POLYNOMIALS WITH INTEGER COEFFICIENTS AND SMALL NORM

Peter Borwein

Simon Fraser University Centre for Constructive and Experimental Mathematics

http://www.cecm.sfu.ca/~pborwein

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

We survey a number of old and difficult problems all of which involve finding polynomials with integer coefficients with small norm.

These problems are unsolved and most are at least 35 years old.

- Section I: Integer Chebyshev Problems

- Section II: Prouhet-Tarry-Escott Problems.

- Section III: Littlewood Type Problems.

I – 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

$$\Omega_N[\alpha, \beta] :$$

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

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.

Since

$$\Omega[a,b] \leq \Omega_n[a,b]$$

for any particular n upper bounds can be derived computationally from the computation of any specific $\Omega_n[a,b]$. So if

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

We have

Proposition 1.1. *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

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

and hence

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

Refinements on the method

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

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 the limit (provided $a_N = 1$) gives the usual transfinite diameter. From the unrestricted case we have the obvious inequality

$$\Omega_n[a,b] \geq 2^{1/n}\frac{b-a}{4},$$

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 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 proves these polynomials irreducible. If follows now from Lemma 1.3 that

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

Montogomery conjectured 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 $\Omega[0,1] = s$. Chudnovsky further conjectured that the minimal s arises from the Gorshkov–Wirsing polynomials and so s would equal $(2.3768417062\ldots)^{-1}$.

We show that

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

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

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

Habsieger and Salvy show that Integer Chebyshev polynomials on $[0,1]$ need not have all real roots. The first non totally real factor occurs for $n = 70$.

This is a non-trivial computation and is quite likely NP hard.

II. Ideal Solutions of the Prouhet-Tarry-Escott Problem

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 $[\alpha_1, \ldots, \alpha_N]$ and $[\beta_1, \ldots, \beta_N]$ so that

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

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. 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.)

Suppose

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

We write the solutions 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.

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).

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).*

There are only two of size $N = 9$ known.

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

and

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

Variations on the Theme.

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* $p_N \in \mathcal{Z}[x]$ *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 combinatorial argument shows that

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

is possible for all N.

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 observed that if

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

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

$$l_1(p) = 0((\log N)N^2)$$

is possible but this is all that is known (Hua).

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 be interesting.

Problem of Erdős 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	$\|p\|_{l_1}$	$\{\alpha_1, \dots, \alpha_N\}$
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	$\{1, \dots, 9, 11, 13, 17\}$
13	48	$\{1, \dots, 9, 11, 13, 17, 19\}$

For $N := 1, 2, 3, 4, 5, 6, 8$ this provides a ideal solution of the Prouhet-Tarry-Escott problem. For $N = 7, 9, 10, 11$. that these kind of products cannot solve the Prouhet-Tarry-Escott problem. For $N = 7, 9, 10$ the above examples are provably optimal.

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

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

Erdős and Szekeres conjecture that E_N^* grows fairly rapidly.

Conjecture 2.6. *For any* K

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

for N *sufficiently large.*

III - 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

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

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

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 $C_1 \le 1$ and $C_2 \ge 1$.

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:

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

and

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

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

These have all coefficients ± 1 and are of degree $2^n - 1$. From

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

we have for all z of modulus 1

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

and

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

This conjecture is complemented by a conjecture of Erdős.

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 shows that if the polynomials are allowed to have complex coefficients of modulus 1 then "locally flat" polynomials exist and indeed that it is possible to make C_1 and C_2 asymptotically arbitrarily close to 1. Another striking result due to Beck proves that "locally flat" polynomials exist from the class of polynomials of degree n whose coefficients are 400th roots of unity.

Because of the monotonicity of the L_p norms it is relevant to rephrase Erdős' conjecture in other norms. Newman and Byrnes speculate 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 Erdős' conjecture above. Here

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

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.

Computations suggest that the 7/6 constant may be too large. Although it is conjectured to be best possible.

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

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

There is a large literature on this problem sometimes called the “Merit Factor” problem.

A very interesting question is how to compute the minimal L_4 Littlewood polynomials (say up to degree 200).

A Barker polynomial

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

with each $a_k \in \{-1, +1\}$ so that

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

satisfies $c_0 = n + 1$ and

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

Here

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

If $p(z)$ is a Barker polynomial of degree n then

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

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

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

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

It is conjectured that no Barker polynomials exist for $n > 12$.

We computed expected L_p norm of Littlewood polynomials (B and Lockhart). 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 for derivatives

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

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

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

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

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.

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 $M(p) = 1.176280818259917 50\ldots$. 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.

Mahler raised the problem of the maximum Mahler measure.

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 one Erdős conjecture.

Zeros of Littlewood Polynomials.

Theorem 3.7. *Every polynomial* p_n

$$p_n(x) = \sum_{j=0}^{n} a_j x^j, \qquad |a_0| = 1\,, \quad |a_j| \leq 1\,,$$

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

Theorem 3.8. *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.

Thus 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 3.8. *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 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 3.9. *Prove or disprove that there is an absolute constant c such that every polynomial $p \in \mathcal{L}_n$ can have at most $c \log n$ zeros at 1.*