



Torus polynomials: an algebraic approach to ACC lower bounds

Abhishek Bhrushundi*
Rutgers University
abhishek.bhr@rutgers.edu

Kaave Hosseini†
University of California, San Diego
skhossei@ucsd.edu

Shachar Lovett‡
University of California, San Diego
slovett@ucsd.edu

Sankeerth Rao§
University of California, San Diego
skaringu@ucsd.edu

November 13, 2018

Abstract

We propose an algebraic approach to proving circuit lower bounds for ACC^0 by defining and studying the notion of *torus polynomials*. We show how currently known polynomial-based approximation results for AC^0 and ACC^0 can be reformulated in this framework, implying that ACC^0 can be approximated by low-degree torus polynomials. Furthermore, as a step towards proving ACC^0 lower bounds for the majority function via our approach, we show that MAJORITY cannot be approximated by low-degree *symmetric* torus polynomials. We also pose several open problems related to our framework.

1 Introduction

A major goal of complexity theory is to prove Boolean circuit lower bounds, i.e. find explicit Boolean functions that cannot be computed by small size circuits of a given type. Over the years, three general approaches have been developed to achieve this.

The first approach is based on random restrictions. It applies to circuit classes in which functions simplify when most inputs are fixed to random values. Classic examples are the proofs by Håstad that AC^0 , i.e. polynomial size circuit families of constant depth consisting of AND, OR, and NOT gates, cannot compute or approximate the PARITY function [Hås87], and the shrinkage of De Morgan formulas (Boolean circuits consisting of AND, OR, and NOT gates whose underlying graph is a tree) under random restrictions [Hås98]. However, random restrictions don't seem to be useful against more powerful circuit classes such as $\text{AC}^0[\oplus]$ — the class of AC^0 circuits equipped with PARITY gates.

The second approach is based on approximation by low-degree polynomials. Razborov [Raz87] and Smolensky [Smo87] used this approach to prove lower bounds for $\text{AC}^0[\oplus] = \text{AC}^0[2]$, and more generally for $\text{AC}^0[p]$ for any prime p (This is the class of AC^0 circuits that are allowed to have MOD_p gates¹). This technique is based on showing that any function in the circuit class

*Part of this work was done when the author was visiting the University of California, San Diego. Research supported in part by Rutgers AAUP-AFT TA-GA Professional Development Fund, and by NSF grant CCF-1614023.

†Supported by NSF grant CCF-1614023.

‡Supported by NSF grant CCF-1614023.

§Supported by NSF grant CCF-1614023.

¹a MOD_p gate outputs 1 if and only if the sum of its inputs is congruent to a non-zero value modulo p .

can be approximated by a low-degree polynomial over the finite field \mathbb{F}_p . Then, functions that do not admit such an approximation are provably outside the circuit class. A classic example here is that the MAJORITY function cannot be approximated by a low-degree polynomial over \mathbb{F}_p , and thus cannot be computed by $AC^0[p]$. However, this method also breaks down when considering more powerful circuit classes such as $AC^0[6]$, and more generally ACC^0 , i.e. AC^0 circuits with MOD_m gates where m is a composite that is not a prime power.

The third method involves designing nontrivial satisfiability algorithms and then using them along with classical tools from structural complexity theory (among other techniques and results) to prove circuit lower bounds against ACC^0 for functions in high complexity classes such as NEXP. Williams [Wil14] used this approach to prove that $NEXP \not\subseteq ACC^0$, and very recently, Williams and Murray [MW18] have extended this to show that $NQP \not\subseteq ACC^0$.

The goal of this paper is to focus on the second approach, namely the use of algebraic techniques, and to try and extend these techniques to prove lower bounds against ACC^0 . We show that an extension of finite field polynomials, which we call *torus polynomials*, is a concrete candidate to achieve this. In particular, using a slightly stronger version of a result of Green et al. [GKT92], we show that functions in ACC^0 can be approximated² by low-degree torus polynomials. We remark that torus polynomials also generalize the class of *nonclassical polynomials* which arose in number theory and in higher order Fourier analysis [TZ12], and are closely related to them.

This new characterization of ACC^0 using torus polynomials raises a host of questions on the approximation of Boolean functions by torus polynomials, the most remarkable being the problem of finding an explicit Boolean function that cannot be approximated by low-degree torus polynomials; an answer to this question would imply ACC^0 lower bounds. In this paper, we take steps towards trying to resolve this question by initiating the study of approximation of Boolean functions by torus polynomials and proving some interesting results along the way. The motivation for our work is two-fold:

1. Given the slew of recent works exploring properties and applications of nonclassical polynomials [Tao08, TZ12, BFH⁺13, BL15, BHS17], and the fact that torus polynomials are closely related to nonclassical polynomials, we believe that our characterization of ACC^0 using torus polynomials might pave a way for new ACC^0 lower bounds.
2. While the works of Williams [Wil14] and Williams and Murray [MW18] are groundbreaking and prove nontrivial lower bounds against ACC^0 , their proofs are not purely combinatorial/algebraic, and it will be interesting to recover their results using purely algebraic/combinatorial techniques. We hope that our work will renew interest in this line of inquiry.

1.1 Torus polynomials

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ denote the one-dimensional torus. A *torus polynomial* is simply a real polynomial restricted to the domain $\{0, 1\}^n$ and evaluated modulo one³. Namely, a degree- d torus polynomial $P : \{0, 1\}^n \rightarrow \mathbb{T}$ is

$$P(x) = \sum_{S \subseteq [n], |S| \leq d} P_S \prod_{i \in S} x_i \pmod{1},$$

where $P_S \in \mathbb{R}$.

As it shall become evident later, torus polynomials extend finite field polynomials in that they provide a uniform way to capture computation of Boolean functions by polynomials over

²The notion of approximation that we use will be made explicit in Section 1.1.

³For $x \in \mathbb{R}$, x modulo one, denoted by $x \bmod 1$, is equal to the fractional part of x given by $x - \lfloor x \rfloor$, where $\lfloor x \rfloor$ is the floor function. For example, $2.6 \bmod 1$ is 0.6, and $-1.3 \bmod 1$ is 0.7.

different finite fields — if a function can be computed by a low-degree polynomial over a finite field then it can be approximated by a low-degree torus polynomial. We will discuss this in detail in Section 2.

For $z \in \mathbb{T}$, let $\iota(z)$ denote the unique representative of z in $[-1/2, 1/2)$ (e.g., $\iota(0.4) = 0.4$ and $\iota(0.7) = -0.3$). Then we can define its norm, denoted by $|z \pmod{1}|$, to be

$$|z \pmod{1}| = |\iota(z)|.$$

For $F : \{0, 1\}^n \rightarrow \mathbb{T}$, define

$$\|F \pmod{1}\|_\infty := \max_{x \in \{0, 1\}^n} |F(x) \pmod{1}|.$$

We embed Boolean functions as functions mapping into the torus by enforcing their output to be in $\{0, 1/2\} \subset \mathbb{T}$ (This can be achieved by scaling the output of the function by $1/2$). The following is the main definition of approximation that we consider:

Definition 1.1. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function. For $\varepsilon > 0$, a torus polynomial $P : \{0, 1\}^n \rightarrow \mathbb{T}$ is said to ε -approximate f if*

$$\left\| P - \frac{f}{2} \pmod{1} \right\|_\infty \leq \varepsilon.$$

Intuitively, a torus polynomial that approximates f takes a value “close” to 0 in the torus \mathbb{T} whenever f takes the value 0, and takes a value “close” to $1/2$ in the torus whenever f takes the value 1.

We now introduce the notion of the *toroidal approximation degree* of a Boolean function.

Definition 1.2 (Toroidal approximation degree of Boolean functions). *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function. For $\varepsilon > 0$, the toroidal ε -approximation degree of f is the minimal $d \geq 0$, for which there exists a torus polynomial $P : \{0, 1\}^n \rightarrow \mathbb{T}$ of degree d , that satisfies*

$$\left\| P - \frac{f}{2} \pmod{1} \right\|_\infty \leq \varepsilon.$$

We denote this by $\overline{\text{deg}}_\varepsilon(f) = d$.

We illustrate in Section 2, in increasing generality, the power of torus polynomials. The most general result (Corollary 2.11) shows that if f can be computed by an ACC^0 circuit then

$$\overline{\text{deg}}_\varepsilon(f) \leq \text{polylog}(n/\varepsilon).$$

The proof of this result uses a slightly stronger version of a result of Green et al. [GKT92].

The above characterization paves way for a new approach to proving lower bounds against ACC^0 for an explicit function, ideally in the class P . Concretely, we pose the following open problem.

Problem 1.3. *Find an explicit function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ in P whose toroidal ε -approximation degree is $\omega(\text{polylog}(n/\varepsilon))$. By Corollary 2.11, it cannot be computed by ACC^0 circuits.*

Williams [Wil14] proved that $\text{NEXP} \not\subseteq \text{ACC}^0$ via designing nontrivial satisfiability algorithms for ACC^0 , and Williams and Murray [MW18] improved the approach to show that $\text{NQP} \not\subseteq \text{ACC}^0$. Thus, an intermediate goal towards resolving Problem 1.3 is to prove toroidal approximation lower bounds for functions $f \in \text{NEXP}$ or $f \in \text{NQP}$.

A long-standing open problem in circuit complexity is to show that MAJORITY cannot be computed in ACC^0 . Thus the following question is natural.

Problem 1.4. *What is the toroidal ε -approximation degree of MAJORITY?*

How can one go about answering this question? We now turn to the setting of approximation of Boolean functions by real polynomials – which *prima facie* shares some similarities with our setting – for inspiration, highlighting the main differences between the two notions.

1.2 Comparison with real polynomials

Given a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, the real ε -approximation degree of f , denoted by $\widetilde{\text{deg}}_\varepsilon(f)$, is the minimal d such that there is a real polynomial P of degree d such that $\|f - P\|_\infty \leq \varepsilon$ (this is the ℓ_∞ -norm restricted to the domain $\{0, 1\}^n$). It is clear that $\overline{\text{deg}}_\varepsilon(f) \leq \widetilde{\text{deg}}_\varepsilon(f)$.

A beautiful result of Nisan and Szegedy [NS92] shows that the real ε -approximation degree of MAJORITY is $\Omega(\sqrt{n})$ for $\varepsilon < 1/2$. Their proof proceeds in two stages: (i) showing that if a *symmetric* real polynomial ε -approximates MAJORITY then it must have degree $\Omega(\sqrt{n})$; and (ii) that any polynomial that ε -approximates MAJORITY can be *symmetrized* and made into a symmetric polynomial with the same degree and approximation guarantee.

Attempting to follow the same strategy in the case of torus polynomials, we show in Corollary 3.3 in Section 3 that if one restricts attention to *symmetric* torus polynomials (namely, symmetric real polynomials evaluated modulo one), then the toroidal $(1/20n)$ -approximation degree of MAJORITY is $\Omega(\sqrt{n/\log n})$.

Unfortunately, the aforementioned idea of symmetrization cannot be used in the setting of torus polynomials in a straightforward manner and so it's unclear how powerful non-symmetric torus polynomials are compared to their symmetric counterparts. We conjecture that they are not any better at approximating MAJORITY than symmetric torus polynomials:

Conjecture 1.5. *The toroidal $(1/20n)$ -approximation degree of MAJORITY is $\Omega(\sqrt{n/\log n})$.*

We remark that a positive answer to the above conjecture will give an algebraic proof that MAJORITY is not in ACC^0 .

Let $\Delta_w : \{0, 1\}^n \rightarrow \{0, 1\}$ denote the delta function which takes the value 1 on inputs of Hamming weight w and is 0 elsewhere. En route to proving the aforementioned lower bound for MAJORITY we also prove lower bounds for the delta functions in Lemma 3.1, showing that one needs symmetric torus polynomials of degree $\Omega(\sqrt{n/\log n})$ in order to be able to $(1/20n)$ -approximate the delta functions.

Somewhat surprisingly, for relatively large values of ε , the delta functions can be nontrivially ε -approximated by low-degree *symmetric* torus polynomials. In particular, we show in Lemma 4.1 in Section 4 that for every delta function there is a symmetric torus polynomial of degree $\text{polylog}(n/\varepsilon)/\varepsilon$ that ε -approximates it, and thus

$$\overline{\text{deg}}_\varepsilon(\Delta_w) \leq \frac{\text{polylog}(n/\varepsilon)}{\varepsilon}.$$

This kind of dependence of the toroidal approximation degree on ε is quite interesting, and is unlike the case of real approximation — the real approximation degree of the delta functions is $\Omega(\sqrt{n})$ for both small and large values of ε . In fact, for constant ε , this also shows a super-polynomial separation between real and toroidal approximation degree.

This also highlights other major differences between the real and the toroidal setting. Nisan and Szegedy [NS92] show that for every Boolean function the real approximation degree is polynomially related to the degree of exact representation by real polynomials. However, in the case of torus polynomials, this is not true: the delta functions require the degree to be $\Omega(n)^4$ for exact representation whereas their toroidal $1/3$ -approximation degree is $O(\text{polylog}(n))$.

⁴To see this, note that the delta function $\Delta_n(x)$ has a unique representation as a torus polynomial given by $\Delta_n(x) = \frac{x_1 \cdots x_n}{2}$.

An interesting property of real approximation is its amenability to amplification, namely the fact that, for any Boolean function f and $\varepsilon < 1/3$, given a polynomial p of degree d that $1/3$ -approximates f , it can be transformed into a polynomial p' of degree $d' = O(d \log(1/\varepsilon))$ that ε -approximates f . In other words, $\widetilde{\deg}_\varepsilon(f) \leq O(\widetilde{\deg}_{1/3}(f) \log(1/\varepsilon))$. It is not clear whether such a transformation is possible in the case of toroidal approximation. In the case of real approximation, the transformation is symmetry preserving, but, given the results for the delta functions discussed in the previous paragraphs, we should not expect this in the toroidal case. This motivates the following problem.

Problem 1.6. *How is $\overline{\deg}_\varepsilon(f)$ related to $\overline{\deg}_{1/3}(f)$?*

1.3 Comparison with nonclassical polynomials

As mentioned before, torus polynomials generalize the class of nonclassical polynomials (this will be evident from the definition of nonclassical polynomials stated below). We remark that the results of this paper can be similarly phrased in terms of nonclassical polynomials instead of torus polynomials. This is because for the purpose of approximation of Boolean functions – which is the topic of this paper – torus polynomials and nonclassical polynomials are equivalent, as we shall see below. However, torus polynomials are simpler to describe (they are just real polynomials evaluated modulo 1) and more elegant (they are field independent), and hence we believe are a better choice for an algebraic model and for stating our results.

We now give the definition of nonclassical polynomials; here we provide what is known as the global definition of nonclassical polynomials over $\{0, 1\}^n$. For simplicity, we restrict our attention to nonclassical polynomials defined over \mathbb{F}_2^n , but note that the results generalize to nonclassical polynomials defined over \mathbb{F}_p^n for any constant prime p .

Definition 1.7 (Nonclassical polynomials). *A function $Q : \{0, 1\}^n \rightarrow \mathbb{T}$ is a nonclassical polynomial (over \mathbb{F}_2) of degree at most d if and only if it can be written as*

$$Q(x) = \alpha + \sum_{\emptyset \subset S \subseteq [n]; k \geq 0; 0 < |S| + k \leq d} \frac{c_{S,k}}{2^{k+1}} \prod_{i \in S} x_i \pmod{1}$$

where $c_{S,k} \in \{0, 1\}$ and $\alpha \in \mathbb{T}$.

The following simple claim shows that torus polynomials can be approximated by nonclassical polynomials.

Claim 1.8. *Let $P : \{0, 1\}^n \rightarrow \mathbb{T}$ be a torus polynomial of degree at most d and let $\varepsilon \in (0, 1)$. Then there exists a nonclassical polynomial Q of degree at most $O(d \log n + \log(1/\varepsilon))$ such that $\|P - Q \pmod{1}\|_\infty \leq \varepsilon$.*

Proof. Suppose $P(x) = \alpha + \sum_{\emptyset \subset S \subseteq [n], |S| \leq d} P_S \prod_{i \in S} x_i \pmod{1}$. We can assume without loss of generality that $P_S \in [0, 1)$ for all S . We approximate each P_S separately using dyadic rationals. Let $P_S = 0.c_{S,0}c_{S,1}c_{S,2}\dots$, where $c_{S,i} \in \{0, 1\}$, be its binary expansion. Let $t \geq 1$ be a parameter that we will fix later, and note that

$$\left| P_S - \sum_{0 \leq k \leq t} \frac{c_{S,k}}{2^{k+1}} \right| \leq 2^{-t}.$$

Define the nonclassical polynomial

$$Q(x) = \alpha + \sum_{\emptyset \subset S \subseteq [n]; k \geq 0; 0 < |S| + k \leq t + d} \frac{c'_{S,k}}{2^{k+1}} \prod_{i \in S} x_i \pmod{1},$$

where $c'_{S,k} = c_{S,k}$ for $|S| \leq d, k \leq t$, and is 0 otherwise. Then $\deg(Q) \leq t + d$, and

$$|P(x) - Q(x) \pmod{1}| \leq \binom{n}{\leq d} 2^{-t}$$

for all $x \in \{0, 1\}^n$. Setting $t = O(d \log n + \log(1/\varepsilon))$ completes the proof. \square

Recall that our goal, motivated by proving ACC^0 lower bounds, is to find a Boolean function which cannot be $1/\text{poly}(n)$ -approximated by a torus polynomial of degree $\text{polylog}(n)$. Given Claim 1.8, this is equivalent to the problem of finding a Boolean function which cannot be $1/\text{poly}(n)$ -approximated by a nonclassical polynomial of degree $\text{polylog}(n)$. As we mentioned before, owing to the elegance and ease of description of torus polynomials relative to nonclassical polynomials, torus polynomials make for a more convenient choice in our setting.

1.4 Comparison with other notions of approximation

It's clear from our discussion in the previous section that torus polynomials are closely related to nonclassical polynomials, and so it's worthwhile to discuss two notions of approximation of Boolean functions by nonclassical polynomials that have been studied in the literature. The first deals with the *exact* computation of a Boolean function by a nonclassical polynomial on a nontrivial fraction of the domain [BL15]. For example, the work of Bhrushundi et al. [BHS17] shows that any polynomial that computes MAJORITY correctly even on two-thirds of the points must have degree $\Omega(\sqrt{n})$. While many of these bounds for nonclassical polynomials should also hold for torus polynomials, we remark that they are not relevant to our setting since our notion of approximation (i.e., point-wise) is incomparable to the above notion.

The second notion is that of correlation with polynomials, which was studied, for example, by Bhowmick and Lovett [BL15]. Without getting into definitions here, we note that this notion of approximation is *weaker* than that of point-wise approximation⁵, and thus for the purpose of proving lower bounds for ACC^0 it makes sense to work with only the latter. This also means that the upper bound results proved in the work of Bhowmick and Lovett (i.e., showing how certain Boolean functions can be approximated by low-degree nonclassical polynomials in the correlation sense) don't have any implications for our setting. Even their lower bound results, unfortunately, are not useful for us given that they only work for polynomials of degree $\ll \log(n)$, whereas we are dealing with polynomials of degree $\text{polylog}(n)$.

1.5 Natural proofs

The natural proofs barrier of Razborov and Rudich [RR97] isn't really a problem for our approach since we are only trying to prove lower bounds against ACC^0 and pseudorandom generators are not believed to be contained in this class. It is also not clear whether the property in question, i.e. (in)approximability by torus polynomials, is *natural*, and, in particular, it will be interesting to investigate whether one can efficiently distinguish between Boolean functions which can be approximated by low-degree torus polynomials and a random Boolean function, i.e. whether this property is *constructive*:

Problem 1.9. *Given the truth table of a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ and $\varepsilon > 0$, decide in polynomial time (in 2^n and $1/\varepsilon$) whether $\deg_\varepsilon(f) \leq \text{polylog}(n/\varepsilon)$.*

⁵By this we mean that if a function is point-wise approximated by a low-degree torus polynomial then it is also approximated by that polynomial in the correlation sense.

Paper organization. In Section 2, we prove toroidal approximation results for Boolean functions in bounded circuit classes such as $AC^0[p]$ and ACC^0 . In Section 3, we prove lower bounds against symmetric torus polynomials approximating the MAJORITY function and the delta functions. In Section 4, we show that symmetric torus polynomials have surprising power in approximating the delta functions when the error ε is not too small. We introduce definitions and notation along the way, as and when needed.

2 Approximation of circuit classes

In this section, we illustrate how the framework of approximation by torus polynomials captures computation of Boolean functions in various models of computation. We begin by showing that functions that are computable by low-degree polynomials over finite fields can be approximated by low-degree torus polynomials.

It might be instructive to keep in mind that, for the scope of the entire paper, whenever we consider polynomials we restrict ourselves to only *multilinear* polynomials, i.e. polynomials in which the maximum degree of any variable is at most 1. Even if we encounter polynomials that do not adhere to this form during intermediate steps in certain proofs, we can always *multilinearize* the polynomials by making the degrees of all the variables equal to 1 wherever they appear. It suffices to consider multilinear polynomials because we always restrict the variables to the domain $\{0, 1\}$.

2.1 Polynomials over finite fields

Let \mathbb{F}_p be a prime finite field. We say a polynomial $P(x) \in \mathbb{F}_p[x_1, \dots, x_n]$ computes a Boolean function f if

$$\forall x \in \{0, 1\}^n, f(x) = P(x).$$

Consider a function f which is computed by a low-degree polynomial over \mathbb{F}_p . We will now show that it can be approximated by a low-degree torus polynomial. We would require the following theorem on modulus-amplifying polynomials of Beigel and Tarui [BT91], following previous results of Toda [Tod91] and Yao [Yao85].

Lemma 2.1 (Beigel and Tarui [BT91]). *For every $k \geq 1$, there exists a univariate polynomial $A_k : \mathbb{Z} \rightarrow \mathbb{Z}$ of degree $2k - 1$ such that the following holds. For every $m \geq 2$,*

- *If $x \in \mathbb{Z}$ satisfies $x \equiv 0 \pmod{m}$ then $A_k(x) \equiv 0 \pmod{m^k}$.*
- *If $x \in \mathbb{Z}$ satisfies $x \equiv 1 \pmod{m}$ then $A_k(x) \equiv 1 \pmod{m^k}$.*

Lemma 2.2. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Assume that f can be computed by a polynomial over \mathbb{F}_p of degree d . Then for every $\varepsilon > 0$,*

$$\overline{\deg}_\varepsilon(f) \leq O(d \log(1/\varepsilon)).$$

Proof. Since f is computable by degree- d polynomials over \mathbb{F}_p , there must be an integer polynomial $F(x)$ (i.e., a polynomial with coefficients in \mathbb{Z}) of degree d such that

$$F(x) \equiv f(x) \pmod{p} \quad \forall x \in \{0, 1\}^n.$$

Let $k \geq 1$ be large enough so that $1/p^k \leq \varepsilon$. Let $0 \leq q \leq p^k - 1$ be such that

$$\left| \frac{q}{p^k} - \frac{1}{2} \pmod{1} \right| \leq \varepsilon.$$

Define

$$G(x) = \frac{qA_k(F(x))}{p^k} \pmod{1}.$$

We claim that

$$\left| G(x) - \frac{f(x)}{2} \pmod{1} \right| \leq \varepsilon \quad (1)$$

for all x . To see this, fix x , and recall that $F(x) \equiv f(x) \pmod{p}$, which means that $A_k(F(x)) \equiv f(x) \pmod{p^k}$, and hence $G(x) \equiv \frac{q}{p^k} f(x) \pmod{1}$. (1) now follows from our choice of q .

Noting that the degree of G is $(2k-1)d \leq O(d \log(1/\varepsilon))$ completes the proof. \square

We will later need the following simple variant of Lemma 2.2. Its proof is identical.

Lemma 2.3. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Assume that f can be computed by a polynomial over \mathbb{F}_p of degree d . Then for every $\alpha \in [0, 1]$ and every $\varepsilon > 0$, there exists a torus polynomial $P : \{0, 1\}^n \rightarrow \mathbb{T}$ of degree $O(d \log(1/\varepsilon))$ such that*

$$\|P - \alpha f \pmod{1}\|_\infty \leq \varepsilon.$$

2.2 Circuit class $AC^0[p]$

Recall that, for a fixed prime p , $AC^0[p]$ is the class of functions computable by polynomial size circuits of constant depth, consisting of AND, OR, NOT, and MOD_p gates. Here a MOD_p gate is one that outputs 1 if and only if the sum of its inputs is congruent to a non-zero value modulo p .

Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a function in $AC^0[p]$. We show that it can also be approximated by low-degree torus polynomials. The starting point is the classic result of Razborov [Raz87] and Smolensky [Smo87] which shows that $AC^0[p]$ circuits can be approximated by random low-degree polynomials over \mathbb{F}_p in the following sense.

Theorem 2.4 (Razborov-Smolensky [Raz87, Smo87]). *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be computed by an $AC^0[p]$ circuit. Then for every $\varepsilon > 0$, there exists a distribution ν supported on polynomials $F : \mathbb{F}_p^n \rightarrow \{0, 1\}$ of degree $d = \text{polylog}(n/\varepsilon)$ such that*

$$\Pr_{P \sim \nu} [P(x) = f(x)] \geq 1 - \varepsilon \quad \forall x \in \{0, 1\}^n.$$

We can assume without loss of generality that all the polynomials in the support of the distribution ν have range $\{0, 1\}$. This is because given an arbitrary polynomial $P(x)$ over \mathbb{F}_p we can convert it into the polynomial $P'(x) = (P(x))^{p-1}$ which has range $\{0, 1\}$ by Fermat's little theorem. Note that the degree of P' is at most p times the degree of P which is not really a problem since $p = O(1)$ for us.

We now show why torus polynomials approximate $AC^0[p]$ functions.

Lemma 2.5. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Assume that there exists a distribution ν supported on polynomials $F : \mathbb{F}_p^n \rightarrow \{0, 1\}$ of degree d such that*

$$\Pr_{P \sim \nu} [P(x) = f(x)] \geq 1 - \varepsilon \quad \forall x \in \{0, 1\}^n.$$

Then

$$\overline{\text{deg}}_{3\varepsilon}(f) \leq O(d \log(n/\varepsilon)).$$

Proof. By standard Chernoff bounds, if we sample $F_1, \dots, F_m \sim \nu$ independently for $m = O(n/\varepsilon^2)$ then with high probability,

$$|\{i \in [m] : F_i(x) \neq f(x)\}| \leq 2\varepsilon m \quad \forall x \in \{0, 1\}^n.$$

Fix such a sample. Recall that $F_i : \mathbb{F}_p^n \rightarrow \{0, 1\}$ are computed by degree d polynomials over \mathbb{F}_p . Next, apply Lemma 2.3 with $\alpha = 1/2m$ and error ε/m . This gives us torus polynomials $P_i : \{0, 1\}^n \rightarrow \mathbb{T}$ of degree $O(d \log(m/\varepsilon))$ such that

$$\left| P_i(x) - \frac{1}{2m} F_i(x) \pmod{1} \right| \leq \frac{\varepsilon}{m} \quad \forall x \in \{0, 1\}^n.$$

Finally, take

$$P(x) = P_1(x) + \dots + P_m(x) \pmod{1}.$$

We claim that $P(x)$ is a torus polynomial which 3ε -approximates $f(x)$. To see this, fix $x \in \{0, 1\}^n$, and observe that

$$\left| P(x) - \frac{F_1(x) + \dots + F_m(x)}{2m} \pmod{1} \right| \leq \varepsilon$$

and

$$\left| \frac{F_1(x) + \dots + F_m(x)}{2m} - \frac{f(x)}{2} \pmod{1} \right| \leq 2\varepsilon,$$

and so

$$\left| P(x) - \frac{f(x)}{2} \pmod{1} \right| \leq 3\varepsilon.$$

This means that

$$\overline{\deg}_{3\varepsilon}(f) \leq \deg(P) = \max\{\deg(P_i) : i \in [m]\} = O(d \log(m/\varepsilon)) = O(d \log(n/\varepsilon)).$$

□

Corollary 2.6. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a function in $AC^0[p]$. Then for every $\varepsilon > 0$,*

$$\overline{\deg}_\varepsilon(f) \leq \text{polylog}(n/\varepsilon).$$

An interesting question that is motivated by the above results is whether we can have a mini-max type theorem for torus polynomials. Lemma 2.5 gives such a theorem in a very limited regime. The following is an attempt to generalize this.

Problem 2.7. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Assume that for any distribution ν over $\{0, 1\}^n$, there exists a low-degree torus polynomial $P_\nu : \{0, 1\}^n \rightarrow \mathbb{T}$ such that*

$$\mathbb{E}_{x \sim \nu} \left[\left| P_\nu(x) - \frac{f(x)}{2} \pmod{1} \right| \right] \leq \varepsilon.$$

Does that imply that the toroidal approximation degree of f is small? That is, does there exist a single low-degree torus polynomial which approximates f on all inputs?

It might also be useful to assume the stronger assumption that for any distribution ν over $\{0, 1\}^n$ and any $\alpha \in [0, 1]$ there exists a torus polynomial $P_{\nu, \alpha} : \{0, 1\}^n \rightarrow \mathbb{T}$ of degree d such that

$$\mathbb{E}_{x \sim \nu} [|P_{\nu, \alpha}(x) - \alpha f(x) \pmod{1}|] \leq \varepsilon.$$

This is also related to the following problem.

Problem 2.8. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$. For any $\alpha \in [0, 1]$ and $\varepsilon > 0$ define $d(\alpha, \varepsilon)$ to be the minimal degree of a torus polynomial $P : \{0, 1\}^n \rightarrow \mathbb{T}$ such that*

$$\|P - \alpha f \pmod{1}\|_\infty \leq \varepsilon.$$

What is the behavior of $d(\alpha, \varepsilon)$ as a function of α and of ε ? Specifically,

- *Can we bound $\max_\alpha d(\alpha, \varepsilon)$ in terms of $d(1/2, \varepsilon)$?*
- *Can we bound $\max_\alpha d(\alpha, \varepsilon)$ in terms of $\max_\alpha d(\alpha, 0.1)$?*

2.3 Circuit class ACC^0

We now turn our attention to ACC^0 functions and show that they too can be approximated by low-degree torus polynomials. Recall that a function is in ACC^0 if it can be computed by polynomial size circuits of constant depth with AND, OR, NOT, and MOD_m gates where m may be composite.

Our starting point is the following result of Green et al. [GKT92] which extends previous results of [Yao85, BT91].

Theorem 2.9 (Green et al. [GKT92]). *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be computable by ACC^0 circuits of depth ℓ and size $\text{poly}(n)$. Then for any $e \geq 1$ there exists an integer polynomial $F(x)$ of degree $d = e^{O(\ell)} \log^{O(\ell^2)} n$ which satisfies the following: there is some $k \geq e$ such that*

$$\forall x \in \{0, 1\}^n, \quad F(x) = f(x)2^k + E(x) \pmod{2^{k+e}}$$

for some error $E(x) \leq 2^{k-1}$.

Note that the above theorem states that the k^{th} bit of $F(x)$ in binary always equals to $f(x)$ and that it's padded with $e - 1$ zeros to its left, i.e the $(k + 1)^{\text{th}}$, $(k + 2)^{\text{th}}$, \dots , $(k + e - 1)^{\text{th}}$ bits are all guaranteed to be equal to 0. It turns out that, implicit in their work, is the following slightly stronger version of the above result which lets us pad zeros on both sides of the output bit (i.e., the k^{th} bit).

Theorem 2.10 (Implicit in Green et al. [GKT92]). *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be computable by ACC^0 circuits of depth ℓ and size $\text{poly}(n)$. Then for any $e \geq 1$ there exists an integer polynomial $F(x)$ of degree $d = e^{O(\ell)} \log^{O(\ell^2)} n$ which satisfies the following: there is some $k \geq e$ such that*

$$\forall x \in \{0, 1\}^n, \quad F(x) = f(x)2^k + E(x) \pmod{2^{k+e}}$$

for some error $E(x) \leq 2^{k-e}$.

Note the difference between the statements of Theorem 2.9 and Theorem 2.10: while the former upper-bounds the error $E(x)$ by 2^{k-1} the latter bounds it by 2^{k-e} , thus padding the output bit with $e - 1$ zeros on both the sides.

We remark that the proof of Theorem 2.10 is essentially the same as that of Theorem 2.9, with some minor tweaks, and so we omit it here. We now show how to use Theorem 2.10 to prove that low-degree torus polynomials approximate functions in ACC^0 .

Corollary 2.11. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a function in ACC^0 . Then for every $\varepsilon > 0$, there is a torus polynomial of degree $\text{polylog}(n/\varepsilon)$ that ε -approximates f . In other words,*

$$\overline{\deg}_\varepsilon(f) \leq \text{polylog}(n/\varepsilon).$$

Proof. Let us assume that f is computable by ACC^0 circuits of size $\text{poly}(n)$ and depth ℓ . Recall that, by definition of ACC^0 , $\ell = O(1)$. Let $F(x)$ be the polynomial obtained by applying Theorem 2.10 to f with $e = \log(1/\varepsilon)$ such that for some $k \geq e$

$$\forall x \in \{0, 1\}^n, \quad F(x) = f(x)2^k + E(x) \pmod{2^{k+e}}.$$

The degree of $F(x)$ is $d = e^{O(\ell)} \log^{O(\ell^2)} n = \text{polylog}(n/\varepsilon)$. Define the following torus polynomial

$$P(x) = \frac{F(x)}{2^{k+1}} \pmod{1}.$$

Clearly $\deg(P) = d$. For $i \geq 0$, let $F_i(x)$ denote the i^{th} bit of $F(x)$. Then, by the definition of F ,

$$\frac{F(x)}{2^{k+1}} \pmod{1} = \sum_{i=0}^k 2^{i-k-1} F_i(x) \pmod{1} = \frac{f(x)}{2} + \sum_{i=0}^{k-e} 2^{i-k-1} F_i(x) \pmod{1}.$$

As $F_i(x) \in \{0, 1\}$ for all i , we can bound

$$\left| P(x) - \frac{f(x)}{2} \pmod{1} \right| \leq 2^{-e} \leq \varepsilon \quad \forall x \in \{0, 1\}^n.$$

□

3 Lower bound for symmetric torus polynomials

In this section we prove a lower bound on the degree of *symmetric* torus polynomials that approximate MAJORITY. It will be instructive to think of symmetric torus polynomials as symmetric real polynomials evaluated modulo one. We start by examining the question for delta functions.

For $x \in \{0, 1\}^n$, let $|x| = \sum x_i$ denote its Hamming weight. The delta function

$$\Delta_w : \{0, 1\}^n \rightarrow \{0, 1\},$$

for $0 \leq w \leq n$, is defined as

$$\Delta_w(x) = \begin{cases} 1 & |x| = w \\ 0 & \text{otherwise} \end{cases}.$$

Lemma 3.1. *Let n, d be positive integers such that for every $0 \leq w \leq n$ there exists a symmetric torus polynomial $Q_w : \{0, 1\}^n \rightarrow \mathbb{T}$ of degree d that $\frac{1}{20n}$ -approximates $\Delta_w(x)$. Then $d = \Omega\left(\sqrt{\frac{n}{\log n}}\right)$.*

Proof. Let $\text{Sym}(n)$ denote the set of symmetric Boolean functions in n variables and let $\text{SymPoly}_{d,k}(n)$ denote the set of symmetric torus polynomials in n variables of degree d whose coefficients are of the form $q/2^k$ for $q \in \{-(2^k - 1), \dots, 0, \dots, 2^k - 1\}$.

Let f be an arbitrary function in $\text{Sym}(n)$. Abusing notation, we let $f^{-1}(1)$ denote the set of weights of the layers of the Hamming cube where f takes value 1. Now define the torus polynomial Q_f as

$$Q_f(x) = \sum_{i \in f^{-1}(1)} Q_i(x) \pmod{1}.$$

It follows that Q_f is a symmetric torus polynomial of degree d that $\frac{1}{20}$ -approximates f . Since Q_f is a symmetric torus polynomial, namely a symmetric real polynomial modulo one, it may be written without loss of generality as

$$Q_f(x) = \sum_{j=0}^d c_j \left(\sum x_i \right)^j \pmod{1},$$

where $c_j \in [0, 1)$. Let $k \geq 0$ be an integer whose value we will fix later. For $0 \leq j \leq d$, let $q_j \in \{-(2^k - 1), \dots, 0, \dots, 2^k - 1\}$ be such that

$$\left| \frac{q_j}{2^k} - c_j \right| \leq \frac{1}{2^k},$$

and define Q'_f to be the polynomial

$$Q'_f(x) = \sum_{j=0}^d \frac{q_j}{2^k} \cdot \left(\sum x_i \right)^j \pmod{1}.$$

Observe that for every $x \in \{0, 1\}^n$,

$$|Q_f(x) - Q'_f(x) \pmod{1}| \leq \sum_{j=0}^d \left| \frac{q_j}{2^k} - c_j \right| \cdot |x|^j \leq \frac{(d+1) \cdot n^d}{2^k}.$$

If k is such that $\frac{(d+1) \cdot n^d}{2^k} \leq \frac{1}{20}$ then

$$\|Q_f - Q'_f \pmod{1}\|_\infty \leq \frac{1}{20},$$

and so

$$\left\| \frac{f}{2} - Q'_f \pmod{1} \right\|_\infty \leq \left\| \frac{f}{2} - Q_f \pmod{1} \right\|_\infty + \|Q_f - Q'_f \pmod{1}\|_\infty \leq \frac{1}{10}.$$

Note that we can choose $k = O(d \log n)$ while still satisfying the required condition on k .

So far we have shown that for every $f \in \text{Sym}(n)$ there is a polynomial $Q_f \in \text{SymPoly}_{d,k}(n)$ that $1/10$ -approximates f where $k = O(d \log n)$. In the other direction, one can easily verify that every polynomial in $\text{SymPoly}_{d,k}(n)$ can $1/10$ -approximate *at most* one function in $\text{Sym}(n)$. This implies that

$$|\text{SymPoly}_{d,k}(n)| \geq |\text{Sym}(n)|.$$

Plugging in $|\text{SymPoly}_{d,k}(n)| = 2^{(k+1)(d+1)}$ and $|\text{Sym}(n)| = 2^n$, and using $k = O(d \log n)$, yields the bound $d = \Omega\left(\sqrt{\frac{n}{\log n}}\right)$. \square

Before we proceed, we formally define MAJORITY on n bits, denoted by $\text{Maj}_n(x)$, as

$$\text{Maj}_n(x) = \begin{cases} 1 & |x| \geq \frac{n}{2} \\ 0 & \text{otherwise} \end{cases}.$$

Lemma 3.2. *If there is a symmetric torus polynomial of degree $o\left(\sqrt{\frac{n}{\log n}}\right)$ that $\frac{1}{20n}$ -approximates $\text{Maj}_n(x)$, then for every $0 \leq w \leq n$ there is a symmetric torus polynomial of degree $o\left(\sqrt{\frac{n}{\log n}}\right)$ that $\frac{1}{20n}$ -approximates $\Delta_w(x)$.*

Proof. Fix w . Let $\Delta_{\geq w}(x)$ denote the function that takes value 1 iff $|x| \geq w$. Then we can write

$$\Delta_{\geq w}(x_1, \dots, x_n) = \text{Maj}_{2n+1}(x_1, \dots, x_n, c_1, \dots, c_{n+1}), \quad (2)$$

where $c \in \{0, 1\}^{n+1}$ is the string whose first $n - w + 1$ bits are set to 1 and the rest of the bits are set to 0. Let $Q(x_1, \dots, x_{2n+1})$ be the symmetric torus polynomial in $2n + 1$ variables that $\frac{1}{20(2n+1)}$ -approximates $\text{Maj}_{2n+1}(x)$. Let $Q_{\geq w}(x_1, \dots, x_n)$ be the torus polynomial defined as

$$Q_{\geq w}(x_1, \dots, x_n) = Q(x_1, \dots, x_n, c_1, \dots, c_{n+1}),$$

where $c \in \{0, 1\}^{n+1}$ is as defined above. It follows from (2) that $Q_{\geq w}(x_1, \dots, x_n)$ $\frac{1}{40n}$ -approximates $\Delta_w(x_1, \dots, x_n)$. Furthermore,

$$\deg(Q_{\geq w}) = o\left(\sqrt{\frac{n}{\log n}}\right).$$

Similarly, we can obtain a symmetric torus polynomial $Q_{\geq w+1}(x_1, \dots, x_n)$ that $\frac{1}{40n}$ -approximates $\Delta_{\geq w+1}(x_1, \dots, x_n)$ such that

$$\deg(Q_{\geq w+1}) = o\left(\sqrt{\frac{n}{\log n}}\right).$$

Note that

$$\frac{\Delta_w(x)}{2} \pmod{1} = \left(\frac{\Delta_{\geq w}(x)}{2} - \frac{\Delta_{\geq w+1}(x)}{2} \right) \pmod{1}.$$

Defining $Q_w(x) = Q_{\geq w}(x) - Q_{\geq w+1}(x) \pmod{1}$, it follows that

$$\left\| \frac{\Delta_w(x)}{2} - Q_w(x) \pmod{1} \right\|_{\infty} \leq \frac{1}{20n}.$$

This completes the proof. \square

The main result of this section now follows from Lemma 3.1 and Lemma 3.2:

Corollary 3.3. *Any symmetric torus polynomial of degree d that $\frac{1}{20n}$ -approximates $\text{Maj}_n(x)$ must satisfy $d = \Omega\left(\sqrt{\frac{n}{\log n}}\right)$.*

4 Upper bound for delta functions

In this section, we prove the somewhat surprising result that if the approximation parameter $\varepsilon > 0$ is not too small (say, ε is a small constant), then the delta function Δ_w can be nontrivially approximated by *symmetric* low-degree torus polynomials.

Lemma 4.1. *For every $0 \leq w \leq n$ and $\varepsilon > 0$, there is a symmetric torus polynomial of degree $\frac{\text{polylog}(n/\varepsilon)}{\varepsilon}$ that ε -approximates $\Delta_w(x)$, and thus*

$$\overline{\text{deg}}_{\varepsilon}(\Delta_w) \leq \frac{\text{polylog}(n/\varepsilon)}{\varepsilon}.$$

Proof. For any prime $p \geq 2$, let $f_p : \{0, 1\}^n \rightarrow \{0, 1\}$ denote the function

$$f_p(x) = \begin{cases} 1 & |x| \equiv w \pmod{p} \\ 0 & \text{otherwise} \end{cases}.$$

It is computed by the \mathbb{F}_p -polynomial of degree $p - 1$

$$f_p(x) = 1 - \left(\sum x_i - w \right)^{p-1} \pmod{p}.$$

Let $P = \{p_1, \dots, p_t\}$ be the first t primes, for t to be chosen later. Applying Lemma 2.3 with $\alpha = 1/2t$ and error $\varepsilon/2t$, for each $p \in P$ we obtain a torus polynomial $Q_p : \{0, 1\} \rightarrow \mathbb{T}$ of degree $O(p \log(t/\varepsilon))$ such that

$$\left\| Q_p - \frac{1}{2t} f_p \pmod{1} \right\|_{\infty} \leq \frac{\varepsilon}{2t}.$$

Define

$$Q(x) = \sum_{p \in P} Q_p(x) \pmod{1}.$$

We claim that Q is a symmetric torus polynomial that ε -approximates Δ_w .

Consider first $x \in \{0, 1\}^n$ with $|x| = w$. In this case, for each $p \in P$ we have $f_p(x) = 1$, $|Q_p(x) - \frac{1}{2t} \pmod{1}| \leq \varepsilon/2t$ and hence

$$\left| Q(x) - \frac{1}{2} \pmod{1} \right| \leq \varepsilon/2.$$

Next, assume that $|x| \neq w$. Then $f_p(x) = 1$ only if p divides $|x| - w$. As there are at most $\log n$ such primes, we have that

$$|Q(x) \pmod{1}| \leq \frac{\varepsilon}{2} + \frac{\log n}{t}.$$

To conclude we choose $t = O(\log(n)/\varepsilon)$. The largest prime in P has size $O(t \log t)$ which means that

$$\overline{\deg}_\varepsilon(f) \leq \deg(Q) = \max\{\deg(Q_p) : p \in P\} \leq O(t \log t \cdot \log(t/\varepsilon)) = \frac{\text{polylog}(n/\varepsilon)}{\varepsilon}.$$

To see why Q is symmetric, observe that Lemma 2.3 preserves symmetry. \square

Acknowledgements. We thank Marco Carmosino for useful discussions regarding this work. We would also like to thank Eric Allender and Sivakanth Gopi for helpful feedback on earlier drafts of this work.

References

- [BFH⁺13] Arnab Bhattacharyya, Eldar Fischer, Hamed Hatami, Pooya Hatami, and Shachar Lovett. Every locally characterized affine-invariant property is testable. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 429–436. ACM, 2013.
- [BHS17] Abhishek Bhrushundi, Prahladh Harsha, and Srikanth Srinivasan. On polynomial approximations over $\mathbb{Z}/2^k\mathbb{Z}$. In *34th Symposium on Theoretical Aspects of Computer Science, (STACS 2017)*, pages 12:1–12:12, 2017.
- [BL15] Abhishek Bhowmick and Shachar Lovett. Nonclassical polynomials as a barrier to polynomial lower bounds. In *Proceedings of the 30th Conference on Computational Complexity*, pages 72–87. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.
- [BT91] Richard Beigel and Jun Tarui. On ACC (circuit complexity). In *Foundations of Computer Science, 1991. Proceedings., 32nd Annual Symposium on*, pages 783–792. IEEE, 1991.
- [GKT92] Frederic Green, Johannes Kobler, and Jacobo Toran. The power of the middle bit. In *Structure in Complexity Theory Conference, 1992., Proceedings of the Seventh Annual*, pages 111–117. IEEE, 1992.
- [Hås87] Johan Håstad. Computational limitations of small-depth circuits. 1987.
- [Hås98] Johan Håstad. The shrinkage exponent of De Morgan formulas is 2. *SIAM Journal on Computing*, 27(1):48–64, 1998.
- [MW18] Cody D Murray and R Ryan Williams. Circuit lower bounds for nondeterministic quasi-polytime: An easy witness lemma for NP and NQP. 2018.
- [NS92] Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. In *Proceedings of the Twenty-fourth Annual ACM Symposium on Theory of Computing*, STOC '92, pages 462–467. ACM, 1992.
- [Raz87] Alexander A Razborov. Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. *Math. notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.
- [RR97] Alexander A Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24 – 35, 1997.

- [Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 77–82. ACM, 1987.
- [Tao08] Terence Tao. Some notes on non-classical polynomials in finite characteristic. 2008.
- [Tod91] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.
- [TZ12] Terence Tao and Tamar Ziegler. The inverse conjecture for the Gowers norm over finite fields in low characteristic. *Annals of Combinatorics*, 16(1):121–188, 2012.
- [Wil14] Ryan Williams. Nonuniform ACC circuit lower bounds. *Journal of the ACM (JACM)*, 61(1):2, 2014.
- [Yao85] Andrew Chi-Chih Yao. Separating the polynomial-time hierarchy by oracles. In *Foundations of Computer Science, 1985., 26th Annual Symposium on*, pages 1–10. IEEE, 1985.