Part 0

This is 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.

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.

Chapter 1

Introduction

Notation

Let

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

and let $\mathcal{Z}$ denote the union over n of all such polynomials.

Let

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

and let $\mathcal{F}$ denote the set of all height 1 polynomials.

Let

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

and denote the set of all such polynomials by $\mathcal{L}$.

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

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

For $p(z) := a_n z^n + \cdots + a_1 z + a_0$

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

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

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

This latter quantity is called the *Mahler measure*.

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

and

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

Some Results from Real and Complex Analysis

For $0 \le \alpha \le \beta$,

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

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

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

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

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

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 $a_1,a_2,\ldots,a_m$, 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].

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 $m \neq 0$,

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

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*

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

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

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

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.*

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

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

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.

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.

Example 1

Consider the Prouhet–Tarry–Escott problem.

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

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

Example 2

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

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

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.

Example 3

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.

Example 4

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

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.

The cyclotomic polynomial $\Phi_n.$ 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

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

so for p a prime,

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

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 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.

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

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

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 smallest limit point of measures (as in P12) is believed to be approximately 1.255433 . . . . 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

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

***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 $G(z) = h(z)/g(z)$,

$$1 + a_k z^k + \cdots = \frac{b + b_1 z + \cdots}{c + c_1 z + \cdots},$$

$$(c + c_1 z + \cdots)(1 + a_k z^k + \cdots) = b + b_1 z + \cdots ,$$

and

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

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

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

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

Without loss of generality, assume that $|b_k| \geq |b/2|$ (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

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

and

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

so

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

But

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

□

***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 $M(p) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}$.*

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 $1 + c/n$.*

If p is a nonreciprocal monic irreducible polynomial of degree $n > 1$, then at least one root ρ satisfies

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

where $\phi = 1.3247\ldots$ is the smallest Pisot number, namely, the real root of $z^3 - z - 1$.

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 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

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].

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 $m \to \infty$,

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

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

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

and since

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

we have

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

So

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

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 $|s(\alpha_1)| \leq n+1$. 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. □

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

P4. Littlewood's Problem in L_∞. *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 $|z| = 1$.

The Rudin–Shapiro polynomials are defined by

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

and

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

These have 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 for all z of modulus 1

$$\begin{aligned} |P_n(z)| &\le \sqrt{2^{n+1}} = \sqrt{2}\sqrt{\text{degree}(P_n) + 1} \\ |Q_n(z)| &\le \sqrt{2^{n+1}} = \sqrt{2}\sqrt{\text{degree}(Q_n) + 1} \end{aligned}$$

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*

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

Introductory Exercises

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

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

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

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

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

(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.)

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

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

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

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

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 $\chi(ab) = \chi(a)\chi(b)$.

The L_2 norm of $f_p(z)$ is $\sqrt{p-1}$.

***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

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

$$= \sum_{a,b=1}^{p-1}\left(\frac{ab}{p}\right)\sum_{j=0}^{p-1}\zeta_p^{(a+b)j} = p\sum_{\substack{a=1\\ b=p-a}}^{p-1}\left(\frac{ab}{p}\right) = p\left(\frac{-1}{p}\right)(p-1)$$

□

The choice of root in the above lemma is more subtle.

***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 $\gcd(k,p)=1$,

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

The supremum norm of $f_p(z)$ on D grows at least like $\sqrt{p}\log\log p$. (See R1.)

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

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

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 $\zeta := e^{2\pi i/N}$.

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

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 $L\big(s, (\frac{\cdot}{p})\big)$ 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.

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?

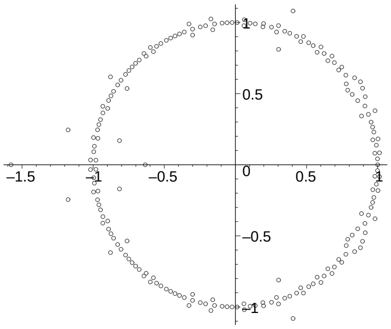
c2. Explore the zeros of the Fekete polynomials and the shifted Fekete polynomials. Formulate some reasonable conjectures.

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

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

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

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.

We now characterize the monic polynomials with measure 1 and all coefficients odd.

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 $T_p(P)$.

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

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

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 $\mathbb{Z}_p$. 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. □

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 $2N$.*

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

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

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

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.

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.*

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*

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

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.

Corollary 2. *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*

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

The following conjecture 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

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

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].

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 $\{|z| \leq 1\}$, 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. □

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.

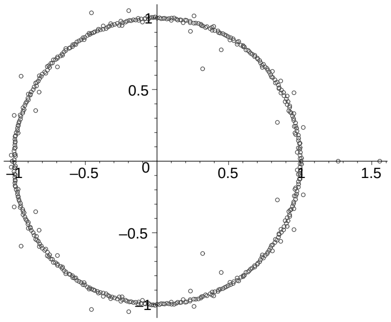
2. R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

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

Chapter 7

Location of Zeros

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



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

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

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.

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*

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

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

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

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*

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

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*

$$m \leq \left\lfloor \tfrac{16}{7}\sqrt{n} \right\rfloor + 4$$

such that

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

Proof. Let

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

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 $0 < t \leq \pi$,

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

and

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

Let

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

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

$$|q(1)| + |q(2)| + \cdots + |q(n)|$$

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

and the proof is finished. □

Proof of Theorem 5. If p has a zero at 1 of multiplicity m, then for every polynomial $q \in \mathcal{P}^c_{m-1}$, 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 $i = 0, 1, \ldots, m-1$.) Lemma 1 constructs a polynomial q of degree at most

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

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 $[-1,1]$,

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

Observe that the zeros of T_n are precisely the points

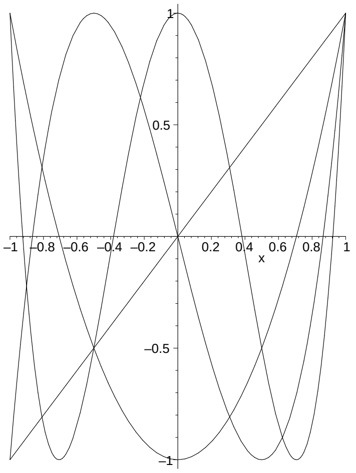
$$x_k = \cos\tfrac{(2k-1)\pi}{2n}, \quad k = 1,2,\ldots,n.$$

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

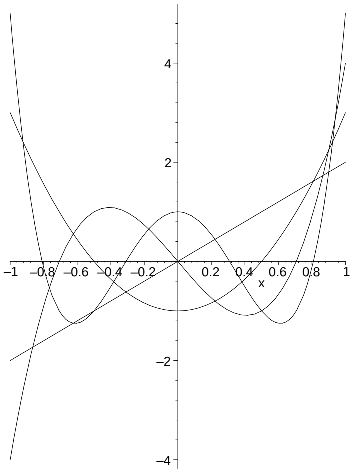
$$\min_{p \in \mathcal{P}_{n-1}^c} \|x^n - p(x)\|_{[-1,1]} = \|2^{1-n}T_n\|_{[-1,1]} = 2^{1-n},$$

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.

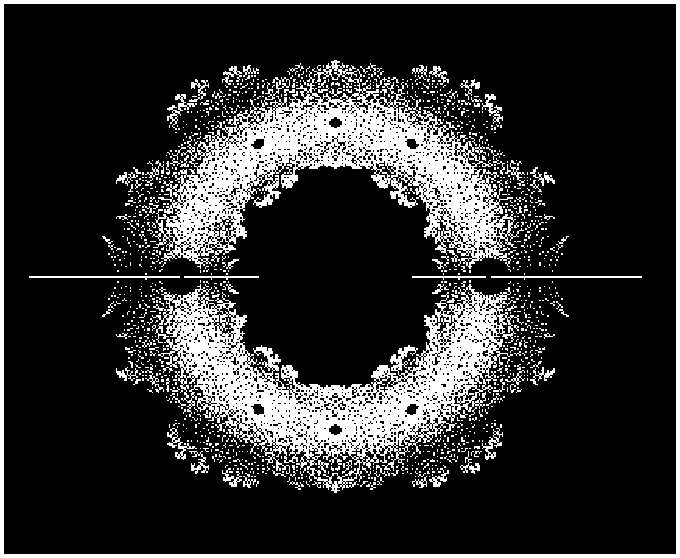
2. P. Borwein, T. Erdélyi, and G. Kós, *Littlewood-type problems on* $[0, 1]$, Proc. London Math. Soc. (3) **79** (1999), 22–46.

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

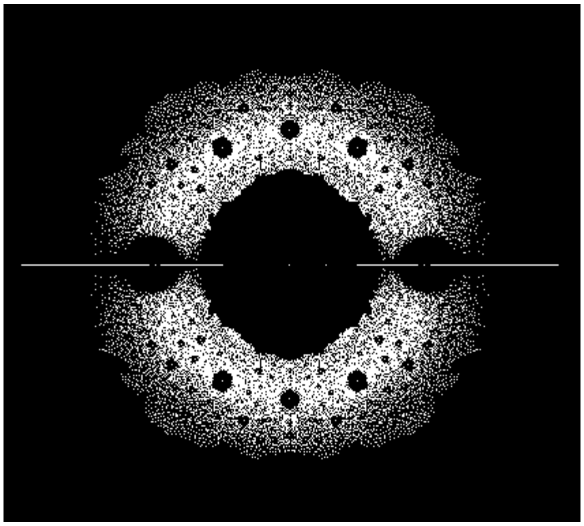
Chapter 8

Maximal Vanishing

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



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



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

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.

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 $O(\log n)$.

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 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. This is true for n up to 6 but fails for $n = 6$ and therefore fails for all higher n.

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*

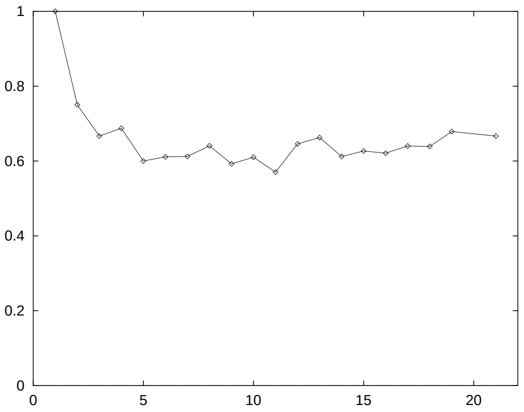
$$\frac{\log p}{p-1} > \frac{\log L(f)}{m},$$

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

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

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

All the minimal examples found factor as products of the form

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

It would be very surprising if this were always true.

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.

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.

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 $|z| = 1$.

E8. There is a question of Erdős dating from 1931 with a \$500 prize attached to it.

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 $n \leq 25$ 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 $p \in \mathcal{A}_n$?

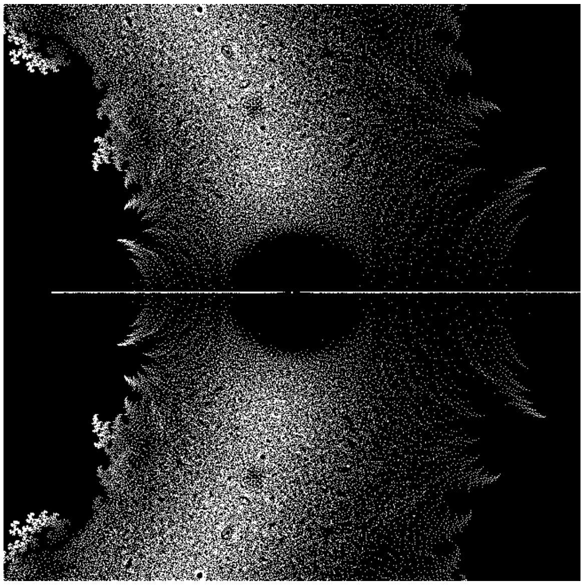
Selected References

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.



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

$$|\alpha - \beta| > \exp(-c(\alpha)N + O(\log N)),$$

if α is not a root of unity. Otherwise,

$$|\alpha - \beta| > \exp\left(-c(\alpha)\sqrt{N}\log N + O(\sqrt{N})\right),$$

if α is an nth root of unity.

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*

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

Introductory Exercises

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 $N \geq 2$ the extremal polynomials $F(z;N)$ take the form

$$\pm\frac{\left(z^{2m+1} - 2z^m + 1\right)}{(1-z)}, \qquad \text{if } N = 2m,$$

$$\pm\frac{\left(z^{2m+2} - z^{m+1} - z^m + 1\right)}{(1-z)}, \qquad \text{if } N = 2m+1.$$

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

P1. *For any interval* $[a, b]$ *find*

$$\Omega[a,b] := \lim_{n\to\infty} \Omega_n[a,b],$$

where

$$\Omega_n[a,b] := \min_{p_n \neq 0, p_n \in \mathcal{Z}_n} \|p_n(z)\|_{[a,b]}^{1/n}.$$

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 $[a, b]$.

For $b - a < 4$, Fekete [1923] showed that

$$\Omega[a,b] \leq \left(\frac{b-a}{4}\right)^{1/2}.$$

One can deduce 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

$$\Omega[0,1] \le \left(\|P_{210}\|_{[0,1]}\right)^{1/210} = \frac{1}{2.3543\ldots}.$$

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

$$u^{(n)} = \frac{q_{n-1}^2 - q_n}{2q_{n-1}^2 - q_n}.$$

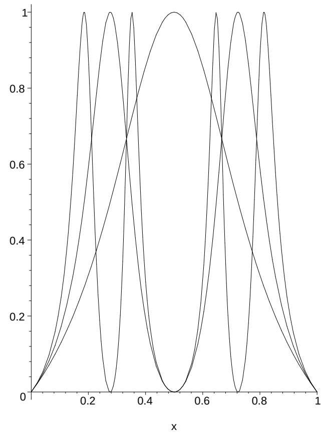
Each q_k is a polynomial of degree 2^k with simple zeros, all in $(0, 1)$, and if b_k is the leading coefficient of q_k, then

$$\lim b_k^{1/2^k} = 2.3768417062\ldots .$$

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.

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?*

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].

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.

□

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,

$$|a_{n-1}| \geq (1.744)n.$$

Introductory Exercises

E3. Monic Integer Chebyshev Polynomials. 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].

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

$$\begin{aligned}
\alpha_1 + \cdots + \alpha_n &= \beta_1 + \cdots + \beta_n \\
\alpha_1^2 + \cdots + \alpha_n^2 &= \beta_1^2 + \cdots + \beta_n^2 \\
\vdots \qquad & \vdots \qquad \vdots \\
\alpha_1^k + \cdots + \alpha_n^k &= \beta_1^k + \cdots + \beta_n^k.
\end{aligned}$$

We call n the size of the solution and k the degree.

We abbreviate the above system by writing $[\alpha_i] =_k [\beta_i]$.

The Diophantine equation above can be reformulated as a question about polynomials in two ways.

Theorem 1. *The following are equivalent:*

$$\text{(a)} \qquad \sum_{i=1}^{n} \alpha_i^j = \sum_{i=1}^{n} \beta_i^j \textit{ for } j = 1, \ldots, k-1.$$

$$\text{(b)} \qquad \deg\left(\prod_{i=1}^{n}(z-\alpha_i) - \prod_{i=1}^{n}(z-\beta_i)\right) \le n-k.$$

$$\text{(c)} \qquad (z-1)^k \,\Bigg|\, \sum_{i=1}^{n} z^{\alpha_i} - \sum_{i=1}^{n} z^{\beta_i}.$$

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:

$$\text{(a)} \qquad \sum_{i=1}^{n/2} \alpha_i^{2j} = \sum_{i=1}^{n/2} \beta_i^{2j} \text{ for } j = 1, \ldots, \frac{n-2}{2}.$$

$$\text{(b)} \qquad \prod_{i=1}^{n/2}\left(z^2-\alpha_i^2\right) - \prod_{i=1}^{n/2}\left(z^2-\beta_i^2\right) = C \text{ for some constant } C.$$

$$\text{(c)} \qquad (1-z)^n \,\Bigg|\, \sum_{i=1}^{n/2}\left(z^{\alpha_i}+z^{-\alpha_i}\right) - \sum_{i=1}^{n/2}\left(z^{\beta_i}+z^{-\beta_i}\right).$$

Note that the third form of an even symmetric solution gives rise to a real (cosine) polynomial on the boundary of the unit disk.

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.

$$\begin{aligned}
[\pm 2] &=_1 [\pm 1],\\
[-2,-1,3] &=_2 [2,1,-3],\\
[-5,-1,2,6] &=_3 [-4,-2,4,5],\\
[-8,-7,1,5,9] &=_4 [8,7,-1,-5,-9],\\
[\pm 1,\pm 11,\pm 12] &=_5 [\pm 4,\pm 9,\pm 13],\\
[-50,-38,-13,-7,24,33,51] &=_6 [50,38,13,7,-24,-33,-51],\\
[\pm 5,\pm 14,\pm 23,\pm 24] &=_7 [\pm 2,\pm 16,\pm 21,\pm 25],\\
[-98,-82,-58,-34,13,16,69,75,99]&\\
&=_8 [98,82,58,34,-13,-16,-69,-75,-99],\\
[174,148,132,50,8,-63,-119,-161,-169]&\\
&=_8 [-174,-148,-132,-50,-8,63,119,161,169],\\
[\pm 99,\pm 100,\pm 188,\pm 301,\pm 313] &=_9 [\pm 71,\pm 131,\pm 180,\pm 307,\pm 308],\\
[\pm 103,\pm 189,\pm 366,\pm 452,\pm 515] &=_9 [\pm 18,\pm 245,\pm 331,\pm 471,\pm 508],\\
[\pm 151,\pm 140,\pm 127,\pm 86,\pm 61,\pm 22] &=_{11} [\pm 148,\pm 146,\pm 121,\pm 94,\pm 47,\pm 35].
\end{aligned}$$

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:

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.

$$\begin{aligned} F_7 := {} & (t-R_1)(t-R_2)(t-R_3)(t-R_4)(t-R_5)(t-R_6)(t-R_7) \\ & -(t+R_1)(t+R_2)(t+R_3)(t+R_4)(t+R_5)(t+R_6)(t+R_7), \end{aligned}$$

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,

$$\begin{aligned} F_7 = {} & 2j^3k^3(-k+2j)(j-2k)(j+k) \\ & \times\left(j^2+kj-k^2\right)\left(j^2-kj-k^2\right)\left(j^2-3kj+k^2\right) \\ & \times\left(-3j^2k+k^3+j^3\right)\left(j^4-4kj^3+5j^2k^2-k^4\right) \\ & \times\left(j^2-kj+k^2\right)(j-k)^3, \end{aligned}$$

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.

$$\begin{aligned} &[-98, -82, -58, -34, 13, 16, 69, 75, 99] \\ &\quad =_8 [98, 82, 58, 34, -13, -16, -69, -75, -99] \end{aligned}$$

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.

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.

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

$$m^2 n^2 - 13n^2 + 121 - 13m^2.$$

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.

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

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

$$\prod_{i=1}^{n}(z^2 - \alpha_i^2) - \prod_{i=1}^{n}(z^2 - \beta_i^2) = C,$$

$$\prod_{i=1}^{n}(\beta_j^2 - \alpha_i^2) - 0 = C \text{ for } j = 1, \ldots, n,$$

and so

$$\frac{1}{C} \prod_{i=n-k+2}^{n} \left(\beta_j^2 - \alpha_i^2\right) = \prod_{i=1}^{n-k+1} \left(\beta_j^2 - \alpha_i^2\right)^{-1} \text{ for } j = 1, \ldots, k,$$

which gives us k evaluations of the unique degree $k-1$ polynomial with leading coefficient $1/C$ and roots

$$\alpha_{n-k+2}, \ldots, \alpha_n.$$

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 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.

Introductory Exercises

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 $\alpha_i \neq \beta_j$ 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.

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

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 $v(k)$.

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 $O(k)$).

$N(k)$ is 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 $N(k) = k + 1$.

$N^*(k)$ 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 $k + 1$.

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

$$s \le s_j(\mathbf{a}) \le sn^j,$$

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. □

Hua [1982] shows that

$$N^*(k) \le (k+1)\left(\frac{\log \frac{1}{2}(k+2)}{\log(1+\frac{1}{k})} + 1\right) \sim k^2 \log k.$$

The connection to the easier Waring problem.

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

$$D = \sum_{i=1}^{n} \alpha_i^k - \sum_{i=1}^{n} \beta_i^k.$$

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

$$\Delta(k) \le v(k) \le 2n + \Delta(k, C) \le 2n + \Delta(k).$$

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,*

$$\Delta(k) \le 2k.$$

(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*

$$\Delta(k) = (p^{n+1} - 1)/2 \ge k + 1.$$

(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

$$\begin{gathered}(z+8)^7 + (z-8)^7 + (z+5)^7 + (z-5)^7 + (z-3)^7 \\ + (z+3)^7 - 2z^7 - 2(z-7)^7 - 2(z+7)^7 = 604800z\end{gathered}$$

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.

An ideal solution of the Prouhet–Tarry–Escott problem arises when $E_N^* = 2N$ (as in Theorem 1(c) of Chapter 11).

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

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

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 $N \in \{1, 2, 3, 4, 5, 6, 8\}$ this provides an ideal solution of the Prouhet–Tarry–Escott problem.

R.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.

The best subexponential upper bounds are

$$\log(E_N^*) \ll \log^4(N)$$

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,

$$\left\| \prod_{i=1}^{N} \left(1 - z^{\beta_i}\right) \right\|_\infty \leq (2N)^{\sqrt{N/8}}.$$

Lemma 1. *Let $1 \leq \beta_1 < \beta_2 < \cdots$ and let*

$$V_n(z) := \prod_{1 \leq i < j \leq n} \left(1 - z^{\beta_j - \beta_i}\right).$$

Then

$$\|V_n(z)\|_\infty \leq n^{n/2}.$$

Proof. We can explicitly evaluate the Vandermonde determinant

$$D_n := \prod_{1 \leq i < j \leq n} \left(z^{\beta_j} - z^{\beta_i}\right) = \begin{vmatrix} 1 & z^{\beta_1} & \dots & z^{(n-1)\beta_1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z^{\beta_n} & \dots & z^{(n-1)\beta_n} \end{vmatrix}.$$

By Hadamard's inequality, since each entry of the matrix has modulus at most 1 in the unit disk,

$$\|D_n\|_\infty \leq n^{n/2}.$$

Thus

$$\left\| \prod_{1 \leq i < j \leq n} \left(1 - z^{\beta_j - \beta_i}\right) \right\|_\infty = \left\| \prod_{1 \leq i < j \leq n} \left(z^{\beta_j} - z^{\beta_i}\right) \right\|_\infty \leq n^{n/2}.$$

□

Theorem 2. *If $\gcd(p, \alpha_i) = 1$ and p is prime, then*

$$\left\| \prod_{i=1}^{N} \left(1 - z^{\alpha_i}\right) \right\|_\infty \geq p^{N/(p-1)}.$$

This is best possible for $p \in \{2, 3, 5, 7, 11, 13\}$, with extremal examples given by the partial products of

$$\prod_{\substack{n=1 \\ \gcd(p,n)=1}}^{\infty} (1 - z^n).$$

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

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

$$\left\| \prod_{i=1}^{N} (1 - z^{\alpha_i}) \right\|_\infty \geq p^{N/(p-1)}.$$

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

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

$$|c_j| \leq 1, \quad j = 1, 2, \ldots, n.$$

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) of polynomials from the class $\mathcal{L}_n$.

It is widely believed that no Barker polynomials exist of degree greater than 12.

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.

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. □

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.*

Sketch of proof 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

$$V(z) := \frac{B\left(z^{n+1}\right)\left(X(z)+Y(z)\right) + A^*\left(z^{n+1}\right)\left(X(z)-Y(z)\right)}{2}.$$

Now $1-z$ and $1+z$ are a Golay complementary pair. So are

$$1 - z - z^2 + z^3 - z^4 + z^5 - z^6 - z^7 - z^8 + z^9$$

$$1 - z - z^2 - z^3 - z^4 - z^5 - z^6 + z^7 + z^8 - z^9$$

Finally

$$\begin{gathered} -z^{25} + z^{24} - z^{23} + z^{22} + z^{21} + z^{20} - z^{19} - z^{18} + z^{17} + z^{16} + z^{15} + z^{14} - z^{13} \\ + z^{12} - z^{11} + z^{10} + z^9 + z^8 + z^7 - z^6 + z^5 + z^4 - z^3 - z^2 + z - 1 \end{gathered}$$

$$\begin{gathered} -z^{25} + z^{24} - z^{23} + z^{22} + z^{21} + z^{20} - z^{19} - z^{18} + z^{17} + z^{16} + z^{15} + z^{14} + z^{13} \\ + z^{12} + z^{11} - z^{10} - z^9 - z^8 - z^7 + z^6 - z^5 - z^4 + z^3 + z^2 - z + 1 \end{gathered}$$

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.

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.

Introductory Exercises

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.

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.

When $p < 2$ it asks how large the L_p norm can be.

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 $1 \leq \alpha < \beta \leq \infty$ and $\alpha^{-1} + \beta^{-1} = 1$, that

$$\|P\|_2^2 \leq \|P\|_\alpha \|P\|_\beta.$$

The Littlewood Problem in L_p

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.

$$p(z) := \sum_{k=0}^{n} a_k z^k$$

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

$$c_k := \sum_{j=0}^{n-k} a_j a_{j+k} \quad \text{and} \quad c_{-k} := c_k,$$

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.

The Rudin–Shapiro polynomials have merit factors that tend to 3.

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].

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 $14.0833\ldots$. 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.

Golay gives a heuristic argument based on something he calls "the ergodicity postulate" which suggests that the asymptotic limit is approximately 12.32.

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.

Other L_p Norms

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.

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 $c_2 > 1$.

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

$$|q(z)| \ge (d+1)^\alpha$$

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.

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.

Beck [1991b], proves that "flat" polynomials exist from the class of polynomials of degree n whose coefficients are 1200th roots of unity.

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.

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.

E3. Show that a reciprocal Littlewood polynomial of sufficiently large degree has at least one zero of modulus 1.

E6. Golomb Rulers. Consider polynomials of the form

$$p(z) = z^{\alpha_1} + z^{\alpha_2} + \cdots + z^{\alpha_k},$$

where $0 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_k$. Let $\mathcal{G}_k$ denote the collection of all such polynomials.

Show that $p(z) \in \mathcal{G}_k$ satisfies

$$\|p(z)\|_4 \geq \left(2k^2 - k\right)^{1/4}$$

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 $k \leq 10$.

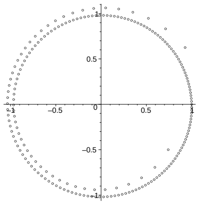
Computational Problems

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.