Upper Bound for Torus Polynomials

Vaibhav Krishan

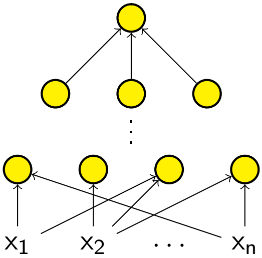
Computer Science and Engineering, IIT Bombay

The 16th International Computer Science Symposium in Russia, Sochi, Russia
29 June 2021

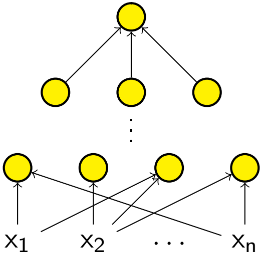
Outline

1. Introduction
2. Our Results
3. Proof
4. Conclusion

Boolean Circuits



Boolean Circuits



size: # of gates/wires

depth: length of longest path

$\mathcal{G}$: allowed gates

Early Lower Bounds

Definition (AC^0)

$\mathcal{G} = \{\wedge, \vee, \neg\}$.

Early Lower Bounds

Definition (AC^0)

$\mathcal{G} = \{\wedge, \vee, \neg\}$.

Theorem ([FSS84, Ajt83, Yao85, Hås87])

$\oplus \notin \mathsf{AC}^0$.

Early Lower Bounds

Definition (AC^0)

$\mathcal{G} = \{\wedge, \vee, \neg\}$.

Theorem ([FSS84, Ajt83, Yao85, Hås87])

$\oplus \notin AC^0$.

Definition ($AC^0[p]$)

$\mathcal{G} = \{\wedge, \vee, \neg, MOD_p\}$, p a prime.

Early Lower Bounds

Definition (AC^0)

$\mathcal{G} = \{\wedge, \vee, \neg\}$.

Theorem ([FSS84, Ajt83, Yao85, Hås87])

$\oplus \notin AC^0$.

Definition ($AC^0[p]$)

$\mathcal{G} = \{\wedge, \vee, \neg, MOD_p\}$, p a prime.

Theorem ([Raz87, Smo87])

$MAJ \notin AC^0[p]$.

ACC Lower Bounds

Definition (ACC)

$\mathcal{G} = \{\wedge, \vee, \neg, \mathrm{MOD}_m\}$.

ACC Lower Bounds

Definition (ACC)

$\mathcal{G} = \{\wedge, \vee, \neg, \mathrm{MOD}_m\}$.

Theorem ([Wil14])

$\mathrm{NEXP} \not\subset \mathrm{ACC}$.

Torus Polynomials

Definition (Torus Polynomial)

$P(x_1, \ldots, x_n) \in \mathbb{R}[X_1, \ldots, X_n]$ is a torus polynomial that ε-approximates f if

$$P(x) - f(x)/2 \in [N(x) - \varepsilon, N(x) + \varepsilon], N(x) \in \mathbb{Z}$$

Torus Polynomials

Definition (Torus Polynomial)

$P(x_1, \ldots, x_n) \in \mathbb{R}[X_1, \ldots, X_n]$ is a torus polynomial that ε-approximates f if

$$P(x) - f(x)/2 \in [N(x) - \varepsilon, N(x) + \varepsilon], N(x) \in \mathbb{Z}$$

$deg_{\varepsilon}(f)$ smallest degree of torus polynomial that ε-approximates f.

Torus Polynomials

Definition (Torus Polynomial)

$P(x_1, \ldots, x_n) \in \mathbb{R}[X_1, \ldots, X_n]$ is a torus polynomial that ε-approximates f if

$$P(x) - f(x)/2 \in [N(x) - \varepsilon, N(x) + \varepsilon], N(x) \in \mathbb{Z}$$

$deg_\varepsilon(f)$ smallest degree of torus polynomial that ε-approximates f.

Theorem ([BHLR18])

Let $f \in \mathrm{ACC}$ and $\varepsilon = n^{-O(1)}$. Then $deg_\varepsilon(f) \leq (\log(n))^{O(1)}$.

Outline

1 Introduction

2 Our Results

3 Proof

4 Conclusion

MidBit$^+$

Definition (MidBit)

$\text{MidBit} : \{0,1\}^n \to \{0,1\}, \ell = \lfloor \log_2(n) \rfloor + 1$

$bin\left(\sum_{i=1}^{n} x_i\right) = b_{\ell-1} \dots b_{\lfloor \ell/2 \rfloor+1} \text{MidBit}(x) b_{\lfloor \ell/2 \rfloor-1} \dots b_0$

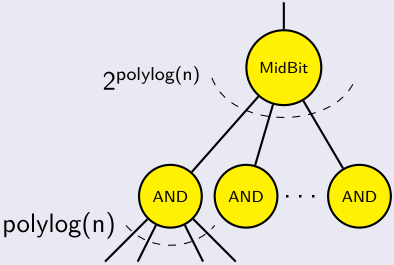
MidBit$^+$

Definition (MidBit)

MidBit : $\{0,1\}^n \to \{0,1\}, \ell = \lfloor \log_2(n) \rfloor + 1$

$bin\left(\sum_{i=1}^{n} x_i\right) = b_{\ell-1} \ldots b_{\lfloor \ell/2 \rfloor+1} \mathrm{MidBit}(x) b_{\lfloor \ell/2 \rfloor-1} \ldots b_0$

Definition (MidBit$^+$)



Power of MidBit^+

Theorem (GKT'92)

$\mathrm{ACC} \subseteq \mathrm{MidBit}^+$

Power of MidBit^+

Theorem (GKT'92)

$\mathrm{ACC} \subseteq \mathrm{MidBit}^+$

Lemma

$\mathrm{MAJ} \in \mathrm{MidBit}^+$

Upper Bound for Torus Polynomials

Theorem

Let $\varepsilon < 1/8$. $deg_{\varepsilon}(f) \leq (\log(n))^{O(1)} \implies f \in \mathrm{MidBit}^{+}$

Upper Bound for Torus Polynomials

Theorem

Let $\varepsilon < 1/8$. $deg_{\varepsilon}(f) \leq (\log(n))^{O(1)} \implies f \in \mathrm{MidBit}^{+}$

Theorem

Let $\varepsilon < 1/8$. *Let* $deg_{\varepsilon}(f) = d$. *Then, there is* MidBit^{+} *circuit computing* f*, of the following form:*

- *fan-in of each* AND *gate is bounded by* d*,*
- *fan-in of the* MidBit *gate is bounded by* 2^{2k-1} *where* $2^k = (d+1)n^d/\varepsilon$*,*
- *for* $x \in \{0,1\}^n$*, let* $A(x)$ *be the number of* AND *gates that output 1. Then* $A(x) \equiv f(x)2^{k-1} + E(x) \mod 2^k$*, where* $E(x) \leq 4\varepsilon 2^k$*.*

Outline

1. Introduction
2. Our Results
3. Proof
4. Conclusion

Proof

- Let $P = \sum_{\alpha} c_{\alpha} X^{\alpha}$ ε-approximate f.
  $P(x) \in [N(x) + f(x)/2 - \varepsilon, N(x) + f(x)/2 + \varepsilon]$

Proof

- Let $P = \sum_\alpha c_\alpha X^\alpha$ ε-approximate f.
  $P(x) \in [N(x) + f(x)/2 - \varepsilon, N(x) + f(x)/2 + \varepsilon]$
- Take $P_{pos} = P + \varepsilon$.
  $P_{pos}(x) \in [N(x) + f(x)/2, N(x) + f(x)/2 + 2 * \varepsilon]$

Proof

- Let $P = \sum_{\alpha} c_{\alpha} X^{\alpha}$ ε-approximate f.
  $P(x) \in [N(x) + f(x)/2 - \varepsilon, N(x) + f(x)/2 + \varepsilon]$
- Take $P_{pos} = P + \varepsilon$.
  $P_{pos}(x) \in [N(x) + f(x)/2, N(x) + f(x)/2 + 2 * \varepsilon]$
- $bin(P_{pos}(x)) = \ldots 101.f(x)0110010\ldots$

Proof - Continued

- Choose a k. For each c_α, calculate $q_\alpha \in \mathbb{Z}$ such that $\left| c_\alpha - \frac{q_\alpha}{2^k} \right| \leq \frac{1}{2^k}$

Proof - Continued

- Choose a k. For each c_α, calculate $q_\alpha \in \mathbb{Z}$ such that $\left| c_\alpha - \frac{q_\alpha}{2^k} \right| \leq \frac{1}{2^k}$
- $P_{disc}(x) = \sum_\alpha q_\alpha / 2^k X^\alpha$.
  $bin(P_{disc}(x)) = \ldots 101.f(x)0110010\ldots$

Proof - Continued

- Choose a k. For each c_α, calculate $q_\alpha \in \mathbb{Z}$ such that $\left| c_\alpha - \frac{q_\alpha}{2^k} \right| \leq \frac{1}{2^k}$
- $P_{disc}(x) = \sum_\alpha q_\alpha / 2^k X^\alpha$.
  $bin(P_{disc}(x)) = \ldots 101.f(x)0110010\ldots$
- $P_{int}(x) = 2^k P_{disc}(x) = \sum_\alpha q_\alpha X^\alpha$
  $bin(P_{int}(x)) = \ldots 101f(x)0110$

Proof - Continued

- Choose a k. For each c_α, calculate $q_\alpha \in \mathbb{Z}$ such that $\left|c_\alpha - \frac{q_\alpha}{2^k}\right| \leq \frac{1}{2^k}$
- $P_{disc}(x) = \sum_\alpha q_\alpha/2^k X^\alpha$.
  $bin(P_{disc}(x)) = \ldots 101.f(x)0110010\ldots$
- $P_{int}(x) = 2^k P_{disc}(x) = \sum_\alpha q_\alpha X^\alpha$
  $bin(P_{int}(x)) = \ldots 101f(x)0110$
- Convert to MidBit$^+$.

Parity over Torus Polynomials

Introduction

Our Results

Proof

Conclusion

Theorem

Let $deg_{\varepsilon_1}(f_1) = d_1$ *and* $deg_{\varepsilon_2}(f_2) = d_2$. *Then* $deg_{\varepsilon_1+\varepsilon_2}(f_1 \oplus f_2) \leq \max(d_1, d_2)$

Parity over Torus Polynomials

Theorem

Let $deg_{\varepsilon_1}(f_1) = d_1$ *and* $deg_{\varepsilon_2}(f_2) = d_2$. *Then* $deg_{\varepsilon_1+\varepsilon_2}(f_1 \oplus f_2) \leq \max(d_1, d_2)$

Proof.

Let P_1 ε_1-approximate f_1 and P_2 ε_2-approximate f_2. Consider $P_1 + P_2$. $\square$

Outline

1 Introduction

2 Our Results

3 Proof

4 Conclusion

Conclusion

- Power of torus polynomials is upper bounded by MidBit^+.

Conclusion

- Power of torus polynomials is upper bounded by MidBit^{+}.
- Torus polynomials are closed under parity.

Thank You

Thank You

References I

Miklós Ajtai, Σ_1^1-*formulae on finite structures*, Annals of pure and applied logic **24** (1983), no. 1, 1–48.

Abhishek Bhrushundi, Kaave Hosseini, Shachar Lovett, and Sankeerth Rao, *Torus polynomials: An algebraic approach to* ACC *lower bounds*, 10th Innovations in Theoretical Computer Science Conference (ITCS 2019), Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

Merrick Furst, James B Saxe, and Michael Sipser, *Parity, circuits, and the polynomial-time hierarchy*, Mathematical systems theory **17** (1984), no. 1, 13–27.

Johan Håstad, *Computational limitations of small-depth circuits*, MIT press, 1987.

References II

Alexander A Razborov, *Lower bounds on the size of bounded depth circuits over a complete basis with logical addition*, Mathematical Notes of the Academy of Sciences of the USSR **41** (1987), no. 4, 333–338.

Roman Smolensky, *Algebraic methods in the theory of lower bounds for boolean circuit complexity*, Proceedings of the nineteenth annual ACM symposium on Theory of computing, 1987, pp. 77–82.

Ryan Williams, *Nonuniform* ACC *circuit lower bounds*, Journal of the ACM (JACM) **61** (2014), no. 1, 1–32.

References III

Andrew Chi-Chih Yao, *Separating the polynomial-time hierarchy by oracles*, 26th Annual Symposium on Foundations of Computer Science (sfcs 1985), IEEE, 1985, pp. 1–10.