COPPERSMITH-RIVLIN TYPE INEQUALITIES AND THE ORDER OF VANISHING OF POLYNOMIALS AT 1

Tamás Erdélyi

Texas A&M University

1. Introduction and Notation

In [B-99] and [B-13] we (P. Borwein, T.E., and G. Kós) examined a number of problems concerning polynomials with coefficients restricted in various ways. We were particularly interested in how small such polynomials can be on $[0,1]$. For example, we proved that there are absolute constants $c_1 > 0$ and $c_2 > 0$ such that

$$e^{-c_1\sqrt{n}} \leq \min_{0 \neq Q \in \mathcal{F}_n} \left\{ \max_{x \in [0,1]} |Q(x)| \right\} \leq e^{-c_2\sqrt{n}}$$

for every $n \geq 2$, where $\mathcal{F}_n$ denotes the set of all polynomials of degree at most n with coefficients from $\{-1,0,1\}$.

Littlewood considered minimization problems of this variety on the unit disk. His most famous, now solved, conjecture was that the L_1 norm of an element $f \in \mathcal{F}_n$ on the unit circle grows at least as fast as $c \log N$, where N is the number of non-zero coefficients in f and $c > 0$ is an absolute constant.

When the coefficients are required to be integers, the questions have a Diophantine nature and have been studied from a variety of points of view.

One key to the analysis is a study of the related problem of giving an upper bound for the multiplicity of the zero these restricted polynomials can have at 1. In [B-99] and [B-13] we answer this latter question precisely for the class of polynomials of the form

$$Q(x) = \sum_{j=0}^{n} a_j x^j \,,$$

$$|a_j| \leq 1 \,, \quad a_j \in \mathbb{C} \,, \quad j = 1, 2, \ldots, n \,,$$

with fixed $|a_0| \neq 0$.

Various forms of these questions have attracted considerable study, though rarely have precise answers been possible to give. Indeed, the classical, much studied, and presumably very difficult problem of Prouhet, Tarry, and Escott rephrases as a question of this variety. (Precisely: what is the maximal vanishing at 1 of a polynomial with integer coefficients with l_1 norm $2n$? It is conjectured to be n.)

For $n \in \mathbb{N}$, $L > 0$, and $p \geq 1$ let $\kappa_p(n, L)$ be the largest possible value of k for which there is a polynomial $Q \neq 0$ of the form

$$Q(x) = \sum_{j=0}^{n} a_j x^j \,, \qquad a_j \in \mathbb{C}\,,$$

$$|a_0| \geq L \left(\sum_{j=1}^{n} |a_j|^p \right)^{1/p} ,$$

such that $(x-1)^k$ divides $Q(x)$.

For $n \in \mathbb{N}$ and $L > 0$ let $\kappa_\infty(n, L)$ the largest possible value of k for which there is a polynomial $Q \neq 0$ of the form

$$Q(x) = \sum_{j=0}^{n} a_j x^j \,, \qquad a_j \in \mathbb{C}\,,$$

$$|a_0| \geq L \max_{1 \leq j \leq n} |a_j|\,,$$

such that $(x-1)^k$ divides $Q(x)$.

In [B-99] we proved that there is an absolute constant $c_3 > 0$ such that

$$\min\left\{\frac{1}{6}\sqrt{(n(1-\log L)} - 1\,, n\right\} \leq \kappa_\infty(n, L)$$

$$\leq \min\left\{c_3\sqrt{n(1-\log L)}\,, n\right\}$$

for every $n \in \mathbb{N}$ and $L \in (0, 1]$. However, we were far from being able to establish the right result in the case of $L \geq 1$. In [B-13] we proved the right order of magnitude of $\kappa_\infty(n, L)$ and $\kappa_2(n, L)$ in the case of $L \geq 1$. Our results in [B-99] and [B-13] sharpen and generalize results of Schur [Sch-33], Amoroso [A-90], Bombieri and Vaaler [B-87], and Hua [H-82] who gave versions of this result for polynomials with integer coefficients. Our results in [B-99] have turned out to be related to a number of recent papers from a rather wide range of research areas.

For $n \in \mathbb{N}$, $L > 0$, and $q \geq 1$ let $\mu_q(n, L)$ be the smallest value of k for which there is a polynomial of degree k with complex coefficients such that

$$|Q(0)| > \frac{1}{L} \left(\sum_{j=1}^{n} |Q(j)|^q \right)^{1/q} .$$

For $n \in \mathbb{N}$ and $L > 0$ let $\mu_\infty(n, L)$ be the smallest value of k for which there is a polynomial of degree k with complex coefficients such that

$$|Q(0)| > \frac{1}{L} \max_{j \in \{1,2,\dots,n\}} |Q(j)| .$$

It is a simple consequence of Hölder's inequality (see Lemma 3.6) that

$$\kappa_p(n, L) \leq \mu_q(n, L)$$

whenever $n \in \mathbb{N}$, $L > 0$, $1 \leq p, q \leq \infty$, and

$$1/p + 1/q = 1 .$$

In [E15] we find the the size of $\kappa_p(n, L)$ and $\mu_q(n, L)$ for all $n \in \mathbb{N}$, $L > 0$, and $1 \le p, q \le \infty$. The result about $\mu_\infty(n, L)$ is due to Coppersmith and Rivlin, [C-92], but our proof presented in [E15] is completely different and much shorter even in that special case.

2 New Results

Theorem 2.1. *Let* $p \in (1, \infty]$ *and* $q \in [1, \infty)$ *satisfy* $1/p + 1/q = 1$*. There are absolute constants* $c_1 > 0$ *and* $c_2 > 0$ *such that*

$$\sqrt{n}(c_1 L)^{-q/2} - 1 \le \kappa_p(n, L) \le \mu_q(n, L) \le \sqrt{n}(c_2 L)^{-q/2} + 2$$

for every $n \in \mathbb{N}$ *and* $L > 1/2$*, and*

$$c_3 \min\left\{\sqrt{n(-\log L)}, n\right\} \le \kappa_p(n, L) \le \mu_q(n, L)$$

$$\le c_4 \min\left\{\sqrt{n(-\log L)}, n\right\} + 4$$

for every $n \in \mathbb{N}$ *and* $L \in (0, 1/2]$*. Here* $c_1 := 1/53$*,* $c_2 := 40$*,* $c_3 := 2/7$*, and* $c_4 := 13$ *are appropriate choices.*

Theorem 2.2. *There are absolute constants* $c_1 > 0$ *and* $c_2 > 0$ *such that*

$$c_1\sqrt{n(1-L)} - 1 \le \kappa_1(n,L) \le \mu_\infty(n,L) \le c_2\sqrt{n(1-L)} + 1$$

for every $n \in \mathbb{N}$ *and* $L \in (1/2, 1]$, *and*

$$c_3 \min\left\{\sqrt{n(-\log L)}, n\right\} \le \kappa_1(n,L) \le \mu_\infty(n,L)$$

$$\le c_4 \min\left\{\sqrt{n(-\log L)}, n\right\} + 4$$

for every $n \in \mathbb{N}$ *and* $L \in (0, 1/2]$. *Note that* $\kappa_1(n,L) = \mu_\infty(n,L) = 0$ *for every* $n \in \mathbb{N}$ *and* $L > 1$. *Here* $c_1 := 1/5$, $c_2 := 1$, $c_3 := 2/7$, *and* $c_4 := 13$ *are appropriate choices.*

3. Lemmas

The following lemma is a simple observation.

Lemma 3.5. *Let $P \neq 0$ be a polynomial of the form $P(x) = \sum_{j=0}^{n} a_j x^j$. Then $(x-1)^k$ divides P if and only if $\sum_{j=0}^{n} a_j Q(j) = 0$ for all polynomials $Q \in \mathcal{P}_{k-1}^c$.*

Our next lemma is a simple consequence of Hölder's inequality.

Lemma 3.6. *Let $1 \le p, q \le \infty$ and $1/p + 1/q = 1$. Then for every $n \in \mathbb{N}$ and $L > 0$, we have*

$$\kappa_p(n, L) \le \mu_q(n, L)\,.$$

Proof of Lemma 3.6. Let $p, q \in (1, \infty)$, the result in the cases

$$p = 1, \;\; q = \infty \qquad \text{and} \qquad p = \infty, \;\; q = 1$$

can be proved similarly with straightforward modification of the proof. Let $m := \mu_q(n, L)$. Let Q be a polynomial of degree m with complex coefficients such that

$$|Q(0)| > \frac{1}{L} \left(\sum_{j=1}^{n} |Q(j)|^q \right)^{1/q}.$$

Now let P be a polynomial of the form

$$P(x) = \sum_{j=0}^{n} a_j x^j \,, \qquad |a_0| \geq L \left(\sum_{j=1}^{n} |a_j|^p \right)^{1/p},$$

$$a_j \in \mathbb{C} \,.$$

It follows from Hölder's inequality that

$$\left|\sum_{j=1}^{n} a_j Q(j)\right| \le \left(\sum_{j=1}^{n} |a_j|^p\right)^{1/p} \left(\sum_{j=1}^{n} |Q(j)|^q\right)^{1/q}$$

$$< \frac{|a_0|}{L} L|Q(0)| = |a_0 Q(0)|\,.$$

Then $\sum_{j=0}^{n} a_j Q(j) \neq 0$, and hence Lemma 3.5 implies that $(x-1)^{m+1}$ does not divide P. We conclude that $\kappa_p(n, L) \le m = \mu_q(n, L)$. $\square$

4. Pseudo-Boolean Functions and the Multiplicity of the Zeros of Polynomials

A function $f : \{-1, 1\}^n \to \mathbb{R}$ is called an n-bit pseudo-Boolean function.

In the context of the study of pseudo-Boolean functions in October, 2002, Mario Szegedy sent me the following question. "I know that there must exist a polynomial Q of degree $n - \lfloor\sqrt{n}\rfloor$ such that

$$\sum_{k=0}^{n} \binom{n}{k} |Q(k)| \leq c|Q(0)|$$

with an absolute constant $c > 0$, but I cannot give it explicitly. Can you give it explicitly by any chance?" A year later Robert Špalek [Š-03] answered this question.

Motivated by Špalek's result and the already mentioned Coppersmith-Rivlin inequality in [E-15b] we prove the following results.

Let $D_n := \{0,1,\dots,n\}$. Let $m = \lfloor \sqrt{n} \rfloor$ and let $S_n = \{j^2 : j \in D_m\} \cup \{2\}$ denote the set containing the squares up to n and the number 2.

Theorem 4.1. *Any polynomial P of the form*

$$P(z) = \sum_{j=0}^{n} a_j z^j \,, \qquad a_j \in \mathbb{C}\,,$$

satisfying

$$\frac{12|a_2|}{\binom{n}{2}} + \sum_{j \in S_n \setminus \{0,2\}} \frac{8|a_j|}{j\binom{n}{j}} < |a_0|\,,$$

has at most $n - \lfloor \sqrt{n} \rfloor - 1$ zeros at 1.

Note that in Theorem 4.1 there is no restriction on the coefficient $a_j \in \mathbb{C}$ whenever $j \in D_n \setminus S_n$.

Theorem 4.2. *An absolute constant $c_1 > 0$ exists such that every polynomial P of the form*

$$P(z) = \sum_{j=0}^{n} a_j z^j \,, \qquad a_j \in \mathbb{C} \,,$$

satisfying

$$|a_0| = 1 \,, \qquad |a_j| \le M^{-1} \binom{n}{j} \,,$$

$$j = 1, 2, \dots, n \,,$$

with some $2 \le M \le e^n$ has at most

$$n - \lfloor c_1 \sqrt{n \log M} \rfloor$$

zeros at 1*.*

Remark 4.3. Theorem 4.1 is essentially sharp in a rather strong sense. Using the basics of Chebyshev spaces (see Section 3.1, pages 92-100, in [B-95]), one can easily see that there is a polynomial P of the form

$$P(z) = 1 + \sum_{j \in D_n \setminus S_n} a_j z^j\,, \qquad a_j \in \mathbb{C}\,,$$

having at least $n - m - 1 = n - \lfloor \sqrt{n} \rfloor - 1$ zeros at 1.

Theorem 4.4. *Let $0 < m < \sqrt{n/2}$. Every polynomial P of the form*

$$P(z) = \sum_{j=0}^{n} a_j z^j\,, \qquad a_j \in \mathbb{C}\,,$$

satisfying

$$|a_0| = 1\,, \qquad |a_j| \leq \frac{n - 2m^2}{n} \binom{n}{j}\,,$$

$$j = 1, 2, \ldots, n\,,$$

has at most $n - m$ zeros at 1.

5. Remarks and Problems

A question that we have not really considered in this paper is if there are examples of n, L, and p for which the values of $\kappa_p(n,L)$ are significantly smaller if the coefficients are required to be rational (perhaps together with other restrictions). The same question may be raised about $\mu_q(n,L)$. As the conditions on the coefficients of the polynomials in Theorems 2.1 and 2.2 are homogeneous, assuming rational coefficients and integer coefficients lead to the same results. Three special classes of interest are

$$\mathcal{F}_n := \left\{ Q : Q(z) = \sum_{j=0}^{n} a_j z^j \,, \;\; a_j \in \{-1, 0, 1\} \right\} ,$$

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

and

$$\mathcal{K}_n$$

$$:= \left\{ Q : Q(z) = \sum_{j=0}^{n} a_j z^j \,, \;\; a_j \in \mathbb{C}, \;\; |a_j| = 1 \right\} .$$

The following three problems arise naturally.

Problem 5.1. *How many zeros can a polynomial* $0 \not\equiv Q \in \mathcal{F}_n$ *have at* 1*?*

Problem 5.2. *How many zeros can a polynomial* $Q \in \mathcal{L}_n$ *have at* 1*?*

Problem 5.3. *How many zeros can a polynomial* $Q \in \mathcal{K}_n$ *have at* 1*?*

The case when $p = \infty$ and $L = 1$ in our Theorem 2.1 gives that every $0 \not\equiv Q \in \mathcal{F}_n$, every $Q \in \mathcal{L}_n$, and every $Q \in \mathcal{K}_n$ can have at most $cn^{1/2}$ zeros at 1 with an absolute constant $c > 0$, but one may expect better results by utilizing the additional pieces of information on their coefficients.

It was observed in [B-99] that for every integer $n \geq 2$ there is a $Q \in \mathcal{F}_n$ having at least $c(n/\log n)^{1/2}$ zeros at 1 with an absolute constant $c > 0$. This is a simple pigeon hole argument. However, as far as we know, closing the gap between $cn^{1/2}$ and $c(n/\log n)^{1/2}$ in Problem 5.1 is an open and most likely very difficult problem.

As far as Problem 5.2 is concerned, Boyd [B-97] showed that for $n \geq 3$ every $Q \in \mathcal{L}_n$ has at most

$$\frac{c(\log n)^2}{\log \log n} \tag{5.1}$$

zeros at 1, and this is the best known upper bound even today. Boyd's proof is very clever and up to an application of the Prime Number Theorem is completely elementary. It is reasonable to conjecture that for $n \geq 2$ every $Q \in \mathcal{L}_n$ has at most $c \log n$ zeros at 1. It is easy to see that for every integer $n \geq 2$ there are $Q_n \in \mathcal{L}_n$ with at least $c \log n$ zeros at 1 with an absolute constant $c > 0$.

As far as Problem 5.3 is concerned, one may suspect that every for $n \geq 2$ every $Q \in \mathcal{K}_n$ has at most $c \log n$ zeros at 1. However, just to see if Boyd's bound (4.1) holds for every $Q \in \mathcal{K}_n$ seems quite challenging and beyond reach at the moment.