Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 74 (2024)

Degree Lower Bounds for Torus Polynomials and MAJORITY vs ACC^0

Vaibhav Krishan[1] and Sundar Vishwanathan[2]

[1]The Institute of Mathematical Sciences, Chennai, India
[2]Indian Institute of Technology Bombay, Mumbai, India

Abstract

The class ACC^0 consists of Boolean functions that can be computed by constant-depth circuits of polynomial size with $\mathsf{AND}, \mathsf{NOT}$ and MOD_m gates, where m is a natural number. At the frontier of our understanding lies a widely believed conjecture asserting that $\mathsf{MAJORITY}$ does not belong to ACC^0.

A few years ago, Bhrushundi, Hosseini, Lovett and Rao (ITCS 2019) introduced torus polynomial approximations as an approach towards this conjecture. Torus polynomials approximate Boolean functions when the fractional part of their value on Boolean points is close to half the value of the function. They reduced the conjecture that $\mathsf{MAJORITY} \notin \mathsf{ACC}^0$ to a conjecture concerning the non-existence of low degree torus polynomials that approximate $\mathsf{MAJORITY}$.

We reduce the non-existence problem further, to a statement about finding feasible solutions for an infinite family of linear programs. The main advantage of this statement is that it allows for incremental progress, which means finding feasible solutions for successively larger collections of these programs. As an immediate first step, we find feasible solutions for a large class of these linear programs, leaving only a finite set for further consideration. Our method is inspired by the *method of dual polynomials*, which is used to study the approximate degree of Boolean functions. Using our method, we also propose a way to progress further.

We prove several additional key results with the same method, which include:

- A lower bound on the degree of *symmetric* torus polynomials that approximate the AND function. As a consequence, we get a separation that symmetric torus polynomials are *weaker* than their asymmetric counterparts.
- An error-degree trade-off for symmetric torus polynomials approximating the $\mathsf{MAJORITY}$ function, strengthening the corresponding result of Bhrushundi, Hosseini, Lovett and Rao (ITCS 2019).
- The *first* lower bounds against torus polynomials approximating AND, showcasing the power of the machinery we develop. This lower bound nearly matches the corresponding upper bound. Hence, we get an almost complete characterization of the torus polynomial approximation degree of AND.
- Lower bounds against asymmetric torus polynomials approximating $\mathsf{MAJORITY}$, or AND, in the very low error regime. This partially answers a question posed in Bhrushundi, Hosseini, Lovett and Rao (ITCS 2019) about error-reduction for torus polynomials.

ISSN 1433-8092

1 Introduction

Proving that an explicit function is not contained in a complexity class is the prime focus of complexity theorists, and such questions make up some of the hardest problems in computer science. We study such a question at the frontier of our knowledge about Boolean circuit complexity classes. To state the question, we first need to define the class of Boolean circuits we consider.

Denote by ACC^0 the class of constant-depth Boolean circuits of polynomial size comprising $\mathsf{AND}, \mathsf{NOT}$, and MOD_m gates. A MOD_m gate outputs 1 if and only if the count of 1s in the input is divisible by m. Nearly 35 years ago, Barrington [Bar89] conjectured that ACC^0 does not contain $\mathsf{MAJORITY}$. Here, $\mathsf{MAJORITY}$ outputs 1 if and only if the number of 1s is at least half of the total number of inputs. This conjecture has remained unresolved since.

Conjecture 1 (Barrington's conjecture [Bar89])**.** $\mathsf{MAJORITY} \notin \mathsf{ACC}^0$.

The objective of the conjecture is to prove that a particular circuit class cannot compute a certain function. In the literature, this task is referred to as proving *lower bounds* against that class. We outline a few major approaches that have led to Boolean circuit lower bounds in the past.

One of the approaches is based on "simplification", and the probabilistic method, for example: using *random restrictions*. This is a classical technique, developed for studying various complexity classes, such as AC^0, the class of constant-depth circuits comprising AND and NOT gates. A classic example is the landmark result of Håstad [Hås86], who proved that AC^0 circuits simplify when a significant fraction of the input variables are assigned values randomly. It is easy to see that the parity function does not undergo such simplification. The author formalized this intuition to prove nearly optimal lower bounds against AC^0 circuits. However, random restrictions do not seem useful for lower bounds against ACC^0, as it contains the parity function.

Another approach is to use the *satisfiability algorithms*–to–lower bounds connection, to prove lower bounds from high complexity classes such as NEXP. Williams [Wil14] developed this approach in a groundbreaking work, and used it to prove that NEXP is not contained in ACC^0. Subsequent works [COS18, MW19, Che19, CLW20, Che23] have considerably strengthened this connection. In particular, Murray and Williams [MW19] have proved that NQP is not contained in ACC^0, improving the lower bound. However, it is not clear how to use this method to prove that an easily computable function, such as $\mathsf{MAJORITY}$, is not contained in ACC^0.

This leads us toward another classical approach, based on the *polynomial method*. In this framework, researchers study various notions of representing Boolean functions using polynomials. This framework is quite powerful, and has numerous applications across theoretical computer science, see Aaronson's survey [Aar08] for an interesting and insightful account. We describe two notions of polynomial representations that have found uses in the study of Boolean circuits.

The first notion, called real polynomial approximation, uses polynomials over the reals to approximate Boolean functions pointwise. Nisan and Szegedy [NS94], in a seminal work, studied this model, and proved its connections with other natural computational models, such as *decision trees*. Their work provided considerable impetus to the study of real polynomial approximations, and firmly established their use in mainstream complexity theory. Today, the study of real polynomial approximations is a subfield by itself, with well-developed techniques for lower bounds and upper bounds, and numerous applications. See Bun and Thaler's survey [BT22] for a comprehensive discussion of real polynomial approximations.

The second notion of polynomial approximation, called *probabilistic polynomials*, uses a distribution of polynomials over a finite field. On any Boolean point, a polynomial from the distribution should match the value of the given function with "high" probability. Razborov [Raz87], and

Smolensky [Smo87], pioneered the use of this model in independent works. Consider any function f computable by constant-depth circuits of polynomial size with $\mathsf{AND}, \mathsf{NOT}$ and MOD_p gates, for a prime p. The authors, independently, proved that there exists a distribution of "low" degree polynomial over $\mathbb{F}_p$ that matches f with "high" probability. They also proved that the same does not hold for $\mathsf{MAJORITY}$, or MOD_q for a prime $q \neq p$, leading to a lower bound.

Broadly speaking, in order to prove that a function f is not contained in a class $\mathcal{C}$, the theme here is to find a *distinguisher*. A distinguisher is a function μ that maps f to a point outside the image of $\mathcal{C}$ under μ, proving $f \notin \mathcal{C}$. That is, proving $\mu(f) \notin \mu(\mathcal{C})$ implies $f \notin \mathcal{C}$. For example, in [Raz87, Smo87], the degree of the probabilistic polynomial acts as the distinguisher. This degree is low for functions in $\mathsf{AC}^0[p]$, while $\mathsf{MAJORITY}$ requires large degree, hence the lower bound $\mathsf{MAJORITY} \notin \mathsf{AC}^0[p]$.

The models of polynomial approximation defined above do not seem to give a distinguisher against ACC^0. For example, ACC^0 circuits can use MOD_6, which requires large degree in either model. In fact, for a long time, there were no polynomial method based approaches known for proving ACC^0 lower bounds.

Then, in a pivotal work few years ago, Bhrushundi, Hosseini, Lovett and Rao [BHLR19] made an inspired suggestion of using the degree of torus polynomials as a distinguisher towards the $\mathsf{MAJORITY}$ vs ACC^0 question. Torus polynomials approximate a Boolean function f if their fractional part is close to $\frac{f}{2}$[1]. They proved that torus polynomial approximations extend both real polynomial approximations and approximation using probabilistic polynomials (see [BHLR19, Lemma 14]). In fact, torus polynomials are more powerful, they can efficiently approximate MOD_m for any m. We define this model below, rephrasing [BHLR19, Definition 1].

Definition 1 (Torus Polynomial Approximation [BHLR19])**.** *Consider a Boolean function $f : \{0,1\}^n \to \{0,1\}$, a polynomial $P \in \mathbb{R}[X_1, \ldots, X_n]$ (we assume that P is multilinear without losing generality) and a real number $0 \leq \varepsilon < \frac{1}{4}$. P is a torus polynomial that ε-approximates f, if the following holds:*

There exists a function $Z : \{0,1\}^n \to \mathbb{Z}$, such that for any Boolean point $a \in \{0,1\}^n$, we have $\left|P(a) - \frac{f(a)}{2} - Z(a)\right| \leq \varepsilon$. In other words, the fractional part *of $P(a)$ is within ε of $\frac{f(a)}{2}$.*

Denote the minimum degree of such a polynomial by $\overline{\deg}_\varepsilon(f)$.

Given any function $f : \{0,1\}^n \to \{0,1\}$, consider the unique multilinear polynomial that exactly matches f on all Boolean points[2]. This would require degree n for most functions, with zero error of approximation. Naturally, the question is, for which functions f can we construct a torus polynomial of much smaller degree, say $\log^2(n)$, that $\frac{1}{n^2}$-approximate f, for example. In [BHLR19, Corollary 20], the authors proved that something similar holds for all functions in ACC^0.

Theorem 1.1 ([BHLR19])**.** *Consider any function $f : \{0,1\}^n \to \{0,1\}$ such that $f \in \mathsf{ACC}^0$. Then, $\overline{\deg}_\varepsilon(f) \leq \log(n)^{O(1)}$ for any $\varepsilon \geq \frac{1}{n^{O(1)}}$.*

Hence, proving that the same does not hold for the majority function would prove $\mathsf{MAJORITY}$ is not contained in ACC^0. This is precisely the goal of our work in this paper. While we could not take this task to completion, we do make progress towards it. Before discussing our contributions, we discuss previous work related to ACC^0 as well as torus polynomials.

[1] 0 and 1 have the same fractional part. Dividing $f : \{0,1\}^n \to \{0,1\}$ by 2 makes the fractional parts different.

[2] The existence of such a polynomial is folklore.

1.1 Previous Work

Various works in the 90's had proved conversion results for ACC^0, with the purpose of proving ACC^0 lower bounds. For example, strengthening the results from [Yao90, BT94], Green, Köbler, Regan, Schwentick and Torán [GKR+95] proved that all ACC^0 functions have MidBit^+ circuits computing them. Here, MidBit^+ is the class of depth-two circuits, with AND gates at the bottom and a MidBit gate[3] at the top. The authors proposed to prove lower bounds against MidBit^+ as an approach to prove ACC^0 lower bounds. They argued that the simpler structure of MidBit^+ circuits might make it easier to prove lower bounds.

Along similar lines, by combining [HG91, RW93], one gets a communication complexity based approach. These works together imply that lower bounds against the *number-on-forehead* communication model lead to ACC^0 lower bounds. However, lower bounds against this communication model also imply MidBit^+ lower bounds. Hence, logically speaking, lower bounds against MidBit^+ are an easier route to ACC^0 lower bounds.

In Krishan [Kri21], the author proved that functions with low degree torus polynomial approximations belong to MidBit^+. Hence, one can argue that lower bounds against torus polynomials is an even more refined approach for ACC^0 lower bounds. Moreover, Chen, Lu, Lyu and Oliveira [CLLO21] proved that lower bounds against torus polynomials lead to *average-case* lower bounds, and *pseudorandom generators*, against ACC^0. Both of these are major open questions, which gives us further impetus for proving lower bounds against torus polynomials.

In [BHLR19], the authors introduced torus polynomials with the goal of proving that $\mathsf{MAJORITY}$ does not belong to ACC^0. Now, $\mathsf{MAJORITY}$ is a symmetric function, as its value only depends on the number of 1s in the input. Hence, it is natural to study *symmetric*[4] torus polynomials that approximate $\mathsf{MAJORITY}$ as the first step. The authors used a counting-based argument to prove the following lower bound.

Theorem 1.2 (Corollary 23 of [BHLR19])**.** *Any symmetric torus polynomial, that* $\frac{1}{20n}$*-approximates* $\mathsf{MAJORITY}$*, must have degree* $\Omega\left(\sqrt{\frac{n}{\log(n)}}\right)$.

Now, a priori, this does not resolve Barrington's conjecture, it needs an analogous statement for *asymmetric* torus polynomials. Indeed, in [BHLR19, Conjecture 5], the authors conjectured that Theorem 1.2 holds for asymmetric torus polynomials.

Conjecture 2 ([BHLR19])**.** *Any torus polynomial, that* $\frac{1}{20n}$*-approximates* $\mathsf{MAJORITY}$*, must have degree* $\Omega\left(\sqrt{\frac{n}{\log(n)}}\right)$.

This conjecture, if true, proves Barrington's conjecture. Moreover, it will separate P from ACC^0, improving our knowledge well beyond what is currently known.

1.2 Our Results

The main goal of our work is to resolve Conjecture 2. Towards this end, we outline a plan of attack in Section 3. A major contribution of this paper is a reduction of Conjecture 2 to a statement that allows for incremental progress.

Fix n and $d = o\left(\sqrt{\frac{n}{\log(n)}}\right)$, and suppose the goal is to prove the following: Any torus polynomial that ε-approximates $\mathsf{MAJORITY}$ over n variables must have degree more than d. Informally stated,

[3] A MidBit outputs the middle bit from the binary expansion of the number of 1s, with a fixed tie-breaking choice.
[4] A polynomial is symmetric if it is invariant under permutation of its variables.

we define a vector space Γ of dimension 2^n, a vector v' of dimension 2^n, and conjecture that for any vector $v \in \mathbb{Z}^{2^n}$, there is a $\gamma \in \Gamma$ such that:

$$\sum_{i=1}^{2^n}(v_i + v'_i)\gamma_i > \varepsilon \sum_{i=1}^{2^n}|\gamma_i|$$

The vector v' has a very simple structure, it encodes the function for which we wish to prove the lower bound, say MAJORITY. See Theorem 2.1 for an exact statement. Incremental progress would mean proving the statement for larger and larger subsets of $\mathbb{Z}^{2^n}$.

We take the first steps in this direction by first bounding the entries in v, see Theorem 3.3. This immediately leaves us with only a finite subset of $\mathbb{Z}^{2^n}$ for which we need to argue further. Here, each entry of v can independently take a value that satisfies the upper bound, allowing 2^n degrees of freedom. As the next step, in Theorem 3.5, we show that a few entries in v determine the other entries. This reduces the degrees of freedom to a tiny fraction of 2^n.

We demonstrate the power of our method by proving a lower bound against torus polynomials approximating AND. No lower bounds were known for asymmetric torus polynomials prior to our work, and the lower bound we prove is only quadratically away from the corresponding upper bound for inverse-polynomial error. Following is the formal statement of the result.

Theorem 1.3. *Any torus polynomial, that ε-approximates* AND*, must have degree* $\Omega\left(\log\left(\frac{1}{\varepsilon}\right)\right)$.

The result above also holds for MAJORITY, but it does not suffice to prove MAJORITY $\notin \mathsf{ACC}^0$, which requires a lower bound of the form $\log^{\omega(1)}(n)$ for some inverse-polynomial error. Further, as a special case of the result above, we study the case when ε is exponentially small. We show that AND requires full degree in this regime, and so does MAJORITY. In [BHLR19, Problem 6], the authors ask about error-reduction for torus polynomials. The full-degree lower bound allows us to conditionally answer this question for a particular error-regime, which we discuss in Subsection 4.1.

Our method also applies to symmetric torus polynomials, which we use to prove a much stronger lower bound against symmetric torus polynomials approximating AND. This lower bound matches the lower bound from [BHLR19, Corollary 23] (refer to Theorem 1.2), but for AND, rather than MAJORITY. Note that no such lower bound was known for AND before our work, and it matches the corresponding upper bound, barring some log factors. We state the result below.

Theorem 1.4. *Any symmetric torus polynomial, that $\frac{1}{20n}$-approximates* AND*, must have degree* $\Omega\left(\sqrt{\frac{n}{\log(n)}}\right)$.

The lower bound for symmetric torus polynomials is higher than the upper bound for asymmetric torus polynomials approximating AND. Hence, as a corollary, we prove that symmetric torus polynomials are weaker than their asymmetric counterparts, see Corollary 1. Moreover, this shows that a symmetrization based approach is unlikely to work for Conjecture 2.

We also strengthen [BHLR19, Corollary 23], and prove stronger degree lower bounds for smaller error. If one follows the proof of [BHLR19, Corollary 23], for symmetric torus polynomials that $\frac{1}{n^2}$-approximate MAJORITY, the lower bound remains the same, i.e. $\Omega\left(\sqrt{\frac{n}{\log(n)}}\right)$. We are able to prove $\Omega\left(\sqrt{n}\right)$ as the lower bound in this case, strictly improving the degree, albeit by a log factor. In fact, we are able to prove an error-degree trade-off, see Theorem 5.8 for the exact statement.

Our Method

We use a linear programming based approach to prove our lower bound results. This approach, based on duality in linear programs, allows us to find a witness that certifies the non-existence of a torus polynomial approximation. We describe a broad outline of the method below.

Consider a torus polynomial P, of degree at most d, that ε-approximates f. Then, there exists some integer function $Z : \{0,1\}^n \to \mathbb{Z}$, such that $P(a)$ is at most ε away from $Z(a) + \frac{f(a)}{2}$ for any $a \in \{0,1\}^n$. For each a, we can write $P(a)$ as a particular linear combination of its coefficients, hence, the condition above is a linear constraint. Here, we make a crucial choice, with respect to how we treat Z. If we treat each $Z(a)$ as an integer-valued variable, we get a system of linear Diophantine inequalities, that are much harder to handle. Instead, we treat each $Z(a)$ as an indeterminate, and write one linear program for each possible function Z.

Thereby, we get an infinite family of linear programs, such that P exists if and only if some program from the family is feasible. Hence, to prove that P does not exist, we need to prove that each program is infeasible, for which we look at the dual of these programs. Using strong duality in linear programs, P does not exist if and only if each of the dual programs is feasible.

Now, given a function Z, the dual program we obtain is as follows: For each n, and each degree d, we have a matrix $M(n,d)$, comprising the evaluations of all monomials of degree at most d on each Boolean point. The set of solutions for the dual program consists of the nullspace of $M(n,d)$, i.e., vectors γ such that $M(n,d)\gamma = 0$. Here, γ is a vector with 2^n many real entries, with each entry γ_a indexed by a Boolean point a. A vector γ is a feasible solution for the dual, if it satisfies $\left|\sum_{a\in\{0,1\}^n} \gamma_a \left(Z(a) + \frac{f(a)}{2}\right)\right| > \varepsilon \sum_{a\in\{0,1\}^n} |\gamma_a|$. For a detailed explanation on how we obtain the dual, please refer to Theorem 2.1.

With this method, our plan to prove Conjecture 2 is as follows. Fix n, and any $d = o\left(\sqrt{\frac{n}{\log(n)}}\right)$, with $f = \mathsf{MAJORITY}$ and $\varepsilon = \frac{1}{20n}$. For any function $Z : \{0,1\}^n \to \mathbb{Z}$, we plan to find a feasible solution γ for the dual corresponding to Z. To start, we find such a feasible solution if $|Z(a)|$ exceeds an upper bound for any $a \in \{0,1\}^n$, where the upper bound depends on a. Then, we show how to infer the values of $Z(a)$ for each a with Hamming weight $|a| \geq (d+1)^2$, when all $Z(a)$ for $|a| < (d+1)^2$ are fixed. In other words, if $Z(a)$ does not take the inferred value for some a, we find a feasible solution for the dual corresponding to Z. We propose to continue this plan further, by finding more feasible solutions to incrementally rule out all possible Zs.

Our method shares some similarities to how dual polynomials are used to prove lower bounds for real polynomial approximations. Each vector γ in the nullspace of $M(n,d)$ is in fact a dual polynomial, with *pure high-degree* more than d. We use a geometric perspective, as we find it more useful, especially for our lower bound results.

Organization

We discuss some preliminaries, and a general method for proving torus polynomial lower bounds, in Section 2. Based on this method, we propose a plan to prove Conjecture 2 in Section 3. Our lower bound results for asymmetric torus polynomials appear in Section 4. Finally, we prove lower bounds for symmetric torus polynomials in Section 5.

2 Preliminaries

We consider natural numbers without including 0, and denote it by $\mathbb{N} = \{1, 2, \ldots\}$. For $n \in \mathbb{N}$ and $d \in \mathbb{N}$, we use the following notation for brevity:

$$\binom{n}{\leq d} = \sum_{i \leq d} \binom{n}{i} \qquad \binom{n}{> d} = \sum_{i > d} \binom{n}{i}$$

$$[n] = \{1, \ldots, n\} \qquad [n]^* = \{0, \ldots, n\}$$

$$\binom{[n]}{\leq d} = \{S : S \subseteq [n], |S| \leq d\} \qquad \binom{[n]}{> d} = \{S : S \subseteq [n], |S| > d\}$$

2.1 Sets and Boolean Points

We identify $2^{[n]}$ with $\{0,1\}^n$ in the natural way, as follows. For $S \subseteq [n]$, the corresponding Boolean point has a 1 at position i if and only if i is present in S. This defines a bijection between $2^{[n]}$ and $\{0,1\}^n$. Using this bijection, we will often interpret a set $S \subseteq [n]$ as a Boolean point, and a Boolean point $a \in \{0,1\}^n$ as a set, making the interpretation explicit wherever it is not clear from the context. $|a|$ denotes the Hamming weight of $a \in \{0,1\}^n$, which also equals its size when considered as a set.

2.2 Linear Algebra

Over the reals $\mathbb{R}$, we denote the set of matrices of size $m \times n$ by $\mathcal{M}_{m \times n}(\mathbb{R})$. For a matrix $M \in \mathcal{M}_{m \times n}(\mathbb{R})$, we denote its nullspace by $nullspace(M) = \{\gamma \in \mathbb{R}^n : M\gamma = 0\}$. For a vector $\gamma \in \mathbb{R}^n$, we denote its ℓ^p-norm by $\|\gamma\|_p = (\sum_{i=1}^n |\gamma_i|^p)^{\frac{1}{p}}$. Of particular interest to us are the ℓ^1-norm and the ℓ^2-norm, defined for $p = 1, 2$ respectively. We will also consider the ℓ^∞-norm, defined as $\|\gamma\|_\infty = \max_{i=1}^n |\gamma_i|$.

2.3 Our Method for Torus Polynomial Lower Bounds

Now, we describe a general method for proving lower bounds on torus polynomial approximations. Fix $n \in \mathbb{N}$ and $d \in \mathbb{N}$, such that $d < n$. Also, fix a Boolean function $f : \{0,1\}^n \to \{0,1\}$, and an error of approximation $\varepsilon < \frac{1}{4}$. We start by defining a family of set-inclusion matrices that will be relevant for the method. For each monomial of degree at most d over n variables, the matrix contains one row, and the row encodes the evaluation of the monomial over all Boolean points.

Construction 1. *Define the matrix $M(n,d)$ of size $\binom{n}{\leq d} \times 2^n$ as follows. Its rows are indexed by elements of $\binom{[n]}{\leq d}$, and columns by elements of $2^{[n]}$. The entries for $1 \leq i \leq \binom{n}{\leq d}, 1 \leq j \leq 2^n$ are:*

$$M_{i,j} = 1_{S_i \subseteq S_j}$$

Here, $1_{S_i \subseteq S_j}$ is an indicator function, evaluating to 1 if $S_i \subseteq S_j$, and zero otherwise.

In the following statement, we convert the question of torus polynomial lower bounds to an existence based question. The proof of the statement is very similar to that for the method of dual polynomials (see [BT22]), we present it here for the sake of completeness.

Theorem 2.1. *The following are equivalent for any $n \in \mathbb{N}, d \in \mathbb{N}$ such that $d < n$, $\varepsilon < \frac{1}{4}$ and $f : \{0,1\}^n \to \{0,1\}$:*

- *Any torus polynomial that ε-approximates f has degree more than d.*
- *For any $Z : \{0,1\}^n \to \mathbb{Z}$, there exists a vector $\gamma \in nullspace(M(n,d))$, such that:*

$$\left|\left\langle Z + \frac{f}{2}, \gamma \right\rangle\right| > \varepsilon \|\gamma\|_1$$

Proof. To start the proof, assume that there exists a torus polynomial P of degree at most d, that ε-approximates f. As per Definition 1, there exists $Z : \{0,1\}^n \to \mathbb{Z}$, such that $P(a)$ is within ε distance from $Z(a) + \frac{f(a)}{2}$ for each Boolean point a. We plan to use linear programming to capture the conditions that P must satisfy. Denote the coefficients of P as a vector $\alpha \in \mathbb{R}^{\binom{n}{\leq d}}$, where each entry of α, indexed by a set S of size at most d, acts as a variable in the program. For $a \in \{0,1\}^n$, the value of $P(a) = \sum_{S \in \binom{[n]}{\leq d}} \alpha_S \cdot 1_{S \subseteq a}$. Note that we can rewrite this expression as the inner-product of α with the column of $M(n,d)$ indexed by a. We treat Z as an indeterminate, and collect the constraints over all $a \in \{0,1\}^n$ as the following linear program:

$$\begin{array}{ll} \min_{\alpha} & \epsilon \\ \text{such that} & \left|\alpha^T M(n,d) - Z - \frac{f}{2}\right| \leq \epsilon \\ & \alpha \in \mathbb{R}^{\binom{n}{\leq d}} \end{array}$$

Now, P is a torus polynomial that ε-approximates f if and only if the program above achieves an objective of ε for some Z. Hence, our goal is to prove that all the programs above achieve an optimal objective value more than ε. We use standard tools from the theory of linear programming, and write the dual of these programs as follows.

$$\begin{array}{ll} \max_{\gamma} & \left\langle \gamma, Z + \frac{f}{2} \right\rangle \\ \text{such that} & \gamma \in nullspace(M(n,d)) \\ & \|\gamma\|_1 = 1 \end{array}$$

Using strong duality, the non-existence of P is equivalent to the statement that each dual above achieves an objective more than ε. To finish the proof, note that the conditions $\left\langle \gamma, Z + \frac{f}{2} \right\rangle > \varepsilon$ and $\|\gamma\|_1 = 1$ together are equivalent to the condition $\left\langle \gamma, Z + \frac{f}{2} \right\rangle > \varepsilon \|\gamma\|_1$. Finally, if $\left|\left\langle \gamma, Z + \frac{f}{2} \right\rangle\right| > \varepsilon \|\gamma\|_1$, then either $\left\langle \gamma, Z + \frac{f}{2} \right\rangle > \varepsilon \|\gamma\|_1$ or $\left\langle -\gamma, Z + \frac{f}{2} \right\rangle > \varepsilon \|-\gamma\|_1$ holds, which suffices for our purpose. This completes the proof. □

3 Plan for Majority

In this section, we set up a program towards proving Conjecture 2. Fix the function for this section $f = \mathsf{MAJORITY}$, some large enough $n \in \mathbb{N}$, any $d \leq O\left(\sqrt{\frac{n}{\log(n)}}\right)$, and $\varepsilon = \frac{1}{20n}$. Call a function $Z : \{0,1\}^n \to \mathbb{Z}$ *good*, if there is a witness $\gamma \in nullspace(M(n,d))$ such that:

$$\left|\left\langle Z + \frac{\mathsf{MAJORITY}}{2}, \gamma \right\rangle\right| > \varepsilon \|\gamma\|_1$$

In other words, Z is good, if we can prove that the dual corresponding to Z is feasible. Conjecture 2 posits that all Zs are good. In this language, the lower bound result by Bhrushundi, Hosseini, Lovett and Rao [BHLR19, Corollary 3.3] states that all *symmetric* Zs are good.

Now, the challenge is that we need to argue about infinitely many Zs, and find a feasible solution γ from the vector space $nullspace(M(n,d))$, which is also infinite. The latter is easy to fix using the theory of linear programming, as we can choose γ from the set of *basic solutions*, which is a finite set. Therefore, we focus on the set of good Zs, and show that it is cofinite. In other words, we show that all Zs, except for a finite set, are good.

Towards this goal, we first make an observation that allows us to consider Zs as functions over a smaller domain. Consider two functions Z and Z', such that $Z - Z' \in row\text{–}span(M)$. Then, $\langle Z, \gamma \rangle$ equals $\langle Z', \gamma \rangle$ for any $\gamma \in nullspace(M)$. Hence, if Z is good, then any Z' such that $Z - Z' \in row\text{–}span(M)$ is also good. Therefore, define the relation $Z \sim Z'$ if $Z - Z' \in row\text{–}span(M)$, which is an equivalence relation. We can pick a representative Z from each equivalence class of the relation, and it suffices to prove that the representative Z is good. The following statement formalizes this intuition.

Lemma 3.1. *Consider a polynomial $P \in \mathbb{R}[X_1, \ldots, X_n]$ of degree at most d. Then, there exists a polynomial $P' \in \mathbb{R}[X_1, \ldots, X_n]$ of degree at most d, satisfying the following conditions:*

- *If P ε-approximates f, then P' also ε-approximates f.*
- *If Z' denotes the integer part of P', then $Z'(a) = 0$ for any a with $|a| \leq d$.*

Proof. The proof follows from an inductive procedure, where we start with $|a| = 0$, and end after considering $|a| = d$. The initial polynomial P is of the form

$$P = \sum_{S \in \binom{[n]}{\leq d}} c_S X^S$$

As we perform our inductive procedure, after considering the case of $|a| = i$, we will obtain a polynomial P_i, which will satisfy the following conditions:

- P_i has degree at most d.
- For any $a \in \{0,1\}^n$, $P(a) - P_i(a)$ is an integer.
- If P is a torus polynomial that ε-approximates f, then, for any $a \in \{0,1\}^n$ with $|a| \leq i$,

$$P_i(a) \in \left[-\varepsilon + \frac{f(a)}{2}, \varepsilon + \frac{f(a)}{2} \right].$$

For a point $a \in \{0,1\}^n$, $P(a) = \sum_{S \subseteq a} c_S$. The crucial observation for this inductive procedure is that, if $|a| \leq i$, then, the expression for $P(a)$ only depends on S such that $|S| \leq i$. Therefore, any change to a coefficient c_S with $|S| = i$ does not affect $P(a)$ with $|a| < i$.

For the base case, consider the all zeros point, $a = 0$. Modify P by subtracting $m_0 = \left\lfloor P(0) - \frac{f(0)}{2} \right\rceil$ from it, to get P_0. Note that P_0 is as desired.

For the inductive step, say P_i satisfies all the three conditions listed above. For each point a with $|a| = i+1$, subtract $m_a = \left\lfloor P_i(a) - \frac{f(a)}{2} \right\rceil \prod_{i \in a} X_i$ from P_i. After subtracting each m_a, denote the obtained polynomial as P_{i+1}. One can verify easily that P_{i+1} satisfies the required conditions for the inductive procedure.

The final polynomial $P' = P_d$ has the desired properties to complete the proof. □

Henceforth, we will always assume that $Z(a) = 0$ for any $a \in \{0,1\}^n$ with $|a| \leq d$. Now, we begin the task of proving that certain Zs are good. We will produce the vectors we need for this task using the following construction, which is only a minor generalization of the construction from [BT15].

Construction 2. *Construct a vector γ as follows.*

Input:

- *two natural numbers $n \in \mathbb{N}$ and $d \in [n-1]^*$,*
- *two subsets $S_1, S_2 \subseteq [n]$, such that $S_1 \subseteq S_2$, and $|S_2 \setminus S_1| \geq d+1$,*
- *a set $I \subseteq [|S_2 \setminus S_1|]^*$ of size $|I| = d+2$.*

Output: *A vector $\gamma \in \mathbb{R}^{2^n}$.*

Construction: *First, define a univariate polynomial $q_I(t) = \prod_{i \in [k]^* \setminus I}(t-i)$, where $k = |S_2 \setminus S_1|$. For any set T, if $S_1 \subseteq T \subseteq S_2$, keep $\gamma_T = (-1)^{|T|} q_I(|T \setminus S_1|)$. Otherwise, keep $\gamma_T = 0$.*

Output γ.

We claim that the construction produces a vector in $nullspace(M(n,d))$. The proof is similar to the proof of [BT22, Lemma 31], we present it here for the sake of completeness.

Lemma 3.2. *Consider any $n \in \mathbb{N}$, $d \in [n-1]^*$, $S_1, S_2 \subseteq [n]$ such that $S_1 \subseteq S_2$ and $|S_2 \setminus S_1| \geq d+1$, and $I \subseteq [|S_2 \setminus S_1|]^*$ of size $|I| = d+2$. Then, Construction 2, on input n, d, S_1, S_2 and I, outputs a vector $\gamma \in nullspace(M(n,d))$.*

Proof of Lemma 3.2. We follow along the proof of [BT22, Lemma 31]. For simplicity, consider the case when $S_1 = \emptyset, S_2 = [n]$. Choose any set $I \subseteq [n]^*$ of size $|I| = d+2$. Construct γ as described in the statement, using Construction 2. We need to prove that $M\gamma = 0$.

Consider any row of M as a vector $\mathbf{m}$. We need to prove that $\langle \mathbf{m}, \gamma \rangle = 0$. Recall the construction for M, from Construction 1. Say $\mathbf{m}$ is the row of M indexed by $S \subseteq [n]$. Then, $\mathbf{m}$ corresponds to the evaluations of the monomial $\prod_{i \in S} x_i$ over all Boolean points. Note that $|S| \leq d$, hence any monomial we consider here has degree at most d. We abuse notation, and use $\mathbf{m}$ to denote this monomial as well.

To prove $\langle \mathbf{m}, \gamma \rangle = 0$, we expand this expression.

$$\langle \mathbf{m}, \gamma \rangle = \sum_{S \subseteq [n]} \mathbf{m}(S)\gamma(S)$$

Now, notice that γ is a symmetric vector, i.e. $\gamma_{S_1} = \gamma_{S_2}$ if $|S_1| = |S_2|$. Hence, we can rewrite the expression above as:

$$\langle \mathbf{m}, \gamma \rangle = \sum_{t \in [n]^*} \gamma_{[t]} \sum_{S \in \binom{[n]}{t}} m(S)$$

Next, a straightforward calculation yields $\sum_{S \in \binom{[n]}{t}} m(S) = \binom{n-\deg(m)}{t-\deg(m)}$. Moreover, $\gamma_{[t]} = (-1)^t q_I(t)$ as per the construction of γ. Therefore, we get the following expression:

$$\langle \mathbf{m}, \gamma \rangle = \sum_{t \in [n]^*} (-1)^t \binom{n-\deg(m)}{t-\deg(m)} q_I(t)$$

The following commonly-known fact (cf. [BT22, Fact 30]) allows us to complete the proof.

Fact 3 (Folklore)**.** *For any univariate polynomial $p \in \mathbb{R}[t]$ of degree at most $n-d-1$, and any $d' \le d$, the following holds:*

$$\sum_{t=0}^{n}(-1)^t\binom{n-d'}{t-d'}p(t)=0$$

To see why this fact is useful, just note that $\deg(m) \le d$, and q_I has degree $n-d-1$.
The general case of S_1, S_2, I follows similarly. We leave the proof to the reader. □

Using these vectors constructed above, we prove an upper bound on the value of each $Z(a)$. In other words, for each a we describe an upper bound, such that if $Z(a)$ violates this bound, then Z is good. The reader may think of this as an upper bound on an appropriately defined weighted ℓ^∞-norm of Z.

Theorem 3.3. *Choose a large enough $n \in \mathbb{N}$. Consider a torus polynomial P, of degree at most $d < \frac{n}{2}$, that approximates $f = \mathsf{MAJORITY}$ within an error of ε. Then, the following holds for any $a \in \{0,1\}^n$ and the function Z corresponding to P:*

$$|Z(a)| \le \varepsilon 2^{d+1}\binom{|a|}{d+1}$$

In other words, if $|Z(a)| > \varepsilon 2^{d+1}\binom{|a|}{d+1}$ for some $a \in \{0,1\}^n$, then Z is good.

The statement above holds for any f such that $f(a)=0$ for each $a \in \binom{[n]}{\le d}$, e.g. $f = \mathsf{AND}$[5]*.*

Proof. Consider a set S of size $|S| = k \ge d+1$. Construct a ray $\overline{\gamma} \in null(M)$ using Construction 2 with $S_1 = \emptyset, S_2 = S$ and $I = [d]^* \cup \{k\}$. The values we need to compare are $\left\langle Z + \frac{f}{2}, \overline{\gamma} \right\rangle$ and $\varepsilon\|\overline{\gamma}\|_1$. Note that $Z(a) = f(a) = 0$ for any a with $|a| \le d$. Hence, $\left\langle \overline{\gamma}, Z + \frac{f}{2} \right\rangle = \overline{\gamma}_S\left(Z(S) + \frac{f(S)}{2}\right)$. Therefore, if $\left|Z(S) + \frac{f(S)}{2}\right| > \frac{\varepsilon\|\overline{\gamma}\|_1}{|\overline{\gamma}_S|}$, then Z is good.

For a set $T \subseteq S$ of size $|T| \in \{d+1, \ldots, k-1\}$, $\overline{\gamma}_T = 0$ by construction. Then, $|\overline{\gamma}_S| = \prod_{i=1}^{k-(d+1)} i = (k-d-1)!$. Finally, for a set $T \subseteq S$ of size $|T| = t \le d$, $|\overline{\gamma}_T| = \prod_{i=d+1}^{k-1}(i-t) = \frac{(k-1-t)!}{(d-t)!}$. Note that there are $\binom{k}{t}$ such sets T.

Hence, $\|\overline{\gamma}\|_1 = (k-d-1)! + \sum_{t=0}^{d}\binom{k}{t}\frac{(k-1-t)!}{(d-t)!}$. Dividing by $|\overline{\gamma}_S|$, we get:

$$\begin{aligned}
\frac{\|\overline{\gamma}\|_1}{|\overline{\gamma}_S|} &= 1 + \sum_{t=0}^{d}\binom{k}{t}\frac{(k-1-t)!}{(d-t)!(k-d-1)!} && = 1 + \sum_{t=0}^{d}\frac{k!}{t!(d-t)!(k-d-1)!(k-t)} \\
&= 1 + \binom{k}{d+1}\sum_{t=0}^{d}\binom{d}{t}\frac{d+1}{k-t} && \le 1 + \binom{k}{d+1}\sum_{t=0}^{d}\binom{d}{t}\frac{d+1}{d+1-t} \\
&= 1 + \binom{k}{d+1}\sum_{t=0}^{d}\binom{d+1}{t} && = 1 + \binom{k}{d+1}\left(2^{d+1}-1\right) \\
&\le 2^{d+1}\binom{k}{d+1}
\end{aligned}$$

This proves the claim as desired. □

[5] As noted by an anonymous ITCS 2026 reviewer.

With the previous result, we have only a finite set of Zs remaining, that we need to prove are good. Now, we argue that we only need to look at a few values of $Z(a)$ to figure out the rest of them. This reduces the degrees of freedom for the family of linear programs we study, from 2^n to a small fraction of 2^n. To that effect, we introduce the following definition.

Definition 2 (ε-isolator)**.** *A vector $\gamma \in nullspace(M(n,d))$ is defined to be an* ε-isolator *for a set $a \subseteq [n]$ if the following holds: Given values of $Z(b) \in \mathbb{Z}$ for every $b \subsetneq a$, there is at most one value $z_a \in \mathbb{Z}$ for $Z(a)$ such that $\left|\left\langle Z + \frac{f}{2}, \gamma \right\rangle\right| \leq \varepsilon \|\gamma\|_1$.*

In other words, if $Z(a) \neq z_a$, then Z is good with γ as the witness.

We show that for large enough n and any $d < \sqrt{n} - 1$, any point a with $|a| \geq (d+1)^2$ has an ε-isolator for $\varepsilon = \frac{1}{20n}$. Note that if $d = O(\sqrt{n})$ is small enough, then a large fraction of points a have an ε-isolator, hence, reducing the degrees of freedom. The formal statement is as follows.

Theorem 3.4. *For any large enough $n \in \mathbb{N}$, any $d < \sqrt{n} - 1$, and $\varepsilon = \frac{1}{20n}$, any $a \in \{0,1\}^n$ with $|a| \geq (d+1)^2$ has an ε-isolator.*

The above statement follows from the statement below.

Theorem 3.5. *For any large enough $n \in \mathbb{N}$, any $d < \sqrt{n} - 1$, and $\varepsilon = \frac{1}{20n}$, the following holds: Fix values of $Z(b)$ for each point $b \in \{0,1\}^n$ with $|b| < (d+1)^2$. Then, consider a point $a \in \{0,1\}^n$ with $|a| \geq (d+1)^2$. For each $a' \subseteq a$ with $|a'| = |a| - (d+1)^2$, define the following rational number:*

$$R_{a,a'} = 2\sum_{i=1}^{d+1} (-1)^i \frac{\binom{d+1}{i}}{\binom{d+i+1}{i}} \left(\frac{\sum_{a' \subseteq b \subseteq a : |b| = |a| - i^2} Z(b) + \frac{f(b)}{2}}{\binom{(d+1)^2}{i^2}} \right)$$

If the following holds for any a':

$$\left| Z(a) + R_{a,a'} + \frac{f(a)}{2} \right| > \frac{1}{\sqrt{n}}$$

Then, Z is good. Note that all choices of $Z(a) \in \mathbb{Z}$, except for possibly a single choice, lead to a good Z. In other words, $Z(a)$ is uniquely determined.

Before we begin the proof, we would like to explain the expression in simple words as it may look complicated at first glance. First, the expression only looks at $Z(b) + \frac{f(b)}{2}$ where b belongs to the Hamming sub-cube between a' and a. The expression $\frac{\sum_{a' \subseteq b \subseteq a : |b| = |a| - i^2} Z(b) + \frac{f(b)}{2}}{\binom{(d+1)^2}{i^2}}$ is simply the average over the Hamming layer at distance i^2 below a. This average is multiplied with the coefficient $2 \cdot (-1)^i \frac{\binom{d+1}{i}}{\binom{d+i+1}{i}}$ to obtain the expression. Now, we begin the proof.

Proof. Fix a point $a \in \{0,1\}^n$ with $|a| \geq (d+1)^2$, and choose a subset $a' \subseteq a$ with $|a'| = |a| - (d+1)^2$. Use Construction 3.2 with $n, d, S_1 = a', S_2 = a, I = \left\{(d+1)^2 - i^2 : i \in [d+1]^*\right\}$, to obtain $\overline{\gamma} \in nullspace(M)$. We denote the polynomial q_I from the construction by q for brevity.

Now, assume that the condition from the statement holds, which is as follows:

$$\left| Z(a) + R_{a,a'} + \frac{f(a)}{2} \right| > \frac{1}{\sqrt{n}} \tag{1}$$

Then, we claim that Z is good, with $\overline{\gamma}$ as the witness, i.e.,

$$\left|\left\langle Z + \frac{f}{2}, \overline{\gamma} \right\rangle\right| > \varepsilon \|\overline{\gamma}\|_1 \tag{2}$$

To see why 1 implies 2, consider the following equalities:

$$\left\langle Z + \frac{f}{2}, \overline{\gamma} \right\rangle = \sum_{b \in \{0,1\}^n} \left(Z(b) + \frac{f(b)}{2}\right) \overline{\gamma}_b \tag{3}$$

$$= \sum_{a' \subseteq b \subseteq a} \left(Z(b) + \frac{f(b)}{2}\right) \overline{\gamma}_b \tag{4}$$

$$= \sum_{i=0}^{d+1} (-1)^{i^2} q((d+1)^2 - i^2) \sum_{a' \subseteq b \subseteq a : |b| = |a| - i^2} \left(Z(b) + \frac{f(b)}{2}\right) \tag{5}$$

Equality 3 follows by expanding the expression. Note that $\overline{\gamma}_b = 0$ for any b with either $a' \not\subseteq b$ or $b \not\subseteq a$, as per the construction of $\overline{\gamma}$. Hence, equality 4 follows. Finally, we substitute the values of $\overline{\gamma}_b$ to obtain equality 5.

Now, to calculate the RHS of inequality 2, expand the ℓ^1-norm of $\overline{\gamma}$ as $\|\overline{\gamma}\|_1 = \sum_{i=0}^{d+1} \binom{(d+1)^2}{i^2} \left|q((d+1)^2 - i^2)\right|$. We divide the expression of the inner-product, as well as the ℓ^1-norm, to modify inequality 2 as:

$$\left|\sum_{i=0}^{d+1} \frac{q((d+1)^2 - i^2)}{q((d+1)^2)} \left(\sum_{\substack{a' \subseteq b \subseteq a \\ |a| - |b| = i^2}} Z(b) + \frac{f(b)}{2} \right)\right| > \varepsilon \sum_{i=0}^{d+1} \binom{(d+1)^2}{i^2} \frac{\left|q((d+1)^2 - i^2)\right|}{q((d+1)^2)} \tag{6}$$

Note that $q((d+1)^2) > 0$, hence, dividing by $q((d+1)^2)$ does not change the direction of the inequality. Next, we calculate $\binom{(d+1)^2}{i^2} \frac{q(i^2)}{q((d+1)^2)}$ as follows. Recall the expression for $q(t) = q_I(t) = \prod_{i \in [(d+1)^2]^* \setminus I} (t - i)$. Hence, we get the following expression for $\binom{(d+1)^2}{i^2} \frac{q((d+1)^2 - i^2)}{q((d+1)^2)}$:

$$\begin{aligned}
\binom{(d+1)^2}{i^2} \frac{q((d+1)^2 - i^2)}{q((d+1)^2)} &= \binom{(d+1)^2}{i^2} \frac{\prod_{j \in [(d+1)^2]^* \setminus I} ((d+1)^2 - i^2 - j)}{\prod_{j \in [(d+1)^2]^* \setminus I} ((d+1)^2 - j)} \\
&= \binom{(d+1)^2}{i^2} \frac{\prod_{j \in [(d+1)^2 - 2, (d+1)^2 - 3, \ldots, 1]} ((d+1)^2 - i^2 - j)}{\prod_{j \in [(d+1)^2 - 2, (d+1)^2 - 3, \ldots, 1]} ((d+1)^2 - j)} \\
&= \binom{(d+1)^2}{i^2} \frac{\prod_{j \in [2,3,5,\ldots,(d+1)^2 - 1]} (j - i^2)}{\prod_{j \in [2,3,5,\ldots,(d+1)^2 - 1]} (j)} \\
&= \frac{\prod_{j \in [d+1]} j^2}{\prod_{j \in [d+1]^* \setminus \{i\}} (j - i)(j + i)} = (-1)^i \cdot 2 \cdot \frac{\binom{d+1}{i}}{\binom{d+i+1}{i}}
\end{aligned}$$

The calculation here is similar to the calculation performed in Section 6.1 of [BT22], following Fact 32 in the survey. Now, this calculation allows us to infer the following upper bound on the absolute value of the final ratio, for any $i \in [d+1]$:

$$\left|\binom{(d+1)^2}{i^2} \frac{q((d+1)^2 - i^2)}{q((d+1)^2)}\right| \leq 2$$

Hence, we get that the RHS of inequality 6 is at most $\sum_{i=0}^{d+1} 2 = 2(d+2) \leq 4\sqrt{n}$ for large enough n. Also, with a little rearrangement, the LHS of inequality 6 equals $\left|Z(a) + R_{a,a'} + \frac{f(a)}{2}\right|$. Therefore, if $\left|\left\langle Z + \frac{f}{2}, \overline{\gamma}\right\rangle\right| = \left|Z(a) + R_{a,a'} + \frac{f(a)}{2}\right| > \frac{1}{\sqrt{n}} \geq \frac{1}{20n} 4\sqrt{n} \geq \varepsilon\|\gamma\|_1$ holds, then Z is good, with $\overline{\gamma}$ as the witness. This completes the proof. □

3.1 Proposed Directions

Finally, we pose the question to extend the set of good Zs.

Open Problem 1. *Find witnesses to extend the set of good Zs.*

For example, can one find feasible solutions to prove that any Z with $\{-1, 0, 1\}$ as its range is good?

Open Problem 2. *Prove that any $Z : \{0,1\}^n \to \{-1, 0, 1\}$ is good.*

Such statements will complement Theorem 3.3, as they will prove lower bounds on the values of Z. We believe that finding more structure in $nullspace(M(n, d))$ will help toward these problems. To that effect, we present a simple construction for vectors in $nullspace(M(n, d))$, which we could not find in current literature.

Construction 3. *Fix some $n \in \mathbb{N}$, $d \in \mathbb{N}$ such that $d < \left\lfloor \frac{n}{2} \right\rfloor$, and $k \in \mathbb{N}$ such that $d < k < n - d$. Construct a vector $\gamma \in \mathbb{R}^{2^n}$, indexed by $2^{[n]}$, as follows:*

If the indexing set T has size $|T| \neq k$, then set $\gamma_T = 0$. Otherwise, for each $i \in [d+1]$, check whether $|T \cap \{i, d+1+i\}| = 1$. If the check above fails for some $i \in [d+1]$, set $\gamma_T = 0$.

Otherwise, T intersects exactly once with each pair $\{i, d+1+i\}$. Then, set $\gamma_T = (-1)^{|T \cap [d+1]|}$.

Output γ.

We claim that the construction above produces a vector $\gamma \in nullspace(M(n, d))$. The proof follows by a simple argument, which we present below.

Lemma 3.6. *For any $n \in \mathbb{N}, d \in \mathbb{N}$ and $k \in \mathbb{N}$, such that $d < k < n - d$, Construction 3 produces a vector $\gamma \in nullspace(M(n, d))$.*

Proof. To show that $\gamma \in nullspace(M(n, d))$, we need to prove that each of its rows is orthogonal to γ. Hence, for each row indexed by a set $S \in \binom{[n]}{\leq d}$, we need to show that $\sum_{T \in 2^{[n]}} 1_{S \subseteq T} \cdot \gamma_T = \sum_{S \subseteq T} \gamma_T = 0$. Note that for sets T with size $|T| \neq k$, we have $\gamma_T = 0$ as per the construction. Hence, we can simplify the expression further as $\sum_{S \subseteq T : |T| = k} \gamma_T = 0$.

We break the analysis in two cases.

1. $|S| = d$. In this case, we need to consider two possibilities, based on the intersection of S with $\{i, i + d + 1\}$ pair for each $i \in [d + 1]$.

   - Consider the case when S intersects with some $\{i_0, i_0 + d + 1\}$ pair twice. Then, any set T containing S will also intersect $\{i_0, i_0 + d + 1\}$ twice. Hence, $\gamma_T = 0$ for any T containing such a set S. Therefore, $\sum_{S \subseteq T} \gamma_T = 0$.
   - Consider the case when S intersects at most once with each $\{i, i+d+1\}$ pair for $i \in [d+1]$. Then, as $|S| = d = k - 1$, there is exactly one pair $\{i_0, i_0 + d + 1\}$ with which S does not intersect.

     Consider any set T containing S, with size $|T| = k$. If T does not intersect $\{i_0, i_0+d+1\}$, then $\gamma_T = 0$ by construction. Otherwise, either $i_0 \in T$, $i_0 + d + 1 \in T$, or both. If both

$i_0 \in T$ and $i_0 + d + 1 \in T$, then $\gamma_T = 0$ by construction. Hence, we only consider the case when either $i_0 \in T$ or $i_0 + d + 1 \in T$, but not both.
If $i_0 \in T$, then $\gamma_T = (-1)^{|T| \cap [d+1]} = (-1)^{|S \cap [d+1]|+1}$. Otherwise, if $i_0 + d + 1 \in T$, then $\gamma_T = (-1)^{|S \cap [d+1]|}$. Moreover, both the cases occur for exactly the same number of sets T. Hence, $\sum_{S \subseteq T} \gamma_T = 0$.

2. $|S| = s$, where $s < d$. Our goal in this case is to prove $\sum_{S \subseteq T : |T| = k} \gamma_T = 0$ indirectly using the previous case. To that effect, we compare this expression with $\sum_{S \subseteq S' : |S'| = d} \sum_{S' \subseteq T : |T| = k} \gamma_T$. We claim that the latter expression is a multiple of the former.

   To see why, consider a fixed T. We can remove any element of $T \setminus S$ from T to obtain S' in $k - s$ ways. Then, the way to obtain S from S' is unique, which is to remove all elements of $S' \setminus S$. Hence, we get that

$$(k - s) \cdot \sum_{S \subseteq T : |T| = k} \gamma_T = \sum_{S \subseteq S' : |S'| = d} \sum_{S' \subseteq T : |T| = k} \gamma_T$$

   Now, from the previous case, we have that $\sum_{S' \subseteq T : |T| = k} \gamma_T = 0$ for any S' with $|S'| = d$. Hence, $\sum_{S \subseteq T : |T| = k} \gamma_T = 0$ as well.

The proof is complete. □

Intuitively speaking, the construction above produces a vector with balanced -1 and 1 entries on the given Hamming layer. Hence, it may help with Zs that are highly unbalanced along the entries of this vector. We leave it open to characterize the set of Zs that can be ruled out based on this vector.

Open Problem 3. *Characterize the set of good Zs witnessed by the vector from Construction 3.*

4 Lower Bounds for AND

In this section, we prove a lower bound for torus polynomials approximating AND. We restate the result below.

Theorem 1.3. *Any torus polynomial, that ε-approximates* AND*, must have degree $\Omega\left(\log\left(\frac{1}{\varepsilon}\right)\right)$.*

We plan to use Theorem 2.1 to prove this result. In this task, the main challenge is that there are infinitely many choices for Z, and we need to find a feasible solution γ for each choice. To make this task easier, we find a vector $\gamma \in nullspace(M(n, d))$ with integer entries and small ℓ^1-norm. This vector will serve as a feasible solution for any Z, if it satisfies the conditions that we detail in the next statement.

Lemma 4.1. *Fix a Boolean function $f : \{0,1\}^n \to \{0,1\}$ and some $d \in [n-1]$. Consider a vector $\gamma \in nullspace(M(n, d))$ with integer entries, i.e. $\gamma \in \mathbb{Z}^{2^n}$, such that $\langle f, \gamma \rangle$ is an* odd *integer. Then, for any $Z : \{0,1\}^n \to \mathbb{Z}$ and $\varepsilon < \frac{1}{2\|\gamma\|_1}$, the following holds:*

$$\left| \left\langle Z + \frac{f}{2}, \gamma \right\rangle \right| > \varepsilon \|\gamma\|_1$$

Proof. Let $\langle f, \gamma \rangle = 2z + 1$ for some integer $z \in \mathbb{Z}$. Then, $\left\langle \frac{f}{2}, \gamma \right\rangle = z + \frac{1}{2}$. Fix a function $Z : \{0,1\}^n \to \mathbb{Z}$. Then, $\langle Z, \gamma \rangle = z'$ for some integer $z' \in \mathbb{Z}$. Hence, $\left\langle Z + \frac{f}{2}, \gamma \right\rangle = z' + z + \frac{1}{2}$. Consider the following two cases:

- $z + z' \geq 0$. In this case, $\left\langle Z + \frac{f}{2}, \gamma \right\rangle \geq \frac{1}{2}$.
- $z + z' \leq -1$. In this case, $\left\langle Z + \frac{f}{2}, \gamma \right\rangle \leq -\frac{1}{2}$.

In both the cases, we observe that $\left|\left\langle Z + \frac{f}{2}, \gamma \right\rangle\right| \geq \frac{1}{2}$. Note that by the choice of $\varepsilon < \frac{1}{2\|\gamma\|_1}$, we have $\varepsilon\|\gamma\|_1 < \frac{1}{2}$. This completes the proof. □

To use the preceding statement for $f = \mathsf{AND}_n$, we proceed as follows. For a vector $\gamma \in nullspace(M)$, its inner product with AND_n is $\langle \gamma, \mathsf{AND}_n \rangle = \gamma_{[n]}$. Hence, we need a vector $\gamma \in nullspace(M) \cap \mathbb{Z}^{2^n}$, such that $\gamma_{[n]}$ is odd and $\|\gamma\|_1$ is not too large. We find this vector in a basis for $nullspace(M)$, we will find the basis useful later, such that each vector in that basis is integral and has a small enough ℓ^1-norm. One such vector $\overline{\gamma}$ in this basis will have $\left|\overline{\gamma}_{[n]}\right| = 1$. We present the construction below.

Construction 4. *Construct a matrix B as follows.*

> ***Input**: $n, d \in [n-1]$.*
>
> ***Output**: A matrix $B \in \mathcal{M}_{2^n \times \binom{n}{>d}}(\mathbb{R})$.*
>
> ***Construction**: For any set $S \subseteq [n]$ with $|S| \geq d+1$, consider its elements $(s_0, s_1, \ldots, s_{|S|-1})$ in the increasing order $s_0 < s_1 < \ldots < s_{|S|-1}$. Denote $S[> d] = \{s_{d+1}, \ldots, s_{|S|-1}\}$ as the set remaining after ignoring the first d elements.*
>
> *Now, create a matrix B, of size $2^n \times \binom{n}{>d}$, and index its rows by elements of $2^{[n]}$ and columns by elements of $\binom{[n]}{>d}$. For $1 \leq i \leq 2^n$ and $1 \leq j \leq \binom{n}{>d}$, set the corresponding entry of B as $B_{i,j} = (-1)^{|S_i|+|S_j|} \cdot 1_{S_i \subseteq S_j} \cdot 1_{S_j[>d] \subseteq S_i}$. Here, S_i and S_j denote the sets indexing the i^{th} row and the j^{th} column of B, respectively.*
>
> *Output B.*

We claim that, when given n and d as input, the construction above produces a basis $B(n,d)$ for $nullspace(M(n,d))$. To prove the claim, we plan to use an extension trick. Consider the matrix $D(n)$ of size $2^n \times 2^n$ where $D_{i,j} = 1_{S_i \subseteq S_j}$. This extends the matrix $M(n,d)$ to a square matrix. Note that $D(n)$ is an upper triangular matrix with 1s on the diagonal. Hence, it has full rank. Therefore, the following statement follows easily, which we state without proof.

Lemma 4.2. *A basis $B'(n,d)$ for $nullspace(M(n,d))$ consists of the last $\binom{n}{>d}$ columns of $D(n)^{-1}$.*

Now, we describe $D(n)^{-1}$ explicitly. This is simply the Möbius function over the Boolean hypercube. We prove its correctness for the sake of completeness.

Lemma 4.3. *For $1 \leq i, j \leq 2^n$, $D(n)^{-1}_{i,j} = (-1)^{|S_i|+|S_j|} \cdot 1_{S_i \subseteq S_j}$.*

Proof. Towards a proof, consider $(DD^{-1})_{k,i} = \sum_{j=1}^{2^n} 1_{S_k \subseteq S_j} (-1)^{|S_i|+|S_j|} 1_{S_j \subseteq S_i}$. If $k = i$, the only non-zero entry on the RHS is when $S_j = S_i = S_k$, which is 1, therefore $(DD^{-1})_{i,i} = 1$. When $k > i$, there is no subset S_j such that $S_j \subseteq S_i$ and $S_k \subseteq S_j$, therefore $(DD^{-1})_{k,i} = 0$.

For $k < i$, consider two cases.

- Let $S_k \subseteq S_i$ with $|S_i| = |S_k| + m$ where $m \geq 1$. Then, for any $0 \leq m' \leq m$, there are $\binom{m}{m'}$ many sets such that $|S_j| = |S_k| + m'$ and $S_k \subseteq S_j \subseteq S_i$. Hence, $DD^{-1}_{k,i} = \sum_{m'=0}^{m} (-1)^{m'} \binom{m}{m'} = 0$.

- Let $S_k \not\subseteq S_i$. Consider any set S_j such that $S_k \subseteq S_j$. Then, there is $s \in S_j$ such that $s \notin S_i$. Hence, $S_j \not\subseteq S_i$. Similarly, if $S_j \subseteq S_i$, then $S_k \not\subseteq S_j$. Therefore, $DD^{-1}_{k,i} = 0$.

This completes the proof. ■

By combining Lemma 4.2 and Lemma 4.3, we get a basis $B'(n,d)$ for $nullspace(M(n,d))$. Now, we prove that $B(n,d) = B'(n,d)R(n,d)$ for some square matrix R with full rank. This implies that $B(n,d)$ and $B'(n,d)$ have the same rank. The proof of this statement is a straightforward calculation, which we omit.

Lemma 4.4. *For any set $S \subseteq [n]$, define $S[\leq d] = S \setminus S[> d]$. Consider the following matrix $R(n,d)$ of $\binom{n}{>d} \times \binom{n}{>d}$ dimensions. For any $\binom{n}{\leq d} + 1 \leq i,j \leq 2^n$, the corresponding entry is $R(n,d)_{i-\binom{n}{\leq d},j-\binom{n}{\leq d}} = 1_{S_i \subseteq S_j} \cdot 1_{(S_j[\leq d]) \subseteq S_i}$. Then, $B(n,d) = B'(n,d)R(n,d)$.*

The statement above allows us to prove the claim that $B(n,d)$ is a basis for $nullspace(M(n,d))$.

Claim 4.5. *Construction 4, on input $n, d \in [n-1]$, outputs a basis for $nullspace(M(n,d))$.*

We use this basis to prove Theorem 1.3 as follows.

Proof of Theorem 1.3. First, construct B using Construction 4, with n and d as the inputs to the construction. Now, denote by $\overline{\gamma}$ the column of B indexed by $[n]$. Clearly, $\left|\overline{\gamma}_{[n]}\right| = 1$, hence, $\langle \mathsf{AND}, \overline{\gamma} \rangle$ is an odd integer. Moreover, $\|\overline{\gamma}\|_1 = 2^{d+1}$. Therefore, if we apply Lemma 4.1, we get the following lower bound for $\varepsilon < \frac{1}{2 \cdot 2^{d+1}}$: any torus polynomial that ε-approximates the AND function must have degree more than d. This completes the proof. □

Remark 1. *Consider the probabilistic polynomial that approximates AND over $\mathbb{F}_2$ with probability ε, from [Raz87], and combine it with [BHLR19, Lemma 14]. Then, one gets the following upper bound on $\overline{\deg}_\varepsilon(\mathsf{AND})$.*

Lemma 4.6 ([BHLR19, Raz87])**.** *For any $\varepsilon > 0$, $\overline{\deg}_\varepsilon(\mathsf{AND}) \leq \log^2\left(\frac{n}{\varepsilon}\right)$.*

Hence, the lower bound we have proved in Theorem 1.3 is only quadratically away from the upper bound for any $\varepsilon = \frac{1}{n^{\Omega(1)}}$.

Although we had infinitely many linear programs to work with, we have only used one vector for proving their feasibility. One could use multiple vectors in $nullspace(M(n,d))$, such that for each dual corresponding to $Z \in \mathbb{Z}^{2^n}$, one of these vectors is a feasible solution. By using multiple vectors, we believe that one can get stronger degree lower bounds, bringing it closer to the upper bound. We leave this task as an open problem.

Open Problem 4. *Bridge the gap between the lower and upper bound for the AND function.*

4.1 The Very Small Error Case

The literature on polynomial approximations usually focuses on inverse-polynomial error regime. We study the case where the error is very small, as it allows us to partially answer a question posed in [BHLR19, Problem 6]. In [BHLR19, Problem 6], the authors ask about the relationship between $\overline{\deg}_{\frac{1}{3}}(f)$ and $\overline{\deg}_\varepsilon(f)$. In general, one can ask if there is an error-reduction procedure for torus polynomials. This procedure should take as input $\varepsilon, \varepsilon' < \varepsilon, \overline{\deg}_\varepsilon(f)$, and output an estimate for $\overline{\deg}_{\varepsilon'}(f)$. Ideally, the output should not depend on f, and the estimate should be reasonably close to optimal.

In what follows, we prove that torus polynomials require the same degree to approximate AND and MAJORITY when the error is very small. Now, if we assume Conjecture 2, then the degree required to $\frac{1}{20n}$-approximate AND is much smaller than the degree required for MAJORITY. Hence, any error-reduction procedure as described above will produce a suboptimal output if it does not depend on the function being approximated, conditionally answering [BHLR19, Problem 6] for the error-regime $\varepsilon < \frac{1}{2^{n+1}}$. Formally, we prove the following result.

Theorem 4.7. *Depending on the value of ε, the following cases hold.*

- *If $\varepsilon < \frac{1}{2^{n+1}}$, then the following holds for $f = \mathsf{MAJORITY}$ as well as $f = \mathsf{AND}$, and infinitely many n. Any torus polynomial that ε-approximates f has degree n.*
- *If $\varepsilon \geq \frac{1}{2^{n+1}}$, then the following holds for any Boolean function $f : \{0,1\}^n \to \{0,1\}$. There exists a torus polynomial P of degree at most $n-1$ approximating f within an error of ε. Moreover, if f is symmetric, then we can take P to be symmetric as well.*

Proof. To prove the lower bound, first construct the matrix B using Construction 4, with n and $d = n-1$ as the inputs to the construction. In this case, there is a single vector $\overline{\gamma}$ in the basis, with $\overline{\gamma}_S = (-1)^{|S|}$.

Now, for MAJORITY, we have $\langle \mathsf{MAJORITY}, \overline{\gamma} \rangle = \sum_{i > \frac{n}{2}} (-1)^i \binom{n}{i}$. Consider $n = 2^t$ for some natural number $t \geq 2$. Then, $\binom{n}{i}$ is even for all $1 \leq i \leq n-1$, while $\binom{n}{n} = 1$ is odd. Hence, $\langle \mathsf{MAJORITY}, \overline{\gamma} \rangle$ is odd. Therefore, using Lemme 4.1, the lower bound holds for $\varepsilon < \frac{1}{2\|\overline{\gamma}\|_1} = \frac{1}{2^{n+1}}$.

For AND, simply note that $|\overline{\gamma}_{[n]}| = 1$. Hence, we get the lower bound for AND as well.

To prove the upper bound, we continue with the vector $\overline{\gamma}$ from above. Now, consider any function $f : \{0,1\}^n \to \{0,1\}$, and proceed as follows based on the value of $\langle f, \overline{\gamma} \rangle$.

- **Case 1:** $\langle f, \overline{\gamma} \rangle$ is even.

  In this case, define the function Z, with $Z([n]) = \frac{-\langle f, \overline{\gamma} \rangle}{2}$, and $Z(a) = 0$ otherwise. Then, $\langle Z + \frac{f}{2}, \overline{\gamma} \rangle = 0$.

- **Case 2:** $\langle f, \overline{\gamma} \rangle$ is odd.

  In this case, define the function Z, with $Z([n]) = -\left\lfloor \frac{\langle f, \overline{\gamma} \rangle}{2} \right\rfloor$, and $Z(a) = 0$ otherwise. Then, $\left| \langle Z + \frac{f}{2}, \overline{\gamma} \rangle \right| = \frac{1}{2}$.

In both the case, we have found a Z, such that $\left| \langle Z + \frac{f}{2}, \overline{\gamma} \rangle \right| \leq \frac{1}{2} = \frac{1}{2^{n+1}} \|\overline{\gamma}\|_1$. Now, note that $\overline{\gamma}$ along generates $nullspace(M(n, n-1))$, hence, all vectors in $nullspace(M(n, n-1))$ are multiples of $\overline{\gamma}$. Therefore, for any vector $\gamma \in nullspace(M(n, n-1))$, we have $\left| \langle Z + \frac{f}{2}, \gamma \rangle \right| \leq \varepsilon \|\gamma\|_1$. To complete the proof, note that Theorem 2.1 is an equivalence statement. This proves the upper bound.

Finally, if f is symmetric, then simply note that the Z we have constructed is also symmetric. This suffices to construct a symmetric torus polynomial, we leave the small details to the reader. □

The upper bound above only states the existence of torus polynomials approximating Boolean functions for a tiny error. We leave it as an open problem to explicitly construct them.

Open Problem 5. *For $\varepsilon = \frac{1}{2^{n+1}}$ and a given function $f : \{0,1\}^n \to \{0,1\}$, construct a torus polynomial of degree at most $n-1$ that ε-approximates f.*

5 Lower Bounds for the Symmetric Case

In this section, we prove lower bounds against symmetric torus polynomials approximating symmetric functions. To describe the general method, we proceed along the lines of the proof for Theorem 2.1, with two crucial modifications. The polynomial is symmetric if each monomial of the same degree has the same coefficient, which reduces the number of variables to $d+1$. Similarly, as the function is symmetric, the number of constraints reduces to $n+1$. To describe the much shorter linear program we obtain, we first construct the following matrix.

Construction 5. *Define the matrix $\widehat{M}(n,d)$ of size $(d+1)\times(n+1)$. For $0\le j\le d, 0\le i\le n$, the corresponding entry is $\widehat{M}_{j,i}=\binom{i}{j}$.*

Now, the analogue of Theorem 2.1 for symmetric torus polynomials is as follows. Note that we define symmetric functions with $[n]^*$ as the domain, such that $f(i)$ is the output when the input has Hamming weight i.

Theorem 5.1. *The following statements are equivalent for any n, d, $\varepsilon<\frac{1}{10}$, and any symmetric function $f:[n]^*\to\{0,1\}$.*

- *Any symmetric torus polynomial that ε-approximates f has degree more than d.*
- *For any function $Z:[n]^*\to\mathbb{Z}$, there exists a vector $\psi\in nullspace(\widehat{M}(n,d))$ such that:*

$$\left|\left\langle Z+\frac{f}{2},\psi\right\rangle\right|>\varepsilon\|\psi\|_1$$

The proof of this statement is very similar to the proof of Theorem 2.1, which we skip. The challenge here is also similar, having to deal with infinitely many linear programs, and proving that they are all feasible. We proceed similar to the previous section, by choosing a short enough ψ with integer entries, which gives us the following analogue of Lemma 4.1.

Lemma 5.2. *Fix a symmetric Boolean function $f:[n]^*\to\{0,1\}$ and some $d\in[n]^*$. Consider a vector $\psi\in nullspace(\widehat{M}(n,d))$ with integer entries, i.e. $\psi\in\mathbb{Z}^{n+1}$, such that $\langle f,\psi\rangle$ is an* odd *integer. Then, for any $Z:[n]^*\to\mathbb{Z}$ and $\varepsilon<\frac{1}{2\|\psi\|_1}$, the following holds:*

$$\left|\left\langle Z+\frac{f}{2},\psi\right\rangle\right|>\varepsilon\|\psi\|_1$$

Now, we recall the statement of our main lower bound against symmetric torus polynomial approximations.

Theorem 1.4. *Any symmetric torus polynomial, that $\frac{1}{20n}$-approximates* AND*, must have degree $\Omega\left(\sqrt{\frac{n}{\log(n)}}\right)$.*

Proof. To prove this statement, we claim that for any $d\le O\left(\sqrt{\frac{n}{\log(n)}}\right)$, $nullspace(\widehat{M}(n,d))$ contains a vector $\overline{\psi}$ with ℓ^∞-norm 1. Moreover, the last entry of $\overline{\psi}$ is $\overline{\psi}_n=1$. Hence, its inner product with the AND function is $\langle \mathsf{AND},\overline{\psi}\rangle=1$, which is an odd integer. We state the claim formally below.

Claim 5.3. *For some universal constant c, consider any large enough $n \in \mathbb{N}$ and $d \leq \sqrt{\frac{n}{c\log(n)}}$. Then, nullspace$(M(n,d))$ contains a vector $\overline{\psi}$ with $\|\overline{\psi}\|_\infty = 1$ and $\overline{\psi}_n = 1$.*

Assume, for now, that the claim is true. Then, we have $\langle \mathsf{AND}, \overline{\psi} \rangle = 1$. Further, we get $\|\overline{\psi}\|_1 \leq (n+1)\|\overline{\psi}\|_\infty \leq n+1$. Finally, we use Lemma 5.2, using $\overline{\psi}$, which we can apply for any $\varepsilon \leq \frac{1}{2\|\overline{\psi}\|_1} \leq \frac{1}{2(n+1)}$. Note that our choice of $\varepsilon = \frac{1}{20n}$ satisfies this inequality for large enough n. This completes the proof. □

Remark 2. *Buhrman, Cleve, de Wolf and Zalka [BCDWZ99] proved an upper bound of $O\left(\sqrt{n\log\left(\frac{1}{\varepsilon}\right)}\right)$ on the degree of a real polynomial approximating the* AND *function within an error of ε. Note that we can consider this real polynomial, after symmetrizing, as a symmetric torus polynomial approximating the* AND *function within an error of ε. For $\varepsilon = \frac{1}{O(n)}$, this gives an upper bound of $O(\sqrt{n\log(n)})$ on the degree. Hence, the lower bound of $\Omega\left(\sqrt{\frac{n}{\log(n)}}\right)$ we have proved above is tight within logarithmic factors in n.*

We also get a separation between symmetric torus polynomials and asymmetric torus polynomials as a corollary of Theorem 1.4.

Corollary 1. *Symmetric torus polynomials are weaker than their asymmetric counterparts.*

Proof. We compare the symmetric torus polynomial lower bound with the upper bound from Lemma 4.6. Using Lemma 4.6, we get $\overline{\deg}_{\frac{1}{20n}}(\mathsf{AND}) \leq \log^2(n)$. On the other hand, symmetric torus polynomials require much higher degree to $\frac{1}{20n}$-approximate AND. This proves the separation of their power. □

We complete the remaining part of the proof for Theorem 1.4, which is to prove Claim 5.3. For this purpose, we will need the following statement from [BV83].

Theorem 5.4 ([BV83])**.** *Consider a full-rank integer matrix B of size $n \times m$, with $n > m$. Then, $\mathcal{L}(B) = B\mathbb{Z}^m$ contains a non-zero vector $\mathbf{v} \in \mathbb{Z}^n$ with its ℓ^∞-norm bounded by:*

$$\|\mathbf{v}\|_\infty \leq \left(\frac{\sqrt{\det(B^T B)}}{D}\right)^{\frac{1}{n-m}}$$

Here, D is the GCD of all $m \times m$ minors of B.

To prove Claim 5.3 using Theorem 5.4, we first describe a basis for *nullspace*$(\widehat{M}(n,d))$. We state the construction without proof, omitting tedious calculations.

Lemma 5.5. *For $n \in \mathbb{N}$, and $d \in [n-1]^*$, construct a matrix $\widehat{B}(n,d)$, of size $(n+1) \times (n-d)$. Keep the following entry for $i \in [n]^*$ and $j \in [n-d-1]^*$: $\widehat{B}(n,d)_{i,k} = (-1)^{i-k}\binom{d+1}{i-k}$.*

Then, the columns of $\widehat{B}(n,d)$ form a basis for $\widehat{M}(n,d)$.

Now, to apply Theorem 5.4, we need to estimate $\det(\widehat{B}(n,d)^T \widehat{B}(n,d))$. We state the result below, deferring the calculations to the appendix.

Lemma 5.6. *There exists a universal constant c such that $\det(\widehat{B}(n,d)^T \widehat{B}(n,d)) \leq 2^{cd^2\log(n)}$.*

Finally, we need the following statement to find a vector ψ with an odd entry at the desired place. Informally speaking, consider a vector ψ such that $\psi_n = 0$. Then, we note that $\widehat{B}$ is a column-circulant matrix, with 0s beyond the two main diagonals. Hence, we can shift ψ to obtain $\overline{\psi}'$ such that $\overline{\psi}'_n$ contains the *last* non-zero entry of ψ. We formalize this in the statement below, stated without proof.

Lemma 5.7. *Consider a vector $\psi \in nullspace(\widehat{M}(n,d))$ such that the maximum index i where $\psi_i \neq 0$ is i_0. Define the following vector ψ':*

$$\psi'_i = \begin{cases} \psi_{i+i_0-n} & n - i_0 \leq i \leq n \\ 0 & 0 \leq i < n - i_0 \end{cases}$$

Then, $\psi' \in nullspace(\widehat{M}(n,d))$.

Now, we are ready to prove Claim 5.3, as follows.

Proof of Claim 5.3. First, choose any $d \leq \sqrt{\frac{n}{c\log(n)}}$. Then, apply Theorem 5.4 for $nullspace(\widehat{M}(n,d))$ with $\widehat{B}(n,d)$ as its basis. Note that $\widehat{B}(n,d)$ contains a minor, of size $(n-d) \times (n-d)$, with value 1. Hence, we get $D = 1$ when we apply Theorem 5.4. Therefore, there exists a non-zero vector $\overline{\psi} \in nullspace(\widehat{M}) \cap \mathbb{Z}^{n+1}$ with $\|\overline{\psi}\|_\infty \leq 2^{c\frac{n}{c\log(n)}\log(n)\frac{1}{2(n-d)}} \leq \sqrt{2}$. As $\|\overline{\psi}\|_\infty$ must be a positive integer, and $\sqrt{2} < 2$, this shows that $\|\overline{\psi}\|_\infty = 1$.

Now, if $\overline{\psi}_n = \pm 1$, then, either $\overline{\psi}$ or $-\overline{\psi}$ satisfies the claimed conditions. Otherwise, if $\overline{\psi}_n = 0$, use Lemma 5.7 to obtain $\overline{\psi'}$ from $\overline{\psi}$. Note that $\|\overline{\psi'}\|_1 = \|\overline{\psi}\|_1 \leq n+1$, and $|\overline{\psi'}_n| = 1$. Hence, we get the desired lower bound using ψ'. This completes the proof of the claim. □

5.1 Error-Degree Trade-off

The lower bound described in Theorem 1.4 applies to a particular error. It is natural to attempt to prove a stronger lower bound for a tighter error. Indeed, we are able to prove stronger lower bounds for tighter errors, but for MAJORITY. This significantly strengthens the lower bound from [BHLR19, Corollary 23]. Following is the statement of the lower bound.

Theorem 5.8. *Fix $r \in \mathbb{R}$, $r \geq 0$. For any $\varepsilon \leq 2^{-\Omega(\log^{r+1}(n))}$, any symmetric torus polynomial that ε-approximates $\mathsf{MAJORITY}_n$ has degree at least $\Omega\left(\sqrt{n\log^r(n)}\right)$.*

To prove this statement, we plan to use Minkowski's Theorem on the length of shortest vectors in a lattice. Following is the version we need.

Lemma 5.9 (Minkowski's Theorem [Min10])**.** *Consider a full-rank integer matrix B of size $n \times m$, with $n > m$. Then, the lattice $\mathcal{L}(B) = B\mathbb{Z}^m$ contains a vector $\mathbf{v} \neq 0$ with*

$$\|\mathbf{v}\|_1 \leq \sqrt{mn}\, det(B^T B)^{\frac{1}{2n}}$$

We plan to produce short vectors using Minkowski's Theorem, and then invoke Lemma 5.2 to argue the lower bound. Toward this, we need to argue that $\langle \mathsf{MAJORITY}, \overline{\psi} \rangle$ should be odd for a short vector $\overline{\psi}$ which, unfortunately, we could not prove. We prove the lower bound indirectly, by looking at a wider class of symmetric functions. The Δ_w function is defined as follows: $\Delta_w(x) = 1$ if and only if $|x| = w$. We obtain the following lower bound for these functions.

Lemma 5.10. *For any large enough $n \in \mathbb{N}$, there exists a $w \in [n]^*$, such that the following holds:*

Any symmetric torus polynomial that ε-approximates the Δ_w function over n variables, for $\varepsilon \leq 2^{-\Omega(\log^{r+1}(n))}$, must have degree $\Omega\left(\sqrt{n \log^r(n)}\right)$.

Proof. We start by appealing to Minkowski's theorem (Lemma 5.9).

Say $d = o\left(\sqrt{n \log^r(n)}\right)$ for some $r \geq 0$, and denote $\widehat{M} = \widehat{M}(n, d)$. We use Lemma 5.6, together with Minkowski's theorem, to get that there exists a non-zero vector $\overline{\psi} \in \mathit{nullspace}(\widehat{M}) \cap \mathbb{Z}^{n+1}$ with $\|\overline{\psi}\|_1 \leq n2^{o\left(\log^{r+1}(n)\right)}$. We want to choose a w, and prove the lower bound with respect to that Δ_w. Hence, we need to find a w such that $\langle \overline{\psi}, \Delta_w \rangle$ is odd.

Consider a non-zero vector $\overline{\psi} \in \mathit{nullspace}(\widehat{M}) \cap \mathbb{Z}^{n+1}$ with the smallest ℓ^1-norm. At least one of the entries of $\overline{\psi}$ must be odd. Otherwise, if they are all even, then $\overline{\psi}/2$ has strictly smaller ℓ^1-norm. The containment $\overline{\psi}/2 \in \mathit{nullspace}(\widehat{M}) \cap \mathbb{Z}^{n+1}$ follows, because $\mathit{nullspace}(\widehat{M})$ is a vector space, and $\overline{\psi}/2$ has integral entries. This is a contradiction.

This still does not tell us which entry of $\overline{\psi}$ will be odd. Hence, it is still not clear which Δ_w we should choose. Note that we have to choose w to write the family of linear programs, all of them must use the same function $f = \Delta_w$. To make our life easy, we turn the problem over its head.

We notice that we just need to choose w independent of Z, but it can depend on n, d. Hence, as the vector $\overline{\psi}$ with the smallest ℓ^1-norm depends only on n, d, we can choose w based on $\overline{\psi}$. This is exactly what we do, we choose w such that $\overline{\psi}_w$ is odd. Note that at least one such w must exist, we pick one of them arbitrarily. This completes the proof of the statement. □

Now, we apply a trick employed in the proof of [BHLR19, Corollary 23]. We describe it below without proof, as it is very similar to [BHLR19, Lemma 22].

Lemma 5.11. *For any $r \geq 0$, $\varepsilon \leq 2^{-\Omega\left(\log^{r+1}(n)\right)}$, and large enough n, the following holds: If there exists a symmetric torus polynomial of degree $o\left(\sqrt{n \log^r(n)}\right)$ that ε-approximates* MAJORITY*, then for any $w \in [n]^*$, there exists a symmetric torus polynomial of degree $o\left(\sqrt{n \log^r(n)}\right)$ that ε-approximates Δ_w.*

Now, we can finish the proof of Theorem 5.8 as follows.

Proof of Theorem 5.8. For some $r \in \mathbb{R}, r \geq 0$, consider $\varepsilon = 2^{-\Omega\left(\log^{r+1}(n)\right)}$. Assume that there exists a symmetric torus polynomial that ε-approximates MAJORITY with degree $d = o\left(\sqrt{n \log^r(n)}\right)$. Then, for each $w \in [n]^*$, there exists a symmetric torus polynomial that ε-approximates Δ_w. Moreover, each of these polynomials have degree $d = o\left(\sqrt{n \log^r(n)}\right)$. This contradicts Lemma 5.10, completing the proof of the theorem. □

To us, it is a bit unsatisfactory that we cannot prove this lower bound for AND. Note that the main hurdle for us is not knowing which entry of $\overline{\psi}$ is odd. If we can prove that $\overline{\psi}_n$ is odd, then the lower bound goes through for AND. Hence, we state a conjecture that will prove the error-degree trade-off for AND as well. In fact, we believe that the following holds, which is stronger than what we need.

Conjecture 4. *For any $n \in \mathbb{N}, 0 \leq d < n$, there is a vector $\overline{\psi} \in \mathit{nullspace}(\widehat{M}(n, d)) \cap Z^{n+1}$ with the smallest ℓ^1-norm and $\overline{\psi}_n = 1$.*

Acknowledgements

We thank Shachar Lovett for helpful feedback on an earlier draft. We also thank anonymous ITCS 2026 referees for their detailed feedback.

References

[Aar08] Scott Aaronson. The polynomial method in quantum and classical computing. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 3–3. IEEE, 2008.

[Bar89] David A Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC. *Journal of Computer and System Sciences*, 38(1):150–164, 1989.

[BCDWZ99] Harry Buhrman, Richard Cleve, Ronald De Wolf, and Christof Zalka. Bounds for small-error and zero-error quantum algorithms. In *40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039)*, pages 358–368. IEEE, 1999.

[BHLR19] Abhishek Bhrushundi, Kaave Hosseini, Shachar Lovett, and Sankeerth Rao. Torus Polynomials: An Algebraic Approach to ACC Lower Bounds. *10th Innovations in Theoretical Computer Science*, 2019.

[BT94] Richard Beigel and Jun Tarui. On ACC. *computational complexity*, 4:350–366, 1994.

[BT15] Mark Bun and Justin Thaler. Dual lower bounds for approximate degree and Markov–Bernstein inequalities. *Information and Computation*, 243:2–25, 2015.

[BT22] Mark Bun and Justin Thaler. Approximate degree in classical and quantum computing. *Foundations and Trends® in Theoretical Computer Science*, 15(3-4):229–423, 2022.

[BV83] Enrico Bombieri and Jeffrey D. Vaaler. On Siegel's lemma. *Inventiones mathematicae*, 73:11–32, 1983.

[Che19] Lijie Chen. Non-deterministic quasi-polynomial time is average-case hard for ACC circuits. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1281–1304. IEEE, 2019.

[Che23] Lijie Chen. New Lower Bounds and Derandomization for ACC, and a Derandomization-Centric View on the Algorithmic Method. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2023.

[CLLO21] Lijie Chen, Zhenjian Lu, Xin Lyu, and Igor C Oliveira. Majority vs. approximate linear sum and average-case complexity below NC^1. In *48th International Colloquium on Automata, Languages, and Programming (ICALP 2021)*, volume 198, page 51. Leibniz International Proceedings in Informatics, 2021.

[CLW20] Lijie Chen, Xin Lyu, and R Ryan Williams. Almost-everywhere circuit lower bounds from non-trivial derandomization. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1–12. IEEE, 2020.

[COS18] Ruiwen Chen, Igor C Oliveira, and Rahul Santhanam. An Average-Case Lower Bound Against ACC^0. In *Latin American Symposium on Theoretical Informatics*, pages 317–330. Springer, 2018.

[GKR+95] Frederic Green, Johannes Köbler, Kenneth W Regan, Thomas Schwentick, and Jacobo Torán. The power of the middle bit of a# P function. *Journal of Computer and System Sciences*, 50(3):456–467, 1995.

[Hås86] John Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 6–20, 1986.

[HG91] Johan Håstad and Mikael Goldmann. On the power of small-depth threshold circuits. *computational complexity*, 1(2):113–129, 1991.

[Kri21] Vaibhav Krishan. Upper bound for torus polynomials. In *Computer Science–Theory and Applications: 16th International Computer Science Symposium in Russia, CSR 2021, Sochi, Russia, June 28–July 2, 2021, Proceedings*, pages 257–263. Springer, 2021.

[Min10] Hermann Minkowski. *Geometrie der zahlen*. BG Teubner, 1910.

[MW19] Cody D Murray and R Ryan Williams. Circuit lower bounds for nondeterministic quasi-polytime from a new easy witness lemma. *SIAM Journal on Computing*, 49(5):STOC18–300, 2019.

[NS94] Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. *Computational complexity*, 4:301–313, 1994.

[Raz87] Alexander Alexandrovich Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Matematicheskie Zametki*, 41(4):598–607, 1987.

[RW93] Alexander Razborov and Avi Wigderson. $n^{\Omega(logn)}$ lower bounds on the size of depth-3 threshold cicuits with and gates at the bottom. *Information Processing Letters*, 45(6):303–307, 1993.

[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, 1987.

[Wil14] Ryan Williams. Nonuniform ACC circuit lower bounds. *Journal of the ACM (JACM)*, 61(1):1–32, 2014.

[Yao90] AC-C Yao. On ACC and threshold circuits. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 619–627. IEEE, 1990.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il