# PAUL ERDŐS AND POLYNOMIALS

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

There is an explicit formula for the $L_4$ norm of an example of Turyn's that is constructed by cyclically permuting the first quarter of the coefficients of $f_q$. This is the sequence that has the largest known asymptotic merit factor. Explicitly,

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

where $[\cdot]$ denotes the nearest integer, satisfies

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

where

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

Here $h(-q)$ is the class number of $\mathbb{Q}(\sqrt{-q})$

A mathematician named Erdős

Eccentric, perhaps even wierdős

Could never endeavour

No matter how clever

To publish a paper in Kurdős

# 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

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

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.

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

# References

P. Erdős and G. Szekeres, *On the product* $\prod_{k=1}^{n}(1-z^{a_k})$, Publications de L'Institut Math. **12** (1952), 29-34.

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

P. Borwein and C. Ingalls, *The Prouhet, Tarry, Escott problem*, Ens. Math. **40** (1994), 3–27.

A.S. Belov and S.V. Konyagin, *On estimates for the constant term of a nonnegative trigonometric polynomial with integral coefficients*, Mat Zametki **59** (1996), 627–629.

# 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

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

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 (Littlewood).** *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

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

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

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 (Erdős 1962).** *The constant $C_2$ in the conjecture of Littlewood 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 1200th 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.

There is an explicit formula for the $L_4$ norm of an example of Turyn's that is constructed by cyclically permuting the first quarter of the coefficients of $f_q$. This is the sequence that has the largest known asymptotic merit factor. Explicitly,

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

where $[\cdot]$ denotes the nearest integer, satisfies

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

where

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

Here $h(-q)$ is the class number of $\mathbb{Q}(\sqrt{-q})$

**Conjecture.** *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

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

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 Erdős conjecture and is still open.

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

Mahler raised the problem of the maximum Mahler measure.

**Problem.** *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 also a weak form of the one Erdős conjecture.

# References

J. Beck, *The modulus of polynomials with zeros on the unit circle: A problem of Erdös*, Annals of Math **134** (1991), 609-651.

P. Borwein, *Some Old Problems on Polynomials with Integer Coefficients*, Proceedings of the Ninth Conference on Approximation Theory, 1998.

P. Erdős, *An inequality for the maximum of trigonometric polynomials*, Annales Polonica Math. **12** (1962), 151–154.

J-P. Kahane, *Sur les polynômes á coefficients unimodulaires*, Bull. London Math. Soc **12** (1980), 321–342.

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

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

# An Arc Length Problem

In 1958 Erdős, Herzog and Piranian raised a number of problems concerned with the lemniscate

$$E_n := E_n(p) := \{z \in \mathbb{C} : |p(z)| = 1\}$$

where $p$ is a monic polynomial of degree $n$, so

$$p(z) := \Pi_{i=1}^{n}(z - \alpha_l) \qquad \alpha_i \in \mathbb{C}.$$

Problem 12, conjectures that the maximum length of $E_n$ is achieved for

$$p(z) := z^n - 1.$$

This is of length $2n + 0(1)$.

This problem has been re-posed by Erdős several times, including at the Budapest meeting honouring his 80th birthday. It now carries with it a cash prize from Erdős of \$250.

Up to 1995 the best partial to date was due to Pommerenke who showed that the maximum length is at most $74n^2$. We improved this in 1995 to derives an upper bound of $8\pi en$, which at least gives the correct rate of growth.

**Theorem.** *Let* $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. *Then the length of*

$$E_n := \{z \in \mathbb{C} : |\Pi_{i=1}^n (z - \alpha_i)| = 1\}$$

*is at most* $8\pi en \, (\leq 69n)$.

The proof relies on two classical theorems.

**Cartan's Lemma.** *If* $p(z) := \prod_{i=1}^{n}(z - \alpha_i)$ *then the inequality*

$$|p(z)| > 1$$

*holds outside at most* $n$ *circular discs, the sum of whose radii is at most* $2e$.

**Poincaré's Formula.** *Let* $\Gamma$ *be a rectifiable curve contained in* $\mathbb{S}$ *(the Riemann sphere). Let* $v(\Gamma, x)$ *denote the number of times that a great circle consisting of points equidistant from the antipodes* $\pm x$ *intersects* $\Gamma$. *Then the length of* $\Gamma$, $L_{\mathbb{S}}(\Gamma)$, *is given by*

$$L_{\mathbb{S}}(\Gamma) = \frac{1}{4}\int_{\mathbb{S}} v(\Gamma, x)dx$$

*where* $dx$ *is area measure on* $\mathbb{S}$.

Pommerenke shows that if the roots in the Theorem are all real then the length is at most $4\pi$.

Pommerenke also shows that if the set $E_n$ is connected then the length is at least $2\pi$, with equality only for $z^n$.

When $E_n$ is connected one can find a disc of radius 2 that contains it. So in this case the length of $E_n$ is at most $4\pi n$.

One of the results of Erdős, Herzog, and Piranian is:

The infimum of $m(E(f))$ is 0, where the infimum is taken over all monic polynomials $f$ with all their zeros in the closed unit disk ($n$ varies and $m$ denotes the two-dimensional Lebesgue measure).

With the related result:

Let $F$ be a closed set of transfinite diameter less than 1. Then there exists a positive number $\rho(F)$ such that, for every monic polynomial whose zeros lie in $F$, the set $E(f)$ contains a disk of radius $\rho(F)$.

# References

P. Borwein, *The arc length of the lemniscate* $|p(z)| = 1$, Proc. Amer. Math. Soc. **123** (1995), 797–799.

Erdős, P., F. Herzog and G. Piranian, *Metric Properties of Polynomials*, J. D'Analyse Math. **6** (1958), 125–148.

Erdős, P., *Extremal Problems on Polynomials, in Approximation Theory II, Academic Press* (1976), 347–355.

Pommerenke, Ch., *On metric properties of complex polynomials*, Mich. Math. J. **8** (1961), 97–115.

## Some Inequalities

Let $\mathcal{P}_n$ denote the algebraic polynomials of degree at most $n$ with real coefficients.

**Markov's Inequality.** *The inequality*

$$\|p'\|_{L^\infty[-1,1]} \le n^2 \|p\|_{L^\infty[-1,1]}$$

*holds for every* $p \in \mathcal{P}_n$.

**Bernstein Inequality.** *The inequality*

$$|p'(y)| \le \frac{n}{\sqrt{1-y^2}} \|p\|_{L^\infty[-1,1]}$$

*holds for every* $p \in \mathcal{P}_n$ *and* $y \in (-1,1)$.

It had been observed by Bernstein that Markov's inequality for monotone polynomials is not essentially better than for arbitrary polynomials. Bernstein proved that *if $n$ is odd, then*

$$\sup_p \frac{\|p'\|_{L^\infty[-1,1]}}{\|p\|_{L^\infty[-1,1]}} = \left(\frac{n+1}{2}\right)^2 ,$$

*where the supremum is taken over all $0 \neq p \in \mathcal{P}_n$ that are monotone on $[-1,1]$.*

This is surprising, since one would expect that if a polynomial is this far away from the "equioscillating" property of the Chebyshev polynomial, then there should be a more significant improvement in the Markov inequality.

In the short paper in the Annals in 1940. Erdős gave a class of restricted polynomials for which the Markov factor $n^2$ improves to $cn$. He proved that there is an absolute constant $c$ such that

$$|p'(y)| \le \min\left\{\frac{c\sqrt{n}}{(1-y^2)^2}, \ \frac{en}{2}\right\} \|p\|_{L^\infty[-1,1]}$$

for every polynomial of degree at most $n$ that has all its zeros in $\mathbb{R} \setminus (-1,1)$.

Generalizations of the above Markov- and Bernstein-type inequality of Erdős have been extended in many directions by many people including Lorentz, Scheick, Szabados, Varma, Máté, Rahman, Govil, Erdélyi, PB and others.

Many of these results are contained in the following,

*There is an absolute constant $c$ such that*

$$|p'(y)| \leq$$

$$c \min\left\{\sqrt{\frac{n(k+1)}{1-y^2}},\ \ n(k+1)\right\} \|p\|_{L^\infty[-1,1]}$$

*for every polynomial $p$ of degree at most $n$ with real coefficients that has at most $k$ zeros in the open unit disk.*

Another attractive result concerns the growth of polynomials in the complex plane. Specifically

$$|p(z)| \leq |T_n(z)| \cdot \max_{x \in [-1,1]} |p(x)|$$

for every polynomial $p \in \mathcal{P}_n$ and for every $z \in \mathbb{C}$ with $|z| \geq 1$. Here $T_n$ denotes the usual Chebyshev polynomial of degree $n$.

Borwein, P.B., & T. Erdélyi, *Sharp Markov-Bernstein type inequalities for classes of polynomials with restricted zeros*, Constr. Approx. **10** (1994), 411–425.

Erdős, P., *On extremal properties of the derivatives of polynomials*, Ann. of Math. **2** (1940), 310–313.

## Distribution of Zeros

Erdős and Turán established a number of results on the spacing of zeros of orthogonal polynomials with respect to a weight w.

Let

$$(1 >)\, x_{1,n} > x_{2,n} > \cdots > x_{n,n}\, (> -1)$$

be the zeros of the associated orthonormal polynomials $p_n$ in decreasing order and let

$$x_{\nu,n} = \cos\theta_{\nu,n}\,, \qquad 0 < \theta_{\nu,n} < \pi\,,$$

Then there is a constant $K$ such that

$$\theta_{\nu+1,n} - \theta_{\nu,n} < \frac{K \log n}{n}.$$

This result has been extended by various people in many directions.

The following result of Erdős and Turán is especially attractive.

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

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

This result was originally due to Schur. Erdős and Turán rediscovered it with a short proof.

In this same paper Erdős and Turán discuss the angular distribution of the zeros of polynomials in terms of the size of the coefficients.

The result says that "if the middle coefficients of a polynomial are not too large compared with the extreme ones" then the angular distribution of the zeros is uniform.

This has been further explored by Blatt, Kroó, Peherstorfer and others.

# References

Erdős, P., & P. Turán, *On the distribution of the fundamental points of Lagrange and Hermite interpolation*, Ann. of Math. **39** (1938), 703–724.

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

# Cyclotomic Polynomials

The cyclotomic polynomial $C_n$ is defined as the monic polynomial whose zeros are the primitive $n$th roots of unity. So

$$C_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}\,.$$

For $n < 105$, all coefficients of $C_n$ are $\pm 1$ or 0. For $n = 105$, the coefficient 2 occurs for the first time. Denote by $A_n$ the maximum over the absolute values of the coefficients of $C_n$.

Schur proved that

$$\limsup A_n = \infty.$$

Emma Lehmer proved that, for infinitely many $n$,

$$A_n > cn^{1/3}.$$

Erdős proved that *for every $k$,*

$$A_n > n^k$$

*for infinitely many $n$.*

This is implied by his even sharper theorem to the effect that

$$A_n > \exp\left[c\,(\log n)^{4/3}\right]$$

*for $n = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p_k$ with $k$ sufficiently large.*

Many recent improvements and generalizations of this are due to Maier

## References

Erdös, P., *On the coefficients of the cyclotomic polynomials*, Bull AMS **52** (1946), 179–183.