

# On the Degree of Polynomials that Approximate Symmetric Boolean Functions

(Preliminary Version)

Ramamohan Paturi

Department of Computer Science and Engineering  
University of California, San Diego  
La Jolla, CA 92093

## Abstract

In this paper, we provide matching (up to a constant factor) upper and lower bounds on the degree of polynomials that represent symmetric boolean functions within an error  $1/3$ . Let  $\Gamma(f) = \min\{|2k - n + 1| : f_k \neq f_{k+1} \text{ and } 0 \leq k \leq n - 1\}$  where  $f_i$  is the value of  $f$  on inputs with exactly  $i$  1's. We prove that the minimum degree over all the approximating polynomials of  $f$  is  $\Theta(\sqrt{n(n - \Gamma(f))})$ . We apply the techniques and tools from approximation theory to derive this result.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

24th ANNUAL ACM STOC - 5/92/VICTORIA, B.C., CANADA  
© 1992 ACM 0-89791-512-7/92/0004/0468...\$1.50

## 1 INTRODUCTION

Let  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  be a boolean function. In this paper, we consider representations of  $f$  by multi-variate real polynomials. We say that a multivariate real polynomial  $p(x_1, \dots, x_n)$  represents a boolean function  $f$  if  $f(x_1, \dots, x_n) = p(x_1, \dots, x_n)$  for all  $(x_1, \dots, x_n) \in \{0, 1\}^n$ . Since  $x_i^2 = x_i$  for  $x_i \in \{0, 1\}$ , we restrict ourselves to multi-linear polynomials. It turns out that there exists a unique multi-linear polynomial that represents a given boolean function. The *degree*  $d(f)$  of a boolean function is defined to be the degree of the unique multilinear polynomial that represents  $f$ . The degree of a multi-linear polynomial is the number of variables appearing in the largest monomial with a non-zero coefficient.

In this paper, we are interested in a *weaker* notion of representation of boolean functions. Following Nisan and Szegedy [3], we say that a real polynomial *approximates*  $f$ , if, for every  $\vec{x} \in \{0, 1\}^n$ ,  $|p(\vec{x}) - f(\vec{x})| \leq 1/3$ . As before, we restrict ourselves to multi-linear polynomials. Also the constant  $1/3$  is arbitrary and can be replaced by any constant  $c < 1/2$  without affecting the results. The *approximate degree*  $\tilde{d}(f)$  of  $f$  is defined to be the minimum, over all polynomials  $p$  that approximate  $f$ , of the degree

of  $p$ .

In [3], Nisan and Szegedy relate the approximate degree of a boolean function to its decision tree complexity. They show that  $\tilde{d}(f) \leq d(f) \leq D(f) \leq 1296\tilde{d}(f)^8$  where  $D(f)$  is the decision-tree complexity of  $f$ . In order to establish these relationships, they show that the approximate degree of the OR function is  $\Omega(\sqrt{n})$ . In this paper, we consider the problem of determination of approximate degree of symmetric boolean functions and provide a *complete* (up to a constant factor) solution.

A boolean function  $f$  is called *symmetric* if  $f(x_1, \dots, x_n) = f_i \in \{0, 1\}$  for all  $(x_1, \dots, x_n) \in \{0, 1\}^n$  such that  $\sum_{j=1}^n x_j = i$ . In other words, the value of a symmetric boolean function only depends on the number of 1's in the input. It is not too difficult to see that the degree of any non-constant symmetric function is  $\geq n/2$ . On the other hand, we show in this paper that the approximate degree of a symmetric boolean function is determined by the location of the 'jump' as measured by the quantity  $\Gamma(f)$  given by

$$\Gamma(f) = \min\{2k - n + 1 \mid f_k \neq f_{k+1} \text{ and } 0 \leq k \leq n - 1\}$$

For instance, if  $f$  is the majority or the parity function, then  $\Gamma(f)$  is 1 or 0 (depending on the parity of  $n$ ). On the other hand, we have  $\Gamma(f) = n - 1$  for the AND and the OR functions. Smaller values of  $\Gamma(f)$  indicate that the jump occurs near the origin thereby requiring higher degree to approximate  $f$ . More specifically, we prove the following theorem in this paper.

**Theorem 1** *Let  $f$  be any non-constant symmetric function. The approximate degree of  $f$  is  $\Theta(\sqrt{n(n - \Gamma(f))})$ .*

If  $f$  is the AND or the OR function, this theorem implies that the approximate degree is  $\Theta(\sqrt{n})$  as shown in Nisan and Szegedy [3]. If  $f$  is the majority or parity function, then the approximate degree is  $\Theta(n)$ .

In the following, we give an account of the techniques used in deriving this result. As in the case of Nisan and Szegedy, an important aid in the proof is the symmetrization technique [2, 3]: Given a multivariate polynomial of degree  $d$  that approximates  $f$ , this technique obtains a single-variable polynomial  $p(x)$  of degree at most  $d$  such that  $|p(i) - f_i| \leq 1/3$  for  $0 \leq i \leq n$ . Conversely, if  $p(x)$  is such a single-variable polynomial of degree  $d$ , then the multivariate polynomial  $p(x_1 + \dots + x_n)$  of degree  $d$  approximates  $f$  within error  $1/3$ .

In addition, our result uses tools from approximation theory. A crucial observation from classical approximation theory is that real functions (over a finite interval) which are not smooth in the middle of an interval are hard to approximate by means of polynomials. In the classical case, the best approximating polynomial is found by expanding the function in a *Fourier* fashion and truncating to give the desired degree. The error in the approximation is bounded by the point-wise continuity properties of the function. Our upper bounds on the approximate degree of symmetric boolean functions are the result of a straightforward application of these so called *direct* or *Jackson* theorems from classical approximation theory.

However, our lower bounds require a non-trivial extension of the classical results to the discrete case. To derive lower bounds on the degree of the best approximating polynomial in the classical case of real functions over a finite interval, one could use Bernstein-Markov type point-wise inequalities that bound the magnitude of the derivative of a polynomial in terms of its degree and its supremum in the interval. Although we can easily establish that the best approximating polynomial of the boolean function  $f$  has to have a high derivative at a point as determined by  $\Gamma(f)$ , Bernstein-Markov inequalities are not readily applicable since in our discrete case the value of the polynomial is only bounded at the integer points and it can assume large values at other points in the interval. We overcome this problem by multiplying the polynomial with another suitably chosen polynomial so

that the product polynomial still has a high derivative and its value is small at all points in the interval except in a small neighbourhood of the point where the high derivative occurs. We can now apply Bernstein–Markov inequalities to obtain the desired lower bound on the degree.

## 2 UPPER BOUNDS

In this section we present our upper bound result for the symmetric boolean functions  $f$ . The idea is to consider a piece-wise linear function  $g$  on the interval  $[0, n]$  which coincides with the value  $f_i$  at the integer point  $i$ . We then use the upper bound results from approximation theory to find the best polynomial approximation  $p$  for  $g$ . Then the multi-variate polynomial  $p(x_1 + \dots + x_n)$  will be the desired approximation. We will first need some terminology in order to state the upper bound theorem from approximation theory.

Let  $C[-1, 1]$  denote the space of all continuous functions  $f$  over the interval  $[-1, 1]$ . We endow this space with the *uniform* or *Chebyshev* norm

$$\|f\|_{C[-1,1]} = \|f\| = \sup\{|f(x)| : x \in [-1, 1]\}.$$

For integers  $d \geq 0$ , let  $P_d$  denote the  $d + 1$ -dimensional subspace (over reals) of  $C[-1, 1]$  generated by  $1, x, \dots, x^d$ . The elements of  $P_d$  are called algebraic polynomials of degree  $d$ .

We are interested in approximating arbitrary continuous functions from  $C[-1, 1]$  with algebraic polynomials in  $P_d$  in the uniform norm. Let

$$E_d(f)_{C[-1,1]} = E_d(f) = \inf\{\|f - p\| : p \in P_d\}$$

denote the best uniform approximation of the function  $f \in C[-1, 1]$  by means of algebraic polynomials of degree  $d$ .

The classical approximation theory tells us that such a best uniform approximation exists and is unique [4, 5]. We are now interested in the so called

*direct* or *Jackson* theorems that relate the quantity  $E_d(f)$  to the continuity and the differentiability properties of  $f$ . In particular, we want to characterize  $E_d(f)$  based on the following modulus of continuity.

Let  $\Delta_m(x) = \frac{x}{m}\sqrt{1-x^2} + \frac{1}{m^2}$ . We define  $\tau(f; \Delta_m) = \sup\{|f(x) - f(y)| : x, y \in [-1, 1], |x - y| \leq \Delta_m(x)\}$ .

We will use the following result from approximation theory. This result can be found in [1, 4] and we will include the proof in the full paper.

**Theorem 2** *Let  $f \in C[-1, 1]$ . Then*

$$E_d(f) = O(\tau(f; \Delta_d)).$$

We are now ready to prove our upper bounds.

**Theorem 3** *Let  $f$  be a non-constant symmetric boolean function on  $x_1, \dots, x_n$ . Then the approximate degree of  $f$  is  $O(\sqrt{n(n - \Gamma(f))})$ .*

**Proof:** In this proof, we assume that  $n$  is even. Since every symmetric boolean function can be obtained as a projection of a suitable symmetric boolean function on  $n + 1$  variables, our assumption is without loss of generality. We define the piece-wise linear continuous function  $g \in C[-1, 1]$  by  $g(2i/n - 1) = f_i$  for  $0 \leq i \leq n$ , and by requiring  $g$  to be linear in each interval  $[(2i/n) - 1, (2(i+1)/n) - 1]$  for  $0 \leq i \leq n - 1$ . Let  $p(x)$  be a polynomial of minimal degree which approximates  $g$  with error less than  $1/3$ . We then have that the multilinear polynomial  $q(x_1, \dots, x_n) = p(\sum_{j=1}^n 2x_j/n - 1) \bmod (x_i^2 = x_i)$  of the same degree as  $p(x)$  and approximates  $f$  within error  $1/3$ .

Let  $d$  be the degree of  $p(x)$ . To determine  $d$ , we observe that the  $g'(x) = 0$  for  $x \in ((-\Gamma(f) + 1)/n, (\Gamma(f) - 1)/n)$  and  $|g'(x)| \leq n/2$  for any other  $x \in [-1, 1]$  where  $g'(x)$  is defined. For  $\Gamma(f) \leq 1 + n/\sqrt{1 + 1/d^2}$ , the modulus of continuity  $\tau(g; \Delta_d)$  is bounded by

$$\begin{aligned} \tau(g; \Delta_d) &\leq n\Delta_d((\Gamma(f) - 1)/n)/2 \\ &\leq \frac{n}{2d}(\sqrt{1 - (\Gamma(f) - 1)^2/n^2} + \frac{1}{d}). \end{aligned}$$

Note that the condition  $\Gamma(f) \leq 1 + n/\sqrt{1 + 1/d^2}$  is satisfied for  $n \geq 2$  and  $d \geq \sqrt{n}$ . Hence, from theorem 2, it follows that if  $d \geq c\sqrt{n(n - \Gamma(f))}$  (for a suitably chosen constant  $c > 0$ ), the error in the approximation will be less than  $1/3$ . ♣

### 3 LOWER BOUNDS

Let  $f$  be a non-constant symmetric boolean function on  $x_1, \dots, x_n$ . Let  $f_i$  and  $\Gamma(f)$  be as defined before. Let  $q(x_1, \dots, x_n)$  be a multilinear polynomial of degree  $d$  that approximates  $f$  within error  $1/3$ . We apply the symmetrization technique to  $q$  to obtain a single-variable polynomial  $p_1(x)$  of degree  $d$  such that  $|p_1(i) - f_i| \leq 1/3$  for  $i = 0, \dots, n$ . We now obtain the polynomial  $p(x)$  of degree  $d$  over the interval  $[-1, 1]$  by setting  $p(x) = p_1(nx/2 + n/2)$ . Note that  $-1/3 \leq p(2i/n - 1) \leq 1 + 1/3$  for  $i = 0, \dots, n$ . Our plan is to prove a lower bound on the degree of  $p$  which in turn gives a lower bound on the degree of the multilinear polynomial  $q(x_1, \dots, x_n)$ . We obtain the lower bound on  $p$  by showing that it has to have a high derivative not too far from the origin as determined by the quantity  $\Gamma(f)$ . Notice that  $|p'(x)| \geq n/6$  for some  $x \in [-(\Gamma(f) + 1)/n, -(\Gamma(f) - 1)/n] \cup [(\Gamma(f) - 1)/n, (\Gamma(f) + 1)/n]$ . We then would like to use classical inequalities of Bernstein and Markov that upper bound the derivative of a polynomial point-wise to obtain our lower bound on the degree of  $p$ . However, a successful application of these inequalities requires that the norm of  $p$  in the interval  $[-1, 1]$  be small. But, our construction only guarantees that  $|p(2i/n - 1)| \leq 4/3$  for  $i = 0, \dots, n$  and it is in general possible for  $p$  to have a norm of  $2^d/d^2$  in the interval  $[-1, 1]$  where  $d$  is the degree of  $p$ . We avoid this problem by multiplying the polynomial with a suitable trigonometric polynomial to control the norm of the polynomial and at the same time maintaining the high derivative as does the original polynomial. We then apply Bernstein–Markov inequalities to obtain the desired lower bound.

Before we give the proof of the lower bound theorem, we state two sets of inequalities from approximation theory: the first set deals with the growth of a polynomial given its values on a subset of the interval, and the second set deals with the bounds on the derivatives of algebraic and trigonometric polynomials. Proofs of these classical theorems can be found in [5, 4].

#### 3.1 Bounds on the Chebyshev Norm

The first inequality bounds the magnitude of the polynomial in a closed interval  $[l, m]$  with integer end points in terms of the values of the polynomial at the integer points in  $[l, m]$ . Let  $p(x)$  be a polynomial of degree at most  $d \leq n$ . Assume that  $|p(k)| \leq c$  for integers  $k = l, \dots, l + d$ . Then, we have

**Fact 1**  $|p(x)| \leq c2^d$  for  $x$  in the interval  $[l, l + d]$ .

As a corollary, we have

**Corollary 1** Let  $p(x)$  be a polynomial of degree at most  $d \leq n$  and  $|p(i)| \leq c$  for integers  $i = 0, \dots, n$ , then  $|p(x)| \leq c2^d$  for all  $x$  in the closed interval  $[0, n]$ .

The next inequality bounds the magnitude of a polynomial outside an interval in terms of its norm in the interval. In fact, the inequality shows that Chebyshev polynomials are extremal in this respect.

For  $k \geq 0$ , The  $k$ -th Chebyshev polynomial  $T_k(x)$  is a degree  $k$  algebraic polynomial given by

$$T_k(x) = \frac{1}{2}[(x + \sqrt{x^2 - 1})^k + (x - \sqrt{x^2 - 1})^k].$$

Observe that  $T_k(x)$  is an even polynomial for even  $k$  and an odd polynomial for odd  $k$ . Also, we have  $T_k(1 + \mu) \leq e^{(2\sqrt{2\mu + \mu^2})^k}$  for  $\mu \geq 0$ .

**Fact 2** Let  $p(x)$  be a polynomial of degree at most  $d$ . Assume that  $|p(x)| \leq c$  in the interval  $[-1, 1]$ . We then have  $|p(x)| \leq c|T_d(x)|$  for all  $|x| > 1$ .

By scaling, we have the following corollary.

**Corollary 2** *Let  $p(x)$  be a polynomial of degree at most  $d$ . Assume that  $|p(x)| \leq c$  in the interval  $[-a, a]$  for  $0 < a \leq 1$ . We then have  $|p(x)| \leq c|T_d(1 + \frac{|x|-a}{a})|$  for all  $|x| > a$ .*

### 3.2 Bounds on the Derivative

In the following, we give the inequalities of Bernstein and Markov that bound the magnitude of the derivative of an algebraic or a trigonometric polynomial *point-wise* in terms of its degree. In fact, such point-wise inequalities are essential to obtain the tight lower bounds.

We will first define the class  $Q_d$  of trigonometric polynomials of degree  $d$  as the  $(2d + 1)$ -dimensional space spanned by the functions  $1, \cos x, \sin x, \dots, \cos dx, \sin dx$ . The norm of a trigonometric polynomial  $t(x) \in Q_d$  over the interval  $[-\pi, \pi]$  is defined as

$$\|t\| = \sup\{|t(x)| : x \in [-\pi, \pi]\}.$$

Note that if  $p(x)$  is an algebraic polynomial of degree  $d$ , then  $p(\cos \theta)$  is an even trigonometric polynomial of degree  $d$ .

**Fact 3 [Bernstein]** *Let  $t(x)$  be a trigonometric polynomial of degree  $d$ . We then have, for  $x \in [-\pi, \pi]$ ,*

$$\|t'(x)\| \leq d\|t\|$$

**Fact 4 [Bernstein–Markov]** *Let  $p(x)$  be an algebraic polynomial of degree  $d$ . We then have, for  $x \in [-1, 1]$ ,*

$$\left| \left( \frac{1}{d} \sqrt{1-x^2} + \frac{1}{d^2} \right) p'(x) \right| \leq 2\|p\|.$$

### 3.3 Lower Bound Theorem

We are now ready to prove the lower bound theorem.

**Theorem 4** *Let  $f$  be a non-constant symmetric boolean function on  $x_1, \dots, x_n$ . Then any multilinear polynomial that approximates  $f$  within error  $1/3$  has degree  $\Omega(\sqrt{n(n - \Gamma(f))})$ .*

**Proof:** Let  $p'(x_1, \dots, x_n)$  be a multilinear polynomial that approximates  $f$  within error  $1/3$ . Using the symmetrization technique, we obtain a single variable polynomial  $p(x)$  such that  $|p(2i/n - 1) - f_i| \leq 1/3$  for  $i = 0, \dots, n$ . Without loss of generality, we assume that  $n$  is even and  $f_{n/2} = 0$  which implies  $|p(0)| \leq 1/3$ . Let  $z = z_p = \inf\{|x| : x \in [-1, 1] \text{ and } p(x) \geq 2/3\}$ . Without loss of generality, assume that the infimum is obtained for positive  $x$ . Let  $k = k_p$  be such that  $2k/n < z_p \leq 2(k+1)/n$ . We note that the following conditions are satisfied by  $p$

1. We have  $2k \leq \Gamma(f) - 1$  from the definition of  $\Gamma(f)$ .
2.  $p(2k/n) \leq 1/3$  and  $p(z) \geq 2/3$ .
3. By mean value theorem, it follows that  $|p'(x)| \geq n/6$  for some  $x \in [2k/n, z]$ .

Let  $c_1$  be a constant equal to, say,  $1/100$ . We will consider two cases;

**Case 1;  $z \leq 1 - c_1$ :** By the corollary to fact 1, we have  $|p(x)| \leq 2^{d+1}$  for  $x \in [-1, 1]$ . By applying the fact 2, we have

$$|p(1 + \mu)| \leq 2^{d+1} e^{(2\sqrt{2\mu+\mu^2})d} \quad (1)$$

for  $\mu > 0$ . We consider the polynomial  $q(x) = p(x + z)$ . Since  $2(k+1)/n$  is at most 1, for  $x \in [-1, 1]$ , we have

$$|q(x)| = |p(x + z)| \leq 2^{d+1} e^{2\sqrt{3}d}$$

from the inequality 1. We consider  $\hat{q}(x) = q(x)(1 - x^2)^m$  where  $m = 6\lceil d/c_1^2 \rceil$ . The idea is that  $\hat{q}(x)$  will

have smaller values for  $x$  bounded away from the origin. Indeed, for  $x \in [-1, -c_1] \cup [c_1, 1]$ , we have  $|\hat{q}(x)| = |q(x)|(1-x^2)^m \leq |q(x)|e^{-c_1^2 m} \leq 1$ .

We also show that  $\hat{q}$  has a high derivative near the origin. In fact,  $|\hat{q}(0)| = |q(0)| = |p(z)| \geq 2/3$  and  $|\hat{q}(2k/n-z)| < |q(2k/n-z)| = |p(2k/n)| \leq 1/3$ . From the definition of  $k$ , we have  $|2k/n-z| \leq 2/n$ . Hence, we have  $\hat{q}'(x) \geq n/6$  for some  $x \in [-2/n, 0]$ . We still have to be concerned with the possibility that the value  $|\hat{q}(x)|$  is high for some  $x \in [-c_1, c_1]$ . Note that we have

$$|\hat{q}(2i/n-z)| < |q(2i/n-z)| = |p(2i/n)| \leq 4/3$$

for integers  $i$  such that  $(2i/n-z) \in [-c_1, c_1]$ . Therefore, even if  $\hat{q}$  assumes high values at other points in the interval  $[-c_1, c_1]$ , we can conclude that, for some  $x \in [-c_1, c_1]$ ,  $\hat{q}'(x) \geq n\|\hat{q}\|/8$ . Hence, by applying Bernstein–Markov inequality for  $\hat{q}$ , we obtain that the degree of  $\hat{q}$  is  $\Omega(n) = \Omega(\sqrt{n(n-\Gamma(f))})$  since  $\Gamma(f) < cn$  for some  $c < 1$ .

**Case 2;  $z > 1 - c_1$ :** We assume  $z \neq 1$ . Otherwise, we can readily apply Bernstein–Markov inequality to reach the desired conclusion. We use the following transformation to obtain a trigonometric polynomial  $q(\theta)$  of degree  $d$ . Let  $\theta_z = \cos^{-1} z$ . Since  $1 - c_1 < z < 1$ ,  $0 < \theta_z < 0.2$ . We define  $q(\theta)$  as the trigonometric polynomial  $p(\cos \theta)$ . Notice that  $q(\theta)$  is an even trigonometric polynomial of degree  $d$ .

Moreover, for  $\theta \in [-\pi + \theta_z, -\theta_z] \cup [\theta_z, \pi - \theta_z]$ ,  $|q(\theta)| \leq 2/3$  since  $|p(x)| \leq 2/3$  for  $x \in [-z, z]$ . From corollary to fact 2, we have

$$|p(z+\mu)| \leq \frac{2}{3} T_d(1+\mu/z) \leq e^{2d\sqrt{2\mu/z+\mu^2/z^2}}$$

for  $\mu \geq 0$ . From this we get that, for  $\theta \in [0, 2\theta_z]$ ,

$$\begin{aligned} |q(\theta_z - \theta)| &= |p(\cos(\theta_z - \theta))| \\ &\leq e^{2d\sqrt{2\theta\sqrt{1-z^2}/z+\theta^2(1-z^2)/z^2}} \\ &\leq e^{4d\sqrt{\theta\theta_z}}. \end{aligned} \quad (2)$$

The last inequality follows from  $\cos(\theta_z - \varepsilon) \leq z + \varepsilon\sqrt{1-z^2}$ ,  $\theta_z^2 \geq 2(1-z) \geq (1-z^2)$ ,  $z > 1 - c_1$  and  $0 < \theta_z < 0.2$ .

We define  $\hat{q}(\theta) = q(\theta)h(\theta)$  where  $h(\theta) = [\cos(m_1(\theta - \theta_z))]^{m_2}$ ,  $m_1 = \lfloor 1/2\theta_z \rfloor$  and  $m_2 = c\lceil d/m_1 \rceil$  where  $c$  is a sufficiently large integer constant. Notice that  $\hat{q}$  is a trigonometric polynomial of degree at most  $(c+1)(d+1)$ . Furthermore, we have, for all  $\theta \in [0, 2\theta_z]$ ,

$$\begin{aligned} |h(\theta_z - \theta)| &= |(\cos m_1 \theta)^{m_2}| \\ &\leq e^{-m_2 m_1^2 \theta^2/4} \\ &\leq e^{-cd\theta^2 \lfloor 1/2\theta_z \rfloor/4} \\ &\leq e^{-c'd\theta^2/\theta_z} \end{aligned} \quad (3)$$

where  $c' = c/16$ . Hence, for  $\theta \in [-\theta_z, \theta_z/2]$ ,

$$|\hat{q}(\theta)| = |q(\theta_z - (\theta_z - \theta))||h(\theta_z - (\theta_z - \theta))| \leq 1$$

from equations 2 and 3.

Similarly, from equations 2 and 3, it follows that for  $\theta \in [\pi - \theta_z, \pi]$ ,  $\hat{q}(\theta) \leq 1$ .

Furthermore, we show that  $\hat{q}$  has a high derivative at some point in the interval  $[\theta_z/2, \theta_z]$ . Note that  $\hat{q}(\theta_z) = p(\cos \theta_z) = p(z) \geq 2/3$ . In addition, we show that  $\hat{q}$  is small somewhere in the vicinity of  $\theta_z$ . Let  $\theta_i = \cos^{-1}(2i/n)$ . Note that  $k$  is such that  $2k/n < z \leq 2(k+1)/n$ . We know that  $|\hat{q}(\theta_k)| \leq |q(\theta_k)| \leq |p(2k/n)| \leq 1/3$ . On the other hand, we have  $|\theta_z - \theta_k| \leq 6/n\theta_z$ . (Note that  $(\theta_1 + \theta_2)(\theta_2 - \theta_1)/3 \leq |\cos \theta_1 - \cos \theta_2|$  for  $0 \leq \theta_1 \leq \theta_2 < 1$ ).

Hence, for some  $\theta \in [\theta_z, \theta_k]$ ,  $\hat{q}'(\theta) \geq n\theta_z/18$ . In fact, we have that for some  $\theta \in [\theta_z/2, \theta_k]$ ,  $\hat{q}'(\theta) \geq n\theta_z\|\hat{q}\|/18$ . By applying Bernstein's inequality to the trigonometric polynomial  $\hat{q}$ , we get  $d \geq c'n\theta_z \geq c''n \sin \theta_z \geq c''n\sqrt{1-z^2} \geq c''\sqrt{n(n-\Gamma(f))}$  for some constant  $c'' > 0$ . Hence, the theorem is proved. ♣

**Acknowledgments:** I would like to thank Michael E. Saks, Mario Szegedy and Russell Impagliazzo for their useful suggestions.

## References

- [1] Ivanov, K. (1983). On a new characteristic of functions. II Direct and Converse theorems for

best algebraic approximation in  $C[-1, 1]$  and  $L_p[-1, 1]$ , *Pliska*, **5**, 151-63.

- [2] Minsky, M. and Papert, S.A. (1969), "Perceptrons", MIT Press, Cambridge, Massachusetts.
- [3] Nisan, N. and Szegedy, M. (1991). On the Degree of Boolean Functions as Real Polynomials, *in preparation*.
- [4] Petrushev, P.P. and Popov, V.A. (1987). *Rational Approximation of Real Functions*, Cambridge University Press.
- [5] Rivlin, T.J. (1990). *Chebyshev Polynomials*, John Wiley and Sons Co., 2nd Edition.
- [6] Razborov, A.A. (1986), Lower Bounds on the Size of Bounded Depth Networks over a Complete Basis with Logical Addition, *Mathematische Zametki* **37** pp. 887-00 (in Russian). English Translation in *Mathematical Notes of the Academy of Sciences of the USSR* **37**, pp. 485-509.
- [7] Smolensky, R. (1987), Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity in "Proceedings of 19th Annual ACM symposium on Theory of Computing", pp. 77-82.
- [8] Szegedy, M. (1989), "Algebraic Method in Lower Bounds for Computational Models with Limited Communication", Ph.D. Dissertation, University of Chicago.