PAUL ERDŐS AND POLYNOMIALS

PETER BORWEIN

ABSTRACT. The paper focusses on some of the lovely questions that Erdős raised and answered about polynomials. Some of the problems are analytic and involve inequalities for polynomials or the location of zeros. The rest have some number theoretic component. These problems are all distinguished by having had significant work done on them but none of them are completely solved.

Some of the specific problems we will mention are: The Problem of Erdős and Szekeres on the growth of certain products; Erdős' conjecture related to flat polynomials and Littlewood's other conjecture; Erdős' work on polynomial inequalities and some of his results with Turán on the distribution of zeros of polynomials; a problem on the length of the lemniscates where polynomials have constant modulus; a problem on the growth of coefficients of cyclotomic polynomials.

1. INTRODUCTION

The work of Paul Erdős that we unsystematically survey here lives at the interface of analysis and number theory. The specific problems belong to which ever subdiscipline cares to claim them. The unifying theme is that all of the problems concern polynomials is some way. The problems raised are all decades old and despite considerable attention have all resisted complete solution. The particular choice of problems is eclectic and for the most part represents my taste in Erdős' problems.

The first two problems are elaborated on in [5].

PROBLEM OF ERDŐS AND SZEKERES (1958) [17]

The following conjecture is an old plum called the "Prouhet-Tarry-Escott problem". It holds for $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ and 12 and otherwise very little else is known [8]. With the exception of the size 12 solution these were all discovered by 1940 without the aid of computers.

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

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

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

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

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

This equivalence is an easy exercise in Newton's equations. The later form is the usual Diophantine form in which the problem arises and is stated. The recent size 12 solution due to Chen Shuwen is given by the two sets

$$[0, 11, 24, 65, 90, 129, 173, 212, 237, 278, 291, 302]$$

and

$$[3, 5, 30, 57, 104, 116, 186, 198, 245, 272, 297, 299].$$

Often the size of the problem is given as N-1 corresponding to the number of equations the sets satisfy not the size of the solution sets. This necessitates some care in reading the literature.

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

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

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 [17]). *Minimize over $\{\alpha_1, \ldots, \alpha_N\}$*

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

Call this minimum E_N^*.

The following table gives the smallest known l_1 norm examples 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	$\{1, \ldots, 9, 11, 13, 17, 19\}$

For $N := 1, 2, 3, 4, 5, 6, 8$ this provides a 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. This is due to Roy Maltby [25].

Conjecture. *With the exception of $N = 1, 2, 3, 4, 5, 6$ and 8*

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

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

Conjecture (Erdős and Szekeres [17]). *For any K*

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

for N sufficiently large.

Erdős and Szekeres showed that subexponential growth is possible. The best upper bound to date for E_N^* is that of Belov and Konyagin [2]

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

Previously Atkinson and Dobrowolski proved the upper bound of

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

then Odlyzko [27] gave the upper bound of

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

and Kolountzakis proved the upper bound

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

Some Problems of Erdős and Littlewood

These problems are about polynomials with coefficients in the set $\{+1, -1\}$. We call this set Littlewood polynomials and denote then by $\mathcal{L}_n$. 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 (Littlewood). *For each n there exists $p_n \in \mathcal{L}_n$ so that*

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

for all complex z of modulus 1. The positive constants C_1 and C_2 are independent of n.

Polynomials like this are called "flat". The L_2 norm of a polynomial from $\mathcal{L}_n$ is exactly $\sqrt{n+1}$ and it follows that the constants must satisfy $C_1 \leq 1$ and $C_2 \geq 1$. Littlewood [22] computed extensively on this problem (on all such polynomials up to degree twenty). Subsequent large scale computations by Odlyzko 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.

There is a related conjecture of Erdős [14].

Conjecture (Erdős). *The constant C_2 in conjecture 1 is greater than $1 + \delta$ where $\delta > 0$..*

This is also still open. Though a remarkable result of Kahane's [21] 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 [Bec-91] proves that "flat" polynomials exist from the class of polynomials of degree n whose coefficients are 1200th roots of unity.

It is natural, because of the monotonicity of the L_p norms, to reformulate Erdős' conjecture in other norms. Various people have conjectured that

$$||p||_4^4 \geq (1 + \delta)n^2$$

for $p \in \mathcal{L}_n$ and n sufficiently large. This would imply Erdős' conjecture above. Here and throughout $||q||_p$ 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 an example due to Turyn [20] which he conjectures to be asymptotically best possible. In [6] we derived closed formulae for the merit factors of polynomials related to the Fekete polynomials. So, for example, for q an odd prime,

$$\|f_q\|_4^4 := \frac{5q^2}{3} - 3q + \frac{4}{3} - 12(h(-q))^2$$

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

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

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

This problem of finding Littlewood polynomials of minimal L_4 norm has a considerable literature. The above problem is stated in [26]. See also [20]. The engineering literature calls this the "merit factor" problem. Even computing the minimum for relatively small degrees (say up to 100) is an open, difficult and interesting combinatorial optimization question.

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

$$|c_j| \leq 1, \ j \neq 0.$$

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 tha above problem.

It has been conjectured for decades that no Barker polynomials exist for $n > 12$. See [29] for more on Barker polynomials and a proof of the nonexistence of self inversive Barker polynomials. Turyn showed that no even degree Barker polynomials exist for $n > 12$ (and indeed none exist for any degree between 12 and 1600).

The expected L_p norms of Littlewood polynomials and their derivatives are computed in [9]. So for random $q_n \in \mathcal{L}_n$

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

Problem. *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 concerning the minimum Mahler measure ($M(p)$) of non-cyclotomic polynomials. It seems likely, however, that the answer to the above question is positive. Mahler [23] raised the problem of finding the maximum Mahler measure over the polynomials of degree n with coefficients $\{0, +1, -1\}$.

Problem (Mahler). *Is there 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. The non-existence of a sequence, as in the above problem, implies Erdős' conjecture.

An Arc Length Problem

In 1958 Erdős, Herzog and Piranian [16] raised a number of problems concerning the the lemniscate

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

where p is a monic polynomial of degree n, so

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

Problem 12 of [16], 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 [6] 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 Γ 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 Γ. Then the length of Γ, $L_{\mathbb{S}}(\Gamma)$, is given by*

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

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

Eremenko and Hayman (this proceedings) have made some interesting recent progress on this problem including showing that the extremal lemniscate in this problem is connected.

Pommerenke shows that if the roots in the Theorem are all real then the length is at most 4π. Pommerenke also shows that if the set E_n is connected then the length is at least 2π, with equality only for z^n.

Pommerenke also shows that 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 $4\pi n$ and with the results of Eremenko and Hayman one gets $4\pi n$ in the general case. Though in fact Eremenko and Hayman get the better bound of $9.173n$.

One of the results of Erdős, Herzog, and Piranian [16] 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).

They also have 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 $\rho(F)$.

Some Inequalities

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

Markov's Inequality. *The inequality*

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

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

Bernstein Inequality. *The inequality*

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

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

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

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, and others (see [7]).

Many of these results are contained in the followingresult which may be found in [7].

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.

However in most cases the exact results, with constants, are still open.

Another attractive result, rediscovered by Erdős, 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.

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 [18] 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 [7] the following refinement of the above theorem is given.

Theorem. *Every polynomial p_n of the form $p_n(x) = \sum_{j=0}^{n} a_j x^j, |a_0| = 1, |a_j| \leq 1$, has at most $\lfloor \frac{16}{7}\sqrt{n} \rfloor + 4$ zeros at 1.*

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 Andrievskii, Blatt, Kroó, Peherstorfer and others (see, for example, [1]).

CYCLOTOMIC POLYNOMIALS

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

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

Here μ is the Möbius function. For $n < 105$, all coefficients of C_n are ± 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
$$\limsup A_n = \infty$$
and Emma Lehmer proved that, for infinitely many n,

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

Erdős [13] 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 $n = 2 \cdot 3 \cdot 5 \cdots p_k$ with k sufficiently large.

Many recent improvements and generalizations of this are due to Maier [24].

References

1. V. Andrievskii and H-P Blatt, *Erdős-Turán type theorems on quasiconformal curves and arcs*, J. Approx. Theory **97** (1999), 334-365.

2. 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.

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

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

5. P. Borwein, *Some Old Problems on Polynomials with Integer Coefficients*, in Approximation Theory IX, ed. C. Chui and L. Schumaker, Vanderbilt University Press (1998), 31–50.

6. P. Borwein and S. Choi, *Explicit merit factor formulae for Fekete and Turyn Polynomials.*, Submitted.

7. P. Borwein and T. Erdélyi'elyi, *Polynomials and Polynomial Inequalities*, Springer-Verlag, New York, 1995.

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

9. P. Borwein and R. Lockhart, *The expected L_p norm of random polynomials.*, Proc. Amer. Math. Soc. (to appear).

10. D. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comput. **66** (1977), 1697–170.

11. J. S. Byrnes and D. J. Newman, *Null steering employing polynomials with restricted coefficients*, IEEE Trans. Antennas and Propagation (1988), 1–3.

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

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

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

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

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

17. 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.

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

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

20. T. Hoholdt and H. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Transactions on Information Theory (1988), 161–164.

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

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

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

24. H. Maier, *The size of the coefficients of cyclotomic polynomials*, Progr. Math. **139** (1996), 633–639.

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

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

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

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

29. B.Saffari, *Barker sequences and Littlewood's "two-sided conjectures" on polynomials with ±1 coefficients*,

DEPARTMENT OF MATHEMATICS AND STATISTICS, SIMON FRASER UNIVERSITY, BURNABY, B.C., CANADA V5A 1S6
pborwein@cecm.sfu.ca