# SOME SMALL NORM PROBLEMS

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

## Littlewood Type Problems

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 literature

**Conjecture.** *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 “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

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

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

These have all coefficients $\pm 1$ 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.** *The constant $C_2$ in Littlewood's conjecture 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 "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 "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.

**Problem.** *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*

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

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

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

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

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

This is even weaker than the weak form of the preceding problem.

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

We can compute the 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

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

## Explicit Merit Calculations

Our purpose here is to give explicit formulas for the $L_4$ norms (on the boundary of the unit disc) and hence, also the merit factors of various polynomials that are closely related to the Fekete polynomials.

As usual the $L_\alpha$ norm on the boundary of the unit disc is defined by

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

The $L_4$ norm of a polynomial is particularly easy to work with because it can be computed as the square root of the $L_2$ norm of $p(z)\overline{p(z)}$ and hence, computes exactly as the fourth root of the sum of the squares of the coefficients of $p(z)\overline{p(z)}$. In contrast, the supremum norm or other $L_p$ norms, where $p$ is not an even integer, are computationally difficult.

Let $q$ be a prime number and let $\left(\frac{\cdot}{q}\right)$ be the Legendre symbol.

The Fekete polynomials are defined by

$$f_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

and the closely related polynomials

$$F_q(z) := 1 + f_q(z) = 1 + \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k.$$

The half–Fekete polynomials are defined by

$$G_q(z) := \sum_{k=1}^{(q-1)/2} \left(\frac{k}{q}\right) z^k.$$

If we cyclically permute the coefficients of $f_q$ by about $q/4$ places we get an example of Turyn's which we denote by

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k+[q/4]}{q}\right) z^k$$

where $[\cdot]$ denotes the nearest integer, and we denote the general shifted Fekete polynomials by

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

Note that $R$ has one coefficient that is zero (from the permutation of the constant term in $f$). For example

$$f_{11} := -x^{10} + x^9 - x^8 - x^7 - x^6 + x^5 + x^4 + x^3 - x^2 + x$$

and

$$R_{11} := -x^{10} + x^9 - x^7 + x^6 - x^5 - x^4 - x^3 + x^2 + x + 1.$$

The explicit formulas involve the class number of the imaginary quadratic field of $\mathbb{Q}(\sqrt{-d})$ which is denoted by $h(-d)$. For any odd prime $d$ it can be computed as

$$h(-d) = \lambda_d \sum_{k=1}^{(d-1)/2} \left(\frac{k}{d}\right)(-1)^k = \lambda_d G_d(-1)$$

where

$$\lambda_d := \begin{cases} 1 & \text{if} \quad d \equiv 1, 7 \pmod 8, \\ -1/3 & \text{if} \quad d \equiv 3 \pmod 8, \\ -1 & \text{if} \quad d \equiv 5 \pmod 8. \end{cases}$$

For primes $d \equiv 3 \pmod 4$ it can also be computed as

$$h(-d) = -\frac{f_d'(1)}{d} = -\frac{1}{d} \sum_{k=1}^{d-1} \left(\frac{k}{d}\right) k$$

(this sum is 0 for $d \equiv 1 \pmod 4$).

There are two natural measures of smallness for the $L_4$ norm of a polynomial $p$. One is the ratio of the $L_4$ norm to the $L_2$ norm, $\|p\|_4/\|p\|_2$. The other (equivalent) measure is the merit factor, defined by

$$\mathrm{MF}(p) = \frac{\|p\|_2^4}{\|p\|_4^4 - \|p\|_2^4}.$$

Littlewood polynomials are the set

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

The $L_2$ norm of any element of $\mathcal{L}_{n-1}$ is $\sqrt{n}$ and this is, of course, a lower bound for the $L_4$ norm.

The expected $L_4$ norm of an element of $\mathcal{L}_n$ is is $2^{1/4}\sqrt{n}$. The expected merit factor is thus 1.

The $\{R_q\}$ above are a sequence with asymptotic merit factor 6. Golay gives a heuristic argument for this observation of Turyn's and this is proved rigorously by T. Høholdt and H. Jensen

The Fekete polynomials themselves have asymptotic merit factor 3/2 and different amounts of cyclic permutations can give rise to any asymptotic merit factor between 3/2 and 6.

Golay speculates that 6 may be the largest possible asymptotic merit factor. He writes "the eventuality must be considered that no systematic synthesis will ever be found which will yield higher merit factors."

Newman and Byrnes, apparently independently, make a similar conjecture. As do Høholdt and Jensen.

Computations by a number of people on polynomials up to degree 200 are equivocal. See the web page of A. Reinholz at http://borneo.gmd.de/~andy/ACR.html.

The Fekete polynomial $f_q$ has modulus $\sqrt{q}$ at each $q$th root of unity (as does $f_q^t$) and one might hope that they also satisfy the upper bound in Littlewood's conjecture but Montgomery shows that this is not the case.

Littlewood's conjecture is that it is possible to find $p_n \in \mathcal{L}_{n-1}$ so that

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

for all $z$ of modulus 1 and for two constants $C_1, C_2$ independent of n.

## 2. Results

**Theorem.** *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*

$$\gamma_q := \begin{cases} 0 & \textit{if} \quad q \equiv 1 \pmod 4, \\ 12(h(-q))^2 & \textit{if} \quad q \equiv 3 \pmod 4. \end{cases}$$

**Theorem.** *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*

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

*and*

$$\gamma_q := \begin{cases} h(-q)(h(-q) - 4) & \text{if} \quad q \equiv 1, 5 \pmod 8, \\ 12(h(-q))^2 & \text{if} \quad q \equiv 3 \pmod 8, \\ 0 & \text{if} \quad q \equiv 7 \pmod 8. \end{cases}$$

Montgomery shows that the maximum modulus of $f_q(z)$ at the $2q$th root of unity is at least $\frac{2}{\pi}\sqrt{q} \log \log q$.

**Theorem.** *Let*

$$L_n(z) := \sum_{k=0}^{n-1} e^{\frac{k(k+1)\pi i}{n}} z^k$$

$$\|L_n\|_4^4 = n^2 + \frac{2n^{3/2}}{\pi} + \delta_n \frac{n^{1/2}}{3} + O(n^{-1/2})$$

*where*

$$\delta_n := \begin{cases} -2 & \textit{if} \quad n \equiv 0, 1 \pmod 4, \\ 1 & \textit{if} \quad n \equiv 2, 3 \pmod 4. \end{cases}$$

The above example of Littlewoods depends on the asymptotic series for

$$\sum_{j=1}^{n-1} \frac{sin^2(j^2\pi/n)}{sin^2(j\pi/n)}$$

because, in the above notation,

$$\|L_n\|_4^4 = n^2 + 2\sum_{j=1}^{n-1} \frac{sin^2(j^2\pi/n)}{sin^2(j\pi/n)}.$$

Let $q$ be a prime and $\chi$ be a non-principal character mod $q$. Let

$$f_\chi^t(z) := \sum_{n=0}^{q-1} \chi(n+t) z^n$$

for $1 \le t \le q$ be the character polynomial associated to $\chi$ (cyclically permuted $t$ places).

**Theorem.** *For any non-principal and non-real character $\chi$ modulo $q$ and $1 \le t \le q$, we have*

$$\|f_\chi^t(z)\|_4^4 = \frac{4}{3} q^2 + O(q^{3/2} \log^2 q)$$

*where the implicit constant is independent of $t$ and $q$. Here $\| \cdot \|_4$ denotes the $L_4$ norm on the unit circle.*

It follows from this that all cyclically permuted character polynomials associated with non-principal and non-real characters have merit factors that approach 3.

# Problem of Erdős and Szekeres (1958)

**Conjecture (Wright et al).** *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*

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

In general how small can the $l_1$ norm be. This is a problem with many interesting variants.

Note that the degree of the solution is not the issue. The problem is in terms of the size of the zero at 1.

An entirely equivalent form of the above conjecture asks to find two distint sets of integers $[\alpha_1, \ldots, \alpha_N]$ and $[\beta_1, \ldots, \beta_N]$ so that

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

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 (Erdős and Szekeres).** *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.** *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.** *For any $K$*

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

*for $N$ sufficiently large.*

Erdős and G. Szekeres showed that subexponential growth is possible.

The best upper bound to date for $E_N^*$ is that of Belov and Konyagin

$$E_N^* \leq \exp(O((\log n)^4)).$$

Previously Atkinson and Dobrowolski proved the upper bound of

$$\exp(O(n^{\frac{1}{2}}\log n))$$

then Odlyzko proved the upper bound of

$$\exp(O(n^{\frac{1}{3}}(\log n)^{\frac{4}{3}}))$$

and Kolountzakis proved the upper bound $\exp(O(n^{1/3}\log n))$