On the degree of symmetric functions on the Boolean cube

Gil Cohen [*]   Amir Shpilka [*]

March 1, 2010

Abstract

In this paper we study the degree of non-constant symmetric functions $f : \{0,1\}^n \to \{0,1,\ldots,c\}$, where $c \in \mathbb{N}$, when represented as polynomials over the real numbers. We show that as long as $c < n$ it holds that $\deg(f) = \Omega(n)$. As we can have $\deg(f) = 1$ when $c = n$, our result shows a surprising threshold phenomenon. The question of lower bounding the degree of symmetric functions on the Boolean cube was previously studied by von zur Gathen and Roche [GR97] who showed the lower bound $\deg(f) \geq \frac{n+1}{c+1}$ and so our result greatly improves this bound.

When $c = 1$, namely the function maps the Boolean cube to $\{0,1\}$, we show that if $n = p^2$, when p is a prime, then $\deg(f) \geq n - \sqrt{n}$. This slightly improves the previous bound of [GR97] for this case.

1 Introduction

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, GR97]. 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 tight as the so called address function demonstrates) [NS94]. This result immediately raises 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

---

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

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 [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 $x = x_1 + \ldots + x_n$. 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. In [GR97], von zur Gathen and Roche proved that the degree of such polynomials is $n - o(n)$. In their work von zur Gathen and Roche also raised the question of what can be said when the image of the polynomial has more than two values. Specifically, what can be said about the degree of non-constant polynomials $f : \{0, 1, \ldots, n\} \to \{0, 1, \ldots, c\}$, where $c \in \mathbb{N}$. Going back to the Boolean cube this question concerns symmetric functions from the cube to the integers that take more than two values. Note that when $c = n$ the function $f(x) = x$ has degree 1 and so it is an interesting question to better understand the tradeoff between the size of the range c and the degree of the function f. Von zur Gathen and Roche showed that the degree of any such function is at least $(n + 1)/(c + 1)$ [GR97]. This lower bound follows from the pigeonhole principle; such a function must assume one of its $c + 1$ values on at least $(n + 1)/(c + 1)$ points, while polynomial of degree d cannot obtain the same value on more than d points. In particular, when $c > n/2$ this result does not exclude the possibility that there is a quadratic polynomial mapping $\{0, 1, \ldots, n\}$ to $\{0, 1, \ldots, c\}$. Indeed, von zur Gathen and Roche also asked whether stronger bounds can be proved.

In this work we study this question and show what we find to be an interesting threshold phenomenon. Specifically, we prove that the degree of any non-constant function $f : \{0, 1, \ldots, n\} \to \{0, 1, \ldots, c\}$, where $c < n$ is any positive integer, is $\Omega(n)$. Thus if $c = n - 1$ the degree has to be linear in n and when $c = n$ the degree can be as low as 1. Stating this result differently, we see that low degree polynomials cannot 'squeeze' the set $\{0, 1, \ldots, n\}$ into $\{0, 1, \ldots, n - 1\}$.

1.1 Our Results and techniques

As mentioned above, we give a lower bound for $c = n - 1$ (and therefore for all $c < n$) and by that prove a sharp threshold behavior at $c = n$.

Theorem 1 (Main Theorem). *Let f be a non-constant function of the form $f : \{0, 1, \ldots, n\} \to \{0, 1, \ldots, n - 1\}$. Then $\deg f \geq \frac{9}{22}n - O(n^{0.525})$.*

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

Definition 1. *Let $c \in \mathbb{N}$. We call a non-constant function of the form $f : \{0, 1, \ldots, n\} \to \{0, 1, \ldots, c\}$ an (n, c)-function. We denote by $\mathcal{F}_c(n)$ the set of all (n, c)-functions. Denote $\mathcal{D}_c(n) = \frac{1}{n} \min_{f \in \mathcal{F}_c(n)} \deg f$. We call $\mathcal{D}_c(n)$ the relative degree of (n, c)-functions.*

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 all odd n's greater than 1, while it was proved in [GR97] 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 $1 \leq c < n$. [GR97] 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 $\mathcal{D}_{n-1}(n) \geq \frac{9}{22} - o(1)$.

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. This is expressed in the following lemma.

Lemma 1 (Reduction to $c = 4$)**.** *For any n there exists a prime p such that $n - O(n^{0.525}) < 2p < n$ and $\mathcal{D}_{n-1}(n) \geq \frac{1}{2}\mathcal{D}_4(p) - o(1)$.*

This step together with the trivial lower bound $\mathcal{D}_4(n) > \frac{1}{5}$ already gives a lower bound of $\frac{1}{10} - o(1)$ for $\mathcal{D}_{n-1}(n)$, which is enough to prove the desired threshold behavior. In order to prove a better lower bound we show another reduction. This time the reduction is on n and not on c.

Lemma 2 (Reducing n)**.** *For every $c, m, n \in \mathbb{N} \setminus \{0\}$ such that $n > 2^m c$, it holds that $\mathcal{D}_c(n) \geq \frac{m}{m+1}\mathcal{D}_c(m) - o(1)$.*

Although we've mentioned that $\mathcal{D}_c(n)$ is not monotone in n, Lemma 2 shows that some relaxed property of monotonicity does hold - given a large m, for large enough n's we almost have that $\mathcal{D}_c(n) > \mathcal{D}_c(m)$. Besides this insight, Lemma 2 gives us a way of proving lower bounds on $\mathcal{D}_c(n)$ using a computer search. Indeed, running a computer search we found that $\mathcal{D}_4(21) = \frac{6}{7}$. This result together with Lemma 1 and Lemma 2 yields Theorem 1.

As one cannot prove lower bounds on $\mathcal{D}_{n-1}(n)$ that are better than $\frac{1}{2}$ using Lemma 1, we consider the case $c < n - 1$ and ask for better lower bounds on $\mathcal{D}_c(n)$. When c is very small one can run a computer search and use Lemma 2 to get:

Corollary 1. *For any n it holds that: $\mathcal{D}_2(n) > \frac{8}{9} - o(1)$, $\mathcal{D}_3(n) > \frac{6}{7} - o(1)$, $\mathcal{D}_4(n) > \frac{9}{11} - o(1)$ and $\mathcal{D}_5(n) > \frac{13}{18} - o(1)$.*

A more general result is the next theorem. It gives a lower bound, better than that of Theorem 1, for c's that are still quite large.

Theorem 2. *If $c < \frac{2}{3}n - \Omega\left(n^{0.525}\right)$ then $\mathcal{D}_c(n) > \frac{2}{3} - o(1)$.*

Next, we give a very simple though interesting corollary that can be deduced from Theorem 2.

Corollary 2. *Let C be a finite fixed subset of $\mathbb{Q}$ and let $f : \{0, 1, \ldots, n\} \to C$ be a non-constant function. Then $\deg f \geq \frac{2}{3}n - o(1)$.*

Besides the result for large values of c we also study the case of $c = 1$. Namely, symmetric Boolean functions. For such a function f von zur Gathen and Roche proved that $\deg(f) \geq n - O(n^{0.525})$. 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 [GR97] (achieved by taking $m = 1$).

3

Theorem 3. *Let $n = p^m - 1$ for a prime p. Let f be a non-constant symmetric Boolean function on n variables. Then $\deg f \geq n - n^{1-1/m}$.*

Note that the above theorem slightly improves the result of [GR97] 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.

1.2 Organization

The paper is organized as follows. In Section 2 we develop some tools that will be used in the rest of the paper. In Section 3 we prove Lemma 1. In Section 4 we prove Lemma 2 and deduce Theorem 1 and Corollary 1. In Section 5 we prove Theorem 2 and Corollary 2. Finally, we prove Theorem 3 in Section 6.

1.3 Some notations

Given $f \in \mathcal{F}_c(n)$ we denote with $h_f(x)$ the unique univariate polynomial of degree $\leq n$ that agrees with f on the points in the set $\{0, 1, \ldots, n\}$. We define the *degree* of f to be $\deg h_f$ and denote it by $\deg f$.

We write $a \equiv_p b$ as a shorthand for $a \equiv b \mod p$. Given an integer a we shall say that its base b representation is $a = \langle\, a_s \quad a_{s-1} \quad \ldots \quad a_0 \,\rangle_b$, when $a = a_s b^s + a_{s-1}b^{s-1} + \cdots + a_1 b + a_0$. This representation is unique under the assumption that $a_s \neq 0$, that is up to leading zeros.

2 Periodicity and degree

The strategy we take for proving lower bounds on the degree of functions is basically as follows: we prove that a function having low degree must have a strong periodical structure (in a sense we will formally define). Then we show that a function having a strong periodical structure must be of high degree. Hence a function with a 'too low' degree cannot exist. In this section we prove two lemmas, which formally capture this idea.

2.1 Low degree implies strong periodical structure

The following lemma shows that a low degree function must have some periodical structure.

Lemma 3. *Let $f \in \mathcal{F}_c(n)$ be a function with $\deg f = d$. Let $d < p \leq n$ be a prime number. Then for all $0 \leq j \leq d$ such that $p + j \leq n$ it holds that $f(p + j) \equiv_p f(j)$.*

In order to prove Lemma 3 we will use the following two known facts.

Fact 1. *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 and $\binom{x}{k}$ is defined to be the polynomial $\binom{x}{k} = \frac{x(x-1)\cdot\ldots\cdot(x-k+1)}{k!}$.*

The second fact is Lucas' theorem from 1878. For completeness we give simple proofs of these facts in Appendix A.

Fact 2 (Lucas' theorem)**.** *Let $a, b \in \mathbb{N} \setminus \{0\}$ and let p be a prime number. Denote with $a = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$ and $b = b_0 + b_1 p + b_2 p^2 + \cdots + b_k p^k$ 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 $a_i < b_i$.*

We are now ready to prove Lemma 3.

Proof of Lemma 3. By Fact 1 we can write

$$h_f(p + j) = \sum_{k=0}^{d} c_k \binom{p + j}{k} \tag{1}$$

where all c_k's are integers. Applying Lucas' theorem while remembering that $j, k < p$ we get

$$\binom{p + j}{k} = \binom{\langle 1 \quad j \rangle_p}{\langle 0 \quad k \rangle_p} \equiv_p \binom{1}{0}\binom{j}{k} = \binom{j}{k} . \tag{2}$$

Combining (1), (2) and the assumption that $p + j \leq n$ we obtain

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

$\square$

2.2 Strong periodical structure implies high degree

The next definition is a formalization of what we have earlier referred to as a 'strong periodical structure'.

Definition 2. *Given a function $f \in \mathcal{F}_c(n)$ and $T, \Delta \in \mathbb{N}$ such that $T \geq 1$ we define $P_T^\Delta(f) = \{0 \leq k \leq n - T \colon f(k) + \Delta = f(k + T)\}$.*

In words, $P_T^\Delta(f)$ is the number of elements less or equal than $n - T$ on which f behaves as it has period T (with a shift of Δ). With this definition in mind we are ready to prove that a function having a strong periodical structure, has a high degree.

Lemma 4. *Let $f \in \mathcal{F}_c(n)$, then for all $T, \Delta \in \mathbb{N}$ such that $T \geq 1$ it holds that*

1. If $\Delta = 0$ then $\deg f \geq \left| P_T^\Delta(f) \right|$.

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

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 $\deg g = \deg h_f = d$. Hence, 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 have at least $\left|P_T^\Delta(f)\right|$ agreements. 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,

$$
\begin{aligned}
\sum_{k=0}^{d} a_k x^k + \Delta = h_f(x) + \Delta = g(x) + \Delta = h_f(x+T) &= \sum_{k=0}^{d} a_k (x+T)^k \\
&= \sum_{k=0}^{d} a_k \sum_{j=0}^{k} \binom{k}{j} x^j T^{k-j} = \sum_{m=0}^{d} x^m \sum_{k=m}^{d} \binom{k}{m} a_k T^{k-m} .
\end{aligned}
\tag{3}
$$

Thus, the coefficients of the LHS equal the coefficients of the RHS.

Assume now that $\Delta = 0$. In this case our initial assumption that $d < \left|P_T^\Delta\right|$ leads to a contradiction. Indeed, Equation (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 $\sum_{k=m+1}^{d} \binom{k}{m} a_k T^{k-m} = 0$. Consequently, for $m = d-1$ we get $\binom{d}{d-1} a_d T = 0$. Since $T \geq 1$ and $d \neq 0$ (recall that $f \in \mathcal{F}_c(n)$ is non-constant) 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 $\deg f = 1$. 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)). 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 $d = 1$, and so we are done. $\qquad\square$

3   Reduction to $c = 4$

In this section we prove Lemma 1. We first cite a corollary of the result of Baker et al [BHP01] on the gap between two consecutive primes.

Theorem 4. *For any $n \in \mathbb{N}$ there exists a prime number p such that $n - O(n^{0.525}) < p < n$.*

We are now ready to prove Lemma 1.

Proof of Lemma 1. 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 $\frac{n}{2} - O((\frac{n}{2})^{0.525}) < p < \frac{n}{2}$ guaranteed by Theorem 4. Clearly, $n - O(n^{0.525}) < 2p < n$. Let $\tilde{f}$ be the restriction of f to the domain $\{0, 1, \ldots, 2p\}$. 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 $g \colon \{0, 1, \ldots, p\} \to \mathbb{R}$ as follows: $g(k) = 2 + \frac{\tilde{f}(p+k) - \tilde{f}(k)}{p}$. It is obvious that $\deg g \leq \deg \tilde{f}$. To better understand g, note that Lemma 3 implies that for any $0 \leq k \leq p$ it holds that $\tilde{f}(p+k) \equiv_p \tilde{f}(k)$. Since for all $0 \leq j \leq 2p$ we have that $0 \leq \tilde{f}(j) < n < 3p$, it follows that $\tilde{f}(p+k) - \tilde{f}(k) \in \{-2p, -p, 0, p, 2p\}$. Consequently, g maps $\{0, 1, \ldots, p\}$ to $\{0, 1, 2, 3, 4\}$. In other words, g is a $(p, 4)$-function. If g is not a constant then

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

6

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 $0 \leq k \leq p$ we have that $\tilde{f}(p + k) = \tilde{f}(k) + (G - 2)p$ and therefore $|P_p^{(G-2)p}(\tilde{f})| > p$. By Lemma 4, either $\deg \tilde{f} \geq |P_p^{(G-2)p}(\tilde{f})| > p \geq \frac{n}{2} - o(n)$ 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 $f^R(k) = f(n - k)$. If by applying the proof on f^R we get that $\deg f^R \geq \frac{1}{2}\mathcal{D}_4(p) - o(1)$ 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 linear 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 $f \in \mathcal{F}_{n-1}(n)$. $\qquad\square$

We would like to point out that for the case $n = 2p + 1$, for a prime p, we can do slightly better. In such case g is actually a $(p, 2)$ function rather than a $(p, 4)$ function, as the difference $\tilde{f}(k + p) - \tilde{f}(k)$ is contained in $\{-p, 0, p\}$. Corollary 1 gives better lower bounds for $\mathcal{D}_2(n)$ than for $\mathcal{D}_4(n)$. This in turn yields the stronger result $\mathcal{D}_{n-1}(n) \geq \frac{4}{9} - o(1)$ for such n's.

4   Reducing n

In this section we prove Lemma 2 and deduce Theorem 1. To this end it is more convenient to talk about the *gap* of functions.

Definition 3. *Given* $f \in \mathcal{F}_c(n)$ *define* $\gamma(f) \stackrel{def}{=} n - \deg f$. *We call* $\gamma(f)$ *the* gap of **f**. *Let* $\Gamma_c(n) \stackrel{def}{=} \max_{f \in \mathcal{F}_c(n)} \gamma(f)$. *We call* $\Gamma_c(n)$ *the* gap of (n, c)-functions.

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

Theorem 5 (Theorem 2.2 from [GR97]). *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 2 we will also need to know, given $f \in \mathcal{F}_c(n)$, the value of $h_f(n + t)$ for $t \geq 1$.

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

ing $n + t$ for x we get

$$h_f(n + t) = \sum_{k=0}^{n} \left(\prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{n + t - j}{k - j} \right) f(k) = \sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!} \frac{(n+t)!}{(t-1)!(n+t-k)} f(k)$$

$$= (-1)^n \sum_{k=0}^{n} (-1)^k \frac{(n+t)!}{k!(n+t-k)!} \frac{(n+t-k-1)!}{(n-k)!(t-1)!} f(k)$$

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

$\square$

The following lemma is useful for the proof of Lemma 2.

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. $\square$

It easily follows from the relation between $\mathcal{D}_c(n)$ and $\Gamma_c(n)$ that Lemma 2 is equivalent to the following lemma.

Lemma 7. *For all $c, m, n \in \mathbb{N} - \{0\}$ such that $n > 2^m c$ it holds that $\Gamma_c(n) \leq \left(\frac{\Gamma_c(m)+1}{m+1} \right) n + o(n)$.*

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

Proof. If this inequality does not hold then there is a function $f \in \mathcal{F}_c((m+1)p - 1)$ such that $\deg f < (m-\gamma)p$, where $\gamma \stackrel{\text{def}}{=} \Gamma_c(m)$. 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 $f_j \in \mathcal{F}_c(m)$ 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 2 (with $\Delta = 0$) will yield a contradiction.

8

For every $0 \le r \le \gamma$ and for every $0 \le j \le p - 1$, the value of $h_f((m - r)p + j)$ is determined by the value of f on the points $\{0, 1, \ldots, (m-r)p-1\}$.[2] 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 $0 \le j \le p - 1$ 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 $k_0 \le j$. Assume that $k_0 < j$, that is $j - k_0 - 1 \ge 0$. Note that $(m - r)p + j - k - 1 = \langle m - r - k_1 \quad j - k_0 - 1 \rangle_p$. Consequently, for k to contribute to the sum modulo p, we must have $j - k_0 - 1 \ge j$. Hence $k_0 \le -1$, 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 $\mathbb{F}_p$

$$h_f((m - r)p + j) \equiv_p \tag{4}$$

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

By Lucas' Theorem

$$\binom{(m-r)p+j}{k_1 p + j} \equiv_p \binom{m - r}{k_1} \quad \text{and} \quad \binom{(m - r - k_1)p - 1}{j} \equiv_p \cdot \binom{p - 1}{j}$$

Now $j! \binom{p-1}{j} = (p - 1)(p - 2) \cdot \ldots \cdot (p - j) \equiv_p (-1)^j \cdot j!$ and since $j! \ne 0$ it follows that $\binom{p-1}{j} \equiv_p (-1)^j$. With this we can simplify equation (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 $0 \le j \le p-1$ and all $0 \le r \le \gamma$

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

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 5 we get that for every $0 \le j \le p - 1$, $\gamma(f_j) > \gamma = \Gamma_c(m)$. Hence all f_j's must be constant functions. This implies that f is a periodical function with period p. That is $|P_p^0(f)| = mp$. By Lemma 2 we get that $\deg f \ge mp$. Recalling the assumption $\deg f < (m - \gamma)p$, we get that $\gamma < 0$ in contradiction. □

---

[2]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 $h_f((m-r)p+j)$.

We are now ready to prove Lemma 7.

Proof of Lemma 7. Given n and m, we can apply Theorem 4 to assure the existence of a prime number p such that $n/(m+1)-O\left((n/(m+1))^{0.525}\right) \leq p < n/(m+1)$. Since $m = o(n)$, $n - o(n) \leq (m+1)p - 1 < n$. By Lemma 6

$$\Gamma_c(n) \leq \Gamma_c((m+1)p-1) + n - ((m+1)p-1) \leq \Gamma_c((m+1)p-1) + o(n) \qquad (5)$$

By Lemma 8

$$\Gamma_c((m+1)p-1) < p\left(\Gamma_c(m)+1\right) = (m+1)p\left(\frac{\Gamma_c(m)+1}{m+1}\right) \leq$$

$$n\left(\frac{\Gamma_c(m)+1}{m+1}\right) \qquad (6)$$

Inequalities (5) and (6) together imply that $\Gamma_c(n) \leq \left(\frac{\Gamma_c(m)+1}{m+1}\right)n + o(n)$ as desired. $\qquad \square$

Deducing Theorem 1 is straightforward at this point.

Proof of Theorem 1. A computer search found that $\mathcal{D}_4(21) = 6/7$. By Lemma 2 $\mathcal{D}_4(n) \geq \frac{21}{21+1} \cdot \frac{6}{7} - o(1) = \frac{9}{11} - o(1)$. Lemma 1 gives $\mathcal{D}_{n-1}(n) \geq \frac{1}{2} \cdot \mathcal{D}_4(p) - o(1) \geq \frac{1}{2} \cdot \frac{9}{11} - o(1) = \frac{9}{22} - o(1)$. $\qquad \square$

We end this section by deducing Corollary 1

Proof of Corollary 1. A computer search we have conducted found that $\mathcal{D}_2(35) = \frac{32}{35}$, $\mathcal{D}_3(27) = \frac{8}{9}$, $\mathcal{D}_4(21) = \frac{6}{7}$ and $\mathcal{D}_5(17) = \frac{13}{17}$. Using Lemma 2 we get $\mathcal{D}_2(n) \geq \frac{35}{36} \cdot \frac{32}{35} - o(1) = \frac{8}{9} - o(1)$, $\mathcal{D}_3(n) \geq \frac{27}{28} \cdot \frac{8}{9} - o(1) = \frac{6}{7} - o(1)$, $\mathcal{D}_4(n) \geq \frac{21}{22} \cdot \frac{6}{7} - o(1) = \frac{9}{11} - o(1)$ and $\mathcal{D}_5(n) \geq \frac{17}{18} \cdot \frac{13}{17} - o(1) = \frac{13}{18} - o(1)$. $\qquad \square$

5 Better upper bound for $c < \frac{2}{3}n$

Using the tools above it is quite straightforward to prove Theorem 2.

Proof of Theorem 2. By Theorem 4 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 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 $|P_T^0(f)| > 2(n-p) > \frac{2}{3}n$. By Lemma 2, $\deg f > \frac{2}{3}n$, contradicting our assumption that $\deg f < q < \frac{2}{3}n$. $\qquad \square$

We end this section by proving Corollary 2.

Proof of Corollary 2. Firstly note that we can assume that C contains only non-negative elements, possibly by shifting all elements of C by some Δ. Indeed, for any non-constant polynomial $\deg(h(x)) = \deg(\Delta + h(x))$.

Let us denote $C = \{\frac{a_1}{b_1}, \ldots, \frac{a_k}{b_k}\}$, where $k = |C|$ and all elements in 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 $\tilde{f}$. Therefore, $\deg f = \deg \tilde{f} \geq n - \Gamma_c(n)$. As l, m are constants so is c and thus, by applying Theorem 2, we get that $\deg f \geq \deg \tilde{f} \geq \frac{2}{3}n - o(n)$ as desired. $\square$

In fact one can deduce lower bounds on the degree of functions whose image size is not necessarily constant. For example, consider any non-constant function of the form $f \colon \{0, 1, \ldots, n\} \to \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots, \frac{1}{2^m}\}$, 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 Theorem 2 we again obtain that $\deg f = \deg \tilde{f} \geq \frac{2}{3}n - o(1)$.

6 Back to the Boolean case

In this section we prove Theorem 3 and give a simple alternative proof for the main result of [GR97].

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 $0 \leq j < p^{m-1}$

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

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 $\mathbb{F}_p$

$$-h_f(p^m - p^{m-1} + j) \equiv_p$$
$$\sum_{k_{m-1}=0}^{p-2} (-1)^{j + k_{m-1} p^{m-1}} \binom{p^m - p^{m-1} + j}{k_{m-1} p^{m-1} + j} \binom{p^m - (k_{m-1} + 1) p^{m-1} - 1}{j} \cdot \qquad (7)$$
$$\cdot f(k_{m-1} p^{m-1} + j)$$

11

From Lucas' theorem

$$\binom{p^m - p^{m-1} + j}{k_{m-1}p^{m-1} + j} \equiv_p \binom{p-1}{k_{m-1}} \equiv_p (-1)^{k_{m-1}} \tag{8}$$

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

$$\binom{p^m - (k_{m-1} + 1)p^{m-1} - 1}{j} \equiv_p (-1)^j . \tag{9}$$

Substituting (8) and (9) into (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 $0 \le j < p^{m-1}$

$$\sum_{k_{m-1}=0}^{p-1} f(k_{m-1}p^{m-1} + j) \equiv_p 0 . \tag{10}$$

Since f is a Boolean function, in order to satisfy Equation (10), it must be that for every $0 \le j < p^{m-1}$

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

Therefore, f is periodical with period p^{m-1} which yields that $\left| P_p^0(f) \right| \ge p^m - p^{m-1}$. Lemma 2 now implies that $\deg f \ge p^m - p^{m-1} \ge n - n^{1-\frac{1}{m}}$. □

We end this section by giving an alternative proof for the main result appears in [GR97].

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

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

12

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

$$\deg h_f^{(p)} \leq \deg(h_f) \leq p - 1 \tag{11}$$

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 (11) we get $\deg h_f = p - 1$. $\qquad\square$

7 Open questions

Although we proved that the degree of any $f \in \mathcal{F}_c(n)$ is $\Omega(n)$ (for $c < n$), the exact behavior of the degree is still not completely understood. For example, is it true that in such a case $\deg(f) = n - o(n)$, or is there an example of a polynomial $f : \{0, 1, \ldots, n\} \to \{0, 1, \ldots, n-1\}$ of degree at most $(1 - \epsilon)n$ for some $\epsilon > 0$? This question is interesting also for small values of c. For the case of Boolean functions, i.e. when $c = 1$, von zur Gathen and Roche conjectured that $\deg(f) = n - O(1)$. This problem is still open.

8 Acknowledgement

References

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

[BHP01] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes, ii. *Proceedings of the London Mathematical Society*, 83:532–562, 2001. 6

[Gop06] P. Gopalan. *Computing with Polynomials over Composites*. PhD thesis, Georgia Institute of Technology, August 2006. 1

[GR97] J. von zur Gathen and J. R. Roche. Polynomials with two values. *Combinatorica*, 17(3):345–362, 1997. 1, 2, 3, 4, 7, 11, 12

[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. 2

[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. 2

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

[NS94]   N. Nisan and M. Szegedy. On the degree of boolean functions as real polynomials. *Computational Complexity*, 4:301–313, 1994. 1

[Raz03] A. A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145–159, 2003. 2

[Ste03] D. Stefankovic. Fourier transforms in computer science. Master's thesis, University of Chicago, Department of Computer Science, 2003. 1

A Missing proofs

Proof of Fact 1. It is easy to see that 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 and so 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. □

Proof of Fact 2. Expanding $(1+x)^a$ we get

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

The coefficient of x^b on the LHS is $\binom{a}{b}$. Since there is a unique way to represent b in base p we have that the coefficient of x^b on the RHS is $\prod_{i=0}^{k} \binom{a_i}{b_i}$. □