On the degree of symmetric functions on the Boolean cube

Gil Cohen

On the degree of symmetric functions on the Boolean cube

Research Thesis

Submitted in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Computer Science

Gil Cohen

Submitted to the Senate of the
Technion - Israel Institute of Technology

Tammuz 5770 Haifa July 2010

The research thesis was done under the supervision of Assoc. Prof. Amir Shpilka in the Department of Computer Science.

I would like to thank Amir for his continuous support, devoted guidance and for giving me an excellent introduction to research.

I would like to thank my wife Orit and my son Yahli for their continuous support and interest in my work. This thesis is devoted to them.

The generous financial help of the Technion is gratefully acknowledged.

Contents

Abstract

Given a function $f\colon \{0,1,\ldots,n\} \to \mathcal{C}$ for some $\mathcal{C} \subset \mathbb{R}$, it is a well known fact that there exists a unique interpolation polynomial h for f of degree at most n. A natural question is the following: for a restricted $\mathcal{C}$, how low can the degree of an interpolation polynomial for a non-constant function of the form $f\colon \{0,1,\ldots,n\} \to \mathcal{C}$ be? A first result for a question of that nature appeared in [vzGR97] and handled the case $\mathcal{C} = \{0,1\}$. In this thesis we study two natural generalizations offered in [vzGR97]. The first concerns the restriction $\mathcal{C} = \{0,1,\ldots,c\}$ for some $c \in \mathbb{N}$. The second generalization deals with the case $\mathcal{C} \subset \mathbb{Q}$. In both cases we give new lower bounds. We also simplify and generalize the main result in [vzGR97].

Abbreviations and Notations

$a \equiv_p b$	$a \equiv b \mod p$.
$\mathbb{N}$	the set of natural numbers.
$\mathbb{Q}$	the set of rational numbers.
$\mathbb{R}$	the set of real numbers.
$\langle a_m \quad \cdots \quad a_0 \rangle_p$	the representation of an integer a in base p.

Chapter 1

Introduction

1.1 Overview

Given a function $f\colon \{0,1,\ldots,n\} \to \mathcal{C}$ for some $\mathcal{C} \subset \mathbb{R}$, it is a well known fact that there exists a unique interpolation polynomial h for f (that is $h(x) = f(x)$ for all $x \in \{0,1,\ldots,n\}$) of degree at most n. Indeed, this polynomial can be derived from Lagrange's formula

$$h(x) = \sum_{k=0}^{n} f(k) \cdot \prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{x-j}{k-j} \quad .$$

Due to this fact we can associate the degree of the unique interpolation polynomial with the function. That is, we say that the degree of the function, denoted by $\deg f$, is the degree of the above mentioned polynomial.

The type of questions we are considering is the following: for a restricted $\mathcal{C}$, is there a low degree non-constant function of the form $f\colon \{0,1,\ldots,n\} \to \mathcal{C}$? Obviously, without restricting $\mathcal{C}$ the answer will be yes. A first result for a question of that nature appeared in [vzGR97]. The authors proved that for any non-constant function of the form $f\colon \{0,1,\ldots,n\} \to \{0,1\}$ it holds that $\deg f > n - O(n^{0.525})$. It is easy to see that this result, in fact, yields a lower bound on the degree of every function of the form $f\colon \{0,1,\ldots,n\} \to \mathcal{C}$ for every set $\mathcal{C}$ of size 2. Indeed, the degree of polynomials is invariant under stretching and shifting (that is, $\deg h(x) = \deg(a \cdot h(x) + b)$ for $a \neq 0, b \in \mathbb{R}$). Therefore this result tells us that in the interesting Boolean case, no function of low degree exist.

In this work we study two natural generalizations offered in [vzGR97]

1. The case where $\mathcal{C} = \{0, 1, \ldots, c\}$ for some $c \in \mathbb{N}$.

2. The case where $\mathcal{C} \subset \mathbb{Q}$. That is, we no longer assume that the range is in $\mathbb{N}$. In this case we fix $\mathcal{C}$ and let $n \to \infty$. To put it in other words, we look at families of functions (this is how we usually, implicitly, think of functions in computer science).

On top of that, we further study the case where $\mathcal{C} = \{0, 1\}$. We simplify the proof of [vzGR97] and generalize it.

1.1.1 Applications to Theoretical Computer Science

The motivation of the authors of [vzGR97] for studying lower bounds on the degree of non-constant functions of the form $f\colon \{0, 1, \ldots, n\} \to \{0, 1\}$ originated from theoretical computer science. A Boolean function on the Boolean cube is a function of the form $f\colon \{0, 1\}^n \to \{0, 1\}$. A natural representation of functions on the Boolean cube is as polynomials over various fields, in particular over the real numbers where this representation is also known as the Fourier representation of the function. Understanding such representations has been a major research goal in theoretical computer science for decades (see e.g. [BdW02, Ste03, Gop06]). Specifically, the question of better understanding the degree of the representing real polynomial received a lot of attention [NS94, vzGR97]. Nisan and Szegedy proved that the degree of the representing polynomial of any Boolean function, that depends on all n inputs, is at least[1] $\log(n) - O(\log \log n)$ (this bound is essentially tight as the so called "address function" demonstrates) [NS94]. This result immediately raised the question of whether we can get stronger lower bounds on the degree when the underlying function has additional properties.

A class of functions that was widely studied is the class of symmetric Boolean functions. A symmetric function on the Boolean cube is a function that only depends on the weight of its input (i.e. its number of non-zero entries). Symmetric Boolean functions play an important role in many areas of theoretical computer science. For example, they received a lot of attention in learning theory (see e.g. [KOS04] and references within), circuit complexity

[1] All logarithms in this paper are base 2.

[HMP+93], cryptography [NR04], quantum computation [Raz03], voting theory and more. It is a well known fact that every such function $f(x_1, \ldots, x_n)$ can be represented as a univariate polynomial in $x = x_1 + \ldots + x_n$, keeping the degree intact. In other words, symmetric Boolean functions are in one to one correspondence with functions of the form $F : \{0, 1, \ldots, n\} \to \{0, 1\}$. Thus, for symmetric functions the question boils down to proving a lower bound on the degree of non-constant polynomials on $\{0, 1, \ldots, n\}$ that take two different values. Here enters [vzGR97].

Our work sheds light into the case of symmetric functions on the Boolean cube, having range that is not necessarily Boolean.

1.2 Previous Results

A lower bound for the degree of non-constant functions of the form $f\colon \{0, 1, \ldots, n\} \to \mathcal{C}$ appeared in [vzGR97]. The authors observed that

$$\deg f \geq \frac{n+1}{|\mathcal{C}|} .$$

This lower bound follows from an averaging principle: such function must assume one of its $|\mathcal{C}|$ values on at least $(n+1)/|\mathcal{C}|$ points, while a polynomial of degree d cannot obtain the same value on more than d points. Especially, for $\mathcal{C} = \{0, 1, \ldots, c\}$ we have that

$$\deg f \geq \frac{n+1}{c+1} .$$

We also note that in this case the question is only interesting for $c < n$, since already for $c = n$ the function $f(k) = k$ for $k = 0, 1, \ldots, n$ has degree 1.

1.3 Original Results in the Thesis

We prove three results in this Thesis. The first result gives a much stronger lower bound, than what was previously known, on the degree of non-constant functions of the form $f\colon \{0, 1, \ldots, n\} \to \{0, 1, \ldots, c\}$ for $c < n$ (as mentioned above, the case were $c \geq n$ is trivial).

Theorem 1 (Main Theorem 1) *Let f be a non-constant function of the form $f\colon \{0,1,\ldots,n\} \to \{0,1,\ldots,n-1\}$. Then*

$$\deg f \geq \frac{9}{22}n - O(n^{0.525}) \ .$$

We note that although the theorem is stated for $c = n-1$, it holds, from monotonicity, for every $c < n$. Combining Theorem 1 and the simple observation that for $c = n$ a function of degree 1 exists, we conclude an interesting threshold behavior at $c = n$.

The second main theorem addresses the second generalization. The following theorem gives a lower bound for functions with range that is not in $\mathbb{N}$.

Theorem 2 (Main Theorem 2) *Let $\mathcal{C} \subset \mathbb{Q}$ be a finite set.*
Let $f_n\colon \{0,1,\ldots,n\} \to \mathcal{C}$ be a family of non-constant functions. Then for every n

$$\deg f_n \geq \frac{2}{3}n - O(n^{0.525}) \ .$$

The third main result is a generalization of the main result of [vzGR97]. In order to describe it we explain the proof technique used in that paper. As mentioned, the main result in [vzGR97] is that $\deg(f) > n - O(n^{0.525})$ for any non-constant function of the form $f\colon \{0,1,\ldots,n\} \to \{0,1\}$. The idea behind their proof was to first show that when $n = p-1$, where p is prime, the degree of any non-constant symmetric Boolean function is exactly n. Applying a theorem on the gap between consecutive prime numbers it immediately follows that the degree of non-constant symmetric Boolean function, on n variables, is $n - O(n^{0.525})$. In view of this result it is natural to ask what can be said for n of the form $n = p^m - 1$. We prove the following theorem, which extends the main result of [vzGR97] (achieved by taking $m = 1$).

Theorem 3 (Main Theorem 3) *Let $n = p^m - 1$ for a prime p. Let f be a non-constant symmetric Boolean function on n variables. Then*

$$\deg f \geq p^m - p^{m-1} \geq n - n^{1-\frac{1}{m}} \ .$$

Note that the above theorem slightly improves the result of [vzGR97] for n's of the form $n = p^2 - 1$ as it gives a lower bound of $n - \sqrt{n}$ on the degree rather than $n - O(n^{0.525})$. In addition, and for completeness, we give an alternative simple proof of the fact that non-constant symmetric Boolean functions on $n = p - 1$ variables have degree n.

1.4 Structure of the Thesis

In chapter 2 we introduce some mathematical tools we shall use in the proofs. To all but one result we give a full proof (the one theorem we give no proof for is a very deep result from number theory). In chapter 3 we prove all the new results that we obtained.

Chapter 2

Mathematical Tools

In this chapter we introduce mathematical tools we will need for proving our results. The tools being used are mainly from the realm of Number Theory.

2.1 Integer Valued Polynomials

Definition 1 *For every $k \in \mathbb{N}$ we define the polynomial $\binom{x}{k}$ as follows*

$$\binom{x}{k} = \frac{x(x-1)\cdot\ldots\cdot(x-k+1)}{k!} .$$

It is easy to see that $\{\binom{x}{k}\}_{k=0}^{d}$ forms a basis for polynomials with degree at most d.

Theorem 4 *Let h be a polynomial of degree d assuming integer values at $x = 0, 1, \ldots, d$. Then one can write*

$$h(x) = \sum_{k=0}^{d} c_k \binom{x}{k}$$

where the c_k's are integers.

Proof. As mentioned, the polynomials $\binom{x}{0}, \binom{x}{1}, \ldots, \binom{x}{d}$ form a basis to the space of polynomials of degree not greater than d. Therefore, there exist $c_0, c_1, \ldots, c_d \in \mathbb{R}$ such that

$$h(x) = \sum_{k=0}^{d} c_k \binom{x}{k} .$$

We now show all c_k's are in fact integers. We use an induction on d. For $d = 0$ we have $h(x) = c_0$. Since $h(0)$ is an integer we have that c_0 is an integer. Assume the correctness of the statement for all polynomials with degree up to $d-1$. Let $h(x)$ be a polynomial of degree d that obtains integer values at $x = 0, 1, \ldots, d$. Define $g(x) = h(x+1) - h(x)$ and notice that g takes integer values on $x = 0, 1, \ldots, d-1$. Now,

$$g(x) = \sum_{k=0}^{d} c_k \left(\binom{x+1}{k} - \binom{x}{k} \right) = \sum_{k=1}^{d} c_k \binom{x}{k-1} = \sum_{k=0}^{d-1} c_{k+1} \binom{x}{k} .$$

From the induction hypothesis we now get that $c_1, c_2, \ldots, c_d$ are all integers. As $c_0 = h(0)$ the claim follows. ■

As an interesting corollary we get that a function $f\colon \{0, 1, \ldots, n\} \to \mathcal{C}$ of degree d, assuming integer values at $x = 0, 1, \ldots d$, assumes integer values on all of $\mathbb{N}$.

We should say a word on why integer coefficients are so important for us. In our proofs we would like to look at the behavior of a polynomial modulo prime numbers. We have already established that a polynomial as above assume only integer values over $\mathbb{N}$ so this idea make sense. However, if the coefficients are indeed integers, then we can simplify the analysis by looking at every coefficient modulo the prime number. This idea will prove itself useful in many of the proofs to come.

2.2 Lucas Theorem

In the previous section we established that we might benefit by examining polynomials of the form $\binom{x}{k}$. Especially when assigning an integer value to x. We also hinted that in the proofs to come we would look at such assignments modulo prime numbers. Therefore we are interested in understanding how does a binomial coefficient looks like modulo a prime number. In 1878 Edouard Lucas gave an answer for this question.

Theorem 5 (Lucas' theorem) *Let $a, b \in \mathbb{N} \setminus \{0\}$ and let p be a prime number. Denote with*

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$$

$$b = b_0 + b_1 p + b_2 p^2 + \cdots + b_k p^k$$

their base p representations. Then

$$\binom{a}{b} \equiv_p \prod_{i=0}^{k} \binom{a_i}{b_i}$$

where $\binom{a_i}{b_i} = 0$ *if* $a_i < b_i$.

Many proofs for Lucas' Theorem are known. We present a proof that is most related to the spirit of this thesis.

Proof.

$$(1+x)^a = (1+x)^{\sum_{i=0}^{k} a_i p^i} = \prod_{i=0}^{k} (1+x)^{a_i p^i} \tag{2.1}$$

It is easy to prove (by induction on $i \geq 0$) that

$$(1+x)^{p^i} \equiv_p (1+x^{p^i})$$

Therefore, from equation (2.1)

$$(1+x)^a = \prod_{i=0}^{k} (1+x)^{a_i p^i} \equiv_p \prod_{i=0}^{k} (1+x^{p^i})^{a_i} = \prod_{i=0}^{k} \sum_{j=0}^{a_i} \binom{a_i}{j} x^{j p^i} .$$

The coefficient of x^b on the LHS is $\binom{a}{b}$. Since there is a unique way to represent b in base p, it follows that the coefficient of x^b on the RHS is $\prod_{i=0}^{k} \binom{a_i}{b_i}$. Hence the result follows. ■

2.3 Gap Between Consecutive Primes

Prime numbers proved to be beautiful, enigmatic and useful for thousands of years. Many surprising results on prime numbers were discovered and countless many applications for them have been found. One central question concerns the distribution of prime numbers. Perhaps the earliest result on this question is due to Euclid who proved that there exist infinitely many primes. A more daring conjecture was taken by Joseph Bertrand in 1845. Bertrand's postulated that for an integer $n > 3$, there always exists a prime number p such that $n < p < 2n$. In 1850 Chebyshev proved Bertrand's postulate and in 1932 Erdös gave a simpler proof for it. Interestingly, Erdös

used binomial coefficients in his proof. A deeper result regarding the distribution of prime numbers is the Prime Number Theorem. This famous and deep theorem describes the asymptotic distribution of the prime numbers.

Theorem 6 *Let $\pi(n)$ be the number of positive prime numbers not larger than n. Then*

$$\pi(n) = \Theta\left(\frac{n}{\ln n}\right) .$$

The Prime Number Theorem was proved independently by Hadamard and de la Vallee Poussin in 1986. Perhaps surprisingly, both proofs used methods from complex analysis. That is, to better understand prime numbers, mathematicians had to study the complex plane.

Although Theorem 6 is of great depth, it says nothing about the maximal gap between two consecutive prime numbers as n grows. This kind of result is what we shall need in this work. Specifically, we will use the following theorem of Baker, Harman and Pintz from 2001.

Theorem 7 *For any $n \in \mathbb{N}$ there exists a prime number p such that*

$$n - O(n^{0.525}) < p < n$$

Chapter 3

Proofs of original Thesis' results

3.1 Periodicity and Degree

A common theme that appears in our proofs for lower bounding the degree of a function is to examine the periodicity structure of it.

3.1.1 Low Degree Implies Strong Periodical Structure

We next prove that a low degree function must have, in some sense, strong periodical structure.

Lemma 1 *Let $f\colon \{0,1,\ldots,n\} \to \mathcal{C}$ be a function with $\deg f = d$. Let $d < p \leq n$ be a prime number. Then for all $0 \leq j \leq \min(p-1, n-p)$ it holds that*

$$f(p+j) \equiv_p f(j) \,.$$

Proof. Let $h_f(x) = \sum_{k=0}^{d} c_k \binom{x}{k}$ be the interpolation polynomial of f. By Theorem 4 all c_k's are integers. Substituting $p+j$ for x we get

$$h_f(p+j) = \sum_{k=0}^{d} c_k \binom{p+j}{k} \,. \tag{3.1}$$

Applying Lucas' theorem (Theorem 5) while remembering that $j, k < p$ we get

$$\binom{p+j}{k} = \binom{\langle\, 1 \quad j \,\rangle_p}{\langle\, 0 \quad k \,\rangle_p} \equiv_p \binom{1}{0}\binom{j}{k} = \binom{j}{k} \,. \tag{3.2}$$

Combining (3.1), (3.2) and the assumption that $p + j \leq n$ we obtain

$$f(p+j) = h_f(p+j) = \sum_{k=0}^{d} c_k \binom{p+j}{k} \equiv_p \sum_{k=0}^{d} c_k \binom{j}{k} = h_f(j) = f(j) \ .$$

■

The lower the degree of f is, the larger the number of prime numbers in the interval $[\deg f, n]$ is. Since for each such prime number Lemma 1 reveals one more layer of periodical structure in f, we can see why Lemma 1 is a formalization of the idea mentioned above - the lower the degree of a function is, the stronger its periodical structure is.

3.1.2 Strong Periodical Structure Implies High Degree

Definition 2 *Given a function* $f\colon \{0, 1, \ldots, n\} \to \mathcal{C}$ *and* $T, \Delta \in \mathbb{N}$ *such that* $T \geq 1$ *we define*

$$P_T^{\Delta}(f) = \{0 \leq k \leq n - T\colon f(k) + \Delta = f(k+T)\} \ .$$

To get intuition for the meaning of this definition consider the case $\Delta = 0$. A periodical function with period T is a function f having the following property: for every $0 \leq k \leq n - T$ it holds that $f(k) = f(k + T)$. Given a function f (not necessarily a periodical function), we can think of every k such that $f(k) = f(k + T)$ as a test whereby the function succeeded proving it has a period T. Therefore $P_T^0(f)$ is the set of successful tests, and hence the size of this set measures how close f is to a function with period T. For general Δ the intuition is basically the same, though we relax the traditional periodicity definition. With this definition in mind we are ready to prove that a function having a strong periodical structure in this sense, has a high degree.

Lemma 2 *Let* $f\colon \{0, 1, \ldots, n\} \to \mathcal{C}$*, then for all* $T, \Delta \in \mathbb{N}$ *such that* $T \geq 1$ *it holds that*

1. *If* $\Delta = 0$ *then* $\deg f \geq \left|P_T^{\Delta}(f)\right|$ *or* $\deg f = 0$.
2. *If* $\Delta \neq 0$ *then* $\deg f \geq \left|P_T^{\Delta}(f)\right|$ *or* $\deg f \leq 1$.

Proof. Denote $d = \deg f$ and assume that $d < \left|P_T^{\Delta}(f)\right|$. Let

$$g(x) \stackrel{\text{def}}{=} h_f(x+T) - \Delta \ .$$

We notice that $\deg g = \deg h_f = d$. In addition, for all $k \in P_T^{\Delta}(f)$ it holds that

$$g(k) = h_f(k+T) - \Delta = f(k+T) - \Delta = f(k) = h_f(k) \ .$$

Therefore g and h_f agree on $\left|P_T^{\Delta}(f)\right|$ points. Since these two polynomials have degree $d < \left|P_T^{\Delta}(f)\right|$, it must hold that $g = h_f$. Denote

$$h_f(x) = \sum_{k=0}^{d} a_k x^k \ .$$

Since $\deg f = d$ we have that $a_d \neq 0$. Now,

$$\begin{aligned} \sum_{k=0}^{d} a_k x^k + \Delta = h_f(x) + \Delta = g(x) + \Delta = h_f(x+T) = \sum_{k=0}^{d} a_k (x+T)^k \\ = \sum_{k=0}^{d} a_k \sum_{j=0}^{k} \binom{k}{j} x^j T^{k-j} = \sum_{m=0}^{d} x^m \sum_{k=m}^{d} \binom{k}{m} a_k T^{k-m} \ . \end{aligned} \tag{3.3}$$

Thus, the coefficients of the LHS equal the coefficients of the RHS. Assume now that $\Delta = 0$. In this case our initial assumption that $d < \left|P_T^{\Delta}\right|$ implies $d = 0$. Indeed, Equation (3.3) implies that for $0 \leq m \leq d$

$$a_m = \sum_{k=m}^{d} \binom{k}{m} a_k T^{k-m}$$

and so for $0 \leq m \leq d$ we have

$$\sum_{k=m+1}^{d} \binom{k}{m} a_k T^{k-m} = 0 \ .$$

Assume for a contradiction that $d \geq 1$. Then for $m = d-1$ (which is non-negative) we get

$$\binom{d}{d-1} a_d T = 0 \ .$$

Since $T \geq 1$ and $d \geq 1$ it follows that $a_d = 0$, which is a contradiction.

As for the second part of the theorem, assume that $\Delta \neq 0$. In this case we want to prove that $\deg f \leq 1$. As in the case of $\Delta = 0$ we have that for $1 \leq m \leq d$

$$a_m = \sum_{k=m}^{d} \binom{k}{m} a_k T^{k-m}$$

(for $m = 0$ this equality doesn't hold since the shift by Δ affects the free term, as can be seen in Equation (3.3)). As before, we reach a contradiction by considering $m = d - 1$ (again we derive that $a_d = 0$). We can do so as long as $1 \leq d - 1$, that is, as long as $d > 1$. Therefore our assumption leads to a contradiction unless $d \leq 1$, and so we are done. ■

3.2 Proof of Main Theorem 1

3.2.1 The function $D_c(n)$

Definition 3 *Let $c \in \mathbb{N}$. We call a non-constant function of the form $f\colon \{0, 1, \ldots, n\} \to \{0, 1, \ldots, c\}$ an* (n, c)-function. *We denote by $\mathcal{F}_c(n)$ the set of all (n, c)-functions.*

As we prove a linear lower bound on the degree, it is natural to consider the following definition.

Definition 4 *We denote the* relative degree *of (n, c)-functions by*

$$\mathcal{D}_c(n) = \frac{1}{n} \min_{f \in \mathcal{F}_c(n)} \deg f \ .$$

It is easy to see that $\mathcal{D}_c(n)$ is non-increasing with respect to c. On the other hand, for a fixed c, $\mathcal{D}_c(n)$ has quite a chaotic behavior in n and is certainly not monotone. For example, it can be shown that $\mathcal{D}_1(n) < 1$ for odd n greater than 1, while it was proved in [vzGR97] that $\mathcal{D}_1(p - 1) = 1$ for all primes p.

Using this definition we can restate our question in terms of proving lower bounds on $\mathcal{D}_c(n)$ for any $1 \leq c < n$. [vzGR97] proved that $\mathcal{D}_1(n) = 1 - O(n^{-0.475}) = 1 - o(1)$ and that the trivial lower bound for general c is $\mathcal{D}_c(n) > \frac{1}{c+1}$. Using the same language, our main result shows that $\mathcal{D}_{n-1}(n) \geq \frac{9}{22} - o(1)$.

3.2.2 Proof Strategy

The proof goes in two steps. In the first step we make a reduction from $(n, n-1)$-functions to $(m, 4)$-functions for some m, namely we make a reduction to $c = 4$. This certainly seems like an easier problem to tackle, as c is now constant. In the second step we further reduce the problem by reducing n. That is, we show that a lower bound on $D_c(m)$ implies a lower bound for $D_c(n)$ under some conditions on $n > m$ and c. Although we will apply only the case where $c = 4$, we will give a theorem for general c, that sheds light on the behavior of $D_c(n)$ and is therefore interesting in its own right.

3.2.3 Reduction to $c = 4$

In this section we prove the following lemma, which formalizes the first step of our proof strategy.

Lemma 3 (Reduction to $c = 4$) *For any n there exists a prime p such that $n - O(n^{0.525}) < 2p < n$ and*

$$\mathcal{D}_{n-1}(n) \geq \frac{1}{2}\mathcal{D}_4(p-1) - o(1) \; .$$

Proof. Let $f \in \mathcal{F}_{n-1}(n)$ be a function with minimal degree $n \cdot \mathcal{D}_{n-1}(n)$. Let p be a prime such that

$$\frac{n}{2} - O((\frac{n}{2})^{0.525}) < p < \frac{n}{2}$$

as guaranteed by Theorem 7. Clearly

$$n - O(n^{0.525}) < 2p < n \; .$$

Let $\tilde{f}$ be the restriction of f to the domain $\{0, 1, \ldots, 2p-1\}$. Note that $\deg f \geq \deg \tilde{f}$. If $\deg \tilde{f} \geq p$ then

$$n \cdot \mathcal{D}_{n-1}(n) = \deg f \geq \deg \tilde{f} \geq p > \frac{n}{2} - o(n)$$

and we are done. We can therefore assume that $\deg \tilde{f} < p$.

Define $g \colon \{0, 1, \ldots, p-1\} \to \mathbb{R}$ as follows

$$g(k) = 2 + \frac{\tilde{f}(p+k) - \tilde{f}(k)}{p} \; .$$

It is easy to see that $\deg g < \deg \tilde{f}$. To better understand g, note that Lemma 1 implies that for any $0 \leq k \leq p-1$ it holds that

$$\tilde{f}(p+k) \equiv_p \tilde{f}(k) \ .$$

For large enough n, we have that for all $0 \leq j \leq 2p-1$

$$0 \leq \tilde{f}(j) < n < 3p \ ,$$

therefore

$$\tilde{f}(p+k) - \tilde{f}(k) \in \{-2p, -p, 0, p, 2p\} \ .$$

Consequently, g maps $\{0, 1, \ldots, p-1\}$ to $\{0, 1, 2, 3, 4\}$. In other words, g is a $(p-1, 4)$-function. If g is not a constant then

$$n \cdot \mathcal{D}_{n-1}(n) = \deg f \geq \deg \tilde{f} \geq \deg g \geq (p-1) \cdot \mathcal{D}_4(p-1) > \left(\frac{n}{2} - o(n)\right) \cdot \mathcal{D}_4(p-1) \ .$$

Dividing both sides by n we conclude the proof.

We now deal with the case that g is a constant function, say the constant G. Thus, for all $0 \leq k \leq p-1$ we have that

$$\tilde{f}(p+k) = \tilde{f}(k) + (G-2)p$$

and therefore, recalling Definition 2

$$|P_p^{(G-2)p}(\tilde{f})| \geq p \ .$$

By Lemma 2, either

$$\deg \tilde{f} \geq |P_p^{(G-2)p}(\tilde{f})| \geq p \geq \frac{n}{2} - o(n) \ ,$$

which concludes the proof, or $\tilde{f}$ is a linear function. Assume the latter occurs and repeat the above proof for the function $f^R \in \mathcal{F}_{n-1}(n)$ defined as

$$f^R(k) \stackrel{\text{def}}{=} f(n-k) \ .$$

If by applying the proof on f^R we get that

$$\deg f^R \geq \frac{1}{2}\mathcal{D}_4(p-1) - o(1)$$

then, since $\deg f = \deg f^R$, we are done. Otherwise we again get that $\tilde{f^R}$ is a linear function. Combining the facts that $\tilde{f}$ and $\tilde{f^R}$ are both linear functions we see that f behaves like a linear function on the first and the last $2p$ points. Since $n < 2p + o(n)$, f must itself be a linear function, as the two linear functions $\tilde{f}$ and $\tilde{f^R}$ agree on more than two points. Since f is not constant, this means that f assumes $n+1$ different values on $\{0, 1, \ldots, n\}$, contradicting the fact that $f \in \mathcal{F}_{n-1}(n)$. ■

We would like to point out that for the case $n = 2p - 1$, for a prime p, we can do slightly better. In such a case g is actually a $(p-1, 2)$ function rather than a $(p-1, 4)$ function, as the difference $\tilde{f}(k+p) - \tilde{f}(k)$ is contained in $\{-p, 0, p\}$. In this thesis we prove better lower bounds on $D_2(n)$ than on $D_4(n)$, which in turn implies improved lower bound on $D_{n-1}(n)$ in the case of $n = 2p - 1$. A corollary of Theorem 3 is the following

Corollary 1 *Fore every n*

$$D_{n-1}(n) > \frac{1}{10} - o(1) .$$

Proof. As observed earlier, we have that $D_4(p) > 1/5$. Plugging this into Lemma 3 we get that

$$\mathcal{D}_{n-1}(n) \geq \frac{1}{2}\mathcal{D}_4(p) - o(1) > \frac{1}{2} \cdot \frac{1}{5} - o(1) = \frac{1}{10} - o(1) .$$

■

Corollary 1 already gives us the desired threshold behavior at $c = n$. The next step will be to improve this lower bound.

3.2.4 Reducing n

In this subsection we shall prove the following lemma.

Lemma 4 (Reducing n) *Let $c, m, n \in \mathbb{N} \setminus \{0\}$ be such that $n > 2^{m+1}(m+1)c$. Then, for large enough n*

$$\mathcal{D}_c(n) \geq \frac{m}{m+1}\mathcal{D}_c(m) - o(1) .$$

Although we've mentioned that $\mathcal{D}_c(n)$ is not monotone in n, Lemma 4 shows that some relaxed property of monotonicity does hold - given a large m, for large enough n's we almost have that $\mathcal{D}_c(n) \geq \mathcal{D}_c(m)$. In order to prove Lemma 4, it is more convenient to talk about the *gap* of functions.

Definition 5 *Given $f \in \mathcal{F}_c(n)$, define*

$$\gamma(f) \stackrel{def}{=} n - \deg f \ .$$

We call $\gamma(f)$ the gap of f.

Definition 6 *Define*

$$\Gamma_c(n) \stackrel{def}{=} \max_{f \in \mathcal{F}_c(n)} \gamma(f) \ .$$

We call $\Gamma_c(n)$ the gap of (n,c)-functions.

It is easy to verify the following relation between the relative degree and the gap of functions:

$$\Gamma_c(n) = n(1 - \mathcal{D}_c(n)) \ .$$

Proving Lemma 4 will require some tools. The following theorem from [vzGR97] gives an equivalent condition for a function to have a gap at least r. We give the relevant part of the theorem with some adaptation in notations.

Theorem 8 (Theorem 2.2 from [vzGR97]) *Given $f \in \mathcal{F}_c(n)$ and $0 \leq r \leq n$, $\gamma(f) > r$ iff for all $n - r \leq s \leq n$ it holds that*

$$\sum_{k=0}^{s} (-1)^k \binom{s}{k} f(k) = 0 \ .$$

To prove Lemma 4 we will also need to know, given $f \in \mathcal{F}_c(n)$, the value of $h_f(n+t)$ for $t \in \mathbb{N}$, where h_f is the interpolation polynomial for f. For this we have the following lemma.

Lemma 5 *For any function $f \in \mathcal{F}_c(n)$ and for any $t \in \mathbb{N} - \{0\}$*

$$h_f(n+t) = (-1)^n \sum_{k=0}^{n} (-1)^k \binom{n+t}{k} \binom{n+t-k-1}{t-1} f(k) \ .$$

Proof. Lagrange interpolation formula implies that

$$h_f(x) = \sum_{k=0}^{n} f(k) \prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{x-j}{k-j} \ .$$

Substituting $n+t$ for x we get

$$\begin{aligned} h_f(n+t) &= \sum_{k=0}^{n} \Big(\prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{n+t-j}{k-j} \Big) f(k) = \sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!} \frac{(n+t)!}{(t-1)!(n+t-k)} f(k) \\ &= (-1)^n \sum_{k=0}^{n} (-1)^k \frac{(n+t)!}{k!(n+t-k)!} \frac{(n+t-k-1)!}{(n-k)!(t-1)!} f(k) \\ &= (-1)^n \sum_{k=0}^{n} (-1)^k \binom{n+t}{k} \binom{n+t-k-1}{t-1} f(k) \ . \end{aligned}$$

■

The following lemma is useful for the proof of Lemma 4.

Lemma 6 *For all $n, m, c \in \mathbb{N}$ we have that*

$$\Gamma_c(n+m) \leq \Gamma_c(n) + m \ .$$

Proof. Let $f \in F_c(n+m)$ be a function of minimal degree. That is

$$\deg f = n + m - \Gamma_c(n+m) \ .$$

Assume for a contradiction that $\deg f < n - \Gamma_c(n)$. Let $g \in F_c(n)$ be the restriction of f to $\{0, 1, \ldots, n\}$. By our assumption $\deg f \leq n$ and so by the uniqueness of the representing polynomial, $\deg f = \deg g$. As f is non-constant we get g is non-constant (otherwise, if f is constant on $\{0, 1, \ldots, n\}$ then it must have degree at least n). Hence, $\deg g \geq n - \Gamma_c(n)$. This contradicts the assumption that $\deg g = \deg f < n - \Gamma_c(n)$. Therefore $\deg f \geq n - \Gamma_c(n)$ and we are done. ■

It easily follows from the relation between $\mathcal{D}_c(n)$ and $\Gamma_c(n)$ that Lemma 4 is equivalent to the following lemma.

Lemma 7 *Let $c, m, n \in \mathbb{N} \setminus \{0\}$ be such that $n > 2^{m+1}(m+1)c$. Then, for large enough n*

$$\Gamma_c(n) \leq \left(\frac{\Gamma_c(m)+1}{m+1} \right) n + o(n) \ .$$

We shall therefore focus on proving Lemma 7. The heart of the proof is the following lemma.

Lemma 8 *For all $c, m, p \in \mathbb{N} - \{0\}$ such that p is a prime and $2^m c < p$, it holds that*

$$\Gamma_c\left((m+1)p-1\right) < p\left(\Gamma_c\left(m\right)+1\right) \ .$$

Proof. If this inequality does not hold then there is a function $f \in \mathcal{F}_c\left((m+1)p-1\right)$ such that $\deg f < (m-\gamma)p$, where $\gamma \stackrel{\text{def}}{=} \Gamma_c\left(m\right)$. Hence the value of f on the points $\{0, 1, \ldots, (m-\gamma)p-1\}$ completely determines h_f. For every $0 \leq j \leq p-1$ define the function $f_j \in \mathcal{F}_c\left(m\right)$ as follows: for every $0 \leq i \leq m$

$$f_j(i) \stackrel{\text{def}}{=} f(i \cdot p + j) \ .$$

The strategy of the proof is to show that under the contradiction assumption, all f_j's are constants and therefore f is periodical with period p. At that point, applying Lemma 3.2 (with $\Delta = 0$) will yield a contradiction.

For every $0 \leq r \leq \gamma$ and for every $0 \leq j \leq p-1$, the value of $h_f((m-r)p+j)$ is determined by the value of f on the points $\{0, 1, \ldots, (m-r)p-1\}$.[1] Therefore we can apply Lemma 5 with $n = (m-r)p-1$ and $t = j+1$ to get

$$h_f((m-r)p+j) =$$

$$(-1)^{(m-r)p-1} \sum_{k=0}^{(m-r)p-1} (-1)^k \binom{(m-r)p+j}{k} \binom{(m-r)p+j-k-1}{j} f(k) \ .$$

Since $0 \leq j \leq p-1$ we have

$$(m-r)p+j = \langle\, m-r \quad j \,\rangle_p \ .$$

Observe that $k < p^2$ and so $k = \langle\, k_1 \quad k_0 \,\rangle_p$. Thus, in order for k to contribute to the sum modulo p, it must hold that $k_0 \leq j$. Assume that $k_0 < j$, that is $j - k_0 - 1 \geq 0$. Note that

$$(m-r)p+j-k-1 = \langle\, m-r-k_1 \quad j-k_0-1 \,\rangle_p \ .$$

[1] Actually, as stated above, $h_f((m-r)p+j)$ is determined by the first $(m-\gamma)p$ points from this set, but for the sake of the analysis, it is more convenient to see the affect of all of those points on $h_f((m-r)p+j)$.

Consequently, for k to contribute to the sum modulo p, we must have $j - k_0 - 1 \geq j$. Hence $k_0 \leq -1$, which is impossible. Thus, all k's that contribute to the sum modulo p satisfy $k_0 = j$. With this in mind we can simplify the sum over $\mathbb{F}_p$

$$h_f((m-r)p+j) \equiv_p \tag{3.4}$$
$$(-1)^{m-r-1} \sum_{k_1=0}^{m-r-1} (-1)^{k_1 p+j} \binom{(m-r)p+j}{k_1 p+j} \binom{(m-r-k_1)p-1}{j} f(k_1 p+j) \; .$$

By Lucas' Theorem

$$\binom{(m-r)p+j}{k_1 p+j} \equiv_p \binom{m-r}{k_1}$$

and

$$\binom{(m-r-k_1)p-1}{j} \equiv_p \; . \binom{p-1}{j} \; .$$

Now

$$j! \binom{p-1}{j} = (p-1)(p-2) \cdot \ldots \cdot (p-j) \equiv_p (-1)^j \cdot j!$$

and since $j! \neq 0$ it follows that

$$\binom{p-1}{j} \equiv_p (-1)^j \; .$$

With this we can simplify equation (3.4) a little further

$$h_f((m-r)p+j) \equiv_p (-1)^{m-r-1} \sum_{k_1=0}^{m-r-1} (-1)^{k_1} \binom{m-r}{k_1} f(k_1 p+j) \; .$$

Since $h_f((m-r)p+j) = f((m-r)p+j)$ we have that for all $0 \leq j \leq p-1$ and all $0 \leq r \leq \gamma$

$$\sum_{k_1=0}^{m-r} (-1)^{k_1} \binom{m-r}{k_1} f_j(k_1) \equiv_p 0 \; .$$

The LHS is strictly smaller than $2^m c$ and since we assume that $2^m c < p$, it must hold that

$$\sum_{k_1=0}^{m-r} (-1)^{k_1} \binom{m-r}{k_1} f_j(k_1) = 0 \; .$$

Applying Theorem 8 we get that for every $0 \leq j \leq p-1$, $\gamma(f_j) > \gamma = \Gamma_c(m)$. Hence all f_j's must be constant functions. This implies that f is a periodical function with period p. That is $\left|P_p^0(f)\right| = mp$. By Lemma 3.2 we get that $\deg f \geq mp$. Recalling the assumption $\deg f < (m-\gamma)p$, we contradict the assumption that $\gamma \geq 0$. ■

We are now ready to prove Lemma 7.

Proof of Lemma 7. Given n and m, we can apply Theorem 7 to assure the existence of a prime number p such that

$$\frac{n}{m+1} - O\left(\left(\frac{n}{m+1}\right)^{0.525}\right) \leq p < \frac{n}{m+1} .$$

Since $m = o(n)$, $n - o(n) \leq (m+1)p - 1 < n$. By Lemma 6

$$\Gamma_c(n) \leq \Gamma_c((m+1)p-1) + n - ((m+1)p-1) \leq \Gamma_c((m+1)p-1) + o(n) . \tag{3.5}$$

We now apply Lemma 8 (noticing that $p > 2^m c$, for large enough n)

$$\Gamma_c((m+1)p-1) < p(\Gamma_c(m)+1) = (m+1)p\left(\tfrac{\Gamma_c(m)+1}{m+1}\right) \leq n\left(\tfrac{\Gamma_c(m)+1}{m+1}\right) . \tag{3.6}$$

Inequalities (3.5) and (3.6) together imply that

$$\Gamma_c(n) \leq \left(\frac{\Gamma_c(m)+1}{m+1}\right)n + o(n) ,$$

as desired. ■

3.2.5 Concluding the proof of Theorem 1

All there is left to do is to conclude the main theorem. We will base the proof on Lemma 3, Lemma 4 and on a computer search.

Proof of Theorem 1. A computer search found that $\mathcal{D}_4(21) = 6/7$. The program we wrote computed the degree of all functions of the form $f\colon \{0,1,\ldots,21\} \to \{0,1,2,3,4\}$. In fact, we used some optimizations in order to speed up the search. By Lemma 4

$$\mathcal{D}_4(n) \geq \frac{21}{21+1} \cdot \frac{6}{7} - o(1) = \frac{9}{11} - o(1) .$$

Lemma 3 now gives

$$\mathcal{D}_{n-1}(n) \geq \frac{1}{2} \cdot \mathcal{D}_4(p) - o(1) \geq \frac{1}{2} \cdot \frac{9}{11} - o(1) = \frac{9}{22} - o(1) \ .$$

■

In subsection 3.2.3 we hinted that we can obtain a better lower bound on $\mathcal{D}_2(n)$ than that we proved for $\mathcal{D}_4(n)$. Following the last step of the proof of Theorem 1 and the fact that $\mathcal{D}_2(35) = 8/9$ (again, obtained using a computer search) we get that $\mathcal{D}_2(n) \geq 8/9 - o(1)$.

3.3 Proof of Main Theorem 2

In this section we prove Theorem 2. In order to do so we shall prove the following lemma, which gives better lower bound than Theorem 1 for c's that are not too large.

Lemma 9 *If* $c < \frac{2}{3}n - \Omega\left(n^{0.525}\right)$ *then*

$$\mathcal{D}_c(n) > \frac{2}{3} - o(1) \ .$$

Proof. By Theorem 7 there exist primes p and q such that

$$\frac{2}{3}n - O(n^{0.525}) < q < p < \frac{2}{3}n \ .$$

It suffices to prove that $\deg f \geq q$. Assume for contradiction that $\deg f < q$. Lemma 3.1 implies that, for $0 \leq j \leq n - q$, it holds that

$$f(q + j) \equiv_q f(j) \ .$$

Since $c < \frac{2}{3}n - \Omega(n^{0.525})$ (and so $c < q$) equality must hold. Namely, $f(q+j) = f(j)$ for $0 \leq j \leq n - q$. Applying the same arguments for p instead of q, we also get that $f(p + j) = f(j)$ for $0 \leq j \leq n - p$. Set $T = p - q$. From the discussion above, for all $0 \leq j \leq n - p$ it holds that

$$f(j) = f(p + j) = f(q + (p - q) + j) = f(q + (T + j)) = f(T + j) \ .$$

Therefore

$$\{0, 1, \ldots, n - p\} \subseteq P_T^0(f) \ .$$

As $n-p<n-q$ we get that for $0\leq j\leq n-p<n-q$,

$$f(T+j)=f(j)=f(q+j)\ .$$

Hence, we also have that

$$\{q+0,q+1,\ldots,q+n-p\}\subseteq P_T^0(f)\ .$$

As $n-p<q$ these two intervals do not intersect and so we have that

$$\left|P_T^0(f)\right|>2(n-p)>\frac{2}{3}n\ .$$

By Lemma 3.2, $\deg f>\frac{2}{3}n$, contradicting our assumption that

$$\deg f<q<\frac{2}{3}n\ .$$

■

With Lemma 9 we are ready to prove Theorem 2.

Proof of Theorem 2. Firstly note that we can assume that $\mathcal{C}$ contains only non-negative elements, possibly by shifting all elements of $\mathcal{C}$ by some Δ. Indeed, for any non-constant polynomial

$$\deg(h(x))=\deg\left(\Delta+h(x)\right)\ .$$

Let us denote

$$\mathcal{C}=\{\frac{a_1}{b_1},\ldots,\frac{a_k}{b_k}\}\ ,$$

where $k=|\mathcal{C}|$ and all elements in $\mathcal{C}$ are non-negative. Define $l=\operatorname{lcm}(b_1,\ldots,b_k)$ and $m=\max(x\colon x\in C)$. Finally, set $c=l\cdot m$. Let $\tilde{f}$ be defined as follows: $\tilde{f}(k)=l\cdot f(k)$ for all $0\leq k\leq n$. Clearly, $\tilde{f}\in\mathcal{F}_c(n)$ and $\deg\tilde{f}=\deg f$. Furthermore, since f is non-constant so is $\tilde{f}$. As l,m are constants so is c and thus, by applying Lemma 9, we get that

$$\deg f\geq\deg\tilde{f}\geq\frac{2}{3}n-o(n)\ ,$$

as desired.

■

In fact one can deduce lower bounds on the degree of functions whose image may depend on n. For example, consider any family of non-constant functions of the form

$$f\colon \{0,1,\ldots,n\} \to \{2^{-1},2^{-2},2^{-3},\ldots,2^{-m}\}\ ,$$

where $m < \log n$. In this case we can define the function $\tilde{f}$ as $\tilde{f}(k) = 2^m f(k)$. Clearly $\tilde{f} \in \mathcal{F}_c\,(n)$ for

$$c = 2^{m-1} < \frac{1}{2}n < \frac{2}{3}n - \Omega(n^{0.525})$$

and so applying Lemma 9 we again obtain that

$$\deg f = \deg \tilde{f} \geq \frac{2}{3}n - o(1)\ .$$

3.4 Proof of Main Theorem 3

In this section we prove a Theorem 3.

Proof of Theorem 3. Let $f \in \mathcal{F}_1\,(p^m - 1)$. Assume for contradiction that $\deg f < p^m - p^{m-1}$. Then h_f is determined by the value of f on the points $\{0,1,\ldots,p^m - p^{m-1} - 1\}$. Applying Lemma 5 with $n = p^m - p^{m-1} - 1$ and $t = j+1$, for $0 \leq j < p^{m-1}$, we obtain

$$h_f(p^m - p^{m-1} + j) =$$
$$(-1)^{p^m - p^{m-1} - 1} \sum_{k=0}^{p^m - p^{m-1} - 1} (-1)^k \binom{p^m - p^{m-1} + j}{k} \binom{p^m - p^{m-1} + j - k - 1}{j} f(k)\ .$$

Set $k' = k \mod p^{m-1}$, that is

$$k' = k_0 + k_1 p + \cdots + k_{m-2} p^{m-2}\ .$$

Since $k < p^m$ we can write $k = k' + k_{m-1}p^{m-1}$ for $0 \leq k_{m-1} \leq p-1$. As $0 \leq j < p^{m-1}$

$$p^m - p^{m-1} + j = \langle\, p-1 \quad j_{m-2} \quad \ldots \quad j_0 \,\rangle_p$$

and so in order for k to contribute to the sum modulo p, it must be that $k' \leq j$. Assume that k is such that $k' < j$. Looking at the other binomial

coefficient, for such a k to contribute to the sum modulo p, it must be that $j - k' - 1 \geq j$ which is impossible. Hence the only k's that contribute to the sum, modulo p, are those obeying $k' = j$. With this observation, we can simplify the above sum over $\mathbb{F}_p$

$$\begin{aligned} &- h_f(p^m - p^{m-1} + j) \equiv_p \\ &\sum_{k_{m-1}=0}^{p-2} (-1)^{j+k_{m-1}p^{m-1}} \binom{p^m - p^{m-1} + j}{k_{m-1}p^{m-1} + j} \binom{p^m - (k_{m-1}+1)p^{m-1} - 1}{j} \cdot \\ &\qquad \cdot f(k_{m-1}p^{m-1} + j) \ . \end{aligned} \tag{3.7}$$

From Lucas' theorem

$$\binom{p^m - p^{m-1} + j}{k_{m-1}p^{m-1} + j} \equiv_p \binom{p-1}{k_{m-1}} \equiv_p (-1)^{k_{m-1}} \tag{3.8}$$

and

$$\binom{p^m - (k_{m-1}+1)p^{m-1} - 1}{j} \equiv_p \binom{p^{m-1} - 1}{j} \ .$$

This binomial coefficient is actually quite simple modulo p

$$\binom{p^{m-1} - 1}{j} \equiv_p \prod_{i=0}^{m-2} \binom{p-1}{j_i} \equiv_p \prod_{i=0}^{m-2} (-1)^{j_i} \equiv_p \prod_{i=0}^{m-2} (-1)^{j_i p^i} = (-1)^j$$

and so

$$\binom{p^m - (k_{m-1}+1)p^{m-1} - 1}{j} \equiv_p (-1)^j \ . \tag{3.9}$$

Substituting (3.8) and (3.9) into (3.7) simplifies the expression a little further

$$-h_f(p^m - p^{m-1} + j) \equiv_p \sum_{k_{m-1}=0}^{p-2} f(k_{m-1}p^{m-1} + j) \ .$$

As $h_f(p^m - p^{m-1} + j) = f(p^m - p^{m-1} + j)$ we get that for every $0 \leq j < p^{m-1}$

$$\sum_{k_{m-1}=0}^{p-1} f(k_{m-1}p^{m-1} + j) \equiv_p 0 \ . \tag{3.10}$$

Since f is a Boolean function, in order to satisfy Equation (3.10), it must be that for every $0 \leq j < p^{m-1}$

$$f(j) = f(p^{m-1} + j) = f(2p^{m-1} + j) = \cdots = f((p-1)p^{m-1} + j) \ .$$

Therefore, f is periodical with period p^{m-1} which yields that

$$\left|P_p^0(f)\right| \geq p^m - p^{m-1} \ .$$

Lemma 2 now implies that

$$\deg f \geq p^m - p^{m-1} \geq n - n^{1-\frac{1}{m}} \ .$$

■

3.5 Simplified Alternative Proof for the main result of [vzGR97]

In this section we give a simpler alternative proof for the main result of [vzGR97].

Claim 1 *For any prime p it holds that $\mathcal{D}_1(p-1) = 1$.*

Alternative proof for $\mathcal{D}_1(p-1) = 1$. Let $f \in \mathcal{F}_1(n)$ for $n = p-1$. Obviously, the following polynomial represents f over $\mathbb{F}_p$

$$h(x) = \sum_{k:\ f(k)=1} \left(1 - (x-k)^{p-1}\right) \ .$$

The coefficient of x^{p-1} is the weight of f (i.e the number of 1's f assumes), and since f is not constant this number is not divisible by p. Therefore $\deg h = p-1$. Consider now h_f, the polynomial representing f over $\mathbb{R}$. From Lagrange interpolation formula we have

$$h_f(x) = \sum_{k:\ f(k)=1} \prod_{\substack{j=0 \\ j \neq k}}^{p-1} \frac{x-j}{k-j} \ .$$

Note that none of the denominators of the multiplicands in the above expression is a multiple of p and so we may view h_f as a polynomial over $\mathbb{F}_p$. Formally, we define

$$h_f^{(p)}(x) = \sum_{k:\ f(k)=1} \prod_{\substack{j=0 \\ j\neq k}}^{p-1} (x-j)(k-j)^{-1} \ .$$

It is clear that

$$\deg h_f^{(p)} \leq \deg(h_f) \leq p-1 \tag{3.11}$$

and so $h_f^{(p)}$ is an interpolating polynomial of degree at most $p-1$ of f over $\mathbb{F}_p$. Hence by the uniqueness of the interpolating polynomial $h_f^{(p)} = h$ and in particular $\deg h_f^{(p)} = p-1$. Looking at (3.11) we get $\deg h_f = p-1$. ■

Chapter 4

Open Problems and Future Directions

In this thesis we studied the degree of functions of the form $f\colon \{0,1,\ldots,n\} \to \mathcal{C}$ for two specific types of restrictions on $\mathcal{C}$. Specifically, for $\mathcal{C} = \{0,1,\ldots,c\}$ we proved a threshold behavior at $c = n$. In particular, we proved that whenever $c < n$, a non-constant function of the form $f\colon \{0,1,\ldots,n\} \to \{0,1,\ldots,c\}$ has a degree which is linear in n. We would like to gain better understanding on the behavior of the degree of such functions in terms of n and c. That is, to understand the function $\mathcal{D}_c(n)$.

Open Problem 1: What is the asymptotical behavior of $\mathcal{D}_c(n)$ in terms of n and c?

For the specific case $c = n-1$, using our techniques (specifically Lemma 3), one cannot prove a lower bound that is better than $1/2 - o(1)$ on $\mathcal{D}_{n-1}(n)$. Moreover, if $\mathcal{D}_4(n) = 1 - o(1)$ then, from Lemma 3, we obtain that $\mathcal{D}_{n-1}(n) = 1/2 - o(1)$. On the other hand, looking at some small values of n, using a computer program, we found that for those values $\mathcal{D}_{n-1}(n) \sim 1/2$.

Open Problem 2: Does $\mathcal{D}_{n-1}(n) \sim 1/2$?

For the specific case $c = 1$, the following conjecture from [vzGR97] is still open

Open Problem 3: Does $\Gamma_1(n) = O(1)$?

A natural generalization is the following:

Open Problem 4: Consider a non-constant function of the form $f\colon \{0,1,\ldots,n\}^m \to \{0,1,\ldots,c\}$. What can be said about the degree of functions of this form?

Bibliography

[BdW02] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: a survey. *Theor. Comput. Sci.*, 288(1):21–43, 2002.

[Gop06] P. Gopalan. Constructing ramsey graphs from boolean function representations. *IEEE Conference on Computational Complexity (CCC)*, 2006.

[HMP+93] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, and G. Turán. Threshold circuits of bounded depth. *J. of Computer and System Sciences*, 46(2):129–154, April 1993.

[KOS04] A. R. Klivans, R. O'Donnell, and R. A. Servedio. Learning intersections and thresholds of halfspaces. *J. Comput. Syst. Sci.*, 68(4):808–840, 2004.

[NR04] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, 2004.

[NS94] N. Nisan and M. Szegedy. On the degree of boolean functions as real polynomials. *Computational Complexity*, 4:301–313, 1994.

[Raz03] A. A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145–159, 2003.

[Ste03] D. Stefankovic. Fourier transforms in computer science. Master's thesis, University of Chicago, Department of Computer Science, 2003.

[vzGR97] Joachim von zur Gathen and James R. Roche. Polynomials with two values. *Combinatorica*, 17(3):345–362, 1997.

נעיר עוד כי למה 3 מבטיחה לנו חסם תחתון לינארי על הדרגה של כל פונקציה לא-קבועה מהצורה $f:\{0,1,\ldots,n\}\to\{0,1,\ldots,n-1\}$. אכן, ציינו קודם כי $D_4(n)>1/5$ ולכן, מלמה 3

$$D_{n-1}(n)\geq\frac{1}{2}\cdot\frac{1}{5}-o(1)=\frac{1}{10}-o(1)$$

בשלב השני של ההוכחה אנו משפרים את החסם התחתון הזה ל-$9/22-o(1)$. האופן בו אנו מוכיחים זאת הוא כללי יותר, ונתון בלמה הבאה, המעניינת בפני עצמה.

למה 4

יהיו $c,m,n\in\mathbb{N}\setminus\{0\}$ כך ש-$n>2^m c$. אז

$$D_c(n)\geq\frac{m}{m+1}D_c(m)-o(1)$$

למה 4 מבטיחה לנו מונוטוניות של הפונקציה D_c במובן כלשהו. מונוטוניות פירושה ש-$D_c(n)\geq D_c(m)$ לכל $n>m$. בלמה 4 אי-השוויון הזה מתקיים בגרסה מוחלשת (כאשר $m\to\infty$ אז הפקטור הכפלי שואף ל-1 והפקטור החיבורי השלישי שואף ל-0) עבור n-ים הגדולים אקספוננציאלית מ-m.

תוכנית מחשב פשוטה שהרצנו חישבה ומצאה כי $D_4(21)=6/7$. מלמה 4 נקבל אז כי

$$D_4(n)\geq\frac{21}{21+1}D_4(21)-o(1)=\frac{21}{22}\cdot\frac{6}{7}-o(1)=\frac{9}{11}-o(1)$$

המשפר משמעותית את החסם $D_4(n)\geq1/5$ שהיה ידוע קודם. הצבה של החסם המשופר הזה בלמה 3 נותנת

$$D_{n-1}(n)\geq\frac{1}{2}D_4(p)-o(1)=\frac{1}{2}\cdot\left(\frac{9}{11}-o(1)\right)-o(1)=\frac{9}{22}-o(1)$$

מה שמוכיח את משפט 1.

נציין כי ההוכחות של למה 3 ולמה 4 מתבססות על למה 1 ולמה 2.

תהא $f:\{0,1,2,\ldots,n\}\to\{0,1,2,\ldots,c\}$ פונקציה לא-קבועה ויהיו $T,\Delta\in\mathbb{N}$ כך ש-$T\geq 1$. נגדיר

$$P_T^{\Delta}(f)=\{0\leq k\leq n-T : f(k)+\Delta=f(k+t)\}$$

למה 2

תהא $f:\{0,1,2,\ldots,n\}\to\{0,1,2,\ldots,c\}$ פונקציה לא-קבועה ויהיו $T,\Delta\in\mathbb{N}$ כך ש-$T\geq 1$. אז

1. אם $\Delta=0$ אז $\deg f\geq\left|P_T^{\Delta}(f)\right|$.
2. אם $\Delta\neq 0$ אז $\deg f\geq\left|P_T^{\Delta}(f)\right|$ או ש-f לינארית.

נתאר כעת את האסטרטגיה עליה מבוססת הוכחת משפט 1. ההוכחה מתחלקת לשני שלבים, אותם נתאר לאחר ההגדרה הבאה:

הגדרה

נסמן

$$D_c(n)=\frac{1}{n}\min\{\deg f \mid f:\{0,1,\ldots,n\}\to\{0,1,\ldots,c\} \text{ and } f \text{ is non-constant}\}$$

בשלב הראשון אנו מבצעים רדוקציה מהוכחת חסם תחתון לדרגה של פונקציות לא-קבועות מהצורה $f:\{0,1,2,\ldots,n\}\to\{0,1,2,\ldots,n-1\}$ להוכחת חסם תחתון לדרגה של פונקציות לא-קבועות מהצורה $g:\{0,1,2,\ldots,m\}\to\{0,1,2,3,4\}$. כלומר, אנו מוכיחים כי מספיק לדון בפונקציות המקבלות מספר מצומצם של ערכים. זאת אנו מסכמים בלמה הבאה:

למה 3

לכל n טבעי גדול דיו קיים מספר ראשוני p כך ש-$n-O\left(n^{0.525}\right)<2p<n$ ו-

$$D_{n-1}(n)\geq\frac{1}{2}D_4(p)-o(1)$$

התוצאה השלישית בעבודה זו מכלילה את התוצאה הידועה עבור המקרה בו $C=\{0,1\}$. ההוכחה הידועה התבססה על כך שעבור $n=p-1$, כאשר p ראשוני, הדרגה של כל פונקציה לא-קבועה מהצורה $f:\{0,1,2,\ldots,n\}\to\{0,1\}$ היא מלאה (כלומר n). שימוש במשפט מתורת המספרים הנוגע לצפיפות בין מספרים ראשוניים מסיים את ההוכחה. שאלה טבעית היא מה ניתן לומר על הדרגה של כל פונקציה לא-קבועה מהצורה $f:\{0,1,2,\ldots,n\}\to\{0,1\}$ עבור $n=p^m-1$ כאשר p ראשוני ו- m טבעי כלשהו.

משפט 3

יהא $n=p^m-1$ כאשר p ראשוני ו- m טבעי כלשהו. תהא $f:\{0,1,2,\ldots,n\}\to\{0,1\}$ פונקציה לא-קבועה. אז

$$\deg f \geq n-n^{1-\frac{1}{m}}$$

הערה

משפט 3 אכן מכליל את התוצאה הידועה ($m=1$). בנוסף, עבור $m=2$, אנו מקבלים חסם תחתון טוב יותר במעט מזה הידוע. כלומר, עבור $n=p^2-1$ משפט 3 מבטיח חסם תחתון של $n-\sqrt{n}$ על הדרגה של כל פונקציה לא-קבועה, בעוד התוצאה הקיימת הבטיחה רק $n-O\left(n^{0.525}\right)$.

טכניקות הוכחה

ההוכחות לכל שלושת המשפטים מתבססות על זוג הלמות הבאות. את הלמות הללו הוכחנו בעזרת כלים מתורת המספרים ומאלגברה.

למה 1

תהא $f:\{0,1,2,\ldots,n\}\to\{0,1,2,\ldots,c\}$ פונקציה לא-קבועה עם דרגה d. יהא p מספר ראשוני כך ש- $d<p\leq n$. אז לכל $0\leq j<p$ כך ש- $p+j\leq n$ מתקיים

$$f\left(p+j\right)\equiv_p f\left(j\right)$$

ניסוח הלמה השנייה מתבסס על ההגדרה הבאה:

הגדרה

ערכים שונים, הוא מדרגה d לפחות. בפרט, עבור פונקציות לא-קבועות מהצורה $f:\{0,1,\ldots,n\}\to\{0,1,\ldots,c\}$ אנו מקבלים את החסם התחתון $(n+1)/(c+1)$. התוצאה הראשונה שלנו נתונה במשפט הבא:

משפט 1

תהא $f:\{0,1,2,\ldots,n\}\to\{0,1,2,\ldots,n-1\}$ פונקציה לא-קבועה. אז

$$\deg f \geq \frac{9}{22}n - O\left(n^{0.525}\right)$$

הערה

משפט 1 אמנם מתייחס רק למקרה $c=n-1$, אך קל להיווכח כי די בכך. אכן, עבור $c\geq n$ קיימת פונקציה עם דרגה 1 (למשל, הפונקציה $f(k)=k$ לכל $k\in\{0,1,2,\ldots,n\}$), ולכן מקרים אלו אינם מעניינים כאשר באים לחקור חסם תחתון על הדרגה. מצד שני, לכל $c<n$, כל פונקציה לא-קבועה מהצורה $f:\{0,1,2,\ldots,n\}\to\{0,1,2,\ldots,c\}$ היא גם פונקציה לא-קבועה מהצורה $f:\{0,1,2,\ldots,n\}\to\{0,1,2,\ldots,n-1\}$, ולכן משפט 1 תקף לגביה.

משפט 1 מלמד אותנו, אם כך, על תופעת סף מעניינת: עבור $c\geq n$ קיימת פונקציה עם דרגה 1, ומאידך, עבור $c<n$ כל פונקציה לא קבועה היא מדרגה לינארית ב- n. אנו מייחסים את גילויה של תופעה זו לתוצאה המרכזית בתיזה.

שאלה טבעית היא האם החסם התחתון התקבל בעקבות העובדה שהטווח של הפונקציה מורכב ממספרים שלמים (בטווח חסום). תשובה זו נענית, חלקית, בשלילה על ידי התוצאה השנייה בתיזה.

משפט 2

תהא $C\subset\mathbb{Q}$ קבוצה סופית. תהא $f_n:\{0,1,2,\ldots,n\}\to C$ משפחה של פונקציות לא-קבועות. אז

$$\deg f_n \geq \frac{2}{3}n - O\left(n^{0.525}\right)$$

תקציר המחקר

בהינתן פונקציה בוליאנית $f:\{0,1,\ldots,n\}\to C$ עבור $C\subset\mathbb{R}$, ידוע כי קיים פולינום יחיד $h(x)$ ממעלה שאינה עולה על n, המבצע אינטרפולציה על f (דהיינו, $h(k)=f(k)$ לכל $k\in\{0,1,\ldots,n\}$). שאלה העולה באופן טבעי היא השאלה הבאה: אם נגביל את C, כמה נמוכה עלולה להיות הדרגה של פולינום אינטרפולציה עבור פונקציה לא-קבועה מהצורה $f:\{0,1,\ldots,n\}\to C$? (מכיוון שעבור פונקציה נתונה, פולינום האינטרפולציה הוא, כאמור, יחיד, אנו נזהה את הדרגה עם הפונקציה. כלומר, נדבר על הדרגה של הפונקציה, שנסמנה ב- $\deg f$). תשובה ראשונה לשאלה מסוג זה הוכחה ב-1997 עבור ההגבלה $C=\{0,1\}$, ראה [vzGR97]. במקרה זה הדרגה אינה יורדת מ- $n-O\left(n^{0.525}\right)$.

בתיזה זו נחקור שתי הכללות טבעיות לתוצאה זו. ההכללה הראשונה מתייחסת להגבלה $C=\{0,1,2,\ldots,c\}$ עבור $c\in\mathbb{N}$ (c יכול להיות תלוי ב- n). ההכללה השניה נוגעת למקרה בו $C\subset\mathbb{Q}$ אך C אינה תלויה ב- n. מקרים אלו נלמדו בעבר, ועבור שני המקרים אנו מספקים חסמים תחתונים אשר משפרים באופן משמעותי את הידוע. בנוסף, אנו מכלילים ומציעים הוכחה אלטרנטיבית, פשוטה יותר, לתוצאה הידועה עבור $C=\{0,1\}$.

המוטיבציה לשאלה זו מקורה בחקר פונקציות בוליאניות סימטריות מעל הקוביה הבוליאניות, דהיינו פונקציות מהצורה $f:\{0,1\}^n\to\{0,1\}$. בדומה לפונקציה בעלת משתנה אחד, ניתן לייצג כל פונקציה שכזו באופן טבעי על ידי פולינום בעל n משתנים מעל הממשיים. הבנה של ייצוג זה היא מטרה מרכזית במדעי המחשב. משפחה חשובה של פונקציות בוליאניות מעל הקוביה הבוליאנית היא משפחת הפונקציות הסימטריות. פונקציה נקראת סימטרית אם היא אינווריאנטית תחת כל תמורה של ערכי המשתנים (או במילים אחרות, הפונקציה תלויה רק במספר ה-1-ים שהיא מקבלת ולא במיקום שלהם). עובדה ידועה היא שחקר הדרגה של פונקציות בוליאניות סימטריות מעל הקוביה הבוליאנית ניתן לרדוקציה לחקר הדרגה של פונקציות מהצורה $f:\{0,1,\ldots,n\}\to\{0,1\}$.

עד לעבודה זו, החסם התחתון הטוב ביותר עבור הדרגה של פונקציה לא קבועה מהצורה $f:\{0,1,\ldots,n\}\to C$ היה $(n+1)/|C|$. אכן, מעיקרון מיצוע, קיים ערך המתקבל על ידי הפונקציה לפחות $(n+1)/|C|$ פעמים, ועובדה ידועה היא שפולינום שאינו קבוע המקבל d

המחקר נעשה בהנחיית פרופ׳/ח׳ אמיר שפילקה בפקולטה למדעי המחשב.

ברצוני להודות לאמיר על התמיכה וההנחייה המסורה, ועל שערך לי היכרות מעמיקה עם המחקר המדעי.

ברצוני להודות לאישתי אורית ולבני יהלי על האהבה, התמיכה וההתעניינות בעבודתי. עבודת מחקר זאת מוקדשת להם.

אני מודה לטכניון על התמיכה הכספית הנדיבה בהשתלמותי.

על הדרגה של פונקציה סימטרית על הקוביה הבוליאנית

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת התואר
מגיסטר למדעים במדעי המחשב

גיל כהן

הוגש לסנט הטכניון - מכון טכנולוגי לישראל

תמוז תש״ע חיפה יולי 2010

על הדרגה של פונקציה סימטרית על הקוביה הבוליאנית

גיל כהן