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

By

TAMÁS ERDÉLYI

Abstract. A highlight of this paper states that there is an absolute constant $c_1 > 0$ such that every polynomial P of the form $P(z) = \sum_{j=0}^n a_j z^j$, $a_j \in \mathbb{C}$ with

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

for 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 similar results 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 $F_n = \{1, 2, \ldots, n\}$, there exists 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 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 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 the interval [0, 1]. For example, we proved that there exist 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 in $\{-1, 0, 1\}$. 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 $c \log N$,

JOURNAL D'ANALYSE MATHÉMATIQUE, Vol. 127 (2015)
DOI 10.1007/s11854-015-0025-1

where N is the number of non-zero coefficients in f and $c > 0$ is an absolute constant.

These questions with coefficients restricted to integers have a Diophantine nature and have been studied from several points of view; see [A-79, B-98, B-95, B-94, F-80, O-93].

One key to the analysis is the study of the related problem of giving an upper bound for the multiplicity of zeros these restricted polynomials can have at 1. In [B-99] and [B-13], we found essentially sharp bounds for the classes of polynomials of the form

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

with fixed $|a_0| \neq 0$.

Variants of these questions have attracted considerable study, though rarely have precise answers been given; 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 can be rephrased as this type of question: specifically, "What is the highest possible order of a zero at 1 of a polynomial with l_1 norm $2n$ having integer coefficients?" It is conjectured to be n; see [H-82], [B-94], or [B-02].

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 exists a polynomial $P \neq 0$ of the form

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

such that $(x-1)^k$ divides $P(x)$. Also, let $\kappa_\infty(n, L)$ be the largest possible value of k for which there exists a polynomial $P \neq 0$ of the form

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

such that $(x-1)^k$ divides $P(x)$. In [B-99], we proved that there exists 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 $L \in (0, 1]$. Recently, in [B-13], we found the correct order of magnitude of $\kappa_\infty(n, L)$ in the case $L \geq 1$; there exist absolute constants $c_1 > 0$ and $c_2 > 0$ such that

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

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

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

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

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

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 all 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, e.g., [A-02, B-98, B-95, B-96, B-97b, B-97a, B-97, B-00, B-07, B-08a, B-08b, C-02, C-13, C-10, D-99, D-01, D-03, E-08b, E-08a, 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].

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] in order to obtain sharp bounds for the multiplicity of the zero at 1 of polynomials belonging to various classes of constrained polynomials.

2 Pseudo-Boolean functions

Throughout this paper, n is an integer greater than 1, $D_n = \{0, 1, \dots, n\}$, and $F_n = \{1, 2, \dots, n\}$.

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 σ in the group Σ_n of permutations of $\{1, 2, \dots, n\}$, and $\mathbf{x} \in \{-1, 1\}^n$, where $\mathbf{x}_\sigma := (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$ denotes a σ permuted version of $\mathbf{x}$. Note that if $p : \{-1, 1\}^n \to \mathbb{R}$ is a polynomial in variables $x_1, x_2, \dots, x_n$ then, since $x_j^2 = 1$, 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.

To each symmetric function $f : \{-1, 1\}^n \to \mathbb{R}$ is associated a function $F : D_n \to \mathbb{R}$ such that

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

where $|\mathbf{x}| := \big(n - (x_1 + x_2 + \cdots + x_n)\big)/2$ is the Hamming weight of $\mathbf{x}$, i.e., $\mathbf{x}$ is the number of -1 components of $\mathbf{x}$. Using the fundamental theorem of symmetric polynomials, it can be easily proved (see, e.g., [M-68]) that corresponding to each symmetric multi-linear polynomial $p : \{-1, 1\}^n \to \mathbb{R}$ is a polynomial $P : D_n \to \mathbb{R}$ of the same degree such that

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

Observe 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 $P : D_n \to \mathbb{R}$, 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 $p : D_n \to \mathbb{R}$ of a single variable over $\mathbb{R}$. We define a scalar product on X_n by

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

This induces the scalar product

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

on Y_n, where

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

A function $f : \{-1, 1\}^n \to \{-1, 1\}$ is called an **n-bit Boolean function**. Such functions 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

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

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

Motivated by this question and answer, in this paper we prove the following results. Let $S_n = \{j^2 : j \in D_{\lfloor \sqrt{n} \rfloor}\} \cup \{2\}$.

Theorem 3.1. *Every polynomial P of the form*

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

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 exists an absolute constant $c_1 > 0$ such that every polynomial P of the form*

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

satisfying

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

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 [B-95, pp. 92–100], one can easily see that there exists a polynomial P of the form

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

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

Theorem 3.4. *Let* $0 < m < \sqrt{n/2}$. *Every polynomial* P *of the form*

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

satisfying

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

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

4 Lemmas

In this section, we state some lemmas, which are important in their own right. We prove them in Section 5 and apply them in Section 6, where we prove the theorems formulated in Section 3.

We introduce the polynomials

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

The multiplicative factor in front of the product sign is chosen so that $Q_n(0) = 1$. The degree of Q_n is $n - \lfloor\sqrt{n}\rfloor - 1$.

Lemma 4.1 (Špalek, [Š-03])**.**

$$Q_n(0) = 1, \quad \binom{n}{2}|Q_n(2)| \le 12, \quad \binom{n}{k^2}|Q_n(k^2)| \le \frac{8}{k^2}, \quad k = 1, 2, \ldots, \lfloor\sqrt{n}\rfloor.$$

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].

Lemma 4.2. *Let* $0 \le m \le n$ *be integers. 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 *of multiplicity at least* $m + 1$, *then* $\sum_{j=0}^{n} a_j Q(j) = 0$ *for every polynomial* $Q \in \mathcal{P}_m$.

Lemma 4.3. *Let* $P \in \mathcal{P}_m$ *and* $x_0 < x_1 < \cdots < x_m$ *and* $x_0^* < x_1^* < \cdots < x_m^*$ *be reals.*

(i) $P(x) = \sum_{k=0}^{m} P(x_k)L_k(x)$ *for all real x, where*

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

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

$$\delta_{j,k} := \begin{cases} 0, & j \neq k, \\ 1, & j = k \end{cases}$$

for $j, k \in \{0, 1, \dots, m\}$.

(ii) *Let $E_m := \{x_0, x_1, \dots, x_m\}$ and $y \le x_0$. Then*

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

(iii) *Let $E_m^* = \{x_0^*, x_1^*, \cdots, x_m^*\}$. Suppose*

$$y \le x_0^*, \quad x_{k+1}-x_k \le x_{k+1}^*-x_k^* \quad \textit{for } k=0,1,\dots,m-1, \quad x_m^* \le x_m.$$

Then

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

(iv) *Suppose*

$$y \le x_0^*, \quad x_{k+1}-x_k \le x_{k+1}^*-x_k^* \quad \textit{for } k=0,1,\dots,m-1, \quad x_m^* \le x_m$$

and that $Q \in \mathcal{P}_m$ satisfies $(-1)^k Q(x_k) \ge \delta > 0$ for some $\delta > 0$ and $k = 0, 1, \dots, m$. Then

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

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 4.4. *There exists an absolute constant $c > 0$ such that*

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

for every $P \in \mathcal{P}_m$ with $m \le \sqrt{nL/16}$ and $1 \le L < 16n$. This 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 used prove Lemma 4.4 is somewhat similar to the key idea to prove the bounded Remez-type inequality of [B-97a] for non-dense Müntz spaces. The proof of Lemma 4.4 in the case $n/16 \le m^2 \le n/2$ can also be obtained simply from the Markov inequality for polynomials whereas, in the case $m = n - 1$, it follows from the basics of Lagrange interpolation. However, the proof in the general case is more subtle. The lemma was 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. An interesting recent closely related result is due to E. A. Rakhmanov [R-07].

The result below plays a fundamental role in the proof of Theorem 3.2. We prove it with the help of of Lemma 4.4 in Section 5.

Lemma 4.5. *Let $c > 0$ be as in Lemma 4.4 and $c_1 := (32c)^{-1/2}$. If $e^{2c} \le M < e^{32cn}$, there exists a polynomial Q of degree at most $n - \lfloor c_1\sqrt{n}\log M \rfloor$ such that $\sum_{k=1}^{n} \binom{n}{k}|Q(k)| < M|Q(0)|$.*

The following lemma is quite useful for the case $m \le \sqrt{n/4}$. We prove it in Section 5 as a simple consequence of Markov's inequality.

Lemma 4.6. *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 following lemma below is used in the proof of Theorem 3.4.

Lemma 4.7. *Suppose $m \le \sqrt{n/2}$. There exists 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 Proofs of the lemmas

Proof of Lemma 4.1. We follow Špalek [Š-03]. Let $m = \lfloor\sqrt{n}\rfloor$. First observe that for all integers $0 \le k \le m$,

$$\begin{aligned} \frac{(m!)^2}{(m+k)!(m-k)!} &= \frac{m(m-1)\cdots(m-k+1)}{(m+k)(m+k-1)\cdots(m+1)} \\ &= \prod_{j=1}^{k}\left(1 - \frac{k}{m+j}\right) \le 1. \end{aligned} \tag{5.1}$$

Using this with $k = 2$, we obtain

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

Observe also that for $k \in \{1, 2, \dots, m\}$,

$$\begin{aligned}|Q_n(k^2)| &= 2\frac{(m!)^2}{n!}\prod_{\substack{j\in D_n\\ j\ne k^2}}|k^2-j|\frac{1}{|k^2-2|}\prod_{\substack{j\in D_m\\ j\ne k}}\frac{1}{(k+j)|k-j|}\\ &= 2\frac{(m!)^2}{n!}(k^2)!(n-k^2)!\frac{2k(k-1)!}{(k+m)!k!(m-k)!|k^2-2|}\\ &= 4\frac{(k^2)!(n-k^2)!}{n!}\frac{(m!)^2}{(m+k)!(m-k)!}\frac{1}{|k^2-2|}.\end{aligned}$$

Hence (5.1) yields

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

□

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 $1/k^2$.

Proof of Lemma 4.3. (i) and (ii) are well-known facts about Lagrange interpolation, hence their proof is omitted.

To prove (iii), let

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

By assumption, $0 < (-1)^k L_k^*(y) \le (-1)^k L_k(y)$ for $k = 0, 1, \dots, m$, and the result follows from (4.3).

Part (iv) follows easily from part (iii). □

Proof of Lemma 4.4. First consider the case that for given n, $L < 16n$ and $n < 656L$. Let $m \le \sqrt{nL/16} < n$, $P \in \mathcal{P}_m$, $x_j := j + 1$ for $j = 0, 1, \dots, m$, and $E_m := \{x_0, x_1, \dots, x_m\} \subset F_n$. Let L_k be the basic Lagrange interpolating polynomials defined by (4.2). Observe that

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

and hence

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

completing the proof in this case.

Now assume that $n \geq 328L$. Without loss of generality, we may assume that $n = n_0^2$ and $L = L_0^2$, where n_0 and L_0 are integers, so that $m = \sqrt{(nL)/16}$ is an integer. Let T_m be the Chebyshev polynomial of degree m on the interval $[-1, 1]$, i.e.,

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

Let $\tilde{T}_m$ be the Chebyshev polynomial T_m transformed linearly from $[-1, 1]$ to the interval $[164L, n]$, viz.,

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

Using the explicit form

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

setting $s := 328L/(n-164L)$ and noticing that $s \leq 656L/n \leq 2$, we check easily that

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

Let $\xi_0 < \xi_1 < \cdots < \xi_m$ denote the extreme points of $\tilde{T}_m$ on $[164L, n]$, viz.,

$$\begin{aligned}\xi_0 &= 164L, \\ \xi_j &= \frac{1}{2}(n-164L)\cos\frac{(m-j)\pi}{m} + \frac{1}{2}(n+164L), \quad j = 1, 2, \dots, m-1, \\ \xi_m &= n.\end{aligned}$$

Then

$$\tilde{T}_m(\xi_j) = (-1)^{m-j}, \quad j = 0, 1, \ldots, m. \tag{5.3}$$

Let $\eta_j = \lceil \xi_j \rceil$. Observe that since $n \geq 328L$,

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

and hence

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

Thus

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

Now, since $m^2 = (nL)/16$ and $n \geq 328L$, we deduce that

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

Using the mean value theorem, Bernstein's inequality (see, e.g., [B-95, p. 233]), and (5.4), we have

$$\begin{aligned} |\tilde{T}_m(\xi_j) - \tilde{T}_m(x)| &\leq (x - \xi_j) \max_{\xi \in [\eta_j, \xi_j]} |\tilde{T}_m'(\xi)| \\ &\leq \frac{2m^2}{(n - 164L)L} \leq \frac{4m^2}{nL} \leq \frac{1}{4} \end{aligned} \tag{5.5}$$

for all $x \in [\xi_j, \eta_j]$ and $j \in [L, m - L - 1]$. Also,

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

for all $j \in [0, L - 1] \cup [m - L, m - 1]$. Combining (5.3) and (5.5), we get

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

hence

$$(-1)^{m-j}\tilde{T}_m(\eta_j) \geq \frac{3}{4}, \quad j \in [L, m - L - 1], \tag{5.7}$$

and

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

Define

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

and let $E_m = \{x_0, x_1, \cdots, x_m\}$. Recalling (5.7) and (5.8), we have

$$E_m = \{x_0 < x_1 < \cdots < x_m\}.$$

Now define

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

and let $E_m^* = \{x_0^*, x_1^*, \ldots, x_m^*\}$. Observe that $x_0^* < x_1^* < \cdots < x_m^*$ and $E_m^* \subset F_n$. Also (5.6) implies that the assumptions of Lemma 4.3(iv) on E_m and E_m^* with $Q = \tilde{T}_m$ are satisfied. The inequality of the lemma now follows from Lemma 4.3(iv) and (5.2).

We now 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 $n = n_0^2$ and $L = l6L_0^2$, where n_0 and L_0 are integers, so that $m = \sqrt{(nL)/16}$ is an integer. Let $\hat{T}_m$ be the Chebyshev polynomial T_m transformed linearly from $[-1, 1]$ to the interval $[0, n]$, i.e.,

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

where

$$\begin{aligned} 0 < x_k &= \frac{n}{2}\left(1 + \cos\frac{2k-1}{2m}\pi\right) = n \sin^2 \frac{2k-1}{4m}\pi \\ &\leq \frac{nk^2\pi^2}{4m^2} \leq \frac{4nk^2\pi^2}{nL} \leq \frac{40k^2}{L} \leq \frac{k}{2}, \quad 1 \leq k \leq L' := \left\lfloor \frac{L}{80} \right\rfloor. \end{aligned}$$

Now, defining

$$P_m(x) := \hat{T}_m(x) \prod_{k=1}^{L'} \frac{x-k}{x-x_k},$$

we have

$$|P_m(j)| \le |\hat{T}_m(j)| \le 1, \quad j \in [L'+1, n] \cap F_n,$$

and

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

Hence, for $j \in F_n$, $|P_m(j)| \le 1$. This, together with the fact that

$$|P_m(0)| \ge |\hat{T}_m(0)| \prod_{k=1}^{L'} \left|\frac{k}{x_k}\right| \ge \prod_{k=1}^{L'} \frac{k}{k/2} \ge 2^{L'} \ge 2^{L/80-1}$$

completes the proof. □

Proof of Lemma 4.5. We use the notation introduced in Section 2.

Let F and P be the polynomials $D_n \longrightarrow \mathbb{R}$ associated to $f \in X_n$ and $p \in X_n$, respectively, as described in Section 2. Let $M = \exp(2cL)$, where the constant $c > 0$ is as in Lemma 4.4. Let $m = \lfloor\sqrt{nL/16}\rfloor$,

$$U = \{f \in X_n : F(0) \ge \exp(2cL),\ |F(j)| \le 1,\ j = 1, 2, \ldots, n\},$$

and $V_m = \{p \in X_n : P \in \mathcal{P}_m\}$ where, as before, $\mathcal{P}_m$ denotes the set of all polynomials of degree at most m with real coefficients. Lemma 4.4 implies $U \cap V_m = \emptyset$. Since two disjoint convex sets in a finite dimensional vector space can be separated by a hyper-plane, there exists a symmetric polynomial $g \in X_n$ such that

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

and

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

where G is the polynomial $D_n \longrightarrow \mathbb{R}$ associated to $g \in X_n$. 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 $\sum_{k=0}^{n} \varepsilon_k \binom{n}{k} G(k) \ge \alpha > 0$ whenever $\varepsilon_0 = \exp(2cL)$ and $\varepsilon_k \in \{-1, 1\}$, $k = 1, 2, \ldots, n$. Hence

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

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

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

and $\widetilde{G} \in \mathcal{P}_n$ the polynomial $D_n \to \mathbb{R}$ associated to $\widetilde{g} \in X_n$. Since the pure high degree of $g \in X_n$ is at least $m+1$, $\widetilde{G} \in \mathcal{P}_n$ is 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 $j = 0, 1, \dots, n$,

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

□

Proof of Lemma 4.6. Suppose $P \in \mathcal{P}_m$ and $\|P\|_{F_n} = 1$. Choose $y \in [0,n]$ such 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 [B-95, p. 233] 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 4.7. The proof of this lemma is very similar to that of Lemma 4.5. However, at one point, an application of Lemma 4.6 rather than Lemma 4.4 is needed. □

6 Proof of the theorems

Proof of Theorem 3.1. We prove the contrapositive statement. Suppose that a polynomial P of the form

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

has a zero at 1 of 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 $n - \lfloor\sqrt{n}\rfloor - 1$, and

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

where Q_n is as defined by (4.1). □

Proof of Theorem 3.2. Let the absolute constant $c > 0$ be as in Lemma 4.4. If $2 \le e^{2c}$, then the theorem follows from Theorem 3.4. Hence we may assume that $e^{2c} \le M < e^{32cn}$. Let the absolute constant $c_1 > 0$ be as in Lemma 4.5. Suppose that a polynomial P of the form

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

has a zero at 1 of multiplicity at least $n - \lfloor c_1\sqrt{n\log M}\rfloor + 1$. Lemma 4.2 then gives $\sum_{j=0}^{n} a_j Q(j) = 0$ for all polynomials Q of degree at most $n - \lfloor c_1\sqrt{n\log M}\rfloor$. Using the assumptions

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

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 4.5. □

Proof of Theorem 3.4. The proof of the theorem is very similar to that of Theorem 3.2 given in the case $e^{2c} \le M < e^{32cn}$. However, at one point, an application of Lemma 4.7 rather than Lemma 4.5 is needed. □

Acknowledgments. The author thanks 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-Verlag, 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. (2) **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 Boston, Boston, MA, 1987, pp. 53–73.

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

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

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

[B-97a] P. Borwein and T. Erdélyi, *Generalizations of Müntz's theorem via a Remez-type inequality for Müntz spaces*, J. Amer. Math. Soc. **10** (1997), 327–349.

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

[B-07] P. Borwein and T. Erdélyi, *Lower bounds for the number of zeros of cosine polynomials in the period: 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 polynomials: solution to a 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. (3) **79** (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. **159** (2013), 387–395.

[B-08b] P. Borwein, T. Erdélyi, and F. Littmann, *Polynomials with coefficients from a finite set*, Trans. Amer. Math. Soc. **360** (2008), 5145–5154.

[B-94] P. Borwein and C. Ingalls, *The Prouhet-Tarry-Escott problem*, Enseign. Math. (2) **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), 425–433.

[B-97] D. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comp. **66** (1977), 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*, IEEE Computer Soc., Los Alamitos, CA, pp. 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), 2313–2318.

[C-13] J. M. Cooper and A. M. Dutle, *Greedy Galois games*, Amer. Math. Monthly **120** (2013), 441–451.

[C-92] D. Coppersmith and T. J. Rivlin, *The growth of polynomials bounded at equally spaced points*, SIAM J. Math. Anal. **23** (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), 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 for polynomials of small measure*, Acta Arith. **98** (2001), 279–292.

[D-03] M. Dudik and L. J. Schulman, *Reconstruction from subsequences*, J. Combin. Theory Ser. A **103** (2003), 337–348.

[E-01] T. Erdélyi, *Markov-Bernstein type inequalities for polynomials under Erdős-type constraints*, in *Paul Erdős and his Mathematics I*, Springer-Verlag New York, NY, 2002, pp. 219–239.

[E-02] T. Erdélyi, *Polynomials with Littlewood-type coefficient constraints*, in *Approximation Theory X*, Vanderbilt University Press, Nashville, TN, 2002, pp. 153–196.

[E-08a] T. Erdélyi, *An improvement of the Erdős-Turán theorem on the distribution of zeros of polynomials*, C. R. Acad. Sci. Paris **346** (2008), 267–270.

[E-08b] T. Erdélyi, *Extensions of the Bloch-Pólya theorem on the number of distinct real zeros of polynomials*, J. Théor. Nombres Bordeaux **20** (2008) 281–287.

[E-50] P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Ann. of Math. (2) **51** (1950), 105–119.

[F-80] Le Baron O. Ferguson, *Approximation by Polynomials with Integral Coefficients*, American Mathematical Society, Providence, RI, 1980.

[F-00] W. Foster and I. Krasikov, *An improvement of a Borwein-Erdélyi-Kós result*, Methods Appl. Anal. **7** (2000), 605–614.

[G-05] C. S. Güntürk, *Approximation by power series with* ± 1 *coefficients*, Int. Math. Res. Not. **2005**, 1601–1610.

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

[K-85] J. P. Kahane *Some Random Series of Functions*, 2nd ed., Cambridge University Press, Cambridge, 1985.

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

[K-04] I. Krasikov, *Multiplicity of zeros and discrete orthogonal polynomials*, Results Math. **45** (2004), 59–66.

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

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

[N-94] N. Nisan and M. Szegedy, *On the degree of Boolean functions as real polynomials*, Comput. Complexity **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.

[P-12] A. A. Prikhodko, *On flat Littlewood polynomials with unimodular coefficients*, (2012).

[P-13] I. E. Pritsker and A. A. Sola, *Expected discrepancy for zeros random algebraic polynomials*, Proc. Amer. Math. Soc. **142** (2014), 4251–4263.

[R-07] E. A. Rakhmanov, *Bounds for polynomials with a unit discrete norm*, Ann. of Math. (2) **165** (2007), 55–88.

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

[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*, Kluwer Academic Poublishers, Dordrecht, 1999.

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

[Sz-34] G. Szegő, *Bemerkungen zu einem Satz von E. Schmidt über 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), 593–611.

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

Tamás Erdélyi
Department of Mathematics
Texas A&M University
College Station, TX 77843, USA
email: terdelyi@math.tamu.edu

(Received March 30, 2013 and in revised form June 10, 2013)