Full Reductions	70	6.3 s	150	73.1 s
Multilevel scheme	70	2.1 s	145	20.1 s
	$\alpha_3 = 3^{1/5} + 2^{1/6}$		$\alpha_4 = 3^{1/6} - 2^{1/6}$	
Algorithm	*Digits*	*Time*	*Digits*	*Time*
LLL				
The Basic Algorithm	435	1672.2 s	250	1148.7 s
Maple's `lin_dep` routine	315	296.1 s	265	315.5 s
HJLS				
With full reductions	245	1415.5 s	335	4722.1 s
PSLQ ($\gamma = \sqrt{2}$)				
The Basic Algorithm	245	1125.0 s	330	3400.9 s
Periodic Full Reductions	245	353.7 s	330	1025.1 s
Multilevel scheme	245	136.9 s	325	448.2 s
PSLQ ($\gamma = \sqrt{4/3}$)				
The Basic Algorithm	205	843.2 s	280	3427.3 s
Periodic Full Reductions	210	312.4 s	280	728.9 s
Multilevel scheme	200	94.6 s	280	309.3 s

Table B.1: Selected timings for the various algorithms

Appendix C

Explicit Merit Factor Formulae

The main purpose of this chapter is to give explicit formulae for the L_4 norms (on the boundary of the unit disk), and hence also the merit factors, of various polynomials that are closely related to the Fekete polynomials (see Chapter 5). These are all related to the old problem of constructing sequences of polynomials with coefficients in the set $\{+1, -1\}$ and with small L_4 norm.

Throughout this appendix we will be using the notation (m, n) for the greatest common divisor of m and n. As before, the L_α norm on the boundary of the unit disk is defined by

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

Let p be a prime number and let $(\frac{\cdot}{p})$ be the Legendre symbol. We now define the particular polynomials we consider. The Fekete polynomials are defined by

$$f_p(z) := \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) z^n,$$

and the closely related polynomials, F_p, by

$$F_p(z) := 1 + f_p(z) = 1 + \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) z^n.$$

If we cyclically permute the coefficients of f_p by about $p/4$ places, we get an example of Turyn's that we denote by

$$R_p(z) := \sum_{n=0}^{p-1} \left(\frac{n + [p/4]}{p}\right) z^n,$$

where $[\cdot]$ denotes the nearest integer, and we denote the general shifted Fekete polynomials by

$$f_p^t(z) := \sum_{n=0}^{p-1} \left(\frac{n+t}{p}\right) z^n.$$

Note that the above polynomials are either Littlewood polynomials or differ from Littlewood polynomials in a single coefficient.

The $\{R_p\}$ above are a sequence with asymptotic merit factor 6. Golay [1983] gives a heuristic argument for this observation of Turyn's, and this is proved rigorously in Høholdt and Jensen [1988]. The Fekete polynomials themselves have asymptotic merit factor $\frac{3}{2}$, and different amounts of cyclic permutation can give rise to any asymptotic merit factor between $\frac{3}{2}$ and 6. This result is recovered, in more generality, in Corollary 1. Much material on the Fekete polynomials may be accessed in Conrey et al. [2000].

The Legendre symbol $(\frac{n}{p})$ is an example of a real primitive character modulo p. One can extend the analysis of the L_4 norm to the character polynomials associated with nonreal primitive characters modulo N and to the Jacobi symbol $\left(\frac{n}{N}\right)$ for squarefree odd integers N. Our main objective is to prove explicit formulae for the L_4 norm of Fekete and Turyn polynomials. We also state related results for nonreal primitive characters and Jacobi symbols that can be proved in a similar fashion.

Let χ be a primitive character mod N. Let

$$f_\chi(z) := \sum_{n=0}^{N-1} \chi(n) z^n$$

be the character polynomial associated to χ. Let $\omega := e^{2\pi i/N}$ and let $\tau(\chi)$ be the Gaussian sum defined by

$$\tau(\chi) := \sum_{n=0}^{N-1} \chi(n)\omega^n.$$

Since χ is primitive,

$$f_\chi(\omega^k) = \tau(\chi)\bar{\chi}(k) \tag{1}$$

for $k = 0, 1, \ldots, N-1$. Also, we have

$$|\tau(\chi)|^2 = N \qquad \text{and} \qquad \overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi}) \tag{2}$$

(see Chapter 8 in Apostol [1976]). The shifted polynomial $f_\chi^t(z)$ obtained by shifting the coefficients of $f_\chi(z)$ to the left by t is defined as

$$f_\chi^t(z) := \sum_{n=0}^{N-1} \chi(n+t) z^n$$

for $1 \le t \le N$. Clearly, if $\chi(n) = (\frac{n}{p})$, then the Fekete polynomials $f_p(z)$ and Turyn polynomials $R_p(z)$ are examples of $f_\chi^t(z)$ with $t = p$ and $t = [p/4]$ respectively. It is easy to see that

$$f_\chi^t\left(\omega^k\right) = \omega^{-tk} f_\chi\left(\omega^k\right) \tag{3}$$

for any $0 \le k \le N-1$. Thus, from (1)–(3), we have

$$\left|f_\chi^t(\omega^k)\right|^2 = \begin{cases} 0 & \text{if } (N,k) \neq 1, \\ N & \text{if } (N,k) = 1. \end{cases} \tag{4}$$

Suppose N is odd. It can be shown fairly easily by an interpolation argument (Høholdt and Jensen [1988] or Borwein and Choi [2002]) that

$$\|f_\chi^t\|_4^4 = \frac{1}{2N}\left\{\sum_{k=0}^{N-1}\left|f_\chi^t\left(\omega^k\right)\right|^4 + \sum_{k=0}^{N-1}\left|f_\chi^t\left(-\omega^k\right)\right|^4\right\}. \tag{5}$$

Using (4),

$$\sum_{k=0}^{N-1}\left|f_\chi^t\left(\omega^k\right)\right|^4 = N^2\phi(N). \tag{6}$$

It remains to study the second summation

$$\sum_{k=0}^{N-1}\left|f_\chi^t\left(-\omega^k\right)\right|^4.$$

For $1 \le t \le N$ and $0 \le k \le N-1$, we have

$$f_\chi^{N-t+1}\left(-\omega^k\right) = \omega^{-k}\chi(-1) f_\chi^t\left(-\omega^{-k}\right).$$

In particular, we have $\left|f_\chi^t\left(-\omega^k\right)\right| = \left|f_\chi^{N-t+1}\left(-\omega^{-k}\right)\right|$ for $0 \le k \le N-1$ and hence, for simplicity, we may assume $1 \le t \le (N+1)/2$ from now on.

We use the basic approach of Høholdt and Jensen [1988], which is by interpolation at the $2N$th roots of unity. Using the Lagrange interpolation formula at the Nth roots of unity, we have

$$f_\chi^t(z) = \frac{1}{N}\sum_{j=0}^{N-1}\frac{z^N - 1}{z - \omega^j}\omega^j f_\chi^t(\omega^j).$$

It follows that

$$\begin{aligned} \sum_{k=0}^{N-1}|f_\chi^t(-\omega^k)|^4 &= \frac{16}{N^4}\sum_{k=0}^{N-1}\left|\sum_{j=0}^{N-1}\frac{\omega^j}{\omega^k + \omega^j} f_\chi^t(\omega^j)\right|^4 \\ &= \frac{16}{N^4}\sum_{a,b,c,d=0}^{N-1} f_\chi^t(\omega^a)\overline{f_\chi^t(\omega^b)} f_\chi^t(\omega^c)\overline{f_\chi^t(\omega^d)}\omega^{a+c} \\ &\quad \times \sum_{k=0}^{N-1}\frac{1}{\omega^k + \omega^a}\frac{\omega^k}{\omega^k + \omega^b}\frac{1}{\omega^k + \omega^c}\frac{\omega^k}{\omega^k + \omega^d}. \end{aligned}$$

We group the terms in the above summation over a, b, c, and d by the following cases: (1) $a = c$ and $a \neq b \neq d$; (2) $a = b = c \neq d$; (3) $a = b, c = d$; (4) $a \neq b \neq c \neq d$, and we obtain the following formula:

$$\sum_{k=0}^{N-1} \left| f_\chi^t\left(-\omega^k\right)\right|^4 = \frac{16}{N^4}(A+B+C), \tag{7}$$

where

$$\begin{aligned}
A &= \frac{1}{48}N^2(N^2+2)\sum_{a=0}^{N-1}\left|f_\chi^t\left(\omega^a\right)\right|^4, \\
B &= -\frac{N^2}{2}\operatorname{Re}\left\{\sum_{a=0}^{N-1}\left|f_\chi^t\left(\omega^a\right)\right|^2 f_\chi^t(\omega^a)\sum_{k=1}^{N-1}\frac{\overline{f_\chi^t(\omega^{a-k})}\left(\omega^k+1\right)}{\left|\omega^k-1\right|^2}\right\}, \\
C &= N^2\sum_{a=0}^{N-1}\left|f_\chi^t\left(\omega^a\right)\right|^2\left|\sum_{k=1}^{N-1}\frac{f_\chi^t(\omega^{a-k})}{\omega^k-1}\right|^2 \\
&\quad -\frac{N^2}{2}\operatorname{Re}\left\{\sum_{a=0}^{N-1}\overline{f_\chi^t(\omega^a)^2}\left(\sum_{k=1}^{N-1}\frac{f_\chi^t(\omega^{a-k})}{\omega^k-1}\right)^2\right\}.
\end{aligned} \tag{8}$$

Here A, B, and C are the sums of terms according to the above cases (1), (2), and (3) respectively, and the sum of terms corresponding to case (4) is zero.

Using (4), we have

$$A = \frac{N^4\left(N^2+2\right)\phi(N)}{48} \tag{9}$$

and

$$\begin{aligned}
B &= -\frac{N^4}{2}\operatorname{Re}\left\{\sum_{k=1}^{N-1}\frac{\omega^{-tk}\left(\omega^k+1\right)}{\left|\omega^k-1\right|^2}\sum_{n=0}^{N-1}\overline{\chi(n)}\chi(n-k)\right\} \\
&= \frac{N^4}{2}\operatorname{Re}\left\{\sum_{k=1}^{N-1}\frac{\omega^{tk}\left(\omega^k+1\right)}{\left(\omega^k-1\right)^2}\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)}\right\} \\
&= \frac{N^2}{2}\operatorname{Re}\left\{\sum_{a,b=1}^{N-1}ab\sum_{k=1}^{N-1}\omega^{k(t+a+b)}\left(\omega^k+1\right)\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)}\right\} \\
&= \frac{N^2}{2}\operatorname{Re}\left\{\sum_{a,b=1}^{N-1}ab\sum_{k=0}^{N-1}\left(\omega^{k(1+t+a+b)}+\omega^{k(t+a+b)}\right)\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)}\right\} \\
&\quad -\frac{N^4(N-1)^2\phi(N)}{4},
\end{aligned}$$

because

$$\frac{1}{\omega^j-1} = \frac{1}{N}\sum_{n=1}^{N-1}n\omega^{jn}, \qquad 1 \leq j \leq N-1. \tag{10}$$

We now observe that

$$\begin{aligned}\sum_{k=0}^{N-1}\omega^{k\alpha}\sum_{n=0}^{N-1}\chi(n)\overline{\chi(n-k)} &= \sum_{n=0}^{N-1}\chi(n)\sum_{k=0}^{N-1}\overline{\chi(n-k)}\omega^{k\alpha}\\ &= \sum_{n=0}^{N-1}\chi(n)\omega^{n\alpha}\overline{f_\chi(\omega^\alpha)}\\ &= |f_\chi(\omega^\alpha)|^2 = N|\chi(\alpha)|^2,\end{aligned}$$

and hence

$$B = \frac{N^3}{2}\left(\sum_{\substack{a,b=1\\(a+b+t+1,N)=1}}^{N-1} ab\right) + \frac{N^3}{2}\left(\sum_{\substack{a,b=1\\(a+b+t,N)=1}}^{N-1} ab\right) - \frac{N^4(N-1)^2\phi(N)}{4}. \tag{11}$$

We now study term C in (7). From (1) and (10), the second term in (8) equals

$$\begin{aligned}&-\frac{N^2}{2}\operatorname{Re}\left\{\sum_{a=0}^{N-1}\overline{f_\chi^t(\omega^a)^2}\left(\sum_{k=1}^{N-1}\frac{f_\chi^t(\omega^{a-k})}{\omega^k-1}\right)^2\right\}\\ &= -\frac{N^4}{2}\operatorname{Re}\left\{\sum_{a=0}^{N-1}\chi^2(a)\left(\sum_{k=1}^{N-1}\frac{\omega^{kt}\overline{\chi(a-k)}}{\omega^k-1}\right)^2\right\}\\ &= -\frac{N^4}{2}\operatorname{Re}\left\{\sum_{a=0}^{N-1}\chi^2(a)\left(\frac{1}{N}\sum_{n=1}^{N-1}n\sum_{k=1}^{N-1}\overline{\chi(a-k)}\omega^{k(t+n)}\right)^2\right\}.\end{aligned}$$

Using (1) and (3) again, this is equal to

$$\begin{aligned}&-\frac{N^4}{2}\operatorname{Re}\left\{\sum_{a=0}^{N-1}\chi^2(a)\left(\frac{\overline{\tau(\chi)}}{N}\sum_{n=1}^{N-1}n\chi(n+t)\omega^{a(t+n)} - \frac{N-1}{2}\overline{\chi(a)}\right)^2\right\}\\ &= -\frac{N^4}{2}\operatorname{Re}\left\{\frac{\overline{\tau(\chi)}^2}{N^2}\sum_{n,m=1}^{N-1}nm\chi(n+t)\chi(m+t)\sum_{a=0}^{N-1}\chi^2(a)\omega^{a(n+m+2t)}\right\}\\ &\quad -\frac{N^4}{2}\left(\frac{N-1}{2}\right)^2\phi(N) + \frac{N^4(N-1)}{2}\operatorname{Re}\left\{\frac{\overline{\tau(\chi)}}{N}\sum_{n=1}^{N-1}n\chi(n+t)f_\chi(\omega^{t+n})\right\}\\ &= -\frac{N^2}{2}\operatorname{Re}\left\{\overline{\tau(\chi)}^2\sum_{n,m=1}^{N-1}nm\chi(n+t)\chi(m+t)C_{\chi^2}(n+m+2t)\right\}\\ &\quad -\frac{N^4(N-1)^2\phi(N)}{8} + \frac{N^4(N-1)}{2}\left(\sum_{\substack{n=1\\(n+t,N)=1}}^{N-1} n\right).\end{aligned} \tag{12}$$

Here $C_\chi(l)$ is the character sum defined by

$$C_\chi(l) := \sum_{n=0}^{N-1} \chi(n)\omega^{nl},$$

and if $\chi = \chi_0$, the principal character, then $C_N(l) := C_{\chi_0}(l)$ is the usual Ramanujan sum. Note that $C_\chi(l) = f_\chi\left(\omega^l\right)$. Similarly, the first term in (8) equals

$$\begin{aligned}
&N^2 \sum_{a=0}^{N-1} |f_\chi^t(\omega^a)|^2 \left| \sum_{k=1}^{N-1} \frac{f_\chi^t(\omega^{a-k})}{\omega^k - 1} \right|^2 \\
&= N^4 \sum_{a=0}^{N-1} |\chi^2(a)| \left| \sum_{k=1}^{N-1} \frac{\omega^{kt}\overline{\chi(a-k)}}{\omega^k - 1} \right|^2 \\
&= N^3 \sum_{nm=1}^{N-1} nm\chi(n+t)\overline{\chi(m+t)}C_N(n-m) \\
&\quad + \frac{N^4(N-1)^2\phi(N)}{4} - N^4(N-1)\left(\sum_{\substack{n=1 \\ (n+t,N)=1}}^{N-1} n \right).
\end{aligned} \tag{13}$$

Thus from (7), (9), (11), (12) and (13), we prove the following.

Proposition 1. *For any primitive character χ modulo N and any $1 \le t \le (N+1)/2$, we have*

$$\sum_{k=0}^{N-1} \left| f_\chi^t\left(-\omega^k\right) \right|^4 = \frac{16}{N^4}(A+B+C), \tag{14}$$

where

$$\begin{aligned}
A &= \frac{N^4\left(N^2+2\right)\phi(N)}{48}, \\
B &= \frac{N^3}{2}\left(\sum_{\substack{a,b=1 \\ (a+b+t+1,N)=1}}^{N-1} ab \right) + \frac{N^3}{2}\left(\sum_{\substack{a,b=1 \\ (a+b+t,N)=1}}^{N-1} ab \right) - \frac{N^4(N-1)^2\phi(N)}{4},
\end{aligned} \tag{15}$$

$$\begin{aligned}
C &= -\frac{N^2}{2}\,\mathrm{Re}\left\{ \overline{\tau(\chi)}^2 \sum_{n,m=1}^{N-1} nm\chi(n+t)\chi(m+t)C_{\chi^2}(n+m+2t) \right\} \\
&\quad + \frac{N^4(N-1)^2\phi(N)}{8} \\
&\quad + N^3 \sum_{n,m=1}^{N-1} nm\chi(n+t)\overline{\chi(m+t)}C_N(n-m) - \frac{N^4(N-1)}{2}\left(\sum_{\substack{n=1 \\ (n+t,N)=1}}^{N-1} n \right).
\end{aligned}$$

For convenience, we let

$$C_1(\chi, t) := \sum_{n,m=1}^{N-1} nm\chi(n+t)\chi(m+t)C_{\chi^2}(n+m+2t)$$

and

$$C_2(\chi, t) := \sum_{n,m=1}^{N-1} nm\chi(n+t)\overline{\chi(m+t)}C_N(n-m),$$

so that

$$\begin{aligned} C = &-\frac{N}{2}\operatorname{Re}\{C_1(\chi,t)\} + \frac{N^4(N-1)^2\phi(N)}{8} \\ &+ N^3 C_2(\chi,t) - \frac{N^4(N-1)}{2}\left(\sum_{\substack{n=1\\(n+t,N)=1}}^{N-1} n\right). \end{aligned} \tag{16}$$

We next study the terms B and C in more detail.

For any real x, define

$$\{x\} := \begin{cases} x - [x] & \text{if } x \text{ is not an integer,} \\ 1 & \text{if } x \text{ is an integer,} \end{cases}$$

where $[x]$ is the integral part of x. Note that $\{x\}$ is the fractional part of x except when x is an integer.

Lemma 1. *For any positive integers k and $N \geq 2$, we have*

$$\begin{aligned} &\left(\sum_{\substack{n,m=1\\k+n+m\equiv 0 \pmod N}}^{N-1} nm\right) \\ &= \frac{N}{6}\left(N^2 - 6N - 1 + 3N\left\{\frac{k}{N}\right\}\left(2 + N - N\left\{\frac{k}{N}\right\}\right)\right). \end{aligned}$$

Proof. Clearly, we may assume $1 \leq k \leq N$. Suppose $2 \leq k \leq N-2$. Then

$$\begin{aligned} \left(\sum_{\substack{n,m=1\\k+n+m\equiv 0 \pmod N}}^{N-1} nm\right) &= \sum_{n=1}^{N-k-1} n(N-k-n) + \sum_{n=N-k+1}^{N-1} n(2N-k-n) \\ &= \sum_{n=1}^{N-1} n(N-k-n) + N\sum_{n=N-k+1}^{N-1} n \\ &= \frac{N}{6}\left(N^2 - 6N - 1 + 6k + 3Nk - 3k^2\right). \end{aligned}$$

Our lemma follows by noting that $k = N\{k/N\}$ because k/N is not an integer. The cases $k = 1$, $N-1$, and N can be verified directly. $\square$

Lemma 2. *For any integers t and $N \geq 2$, we have*

$$\left(\sum_{\substack{a,b=1 \\ (a+b+t,N)=1}}^{N-1} ab \right) = \frac{N\phi(N)}{12}(3N^2 - 6N - 2)$$
$$+ \frac{N^2}{12} \sum_{d|N} \mu(d) \left(-d + 6\left\{\frac{t}{d}\right\} \left(2 + d - d\left\{\frac{t}{d}\right\} \right) \right). \quad (17)$$

Proof. By using the formula (Theorem 2.1 of Apostol [1976])

$$\sum_{d|k} \mu(d) = \begin{cases} 1 & \text{if } k = 1, \\ 0 & \text{if } k \neq 1, \end{cases}$$

the left-hand side of (17) is equal to

$$\sum_{a,b=1}^{N-1} ab \sum_{\substack{d|N \\ d|a+b+t}} \mu(d)$$
$$= \sum_{d|N} \mu(d) \left(\sum_{\substack{a,b=1 \\ a+b+t\equiv 0 \pmod d}}^{N-1} ab \right)$$
$$= \sum_{d|N} \mu(d) \sum_{n,m=0}^{\frac{N}{d}-1} \left(\sum_{\substack{a,b=0 \\ a+b+t\equiv 0 \pmod d}}^{d-1} (a+dn)(b+dm) \right).$$

Now formula (17) follows from this, Lemma 1, and the fact that

$$\sum_{d|N} \frac{\mu(d)}{d} = \frac{\phi(N)}{N}$$

(see Theorem 2.3 of Apostol [1976]). $\square$

Formula (17) immediately gives an asymptotic estimate

$$\sum_{\substack{a,b=1 \\ (a+b+t,N)=1}}^{N-1} ab = \frac{1}{4}N^3\phi(N) + O\left(N^3 d(N)\right),$$

and hence from Proposition 1, the term B satisfies

$$B \ll N^6 d(N), \tag{18}$$

where $d(N)$ is the number of divisors of N. One expects that the order of $\left\|f_\chi^t\right\|_4^4$ should be N^2, and this corresponds to the fact that

$$\sum \left|f_\chi^t\left(-\omega^k\right)\right|^4$$

is of order N^3 according to (5). In view of (18) and (14), the term B does not contribute to the main term of $\left\|f_\chi^t\right\|_4^4$.

The term B can be evaluated precisely for some special cases by using formula (17).

Lemma 3. *If $N = p$ is an odd prime, then*

$$B = \frac{p^4}{12}\left(p^2 + 3p + 2 - 6t - 6pt + 6t^2\right). \tag{19}$$

Proof. This follows from (17) and (15) when $N = p$. □

We now study the term C of (16). Unlike the term B, which doesn't depend on the choice of primitive character χ but only on the modulus N, the term C is more sensitive to the character χ. The evaluation of the term $C_1(\chi, t)$ differs according to whether χ is a nonreal or real character.

It is well known (see Apostol [1976]) that $C_N(k)$ is a multiplicative function of N and

$$C_p(k) = \begin{cases} -1 & \text{if } (p,k) = 1, \\ p-1 & \text{if } (p,k) \neq 1. \end{cases} \tag{20}$$

We first consider the term $C_2(\chi, t)$.

Lemma 4. *Let $N = p$ be an odd prime and let χ be any primitive character modulo p. Then*

$$C_2(\chi, t) = \frac{p}{6}\left(2p^3 - 9p^2 + p + 12pt - 6t^2\right) - \left|\sum_{n=1}^{p-1} n\chi(n+t)\right|^2. \tag{21}$$

Proof. In view of (20), we have

$$\begin{aligned}
C_2(\chi,t) &= \sum_{n,m=1}^{p-1} nm\chi(n+t)\overline{\chi(m+t)}(C_p(n-m)+1) - \left|\sum_{n=1}^{p-1} n\chi(n+t)\right|^2 \\
&= p\sum_{n=1}^{\infty} n^2|\chi(n+t)|^2 - \left|\sum_{n=1}^{p-1} n\chi(n+t)\right|^2 \\
&= p\left(\sum_{n=1}^{p-1} n^2 - (p-t)^2\right) - \left|\sum_{n=1}^{p-1} n\chi(n+t)\right|^2 \\
&= p\left(\frac{1}{6}p(p-1)(2p-1) - (p-t)^2\right) - \left|\sum_{n=1}^{p-1} n\chi(n+t)\right|^2 .
\end{aligned}$$

□

If χ is real, then $\chi^2 = \chi_0$, and $C_{\chi^2}(l) = C_N(l)$ is just a Ramanujan sum. From (20), we have the following.

Lemma 5. *Let $N = p$ be an odd prime and let χ be a real primitive character; that is, $\chi(n) = \left(\frac{n}{p}\right)$, the Legendre symbol. Then*

$$\begin{aligned}
C_1(\chi,t) = \frac{1}{6}\left(\frac{-1}{p}\right) p\left(p^3 - 12p^2 - p + 24pt + 6p^2t - 12pt^2 - 6t^2\right) \\
- \left(\sum_{n=1}^{p-1} n\chi(n+t)\right)^2 . \qquad (22)
\end{aligned}$$

Proof. If χ is real, then $\chi^2 = \chi_0$, and hence by (20),

$$\begin{aligned}
C_1(\chi,t) &= \sum_{n,m=1}^{p-1} nm\chi(n+t)\chi(m+t)C_p(n+m+2t) \\
&= \sum_{n,m=1}^{p-1} nm\chi(n+t)\chi(m+t)(C_p(n+m+2t)+1) - \left(\sum_{n=1}^{p-1} n\chi(n+t)\right)^2 \\
&= p\left(\sum_{\substack{n,m=1 \\ n+m+2t\equiv 0 \pmod p}}^{p-1} nm\chi(n+t)\chi(m+t)\right) - \left(\sum_{n=1}^{p-1} n\chi(n+t)\right)^2 .
\end{aligned}$$

Now when $n+m+2t \equiv 0 \pmod p$, $\chi(n+t)\chi(m+t) = \left(\frac{-1}{p}\right)\chi_0(n+t)$, and so

$$
\begin{aligned}
C_1(\chi,t) &= p\left(\frac{-1}{p}\right)\left(\sum_{\substack{n,m=1,(n+t,p)=1\\ n+m+2t\equiv 0 \pmod p}}^{p-1} nm\right) - \left(\sum_{n=1}^{p-1} n\chi(n+t)\right)^2\\
&= p\left(\frac{-1}{p}\right)\left(\sum_{\substack{n,m=1\\ n+m+2t\equiv 0 \pmod p}}^{p-1} nm\right)\\
&\quad - p\left(\frac{-1}{p}\right)(p-t)^2 - \left(\sum_{n=1}^{p-1} n\chi(n+t)\right)^2\\
&= p\left(\frac{-1}{p}\right)\left\{\frac{p}{6}\left(p^2-6p-1+6t(2+p-2t)\right) - (p-t)^2\right\}\\
&\quad - \left(\sum_{n=1}^{p-1} n\chi(n+t)\right)^2
\end{aligned}
$$

by Lemma 1. □

From (16), Lemmas 4 and 5, and the fact that

$$\sum_{\substack{n=1\\(n+t,p)=1}}^{p-1} n = \frac{1}{2}p(p-1) - (p-t),$$

the term C can now be evaluated precisely. From (14), (19), (21), and (22), we have

$$
\begin{aligned}
\sum_{j=0}^{p-1} \left|f_p^t\left(-\omega^j\right)\right|^4 &= \frac{p}{3}\left(7p^2+9p+8+48t^2-24pt-48t\right)\\
&\qquad - \frac{16}{p}\left(1-\frac{1}{2}\left(\frac{-1}{p}\right)\right)\left|\sum_{n=1}^{p-1} n\left(\frac{n+t}{p}\right)\right|^2.
\end{aligned}
$$

We prove the main theorem of this Appendix.

Theorem 1. *Let p be an odd prime and*

$$f_p^t(z) = \sum_{n=1}^{p-1}\left(\frac{n+t}{p}\right) z^n.$$

Then for any $1 \le t \le (p+1)/2$, *we have*

$$\begin{aligned} \|f_p^t\|_4^4 =& \frac{1}{3}\left(5p^2+3p+4\right)+8t^2-4pt-8t \\ & -\frac{8}{p^2}\left(1-\frac{1}{2}\left(\frac{-1}{p}\right)\right)\left|\sum_{n=1}^{p-1} n\left(\frac{n+t}{p}\right)\right|^2 . \end{aligned} \tag{23}$$

The last term in (23) can be further estimated. By using the partial summation formula and the known estimate (Hua [1982, p. 172])

$$\left|\sum_{n=1}^{k-1}\left(\frac{n}{p}\right)\right| < p^{1/2}\log p,$$

one can show that

$$\left|\sum_{n=1}^{p-1} n\left(\frac{n+t}{p}\right)\right| = \left|p\sum_{n=1}^{t-1}\left(\frac{n}{p}\right)+\sum_{n=1}^{p-1} n\left(\frac{n}{p}\right)\right| \ll p^{3/2}\log p.$$

From this and Theorem 1, we have the following.

Corollary 1. *Let p be an odd prime and $1 \le t \le (p+1)/2$. Then*

$$\|f_p^t\|_4^4 = \frac{5}{3}p^2+8t^2-4pt+O\left(p\log^2 p\right).$$

By making the optimal choice of $t = [p/4]$, we obtain the Turyn-type polynomials

$$R_p(z) := \sum_{n=0}^{p-1}\left(\frac{n+[p/4]}{p}\right)z^n,$$

which possess the lowest known asymptotic L_4 norm among such polynomials so far. In this case, the last summation in (23) can be evaluated precisely in terms of the class number $h(-p)$, where

$$h(-d) = -\sum_{k=1}^{d-1}\frac{k}{d}\left(\frac{k}{d}\right)$$

is the class number of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{-d}\right)$. More precisely, we have

Theorem 2. *For any odd prime p, we have*

$$\|R_q\|_4^4 = \frac{7q^2}{6}-q-\frac{1}{6}-\gamma_q$$

where

$$\gamma_q := \begin{cases} h(-q)(h(-q)-4) & \textit{if} \quad q \equiv 1,5 \pmod 8, \\ 12(h(-q))^2 & \textit{if} \quad q \equiv 3 \pmod 8, \\ 0 & \textit{if} \quad q \equiv 7 \pmod 8. \end{cases}$$

We have just shown how to obtain a precise formula for $\left\|f_\chi^t(z)\right\|_4^4$ for the case $N = p$ and $\chi(n) = (\frac{n}{p})$ by using the formulae in Proposition 1. If χ is a nonreal primitive character modulo p, all the evaluations in (14), (19), and (21) of the terms A, B, and $C_2(\chi,t)$ are still valid except for the term $C_1(\chi,t)$, and $C_{\chi^2}(l)$ is no longer a Ramanujan sum. Instead, we have

$$\begin{aligned} C_1(\chi,t) &= \sum_{n,m=1}^{p-1} nm\chi(n+t)\chi(m+t)f_{\chi^2}(\omega^{n+m+2t}) \\ &= \tau(\chi^2)\sum_{n,m=1}^{p-1} nm\chi(n+t)\chi(m+t)\overline{\chi}^2(n+m+2t) \end{aligned}$$

from (1) and the fact that χ^2 is still primitive. In this case, the term $C_1(\chi,t)$ becomes more sensitive to the choice of the primitive character χ. Although a simple form of this term seems to be difficult to obtain for a general primitive character, an asymptotic estimation of $C_1(\chi,t)$ is accessible and is given in Borwein and Choi [to appear]. By transforming $C_1(\chi,t)$ in terms of generalized Dedekind sums, it is shown that

$$C_1(\chi,t) = \frac{p^3\tau(\chi)^2}{4} + O\left(p^3\log^2 p\right).$$

From this, we deduce the following.

Theorem 3. *Let p be an odd prime and let χ be a nonreal primitive character modulo p. Then for any $1 \le t \le (p+1)/2$, we have*

$$\left\|f_\chi^t\right\|_4^4 = \frac{4}{3}p^2 + O\left(p^{3/2}\log^2 p\right).$$

It is worth noting that the main term of $\left\|f_\chi^t\right\|_4^4$ is uniform for any shift t and any nonreal primitive character modulo p. This is quite different from the real primitive (Legendre) case.

One can also study the average of $\left\|f_\chi^t\right\|$ among all characters modulo p. In Borwein and Choi [to appear] it is shown that for any odd prime p and any shift t,

$$\sum_{\chi \pmod p} \left\|f_\chi^t\right\|_4^4 = (2p-3)(p-1)^2,$$

where the summation is over all characters modulo p.

For composite N, since the Ramanujan sum $C_N(k)$ is a multiplicative function of N, $C_1(\chi,t)$ and $C_2(\chi,t)$ can be estimated as before with $\chi(n) = \left(\frac{n}{N}\right)$, the Jacobi symbol. The explicit formulae are as follows.

Theorem 4. *Let $N = pq$, where p and q are odd primes, and*

$$f_N(z) := \sum_{n=0}^{N-1} \left(\frac{n}{N}\right) z^n.$$

If $p = q+2$, then

$$\begin{aligned}\|f\|_4^4 = &\ \frac{1}{3}\left(5N^2 + 9N + 4 - (8N+1)(p+q)\right)\\ &+ 24\frac{q^3}{N^2}\left(2 - \left(\frac{2}{p}\right)\right)h_p^2 - 24\frac{p^3}{N^2}\left(1 - \left(\frac{2}{q}\right)\right)h_q^2 + \frac{12}{N^2}h_N^2,\end{aligned}$$

and if $p = q+4$ and $q \equiv 3 \pmod 4$, then

$$\begin{aligned}\|f\|_4^4 = &\ \frac{1}{3}\left(5N^2 + 9N + 4 - (8N+1)(p+q)\right)\\ &+ 12\frac{q^3}{N^2}\left(5 - 3\left(\frac{2}{p}\right)\right)h_p^2 - 36\frac{p^3}{N^2}\left(1 - \left(\frac{2}{q}\right)\right)h_q^2 + \frac{12}{N^2}h_N^2,\end{aligned}$$

where $h_l := \sum_{n=1}^{l-1} n\left(\frac{n}{l}\right)$ for an odd integer l.

For asymptotic estimates, we have the following.

Theorem 5. *Let $N = p_1 p_2 \cdots p_r$ with $p_1 < p_2 < \cdots < p_r$ and*

$$f_N^t(z) := \sum_{n=0}^{N-1} \left(\frac{n+t}{N}\right) z^n$$

with $1 \le t \le N$. Then

$$\|f_N^t\|_4^4 = \frac{5}{3}N^2 - 4Nt + 8t^2 + O\left(\frac{N^{2+\epsilon}}{p_1}\right).$$

Appendix D

Research Problems

Research Problems

P1. The Integer Chebyshev Problem. *Find a nonzero polynomial in $\mathcal{Z}_n$ that has smallest possible supremum norm on the unit interval. Analyze the asymptotic behaviour as n tends to infinity.*

P2. The Prouhet–Tarry–Escott Problem. *Find a polynomial with integer coefficients that is divisible by $(z-1)^n$ and has smallest possible length. (That is, minimize the sum of the absolute values of the coefficients.)*

P3. The Erdős–Szekeres Problem. *For each n, minimize*

$$\|(1-z^{\alpha_1})(1-z^{\alpha_2})\cdots(1-z^{\alpha_n})\|_\infty,$$

where the α_i are positive integers. In particular, show that these minima grow faster than n^β for any positive constant β.

P4. Littlewood's Problem in L_∞. *Find a polynomial in $\mathcal{L}_n$ that has smallest possible supremum norm on the unit disk. Show that there exist positive constants c_1 and c_2 such that for any n it is possible to find $p_n \in \mathcal{L}_n$ with*

$$c_1\sqrt{n+1} \le |p_n(z)| \le c_2\sqrt{n+1}$$

for all complex z with $|z| = 1$.

P5. Erdős's Problem in L_∞. *Show that there exists a positive constant c_3 such that for all sufficiently large n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \ge (1+c_3)\sqrt{n+1}$.*

P6. Erdős's Problem in L_∞ for Reciprocal Polynomials. *Show that there exists a positive constant c_3' such that for all sufficiently large n and all reciprocal polynomials $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \geq \left(\sqrt{2} + c_3'\right)\sqrt{n+1}$.*

P7. The Merit Factor Problem of Golay. *Find the polynomial in $\mathcal{L}_n$ that has smallest possible L_4 norm on the unit disk. Show that there exists a positive constant c_4 such that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_4 \geq (1+c_4)\sqrt{n+1}$.*

P8. The Barker Polynomial Problem. *For n sufficiently large ($n > 12$ may suffice) and $p_n \in \mathcal{L}_n$ show that*

$$\|p_n\|_4 > \left((n+1)^2 + n + 1\right)^{1/4}.$$

Equivalently, show that no polynomial in $\mathcal{L}_n$ of degree greater than 12 can have all acyclic autocorrelation coefficients of size at most 1.

P9. Lehmer's Problem. *Show that any monic polynomial p, $p(0) \neq 0$, with integer coefficients that is irreducible and is not a cyclotomic polynomial has Mahler measure at least $1.1762\ldots$. (This latter constant is the Mahler measure of $1 + z - z^3 - z^4 - z^5 - z^6 - z^7 + z^9 + z^{10}$.)*

P10. Mahler's Problem. *For each n, find the polynomials in $\mathcal{L}_n$ that have largest possible Mahler measure. Analyze the asymptotic behaviour as n tends to infinity.*

P11. Conjecture of Schinzel and Zassenhaus. *There is a constant $c > 0$ such that any monic polynomial p_n of degree n with integer coefficients either has Mahler measure 1 or has at least one root of modulus at least $1 + c/n$.*

P12. Closure of Measures Conjecture of Boyd. *The set of all possible values of the Mahler measure of polynomials with integer coefficients in any number of variables is a closed set.*

P13. Multiplicity of Zeros of Height One Polynomials. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{F}_n$?*

P14. Multiplicity of Zeros in $\mathcal{L}_n$. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{L}_n$?*

P15. Another Erdős Problem. *Establish whether there is a positive constant c such that if*

$$V_n := \left(1 + z^{b_1}\right)\left(1 + z^{b_2}\right)\cdots\left(1 + z^{b_n}\right)$$

is in $\mathcal{A}$, then

$$\max\{b_i\} > c\,2^n.$$

P16. A Montgomery Question. *Show that the minimal s arising as in Lemma 1 of Chapter 10 does not give the right value for $\Omega[0,1]$. Does $\Omega[0,1]$ have a closed form?*

P17. Schur–Siegel–Smyth Trace Problem. *Fix $\epsilon > 0$. Suppose*

$$p_n(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathcal{Z}_n$$

has all real, positive roots and is irreducible. Show that, independently of n, except for finitely many explicitly computable exceptions,

$$|a_{n-1}| \geq (2 - \epsilon)n.$$

Research Problems from Chapter 2

R1. Is it possible to approach the merit factor problem (P7) using LLL? For which other norms is there an analogue of LLL that gives polynomial-time algorithms for finding short vectors with respect to that norm?

R2. Are there polynomial-time algorithms for any of the problems P1 through P17? (To make sense of this, one has to decide how to measure the size of an instance of the problem.) Note that it isn't clear that P2 is even algorithmic, and indeed, this is an open problem.

Research Problems from Chapter 3

R1. Verify Lehmer's problem up to, say, degree 100. (Currently it has been checked exhaustively by Rhin and Qiang up to degree 40.)

R2. Solve Lehmer's problem for some interesting classes of reciprocal polynomials; for example, the class of reciprocal Littlewood polynomials.

R3. In Exercise E8 of Chapter 3, is it possible to make p divide a height h polynomial with the same measure as p? (That is, can the factor q/p be chosen to be a product of cyclotomic polynomials?)

R4. Show that the minimum Mahler measure (> 1) of a monic polynomial in $\mathcal{Z}$ is attained by a Salem polynomial.

Research Problems from Chapter 4

R1. There are many ways to extend the Rudin–Shapiro construction. One can consider iterations of three or more terms, for example (see E3 of Chapter 4). Is it possible to extend the construction to get good lower bounds in P4?

R2. Extend the formulae of the exercises of Chapter 4 for the average of $\|p(z)\|_n^n$. So, for example, extend the formulae of Theorem 2 of Chapter 4 for $\beta_n(m, H)$ for all even n.

Research Problems from Chapter 5

R1. It is natural to ask about the growth of the Fekete polynomials on the disk D. Montgomery [1980] shows that

$$\|f_p(z)\|_D \gg \sqrt{p}\log\log p$$

and that

$$\|f_p(z)\|_D \ll \sqrt{p}\log p.$$

Which is the correct rate of growth? Extend the above result to the shifted Fekete polynomials of E1 of Chapter 5.

Research Problems from Chapter 6

Conjecture. *A Littlewood polynomial $P(z)$ of degree $N-1$ has Mahler measure 1 if and only if P can be written in the form*

$$P(z) = \pm\Phi_{p_1}(\pm z)\Phi_{p_2}\left(\pm z^{p_1}\right)\cdots\Phi_{p_r}\left(\pm z^{p_1p_2\cdots p_{r-1}}\right),$$

where $N = p_1p_2\cdots p_r$ and the p_i are primes, not necessarily distinct.

R1. Prove the above conjecture for N even.

R2. Is there a characterization of all measure 1 polynomials with coefficients just 0 and 1?

Research Problems from Chapter 7

R1. (Erdélyi) Establish whether every polynomial $p \in \mathcal{L}_n$ has at least one zero in the annulus

$$\left\{1 - \frac{c}{n} < |z| < 1 + \frac{c}{n}\right\},$$

where $c > 0$ is an absolute constant.

Research Problems from Chapter 8

R1. Prove or disprove that a polynomial $p \in \mathcal{A}_n$ has all its repeated zeros at 0 or on the unit circle.

R2. Can the multiplicity of a zero of a height 1 polynomial in $\{z \in \mathbb{C} : 0 < |z| < 1\}$ be arbitrarily large?

R3. Is it true that there is an absolute constant $c > 0$ such that every $p \in \mathcal{A}_n$ with $p(0) = 1$ has at most $c \log n$ *real* zeros? If not, what is the best possible upper bound for the number of *real* zeros of polynomials $p \in \mathcal{A}_n$? What is the best possible upper bound for the number of *distinct real* zeros of polynomials $p \in \mathcal{A}_n$?

Research Problems from Chapter 9

R1. Let Ω denote the set of all zeros of all Littlewood polynomials. Show that the boundary of Ω is a fractal set and compute its Hausdorff dimension. Show that Ω is path connected. (Odlyzko and Poonen [1993] prove that the set of all zeros of all polynomials with coefficients in the set $\{0, 1\}$ is path connected.) Determine whether Ω contains holes. Equivalently, does the complement of Ω have more than two components?

These questions should also be addressed for the polynomials of height 1.

Research Problems from Chapter 10

Conjecture. *Suppose $[a_2/b_2, a_1/b_1]$ is an interval whose endpoints are consecutive nonintegral Farey fractions. This is characterized by $(a_1 b_2 - a_2 b_1) = 1$. Then*

$$\Omega^*\left(\left[\frac{a_2}{b_2}, \frac{a_1}{b_1}\right]\right) = \max\left(\frac{1}{b_1}, \frac{1}{b_2}\right).$$

R1. Compute $\Omega[\alpha, \beta]$ exactly on any interval of length less than 4.

R2. It is very natural to explore the integer Chebyshev question in many variables, say polynomials in two variables on triangles or on squares. See Chudnovsky [1983].

The following two theorems are proved in Borwein, Erdélyi, and Kós [1999]. They relate to how small one can make polynomials in $\mathcal{F}_n$ and $\mathcal{A}_n$.

Theorem. *There are absolute constants $c_1 > 0$ and $c_2 > 0$ such that*

$$\exp\left(-c_1\sqrt{n}\right) \le \inf_{0 \ne p \in \mathcal{F}_n} \|p\|_{[0,1]} \le \exp\left(-c_2\sqrt{n}\right).$$

The left side of the above inequality in fact holds for polynomials p of the form

$$p(z) = \sum_{j=0}^{n} a_j z^j, \quad |a_0| = 1, \quad |a_j| \le 1, \quad a_j \in \mathbb{C}.$$

Theorem. *There are absolute constants $c_1 > 0$ and $c_2 > 0$ such that*

$$\exp\bigl(-c_1 \log^2(n+1)\bigr) \le \inf_{0 \ne p \in \mathcal{A}_n} \|p(-z)\|_{[0,1]} \le \exp\bigl(-c_2 \log^2(n+1)\bigr).$$

In the light of the above two theorems, it is natural to ask the following questions, which are the height 1 analogues of the integer Chebyshev problem.

R3. Does

$$\lim_{n\to\infty} \frac{\log(\inf_{0 \ne p \in \mathcal{F}_n} \|p\|_{[0,1]})}{\sqrt{n}}$$

exist? If it does, what is it?

R4. Does

$$\lim_{n\to\infty} \frac{\log\bigl(\inf_{0 \ne p \in \mathcal{A}_n} \|p(-z)\|_{[0,1]}\bigr)}{\log^2(n+1)}$$

exist? If it does, what is it?

Research Problems from Chapter 11

R1. Find infinite families of ideal solutions of the Prouhet–Tarry–Escott problem of size 9 and size 12 or show they can't exist.

R2. Find an ideal solution of size 11 or any size greater than 12.

R3. Show for some n that no ideal solutions of the Prouhet–Tarry–Escott problem exist.

Research Problems from Chapter 12

R1. Show that $N^*(k) \ll k^2$.

R2. Is it true that $N^*(k) = o(k \log k)$? This would be a significant result, since it would give better bounds for the easier Waring problem than those that follow from the current bounds for the usual Waring problem.

Research Problems from Chapter 13

R1. There is an amusing problem related to Theorem 2 of Chapter 13, whose solution would let one compute the exact l_1 norm in the case $p = 3$.

Problem. *For each n, write*

$$(1-z)\left(1-z^2\right)\left(1-z^4\right)\left(1-z^5\right)\cdots\left(1-z^{3n+1}\right)\left(1-z^{3n+2}\right) = \sum a_i z^i.$$

Show that $a_i \geq 0$ if and only if 3 divides i.

A similar result should hold for $p = 5$. See Andrews [1995].

R2. Prove the conjecture that except for $N \in \{1, 2, 3, 4, 5, 6, 8\}$

$$E_N^* \geq 2N + 2.$$

Research Problems from Chapter 14

R1. Show that no Barker polynomials exist for $n > 12$.

R2. Are there any *primitive* Golay pairs for $n \geq 100$? (See Borwein and Ferguson [to appear].)

R3. If

$$p(z) := \sum_{k=0}^{n} a_k z^k,$$

where the a_k are complex numbers, then the kth *acyclic autocorrelation coefficient* is defined by

$$c_k = \sum_{j=0}^{n-k} \overline{a_j} a_{j+k} \quad \text{and} \quad c_{-k} = \overline{c_k}.$$

Then

$$\|p(z)\|_4^4 = \left\|p(z)\overline{p(z)}\right\|_2^2 = \sum_{k=-n}^{n} |c_k|^2.$$

A natural generalization of a Barker polynomial would be a polynomial with all coefficients complex numbers of modulus 1 that satisfies $|c_k| \le 1$ for $k \ne 0$.

Do generalized Barker polynomials exist for all n?

Research Problems from Chapter 15

R1. Find the maximal merit factors of Littlewood polynomials for degrees up to 100.

R2. Prove that the merit factor of Littlewood polynomials is bounded above independently of the degree.

R3. Prove the conjecture of Konyagin [1997]: for any *fixed* set $E \subset \partial D$ (the boundary of the unit disk) of positive measure there exists a constant $c(E) > 0$ (depending only on E) such that for any distinct positive integers k_j and any integer n,

$$\int_E \left|\sum_{j=0}^{n} z^{k_j}\right| |dz| \ge c(E).$$

R4. What is the minimum number of zeros of modulus 1 of a real-valued Littlewood polynomial of degree n?

Littlewood [1966, problem 22] poses the following research problem, which appears to still be open: "If the n_m are integral and all different, what is the lower bound on the number of real zeros of $\sum_{m=1}^{N} \cos(n_m\theta)$? Possibly $N-1$, or not much less."

R5. Erdős's Problem in L_∞ for Reciprocal Polynomials. *Show that there exists a positive constant c such that for all sufficiently large n and all reciprocal polynomials $p_n \in \mathcal{L}_n$ we have $\|p_n\|_\infty \ge (\sqrt{2}+c)\sqrt{n+1}$.*

Research Problems from Chapter 16

R1. Let $q \in (1,2)$. Show that $l(q) > 0$ if and only if q is a Pisot number.

R2. Find an algorithm that computes $L(q)$.

References

1. M. Ajtai, *The shortest vector problem in L_2 is NP-hard for randomized reductions*, Electronic Colloquium on Computational Complexity (ECCC) **47** (1997).

2. F. Amoroso, *Sur le diamètre transfini entier d'un intervalle réel*, Ann. Inst. Fourier (Grenoble) **40** (1990), 885–911.

3. T. Andres and R. Stanton, *Golay sequences*, Combinatorial mathematics, V (Proc. Fifth Austral. Conf., Roy. Melbourne Inst. Tech., Melbourne, 1976), Lecture Notes in Math., Vol. 622, Springer, Berlin (1977), 44–54.

4. G.E. Andrews, *On a conjecture of Peter Borwein*, J. Symbolic Comput. **20** (1995), 487–501.

5. N. Ankeny and T. Rivlin, *On a theorem of S. Bernstein*, Pacific J. Math. **5** (1955), 849–852.

6. E. Aparicio, *Methods for the approximate calculation of minimum uniform Diophantine deviation from zero on a segment*, Rev. Mat. Hisp.-Amer. **38** (1978), 259–270.

7. E. Aparicio, *New bounds on the minimal Diophantine deviation from zero on* $[0,1]$ *and* $[0,1/4]$, Actus Sextas Jour. Mat. Hisp.-Lusitanas (1979), 289–291.

8. E. Aparicio, *On some systems of algebraic integers of D.S. Gorshkov and their application in calculus*, Rev. Mat. Hisp.-Amer. **41** (1981), 3–17.

9. E. Aparicio, *On some results in the problem of Diophantine approximation of functions by polynomials*, Proc. Steklov Inst. Math. **163** (1985), 7–10.

10. T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York–Heidelberg, 1976.

11. F.A. Atkinson, *On a problem of Erdős and Szekeres*, Canad. Math. Bull. **4** (1961), 7–12.

12. D.H. Bailey and D.J. Broadhurst, *Parallel integer relation detection: techniques and applications*, Math. Comp. **70** (2001), 1719–1736.

13. D.H. Bailey and H.R.P. Ferguson, *Numerical results on relations between fundamental constants using a new algorithm*, Math. Comp. **53** (1989), 649–656.

14. D.H. Bailey and S. Plouffe, *Recognizing numerical constants*, Proceedings of the Workshop on Organic Mathematics, Canadian Mathematical Society **20** (1997), 73–88.

15. R.C. Baker and H.L. Montgomery, *Oscillations of quadratic L-functions*, in *Analytic Number Theory* (ed. B.C. Berndt et al.), Birkhäuser Boston, Boston, MA (1990), 23–40.

16. F. Beaucoup, P. Borwein, D. Boyd, and C. Pinner, *Multiple roots of* $[-1,1]$ *power series*, J. London Math. Soc. (2) **57** (1998), 135–147.

17. F. Beaucoup, P. Borwein, D. Boyd, and C. Pinner, *Power series with restricted coefficients and a root on a given ray*, Math. Comp. **67** (1998), 715–736.

18. B. Beauzamy, E. Bombieri, P. Enflo, and H.L. Montgomery, *Products of polynomials in many variables*, J. Number Theory **36** (1990), 219–245.

19. J. Beck, *The modulus of polynomials with zeros on the unit circle: a problem of Erdős*, Ann. of Math. (2) **134** (1991a), 609–651.

20. J. Beck, *Flat polynomials on the unit circle—note on a problem of Littlewood*, Bull. London Math. Soc. **23** (1991b), 269–277.

21. G. Beenker, T. Claasen, and P. Hermes, *Binary sequences with a maximally flat amplitude sequence*, Philips J. Res. **40** (1985), 289–304.

22. J. Bell, P. Borwein, and B. Richmond, *Growth of the product* $\prod_{j=1}^{n}(1-x^{a_j})$, Acta Arith. **86** (1998), 115–130.

23. E. Beller and D.J. Newman, *The minimum modulus of polynomials*, Proc. Amer. Math. Soc. **45** (1974), 463–465.

24. A.S. Belov and S.V. Konyagin, *An estimate for the free term of a nonnegative trigonometric polynomial with integral coefficients*, Mat. Zametki **59** (1996), 627–629.

25. G. Benke, *On the minimum modulus of trigonometric polynomials*, Proc. Amer. Math. Soc. **114** (1992), 757–761.

26. M.-J. Bertin et al., *Pisot and Salem numbers*, Birkhäuser, Basel, 1992.

27. A.T. Bharucha-Reid and M. Sambandham, *Random Polynomials*, Academic Press, Orlando, FL, 1986.

28. A. Bloch and G. Pólya, *On the roots of certain algebraic equations*, Proc. London Math. Soc. **33** (1932), 102–114.

29. A.M. Boehmer, *Binary pulse compression codes*, IEEE Trans. Inform. Theory **13** (1967), 156–167.

30. E. Bombieri and J. Vaaler, *Polynomials with low height and prescribed vanishing*, in *Analytic Number Theory and Diophantine Problems* (ed. A.C. Adolphson et al.), Birkhäuser Boston, Boston, MA (1987), 53–73.

31. F.F. Bonsall and M. Marden, *Zeros of self-inversive polynomials*, Proc. Amer. Math. Soc. **3** (1952), 471–475.

32. P. Borwein, *Some restricted partition functions*, J. Number Theory **45** (1993), 228–240.

33. P. Borwein, *Some old problems on polynomials with integer coefficients*, in *Approximation Theory IX* (ed. C. Chui and L. Schumaker), Vanderbilt University Press, Nashville, TN (1998), 31–50.

34. P. Borwein and S. Choi, *On cyclotomic polynomials with* ± 1 *coefficients*, Experiment. Math. **8** (1999), 399–407.

35. P. Borwein and S. Choi, *Merit factors of polynomials formed by Jacobi symbols*, Canad. J. Math. **53** (2001), 33–50.

36. P. Borwein and S. Choi, *Explicit merit factor formulae for Fekete and Turyn polynomials*, Trans. Amer. Math. Soc. **354** (2002), 219–234.

37. P. Borwein and S. Choi, *The average norm of polynomials of fixed height* (to appear).

38. P. Borwein, S. Choi, and S. Yazdani, *An extremal property of Fekete polynomials*, Proc. Amer. Math. Soc. **129** (2001), 19–27.

39. P. Borwein and T. Erdélyi, *Polynomials and Polynomial Inequalities*, Springer-Verlag, New York, 1995.

40. P. Borwein and T. Erdélyi, *The integer Chebyshev problem*, Math. Comp. **65** (1996a), 661–681.

41. P. Borwein and T. Erdélyi, *Questions about polynomials with* $\{0, -1, +1\}$ *coefficients*, Constructive Approx. **12** (1996b), 439–442.

42. P. Borwein and T. Erdélyi, *On the zeros of polynomials with restricted coefficients*, Illinois J. Math. **41** (1997a), 667–675.

43. P. Borwein and T. Erdélyi, *Littlewood-type problems on subarcs of the unit circle*, Indiana Univ. Math. J. **46** (1997b), 1323–1346.

44. P. Borwein and T. Erdélyi, *Markov–Bernstein-type inequalities for polynomials with restricted coefficients*, manuscript.

45. P. Borwein and T. Erdélyi, *Lower bounds for the merit factors of trigonometric polynomials from Littlewood classes* (to appear).

46. P. Borwein, T. Erdélyi, and G. Kós, *Littlewood-type problems on* $[0, 1]$, Proc. London Math. Soc. (3) **79** (1999), 22–46.

47. P. Borwein and R. Ferguson, *A complete description of Golay pairs for lengths up to* 100 (to appear).

48. P. Borwein and K.G. Hare, *Some computations on the spectra of Pisot and Salem numbers*, Math. Comp. (to appear).

49. P. Borwein and K.G. Hare, *General forms for minimal spectral values for a class of quadratic Pisot numbers*, J. London Math. Soc. (to appear).

50. P. Borwein and K.G. Hare, *Non-trivial quadratic approximations to zero of a family of cubic Pisot numbers* (to appear).

51. P. Borwein and C. Ingalls, *The Prouhet–Tarry–Escott problem revisited*, Enseign. Math. (2) **40** (1994), 3–27.

52. P. Borwein, P. Lisoněk, and C. Percival, *Computational investigations of the Prouhet–Tarry–Escott problem* (to appear).

53. P. Borwein and R. Lockhart, *The expected* L_p *norm of random polynomials*, Proc. Amer. Math. Soc. **129** (2001), 1463–1472.

54. P. Borwein and M. Mossinghoff, *Polynomials with height* 1 *and prescribed vanishing at* 1, Experiment. Math. **9** (2000a), 425–433.

55. P. Borwein and M. Mossinghoff, *Rudin–Shapiro-like polynomials in* L_4, Math. Comp. **69** (2000b), 1157–1166.

56. P. Borwein and M. Mossinghoff, *Newman polynomials with prescribed vanishing and integer sets with distinct subset sums*, Math. Comp. (to appear).

57. P. Borwein and C. Pinner, *Polynomials with* $\{0, +1, -1\}$ *coefficients and a root close to a given point*, Canad. J. Math. **49** (1997), 887–915.

58. P. Borwein, C. Pinner, and I. Pritsker, *The monic integer Chebyshev problem*, Math. Comp. (to appear).

59. J. Bourgain, *Sur le minimum d'une somme de cosinus*, Acta Arith. **45** (1986), 381–389.

60. D. Boyd, *Variations on a theme of Kronecker*, Canad. Math. Bull. **21** (1978a), 129–133.

61. D. Boyd, *Pisot and Salem numbers in intervals of the real line*, Math. Comp. **32** (1978b), 1244–1260.

62. D. Boyd, *Speculations concerning the range of Mahler's measure*, Canad. Math. Bull. **24** (1981), 453–469.

63. D. Boyd, *The maximal modulus of an algebraic integer*, Math. Comp. **45** (1985), 243–249.

64. D. Boyd, *Two sharp inequalities for the norm of a factor of a polynomial*, Mathematika **39** (1992), 341–349.

65. D. Boyd, *On beta expansions for Pisot numbers*, Math. Comp. **65** (1996), 841–860.

66. D. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comp. **66** (1997), 1697–1703.

67. D. Boyd, *Mahler's measure and special values of L-functions*, Experiment. Math. **7** (1998), 37–82.

68. J. Brillhart, M. Filaseta, and A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Canad. J. Math. **33** (1981), 1055–1059.

69. J. Brillhart, J.S. Lomont, and P. Morton, *Cyclotomic properties of the Rudin–Shapiro polynomials*, J. Reine Angew. Math. **288** (1976), 37–65.

70. N.G. de Bruijn, *On Mahler's partition problem*, Indagationes Math. **10** (1948), 210-220.

71. Y. Bugeaud, *On a property of Pisot numbers and related questions*, Acta Math. Hungar. **73** (1996), 33–39.

72. J.S. Byrnes and D.J. Newman, *Null steering employing polynomials with restricted coefficients*, IEEE Trans. Antennas & Propagation **36** (1988), 301–303.

73. F.W. Carroll, D. Eustice, and T. Figiel, *The minimum modulus of polynomials with coefficients of modulus one*, J. London Math. Soc. (2) **16** (1977), 76–82.

74. J. Chernick, *Ideal solutions of the Tarry–Escott problem*, Amer. Math. Monthly **44** (1937), 627-633.

75. G. Chudnovsky, *Number theoretic applications of polynomials with rational coefficients defined by extremality conditions*, in *Arithmetic and Geometry, Vol. I* (ed. M. Artin and J. Tate), Progress in Math., Vol. 35, Birkhäuser Boston, Boston, MA (1983), 61–105.

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

77. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.

78. P.J. Cohen, *On a conjecture of Littlewood and idempotent measures*, Amer. J. Math. **82** (1960), 191–212.

79. B. Conrey, A. Granville, B. Poonen, and K. Soundararajan, *Zeros of Fekete polynomials*, Ann. Inst. Fourier (Grenoble) **50** (2000), 865–889.

80. J.A. Davis and J. Jedwab, *Peak-to-mean power control in OFDM, Golay complementary sequences and Reed–Muller codes*, IEEE Trans. Inform. Theory **45** (1999), 2397–2417.

81. L.E. Dickson, *History of the Theory of Numbers*, Chelsea Publishing Co., New York, 1952.

82. D. Djoković, *Equivalence classes and representatives of Golay sequences*, Discrete Math. **189** (1998), 79–93.

83. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.

84. E. Dobrowolski, *Mahler's measure of a polynomial in function of the number of its coefficients*, Canad. Math. Bull. **34** (1991), 186–195.

85. H.L. Dorwart and O.E. Brown, *The Tarry–Escott problem*, Amer. Math. Monthly **44** (1937), 613-626.

86. S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combin. Theory Ser. A **55** (1990), 49–59.

87. T. Erdélyi, *The resolution of Saffari's phase problem*, C. R. Acad. Sci. Paris Sér. I Math. **331** (2000), 803–808.

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

89. T. Erdélyi, *How far is an ultraflat sequence of unimodular polynomials from being conjugate-reciprocal?*, Michigan Math. J. **49** (2001b), 259–264.

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

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

92. P. Erdős, *Some old and new problems in approximation theory: research problems 95-1*, Constr. Approx. **11** (1995), 419–421.

93. P. Erdős, I. Joó, and V. Komornik, *Characterization of the unique expansions* $1 = \sum_{i=1}^{\infty} q^{-n_i}$ *and related problems*, Bull. Soc. Math. France **118** (1990), 377–390.

94. P. Erdős, I. Joó, and V. Komornik, *On the sequence of numbers of the form* $\epsilon_0 + \epsilon_1 q + \cdots + \epsilon_n q^n,\ \epsilon_i \in \{0, 1\}$, Acta Arith. **83** (1998), 201–210.

95. P. Erdős, I. Joó, and F.J. Schnitzer, *On Pisot numbers*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **39** (1996), 95–99.

96. P. Erdős, M. Joó, and I. Joó, *On a problem of Tamás Varga*, Bull. Soc. Math. France **120** (1992), 507–521.

97. P. Erdős and V. Komornik, *Developments in non-integer bases*, Acta Math. Hungar. **79** (1998), 57–83.

98. P. Erdős and G. Szekeres, *On the product* $\prod_{k=1}^{n}(1-z^{a_k})$, Acad. Serbe Sci. Publ. Inst. Math. **13** (1959), 29–34.

99. P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Ann. of Math. (2) **51** (1950), 105–119.

100. G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer-Verlag, London, 1999.

101. M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Zeit. **17** (1923), 228–249.

102. H.R.P. Ferguson, *A short proof of the existence of vector Euclidean algorithms*, Proc. Amer. Math. Soc. **97** (1986), 8–10.

103. H.R.P. Ferguson, *A noninductive* $\mathrm{GL}(n,\mathbb{Z})$ *algorithm that constructs integral linear relations for* n $\mathbb{Z}$*-linearly dependent real numbers*, J. Algorithms **8** (1987), 131–145.

104. H.R.P. Ferguson, D.W. Bailey, and S. Arno, *Analysis of PSLQ, an integer relation finding algorithm*, Math. Comp. **68** (1999), 351–369.

105. H.R.P. Ferguson and R.W. Forcade, *Generalization of the Euclidean algorithm for real numbers to all dimensions higher than two*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), 912–914.

106. L.O. Ferguson, *Approximation by Polynomials with Integral Coefficients*, Amer. Math. Soc., Providence, RI, 1980.

107. G.T. Fielding, *The expected value of the integral around the unit circle of a certain class of polynomials*, Bull. London Math. Soc. **2** (1970), 301–306.

108. V. Flammang, G. Rhin, and C.J. Smyth, *The integer transfinite diameter of intervals and totally real algebraic integers*, J. Théor. Nombres Bordeaux **9** (1997), 137–168.

109. C. Frappier, Q.I. Rahman, and St. Ruscheweyh, *New inequalities for polynomials*, Trans. Amer. Math. Soc. **288** (1985), 69–99.

110. W.H.J. Fuchs and E.M. Wright, *The 'easier' Waring problem*, Quart. J. Math. Oxford Ser. **10** (1939), 190–209.

111. E. Ghate and E. Hironaka, *The arithmetic and geometry of Salem numbers*, Bull. Amer. Math. Soc. (N.S.) **38** (2001), 293–314.

112. A. Gloden, *Mehrgradige Gleichungen*, P. Noordhoff, Groningen, 1944.

113. M.J. Golay, *Multislit spectrometry*, J. Opt. Soc. America **39** (1949), 437–444.

114. M.J. Golay, *Static multislit spectrometry and its application to the panoramic display of infrared spectra*, J. Opt. Soc. America **41** (1951), 468–472.

115. M.J. Golay, *Complementary series*, IRE Trans. **IT-7** (1961), 82–87.

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

117. M.J. Golay, *The merit factor of long low autocorrelation binary sequences*, IEEE Trans. Inform. Theory **28** (1982), 543–549.

118. M.J. Golay, *The merit factor of Legendre sequences*, IEEE Trans. Inform. Theory **29** (1983), 934–936.

119. M.J. Golay and D.B. Harris, *A new search for skewsymmetric binary sequences with optimal merit factors*, IEEE Trans. Inform. Theory **36** (1990), 1163–1167.

120. M. von Golitschek and G.G. Lorentz, *Bernstein inequalities in L_p*, $0 \le p \le +\infty$. Constructive Function Theory—86 Conference (Edmonton, AB, 1986). Rocky Mountain J. Math. **19** (1989) 145–156.

121. N.K. Govil, *On the derivative of a polynomial,* Proc. Amer. Math. Soc. **41** (1973), 543–546.

122. W.T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), 529–551.

123. R. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York–Berlin, 1981.

124. L. Habsieger and B. Salvy, *On integer Chebyshev polynomials*, Math. Comp. **66** (1997), 763–770.

125. J. Håstad, B. Just, J.C. Lagarias, and C.-P. Schnorr, *Polynomial time algorithms for finding integer relations among real numbers*, SIAM J. Comput. **18** (1989), 859–881.

126. D. Hilbert, *Ein Beitrag zur Theorie des Legendreschen Polynoms*, Acta Math. **18** (1894), 155–159.

127. T. Høholdt and H. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Trans. Inform. Theory **34** (1988), 161–164.

128. L.K. Hua, *Introduction to Number Theory*, Springer-Verlag, New York–Berlin, 1982.

129. T.W. Hungerford, *Algebra*, GTM **73**, Springer-Verlag, New York–Berlin, 1980.

130. J. Jensen, H. Jensen, and T. Høholdt, *The merit factor of binary sequences related to difference sets*, IEEE Trans. Inform. Theory **37** (1991), 617–626.

131. I. Joó, *On the distribution of the set* $\{\sum_{i=1}^{n} \epsilon_i q^i : \ \epsilon_i \in \{0,1\}, \ n \in \mathbf{N}\}$, Acta Math. Hungar. **58** (1991), 199–202.

132. I. Joó and F.J. Schnitzer, *On some problems concerning expansions by non-integer bases*, Anz. Österreich. Akad. Wiss. Math.-Natur. Kl. **133** (1996), 3–10.

133. M. Kac, *On the average number of real roots of a random algebraic equation. II*, Proc. London Math. Soc. (2) **50** (1949), 390–408.

134. J.-P. Kahane, *Sur les polynômes à coefficients unimodulaires*, Bull. London Math. Soc. **12** (1980), 321–342.

135. J.-P. Kahane, *Some Random Series of Functions*, Cambridge Studies in Advanced Mathematics, Cambridge, 1985.

136. B. Kashin, *Algebraic polynomials with integer coefficients that deviate little from zero on an interval*, Mat. Zametki **50** (1991), 58–67.

137. H. Kleiman, *A note on the Tarry–Escott problem*, J. Reine Angew. Math. **278/279** (1975), 48–51.

138. I. Klemeš, *Finite Toeplitz matrices and sharp Littlewood conjectures*, Algebra i Analiz **13** (2001), 39–59.

139. D.E. Knuth, *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1981.

140. M. Kolountzakis, *Probabilistic and constructive methods in harmonic analysis and additive number theory*, PhD thesis, Stanford University, 1994.

141. V. Komornik, P. Loreti, and M. Pedicini, *An approximation property of Pisot numbers*, J. Number Theory **80** (2000), 218–237.

142. S. Konyagin, *On the Littlewood problem*, Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), 243–265.

143. S. Konyagin, *On a question of Pichorides*, C. R. Acad. Sci. Paris Sér. I Math. **324** (1997), 385–388.

144. T.W. Körner, *On a polynomial of Byrnes*, Bull. London Math. Soc. **12** (1980), 219–224.

145. K.-S. Lau, *Dimension of a family of singular Bernoulli convolutions*, J. Funct. Anal. **116** (1993), 335–358.

146. P. Lax, *Proof of a conjecture of P. Erdős on the derivative of a polynomial*, Bull. Amer. Math. Soc. **50** (1944), 509–513.

147. D.H. Lehmer, *Factorizations of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.

148. A.K. Lenstra, H.W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

149. R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

150. J.E. Littlewood, *On the mean values of certain trigonometric polynomials*, J. London Math. Soc. **36** (1961), 307–334.

151. J.E. Littlewood, *On polynomials* $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$, J. London Math. Soc. **41** (1966), 367–376.

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

153. J.E. Littlewood and A.C. Offord, *On the number of real roots of a random algebraic equation, II*, Proc. Cam. Phil. Soc. **35** (1939), 133–148.

154. R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), 707–708.

155. K. Mahler, *On two extremum properties of polynomials*, Illinois J. Math. **7** (1963), 681–701.

156. H. Maier, *The size of the coefficients of cyclotomic polynomials*, in *Analytic number theory Vol. 2 (Allerton Park, IL, 1995)* (ed. B.C. Berndt et al.), Progr. Math., 139, Birkhäuser Boston, Boston, MA (1996), 633–639.

157. M. Malik, *On the derivative of a polynomial*, J. London Math. Soc. (2) **1** (1969), 57–60.

158. R. Maltby, *Pure product polynomials of small norm*, PhD thesis, Simon Fraser University, 1996.

159. R. Maltby, *Pure product polynomials and the Prouhet–Tarry–Escott problem,* Math. Comp. **66** (1997), 1323–1340.

160. O.C. McGehee, L. Pigno, and B. Smith, *Hardy's inequality and the L^1 norm of exponential sums*, Ann. of Math. (2) **113** (1981), 613–618.

161. A. Meichsner, *Integer relation algorithms and the recognition of numerical constants*, M.Sc. thesis, Simon Fraser University, 2001.

162. Z.A. Melzak, *A note on the Tarry–Escott problem*, Canad. Math. Bull. **4** (1961), 233–237.

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

164. M. Mignotte, *Mathematics for Computer Algebra*, Springer-Verlag, New York, 1992.

165. M. Mignotte and D. Ştefănescu, *Polynomials. An Algorithmic Approach*, Springer-Verlag Singapore, Singapore, 1999.

166. G.V. Milovanović, D.S. Mitrinović, and Th.M. Rassias, *Topics in Polynomials: Extremal Problems, Inequalities, Zeros*, World Scientific Publishing, River Edge, NJ, 1994.

167. H.L. Montgomery, *An exponential polynomial formed with the Legendre symbol*, Acta Arith. **37** (1980), 375–380.

168. H.L. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, CBMS, Vol. 84, Amer. Math. Soc., Providence, RI, 1994.

169. M. Mossinghoff, C. Pinner, and J. Vaaler, *Perturbing polynomials with all their roots on the unit circle*, Math. Comp. **67** (1998), 1707–1726.

170. M. Nazarathy, S.A. Newton, R.P. Giffard, D.S. Moberly, F. Sischka, W.R. Trutna Jr., and S. Foster, *Real-time long range complementary correlation optical time domain reflectometer*, IEEE J. Lightwave Technology **7** (1989), 24–38.

171. D.J. Newman, *An L^1 extremal problem for polynomials*, Proc. Amer. Math. Soc. **16** (1965), 1287–1290.

172. D.J. Newman and J.S. Byrnes, *The L^4 norm of a polynomial with coefficients* ± 1, Amer. Math. Monthly **97** (1990), 42–45.

173. D.J. Newman and A. Giroux, *Properties on the unit circle of polynomials with unimodular coefficients*, in *Recent Advances in Fourier Analysis and its Applications* (ed. J.S. Byrnes and J.L. Byrnes), Kluwer (1990), 79–81.

174. A. Odlyzko, *Minima of cosine sums and maxima of polynomials on the unit circle*, J. London Math. Soc. (2) **26** (1982), 412–420.

175. A. Odlyzko and B. Poonen, *Zeros of polynomials with* $0, 1$ *coefficients*, Enseign. Math. (2) **39** (1993), 317–348.

176. Y. Peres and B. Solomyak, *Approximation by polynomials with coefficients* ± 1, J. Number Theory **84** (2000), 185–198.

177. G. Pólya and G. Szegő, *Problems and Theorems in Analysis, Volume I*, Springer-Verlag, New York–Berlin, 1972.

178. Ch. Pommerenke, *Univalent Functions*, Vandenhoeck & Ruprecht, Göttingen, 1975.

179. Ch. Pommerenke, *Boundary Behaviour of Conformal Maps*, Springer-Verlag, Berlin, 1992.

180. A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, 1601, Springer-Verlag, Berlin, 1995.

181. I. Pritsker, *Small polynomials with integer coefficients*, preprint.

182. H. Queffélec and B. Saffari, *On Bernstein's inequality and Kahane's ultraflat polynomials*, J. Fourier Anal. Appl. **2** (1996), 519–582.

183. E. Rees and C.J. Smyth, *On the constant in the Tarry–Escott problem*, in *Cinquante Ans de Polynômes*, Springer-Verlag, Berlin, 1990.

184. A. Reinholz, *Ein paralleler genetische Algorithmus zur Optimierung der binären Autokorrelations-Funktion*, Diplomarbeit, Rheinische Friedrich-Wilhelms-Universität Bonn, 1993.

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

186. W. Rudin, *Real and Complex Analysis*, third edition, McGraw-Hill, New York, 1987.

187. B. Saffari, *Polynômes réciproques: conjecture d'Erdős en norme L^4, taille des autocorrélations et inexistence des codes de Barker*, C. R. Acad. Sci. Paris Sér. I Math **308** (1989), 461–464.

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

189. R. Salem, *Algebraic Numbers and Fourier Analysis*, D.C. Heath and Co., Boston, MA, 1963.

190. R. Salem and A. Zygmund, *Some properties of trigonometric series whose terms have random signs*, Acta Math. **91** (1954), 254–301.

191. A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399.

192. A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge University Press, Cambridge, 2000.

193. A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Michigan Math. J. **12** (1965), 81–85.

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

195. E. Schmidt, *Über algebraische Gleichungen vom Pólya–Bloch-Typos*, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1932), 321.

196. I. Schur, *Untersuchungen über algebraische Gleichungen*, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 403–428.

197. H. Shapiro, *Extremal problems for polynomials and power series*, M.Sc. thesis, MIT, 1951.

198. C.L. Siegel, *The trace of totally positive and real algebraic integers*, Ann. of Math. **46** (1945), 302–312.

199. T.N. Sinha, *On the Tarry–Escott problem*, Amer. Math. Monthly **73** (1966), 280–285.

200. C.J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175.

201. C.J. Smyth, *The mean values of totally real algebraic integers*, Math. Comp. **42** (1984a), 663–681.

202. C.J. Smyth, *Totally positive algebraic integers of small trace*, Ann. Inst. Fourier (Grenoble) **34** (1984b), 1–28.

203. C.J. Smyth, *Ideal 9th-order multigrades and Letac's elliptic curve*, Math. Comp. **57** (1991), 817–823.

204. C.J. Smyth, *An inequality for polynomials*, in *Number theory (Ottawa, ON, 1996)* (ed. R. Gupta and K.S. Williams), CRM Proceedings & Lecture Notes, 19, American Mathematical Society, Providence, RI (1999), 315–321.

205. C.J. Smyth, *Cyclotomic factors of reciprocal polynomials and totally positive algebraic integers of small trace*, Edinburgh University Maths. Dept. preprint MS-96-024.

206. B. Solomyak, *On the random series $\sum \pm\lambda^n$ (an Erdős problem)*, Ann. of Math. (2) **142** (1995), 611–625.

207. C. Sudler, *An estimate for a restricted partition function*, Quart. J. Math. Oxford Ser. (2) **15** (1964), 1–10.

208. G. Szegő, *Bemerkungen zu einem Satz von E. Schmidt uber algebraische Gleichungen*, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1934), 86–98.

209. R.M. Trigub, *Approximation of functions with Diophantine conditions by polynomials with integral coefficients*, in *Metric Questions of the Theory of Functions and Mappings*, No. 2, Naukova Dumka, Kiev (1971), 267–333. (Russian)

210. C.-C. Tseng, *Signal multiplexing in surface-wave delay lines using orthogonal pairs of Golay's complementary sequences*, IEEE Trans. Sonics Ultrasonics **SU-18** (1971), 103–107.

211. M. Tsuji, *Potential Theory in Modern Function Theory*, Chelsea Publishing Co., New York, 1975.

212. P. Turán, *On a New Method of Analysis and its Applications*, John Wiley & Sons, New York, 1984.

213. R.J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.

214. R.J. Turyn, *Hadamard matrices, Baumert–Hall units, four-symbol sequences, pulse compression, and surface wave encodings*, J. Combinatorial Theory Ser. A **16** (1974), 313–333.

215. R.J. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.

216. B. Vallée, *Une approche géométrique des algorithmes de réduction en petite dimension*, PhD thesis, University of Caen, 1986.

217. R.C. Vaughan and T.D. Wooley, *Further improvements in Waring's problem*, Acta Math. **174** (1995), 147–240.

218. R.C. Vaughan and T.D. Wooley, *A special case of Vinogradov's mean value theorem*, Acta Arith. **79** (1997), 193–204.

219. P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. **74** (1996), 81–95.

220. E.M. Wright, *An easier Waring's problem*, J. London Math. Soc. **9** (1934), 267–272.

221. E.M. Wright, *On Tarry's Problem (I)*, Quart. J. Math. **6** (1935), 261–267.

222. E.M. Wright, *Prouhet's 1851 solution of the Tarry–Escott problem of 1910*, Amer. Math. Monthly **66** (1959), 199–201.

223. E.M. Wright, *The Tarry–Escott and the "easier" Waring problems*, J. Reine Angew. Math. **311/312** (1979), 170–173.

Index