PSEUDO-BOOLEAN FUNCTIONS AND THE MULTIPLICITY OF THE ZEROS OF POLYNOMIALS

Tamás Erdélyi

Abstract. A highlight of this paper states that there is an absolute constant $c_1 > 0$ such that any polynomial P of the form

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

satisfying

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

with some $2 \leq M \leq e^n$ has at most $n - \lfloor c_1 \sqrt{n \log M} \rfloor$ zeros at 1. This is compared with some earlier results of similar type reviewed in the introduction and closely related to some interesting Diophantine problems. Our most important tool is an essentially sharp result due to Coppersmith and Rivlin asserting that if $F_n := \{1, 2, \dots, n\}$, then there is an absolute constant $c > 0$ such that

$$|P(0)| \leq \exp(cL) \max_{x \in F_n} |P(x)|$$

for every polynomial P of degree at most $m \leq \sqrt{nL/16}$ with $1 \leq L < 16n$. A short new proof of this inequality is included in our discussion.

1. Number of Zeros at 1 of Polynomials with Restricted Coefficients

In [B-99] and [B-13] we examine a number of problems concerning polynomials with coefficients restricted in various ways. We are particularly interested in how small such polynomials can be on the interval $[0,1]$. For example, we prove that there are absolute constants $c_1 > 0$ and $c_2 > 0$ such that

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

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

Key words and phrases. Boolean functions, symmetric polynomials, zeros of polynomials, multiplicity.
2000 Mathematics Subject Classifications. 11C08, 41A17

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX 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. See [A-79, B-98, B-95, B-94, F-80, O-93].

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 classes of polynomials of the form

$$p(x) = \sum_{j=0}^{n} a_j x^j \,, \qquad |a_j| \le 1 \,, \quad a_j \in \mathbb{C} \,, \quad j = 1, 2, \ldots, n \,,$$

with fixed $|a_0| \ne 0$.

Variants of these questions have attracted considerable study, though rarely have precise answers been possible to give. See in particular [A-90, B-32, B-87, E-50, Sch-33, Sz-34]. 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.) See [H-82], [B-94], or [B-02].

For $n \in \mathbb{N}$, $L > 0$, and $p \ge 1$ we define the following numbers. Let $\kappa_p(n, L)$ be the largest possible value of k for which there is a polynomial $P \ne 0$ of the form

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

such that $(x-1)^k$ divides $P(x)$. 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 $P \ne 0$ of the form

$$P(x) = \sum_{j=0}^{n} a_j x^j \,, \qquad |a_0| \ge L \max_{1 \le j \le n} |a_j| \,, \quad a_j \in \mathbb{C} \,,$$

such that $(x-1)^k$ divides $P(x)$. In [B-99] we proved that there is an absolute constant $c_3 > 0$ such that

$$\min \left\{ \frac{1}{6} \sqrt{(n(1 - \log L)} - 1 \,, n \right\} \le \kappa_\infty(n, L) \le \min \left\{ c_3 \sqrt{n(1 - \log L)} \,, n \right\}$$

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 when $L \ge 1$. Recently in [B-13] we found the right order of magnitude of $\kappa_\infty(n, L)$ in the case when $L \ge 1$, that is, there are absolute constants $c_1 > 0$ and $c_2 > 0$ such that

$$c_1 \sqrt{n/L} - 1 \le \kappa_\infty(n, L) \le c_2 \sqrt{n/L}$$

for every $n \in \mathbb{N}$ and $L \ge 1$. To prove this, the lower bound, in particular, required some subtle new ideas. An interesting connection to number theory is explored. The fact that the density of square free integers is positive (in fact, it is $\pi^2/6$), appears in our proof. In [B-13] we also prove that there are absolute constants $c_1 > 0$ and $c_2 > 0$ such that

$$c_1\sqrt{n}/L - 1 \le \kappa_2(n, L) \le c_2\sqrt{n}/L$$

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

$$\min\left\{c_1\sqrt{n(-\log L)} - 1\,, n\right\} \le \kappa_2(n, L) \le \min\left\{c_2\sqrt{n(-\log L)}\,, n\right\}$$

for every $n \in \mathbb{N}$ and $L \in (0, 2^{-1/2}]$. 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] and [B-13] have turned out to be related to a number of recent papers from a rather wide range of research areas. See [A-02, B-98, B-95, B-96 B-97a, B-97b, B-97, B-00, B-07, B-08a, B-08b, C-02, C-13, C-10, D-99, D-01, D-03, E-08a, E-08b, E-13, F-00, G-05, K-04, K-09, M-03, M-68, N-94, O-93, P-12, P-13, S-99, T-07, T-84], for example.

More on the zeros of polynomials with Littlewood-type coefficient constraints may be found in [E-02]. Markov and Bernstein type inequalities under Erdős type coefficient constraints are surveyed in [E-01].

Our goal in this paper is to explore a variety of new ideas essentially different from those used in [B-99] and [B-13] to obtain essentially sharp bounds for the multiplicity of the zero at 1 of polynomials from various classes of constrained polynomials.

2. Pseudo-Boolean Functions

A function $f : \{-1, 1\}^n \to \mathbb{R}$ is called an n-bit pseudo-Boolean function. We say that an n-bit pseudo-Boolean function $f : \{-1, 1\}^n \to \mathbb{R}$ is *symmetric* if $f(\mathbf{x}) = f(\mathbf{x}_\sigma)$ for every permutation $\sigma \in S_n$ and $\mathbf{x} \in \{-1, 1\}^n$, where

$$\mathbf{x}_\sigma := (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

denotes a σ permuted version of $\mathbf{x}$. Note that if $p : \{-1, 1\}^n \to \mathbb{R}$ is a polynomial in variables $x_1, x_2, \ldots, x_n$ then the fact $x_j^2 = 1$ implies that we can view p as a *multi-linear* polynomial in which each variable appears with degree at most 1. We say that a multi-linear polynomial p has degree at most d_1 and pure high degree at least d_2 if each term in p is a product of at most d_1 and at least d_2 variables.

Let $D_n := \{0, 1, \ldots, n\}$. Associated with any symmetric function $f : \{-1, 1\}^n \to \mathbb{R}$ there is a function F of a single variable $F : D_n \to \mathbb{R}$ such that

$$f(\mathbf{x}) = F(|\mathbf{x}|)\,, \qquad \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \{-1, 1\}^n\,,$$

where

$$|\mathbf{x}| := \frac{n - (x_1 + x_2 + \cdots + x_n)}{2}$$

is the Hamming weight of $\mathbf{x}$, that is $|\mathbf{x}|$ is the number of -1 components of $\mathbf{x}$. By using the fundamental theorem of symmetric polynomials it can be easily proved (see [M-69], for example) that for every symmetric multi-linear polynomial $p : \{-1,1\}^n \to \mathbb{R}$ there is a polynomial $P : D_n \to \mathbb{R}$ of a single variable of the same degree such that

$$p(\mathbf{x}) = P(|\mathbf{x}|)\,, \qquad \mathbf{x} = (x_1, x_2, \dots, x_n) \in \{-1,1\}^n\,.$$

Note that the pure high degree of p does not correspond to the degree of the term with the lowest degree in P. By the pure high degree of a polynomial $P : D_n \to \mathbb{R}$ of a single variable we mean the pure high degree of its corresponding multi-linear polynomial $p : \{-1,1\}^n \to \mathbb{R}$.

Let X_n be the vector space of all symmetric multi-linear polynomials $p : \{-1,1\}^n \to \mathbb{R}$ over $\mathbb{R}$. Let Y_n be the vector space of all polynomials $D_n \to \mathbb{R}$ of a single variable over $\mathbb{R}$.

We define the *scalar product*

$$\langle p, q \rangle := \sum_{\mathbf{x} \in \{-1,1\}^n} p(\mathbf{x}) q(\mathbf{x})$$

on X_n. This induces the scalar product

$$\langle P, Q \rangle := \sum_{k=0}^{n} \binom{n}{k} P(k) Q(k)\,.$$

on Y_n, where

$$p(\mathbf{x}) = P(|\mathbf{x}|) \quad \text{and} \quad q(\mathbf{x}) = Q(|\mathbf{x}|)\,, \qquad \mathbf{x} = (x_1, x_2, \dots, x_n) \in \{-1,1\}^n\,.$$

A function $f : \{-1,1\}^n \to \{-1,1\}$ is called an n-bit Boolean function. Boolean functions on the space $\{-1,1\}^n$ are important not only in the theory of error-correcting codes, but also in cryptography, where they occur in private key systems. Boolean functions are studied in [R-04], for example, a paper inspired by works of Salem and Zygmund [S-54], Kahane [K-85], and others about the related problem of real polynomials with random coefficients.

3. New Results

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

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

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. We state his result as Lemma 4.1 and for the sake of completeness we reproduce his short and clever proof.

Motivated by this question and answer, in this paper we prove the following results.

Let, as before, $D_n := \{0, 1, \dots, n\}$. 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 3.1. *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 3.1 there is no restriction on the coefficient $a_j \in \mathbb{C}$ whenever $j \in D_n \setminus S_n$.

Theorem 3.2. *There is an absolute constant $c_1 > 0$ such that any polynomial P of the form*

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

satisfying

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

with some $2 \leq M \leq e^n$ has at most $n - \lfloor c_1 \sqrt{n \log M} \rfloor$ zeros at 1.

Remark 3.3. Theorem 3.1 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 3.4. *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

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

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

4. Lemmas

We call the results in this section lemmas although some of them would deserve to be called theorems. We prove these lemmas in Section 5. We apply them in Section 6 where we prove our theorems formulated in Section 3. Let $\mu = \lfloor \sqrt{n} \rfloor$ and let

$$S_n = \{j^2 : j \in D_\mu\} \cup \{2\}$$

denote the set containing the squares up to n and the number 2. We introduce the polynomial

$$Q_n(x) := 2(-1)^{n-\mu-1} \frac{(\mu!)^2}{n!} \prod_{j \in D_n \setminus S_n} (x-j)\,. \tag{4.1}$$

The multiplicative factor of Q in front of the product sign is chosen so that $Q_n(0) = 1$. The degree of Q_n is $n - \mu - 1$. The lemma below is due to Špalek [Š-03], who was the first to answer Szegedy's question quoted in the beginning of Section 3 by having the fortunate idea of studying the polynomial Q_n defined above.

Lemma 4.1. *Let Q_n be the polynomial of degree $n - \lfloor \sqrt{n} \rfloor - 1$ defined in (4.1). In addition to $Q(0) = 1$ we have*

$$\binom{n}{2} |Q(2)| \le 12\,, \qquad \binom{n}{k^2} |Q(k^2)| \le \frac{8}{k^2}\,, \qquad k = 1, 2, \dots, \mu\,.$$

Let $\mathcal{P}_m$ denote the set of all polynomials of degree at most m with real coefficients. The following result is well known and can easily be proved as a simple exercise. It was observed and used in [B-99], for instance.

Lemma 4.2. *If a polynomial P of the form $P(z) = \sum_{j=0}^{n} a_j z^j$, $a_j \in \mathbb{C}$, has a zero at 1 with multiplicity at least $m+1$, then $\sum_{j=0}^{n} a_j Q(j) = 0$ for every polynomial $Q \in \mathcal{P}_m$.*

The following facts are well-known about Lagrange interpolation. If $P \in \mathcal{P}_m$ and

$$x_0 < x_1 < \cdots < x_m$$

are real numbers, then

$$P(x) = \sum_{k=0}^{m} P(x_k) L_k(x)\,, \qquad x \in \mathbb{R}\,,$$

where

$$L_k(x) := \prod_{\substack{j=0 \\ j \ne k}}^{m} \frac{x - x_j}{x_k - x_j}\,, \qquad k = 0, 1, \dots, m\,. \tag{4.2}$$

Note that $L_k(x_j) = \delta_{k,j}$, where

$$\delta_{j,k} := \begin{cases} 0, & j \neq k \\ 1, & j = k \end{cases} \qquad \text{for} \quad j, k \in \{0, 1, \dots, m\}\,.$$

If $y \leq x_0 < x_1 < \cdots < x_m$ and $E_m := \{x_0, x_1, \dots, x_m\}$ then

$$\max_{0 \neq P \in \mathcal{P}_m} \frac{|P(y)|}{\max_{x \in E_m} |P(x)|} = \sum_{k=0}^{m} |L_k(y)| = \sum_{k=0}^{m} (-1)^k L_k(y)\,. \tag{4.3}$$

Let

$$E_m = \{x_0 < x_1 < \cdots < x_m\} \qquad \text{and} \qquad E_m^* = \{x_0^* < x_1^* < \cdots < x_m^*\}\,.$$

Lemma 4.3. *Suppose $y \leq x_0^*$, $x_m^* \leq x_m$, and*

$$x_{j+1} - x_j \leq x_{j+1}^* - x_j^*\,, \qquad j = 0, 1, \dots, m-1\,.$$

Then

$$\max_{P \in \mathcal{P}_m} \frac{|P(y)|}{\max_{x \in E_m^*} |P(x)|} \leq \max_{P \in \mathcal{P}_m} \frac{|P(y)|}{\max_{x \in E_m} |P(x)|}\,.$$

The lemma below is a straightforward consequence of Lemma 4.3.

Lemma 4.4. *Suppose $y \leq x_0^*$, $x_m^* \leq x_m$, and*

$$x_{j+1} - x_j \leq x_{j+1}^* - x_j^*\,, \qquad j = 0, 1, \dots, m-1\,,$$

and the polynomial $Q \in \mathcal{P}_m$ satisfies

$$(-1)^j Q(x_j) \geq \delta > 0\,.$$

Then

$$\max_{P \in \mathcal{P}_m} \frac{|P(y)|}{\max_{x \in E_m^*} |P(x)|} \leq \delta^{-1} |Q(0)|\,.$$

A key to the proof of Theorem 3.2 is the Coppersmith-Rivlin inequality in [C-92], an equivalent form of which may be formulated as follows.

Lemma 4.5. *Let $F_n := \{1, 2, \dots, n\}$. There exists an absolute constant $c > 0$ such that*

$$|P(0)| \leq \exp(cL) \max_{x \in F_n} |P(x)|$$

for every $P \in \mathcal{P}_m$ with $m \leq \sqrt{nL/16}$ and $1 \leq L < 16n$. The above inequality is sharp up to the absolute constant $c > 0$ in the exponent.

In Section 5 we give a shorter new proof of the Coppersmith-Rivlin inequality. Our main idea to prove Lemma 4.5 is somewhat similar to the key idea to prove the bounded Remez-type inequality of [B-97b] for non-dense Müntz spaces. The proof of Lemma 4.5 in the case $n/16 \leq m^2 \leq n/2$ could also be obtained simply from the Markov inequality for polynomials, while in the case $m = n-1$ it follows from the basics of Lagrange interpolation. However, the proof of Lemma 4.5 in general is more subtle. Lemma 4.5 is proved to be essentially sharp in [C-92] and is used in [Bu-99] in the study of small-error and zero-error quantum algorithms. A recent closely related interesting result is due to E.A. Rakhmanov [R-07].

The result below plays a fundamental role in the proof of Theorem 3.2. We will prove it with the help of of Lemma 4.5 in Section 5.

Lemma 4.6. *Let $c_1 := (32c)^{-1/2}$, where the absolute constant $c > 0$ is the same as in Lemma 4.5. Suppose $e^{2c} \leq M < e^{32cn}$. There is a polynomial Q of degree at most*

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

such that

$$\sum_{k=1}^{n} \binom{n}{k} |Q(k)| < M|Q(0)|\,.$$

The lemma below is quite useful when $m \leq \sqrt{n/4}$. We prove it in Section 5 as a simple consequence of Markov's inequality.

Lemma 4.7. *Let $F_n := \{1, 2, \dots, n\}$. We have*

$$|P(0)| < \frac{n}{n-2m^2} \max_{x \in F_n} |P(x)|$$

for every $P \in \mathcal{P}_m$ with $0 < m < \sqrt{n/2}$.

The lemma below can be used in the proof of Theorem 3.4.

Lemma 4.8. *Suppose $m \leq \sqrt{n/2}$. There is a polynomial Q of degree at most $n-m-1$ such that*

$$\sum_{k=1}^{n} \binom{n}{k} |Q(k)| < \frac{n}{n-2m^2}\, |Q(0)|\,.$$

5. Proof of the Lemmas

Proof of Lemma 4.1. We follow Špalek [Š-03]. First observe that if $0 \leq k \leq m$ then

$$\text{(5.1)} \qquad \frac{(\mu!)^2}{(\mu+k)!(\mu-k)!} = \frac{\mu(\mu-1)\cdots(\mu-k+1)}{(\mu+k)(\mu+k-1)\cdots(\mu+1)} = \prod_{j=1}^{k}\left(1 - \frac{k}{\mu+j}\right) \leq 1\,.$$

Using this with $k = 2$, we obtain

$$\begin{aligned}
|Q_n(2)| &= 2\frac{(\mu!)^2}{n!}(n-2)!\frac{1}{2}\prod_{j=3}^{\mu}\frac{1}{|2-j^2|} < \frac{(\mu!)^2}{n!}(n-2)!\prod_{j=3}^{\mu}\frac{1}{(j^2-4)} \\
&= \frac{(\mu!)^2}{n!}(n-2)!\prod_{j=3}^{\mu}\frac{1}{(j+2)(j-2)} = \frac{1}{n(n-1)}\frac{(\mu!)^2}{\frac{1}{4!}(\mu+2)!(\mu-2)!} \\
&\le \frac{4!}{n(n-1)} = \frac{12}{\binom{n}{2}}\,.
\end{aligned}$$

Observe also that if $k \in \{1, 2, \ldots, \mu\}$, then

$$\begin{aligned}
|Q_n(k^2)| &= 2\,\frac{(\mu!)^2}{n!}\prod_{\substack{j\in D_n\\ j\neq k^2}}|k^2-j|\;\frac{1}{|k^2-2|}\prod_{\substack{j\in D_\mu\\ j\neq k}}\frac{1}{(k+j)|k-j|} \\
&= 2\,\frac{(\mu!)^2}{n!}\,(k^2)!(n-k^2)!\frac{2k\,(k-1)!}{(k+\mu)!k!(\mu-k)!|k^2-2|} \\
&= 4\frac{(k^2)!(n-k^2)!}{n!}\;\frac{(\mu!)^2}{(\mu+k)!(\mu-k)!}\;\frac{1}{|k^2-2|}\,.
\end{aligned}$$

Hence (5.1) yields

$$|Q_n(k^2)| \le \frac{4}{\binom{n}{k^2}}\,\frac{1}{|k^2-2|} \le \frac{4}{\binom{n}{k^2}}\,\frac{1}{k^2/2} \le \frac{8}{k^2\binom{n}{k^2}}\,, \qquad k = 1, 2, \ldots, \mu\,.$$

Note that if we did not include the number 2 in S_n, then the upper bound for $|Q_n(k^2)|$ would be much weaker, without the factor $1/k^2$. $\square$

Proof of Lemma 4.3. Let

$$L_k(x) := \prod_{\substack{j=0\\ j\neq k}}^{m}\frac{x-x_j}{x_k-x_j}\,, \qquad L_k^*(x) := \prod_{\substack{j=0\\ j\neq k}}^{m}\frac{x-x_j^*}{x_k^*-x_j^*}\,, \qquad k = 0, 1, \ldots, m\,.$$

Note that the assumptions on y, x_j, and x_j^* imply that

$$0 < (-1)^k L_k^*(y) \le (-1)^k L_k(y)\,, \qquad k = 0, 1, \ldots, m\,,$$

and the lemma follows from (4.2).

Proof of Lemma 4.5. To prove the inequality of the lemma in the case when, together with $L < 16n$ we also have $n < 656L$, let $m \le \sqrt{nL/16} < n$ and $P \in \mathcal{P}_m$. Let

$$x_j := j + 1\,, \qquad j = 0, 1, \ldots, m\,,$$

$$E_m := \{x_0, x_1, \dots, x_m\} \subset F_n\,,$$

and let the basic Lagrange interpolating polynomials L_k defined by (4.2). Observe that

$$L_k(0) = (-1)^k \frac{m+1}{k}\binom{m}{k}\,, \qquad k = 0, 1, \dots, m\,,$$

and hence

$$\begin{aligned}\max_{0 \neq P \in \mathcal{P}_m} \frac{|P(0)|}{\max_{x \in F_n} |P(x)|} &= \max_{0 \neq P \in \mathcal{P}_m} \frac{|P(0)|}{\max_{x \in E_m} |P(x)|} \sum_{k=0}^{m} |L_k(0)| = \sum_{k=0}^{m} (-1)^k L_k(0) \\ &\le (m+1) \sum_{k=0}^{m} \binom{m}{k} \le n2^n \le 656L \exp(656L)\,.\end{aligned}$$

This finishes the proof of the inequality of the lemma in the case when together with $L < 16n$ we also have $n < 656L$.

Now assume that $n \ge 328L$. Without loss of generality we may assume that both n and $L/16$ are squares, so $m \ge 1$ defined by $m^2 = (nL)/16$ is an integer. Let T_m be the Chebyshev polynomial of degree m on the interval $[-1, 1]$, that is,

$$T_m(x) = \cos(m \arccos x)\,, \qquad x \in [-1, 1]\,.$$

Let Q_m be the Chebyshev polynomial T_m transformed linearly from $[-1, 1]$ to the interval $[164L, n]$, that is,

$$Q_m(x) := T_m\left(\frac{2x}{n - 164L} - \frac{n + 164L}{n - 164L}\right)\,, \qquad x \in [164L, n]\,.$$

Using the explicit form

$$T_m(x) = \frac{1}{2}\left(\left(x + \sqrt{x^2 - 1}\right)^m + \left(x - \sqrt{x^2 - 1}\right)^m\right)\,, \qquad x \in \mathbb{R} \setminus [-1, 1]\,,$$

of the Chebyshev polynomial T_m, with the notation

$$s := \frac{328L}{n - 164L} \le \frac{656L}{n} \le 2$$

we can easily deduce that

$$\begin{aligned}|Q_m(0)| &= |T_m(-1 - s)| = T_m(1 + s) \le \left(1 + s + \sqrt{2s + s^2}\right)^m \\ &\le \left(1 + 4\sqrt{s}\right)^m \le \exp\left(4m26\sqrt{L/n}\right) \le \exp\left(26\sqrt{Ln}\sqrt{L/n}\right) \\ &\le \exp(26L)\,.\end{aligned} \tag{5.2}$$

We denote the extreme points of Q_m on $[164L, n]$ by

$$164L = \xi_0 < \xi_1 < \cdots < \xi_m = n\,,$$

that is,

$$\xi_j := \frac{1}{2}(n - 164L)\cos\frac{(m-j)\pi}{m} + \frac{1}{2}(n + 164L)\,, \qquad j = 0, 1, \dots, m\,,$$

and

$$Q_m(\xi_j) = (-1)^{m-j}\,, \qquad j = 0, 1, \dots, m\,. \tag{5.3}$$

Let η_j be the smallest integer greater than ξ_j. Observe that $n \ge 328L$ implies

$$m = \frac{1}{4}\sqrt{nL} \ge \frac{1}{4}\sqrt{328L^2} \ge 4L\,,$$

and hence

$$1 - \cos\frac{L\pi}{m} = 2\sin^2\frac{L\pi}{2m} \ge \frac{2L^2}{m^2}\,.$$

So

$$164L + (n - 164L)\frac{L^2}{m^2} \le \xi_j \le n - (n - 164L)\frac{L^2}{m^2}\,, \qquad j \in [L, m - L]\,.$$

Moreover, using also $m^2 = (nL)/16$ and $n \ge 328L$, we deduce that

$$\begin{aligned} 164L + (n - 164L)\frac{L^2}{m^2} \le \xi_L < \eta_{m-L-1} &\le n - (n - 164L)\frac{(L+1)^2}{m^2} + 1 \\ &\le n - (n - 164L)\frac{L^2}{m^2}\,. \end{aligned} \tag{5.4}$$

Using the Mean Value Theorem, Bernstein's inequality (see p. 233 of [B-95], for instance), and (5.4) we obtain

$$\begin{aligned} |Q_m(\xi_j) - Q_m(x)| &\le (x - \xi_j) \max_{\xi \in [\eta_j, \xi_j]} |Q_m'(\xi)| \\ &\le \frac{2m^2}{(n - 164L)L} \le \frac{4m^2}{nL} \\ &\le \frac{1}{4}\,, \qquad x \in [\xi_j, \eta_j]\,, \quad j \in [L, m - L - 1]\,. \end{aligned} \tag{5.5}$$

Also,

$$\begin{aligned} \xi_{j+1} - \xi_j =& \frac{1}{2}(n - 164L)\left(\cos\frac{(m - (j+1))\pi}{m} - \cos\frac{(m-j)\pi}{m}\right) \\ \le& \frac{1}{2}(n - 164L)\frac{\pi}{m}\,\sin\frac{L\pi}{m} \le \frac{1}{2}\frac{\pi^2 nL}{m^2} \le 80\,, \end{aligned} \tag{5.6}$$

$$j \in [0, L-1] \cup [m-L, m-1] \,.$$

Combining (5.3) and (5.5) we get

$$(-1)^{m-j} Q_m(x) \geq \frac{3}{4}\,, \qquad x \in [\xi_j, \eta_j]\,, \quad j \in [L, m-L-1]\,,$$

and hence

$$(5.7) \qquad (-1)^{m-j} Q_m(\eta_j) \geq \frac{3}{4}\,, \qquad j \in [L, m-L-1]\,,$$

and

$$(5.8) \qquad \xi_j < \eta_j < \xi_{j+1}\,, \qquad j \in [L, m-L-1]\,.$$

We define

$$\begin{aligned} x_j &:= \xi_j\,, \qquad j \in [0, L-1] \cup [m-L, m]\,, \\ x_j &:= \eta_j\,, \qquad j \in [L, m-L-1]\,, \end{aligned}$$

and let $E_m = \{x_0, x_1, \cdots, x_m\}$. Recalling (5.7) we have $E_m = \{x_0 < x_1 < \cdots < x_m\}$. Now we define $E_m^* = \{x_0^* < x_1^* < \cdots < x_m^*\} \subset F_n = \{1, 2, \ldots, n\}$ as follows. Let

$$\begin{aligned} x_j^* &:= n - 80(m-j)\,, \qquad j \in [m-L, m]\,, \\ x_j^* &:= \eta_j - 80L\,, \qquad j \in [L, m-L-1]\,, \\ x_j^* &:= \eta_L - 1 - 80L - 80(L-j)\,, \qquad j \in [0, L-1]\,. \end{aligned}$$

Observe that (5.6) implies that the assumptions of Lemma 4.3 on E_m and E_m^* with $Q = Q_m$ are satisfied. iNow the inequality of the lemma follows from Lemma 4.4 and (5.2).

Now we prove that the inequality of the lemma is sharp up to the constant $c > 0$ in the exponent. Without loss of generality we may assume that both n and $L/16$ are squares, so $m \geq 1$ defined by $m^2 = (nL)/16$ is an integer. Let T_m be the Chebyshev polynomial of degree m on the interval $[-1, 1]$, that is,

$$T_m(x) = \cos(m \arccos x)\,, \qquad x \in [-1, 1]\,.$$

Let Q_m be the Chebyshev polynomial T_m transformed linearly from $[-1, 1]$ to the interval $[0, n]$, that is,

$$Q_m(x) := T_m\left(\frac{2x}{n} - 1\right) = \frac{2}{n^n} \prod_{k=1}^{m} (x - x_k)\,, \qquad x \in [0, n]\,,$$

where, for $1 \leq k \leq L' := L/80$ we have

$$\begin{aligned} 0 < x_k &= \frac{n}{2}\left(1 + \cos\frac{2k-1}{2m}\pi\right) = n \sin^2 \frac{2k-1}{4m}\pi \\ &\leq \frac{nk^2\pi^2}{4m^2} \leq \frac{4nk^2\pi^2}{nL} \leq \frac{40k^2}{L} \leq \frac{k}{2}\,. \end{aligned}$$

Now we define the polynomial P_m of degree m by

$$P_m(x) := Q_m(x) \prod_{k=1}^{L'} \frac{x-k}{x-x_k} \,.$$

Then, we have

$$|P_m(j)| \leq |Q_m(j)| \leq 1 \,, \qquad j \in [L'+1, n] \cap F_n \,,$$

and

$$|P_m(j)| = 0 < 1 \,, \qquad j \in [1, L'] \cap F_n \,,$$

hence

$$|P_m(j)| \leq 1 \,, \qquad j \in F_n \,.$$

This, together with

$$|P_m(0)| \geq |Q_m(0)| \prod_{k=1}^{L'} \left| \frac{k}{x_k} \right| \geq \prod_{k=1}^{L'} \frac{k}{k/2} \geq 2^{L'} \geq 2^{L/80-1}$$

finishes the proof of the fact that the inequality of the lemma is sharp up to the absolute constant $c > 0$ in the exponent. $\square$

Proof of Lemma 4.6. We use the notation introduced in Section 2. Let $D_n := \{0, 1, \dots, n\}$. Let X_n be the vector space of all symmetric multi-linear polynomials $p : \{-1,1\}^n \to \mathbb{R}$ over $\mathbb{R}$, equipped with the scalar product defined in Section 2. Let Y_n be the vector space of all polynomials $D_n \to \mathbb{R}$ of a single variable over $\mathbb{R}$, equipped with the scalar product defined in Section 2.

Let F and P be the polynomials $D_n \to \mathbb{R}$ of a single variable induced by $f \in X_n$ and $p \in X_n$, respectively. That is,

$$f(\mathbf{x}) = F(|\mathbf{x}|) \,, \qquad \mathbf{x} = (x_1, x_2, \dots, x_n) \in \{-1,1\}^n \,,$$

and

$$p(\mathbf{x}) = P(|\mathbf{x}|) \,, \qquad \mathbf{x} = (x_1, x_2, \dots, x_n) \in \{-1,1\}^n \,.$$

Let $M = \exp(2cL)$, where the constant $c > 0$ is the same as in Lemma 4.5. Let $m \geq 0$ be the largest integer not greater than $\sqrt{nL/16}$ and we define

$$U := \{f \in X_n : F(0) \geq \exp(2cL) \,, \;\; |F(j)| \leq 1 \,, \;\; j = 1, 2, \dots, n\} \,.$$

Let

$$V_m = \{p \in X_n : P \in \mathcal{P}_m\} \,,$$

where, as before, $\mathcal{P}_m$ denotes the set of all polynomials of degree at most m with real coefficients. Lemma 4.5 tells us that $U \cap V_m = \emptyset$. Since any two disjoint convex sets in a finite dimensional vector space can be separated by a hyper-plane, there is a symmetric polynomial $g \in X_n$ such that

$$\langle g, p \rangle = \langle G, P \rangle = 0\,, \qquad P \in \mathcal{P}_m\,, \tag{5.9}$$

and

$$\langle g, f \rangle = \langle G, F \rangle \geq \alpha > 0\,, \qquad f \in U\,, \tag{5.10}$$

where G is the polynomial $D_n \to \mathbb{R}$ of a single variable induced by $g \in X_n$, that is,

$$G(\mathbf{x}) = g(|\mathbf{x}|)\,, \qquad \mathbf{x} = (x_1, x_2, \dots, x_n) \in \{-1, 1\}^n\,.$$

From (5.9) we easily deduce that the pure high degree of $g \in X_n$ is at least $m+1$. It follows from (5.10) that

$$\sum_{k=0}^{n} \varepsilon_k \binom{n}{k} G(k) \geq \alpha > 0$$

whenever

$$\varepsilon_0 = \exp(2cL)\,, \quad \varepsilon_k \in \{-1, 1\}\,, \quad k = 1, 2, \dots, n\,.$$

Hence

$$\exp(2cL)G(0) - \sum_{k=1}^{n} \binom{n}{k} |G(k)| > 0\,,$$

that is,

$$G(0) > \exp(-2cL) \sum_{k=1}^{n} \binom{n}{k} |G(k)|\,.$$

Now let $\widetilde{g} \in X_n$ be the symmetric multi-linear polynomial defined by

$$\widetilde{g}(x_1, x_2, \dots, x_n) := (x_1 x_2 \cdots x_n) g(x_1, x_2, \dots, x_n)\,,$$

and let $\widetilde{G} \in \mathcal{P}_n$ be the polynomial $D_n \to \mathbb{R}$ of a single variable induced by $\widetilde{g} \in X_n$, that is,

$$\widetilde{g}(\mathbf{x}) = \widetilde{G}(|\mathbf{x}|)\,, \qquad \mathbf{x} = (x_1, x_2, \dots, x_n) \in \{-1, 1\}^n\,.$$

Since the pure high degree of $g \in X_n$ is at least $m+1$, $\widetilde{G} \in \mathcal{P}_n$ is in fact a polynomial of degree at most $n - m - 1$. Here

$$m + 1 \geq \sqrt{nL/16} \geq \frac{1}{4\sqrt{2c}} \sqrt{n \log M} = c_1 \sqrt{n \log M}\,.$$

Also, since $|\widetilde{G}(j)| = |G(j)|$ for each $j = 0, 1, \dots, n$, we have

$$\sum_{k=1}^{n} \binom{n}{k} |\widetilde{G}(k)| < \exp(2cL) |\widetilde{G}(0)| = M |\widetilde{G}(0)|\,.$$

□

Proof of Lemma 4.7. Suppose $P \in \mathcal{P}_m$ and $\|P\|_{F_n} = 1$. Pick $y \in [0, n]$ so that $|P(y)| = M := \|P\|_{[0,n]}$. Without loss of generality we may assume that $P(y) > 0$. Let $k \in [1, n]$ be the integer closest to y. Combining Markov's polynomial inequality (see p. 233 of [B-95], for instance) transformed linearly from $[-1, 1]$ to $[0, n]$ with the Mean Value Theorem, we obtain

$$|M - P(k)| = |P(y) - P(k)| = |y - k||P'(\xi)| < \frac{2m^2}{n} M\,,$$

hence

$$1 \geq |P(k)| \geq M - |M - P(k)| > M\left(1 - \frac{2m^2}{n}\right)\,,$$

and the lemma follows. □

Proof of Lemma 4.8. The proof of the lemma is very similar to that of Lemma 4.6. However, at one point an application of Lemma 4.7 rather than Lemma 4.5 is needed. □

6. Proof of the Theorems

Proof of Theorem 3.1. Suppose that a polynomial P of the form

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

has a zero at 1 with multiplicity at least $n - \lfloor \sqrt{n} \rfloor$. Then

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

for all polynomials Q of degree at most $n - \lfloor \sqrt{n} \rfloor - 1$. Choosing Q_n with the properties of Lemma 4.1 we obtain

$$|a_0| = |a_0 Q_n(0)| \leq \sum_{j=1}^{n} |a_j||Q_n(j)| \leq \frac{12|a_2|}{\binom{n}{2}} + \sum_{j \in S_n \setminus \{0,2\}} \frac{8|a_j|}{j\binom{n}{j}}\,,$$

and this contradicts the assumption of the theorem. □

Proof of Theorem 3.2. Let the absolute constant $c > 0$ be the same as in Lemma 4.5. If $2 \leq e^{2c}$, then the theorem follows from Theorem 3.4. Hence we may assume that $e^{2c} \leq M < e^{32cn}$. Let the absolute constant $c_1 > 0$ be the same as in Lemma 4.6. Suppose that a polynomial P of the form

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

has a zero at 1 with multiplicity at least $n - \lfloor c_1\sqrt{n \log M}\rfloor + 1$. Then, by Lemma 4.2, we have

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

for all polynomials Q of degree at most $n - \lfloor c_1\sqrt{n \log M}\rfloor$. Using the assumptions

$$|a_0| = 1\,, \qquad |a_j| \le M^{-1}\binom{n}{j}, \qquad j = 1, 2, \ldots, n\,,$$

we can deduce that

$$|Q(0)| = |a_0 Q(0)| \le \sum_{j=1}^{n} |a_j||Q(j)| \le M^{-1}\sum_{j=1}^{n}\binom{n}{j}|Q(j)|\,.$$

However, this is impossible for the polynomial Q with the properties of Lemma 4.6. □

Proof of Theorem 3.4. The proof of the theorem is very similar to that of Theorem 3.2 in the case of $e^{2c} \le M < e^{32cn}$. However, at one point an application of Lemma 4.8 rather than Lemma 4.6 is needed. □

7. Acknowledgment. The author wishes to thank Peter Borwein and Mario Szegedy for their comments.

References

A-90. F. Amoroso, *Sur le diamètre transfini entier d'un intervalle réel*, Ann. Inst. Fourier, Grenoble **40** (1990), 885–911.

A-02. V.V. Andrievskii and H-P. Blatt, *Discrepancy of Signed Measures and Polynomial Approximation*, Springer, New York, 2002.

A-79. B. Aparicio, *New bounds on the minimal Diophantine deviation from zero on* $[0,1]$ *and* $[0,1/4]$, Actus Sextas Jour. Mat. Hisp.-Lusitanas (1979), 289–291.

B-98. F. Beaucoup, P. Borwein, D.W. Boyd, and C. Pinner, *Multiple roots of* $[-1,1]$ *power series*, J. London Math. Soc. (2) **57** (1998), 135–147.

B-32. A. Bloch and G. Pólya, *On the roots of certain algebraic equations*, Proc. London Math. Soc **33** (1932), 102–114.

B-87. E. Bombieri and J. Vaaler, *Polynomials with low height and prescribed vanishing*, in Analytic Number Theory and Diophantine Problems, Birkhäuser (1987), 53–73.

B-95. P. Borwein and T. Erdélyi, *Polynomials and Polynomial Inequalities*, Springer, New York, 1995.

B-02. P. Borwein, *Computational Excursions in Analysis and Number Theory*, Springer, New York, 2002.

B-96. P. Borwein and T. Erdélyi, *The integer Chebyshev problem*, Math. Computat. **65** (1996), 661–681.

B-97a. P. Borwein and T. Erdélyi, *On the zeros of polynomials with restricted coefficients*, Illinois J. Math. **41** (1997), 667–675.

B-97b. P.B. Borwein and T. Erdélyi, *Generalizations of Müntz's theorem via a Remez-type inequality for Müntz spaces*, J. Amer. Math. Soc. **10** (1997), 327–329.

B-07. P. Borwein & T. Erdélyi, *Lower bounds for the number of zeros of cosine polynomials: a problem of Littlewood*, Acta Arith. **128** (2007), 377–384.

B-08a. P. Borwein, T. Erdélyi, R. Ferguson, and R. Lockhart, *On the zeros of cosine polynomial : an old problem of Littlewood*, Ann. of Math. (2) **167** (2008), 1109–1117.

B-99. P. Borwein, T. Erdélyi, and G. Kós, *Littlewood-type problems on* $[0, 1]$, Proc. London Math. Soc. **79 (3)** (1999), 22–46.

B-13. P. Borwein, T. Erdélyi, and G. Kós, *The multiplicity of the zero at* 1 *of polynomials with constrained coefficients*, Acta Arith. (to appear).

B-08b. P. Borwein, T. Erdélyi, and F. Littmann, *Zeros of polynomials with finitely many different coefficients*, Trans. Amer. Math. Soc. **360** (2008), 5145–5154.

B-94. P. Borwein and C. Ingalls, *The Prouhet, Tarry, Escott problem*, Ens. Math. **40** (1994), 3–27.

B-00. P. Borwein and M.J. Mossinghoff, *Polynomials with height* 1 *and prescribed vanishing at* 1, Experiment. Math. **9** (2000), no. 3, 425–433.

B-97. D. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comput. **66** (1997), 1697–1703.

Bu-99. H. Buhrman, R. Cleve, R. de Wolf, and C. Zalka, *Bounds for small-error and zero-error quantum algorithms*, in 40th Annual Symposium on Foundations of Computer Science (New York, 1999), IEEE Computer Soc., Los Alamitos, CA, 358–368.

C-02. P.G. Casazza and N.J. Kalton, *Roots of complex polynomials and Weyl-Heisenberg frame sets*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2313–2318.

C-13. J.M. Cooper and A.M. Dutle, *Greedy Galois games*, manuscript.

C-92. D. Coppersmith and T.J. Rivlin, *The growth of polynomials bounded at equally spaced points*, SIAM J. Math. Anal. **23(4)** (1992), 970–983.

C-10. E. Croot and D. Hart, *h-fold sums from a set with few products*, SIAM J. Discrete Math. **24** (2010), no. 2, 505–519.

D-99. A. Dubickas, *On the order of vanishing at* 1 *of a polynomial*, Lithuanian Math. J. **39** (1999), 365–370.

D-01. A. Dubickas, *Three problems of polynomials of small measure*, Acta Arith. **98** (2001), 279–292.

D-03. M. Dudik and L.J. Schulman, *Reconstruction from subsequences*, Journal of Combinatorial Theory, Series A **103** (2003), no. 2, 337–348.

E-01. T. Erdélyi, *Markov-Bernstein type inequalities for polynomials under Erdős-type constraints*, in Paul Erdős and his Mathematics I, Bolyai Society Mathematical Studies, 11, Gábor Halász, László Lovász, Dezső Miklós, and Vera T. Sós (Eds.) (2002), Springer Verlag, New York, NY, 219–239.

E-02. T. Erdélyi, *Polynomials with Littlewood-type coefficient constraints*, in Approximation Theory X: Abstract and Classical Analysis, Charles K. Chui, Larry L. Schumaker, and Joachim Stöckler (Eds.) (2002), Vanderbilt University Press, Nashville, TN, 153–196.

E-08a. T. Erdélyi, *Extensions of the Bloch-Pólya theorem on the number of distinct real zeros of polynomials*, Journal de théorie des nombres de Bordeaux **20** (2008), 281–287.

E-08b. T. Erdélyi, *An improvement of the Erdős-Turán theorem on the zero distribution of polynomials*, C. R. Acad. Sci. Paris Sér. I Math. **346** (2008), 267–270.

E-50. P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Annals of Math. **57** (1950), 105–119.

F-80. Le Baron O. Ferguson, *Approximation by Polynomials with Integral Coefficients*, Amer. Math. Soc., Rhode Island, 1980.

F-00. W. Foster and I. Krasikov, *An improvement of a Borwein-Erdélyi-Kós result*, Methods Appl. Anal. **7** (2000), no. 4, 605-614.

G-05. C.S. Güntürk, *Approximation by power series with* ± 1 *coefficients*, Int. Math. Res. Not. (2005), no. 26, 1601–1610.

H-82. L.K. Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin Heidelberg, New York, 1982.

K-85. J.-P. Kahane, *Some Random Series of Functions*, 2nd ed. Cambridge Stud. Adv. Math. 5, Cambridge Univ. Press, Cambridge, 1985.

K-04. I. Krasikov, *Multiplicity of zeros and discrete orthogonal polynomials*, Results Math. **45** (2004), no. 1-2, 59–66.

K-09. G. Kós, P. Ligeti, and P. Sziklai, *Reconstruction of matrices from submatrices*, Math. Comp. **78** (2009), 1733–1747.

M-68. M. Minsky and S. Papert, *Perceptrons: An Introduction to Computational Geometry*, MIT Press, Cambridge Mass., 1968.

M-03. M.J. Mossinghoff, *Polynomials with restricted coefficients and prescribed noncyclotomic factors*, (electronic), London Math. Soc. J. Comput. Math. **6** (2003), 314–325.

N-94. N. Nisan and M. Szegedy, *On the degree of Boolean functions as real polynomials*, Earlier version in STOC92, Computational Complexity **4(4)** (1994), 301–313.

O-93. A.M. Odlyzko and B. Poonen, *Zeros of polynomials with* $0, 1$ *coefficients*, Enseign. Math. (2) **39** (1993), 317–348.

R-07. E.A. Rakhmanov, *Bounds for polynomials with a unit discrete norm*, Ann. of Math. **165** (2007), 55-88.

R-04. F. Rodier, *Sur la non-linéarité des fonctions booléennes*, Acta Arith. **115(1)** (2004), 1–22.

P-12. A.A. Prikhodko, *On flat Littlewood polynomials with unimodular coefficients*, manuscript in Russian (2012).

P-13. I.E. Pritsker and A.A. Sola, *Expected discrepancy for zeros random algebraic polynomials*, Proc. Amer. Math. Soc. (to appear).

S-54. R. Salem and A. Zygmund, *Some properties of trigonometric series whose terms have random signs*, Acta Math. **91** (1954), 245–301.

Sch-33. I. Schur, *Untersuchungen über algebraische Gleichungen.*, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 403–428.

S-99. I.E. Shparlinski, *Finite Fields: Theory and Computation: the Meeting Point of Number Theory, Computer Science, Coding Theory and Cryptography*, Dordrecht, London, 1999.

Š-03. R. Špalek, *A dual polynomial for OR*, Technical Report arXiv:0803.4516 [cs.CC], arXiv, 2008.

Sz-34. G. Szegő, *Bemerkungen zu einem Satz von E. Schmidt uber algebraische Gleichungen.*, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1934), 86–98.

T-07. V. Totik and P. Varjú, *Polynomials with prescribed zeros and small norm*, Acta Sci. Math. (Szeged) **73** (2007), no. 3-4, 593–611.

T-84. P. Turán, *On a New Method of Analysis and its Applications*, Wiley, New York, 1984.

Department of Mathematics, Texas A&M University, College Station, Texas 77843
E-mail address: `terdelyi@math.tamu.edu`