# Size Bounds on Low Depth Circuits for Promise Majority

**Joshua Cook**
The University Of Texas At Austin, TX, USA
https://www.cs.utexas.edu/~jacook7/
jac22855@utexas.edu

## Abstract

We give two results on the size of AC0 circuits computing promise majority. $\epsilon$-promise majority is majority promised that either at most an $\epsilon$ fraction of the input bits are 1 or at most $\epsilon$ are 0.

- First, we show super-quadratic size lower bounds on both monotone and general depth-3 circuits for promise majority.
  - For any $\epsilon \in (0, 1/2)$, monotone depth-3 AC0 circuits for $\epsilon$-promise majority have size
    $$\tilde{\Omega}\left(\epsilon^3 n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}\right).$$
  - For any $\epsilon \in (0, 1/2)$, general depth-3 AC0 circuits for $\epsilon$-promise majority have size
    $$\tilde{\Omega}\left(\epsilon^3 n^{2+\frac{\ln(1-\epsilon^2)}{2\ln(\epsilon)}}\right).$$

  These are the first quadratic size lower bounds for depth-3 $\epsilon$-promise majority circuits for $\epsilon < 0.49$.
- Second, we give both uniform and non-uniform sub-quadratic size constant-depth circuits for promise majority.
  - For integer $k \geq 1$ and constant $\epsilon \in (0, 1/2)$, there exists monotone *non* uniform AC0 circuits of depth-$(2 + 2k)$ computing $\epsilon$-promise majority with size
    $$\tilde{O}\left(n^{\frac{1}{1-2^{-k}}}\right).$$
  - For integer $k \geq 1$ and constant $\epsilon \in (0, 1/2)$, there exists monotone *uniform* AC0 circuit of depth-$(2 + 2k)$ computing $\epsilon$-promise majority with size
    $$n^{\frac{1}{1-\left(\frac{2}{3}\right)^k}+o(1)}.$$

  These circuits are based on incremental improvements to existing depth-3 circuits for promise majority given by Ajtai [2] and Viola [14] combined with a divide and conquer strategy.

**2012 ACM Subject Classification** Theory of computation → Circuit complexity

**Keywords and phrases** AC0, Approximate Counting, Approximate Majority, Promise Majority, Depth 3 Circuits, Circuit Lower Bound

**Digital Object Identifier** 10.4230/LIPIcs.FSTTCS.2020.19

**Related Version** A full version of the paper is available at [7], https://eccc.weizmann.ac.il/report/2020/122/.

**Funding** This research was supported by NSF grant number 1705028.

**Acknowledgements** Thanks to Dana Moshkovitz for suggesting I study the size cost of derandomizing AC0 circuits. Thanks to Justin Yirka, Amanda Priestly and an anonymous reviewer for feedback on this paper.


40th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2020).
Editors: Nitin Saxena and Sunil Simon; Article No. 19; pp. 19:1–19:14

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

# 1 Introduction

The majority function is a classic function that cannot be computed in AC0 [9]. But AC0 can compute majority promised the input is either mostly 1s or mostly 0s.

▶ **Definition 1** ($\epsilon$-Promise Majority). *Let $W : \{0,1\}^n \to [n]$ be the function giving the number of ones in the input*[1]*. Let $\epsilon \in (0, 1/2)$. Then define the $\epsilon$ promise inputs to be:*

$$Maj_\epsilon^0 = \{x \in \{0,1\}^n : W(x) \leq \epsilon n\}$$
$$Maj_\epsilon^1 = \{x \in \{0,1\}^n : W(x) \geq (1-\epsilon)n\}$$
$$Maj_\epsilon = Maj_\epsilon^0 \cup Maj_\epsilon^1$$

*We say that function $f$ solves the $\epsilon$-promise majority*[2] *problem if:*

$$f(Maj_\epsilon^0) = 0$$

$$f(Maj_\epsilon^1) = 1$$

*That is, $f$ computes the majority promised the input is in $Maj_\epsilon$.*

We give size[3] lower bounds to depth-3 circuits[4] computing $\epsilon$-promise majority. Then we give small circuits solving promise majority with larger depth.

## 1.1 Motivation

Promise majority is an important tool in derandomizing circuits. We say a function $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ is a randomized function for $g : \{0,1\}^n \to \{0,1\}$ if for all $x \in \{0,1\}^n$, $\Pr_{r \in \{0,1\}^m}[f(x,r) = g(x)] \geq 2/3$. A circuit implementing $f$ is called a randomized circuit for $g$. We call $r \in \{0,1\}^m$ a seed for $f$.

Adleman [1] showed that for any randomized function $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$, implementing some $g : \{0,1\}^n \to \{0,1\}$, there is some choice of seeds $R \subseteq \{0,1\}^m$ with $|R| = O(n)$ such that for all $x$ and the majority of seeds in $R$, $f$ computes $g$, i.e., $\Pr_{r \in R}[f(x,r) = g(x)] > 1/2$. If $f$ has size-$O(n)$ random circuits, this gives a size-$O(n^2)$ deterministic circuits by computing majority of $|R|$ copies of $f$ and taking majority.

Unfortunately, AC0 cannot compute majority, but it can compute $\epsilon$-promise majority. With the same argument, we can get $R$ with $|R| = O(n)$ such that $\Pr_{r \in R}[f(x,r) = g(x)] > 3/5$. So, we only need to compute 2/5-promise majority since $f$ only outputs the wrong bit for at most 2/5 of $r \in R$.

Ajtai [2] gave depth-3 circuits of size $O\left(n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)-\ln(1-\epsilon)}}\right)$ solving the $\epsilon$-promise majority problem. Applying a depth-$d$ promise majority circuit, $M$, to the output of a depth-$k$ circuit, $C$, gives a depth-$(k+d-1)$ circuit since the kind of gate at the lowest level of $M$ can be made the same as the top level of $C$. Combining this result with Adleman takes a size-$O(n)$, depth-$d$ randomized circuit and gives a depth-$(d+2)$, size-$O\left(n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)-\ln(1-\epsilon)}}\right)$ deterministic circuit. This is bigger than the ideal $O(n^2)$ size from the unbounded depth setting.

---

[1] For functions and circuits, we implicitly refer to a family of functions, one for each size $n$ where $n$ is implicit. The same holds for $\text{Maj}_\epsilon$.

[2] Prior work often called promise majority "approximate majority" [14, 15]. But, approximate majority also refers to the standard notion of approximating a Boolean function [5]. To avoid confusion, we follow the convention suggested in [11] to refer to the promise problem version of majority as promise majority.

[3] In this paper, we use size of a circuit to mean the number of gates.

[4] In this paper, all circuits are constant depth alternating circuits (AC0 circuits) unless stated otherwise.

This paper gives new, super-quadratic size lower bounds for depth-3 circuits computing $\epsilon$-promise majority. Thus applying Adleman's technique on AC0 circuits to get size-$O(n^2)$ deterministic circuits using promise majority requires a depth-3 increase. We show this is tight by giving size-$O(n^2)$ depth-4 circuits for $\epsilon$-promise majority. Thus Adleman's technique can be used to get size-$O(n^2)$ deterministic circuits with a depth-3 increase.

## 1.2 Our Results

For notation, let $\tilde{O}(x)$ indicate order $x$ up to polylogarithmic factors:

▶ **Definition 2.** *$f(n) = \tilde{O}(g(n))$ if for some integer $c$, $f = O(g(n)\ln(n)^c)$.*
*$f(n) = \tilde{\Omega}(g(n))$ if for some integer $c$, $f = \Omega(g(n)\ln(n)^c)$.*

First, we give a size lower bound for monotone, depth-3 circuits for promise majority. Note that the best known depth-3 circuits are monotone.

▶ **Theorem 3.** *For any $\epsilon \in (0, 1/2)$, a* monotone*, depth-3 circuit solving the $\epsilon$-promise majority problem must have size $\tilde{\Omega}\left(\epsilon^3 n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}\right)$.*

We follow this up with some weaker, but still super-quadratic, size lower bounds for depth-3 circuits computing promise majority.

▶ **Theorem 4.** *For any $\epsilon \in (0, 1/2)$, a depth-3 circuit solving the $\epsilon$-promise majority problem must have size $\tilde{\Omega}\left(\epsilon^3 n^{2+\frac{\ln(1-\epsilon^2)}{2\ln(\epsilon)}}\right)$.*

Minor improvements to Ajtai's promise majority circuits [2] gives depth-4, quadratic size, promise majority circuits.

▶ **Theorem 5.** *For constant $\epsilon \in (0, 1/2)$, there exists* non *uniform, monotone, depth-4, size-$O\left(n^2\right)$ circuits solving the $\epsilon$-promise majority problem.*

We then show how to solve $\epsilon$-promise majority with even smaller circuits with larger depths using a divide and conquer strategy.

▶ **Theorem 6.** *For constant $\epsilon \in (0, 1/2)$, there exists* non *uniform, monotone, depth-$(2+2k)$ circuits solving the $\epsilon$-promise majority problem with size $\tilde{O}\left(n^{\frac{1}{1-2^{-k}}}\right)$.*

The above circuits are not explicit, or uniform: we do not know how to construct it efficiently. However, we next give P-Uniform circuits for promise majority: circuits with a polynomial-time algorithm to construct them. These circuits use a slight improvement to Viola's depth-3 promise majority circuits [14] with a divide and conquer strategy.

▶ **Theorem 7.** *For constant $\epsilon \in (0, 1/2)$, there exists P-uniform, monotone, depth-$(2+2k)$ circuits solving the $\epsilon$-promise majority problem with size $n^{\frac{1}{1-\left(\frac{2}{3}\right)^k}+o(1)}$.*

For $k = 2$, this gives depth-6, size-$o(n^2)$, P-uniform, monotone circuits for promise majority.

▶ **Corollary 8.** *For constant $\epsilon \in (0, 1/2)$, there exists P-uniform, monotone, depth-6 circuits solving the $\epsilon$-promise majority problem with size $n^{\frac{9}{5}+o(1)}$.*

Thus a P-uniform PRG with $O(n)$ seeds for AC0 could derandomize linear-size, randomized circuits to get quadratic-size, deterministic circuits with a depth increase of 5. Finding such PRGs, or even PRGs with polynomially many seeds, is still open. Though, work by Dean Doron, Dana Moshkovitz, Justin Oh and David Zuckerman constructs nearly quadratic PRGs conditioned on some complexity theoretic assumptions [8].

## 1.3 Related Work

There are well known polynomial-size AC0 circuits for promise majority. First, Ajtai gave polynomial size, depth-3 circuits for $\epsilon$-promise majority [2]. Ajtai later gave uniform, even deterministic log time uniform, AC0 circuits for promise majority [3]. But, these uniform circuits have large depth and their constructions are complicated. Viola later gave simpler P-Uniform, depth-3 AC0 circuits for promise majority [14].

Chaudhuri and Radhakrishnan [6] proved that any depth-$d$ circuit computing $\epsilon$-promise majority must have size $\Omega\left((\epsilon n)^{\frac{1}{1-1/4^d}} - n\right)$. This gives super-linear lower bounds for depth-3 circuits, but not close to quadratic. Their paper uses deterministic restrictions for lower bounds similar to ours, but our paper uses fan-in lower bounds from Viola [14] and different restrictions to get better depth-3 lower bounds.

In the same work [6], Chaudhuri and Radhakrishnan gave, for any k, depth-$O(k)$ circuits with size $O\left(n^{1+\frac{1}{2^k}}\right)$ for $\epsilon$-promise majority. Like our paper, it uses a recursive strategy, but we use a different recursive strategy that gives shallower circuits.

Exact threshold functions in AC0 have been studied extensively. Ragde and Wigderson [13] show that for integer $r > 0$, the $\ln(n)^r$ threshold function, which computes whether $W(x) > \ln(n)^r$, has AC0 circuits with depth $O(r)$ and size $o(n)$. This improves on a result by Ajtai and Ben-Or [4]. Further, Håstad, Wegener, Wurm, and Yi [10] show that polylogarithmic threshold functions have sub-polynomial size, constant-depth circuits.

Results by Amano [5] building on work by O'Donnell and Wimmer [12] prove the minimum size for a depth-$d$ circuit computing majority on most inputs is $\Theta\left(n^{\frac{1}{2d-1}}\right)$. This is consistent with promise majority results because most inputs are close to balanced, within a $O(1/\sqrt{n})$ factor, but promise majority is only guaranteed to give majority on inputs that are far from balanced.

For $\epsilon = \left(\frac{1}{2} - \frac{1}{\ln(n)^k}\right)$, Viola proved that randomized, depth-$(k+1)$, polynomial-size circuits can solve $\epsilon$-promise majority, but deterministic, depth-$(k+2)$, polynomial-size circuits cannot. Further, there are deterministic, depth-$(k+3)$, polynomial-size circuits for $\epsilon$-promise majority [15].

The same work [15] gave size lower bounds for depth-3 $\epsilon$-promise majority circuits, but the bounds are less than linear for $\epsilon < 0.49$. Closer analysis gives better lower bounds, but we could not get quadratic lower bounds for $\epsilon < 0.49$ with this technique.

A later work by Limaye, Srinivasan and Tripathi [11] showed that deterministic, depth-$(k+1)$, polynomial-size AC0 circuits with parity gates also cannot solve $\left(\frac{1}{2} - \frac{1}{\ln(n)^k}\right)$-promise majority.

# 2 Proof Ideas

## 2.1 Monotone Depth-3 Circuit Lower Bounds

For depth-3 promise majority circuits, without loss of generality, assume the first level of gates are AND gates[5]. Call the inputs "variables", the first level gates "clauses", and the second level gates "DNFs".

[5] Switching the ANDs to ORs and ORs to ANDs in a circuit solving $\epsilon$-promise majority still solves $\epsilon$-promise majority. To see this, observe that flipping all the input bits will flip a $\text{Maj}_\epsilon^1$ input to a $\text{Maj}_\epsilon^0$ input. Then apply de Morgan's law.

To prove lower bounds for a depth-3 circuit, we construct adversarial restrictions that simplify the circuit while setting too few variables to violate the promise. To do this, we use two main tools. The first is a lemma from Viola [14] that we use to remove gates with very small fan in at the first level.

The second is a greedy set cover algorithm which shows that any collections of large subsets of variables can have a large fraction of the subsets hit by a small fraction of variables. To do this, we repeatedly select a variable in at least the average number of sets per variable.

First, we show DNFs have $\tilde{\Omega}(n^{1+\alpha})$ clauses for some $\alpha > 0$. To do this, we eliminate small clauses using the first idea, then eliminate a large fraction of clauses with few 0s using the second idea. This leaves many clauses while eliminating a large fraction of clauses, thus we started with many clauses.

Then, we show the circuit has $\tilde{\Omega}(n^{2+\alpha})$ clauses. First, we use the second idea to remove any very large clauses. This lets us fix clauses to 1 without using too many variables. Then, using the second idea again, we can hit many DNFs using few clauses. Thus there must be many clauses so we can not hit every DNF using few clauses.

We generally will not worry about integrality. This only becomes an issue when $\epsilon = \tilde{O}\left(n^{-1/2}\right)$ as some restrictions would not have size greater than one. In that case, our lower bounds hold trivially as $\epsilon n$ gates can be fixed to a constant assigning only $\epsilon n$ variables.

## 2.2 General Depth-3 Circuit Lower Bounds

The proof for non-monotone circuits is similar but with an additional hurdle. In monotone circuits, setting variables to 0 only makes clauses 0. But with negations, we can actually shrink clauses without eliminating them. This is an issue for showing DNFs must be large, but the rest of the argument only needs minor changes.

The solution is to set adversarial bits probabilistically. We independently set each bit to 1 with probability $\epsilon$. With good probability, this will give an input in $\text{Maj}_\epsilon^0$. Some DNFs then must have a good probability of "noticing" and becoming 0.

With high probability, fixing a small fraction of variables according to $D_\epsilon$ will eliminate many clauses. For some $\alpha > 0$, if a DNF is smaller than $n^{1+\alpha}$ this will make it constant. With good probability, setting the rest of the variables gives an input this DNF must "notice" and become 0. Thus, if the DNF is small, for some input it will be fixed to the constant 0 with only a few variables fixed. This cannot happen, so the DNF must be larger than $n^{1+\alpha}$.

## 2.3 Small Sized Circuits

To get small circuits, first we amplify the $\epsilon$ promise input to a $\frac{1}{\text{polylog}(n)}$ promise input by taking majority over $O(\ln(\ln(n)))$ length walks on an expander graph. Then we separate our input into polynomially small groups and run a $\frac{1}{\ln(n)}$-promise majority on each. This gives a polynomially smaller layer which satisfies just an $\ln(n)$ factor worse promise. Applying this several times computes majority of the promise input.

Ajtai's promise majority strategy gives a quadratic-sized $\frac{1}{\ln(n)}$-promise majority circuit. Using this with the divide and conquer strategy above gives non uniform small circuits.

For our uniform circuit, we look at Viola's circuit [14]. It uses a hitting property that requires $n^{3+o(1)}$ many random walks for each of our $n$ bits, requiring an overall size of $n^{4+o(1)}$. We reduce this by showing it suffices to let each bit only range over random walks starting at that bit, giving a size-$n^{3+o(1)}$ circuit for $\frac{1}{\ln(n)}$-promise majority.

Applying this improved version of Viola's depth-3 circuit with our divide and conquer strategy gives our uniform small circuits.

## 2.4 Terminology

We will use biased inputs in our proofs.

▶ **Definition 9** ($\epsilon$ Biased Input). *For any $\epsilon \in [0,1]$ the $\epsilon$ biased input $D_\epsilon$ is a random variable over $\{0,1\}^n$ where each bit independently is 1 with probability $\epsilon$.*

As with $\text{Maj}^0_\epsilon$ and $\text{Maj}^1_\epsilon$, $n$ in $D_\epsilon$ is implicit. $D_\epsilon$ is related to $\text{Maj}^0_\epsilon$ by a central limit theorem: $\Pr[D_\epsilon \in \text{Maj}^0_\epsilon] > \frac{1}{3}$ for large enough $n$.

We will make sub DNFs by only taking some clauses from a larger DNF.

▶ **Definition 10** (Sub DNF). *Let $G$ be a DNF with clauses $C = \{C_i : i \in [k]\}$ so that $G = \bigvee_{i\in[k]} C_i$. Let $\Lambda \subseteq [k]$ and $H$ be a DNF with $H = \bigvee_{i\in\Lambda} C_i$.*

*Then we say that $H$ is sub DNF of $G$ or $G$ has sub DNF $H$.*

Restrictions fix some bits in the input to a function. We formalize this as a function that takes unrestricted bits as input and outputs the restricted and unrestricted bits together[6].

▶ **Definition 11** (Restriction). *A restriction $\rho$ on $n$ variables of size $m$ is a function $\rho : \{0,1\}^{n-m} \to \{0,1\}^n$ such that for some $c \in \{0,1\}^m$ and some permutation of $[n]$, $\pi$, for all $x \in \{0,1\}^{n-m}$ and $i \in n$:*

$$\rho(x)_i = \begin{cases} c_{\pi_i} & \pi_i \leq m \\ x_{\pi_i - m} & \pi_i > m \end{cases}$$

*We write the size of $\rho$ as $|\rho| = m$ and define $f \restriction_\rho = f \circ \rho$.*

When we apply a restriction, $\rho$, to a DNF, $F$, we let $F \restriction_\rho$ be the DNF which is $F$ with variables restricted in $\rho$ set to their restricted value. We simplify such a DNF to remove any clause that has been set to 0. We count the size of a DNF by its number of clauses.

▶ **Definition 12** (DNF Size and Width). *For a DNF $F$, the size of $F$, $|F|$, is the number of clauses in $F$. Any DNF that is the constant 1 or 0 function has size 0.*

*We say a DNF $F$ has width $w$ if no clause in $F$ has width greater than $w$.*

# 3 Monotone Depth-3 Circuit Size Lower Bounds

## 3.1 Removing Small Clauses

We use a result from Viola [14], Lemma 11 therein. Intuitively, this lemma says for a DNF with small width, either there is some setting to a small number of variables that makes it 0, or under a randomized input it is unlikely to be 0.

▶ **Lemma 13.** *Let $G$ be a DNF with a sub DNF $F$. Assume for some positive integers $w$ and $m$, $F$ has width at most $w$ and $\Pr[G(D_\epsilon) = 0] \geq e^{-\epsilon^w \cdot m/w^2}$. Then there exists a restriction $\rho$ with $|\rho| \leq m$ such that $F \restriction_\rho = 0$ and $\Pr[G \restriction_\rho (D_\epsilon) = 0] \geq \Pr[G(D_\epsilon) = 0]$.*

Our result is slightly generalized over the original. See the full version of this paper for details. As a corollary, we can can apply small restrictions to eliminate small width clauses.

[6] This is an equivalent but slightly nonstandard way to define restrictions.

▶ **Corollary 14.** *Suppose we have $\epsilon \in (0, 1/2)$, DNF $F$ and constant $\alpha > 0$ such that $\Pr[F(D_\epsilon) = 0] \geq n^{-\alpha}$. Then for sufficiently large $n$ and*

$$w = \log_\epsilon \left( \frac{\ln(n)^5}{n\epsilon \ln(\epsilon)^2} \right)$$

*there is a restriction $\rho$ restricting at most $m = \frac{\epsilon n}{\ln(n)}$ variables so that any clause $C$ in $F$ with width less than $w$ has $C \restriction_\rho = 0$ and $\Pr[F \restriction_\rho (D_\epsilon) = 0] \geq \Pr[F(D_\epsilon) = 0]$.*

**Proof.** Let $F'$ be the sub DNF of $F$ with clauses of width less than $w$. Then

$$\mathbb{E}[F(D_\epsilon) = 0] \geq n^{-\alpha} = e^{-\alpha \ln(n)} = e^{-\alpha \frac{\ln(n)^5}{n\epsilon \ln(\epsilon)^2} \frac{\epsilon n}{\ln(n)} \frac{\ln(\epsilon)^2}{\ln(n)^3}} = e^{-\alpha \epsilon^w m \frac{\ln(\epsilon)^2}{\ln(n)^3}} \geq e^{-\epsilon^w m \frac{1}{w^2}}$$

From Lemma 13, there is a restriction $\rho$ of size $m$ with $\mathbb{E}[F \restriction_\rho (D_\epsilon) = 0] \geq \mathbb{E}[F(D_\epsilon) = 0]$ setting $F' \restriction_\rho = 0$. Any width $w$ clause $C$ would be in $F'$, thus $C \restriction_\rho = 0$ since $F' \restriction_\rho = 0$. ◀

## 3.2 Covering Many Large Sets with Few Elements

We prove the simplest version of the clause elimination result, but slight variations will be used in multiple places. In particular, in the non-monotone lower bounds, we can't quite reduce the problem to set cover, but the same algorithm still works with a similar bound. Since the proofs look very similar, we only present one in detail. We show how to remove many clauses from a monotone DNF with a small restriction

▶ **Lemma 15.** *Let $F$ be a monotone DNF where each clause has width at least $w$. Then for any positive integer $b$, there is some restriction $\rho$ with $|\rho| = b$ only fixing variables to 0 such that $|F \restriction_\rho| < |F| e^{w \ln\left(1 - \frac{b}{n+1}\right)}$*

**Proof.** The idea is to restrict the variable that intersects the most clauses to 0. This removes at least the average number of clauses per variable, which when we have $m$ clauses and have fixed $i$ variables is at least $\frac{mw}{n-i}$. After $b$ restrictions, we get $\rho$ with $|\rho| = b$ and

$$|F \restriction_\rho| \leq |F| \prod_{i=0}^{b-1} \left(1 - \frac{w}{n-i}\right).$$

We prove this by induction then simplify. For the base case where $b = 0$, $F$ is unchanged and we get the empty product, so the inequality holds.

For $b > 0$, we have some $\rho'$ restricting $b-1$ variables with $|F \restriction_{\rho'}| \leq |F| \prod_{i=0}^{b-2} \left(1 - \frac{w}{n-i}\right)$. Then $F \restriction_{\rho'}$ is a function on $n + 1 - b$ variables. Let $s$ be the variable in the most clauses of $F \restriction_{\rho'}$. Then $s$ is in at least $|F \restriction_{\rho'}| \frac{w}{n+1-b}$ clauses. Let $\rho$ be $\rho'$ also fixing $s$ to 0. Then:

$$|F \restriction_\rho| \leq |F \restriction_{\rho'}| - |F \restriction_{\rho'}| \frac{w}{n+1-b} = |F| \prod_{i=0}^{b-1} \left(1 - \frac{w}{n-i}\right),$$

completing our induction. The above equation simplifies to:

$$|F \restriction_\rho| = |F| \prod_{i=0}^{b-1} \left(1 - \frac{w}{n-i}\right) < |F| e^{\sum_{i=0}^{b-1} -\frac{w}{n-i}} = |F| e^{-w \sum_{i=n+1-b}^{n} 1/i}. \tag{1}$$

From calculus we have

$$\sum_{i=a}^{b} \frac{1}{i} \geq \int_a^{b+1} \frac{1}{x} dx = \ln\left(\frac{b+1}{a}\right),$$

which applied to Equation (1) gives

$$|F\restriction_\rho| < |F|e^{-w\sum_{i=n+1-b}^{n}\frac{1}{i}} \leq |F|e^{-w\ln\left(\frac{n+1}{n+1-b}\right)} = |F|e^{w\ln\left(1-\frac{b}{n+1}\right)}.$$ ◀

The same idea gives the simpler bound:

▶ **Corollary 16.** *Let $F$ be a monotone DNF where each clause has width at least $w$. Then for any integer $b$ there is some restriction $\rho$ with $|\rho| \leq b$ such that $|F\restriction_\rho| < |F|e^{-wb/n}$.*

With this idea, we can remove all large clauses fixing few variables. For the non-monotone case, we only remove half the average number of clauses with each variable, giving:

▶ **Corollary 17.** *Let $F$ be a collection of clauses. Then there is some restriction $\rho$ fixing $n/p$ variables such that $F\restriction_\rho$ has width $w = 2\ln(|F|)p$.*

## 3.3 Monotone DNF Size

We prove that any DNF with a good chance of "noticing" inputs from $D_\epsilon$ has a large size.

▶ **Lemma 18.** *Suppose for $\epsilon \in (0, 1/2)$, there is a monotone DNF $F$ with $F(Maj^1_\epsilon) = 1$ and $\Pr[F(D_\epsilon) = 0] \geq 1/n^\alpha$ for constant $\alpha$. Then $F$ has $\tilde{\Omega}\left(\epsilon n^{1+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}\right)$ clauses.*

**Proof.** The idea is to restrict our function until we are only promised it outputs 1 on an $\mathrm{Maj}^1_{\epsilon/\ln(n)}$ input. Using Lemma 15, we can do this in such a way that eliminates a large fraction of clauses. Then since we still need to output 1 if we have fewer than $\frac{\epsilon n}{\ln(n)}$ more zeros, we can choose these remaining $\frac{\epsilon n}{\ln(n)}$ zeros to each eliminate one clause, showing that there are still $\frac{\epsilon n}{\ln(n)}$ clauses left. This will imply that we must have started with the claimed number of clauses.

For $w = \log_\epsilon\left(\frac{\ln(n)^5}{n\epsilon\ln(\epsilon)^2}\right)$, by Corollary 14, there is restriction $\rho$ with $|\rho| \leq \frac{\epsilon n}{\ln(n)}$ and $F\restriction_\rho$ that has no clauses smaller than $w$. Denote $F_2 = F\restriction_\rho$. Note $F_2$ solves $F_2\left(\mathrm{Maj}^1_{\epsilon(1-1/\ln(n))}\right) = 1$ and has no clauses smaller than $w$.

Now we use Lemma 15 to get restriction $\rho_2$ that assigns $\epsilon n(1 - 2/\ln(n))$ variables and:

$$|F_2\restriction_{\rho_2}| \leq |F_2|e^{w\ln\left(1-\frac{\epsilon n(1-2/\ln(n))}{n+1}\right)}.$$

Now we simplify the above exponent. For $0 < x < \frac{1}{2}$ and $0 < y$, by a Taylor argument we have $\ln(1 - x + y) \leq \ln(1 - x) + 2y$. Then for sufficiently large $n$:

$$\ln\left(1 - \frac{\epsilon n(1-2/\ln(n))}{n+1}\right) = \ln\left(1 - \epsilon + \frac{\epsilon}{n+1} + \frac{2\epsilon n}{n+1}\frac{1}{\ln(n)}\right) \leq \ln(1-\epsilon) + \frac{5\epsilon}{\ln(n)}.$$

Now including $w$,

$$\begin{aligned} w\ln\left(1 - \frac{\epsilon n(1-2/\ln(n))}{n+1}\right) \leq& \frac{\ln(n) - \ln\left(\frac{\ln(n)^5}{\epsilon\ln(\epsilon)^2}\right)}{\ln(1/\epsilon)}\left(\ln(1-\epsilon) + \frac{5\epsilon}{\ln(n)}\right) \\ <& \frac{\ln(n)\ln(1-\epsilon)}{\ln(1/\epsilon)} - \frac{\ln\left(\frac{\ln(n)^5}{\epsilon\ln(\epsilon)^2}\right)\ln(1-\epsilon)}{\ln(1/\epsilon)} + \frac{5}{\ln(1/\epsilon)}. \end{aligned}$$

Then applying this to our size bound

$$\begin{aligned}|F_2 \restriction_{\rho_2}| \leq & |F_2| e^{w \ln\left(1-\frac{\epsilon n(1-2/\ln(n))}{n+1}\right)} \\ < & |F_2| e^{\frac{\ln(n)\ln(1-\epsilon)}{\ln(1/\epsilon)} - \frac{\ln\left(\frac{\ln(n)^5}{\epsilon \ln(\epsilon)^2}\right)\ln(1-\epsilon)}{\ln(1/\epsilon)} + \frac{5}{\ln(1/\epsilon)}} \\ < & |F_2| n^{\frac{\ln(1-\epsilon)}{\ln(1/\epsilon)}} 2\ln(n)^5 e^8.\end{aligned}$$

Since $\rho$ and $\rho_2$ only restricts $\epsilon n\left(1-\frac{1}{\ln(n)}\right)$ clauses, $F_2 \restriction_{\rho_2} (\mathrm{Maj}^1_{\epsilon/\ln(n)}) = 1$. Further, since F is monotone, $\rho$ and $\rho_2$ only fixed variables to 0. Therefore, $F_2 \restriction_{\rho_2} \neq 1$. Then $F_2 \restriction_{\rho_2}$ must have at least $\frac{\epsilon n}{\ln(n)}$ clauses. Thus:

$$\begin{aligned}\frac{\epsilon n}{\ln(n)} \leq & |F_2 \restriction_{\rho_2}| \leq e^8 |F_2| n^{\frac{\ln(1-\epsilon)}{\ln(1/\epsilon)}} 2\ln(n)^5 \\ \frac{\epsilon n^{1+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}}{2e^8 \ln(n)^6} \leq & |F_2|.\end{aligned}$$

$F$ has at least as many clauses as $F_2$, thus $|F| = \tilde{\Omega}\left(\epsilon n^{1+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}\right)$. ◀

## 3.4 Monotone Circuit Size Lower Bounds

Now we prove the monotone depth-3 promise majority circuit lower bounds.

▶ **Theorem 3.** *For any $\epsilon \in (0, 1/2)$, a* monotone*, depth-3 circuit solving the $\epsilon$-promise majority problem must have size $\tilde{\Omega}\left(\epsilon^3 n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}\right)$.*

**Proof.** Let $F$ be a monotone depth-3 circuit computing $\epsilon$-promise majority. We will refer to the first level gates as clauses, and the second level gates as DNFs. Let $|F|$ refer to the number of clauses in $F$, and $\|F\|$ refer to the number of DNFs. If $F$ has more than $n^{2+\alpha}$ gates, we are done. So suppose it does not.

Let $\alpha = \frac{\ln(1-\epsilon+3\epsilon/\ln(n))}{\ln(\epsilon-3\epsilon/\ln(n))}$. We can show that

$$\alpha > \frac{\ln(1-\epsilon)}{\ln(\epsilon)} - O\left(\frac{1}{\ln(n)}\right).$$

So if we show $|F| = \tilde{\Omega}\left(\epsilon^3 n^{2+\alpha}\right)$, then the second term in $\alpha$ becomes a constant.

First, from Corollary 17, we have a restriction $\rho$ fixing $\frac{\epsilon n}{\ln(n)}$ variables such that any clause wider than $w = 2\ln(|F|)\frac{\ln(n)}{\epsilon}$ is set to 0. Let $F_2 = F \restriction_{\rho}$. See that $F_2$ solves the $\epsilon\left(1-\frac{1}{\ln(n)}\right)$-promise majority problem and has no clauses wider than $6\frac{\ln(n)^2}{\epsilon}$.

By Lemma 18, every DNF $G$ with $\Pr[G(D_{\epsilon(1-3/\ln(n))}) = 0] \geq 1/n^{3+\alpha}$ has at least $c\epsilon n^{1+\alpha}$ clauses for some polylogarithm $c$. Let $F_3$ be the sub circuit of $F_2$ with only the DNFs of $F_2$ larger than $c\epsilon n^{1+\alpha}$.

Since no clauses are wider than $w$, we can set any $m$ clauses in $F_3$ to 0 by fixing only $mw$ variables. Then, analogous to Corollary 16, there exists a restriction $\rho_2$ fixing $\epsilon n/\ln(n)$ variables to 1 such that:

$$\|F_3 \restriction_{\rho_2}\| \leq \|F_3\| e^{-c\epsilon n^{1+\alpha}(|\rho_2|/w)/|F_3|},$$

where $\|F_3 \restriction_{\rho_2}\|$ is the number of DNFs in $F_3$ not fixed to 1 or 0 under the restriction $\rho_2$.

See that $F_2 \restriction_{\rho_2}$ still solves the $\epsilon(1-2/\ln(n))$-majority problem. By a central limit theorem, $D_{\epsilon(1-2/\ln(n))}$ has a constant nonzero probability of being in $\mathrm{Maj}^0_{\epsilon(1-2/\ln(n))}$. Since $F_2$ has fewer than $n^{2+\alpha}$ DNFs (by assumption), some DNF in $F_2$, $A$, must be 0 on $D_{\epsilon(1-2/\ln(n))}$ with probability greater than $1/n^{3+\alpha}$. By Lemma 18, $A$ has size at least $c\epsilon n^{1+\alpha}$. Thus $A$ must also be in $F_3$. Thus $\|F_3 \restriction_{\rho_2}\| \geq 1$.

Now we can compute a lower bound for $|F_3|$:

$$\begin{aligned} 1 \leq & \|F_3 \restriction_{\rho_2}\| \leq \|F_3\| e^{-c\epsilon n^{1+\alpha}\frac{|\rho_2|}{w|F_3|}} \\ e^{c\epsilon^2 n^{2+\alpha}\frac{1}{w|F_3|\ln(n)}} \leq & \|F_3\| \\ c\epsilon^3 n^{2+\alpha}\frac{1}{2\ln(|F|)\ln(n)|F_3|\ln(n)} \leq & \ln(\|F_3\|) \\ \tilde{\Omega}\left(\epsilon^3 n^{2+\alpha}\right) \leq & |F_3|. \end{aligned}$$

Using the definition of $\alpha$ and that $|F| > |F_3|$ we get:

$$|F| \geq \tilde{\Omega}\left(\epsilon^3 n^{2+\alpha}\right) \geq \tilde{\Omega}\left(\epsilon^3 n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}-O\left(\frac{1}{\ln(n)}\right)}\right) \geq \tilde{\Omega}\left(\epsilon^3 n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}\right). \quad \blacktriangleleft$$

## 4 General Depth-3 Circuits

The proof of the size lower bound for general depth-3 circuits computing promise majority is almost the same as the monotone case, except for the proof that DNFs must be large. We only prove our DNF size lower bound here, the circuit lower bound follows similar to the proof of Theorem 3.

▶ **Lemma 19.** *Suppose $\epsilon \in (0, 1/2)$, and $F$ is a DNF such that $\Pr[F(D_\epsilon) = 0] \geq 1/n^\alpha$ for some constant $\alpha$ and $F(Maj^1_\epsilon) = 1$. Then $F$ has size at least $\tilde{\Omega}\left(\epsilon n^{1+\frac{\ln(1-\epsilon^2)}{2\ln(\epsilon)}}\right)$.*

**Proof.** First, see that if $F(\mathrm{Maj}^1_\epsilon) = 1$ and $F \neq 1$, there must be at least $\epsilon n$ clauses. Otherwise we could fix one variable in each clause to 0 using fewer than $n\epsilon$ zeros. Then for $\epsilon = \tilde{O}\left(\frac{1}{\sqrt{n}}\right)$ the lemma is satisfied. So take $\epsilon = \omega\left(\frac{\ln(n)^3}{\sqrt{n}}\right)$.

Let $m = \epsilon n(1-2/\ln(n))$ and $w = \log_\epsilon(\frac{\ln(n)^5}{n\epsilon\ln(\epsilon)^2})$. We will define a sequence of probabilistic restrictions, $\rho_0, ..., \rho_m$, each restricting one more variable according to $D_\epsilon$. At the same time we will construct a sequence of sub DNFs of $F$, $F_0, ..., F_m$, each a subset of the last, so that each $F_i \restriction_{\rho_i}$ has width at least $w$.

Informally, with decent probability each $F_i$ is significantly smaller than the last. Thus by a Chernoff bound, with high probability $F_m$ has a small fraction of the clauses of $F$. Then we use Corollary 14 to eliminate the small width clauses in $F_m \restriction_{\rho_m}$. With good probability the DNF will still not be 1, in which case it must still have an almost linear number of clauses. Thus there must have been many clauses to destroy so many and have so many left.

Let $\rho_0$ restrict no variables and $F_0$ be $F$ restricted to clauses wider than $w$. Then for any $i$, let $\rho_i$ be $\rho_{i-1}$ plus restricting whichever variable appears in the most clauses in $F_{i-1} \restriction_{\rho_{i-1}}$ to one with probability $\epsilon$ and 0 otherwise. Then let $F_i$ be the clauses such that they have width greater than $w$ in $F \restriction_{\rho_i}$. See that $F_i \subseteq F_{i-1}$, since further restrictions will only decrease the size and number of clauses.

With probability at least $\epsilon$, $\rho_i$ will eliminate at least $\frac{|F_{i-1}|w}{2(n-i+1)}$ clauses. Thus:

$$\Pr\left[|F_{i+1}| \leq |F_i|\left(1 - \frac{w}{2(n-i)}\right)\right] \geq \epsilon.$$

Let $k$ be the number of times the above inequality holds. By an argument similar to Lemma 15:

$$|F_m| \leq |F_0| \prod_{i=0}^{k-1} \left(1 - \frac{w}{2(n-i)}\right)^k \leq |F_0| e^{\frac{w}{2}\ln\left(1-\frac{k}{n+1}\right)}.$$

See the expected value of $k$ is at least $m\epsilon$. By a Chernoff bound, we have:

$$\Pr[k < (1 - \frac{1}{\ln(n)})\epsilon m] \leq e^{-\frac{\epsilon m}{2\ln(n)^2}} < e^{-\frac{\epsilon^2 n}{\ln(n)^3}}.$$

Now, notice that $\rho_m$ only sets variables according to an $\epsilon$ biased distribution. So if we just finish sampling the rest of the variables from $D_\epsilon$, it is the same as sampling all the variables from $D_\epsilon$. Thus:

$$\mathbb{E}_{\rho_m}[\Pr[F \restriction_{\rho_m} (D_\epsilon) = 0]] = \Pr[F(D_\epsilon) = 0].$$

We need high probability that $F \restriction_{\rho_m}$ still outputs 0 with polynomial probability on $D_\epsilon$. Applying the above equation and our assumption we get:

$$\begin{aligned}
\frac{1}{n^\alpha} \leq& \mathbb{E}_{\rho_m}[\Pr[F \restriction_{\rho_m} (D_\epsilon) = 0]] \\
\leq& \frac{1}{n^{2\alpha}} + \Pr_{\rho_m}\left[\Pr[F \restriction_{\rho_m} (D_\epsilon) = 0] > \frac{1}{n^{2\alpha}}\right] \\
\frac{1}{n^\alpha} - \frac{1}{n^{2\alpha}} \leq& \Pr_{\rho_m}\left[\Pr[F \restriction_{\rho_m} (D_\epsilon) = 0] > \frac{1}{n^{2\alpha}}\right].
\end{aligned}$$

The probability that $\rho_m$ has both $\Pr[F \restriction_{\rho_m} (D_\epsilon) = 0] > 1/n^{2\alpha}$ and $k > (1 - \frac{1}{\ln(n)})\epsilon m$ is at least $\frac{1}{n^\alpha} - \frac{1}{n^{2\alpha}} - e^{-\frac{\epsilon^2 n}{\ln(n)^3}}$, which for large $n$ is positive. Then take such $\rho_m$ as $\rho$.

By Corollary 14, we have a restriction of $F|_\rho$, $\rho'$, which restricts $\epsilon n/\ln(n)$ variables and leaves no clauses of width less than w, and has

$$\Pr[F \restriction_\rho \restriction_{\rho'} (D_\epsilon) = 0] \geq \Pr[F \restriction_\rho (D_\epsilon) = 0] \geq \frac{1}{n^{2\alpha}}.$$

Now call $F' = F \restriction_\rho \restriction_{\rho'}$. See that $F'$ has fixed $\epsilon n(1 - \frac{1}{\ln(n)})$ variables. Thus it still satisfies $F'(\mathrm{Maj}^1_{\epsilon/\ln(n)}) = 1$. Since $F' \neq 1$, $|F'| \geq \epsilon n/\ln(n)$. The clauses in $F'$ had width greater than $w$ in $F_m$, otherwise $\rho'$ would have set them to 0. Thus $|F_m| \geq \epsilon n/\ln(n)$. Together we have:

$$\begin{aligned}
\frac{\epsilon n}{\ln(n)} \leq& |F_0| e^{\frac{w}{2}\ln\left(1-\frac{k}{n+1}\right)} \\
\leq& |F_0| e^{\frac{w}{2}\ln\left(1-\frac{(1-1/\ln(n))\epsilon m}{n+1}\right)} \\
\leq& |F_0| e^{\frac{\ln\left(\frac{n\epsilon\ln(\epsilon)^2}{\ln(n)^5}\right)}{2\ln(1/\epsilon)}\left(\ln\left(1-\epsilon^2\right)+6\epsilon^2/\ln(n)\right)} \\
\tilde{\Omega}\left(\epsilon n^{1+\frac{\ln\left(1-\epsilon^2\right)}{2\ln(\epsilon)}}\right) \leq& |F_0|.
\end{aligned}$$

Thus $F$ has at least $\tilde{\Omega}\left(\epsilon n^{1+\frac{\ln\left(1-\epsilon^2\right)}{2\ln(\epsilon)}}\right)$ clauses. ◀

## 5 Circuit Upper Bounds

This section mostly uses standard techniques and the details are left for the full paper. A close analysis of Ajtai's [2] promise majority circuits gives:

▶ **Theorem 20.** *For any $\epsilon \in (0, 1/2)$, there exists monotone, depth-3 circuits solving the $\epsilon$-promise majority problem with size $O\left((\epsilon \ln(\epsilon))^2 n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)-\ln(1-\epsilon)}}\right)$.*

This also gives the corollary we will use for our stronger upper bounds for higher depth.

▶ **Corollary 21.** *For any $\epsilon = O\left(\frac{\ln(\ln(n))}{\ln(n)}\right)$, there are monotone, depth-3 circuits solving the $\epsilon$-promise majority problem with size $O\left(n^2\right)$.*

Using random walks on expander graphs, we can amplify our promise. The polylogarithmic factor in the size depends on $\epsilon$ and k.

▶ **Lemma 22.** *For any constant $k$ and $\epsilon \in (0, 1/2)$, there exists P-Uniform, monotone, depth-3 circuits with size $\tilde{O}(n)$ amplifying a $Maj_\epsilon^0$ input to a $Maj^0_{\frac{1}{\ln(n)^k}}$ output and a $Maj_\epsilon^1$ input to a $Maj^1_{\frac{1}{\ln(n)^k}}$ output.*

With amplification and quadratic-size circuits, we can trivially prove the existence of depth-4, size-$\tilde{O}(n^2)$ circuits for promise majority. But the circuit size only depends on the number of potential inputs (*not* the number of bits used to represent them). Thus the circuit has size $O(n^2)$.

▶ **Theorem 5.** *For constant $\epsilon \in (0, 1/2)$, there exists* non *uniform, monotone, depth-*4*, size-$O\left(n^2\right)$ circuits solving the $\epsilon$-promise majority problem.*

We can apply promise majority circuits in a divide and conquer fashion to get the following:

▶ **Lemma 23.** *If there are depth-3 circuits with size $n^\alpha$ solving $\frac{1}{\ln(n)}$-promise majority, then for any positive integer $k$, there are depth-$(1+2k)$ circuits solving $\frac{1}{\ln(n)^k}$-promise majority with size*

$$kn^{\frac{1}{1-\left(\frac{\alpha-1}{\alpha}\right)^k}},$$

*which is uniform and monotone if the depth-3 circuits are uniform and monotone.*

Combining Lemma 23 with amplification and our quadratic-sized majority gives:

▶ **Theorem 6.** *For constant $\epsilon \in (0, 1/2)$, there exists* non *uniform, monotone, depth-$(2+2k)$ circuits solving the $\epsilon$-promise majority problem with size $\tilde{O}\left(n^{\frac{1}{1-2^{-k}}}\right)$.*

For uniform circuits, we refine Viola's result [14] by giving a more efficient way to use the random walks in the existing algorithm.

▶ **Theorem 24.** *There exists P-uniform, monotone, depth-3, size-$O\left(n^{3+o(1)}\right)$ circuits solving the $\frac{1}{\ln(n)}$-promise majority problem.*

Again applying amplification and divide and conquer we get:

▶ **Theorem 7.** *For constant $\epsilon \in (0, 1/2)$, there exists P-uniform, monotone, depth-$(2+2k)$ circuits solving the $\epsilon$-promise majority problem with size $n^{\frac{1}{1-\left(\frac{2}{3}\right)^k}+o(1)}$.*

## 6 Closing Statements & Open Problems

Some technical details, especially the upper bounds, have been left to the full version of the paper [7] on ECCC at https://eccc.weizmann.ac.il/report/2020/122/.

These results are essentially tight in the following sense. For a wide range of $\epsilon$, between $\epsilon = o(1)$ and $\epsilon = n^{-o(1)}$, the optimal size of depth-3 circuits for $\epsilon$-promise majority is $n^{2\pm o(1)}$.

These lower bounds do not obviously extend to depth-4 circuits, so the right size for promise majority at higher depths is less clear. Better amplification plus Ajtai's promise majority circuit can actually achieve circuits with size significantly smaller than $n^2$. So our upper bounds are not optimal for depths greater than 3.

For depth-3 circuits computing promise majority, we gave four different size bounds: a lower bound for monotone circuits, a lower bound for general circuits, an upper bound for monotone circuits, and an upper bound for uniform monotone circuits. Each of these bounds differs by a polynomial factor, but we suspect they are equal.

Finally, here are some open problems:

1. Is there a way to derandomize any depth-$d$, size-$O(n)$, randomized circuit to get a depth-$(d+2)$, size-$O(n^2)$, deterministic circuit?
   We did not find any function $f$ that has a randomized, depth-$d$, size-$O(n)$ circuit, $R$, computing $f$, but no deterministic, depth-$(d+2)$, size-$O(n^2)$ circuit computing $f$. We only showed that taking promise majority over $O(n)$ copies of $R$ (as you would with an ideal PRG) would give super-quadratic circuits. There may always be some other deterministic, depth-$(d+2)$, size-$O(n^2)$ circuit computing $f$.
2. Do negations help solve promise majority?
   Our lower bounds for monotone circuits are better than our general lower bounds. It does not seem like negations should help, but we were unable to rule it out.
3. What is optimal size for depth-3 circuits computing $\epsilon$-promise majority?
   For constant $\epsilon \in (0, 1/2)$, there is a polynomial gap between even our monotone lower bounds $\tilde{\Omega}\left(n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)}}\right)$, and upper bounds $O\left(n^{2+\frac{\ln(1-\epsilon)}{\ln(\epsilon)-\ln(1-\epsilon)}}\right)$.
   For constant $\alpha \in (0, 1/2)$ and $\epsilon = n^{-\alpha}$, there is a polynomial gap between our lower bounds $\tilde{\Omega}\left(n^{2-3\alpha}\right)$ and our upper bounds $\tilde{O}\left(n^{2-2\alpha}\right)$.
4. What is the optimal size for depth greater than 3?
   Chaudhuri and Radhakrishnan [6] gave size lower bounds of roughly $\Omega\left(n^{1+\frac{1}{2^{2d}}}\right)$ for depth-$d$ $\epsilon$-promise majority circuits, while we only achieve upper bounds of roughly $\Omega\left(n^{1+\frac{1}{2^{d/2-1}}}\right)$.
5. Do these bounds extend to AC0 with parity, or other circuit classes below TC0?
6. Are there uniform depth-3 circuits for promise majority with the same size as Ajtai's construction? Can we get uniform, depth-4, quadratic size circuits for promise majority?

## References


1 Leonard Adleman. Two theorems on random polynomial time. In *Proceedings of the 19th Annual Symposium on Foundations of Computer Science*, SFCS '78, page 75–83, USA, 1978. IEEE Computer Society.

2 Miklós Ajtai. Sigma11-formulae on finite structures. *Ann. Pure Appl. Log.*, 24:1–48, 1983.

3 Miklós Ajtai. Approximate counting with uniform constant-depth circuits. In *Advances In Computational Complexity Theory*, volume 13, pages 1–20, 1993.

4 Miklós Ajtai and Michael Ben-Or. A theorem on probabilistic constant depth computations. In *STOC '84*, pages 471–474, 1984.

5 Kazuyuki Amano. Bounds on the size of small depth circuits for approximating majority. In *Proceedings of the 36th International Colloquium on Automata, Languages and Programming: Part I*, ICALP '09, page 59–70, Berlin, Heidelberg, 2009. Springer-Verlag.

6 Shiva Chaudhuri and Jaikumar Radhakrishnan. Deterministic restrictions in circuit complexity. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 30–36, New York, NY, USA, 1996. Association for Computing Machinery. doi:10.1145/237814.237824.

7 Joshua Cook. Size bounds on low depth circuits for promise majority. In *The Electronic Colloquium on Computational Complexity*, 2020.

8 Dean Doron, Dana Moshkovitz, Justin Oh, and David Zuckerman. Nearly optimal pseudorandomness from hardness. In *To appear in The proceedings of the 61st IEEE Symposium on Foundations of Computer Science*, 2020.

9 Johan Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, STOC '86, page 6–20, New York, NY, USA, 1986. Association for Computing Machinery.

10 Johan Håstad, Ingo Wegener, Norbert Wurm, and Sang-Zin. Yi. Optimal depth, very small size circuits for symmetrical functions in ac0. *Information and Computation*, 108(2):200–211, 1994.

11 Nutan Limaye, Srikanth Srinivasan, and Utkarsh Tripathi. More on $AC^0[\oplus]$ and variants of the majority function. In *39th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2019)*, volume 150, pages 22:1–22:14, 2019.

12 Ryan O'Donnell and Karl Wimmer. Approximation by dnf: Examples and counterexamples. In *Proceedings of the 34th International Conference on Automata, Languages and Programming*, ICALP'07, page 195–206, Berlin, Heidelberg, 2007. Springer-Verlag.

13 Prabhakar Ragde and Avi Wigderson. Linear-size constant-depth polylog-threshold circuits. *Information Processing Letters*, 39:143–146, 1991.

14 Emanuele Viola. On approximate majority and probabilistic time. *Computational Complexity*, 18:337–375, 2009.

15 Emanuele Viola. Randomness buys depth for approximate counting. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 230–239, 2011.