Some Old Problems on Polynomials with Integer Coefficients

Peter Borwein

Abstract. We survey a number of old and difficult problems all of which involve finding polynomials with integer coefficients with small norm. These problems include: the Integer Chebyshev Problem of Hilbert and Fekete; the Prouhet-Tarry-Escott problem; various conjectures of Littlewood and various conjectures of Erdös. These problems are unsolved and most are at least 35 years old. They do however lend themselves to partial solution and one suspects that they are not, in fact, totally intractable. They are also all amenable to being computed on and offer some interesting computational challenges.

§0. Introduction

We break the paper into three main sections as follows:

- Section 1: Integer Chebyshev Problems
- Section 2: Prouhet-Tarry-Escott Problems.
- Section 3: Littlewood Type Problems.

Each section is largely self-contained and there is a substantial bibliography that more than covers the material in the paper.

§1. Integer Chebyshev Problems

The basic problem is very fundamental. It is to find a polynomial with integer coefficients of minimum supnorm on an interval.

Problem 1.1. *For any interval* $[\alpha, \beta]$ *find*

$$\Omega[\alpha, \beta] := \lim_{N \to \infty} \Omega_N[\alpha, \beta]$$

where

$$\Omega_N[\alpha, \beta] := \left(\min_{a_i \in \mathcal{Z}, a_N \neq 0} \left\| a_0 + a_1 x + \cdots + a_N x^N \right\|_{[\alpha,\beta]} \right)^{\frac{1}{N}}.$$

Approximation Theory IX, Volume 1: Theoretical Aspects
Charles K. Chui and Larry L. Schumaker (eds.), pp. 33–52.

ISBN 0-8265-1325-5.

From

$$(\Omega_{n+m}[a,b])^{n+m} \le (\Omega_n[a,b])^n (\Omega_m[a,b))^m \qquad (*)$$

one can show that

$$\Omega[\alpha,\beta] := \lim_{N\to\infty} \Omega_N[\alpha,\beta]$$

exists. This quantity is called the integer Chebyshev constant for the interval or the integer transfinite diameter.

On $[-2,2]$ (or any interval with integer endpoints of length 4) this problem is solvable because the usual Chebyshev polynomials normalized to have lead coefficient 1 have integer coefficients and supnorm 2. So $\Omega[-2,2] = 1$. There are no other intervals were the explicit value is known.

For $b-a<4$, Hilbert [49] showed that there exists an absolute constant c so that

$$\inf_{0\neq p\in\mathcal{Z}_n} \|p\|_{L_2[a,b]} \le cn^{1/2}\left(\frac{b-a}{4}\right)^{1/2},$$

and Fekete [44] showed that

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

Here $\mathcal{Z}_n$ denotes the polynomials of degree n with integer coefficients. See also Kashin [60].

One sees from $(*)$ above 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

$$\begin{aligned}
p_0(x) &:= x\\
p_1(x) &:= 1-x,\\
p_2(x) &:= 2x-1,\\
p_3(x) &:= 5x^2-5x+1,\\
p_4(x) &:= 13x^3-19x^2+8x-1,\\
p_5(x) &:= 13x^3-20x^2+9x-1,\\
p_6(x) &:= 29x^4-58x^3+40x^2-11x+1,\\
p_7(x) &:= 31x^4-61x^3+41x^2-11x+1,\\
p_8(x) &:= 31x^4-63x^3+44x^2-12x+1,\\
p_9(x) &:= 941x^8-3764x^7+6349x^6-5873x^5\\
&\qquad +3243x^4-1089x^3+216x^2-23x+1,
\end{aligned}$$

then we have

Proposition 1.2. *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

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

and hence

$$\Omega[0,1] \leq \frac{1}{2.3543\ldots}.$$

Here $\|\cdot\|_{[a,b]}$ *denotes the supremum norm on* $[a,b]$.

Refinements on the method in [21] give

$$\Omega[0,1] \leq \frac{1}{2.3605\ldots}.$$

This has been further improved in [53] to

$$\Omega[0,1] \leq \frac{1}{2.3612\ldots}.$$

Of course when the coefficients of the polynomials above are not required to be integers, this reduces to the usual problem of constructing Chebyshev polynomials, and the limit (provided $a_N = 1$) gives the usual transfinite diameter. From the unrestricted case we have the obvious inequality

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

However, inspection of the above example shows that the integer Chebyshev polynomial doesn't look anything like a usual Chebyshev polynomial. In particular, it has many multiple roots and, indeed, this must be the case since we have the following lemma.

Lemma 1.3. *Suppose* $p_n \in \mathcal{Z}_n$ *(the polynomials of degree* 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*

$$\left(\|p_n\|_{[a,b]}\right)^{1/n} \geq |a_k|^{-1/k}.$$

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 sufficiently large n.

There is a sequence of polynomials that Montgomery [72] calls the Gorshkov–Wirsing polynomials that arise from iterating the rational function

$$u(x) := \frac{x(1-x)}{1-3x(1-x)}.$$

These are defined inductively by

$$q_0(x) := 2x - 1, \qquad q_1(x) := 5x^2 - 5x + 1$$

and

$$q_{n+1} := q_n^2 + q_n q_{n-1}^2 - q_{n-1}^4.$$

It transpires 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 all simple zeros in $(0,1)$, and if b_k is the lead coefficient of q_k, then

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

Wirsing has proved that these polynomials are all irreducible [72]. It follows now from Lemma 1.3 that

$$\Omega[0,1] \geq \frac{1}{2.3768417062\ldots}.$$

It is conjectured by Montogomery [72, p. 201] that if s is the least limit point of $|a_k|^{-1/k}$ (as in in Lemma 1.3) over polynomials with all their roots in $[0,1]$, then $\Omega[0,1] = s$. This was also conjectured by Chudnovsky in [34], and Chudnovsky further conjectured that the minimal s arises from the Gorshkov–Wirsing polynomials in which case s would equal $(2.3768417062\ldots)^{-1}$. In [21] we show that

$$\Omega[0,1] \geq \frac{1}{2.3768417062\ldots} + \epsilon.$$

This shows that either Montogomery's conjecture is false or the Gorshkov–Wirsing polynomials do not give rise to the minimal s. This leads us to

Conjecture 1.4. *The minimal s arising in Lemma* 1.3 *does not give the right value for* $\Omega[0,1]$.

In [21] we asked whether integer Chebyshev polynomials on $[0,1]$ have all their roots in $[0,1]$. In [53] Habsieger and Salvy show that this can fail, with the first non-totally-real-factor occurring for $n = 70$. This same paper computes extrema up to degree 75. This is a nontrivial computation and is quite likely NP hard. None-the-less, one suspects that there is a close relationship between $\Omega[0,1]$ and polynomials with integer coefficients and all roots in $[0,1]$. Sorting out this relationship would be of interest.

There is a somewhat related problem that we have called the Schur-Siegel-Smyth trace problem.

Problem 1.5. *Fix $\epsilon > 0$. Suppose*

$$p_n(z) = a_n z^n + \cdots + a_0, a_i \in \mathcal{Z}$$

has all real, positive roots and is irreducible. Then except for finitely many explicit exceptions,

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

There are some partial results. In the notation of Problem 1.5 except for finitely many (explicit) exceptions, $a_{n-1} \geq (1.771..)n$. This is due to Smyth [89]. Previously, in 1918, Schur had shown $a_{n-1} \geq e^{1/2}n$, and in 1943 Siegel had shown that $a_{n-1} \geq (1.733..)n$.

The relationship this has to integer Chebyshev problems is the following.

Lemma 1.6. *If*

$$C[0, 1/m] \leq \frac{1}{m + \delta},$$

then for totally positive polynomials (polynomials as in Problem 1.5*),*

$$a_{n-1} \geq \delta n,$$

with finitely many explicit exceptions.

This reduces finding better bounds in the Schur-Siegel-Smyth trace problem to computations on short intervals. From an example on $[0, 1/100]$ we derive

Corollary 1.7. $\delta > 1.744$.

Smyth has shown that this method can never give the full result of Problem 1.5, but it would be interesting to see how far it can be taken.

The papers by Aparicio and Montgomery's monograph provide a good additional entry point to this subject matter.

§2. Ideal Solutions of the Prouhet-Tarry-Escott Problem

This old conjecture states concisely as

Conjecture 2.1. *For any N there exists $p \in \mathcal{Z}[x]$ (the polynomials with integer coefficients) so that*

$$p(x) = (x - 1)^N q(x) = \Sigma_k a_k x^k$$

and

$$l_1(p) := \Sigma_k |a_k| = 2N.$$

Note that the degree of the solution is not the issue. The problem is in terms of the size of the zero at 1. It is a reasonably simple exercise to see that $2N$ is a lower bound so this would be the best possible result for any N. It is probably equivalent (though not provably so) to restrict to polynomials with

coefficients $\{0,-1,+1\}$, and in this case we are looking for a $p \in \mathcal{Z}[x]$ with a zero of order n at one and with

$$\|p\|_{L_2\{|z|=1\}} = \sqrt{2N}.$$

What is actually provable is that any solution of Problem 2.1 must have all coefficients in the set $\{0,-1,+1,-2,+2\}$.

An entirely equivalent form of Problem 2.1 asks to find two distint sets of integers $[\alpha_1,\cdots,\alpha_N]$ and $[\beta_1,\cdots,\beta_N]$ so that

$$\begin{aligned}
\alpha_1 + \cdots + \alpha_N &= \beta_1 + \cdots + \beta_N \\
\alpha_1^2 + \cdots + \alpha_N^2 &= \beta_1^2 + \cdots + \beta_N^2 \\
\vdots \qquad & \quad \vdots \qquad \quad \vdots \\
\alpha_1^{N-1} + \cdots + \alpha_N^{N-1} &= \beta_1^{N-1} + \cdots + \beta_N^{N-1}.
\end{aligned}$$

This equivalence is an easy exercise in Newton's equations. The later form is the usual form in which the problem arises and is stated.

Sets of integers (as above) are called ideal solutions of the Prouhet-Tarry-Escott problem. Non-ideal solutions are ones where the size of the sets is allowed to be greater than the number of equations plus one.

This conjecture explicitly goes back at least to Wright in 1935 [99]. It is not clear why the conjecture is made. There is not a convincing heuristic for it. Solutions exist for N up to and including 10, and no solutions are known for any $N > 10$. For the cases up to 10, except for 9, there are known to be infinitely many solutions. For $N = 9$ two solutions are known. (We do not count as distinct solutions that arise by linear transformation.)

The following gives solutions up to 10. Suppose

$$x^{\alpha_1} + \cdots + x^{\alpha_N} - x^{\beta_1} - \cdots - x^{\beta_N} = 0((x-1)^N).$$

We write the solutions, as is traditional, in the form

$$[\alpha_1,\ldots,\alpha_N] \quad = \quad [\beta_1,\ldots,\beta_N].$$

Solutions for $N = 2,3,4\ldots,10$ are given by
$[0,3] = [1,2]$
$[1,2,6] = [0,4,5]$
$[0,4,7,11] = [1,2,9,10]$
$[1,2,10,14,18] = [0,4,8,16,17]$
$[0,4,9,17,22,26] = [1,2,12,14,24,25]$
$[0,18,27,58,64,89,101] = [1,13,38,44,75,84,102]$
$[0,4,9,23,27,41,46,50] = [1,2,11,20,30,39,48,49]$
$[0,24,30,83,86,133,157,181,197] = [1,17,41,65,112,115,168,174,198]$
$[0,3083,3301,11893,23314,24186,35607,44199,44417,47500]$
$= [12,2865,3519,11869,23738,23762,35631,43981,44635,47488].$

The size 10 example above illustrates the problems inherent with searching for a solution. While it is not known whether this is the smallest size 10 solution, it is the smallest one known, and is far beyond a size findable by exhaustive searching.

The smaller solutions were found by Escott and Tarry in the early part of this century. The size 9 and 10 solutions are due to Letac and were found in the early forties (without the aid of computers). Indeed very little new on this problem has been found computationally. (See [25] for further survey material.) The following seems a reasonable but as yet unattainable goal.

Problem 2.2. *Design an algorithm to establish whether or not solutions exist of modest size (say $N \leq 15$) and modest height (say 1000).*

The following is Smyth's [91] elegant decoding of Letac's size 10 solution. Let

$$F_{10} := \left(t^2 - {R_1}^2\right)\left(t^2 - {R_2}^2\right)\left(t^2 - {R_3}^2\right)\left(t^2 - {R_4}^2\right)\left(t^2 - {R_5}^2\right) - \left(t^2 - {R_6}^2\right)\left(t^2 - {R_7}^2\right)\left(t^2 - {R_8}^2\right)\left(t^2 - {R_9}^2\right)\left(t^2 - {R_{10}}^2\right).$$

A solution of size 10 will be given as

$$[\pm R_1, \pm R_2, \pm R_3, \pm R_4, \pm R_5] = [\pm R_6, \pm R_7, \pm R_8, \pm R_9, \pm R_{10}]$$

provided F_{10} expands to equal a constant (i.e. all the powers of t expand out). This is another equivalent form of the problem also deduced via Newton's equations. Now we choose

$$R_1 := (4\,n + 4\,m)^2 \qquad R_2 := (mn + n + m - 11)^2$$
$$R_3 := (mn - n - m - 11)^2 \qquad R_4 := (mn + 3\,n - 3\,m + 11)^2$$
$$R_5 := (mn - 3\,n + 3\,m + 11)^2 \qquad R_6 := (4\,n - 4\,m)^2$$
$$R_7 := (-mn + n - m - 11)^2 \qquad R_8 := (-mn - n + m - 11)^2$$
$$R_9 := (-mn + 3\,n + 3\,m + 11)^2 \qquad R_{10} := (-mn - 3\,n - 3\,m + 11)^2.$$

On expansion of F_{10}, the constant coefficient is

$$\begin{aligned} &-64\,mn\left(m^4n^4 - 10\,n^4m^2 + 9\,n^4 - 1210\,n^2 + 14641\right.\\ &\quad\left.-524\,m^2n^2 + 726\,m^2 + 6\,m^4n^2 + 185\,m^4\right)\\ &\times\left(m^4n^4 + 6\,n^4m^2 + 185\,n^4 + 726\,n^2 + 14641\right.\\ &\quad\left.-524\,m^2n^2 - 1210\,m^2 - 10\,m^4n^2 + 9\,m^4\right). \end{aligned}$$

The rest of the expansion is given as

$$\begin{aligned} &+64\,mn\left(5\,m^4n^4 + 62\,n^4m^2 + 125\,n^4 + 62\,m^4n^2 + 1268\,m^2n^2\right.\\ &\quad\left.+7502\,n^2 + 125\,m^4 + 7502\,m^2 + 73205\right)\\ &\times\left(m^2n^2 - 13\,n^2 + 121 - 13\,m^2\right)t^2\\ &-64\,mn\left(7\,m^2n^2 + 53\,n^2 + 847 + 53\,m^2\right)\left(m^2n^2 - 13\,n^2 + 121 - 13\,m^2\right)t^4\\ &\quad+192\,mn\left(m^2n^2 - 13\,n^2 + 121 - 13\,m^2\right)t^6, \end{aligned}$$

and each coefficient of the above polynomial of t has a factor

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

So 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 $m = -1264969/424999$. It is an exercise in elliptic curves to see that the above biquadratic has infinitely many solutions, and hence so does the problem of size $N = 10$.

For sizes 1 through 8, parametric families of solutions exist. The following is a (homogenous) size 8 solution due to Chernick [33]

$$[\pm R_1, \pm R_2, \pm R_3, \pm R_4] = [\pm R_5, \pm R_6, \pm R_7, \pm R_8],$$

where

$$R_1 := 5\,m^2 + 9\,mn + 10\,n^2 \qquad R_2 := m^2 - 13\,mn - 6\,n^2$$

$$R_3 := 7\,m^2 - 5\,mn - 8\,n^2 \qquad R_4 := 9\,m^2 + 7\,mn - 4\,n^2$$

$$R_5 := 9\,m^2 + 5\,mn + 4\,n^2 \qquad R_6 := m^2 + 15\,mn + 8\,n^2$$

$$R_7 := 5\,m^2 - 7\,mn - 10\,n^2 \qquad R_8 := 7\,m^2 + 5\,mn - 6\,n^2.$$

One sees this by noting that if

$$F_8 := \left(t^2 - {R_1}^2\right)\left(t^2 - {R_2}^2\right)\left(t^2 - {R_3}^2\right)\left(t^2 - {R_4}^2\right)$$

$$-\left(t^2 - {R_5}^2\right)\left(t^2 - {R_6}^2\right)\left(t^2 - {R_7}^2\right)\left(t^2 - {R_8}^2\right)$$

then on expansion

$$F_8 = -10752\,mn\,(2\,n + m)\,(n + m)\,(2\,n + 3\,m)\,(n + 2\,m)\,(4\,n - m)\,(5\,n + 4\,m)$$

$$\times\,(n - 2\,m)\,(3\,n + m)\,(n - m)\,(n + 5\,m)\left(3\,n^2 + 2\,mn - 2\,m^2\right)\left(n^2 + mn + m^2\right).$$

Now any integers n and m (provided the expression doesn't collapse) give rise to a solution of size 8.

There are only two non-equivalent solutions of size $N = 9$ known. They are given in symmetric form as

$$[98, 82, 58, 34, -13, -16, -69, -75, -99]$$
$$= [-98, -82, -58, -34, 13, 16, 69, 75, 99]$$

and

$$[174, 148, 132, 50, 8, -63, -119, -161, -169]$$
$$= [-174, -148, -132, -50, -8, 63, 119, 161, 169].$$

It would be of value to know whether there are infinitely many solutions of size 9, and it might be of interest to search for a parametric solution.

2.1. Variations on the Theme

The obvious question arises: If we can't make the l_1 norm of a polynomial with a zero of order N at 1 be $2N$, how small can we make it?

Problem 2.3. *Find* $0 \neq p_N \in \mathcal{Z}[x]$ *where* $p_N(x) = (x-1)^N q(x) = \Sigma a_k x^k$ *so that*

$$l_1(p_N) = \Sigma|a_i| = o(N^2)$$

or

$$l^2(p_N) = (\Sigma|a_i|^2)^{1/2} = o(N^2).$$

A fairly easy combinatorial argument shows that

$$l_1(p_N) \leq N^2/2$$

is possible for all N. (See [25]) However, this is where the problem is stuck (at least in terms of the principal term of the asymptotic), and even getting a bound like $N^2/(2+\epsilon)$ would be major progress.

This problem arises in the context of a problem Wright called the "easier Waring problem." The Waring problem asks how many positive Nth powers are required to write every sufficiently large integer as a sum of Nth powers. The "easier Waring problem" allows for differences as well as sums. The "easier" has proved to be a misnomer since currently the best approaches to the "easier Waring problem" all go through the Waring problem.

Fuchs and Wright [48] observed that if (as in Problem 2.3)

$$l_1(p_N) = O(A_N),$$

then the Easier Waring problem is also $O(A_N)$. (Here N is the power under investigation in Waring's problem.) At the moment Waring's problem is known to be $O(N \log N)$ (though it is suspected to be $O(N)$). So showing that

$$l_1(p_N) = O(N \log N)$$

would be a very major result.

If we demand that p has a zero of order N but not of order $N+1$ at 1, then

$$l_1(p) = O((\log N)N^2)$$

is possible, but this is all that is known [55]. And this argument is considerably harder than the one that gives $O(N^2)$ without the additional requirement that the multiplicity of the zero be *exactly* N. Any improvement on this would also be interesting.

2.2. Problem of Erdös and Szekeres (1958)

One approach to the Prouhet-Tarry-Escott problem is to construct products of the form

$$p(x) := \left(\prod_{k=1}^{N} (1 - x^{\alpha_i}) \right).$$

Obviously, such a product has a zero of order N at 1, and the trick is to minimize the l_1 norm.

Problem 2.4. *Minimize over* $\{\alpha_1, \ldots, \alpha_N\}$

$$l_1 \left(\prod_{k=1}^{N} (1 - x^{\alpha_i}) \right).$$

Call this minimum E_N^*.

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	48	$\{1, \ldots, 9, 11, 13, 17, 19\}$

Note that for $N := 1, 2, 3, 4, 5, 6, 8$, this provides an ideal solution of the Prouhet-Tarry-Escott problem. And indeed the first known solutions were mostly of this form. Maltby [70] shows that for $N = 7, 9, 10, 11$, these kind of products cannot solve the Prouhet-Tarry-Escott problem. For $N = 7, 9, 10$, the above examples are provably optimal. This leads to the following conjecture.

Conjecture 2.5. *Except for* $N = 1, 2, 3, 4, 5, 6$ *and* 8,

$$E_N^* \geq 2N + 2.$$

Actually much more is likely to be true. Erdös and Szekeres [42] conjecture that E_N^* grows fairly rapidly. Specifically,

Conjecture 2.6. *For any K,*

$$E_N^* \geq N^K,$$

for N sufficiently large.

Currently the only lower bounds known (except for Maltby's results for $N = 7, 9, 10$ and 11) are the trivial lower bounds $E_N^* \geq 2N$ of the Prouhet-Tarry-Escott problem.

Sub-exponential upper bounds in this problem of the form

$$E_N^* \ll \exp\left(O(\log^4 N)\right)$$

due to Belov and Konyagin are known [13]. See also [76], [62].

§3. Littlewood Type Problems

Here we are primarily concerned with polynomials with coefficients in the set $\{+1, -1\}$. Since many of these problems were raised by Littlewood, we denote the set of such polynomials by $\mathcal{L}_n$, and refer to them as Littlewood polynomials. Specifically

$$\mathcal{L}_n := \left\{ p : p(x) = \sum_{j=0}^{n} a_j x^j \,, \;\; a_j \in \{-1, 1\} \right\}.$$

The following conjecture is due to Littlewood, probably from some time in the fifties. It has been much studied, and has associated with it a considerable signal processing literature (see for example [31].)

Conjecture 3.1. *It is possible to find $p_n \in \mathcal{L}_n$ so that*

$$C_1\sqrt{n+1} \leq |p_n(z)| \leq C_2\sqrt{n+1}$$

for all complex z of modulus 1. Here the constants C_1 and C_2 are independent of n.

Such polynomials are often called "locally flat." Because the L_2 norm of a polynomial from $\mathcal{L}_n$ is exactly $\sqrt{n+1}$, the constants must satisfy $C_1 \leq 1$ and $C_2 \geq 1$. This is discussed in some detail in problem 19 of Littlewood's charming monograph [67]. Littlewood, in part, based his conjecture on computations of all such polynomials up to degree twenty. Odlyzko has now done extensive computations that tend to confirm the conjecture. However, it is still the case that no sequence is known that satisfies the lower bound.

A sequence of Littlewood polynomials that satisfies just the upper bound is given by the Rudin-Shapiro polynomials. These are defined by

$$p_0(z) := 1, \qquad q_0(z) := 1$$

and

$$p_{n+1}(z) := p_n(z) + z^{2^n} q_n(z),$$

$$q_{n+1}(z) := p_n(z) - z^{2^n} q_n(z).$$

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

$$|p_{n+1}|^2 + |q_{n+1}|^2 = 2(|p_n|^2 + |q_n|^2)$$

and it is easy to deduce that

$$|p_n(z)| \leq 2\sqrt{2}^n = \sqrt{2}\sqrt{\deg(p_n)}$$

and

$$|q_n(z)| \leq 2\sqrt{2}^n = \sqrt{2}\sqrt{\deg(q_n)}$$

for all z of modulus 1.

This conjecture is complemented by a conjecture of Erdős [41].

Conjecture 3.2. *The constant C_2 in conjecture* 3.1 *is bounded away from 1 (independently of n).*

This is also still open. Though a remarkable result of Kahane's [59] shows that if the polynomials are allowed to have complex coefficients of modulus 1, then "locally flat" polynomials exist, and indeed it is possible to make C_1 and C_2 asymptotically arbitrarily close to 1. (Polynomials of this form are sometimes called "ultra-flat.") Another striking result due to Beck [10] proves that "locally flat" polynomials exist from the class of polynomials of degree n whose coefficients are 1200th roots of unity.

Of course, because of the monotonicity of the L_p norms, it is relevant to rephrase Erdős' conjecture in other norms. Newman and Byrnes speculate, too optimistically, in [74] that

$$||p||_4^4 \geq (6 - \delta)n^2/5$$

for $p \in \mathcal{L}_n$ and n sufficiently large. This, of course, would imply Erdös' conjecture above. Here and throughout this section

$$||q||_p = \left(\int_0^{2\pi} |q(\theta)|^p \, d\theta/(2\pi) \right)^{1/p}$$

is the normalized p norm on the boundary of the unit disc.

It is possible to find a sequence of $p_n \in \mathcal{L}_n$ so that

$$||p_n||_4^4 \asymp (7/6)n^2.$$

This sequence is constructed out of the Fekete polynomials

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

where $\left(\frac{\cdot}{p} \right)$ is the Legendre symbol. One now takes the Fekete polynomials and cyclically permutes the coefficients by about $p/4$ to get the above example due to Turyn [54]. Actually, computations suggest that even the 7/6 constant above may also be overly optimistic. Nonetheless, a variety of people conjecture the following.

Problem 3.3. *Show for some absolute constant $\delta > 0$ and for all $p_n \in \mathcal{L}_n$*

$$||p||_4 \geq (1+\delta)\sqrt{n}$$

or even the much weaker

$$||p||_4 \geq \sqrt{n} + \delta.$$

This problem of finding Littlewood polynomials of minimal L_4 norm has a considerable literature. See [52, 51, 54, 56]. The engineering literature calls this the "merit factor" problem.

A Barker polynomial

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

with each $a_k \in \{-1, +1\}$ is a polynomial where

$$p(z)\overline{p(z)} := \sum_{k=-n}^{n} c_k z^k$$

satisfies

$$|c_j| \leq 1, \qquad j = 1, 2, 3 \ldots.$$

Here

$$c_j = \sum_{k=0}^{n-j} a_k a_{k+j} \qquad \textit{and} \qquad c_{-j} = c_j.$$

Note that if $p(z)$ is a Barker polynomial of degree n then

$$||p||_4 \leq ((n+1)^2 + 2n))^{1/4} < (n+1)^{1/2} + (n+1)^{-1/2}/2.$$

The nonexistence of Barker polynomials of degree n is now shown by showing

$$||p||_4 \geq (n+1)^{1/2} + (n+1)^{-1/2}/2.$$

This is even weaker than the weak form of Problem 3.3.

It is conjectured that no Barker polynomials exist for $n > 12$. See [81] for more on Barker polynomials and a proof of the nonexistence of self-inversive Barker polynomials. In [96] it is shown that no even degree Barker polynomials exist for $n > 12$ (and indeed none exist for any degree between 12 and 10^{12}.

The expected L_p norms of Littlewood polynomials and their derivatives are computed in [27]. For random $q_n \in \mathcal{L}_n$

$$\frac{\mathrm{E}(||q_n||_p)}{n^{1/2}} \to (\Gamma(1 + p/2))^{1/p}$$

and

$$\frac{\mathrm{E}(||q_n^{(r)}||_p)}{n^{(2r+1)/2}} \to (2r+1)^{-1/2}(\Gamma(1 + p/2))^{1/p}.$$

3.1. Lehmer's Conjecture

Mahler's Measure is defined as follows: if

$$p(z) := \prod_{i=1}^{n}(z - \alpha_i),$$

then

$$M(p) := \prod_{i=1}^{n} \max\{1, |\alpha_i|\},$$

or equivalently

$$M(p) := \exp\left\{ \int_0^1 \log |p(e^{2\pi i t})|\, dt \right\}.$$

The problem commonly known as Lehmer's Conjecture is

Conjecture 3.4. *Suppose p is a monic polynomial with integer coefficients. Then either $M(p) = 1$ or $M(p) \geq 1.1762808...$.*

See [30] for an exposition of this problem. This can be thought of as a generalization of Kronecker's theorem which can be stated as: $M(p) = 1$ implies that p is cyclotomic (that is, it has all its roots of modulus 1). Note that $M(p)$ is really the L_0 norm, so this too is a growth problem, and in fact for this conjecture it is sufficient to consider only polynomials with coefficients in the set $\{0, -1, +1\}$.

The minimal Mahler measure for a non-cylotomic p is speculated to be given by $p := x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ for which $M(p) = 1.17628081825991750\ldots$. This is also speculated to be the smallest Salem number.

Problem 3.5. *Do there exist polynomials with coefficients $\{0, -1, +1\}$ with roots of arbitrarily high multiplicity inside the unit disk?*

A negative answer to the above would solve Lehmer's conjecture. It seems likely, however, that the answer to the above question is positive. See [7].

Mahler [69] raised the problem of finding the maximum Mahler measure over the polynomials of degree n with coefficients $\{0, +1, -1\}$.

Problem 3.6. *Does there exist a sequence of Littlewood polynomials $p_n \in \mathcal{L}_n$ so that*

$$\lim_n \frac{M(p_n)}{\sqrt{n}} = 1?$$

This is a weak form of the Erdös conjecture. The non-existence of a sequence, as in Problem 3.6, implies Conjecture 3.2.

3.2. Zeros of Littlewood and Related Polynomials

The following result concerning polynomials of height one is proved in [20].

Theorem 3.7. *Every polynomial p_n of the form*

$$p_n(x) = \sum_{j=0}^{n} a_j x^j, \qquad |a_0| = 1\,, \quad |a_j| \le 1\,, \quad a_j \in \mathbb{C} \qquad (**)$$

has at most $\left\lfloor \frac{16}{7}\sqrt{n} \right\rfloor + 4$ zeros at 1.

It is easy to prove the following:

Theorem 3.8. *There is an absolute constant $c > 0$ such that for every n, there is a polynomial p of degree n with coefficients in the set $\{0, -1, +1\}$ having at least $c\sqrt{n/\log(n+1)}$ zeros at 1.*

Theorems 3.7 and 3.8 show that the right upper bound for the number of zeros a polynomial p_n with coefficients in the set $\{0, -1, +1\}$ can have at 1 is somewhere between $c_1\sqrt{n/\log(n+1)}$ and $c_2\sqrt{n}$ with absolute constants $c_1 > 0$ and $c_2 > 0$.

Problem 3.9. *What is the maximum multiplicity of the zero at 1 for a polynomial of degree n with coefficients in $\{0, -1, +1\}$. In particular, is it $O(n^{1/2})$?*

This problem has substantial application to effective bounds in Roth's Theorem, particularly if the answer to the above conjecture is affirmative.

Boyd [29] shows that there is an absolute constant c such that every $p \in \mathcal{L}_n$ can have at most $c \log^2 n / \log\log n$ zeros at 1. Since it is easy to give polynomials $p \in \mathcal{L}_n$ with $c \log n$ zeros at 1, the following question is suggested.

Problem 3.10. *Prove or disprove that there is an absolute constant c such that every polynomial $p \in \mathcal{B}_n$ can have at most $c \log n$ zeros at 1.*

References

1. Amoroso F., Sur le diamètre transfini entier d'un intervalle réel, Ann. Inst. Fourier, Grenoble **40** (1990), 885–911.
2. Aparicio, E., Methods for the approximate calculation of minimum uniform Diophantine deviation from zero on a segment, Rev. Mat. Hisp.-Amer. **38** (1978), 259–270 (Spanish).
3. Aparicio, E., New bounds on the minimal Diophantine deviation from zero on $[0, 1]$ and $[0, 1/4]$, Actus Sextas J. Mat. Hisp.-Lusitanas (1979), 289–291.
4. Aparicio, E., On some systems of algebraic integers of D. S. Gorshkov and their application in calculus, Rev. Mat. Hisp.-Amer. **41** (1981), 3–17 (Spanish).

5. Aparicio, E., On some results in the problem of Diophantine approximation of functions by polynomials, Proc. Steklov Inst. Math. **163** (1985), 7–10.
6. Atkinson, F. A., On a problem of Erdös and Szekeres, Canad. Math. Bull. **1** (1961), 7–12.
7. Beaucoup, F., P. Borwein, D. Boyd, and C. Pinner, Multiple roots of $[-1,1]$ power series, J. London Math. Soc., to appear.
8. Beaucoup, F., P. Borwein, D. Boyd, and C. Pinner, Power series with restricted coefficients and a root on a given ray, Math. Computat, to appear.
9. Beck, J., Flat polynomials on the unit circle – Note on a problem of Littlewood, Bull. London Math. Soc. **23** (1991), 269–277.
10. Beck, J., The modulus of polynomials with zeros on the unit circle: A problem of Erdös, Annals of Math. **134** (1991), 609–651.
11. Bell, J., P. Borwein, and B. Richmond, Growth of the product $\prod_{j=1}^{n}(1-x^{a_j})$, Acta Arith., to appear.
12. Beenker, G., T. Claasen, and P. Hermes, Binary sequences with a maximally flat amplitude sequence, Philips J. Res. **40** (1985), 289–304.
13. Belov, A. S. and S. V. Konyagin, On estimates for the constant term of a nonnegative trigonometric polynomial with integral coefficients, Mat Zametki **59** (1996), 627–629.
14. Bharucha-Reid, A. T. and M. Sambandham, *Random polynomials*, Academic Press, Orlando, 1986.
15. Bloch, A. and G. Pólya, On the roots of certain algebraic equations, Proc. London Math. Soc **33** (1932), 102–114.
16. Boehmer, A. M., Binary pulse compression codes, IEEE Trans. Information Theory **13** (1967), 156–167.
17. Bombieri, E. and J. Vaaler, Polynomials with low height and prescribed vanishing, in *Analytic Number Theory and Diophantine Problems*, Birkhauser, Boston, 1987, pp. 53–73.
18. Borwein, P. and T. Erdélyi, Markov-Bernstein type inequalities under Littlewood-type coefficient constraints, submitted.
19. Borwein, P. and T. Erdélyi, Littlewood-type problems on subarcs of the unit circle, Indiana J. Math. **46** (1997), 1323–1346.
20. Borwein, P. and T. Erdélyi, On the zeros of polynomials with restricted coefficients, Illinois J. Math. **41** (1997), 667–675.
21. Borwein, P. and T. Erdélyi, The integer Chebyshev problem, Math. Computat. **65** (1996), 661–681.
22. Borwein, P. and T. Erdélyi, Markov and Bernstein type inequalities for polynomials with restricted coefficients, Ramanujan J. **1** (1997), 309–323.

23. Borwein, P. and T. Erdélyi, Questions about polynomials with $\{0, -1, +1\}$ coefficients, Constr. Approx. **12** (1996), 439–442.
24. Borwein, P. and T. Erdélyi, *Polynomials and Polynomial Inequalities*, Springer-Verlag, New York, 1995.
25. Borwein, P. and C. Ingalls, The Prouhet, Tarry, Escott problem, Ens. Math. **40** (1994), 3–27.
26. Borwein, P. and C. Pinner, Polynomials with $\{0, +1, -1\}$ coefficients and a root close to a given point, Canadian J. Math. **49** (1997), 887–915.
27. Borwein, P. and R. Lockhart, The expected L_p norm of random polynomials.
28. Bourgain, J., Sul le minimum d'une somme de cosinus, Acta Arith. **45** (1986), 381–389.
29. Boyd, D., On a problem of Byrnes concerning polynomials with restricted coefficients, Math. Comput. **66** (1977), 1697–1703.
30. Boyd, D., Variations on a theme of Kronecker, Canad. Math. Bull. **21** (1978), 1244–1260.
31. Byrnes, J. S. and D. J. Newman, Null steering employing polynomials with restricted coefficients, IEEE Trans. Antennas and Propagation **36** (1988), 301–303.
32. Carrol, F. W., D. Eustice, and T. Figiel, The minimum modulus of polynomials with coefficients of modulus one, J. London Math. Soc. **16** (1977), 76–82.
33. Chernick, J., Ideal solutions of the Tarry-Escott problem, Amer. Math. Monthly **44** (1937), 627-633.
34. Chudnovsky, G., Number theoretic applications of polynomials with rational coefficients defined by extremality conditions, in *Arithmetic and Geometry*, Vol. I, M. Artin and J. Tate, (eds.), Progress in Math., Vol. 35, Birkhäuser, Boston, 1983, pp. 61–105.
35. Clunie, J., On the minimum modulus of a polynomial on the unit circle, Quart. J. Math. **10** (1959), 95–98.
36. Cohen, P. J., On a conjecture of Littlewood and idempotent measures, Amer. J. Math. **82** (1960), 191–212.
37. Dickson, L. E., *History of the Theory of Numbers*, Chelsea Publishing Co., New York, 1952.
38. Dobrowolski, E., On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arithmetica **34** (1979), 341–401.
39. Dorwart, H. L. and O. E. Brown, The Tarry-Escot problem, Amer. Math. Monthly **44** (37), 613–626.
40. Erdös, P., Some old and new problems in approximation theory: research problems 95-1, Constr. Approx. **11** (1995), 419–421.
41. Erdös, P., An inequality for the maximum of trigonometric polynomials, Annales Polonica Math. **12** (1962), 151–154.

42. Erdös, P. and G. Szekeres, On the product $\prod_{k=1}^{n}(1-z^{a_k})$, Publications de L'Institut Math. **12** (1952), 29–34.
43. Erdös, P. and P. Turán, On the distribution of roots of polynomials, Annals of Math. **57** (1950), 105–119.
44. Fekete, M., Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, Math. Zeit. **17** (1923), 228–249.
45. Ferguson, Le Baron O., *Approximation by Polynomials with Integral Coefficients*, Amer. Math. Soc., Rhode Island, 1980.
46. Fielding, G. T., The expected value of the integral around the unit circle of a certain class of polynomials, Bull. London Math. Soc. **2** (1970), 301–306.
47. Flammang, V., G. Rhin, and C. J. Smyth, The integer transfinite diameter of intervals and totally real algebraic integers, manuscript.
48. Fuchs, W. H. J. and E. M. Wright, The easier Waring problem, Quart. J. Math, **10** (1939), 190–209.
49. Hilbert, D., Ein Beitrag zur Theorie des Legendreschen Polynoms, Acta Math. **18** (1894), 155–159.
50. Gloden, A., *Mehrgradige Gleichungen*, Noordhoff, Groningen, 1944.
51. Golay, M. J., The merit factor of Legendre sequences, IEEE Trans. Information Theory **29** (1983), 934–936.
52. Golay, M. J., Sieves for low autocorrelation binary sequences, IEEE Trans. Information Theory **23** (1977), 43–51.
53. Habsieger, L. and B. Salvy, On integer Chebyshev polynomials, Math. Comp. **218** (1997), 763–770.
54. Hoholdt, T. and H. Jensen, Determination of the merit factor of Legendre sequences, IEEE Trans. Information Theory **34** (1988), 161–164.
55. Hua, L. K., *Introduction to Number Theory*, Springer-Verlag, Berlin, Heidelberg, New York, 1982.
56. Jensen, J., H. Jensen, and T. Hoholdt, The merit factor of binary sequences related to difference sets, IEEE Trans. Information Theory **37** (1991), 617–626.
57. Kac, M., On the average number of real roots of a random algebraic equation, II, Proc. London Math. Soc. **50** (1948), 390–408.
58. Kahane, J-P., *Some Random Series of Functions*, Vol. 5, Cambridge Studies in Advanced Mathematics, Cambridge, 1985; Second Edition.
59. Kahane, J-P., Sur les polynômes á coefficients unimodulaires, Bull. London Math. Soc **12** (1980), 321–342.
60. Kashin, B., Algebraic polynomials with integer coefficients with least deviation from zero on an interval, Mat. Zametki **50** (1991), 58–67.
61. Kleiman, H., A note on the Tarry-Escott problem, J. Reine. Angew. Math **278/279** (1975), 48–51.

62. Kolountzakis, M., *Probabilistic and Constructive Methods in Harmonic Anaysis and Additive Number Theory*, Ph.D. Thesis, Stanford University, 1994.

63. Konjagin, S., On a problem of Littlewood, Izv. A. N. SSSR, ser. mat. **45** (2) (1981), 243–265.

64. Körner, T. W., On a polynomial of J.S. Byrnes, Bull. London Math. Soc. **12** (1980), 219–224.

65. Littlewood, J. E., On the mean value of certain trigonometric polynomials, J. London Math. Soc. **36** (1961), 307–334.

66. Littlewood, J. E., On polynomials $\sum^n \pm z^m$ and $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$, J. London Math. Soc. **41** (1966), 367–376.

67. Littlewood, J. E., *Some Problems in Real and Complex Analysis*, Heath Mathematical Monographs, Lexington, Massachusetts, 1968.

68. Littlewood, J. E. and A. C. Offord, On the number of real roots of a random algebraic equation, II, Proc. Cam. Phil. Soc. **35** (1939), 133–148.

69. Mahler, K., On two extremal properties of polynomials, Illinois J. Math. **7** (1963), 681–701.

70. Maltby, R., *Pure Product Polynomials of Small Norm*, Ph.D. Thesis, Simon Fraser University, 1996.

71. Melzak, Z. A., A note on the Tarry-Escott problem, Canad. Math. Bull **4** (1961), 233–237.

72. Montgomery, H. L., *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS, Vol. 84, Amer. Math. Soc., R. I., 1994.

73. Montgomery, H. L., An exponential sum formed with the Legendre symbol, Acta Arithmetica **37** (1980), 375–380.

74. Newman, D. J. and J. S. Byrnes, The L^4 norm of a polynomial with coefficients ± 1, MAA Monthly **97** (1990), 42–45.

75. Newman, D. J. and A. Giroux, Properties on the unit circle of polynomials with unimodular coefficients, in *Recent Advances in Fourier Analysis and its Applications*, J. S. Byrnes and J. F. Byrnes, (eds.), Kluwer, 1990, 79–81.

76. Odlyzko, A., Minima of cosine sums and maxima of polynomials on the unit circle, J. London Math. Soc. **26** (1982), 412–420.

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

78. Pólya, G. and G. Szegö, *Problems and Theorems in Analysis*, Volume I, Springer-Verlag, New York, 1972.

79. Rees, E. and C. J. Smyth, On the Constant in the Tarry-Escott Problem, in *Cinquante Ans de Polynômes*, Fifty Years of Polynomials, Springer-Verlag, New York, 1988.

80. Robinson, L., M.Sc. Thesis, Simon Fraser University, 1997.

81. Saffari, B., *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.
82. Saffari, B., Polynmes réciproques: conjecture d'Erdös en norme L^4, taille des autocorrélations et inexistence des codes de Barker, C. R. Acad. Sci., Paris Sér. I Math **308** (1989), 461–464.
83. Salem, R. and A. Zygmund, Some properties of trigonometric series whose terms have random signs, Acta Math **91** (1954), 254–301.
84. Schmidt, E., Über algebraische Gleichungen vom Pólya-Bloch-Typos, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1932), 321.
85. Schur, I., Untersuchungen über algebraische Gleichungen, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 403–428.
86. Siegel, C. L., The trace of totally positive and real algebraic integers, Annals of Math. **46** (1945), 302–314.
87. Sinha, T. N., On the Tarry-Escott problem, Amer. Math. Monthly **73** (1966), 280–285.
88. Smyth, C. J., Cyclotomic factors of reciprocal polynomials and totally positive algebraic integers of small trace, manuscript.
89. Smyth, C. J., The mean values of totally real algebraic integers, Math. Comp **42** (1984), 663–681.
90. Smyth, C. J., Totally positive algebraic integers of small trace, Ann. Inst. Fourier **33** (1984), 1–28.
91. Smyth, C. J., Ideal 9th-order Multigrades and Letac's Elliptic Curve, Math. Comp. **57** (1991), 817–823.
92. Solomyak, B., On the random series $\sum \pm \lambda^n$ (an Erdös problem), Annals of Math. **142** (1995), 611–625.
93. Sudler, C., An estimate for a restricted partition function, Quart. J. Math. **2** (1964), 1–10.
94. Szegö, G., Bemerkungen zu einem Satz von E. Schmidt uber algebraische Gleichungen, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1934), 86–98.
95. Turán, P., *On a New Method of Analysis and its Applications*, Wiley, New York, 1984.
96. Turyn, R. and J. Storer, On binary sequences, Proc. Amer. Math. Soc. **12** (1961), 394–399.
97. Wright, E. M., The Tarry-Escott and the "easier" Waring Problem, J. Reine Angew Math **311/312** (1972), 170–173.
98. Wright, E. M., Prouhet's 1851 solution of the Tarry-Escott Problem of 1910, Amer. Math. Monthly **66** (1959), 199–201.
99. Wright, E. M., On Tarry's Problem (I), Quart. J. Math. **6** (1935), 261–267.
100. Wright, E. M., An easier Waring's Problem, J. London Math. Soc. **9** (1934), 267–272.