

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

TAMÁS ERDÉLYI

ABSTRACT. Let $p : \{-1, 1\}^n \rightarrow \mathbb{R}$ be a polynomial in variables x_1, x_2, \dots, x_n . Since $x_j^2 = 1$ we can restrict our consideration to *multi-linear* polynomials in which each variable appears with degree at most 1. Using the observation that every $p : \{-1, 1\}^n \rightarrow \mathbb{R}$ symmetric multi-linear polynomial can be represented by a polynomial $P : \{0, 1, \dots, n\} \rightarrow \mathbb{R}$ of a single variable as

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

with

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

we prove a number of surprising new results estimating the multiplicity of the zero at 1 of polynomials from various classes of polynomials with constrained coefficients. Our most important tool is the essentially sharp result below due to Coppersmith and Rivlin. To formulate it let \mathcal{P}_m denote the set of all polynomials of degree at most m with real coefficients, and let $F_n := \{1, 2, \dots, n\}$.

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

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

for every polynomial $P \in \mathcal{P}_m$ with $m \leq \sqrt{nL/16}$ and $1 \leq L < 16n$.

A short and elegant proof of the above result is included in our discussion.

1. NUMBER OF ZEROS AT 1 OF POLYNOMIALS WITH RESTRICTED COEFFICIENTS

In this section we list a few results of [BEK-99] and quote the main results from [BE-97a] and [B-97].

The following two theorems offer upper bounds for the number of zeros polynomial of degree n can have at 1 if the maximum modulus of its coefficients is at most 1. The first result sharpens and generalizes results of Amoroso [A-90], Bombieri and Vaaler [BV-87], and Hua [H-82] who give versions of this result for polynomials with integer coefficients.

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

Theorem 1.1. *There is an absolute constant $c > 0$ such that every polynomial p of the form*

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

has at most

$$c(n(1 - \log |a_0|))^{1/2}$$

zeros at 1.

Applying Theorem 1.1 with $q(x) := x^{-n}p(x^{-1})$ immediately gives the following.

Theorem 1.2. *There is an absolute constant $c > 0$ such that every polynomial p of the form*

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

has at most

$$c(n(1 - \log |a_n|))^{1/2}$$

zeros at 1.

The sharpness of the above theorems is shown by

Theorem 1.3. *For every $n \in \mathbb{N}$ there exists a polynomial p_n of the form*

$$p_n(x) = \sum_{j=0}^n a_j x^j, \quad |a_j| \leq 1, \quad a_j \in \mathbb{R},$$

that has a zero at 1 with multiplicity at least

$$\min \left\{ \frac{1}{6}((n(1 - \log |a_0|))^{1/2} - 1), n \right\}.$$

The following two theorems can be obtained from the results above with slightly worse constants. However, we have distinct attractive proofs of Theorems 1.4 and 1.5 below and in [BEK-99] they are also presented.

Theorem 1.4. *Every polynomial p of the form*

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

has at most $\lfloor \frac{16}{7}\sqrt{n} \rfloor + 4$ zeros at 1.

Theorem 1.5. *For every $n \in \mathbb{N}$, there exists a polynomial*

$$p_n(x) = \sum_{j=0}^{n^2-1} a_j x^j, \quad a_{n^2-1} = 1, \quad a_0, a_1, \dots, a_{n^2-2} \in (-1, 1),$$

that has a zero at 1 with multiplicity at least $n - 1$.

Theorem 1.5 immediately implies

Corollary 1.6. *For every $n \in \mathbb{N}$ there exists a polynomial p_n of the form*

$$p_n(x) = \sum_{j=0}^n a_j x^j, \quad a_n = 1, \quad |a_j| \leq 1, \quad a_j \in \mathbb{R},$$

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

Let

$$\mathcal{F}_n := \left\{ \sum_{j=0}^n a_j x^j : a_j \in \{-1, 0, 1\} \right\}$$

denote the set of polynomials of degree at most n with coefficients from $\{-1, 0, 1\}$. The next related result is well known (in a variety of forms). Its proof is simple and may be found in [BEK-99] too.

Theorem 1.7. *There is an absolute constant $c > 0$ such that for every $n \in \mathbb{N}$ there is a $p \in \mathcal{F}_n$ that has a zero at 1 with multiplicity at least $c\sqrt{n/\log(n+1)}$.*

Theorems 1.4 and 1.7 show that the right upper bound for the number of zeros a polynomial $p \in \mathcal{F}_n$ can have at 1 is somewhere between $c_1\sqrt{n/\log(n+1)}$ and $c_2\sqrt{n}$ with absolute constants $c_1 > 0$ and $c_2 > 0$. Completely closing the gap in this problem looks quite difficult.

Our next theorem slightly generalizes Theorem 1.1 and offers an *explicit* constant.

Theorem 1.8. *If $|a_0| \geq \exp(-L^2)$ and $|a_j| \leq 1$ for each $j = L^2 + 1, L^2 + 2, \dots, n$, then the polynomial*

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

has at most $\frac{44}{7}(L+1)\sqrt{n} + 5$ zeros at 1.

In [BE-97] we proved the following result.

Theorem 1.9. *Every polynomial p of the form*

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

has at most $c\sqrt{n}$ zeros inside any polygon with vertices on the unit circle, where the constant c depends only on the polygon.

As an attractive related result in [BEK-99] we obtained the following.

Theorem 1.10. *There exist absolute constants $c_1 > 0$ and $c_2 > 0$ such that*

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

for every $n \geq 2$.

Let

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

denote the set of polynomials of degree at most n with coefficients from $\{-1, 1\}$. It was conjectured by Byrnes that there is an absolute constant $c > 0$ such that every $p \in \mathcal{L}_n$ has at most $c \log n$ zeros at 1. However, the best known result is the one below due to D. Boyd [B-97].

Theorem 1.11. *There is an absolute constant $c > 0$ such that every $p \in \mathcal{L}_n$ has at most*

$$\frac{c \log^2 n}{\log \log n}$$

zeros at 1.

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].

2. PSEUDO-BOOLEAN FUNCTIONS

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

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

denotes a σ permuted version of \mathbf{x} . Note that if $p : \{-1, 1\}^n \rightarrow \mathbb{R}$ is a polynomial in variables x_1, x_2, \dots, 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 and pure high degree at least d' if each term in p is a product of at most d and at least d' variables.

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

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

where

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

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 [MP-69], for example) that for every symmetric multi-linear polynomial $p : \{-1, 1\}^n \rightarrow \mathbb{R}$ there is a polynomial $P : D_n \rightarrow \mathbb{R}$ of a single variable of the same degree such that

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

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 $P : D_n \rightarrow \mathbb{R}$ of a single variable we mean the pure high degree of its corresponding multi-linear polynomial $p : \{-1, 1\}^n \rightarrow \mathbb{R}$.

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

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

A function $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ 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 [SZ-54], Kahane [K-85], and others about the related problem of real polynomials with random coefficients.

3. NEW RESULTS

In October, 2002, Mario 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 ˆSpalek [S-03] answered this question. We state his result as Lemma 3.1 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 $S = \{j^2 : j \in D_m\} \cup \{2\}$ denote the set containing the squares up to n and the number 2.

Theorem 3.1. *Any polynomial P of the form*

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

satisfying

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

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 $j \in D_n \setminus S$.

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

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

satisfying

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

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

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 [BE-95]), one can easily see that there is a polynomial P of the form

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

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*

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

satisfying

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

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

4. LEMMAS

In what follows, associated with a complex-valued function g defined on a set A we will use the notation

$$\|g\|_A := \sup_{x \in A} |g(x)|.$$

Let $m = \lfloor \sqrt{n} \rfloor$ and let $S = \{j^2 : j \in D_m\} \cup \{2\}$ denote the set containing the squares up to n and the number 2. We introduce the polynomial

$$(4.1) \quad Q(x) := 2(-1)^{n-m-1} \frac{(m!)^2}{n!} \prod_{j \in D_n \setminus S} (x - j).$$

The multiplicative factor of Q in front of the product sign is chosen so that $Q(0) = 1$. The degree of Q is $n - m - 1$. The lemma below is due to Špalek [Š-03], who was the first to give a dual polynomial for OR explicitly by having the fortunate idea of studying the polynomial Q defined above.

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

$$\binom{n}{2} |Q(2)| \leq 12, \quad \binom{n}{k^2} |Q(k^2)| \leq \frac{8}{k^2}, \quad k = 1, 2, \dots, m.$$

The following result is well known and can easily be proved as a simple exercise. It was observed and used in [BEK-99], for instance.

Lemma 4.2. *If 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 with multiplicity at least $m+1$, then $\sum_{j=0}^n a_j Q(j) = 0$ for every polynomial Q of degree at most m .

Let \mathcal{P}_m denote the set of all polynomials of degree at most m with real coefficients. The following facts are well-known about Lagrange interpolation. If $P \in \mathcal{P}_m$ and

$$x_0 < x_1 < \dots < x_m$$

are real numbers, then

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

where

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

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

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

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

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

Let

$$E_m = \{x_0 < x_1 < \dots < x_m\} \quad \text{and} \quad E_m^* = \{x_0^* < x_1^* < \dots < x_m^*\}.$$

Lemma 4.3. *Suppose $y < x_1^*$, $x_m^* \leq x_m$, and*

$$x_{j+1} - x_j < x_{j+1}^* - x_j^*, \quad j = 1, 2, \dots, m.$$

Then

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

The lemma below is a straightforward consequence of Lemma 4.3.

Lemma 4.4. *Suppose $y < x_1^*$, $x_m^* < x_m$, and*

$$x_{j+1} - x_j < x_{j+1}^* - x_j^*, \quad j = 1, 2, \dots, m,$$

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

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

Then

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

A key to the proof of Theorem 3.2 is the Coppersmith-Rivlin inequality in [CR-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*

$$|P(0)| \leq \exp(cL) \|P\|_{F_n}$$

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 and arguably more elegant 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 [BE-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 [CR-92] and is used in [BC-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 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 $m \leq \sqrt{n/4}$.

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

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

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

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

$$(5.1) \quad \frac{(m!)^2}{(m+k)!(m-k)!} = \frac{m(m-1) \cdots (m-k+1)}{(m+k)(m+k-1) \cdots (m+1)} = \prod_{j=1}^k \left(1 - \frac{k}{m+j}\right) \leq 1.$$

Using this with $k = 2$, we obtain

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

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

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

Hence (5.1) yields

$$|Q(k^2)| \leq \frac{4}{\binom{n}{k^2}} \frac{1}{|k^2 - 2|} \leq \frac{4}{\binom{n}{k^2}} \frac{1}{k^2/2} \leq \frac{8}{\binom{n}{k^2} k^2}, \quad k = 1, 2, \dots, m.$$

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

Proof of Lemma 4.3. Let

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

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

$$0 < (-1)^k L_k^*(y) < (-1)^k L_k(y), \quad k = 0, 1, \dots, m,$$

and the lemma follows from (4.2).

Proof of Lemma 4.5. To prove the inequality of the lemma, 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. First we also assume that $n \geq 328L$, we will examine the easier case $n \leq 328L$ separately.

Let T_m be the Chebyshev polynomial of degree m on the interval $[-1, 1]$, that is,

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

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

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

Using the explicit form

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

of the Chebyshev polynomial T_m , with the notation

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

we can easily deduce that

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

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

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

that is,

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

and

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

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

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

and hence

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

So

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

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

$$(5.4) \quad 164L + (n - 164L) \frac{L^2}{m^2} \leq \xi_L < \eta_{m-L-1} \leq n - (n - 164L) \frac{(L+1)^2}{m^2} + 1 \\ \leq n - (n - 164L) \frac{L^2}{m^2}.$$

Using the Mean Value Theorem, Bernstein's inequality, and (5.4) we obtain

$$(5.5) \quad |Q_m(\xi_j) - Q_m(x)| \leq (x - \xi_j) \max_{\xi \in [\eta_j, \xi_j]} |Q'_m(\xi)| \\ \leq \frac{2m^2}{(n - 164L)L} \leq \frac{4m^2}{nL} \\ \leq \frac{1}{4}, \quad x \in [\xi_j, \eta_j], \quad j \in [L, m - L - 1].$$

Also,

$$(5.6) \quad \xi_{j+1} - \xi_j = \frac{1}{2}(n - 164L) \left(\cos \frac{(m - (j+1))\pi}{m} - \cos \frac{(m-j)\pi}{m} \right) \\ \leq \frac{1}{2}(n - 164L) \frac{\pi}{m} \sin \frac{L\pi}{m} \leq \frac{1}{2} \frac{\pi^2 n L}{m^2} \leq 80,$$

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

Combining (5.3) and (5.5) we get

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

and hence

$$(5.7) \quad (-1)^{m-j} Q_m(x_j) \geq \frac{3}{4}, \quad j = 0, 1, \dots, m,$$

and

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

We define

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

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

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

Observe that (5.6) implies that the assumptions of Lemma 4.3 on E_m and E_m^* with $Q = Q_m$ are satisfied. Now Lemma 4.4 together with (5.2) finishes the proof of the inequality of the lemma in the case $n \geq 328L$. To prove the inequality of the lemma in the case when, together with $L < 16n$ we also have $n < 328L$, let $m \leq \sqrt{nL/16} < n$ and $P \in \mathcal{P}_m$. Let

$$x_j := j + 1, \quad j = 0, 1, \dots, m,$$

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

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

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

and hence

$$\begin{aligned} \max_{0 \neq P \in \mathcal{P}_m} \frac{|P(0)|}{\max_{x \in E_m} |P(x)|} &= \sum_{k=0}^m |L_k(0)| = \sum_{k=0}^m (-1)^k L_k(0) \\ &\leq (m+1) \sum_{k=0}^m \binom{m}{k} \leq n 2^n \leq 328L \exp(328L). \end{aligned}$$

This finishes the proof of the inequality of the lemma in the case when together with $L < 16n$ we also have $n < 328L$.

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,

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

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

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

where, for $1 \leq k \leq L/5$ we have

$$\begin{aligned} 0 < x_k &= \frac{n}{2} \left(1 + \cos \frac{2k-1}{2m} \pi\right) = n \sin^2 \frac{2k-1}{4m} \pi \\ &\leq \frac{nk^2\pi^2}{4m^2} \leq \frac{nk^2\pi^2}{4nL} \leq \frac{5k^2}{2L} \leq \frac{k}{2}. \end{aligned}$$

Now let L' be the largest integer not greater than L and we define the polynomial P_m of degree m be defined by

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

Then, we have

$$\begin{aligned} |P_m(j)| &\leq |Q_m(j)| \leq 1, \quad j \in [L' + 1, n], \\ |P_m(j)| &= 0 < 1, \quad j \in [1, L'], \end{aligned}$$

hence

$$|P_m(j)| \leq 1, \quad j \in [1, n].$$

This, together with

$$\begin{aligned} |P_m(0)| &\geq |Q_m(0)| \prod_{k=1}^{L'} \left| \frac{k}{x_k} \right| \geq \prod_{k=1}^{L'} \frac{k}{k/2} \geq 2^{L'} \geq 2^{L/5-1} \\ &\geq 2^{L/10}, \end{aligned}$$

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 $p : \{-1, 1\}^n \rightarrow \mathbb{R}$

over \mathbb{R} , equipped with the scalar product defined in Section 2. Let Y_n be the vector space of all polynomials $D_n \rightarrow \mathbb{R}$ of a single variable over \mathbb{R} , equipped with the scalar product defined in Section 2.

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

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

and

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

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

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

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

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

and

$$(5.10) \quad \langle g, f \rangle = \langle G, F \rangle \geq \alpha > 0, \quad f \in V_m,$$

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

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

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

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

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

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

Since the pure high degree of $g \in X_n$ is at least $m + 1$, $\tilde{G} \in \mathcal{P}_n$ 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 $|\tilde{G}(j)| = |G(j)|$ for each $j = 0, 1, \dots, n$, we have

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

□

Proof of Lemma 4.7. Suppose

$$\max_{x \in F_n} |P(x)| = 1.$$

Pick $y \in [0, n]$ so that

$$|P(y)| = M := \max_{x \in [0, n]} |P(x)|.$$

Without loss of generality we may assume that $P(y) > 0$. Let $k \in [0, n]$ be the integer closest to y . Combining Markov's polynomial inequality (see p. 233 of [BE-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

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

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 with the properties of Lemma 4.1 we obtain

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

and this contradicts the assumption of the theorem. \square

Proof of Theorem 3.2. Without loss of generality we may assume that $e^{2c} \leq M < e^{32cn}$, where the absolute constant $c > 0$ is the same as in Lemma 4.5. Let $c_1 > 0$ be the absolute constant be the same as in Lemma 4.6. Suppose that a polynomial P of the form

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

has a zero at 1 with multiplicity at least $n - \lfloor c_1 \sqrt{n \log M} \rfloor + 1$ zeros at 1. Then

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

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

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

we can deduce that

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

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

Proof of Theorem 3.4. The proof of the theorem is very similar to that of Theorem 3.2. However, at one point an application of Lemma 4.8 rather than Lemma 4.6 is needed. \square

7. Acknowledgment. The author wishes to thank Mario Szegedy and Ronald de Wolf 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.
- BC-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.
- BE-95. P. Borwein and T. Erdélyi, *Polynomials and Polynomial Inequalities*, Springer, New York, 1995.
- BE-97a. P. Borwein and T. Erdélyi, *On the zeros of polynomials with restricted coefficients*, Illinois J. Math. **41** (1997), 667–675.
- BE-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.
- BEK-99. P. Borwein, T. Erdélyi, and G. Kós, *Littlewood-type problems on $[0, 1]$* , Proc. London Math. Soc. **79** (3) (1999), 22–46.
- BV-87. E. Bombieri and J. Vaaler, *Polynomials with low height and prescribed vanishing*, in Analytic Number Theory and Diophantine Problems, Birkhauser (1987), 53–73.
- B-97. D. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comput. **66** (1997), 1697–1703.
- CR-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.
- 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.
- 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.
- MP-68. M. Minsky and S. Papert, *Perceptrons: An Introduction to Computational Geometry*, MIT Press, Cambridge Mass., 1968.
- NS-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.
- 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.
- SZ-54. R. Salem and A. Zygmund, *Some properties of trigonometric series whose terms have random signs*, Acta Math. **91** (1954), 245–301.
- Š-03. R. Špalek, *A dual polynomial for OR*, Technical Report arXiv:0803.4516 [cs.CC], arXiv, 2008.

DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION, TEXAS 77843
E-mail address: `terdelyi@math.tamu.edu`