

Breaking the Parity Barrier for Constant-Depth Circuits

Nikolai Chukhin*

Abstract

A constant-depth circuit consists of AND and OR gates of unbounded fan-in, arranged in a constant number of layers, that read the input literals; for example, a depth-three circuit is an OR of CNFs or an AND of DNFs. The classical lower bound of Håstad (1989) states that every depth- d circuit computing the parity function has $2^{\Omega(n^{1/(d-1)})}$ gates. This *parity barrier* stood for decades: no explicit function was known to require depth- d circuits of size $2^{\omega(n^{1/(d-1)})}$ for any constant d . OpenAI (2026) recently announced that they broke this barrier for depth-three circuits: they gave an explicit function in P that requires OR-AND-OR circuits of size $2^{\omega(\sqrt{n})}$.

In this paper, we break the parity barrier at every constant depth with a simpler function. We prove that for every fixed $d \geq 3$, every depth- d circuit computing the trilinear function $\sum_{i,j} a_{i+j} x_i y_j \bmod 2$ for $x, y \in \{0, 1\}^n$ and $a \in \{0, 1\}^{2n-1}$, requires $2^{\Omega((n \log n / \log \log n)^{1/(d-1)})}$ gates. Our proof combines the restriction lemma of OpenAI, for which we give a short new proof, with Håstad's switching lemma and the sparsification lemma of Calabro, Impagliazzo, and Paturi (2006).

1 Constant-Depth Circuits and the Parity Barrier

Circuits of constant depth with AND and OR gates of unbounded fan-in are one of the few models of computation for which exponential lower bounds are known. Still, proving stronger lower bounds for them is one of the central problems in circuit complexity, because of their connection with general circuits. Valiant [Val77, Val83] showed that every function computed by a circuit of fan-in two, linear size, and logarithmic depth can be computed by a depth-three circuit of size $2^{O(n/\log \log n)}$, so a lower bound of $2^{\omega(n/\log \log n)}$ for an explicit function would give the first superlinear lower bound for such circuits. See [Vio09, GKW21] for stronger connections between constant-depth lower bounds and general circuit lower bounds. Yet, the known lower bounds for explicit functions are far from this.

The parity barrier. A line of work on constant-depth circuits [Ajt83, FSS84, Yao85] culminated in Håstad's switching lemma [Hås89], which gives the bound $2^{\Omega(n^{1/(d-1)})}$ for depth- d circuits computing the parity function. Håstad, Jukna, and Pudlák [HJP95] developed a simple top-down method that improved the constant in the exponent for depth three; Göös, Riazanov, Sofronova, and Sokolov [GRSS23] extended it to depth four, Korten [Kor26] recently extended it to every

*JetBrains Research. Email: buyolitsez1951@gmail.com

depth, and Kardeş and Rossman [KR26] gave a different top-down argument. Paturi, Pudlák, and Zane [PPZ99] proved that parity requires depth-three circuits of size $\Omega(n^{1/4}2^{\sqrt{n}})$, which is tight up to a constant factor [KPPY84, PPZ99]. The best depth-three lower bound for an explicit function was $2^{(\pi/\sqrt{6})\sqrt{n}-o(\sqrt{n})}$, due to Paturi, Pudlák, Saks, and Zane [PPSZ05]. Håstad’s bound $2^{\Omega(n^{1/(d-1)})}$ also holds for the majority function [Hås89], which looked promising for breaking the parity barrier, since no matching upper bound was known for it [Bop86, KPPY84, Ama23], and Håstad, Jukna, and Pudlák [HJP95] asked whether it requires larger depth-three circuits (see also [LRT22, GPP⁺24]). Recently, Lecomte and Ramakrishnan [LR26] constructed depth- d circuits of size $2^{O(n^{1/(d-1)})}$ for every symmetric function and every fixed d , so no symmetric function, and in particular not majority, can break the barrier.

Multilinear functions. Goldreich and Wigderson [GW20] proposed to study t -linear functions over $\mathbb{F}_2$ as candidates for strong lower bounds for constant-depth circuits. A function $F(x^{(1)}, \dots, x^{(t)})$ of t blocks of input bits is t -linear if it is linear over $\mathbb{F}_2$ in each block when the other blocks are fixed; equivalently, F is the parity of some products $x_{i_1}^{(1)} \dots x_{i_t}^{(t)}$, each with one variable from every block. For example, the inner product $\sum_i x_i y_i \bmod 2$ is 2-linear, and parity is 1-linear. They also started a study of *canonical* depth-three circuits for multilinear functions, because of their connection with arithmetic circuits [GW20]. As a first step, they asked for an explicit multilinear function that requires canonical circuits of size $2^{\Omega(n^c)}$ for some $c > 1/2$. Goldreich and Tal [GT18] found one by proving that random Toeplitz matrices are rigid; in particular, they showed that the trilinear function

$$f_n(x, y, a) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{i+j} x_i y_j \bmod 2,$$

where $x, y \in \{0, 1\}^n$ and $a \in \{0, 1\}^{2n-1}$, requires canonical depth-three circuits of size $2^{\Omega(n^{3/5})}$; see also [GT20, Gol22] for further results on canonical circuits. However, for general depth-three circuits, no lower bound of $2^{\omega(\sqrt{n})}$ was known for any explicit t -linear function.

Beyond the barrier. OpenAI [Ope26] recently announced that they broke the parity barrier for depth-three circuits. They constructed an explicit function in P that requires OR–AND–OR circuits of size $2^{\omega(\sqrt{n})}$. Their function hashes a part of the input into the ring $\mathbb{F}_2[Z]/(P)$ for a polynomial P of degree $\Theta(n^{2/3})$ and evaluates a polynomial of degree $\Theta(n^{1/6})$; the hash, P , and the polynomial are part of the input. Implicitly, their proof gives the lower bound $2^{\Omega(\sqrt{n \log \log n / \log \log \log n})}$.

Our results. We show that the trilinear function f_n of Goldreich and Tal [GT18] breaks the barrier at every depth.

Theorem 1.1. *For every fixed $d \geq 3$, every depth- d circuit that computes f_n has*

$$2^{\Omega((n \log n / \log \log n)^{1/(d-1)})}$$

gates.

To our knowledge, for every fixed $d \geq 4$, Theorem 1.1 gives the first lower bound of $2^{\omega(n^{1/(d-1)})}$ for depth- d circuits computing an explicit function. For $d = 3$, our exponent is larger than the one

given by the argument of [Ope26]. Our proof also gives the bound of Theorem 1.1 for their function, at every depth (Section 4).

In fact, our proof shows that for almost every Toeplitz matrix R , the bilinear form $x^\top Ry$ on $2n$ variables requires depth- d circuits of size $2^{\Omega((n \log n / \log \log n)^{1/(d-1)})}$. On the other hand, we observe that f_n has depth- d circuits with $2^{O(n^{2/d})}$ gates (Theorem 5.1), so its depth- d complexity is $2^{n^{\Theta(1/d)}}$ for every fixed $d \geq 3$. We also give a shorter proof of the main lemma of [Ope26], with better parameters (Lemma 3.1).

AI disclosure. The manuscript of [Ope26] was produced by an internal OpenAI model. The author tried to understand and simplify their proof in discussions with ChatGPT 6 Astra, and our improvement for depth three was found in this process. The extension to every depth and the short proof of the restriction lemma were also found during the writing of this manuscript. This manuscript was written with the help of Claude Opus 5.5, which helped to find references and to draft the new proofs. The author takes full responsibility for the correctness of the paper.

Since our results follow a natural route, others may have obtained them as well. Our main goal is to deepen the understanding of constant-depth circuits, so we follow the example of Lecomte and Ramakrishnan [LR26]: we would be glad to merge such work into one paper instead of competing.

Acknowledgments. Lower bounds for constant-depth circuits are close to the author’s research interests, so the author would have read the preprint of OpenAI [Ope26] in any case. The inspiration to write a paper that explains its result to a human reader, however, came from the preprint of Lecomte and Ramakrishnan [LR26], whom the author thanks for it. To our pleasant surprise, the strengthenings of [Ope26] came out of the process of understanding their lower bound.

1.1 Proof Overview

As in [Ope26], we derive the lower bound from an upper bound on the correlation of f_n with CNFs, using random restrictions [Sub61, FSS84, Hås89] and the covering argument of [HJP95]. In this section, we describe this method in detail, first for OR–AND–OR circuits and then for arbitrary constant-depth circuits.

Correlation. Throughout, z is a uniform input in $\{0, 1\}^n$, and $\mathbb{E}$ and $\Pr$ are over z . For a function $f: \{0, 1\}^n \rightarrow \{0, 1\}$, let $g = 2f - 1: \{0, 1\}^n \rightarrow \{-1, 1\}$ be its *sign*, that is, $g(z) = 1$ if f accepts z , and $g(z) = -1$ otherwise. The *correlation* of g with a function $H: \{0, 1\}^n \rightarrow \{0, 1\}$ is

$$\mathbb{E}[gH] = \Pr[H(z) = 1 \text{ and } f(z) = 1] - \Pr[H(z) = 1 \text{ and } f(z) = 0].$$

In other words, it is the fraction of inputs accepted by H times the bias of f on these inputs, so it is small if H accepts few inputs or if f is nearly balanced on the inputs accepted by H . For a uniformly random f and a fixed H , the correlation has mean zero and standard deviation at most $2^{-n/2}$, so small correlation with every function of a class means that f looks random to this class; see [O’D14] for more details. We write $\text{corr}_k(g) = \max_H |\mathbb{E}[gH]|$ for the largest correlation of g with a k -CNF, where H ranges over the CNFs whose clauses have at most k literals.

From circuits to correlations. Consider an OR–AND–OR circuit that computes f as the OR of the CNFs computed by its middle gates. As in the top-down method of [HJP95], we look at these CNFs, which are the inputs of the output gate. Every such CNF H accepts only inputs accepted by f , so $\mathbb{E}[H] = \mathbb{E}[gH]$. If a clause of H has width more than k , then the uniform input z violates it with probability less than 2^{-k} , so deleting such clauses from H changes it only on few inputs. Now suppose that $\text{corr}_k(g) \leq \varepsilon$ and that the circuit has s gates. Every CNF H of a middle gate has at most s clauses, and deleting its clauses of width more than k gives a k -CNF H' with $H \leq H'$. The difference $H' - H$ is nonzero only if one of the deleted clauses is violated, so $\mathbb{E}[H' - H] \leq s2^{-k}$, and hence

$$\mathbb{E}[H] = \mathbb{E}[gH] = \mathbb{E}[gH'] - \mathbb{E}[g(H' - H)] \leq \varepsilon + s2^{-k}.$$

Since f is the OR of at most s such CNFs, we get $\mathbb{E}[f] \leq s(\varepsilon + s2^{-k})$. On the other hand, the constant CNF 1 has width 0, so $|\mathbb{E}[g]| \leq \text{corr}_k(g) \leq \varepsilon$, and therefore $\mathbb{E}[f] = (1 + \mathbb{E}[g])/2 \geq (1 - \varepsilon)/2$. Thus, to show that every OR–AND–OR circuit for f has more than s gates, it suffices to show that $s(\varepsilon + s2^{-k}) < (1 - \varepsilon)/2$, which holds, for example, for $\varepsilon = 1/s^2$ and $k \approx 4 \log s$.¹

The square-root barrier. The question is how small the correlation of an explicit function with all k -CNFs with $k \approx 4 \log s$ can be. For exponential s , the width k can be very large, so correlations with such wide CNFs are hard to bound directly, but correlations with CNFs of small width can be bounded. So we use random restrictions: fixing most variables at random makes a k -CNF behave like a CNF of small width. Namely, for a small width $b \ll k$, we take a random restriction $\rho \in \{0, 1, *\}^n$ that keeps every variable alive with probability $p = b/(64k)$ and fixes it to a random bit otherwise. The main lemma of [Ope26], for which we give a simpler proof in Section 3, shows that the restricted CNFs behave like b -CNFs: on average over ρ , the correlation of a restricted CNF H_ρ with the restriction g_ρ of g is at most about $\text{corr}_b(g_\rho)$. Then, since a uniformly random input z can be obtained by first choosing the random restriction ρ and then the values of the live variables, the correlation of g with a CNF H is the average of the correlations of g_ρ and H_ρ . Hence, if $\text{corr}_b(g_\rho) \leq 2^{-\kappa m}$ for every ρ and some $\kappa > 0$, where $m \approx pn = nb/(64k)$ is the number of live variables, then $\text{corr}_k(g)$ is also about $2^{-\kappa m} \approx 2^{-\kappa nb/(64k)}$. So a larger b gives a better bound on $\text{corr}_k(g)$, but makes the bound on $\text{corr}_b(g_\rho)$ harder to prove.

Now, we describe what lower bound on depth-three circuits this approach can give. Note that there are a few limitations on the choice of the width k . On the one side, it must be at least about $4 \log s$, so that deleting the wide clauses does not change much. On the other side, a larger value of k decreases the probability $p = b/(64k)$ and leaves fewer live variables and hence gives a weaker bound on the correlation. With $k \approx 4 \log s$, the correlation $2^{-\kappa nb/(64k)}$ is at most $1/s^2$ when $\kappa nb/(256 \log s) \geq 2 \log s$, that is, when

$$\log^2 s \approx \kappa nb/512.$$

This is why the lower bound we get is only about $2^{\sqrt{\kappa nb/512}}$. Note that $\kappa \leq 1$, because the AND of one literal for each of the m live variables is a 1-CNF that accepts a single point and thus has correlation $\pm 2^{-m}$. Hence, for constant b , this gives only the square-root bound $2^{\Theta(\sqrt{n})}$, so the gain over the square root must come from a width b that grows with n . For example, for parity, Håstad's switching lemma [Hås89] gives correlation $\varepsilon = 2^{-\Omega(n/k)}$ with every k -CNF (see also [IMP12, Hås14]). Similarly,

¹Actually, it suffices to take $\varepsilon = 1/(8s)$ and $k = 2 \log s + 3$, but this changes only the constant in the exponent of the lower bound, so we use a stronger choice of ε and k to make the calculations simpler.

[Ope26] proves the bound $2^{A\sqrt{n}}$ for every constant $A > 0$ with a constant width $b = \Theta(A^2)$; letting b grow with n , their argument gives $b \approx \log \log n / \log \log \log n$, whereas ours gives $b \approx \log n / \log \log n$, as we explain below.

It remains to explain how to find an explicit function whose restrictions have small correlation with all b -CNFs for b as large as possible.

Random slices of f_n . Now, we are ready to explain why f_n is hard against constant-depth circuits. If we view x and y as the polynomials $x(Z) = \sum_i x_i Z^i$ and $y(Z) = \sum_j y_j Z^j$ over $\mathbb{F}_2$, then $f_n(x, y, a)$ is the inner product of a with the coefficient vector of the product $x(Z)y(Z)$. For the lower bound, we fix a at random, and we call the resulting function $f_n^a(x, y) = f_n(x, y, a)$ a *slice*. As shown above, it suffices to bound $\text{corr}_b(g_\rho^a)$, where g_ρ^a is the sign of f_n^a and ρ is the random restriction. For a fixed ρ and one fixed b -CNF J on the m variables of g_ρ^a , we bound the u -th moment of the correlation of g_ρ^a with J over the random a for some even number u , that is,

$$\mathbb{E}_a \left[\left(\mathbb{E}_z [g_\rho^a(z) J(z)] \right)^u \right],$$

where z is a uniform assignment to these m variables. Since u is even, the u -th power of the correlation is nonnegative, so Markov's inequality gives, for every $\delta > 0$,

$$\Pr_a \left[\left| \mathbb{E}_z [g_\rho^a(z) J(z)] \right| \geq \delta \right] \leq \delta^{-u} \mathbb{E}_a \left[\left(\mathbb{E}_z [g_\rho^a(z) J(z)] \right)^u \right].$$

That is, bounding the u -th moment of the correlation means bounding the probability over a that the correlation of g_ρ^a with J is at least δ . Expanding the u -th power shows that, since f_n is linear in a , the moment is at most the probability that u independent random inputs $(x^{(\ell)}, y^{(\ell)})$ for $\ell \in [u]$ that agree with ρ satisfy $\sum_\ell x^{(\ell)}(Z) y^{(\ell)}(Z) = 0$, so it suffices to show that this equation is unlikely. Lemmas 4.2 and 4.3 do that and show $|\mathbb{E}_z [g_\rho^a(z) J(z)]| \leq 2^{-\Omega(m)}$ with probability $1 - 2^{-\Omega(um)}$ over a . A larger u makes this probability smaller. However, f_n^a must have small correlation with *all* b -CNFs at once, and there are more than $2^{(m/b)^b}$ b -CNFs, far more than the $2^{O(um)}$ that the union bound can afford, so we need a sparsification argument to make the number of CNFs smaller.

Sparsification. The union bound argument above works for CNFs with few clauses: there are only $2^{O(Mmb \log m)}$ b -CNFs with at most $M \cdot m$ clauses over m variables, which is less than $2^{\Omega(um)}$ if $Mb \log m \ll u$. The sparsification lemma of Impagliazzo, Paturi, and Zane [IPZ01] reduces all b -CNFs to sparse ones: for every fixed $\kappa > 0$, every b -CNF on m variables is an OR of at most $2^{\kappa m}$ b -CNFs with at most $M \cdot m$ clauses each, where M depends only on b and κ . For technical reasons, our proof needs to add up the correlations of those sparse b -CNFs, so the OR of the sparse CNFs to be their sum, that is, the sparse CNFs must have disjoint sets of satisfying assignments, and [DHM⁺14] observed that the argument of [IPZ01] can be modified to guarantee this. Hence, if every sparse CNF has correlation at most $2^{-2\kappa m}$ with g_ρ^a , then $\text{corr}_b(g_\rho^a) \leq 2^{\kappa m} \cdot 2^{-2\kappa m} = 2^{-\kappa m}$. Thus, b can grow until the density $M = M(b)$ reaches about $u/(b \log m)$, and since κ is a constant, the lower bound $2^{\sqrt{\kappa n b}/512}$ derived above has exponent about $\sqrt{n b}$ for the largest such b . The original proof of [IPZ01] gives a density M that is doubly exponential in b , that is, $\log M = 2^{O(b)}$, which gives only $b \approx \log \log n$. [Ope26] reproves the disjoint version using the sunflower lemma of Erdős and Rado [ER60], but with an even larger density: $\log M$ grows like a factorial of b , which gives only $b \approx \log \log n / \log \log \log n$. We instead use the sparsification lemma of Calabro, Impagliazzo, and Paturi [CIP06, Cal09], whose density is $b^{O(b)}$, that is, $\log M = O(b \log b)$; this gives $b \approx \log n / \log \log n$ and Theorem 1.1 for $d = 3$.

Arbitrary depth- d circuits. The argument above works for OR-AND-OR circuits. In general, such a lower bound does not extend to all depth-three circuits: Håstad, Jukna, and Pudlák [HJP95] gave a function that requires OR-AND-OR circuits of size $2^{\Omega(\sqrt{n})}$, but has AND-OR-AND circuits of linear size. For f_n , however, the complement of f_n^a has sign $-g^a$, and our correlation bounds hold for it as well, so the argument applies to circuits with either output gate.

For a depth- d circuit with s gates and $d > 3$, we reduce it to a depth-three circuit using Håstad's switching lemma [Hås89]: after $d - 3$ switching steps, we get a depth-three circuit of size $s^{O(1)}$ with bottom fan-in $O(\log s)$ on about $n/O(\log s)^{d-3}$ live variables, and the argument for depth three with this number of variables in place of n gives the lower bound $2^{\Omega((nb)^{1/(d-1)})}$. See Section 4 for more details.

Why the method stops at $(n \log n)^{1/(d-1)}$. As explained above, the exponent is determined by how fast the density M grows with b . If every b -CNF on m variables could be expressed as, say, a disjoint sum of at most $2^{m/128}$ b -CNFs with $2^{O(b)} \cdot m$ clauses each, the same proof would allow $b \approx \log n$ and give the lower bound $2^{\Omega((n \log n)^{1/(d-1)})}$ for depth- d circuits. Calabro [Cal09] asked whether such a sparsification exists.

Even with the best possible sparsification, our method cannot go much further, for the following reason. We check the sparse b -CNFs one by one and then use a union bound, and our bound on the probability that a fixed one of them fails is $2^{-\Theta(um)}$, where $u \leq n$, so the union bound can afford at most $2^{O(um)}$ of them. Also, we know that any b -CNF on m variables can be expressed as a sum of at most $2^{\kappa m}$ sparse b -CNFs for some $\kappa < \frac{1}{2}$. But every family with this property has at least $\exp\left((m/b)2^{\Omega(b)}\right)$ members: a product of m/b independent random ± 1 functions on disjoint blocks of b variables has correlation at least $2^{-m/b}$ in absolute value with some b -CNF, while by the Bonami's [Bon70] (see [O'D14, Theorem 9.23]), its correlation with a fixed function is at least $2^{-m/b}2^{-\kappa m}$ in absolute value only with probability $\exp\left(-(m/b)2^{\Omega(b)}\right)$. So for a smaller family, by a union bound, some product would have correlation less than $2^{-m/b}2^{-\kappa m}$ in absolute value with every member, and hence less than $2^{-m/b}$ with every b -CNF, which is impossible. Comparing the two sizes gives $2^{\Omega(b)} \leq O(bu)$, that is, $b = O(\log n)$, so our method cannot go beyond $\sqrt{n \log n}$ for depth three, or beyond $(n \log n)^{1/(d-1)}$ for depth d . See also [SS12], which builds on [MRW05], for limits of sparsification.

2 Preliminaries

All logarithms in our paper are base two. Unless stated otherwise, the expected value $\mathbb{E}$ and probability $\Pr$ are taken over the uniform distribution on the Boolean cube $\{0, 1\}^V$. The *sign* of a function $f: \{0, 1\}^V \rightarrow \{0, 1\}$ is the function $2f - 1: \{0, 1\}^V \rightarrow \{-1, 1\}$, which is $+1$ on accepted inputs and -1 on rejected inputs.

Circuits. Circuits in this paper consist of AND and OR gates of unbounded fan-in and fan-out. They read literals, that is, variables and their negations, and constants, and the *size* of a circuit is the number of its AND and OR gates. An OR-AND-OR circuit has three layers: bottom OR gates read literals and constants, middle AND gates read bottom gates, and the output OR gate reads middle gates. Thus every middle gate computes a CNF, and the circuit computes the OR of these

CNFs. An AND–OR–AND *circuit* is defined analogously. A *depth- d circuit* is a circuit in which every path from an input to the output passes through at most d gates.

CNFs and correlation. A clause is an OR of literals, a CNF is an AND of clauses, a *term* is an AND of literals, and a DNF is an OR of terms. We always remove tautological clauses and repeated literals, so the *width* of a clause is the number of variables in it, and the width of a CNF is the maximum width of its clauses; a *b -CNF* is a CNF of width at most b , and *b -DNFs* are defined similarly. For a function $F: \{0, 1\}^V \rightarrow \mathbb{R}$, let $\text{size}_b(F)$ be the smallest sum $\sum_j |c_j|$ over all ways to write $F = \sum_j c_j J_j$ with numbers $c_j \in \mathbb{R}$ and b -CNFs J_j on $\{0, 1\}^V$. For a function $\psi: \{0, 1\}^V \rightarrow \mathbb{R}$, let $\text{corr}_b(\psi) = \max_J |\mathbb{E}[\psi J]|$, where J ranges over the b -CNFs on $\{0, 1\}^V$. By linearity, for all functions $\psi, F: \{0, 1\}^V \rightarrow \mathbb{R}$,

$$|\mathbb{E}[\psi F]| \leq \text{size}_b(F) \text{corr}_b(\psi). \quad (1)$$

Random restrictions. For $0 < p \leq 1$ and a set V of variables, a *p -random restriction* of V is a random $\rho \in \{0, 1, *\}^V$ with independent coordinates, each equal to $*$ with probability p , and to 0 and to 1 with probability $(1-p)/2$ each. We write $\text{live}(\rho) = \rho^{-1}(*)$ for the set of *live* coordinates of ρ . For a function $\psi: \{0, 1\}^V \rightarrow \mathbb{R}$, we write $\psi_\rho: \{0, 1\}^{\text{live}(\rho)} \rightarrow \mathbb{R}$ for the function obtained by fixing the coordinates outside $\text{live}(\rho)$ according to ρ . Filling the live coordinates with uniform bits produces a uniform point of $\{0, 1\}^V$, so for all functions $\psi, H: \{0, 1\}^V \rightarrow \mathbb{R}$,

$$\mathbb{E}[\psi H] = \mathbb{E}_\rho \mathbb{E}_z [\psi_\rho(z) H_\rho(z)], \quad (2)$$

where z is uniform in $\{0, 1\}^{\text{live}(\rho)}$.

Sparsification. The sparsification lemma of Impagliazzo, Paturi, and Zane [IPZ01] writes, for every fixed $\kappa > 0$, every b -CNF on m variables as an OR of at most $2^{\kappa m}$ b -CNFs, each with linearly many clauses. We use its version due to Calabro, Impagliazzo, and Paturi [CIP06, Cal09] (see also [LSX26] for a shorter proof), together with the observation of Dell, Husfeldt, Marx, Taslaman, and Wahlén [DHM⁺14] that these CNFs can be made to have disjoint sets of satisfying assignments, so that their OR is their sum.

Lemma 2.1 ([Cal09, DHM⁺14]). *For every integer $b \geq 2$ and every $0 < \kappa \leq 1$, every b -CNF H on m variables is a sum of at most $2^{\kappa m}$ b -CNFs with pairwise disjoint sets of satisfying assignments, each having at most $(b/\kappa)^{O(b)} \cdot m$ clauses.*

The switching lemma. Håstad’s switching lemma states that a random restriction is likely to turn a CNF of small width into a DNF of small width, and vice versa.

Lemma 2.2 ([Hås89], see [O’D14, Section 4.4]). *Let H be a k -CNF or a k -DNF on $\{0, 1\}^V$, let $k' \geq 1$ be an integer, and let ρ be a p -random restriction of V . Then, except with probability at most $(5pk)^{k'}$, the function H_ρ is both a k' -CNF with at most $2^{k'}$ clauses and a k' -DNF with at most $2^{k'}$ terms.*

Applying the switching lemma repeatedly gives Håstad’s depth reduction, which turns a depth- d circuit into an OR of k -CNFs.

Lemma 2.3 ([Hås89], see [O’D14, Lemma 4.28]). *Let $d \geq 3$ be an integer, let V be a set of at least two variables, and let $s \geq |V| \geq 2$. There are numbers $k = \Theta(\log s)$ and q with $1/q = \Theta(\log^{d-3} s)$, such that for every function $F: \{0, 1\}^V \rightarrow \{0, 1\}$ computed by a depth- d circuit with at most s gates and an OR output gate, it follows that for a q -random restriction φ , the function F_φ is the OR of at most $s^{O(1)}$ k -CNFs with probability at least $\frac{3}{4}$.*

3 Wide CNFs under Random Restrictions

The restriction lemma of OpenAI [Ope26, Lemma 3.1] shows that a restricted k -CNF H_ρ has bounded expected size $\text{size}_b(H_\rho)$, so by (1), it correlates with any function at most about as much as b -CNFs do, no matter how many clauses the CNF has. Below, we explain why this is not straightforward, compare the proof of [Ope26] with ours, and then give our proof, which is shorter and gives a better bound.

Let $b \geq 1$ be an integer, let H be a k -CNF on $\{0, 1\}^V$ with N clauses, and let ρ be a p -random restriction of V . A restriction ρ *falsifies* a clause C if it sets all literals of C to zero, and C is *wide* under ρ if ρ sets no literal of C to one and leaves more than b variables of C alive. Let K be the AND of the restricted clauses that are not wide, which is a b -CNF; then H_ρ is the AND of K and the wide restricted clauses, so H_ρ differs from K only at points where some wide clause is violated. We first compute how likely a clause is to be wide. Consider a clause C of width k . Then, ρ falsifies C with probability $((1-p)/2)^k$, while C is wide under ρ if and only if some $\ell > b$ of its variables are live and the other $k - \ell$ are fixed so that their literals are false, which happens with probability

$$\sum_{\ell=b+1}^k \binom{k}{\ell} p^\ell \left(\frac{1-p}{2}\right)^{k-\ell} = \theta \left(\frac{1-p}{2}\right)^k, \quad \text{where } \theta = \sum_{\ell=b+1}^k \binom{k}{\ell} \left(\frac{2p}{1-p}\right)^\ell.$$

So θ is the ratio of the probability that C is wide to the probability that ρ falsifies C . Hence, θ is small if $pk \ll b$, since then a clause of width at most k keeps on average only pk live variables, while being wide requires more than b . For our choice of $p \leq b/(64k)$, it follows that $\theta \leq 4^{-b}$. One issue is that under ρ some of the clauses can still remain wide, we will express them as a sum of b -CNFs (recall size_b).

One can use the inclusion–exclusion trick to convert all wide clauses using only clauses of width b . For a wide clause C , let v_C be the indicator that the live variables of C falsify C , so $C_\rho = 1 - v_C$, and v_C is an AND of unit clauses. Inclusion–exclusion over the wide clauses gives

$$H_\rho = K \prod_{C \text{ - wide}} (1 - v_C) = \sum_S (-1)^{|S|} K \prod_{C \in S} v_C,$$

where S ranges over the sets of wide clauses. Every summand in this expression is a b -CNF, and this sum has 2^w summands with coefficients ± 1 , where w is the number of wide clauses, so $\text{size}_b(H_\rho) \leq 2^w$; but 2^w can be huge, for example, if all N clauses share the same $k - 1$ variables, then with positive probability more than b of these variables are live and the literals of the others are false, and then every clause is wide unless ρ sets its remaining literal to one, so $\mathbb{E} 2^w$ grows exponentially with N .

The proof of [Ope26] uses ideas similar to the Razborov’s proof [Raz09] of Bazzi’s theorem [Baz09] and gives the bound $\mathbb{E} \text{size}_b(H_\rho) \leq 1/(1 - \theta)$ for $\theta < 1$, whatever N is. We give a simplified proof which gives a better bound, our argument is similar as in Wigderson’s simplification of Razborov’s proof [Raz09, Remark]; this gives $\mathbb{E} \text{size}_b(H_\rho) \leq 1$ for $\theta \leq 1$.

Lemma 3.1. *Let $k \geq 0$ and $b \geq 1$ be integers, let H be a k -CNF on $\{0, 1\}^V$, and let $0 < p < 1$ satisfy*

$$\theta = \sum_{\ell=b+1}^k \binom{k}{\ell} \left(\frac{2p}{1-p} \right)^\ell \leq 1.$$

Then, for a p -random restriction ρ of V ,

$$\mathbb{E}_\rho \text{size}_b(H_\rho) \leq 1.$$

Proof. Let $C_1, \dots, C_N$ be the clauses of H , and let $H_j = C_1 \wedge \dots \wedge C_j$, so that $H_0 = 1$ and $H_N = H$. If a clause C is wide under ρ , denote ρ^C to be the restriction that agrees with ρ and also sets the live literals of C to zero, so that it falsifies C , and let v_C be as above.

We bound $\mathbb{E}_\rho \text{size}_b((H_j)_\rho)$ by induction on j . For $j = 0$, the function $(H_0)_\rho = 1$ is a b -CNF, so $\text{size}_b((H_0)_\rho) \leq 1$. Now let $j \geq 1$ and let $C = C_j$. If ρ falsifies C , then $(H_j)_\rho = 0$, and $\text{size}_b((H_j)_\rho) = 0$. If ρ does not falsify C and C is not wide under ρ , then C_ρ is the constant 1 or a clause of width at most b , and adding it to every b -CNF of an expansion of $(H_{j-1})_\rho$ gives $\text{size}_b((H_j)_\rho) \leq \text{size}_b((H_{j-1})_\rho)$.

Otherwise, C is wide under ρ . Then $C_\rho = 1 - v_C$, and $v_C \cdot (H_{j-1})_\rho = v_C \cdot (H_{j-1})_{\rho^C}$, because $\rho(z) = \rho^C(z)$ for every z such that $v_C(z) = 1$, so

$$(H_j)_\rho = (H_{j-1})_\rho \cdot C_\rho = (H_{j-1})_\rho - v_C \cdot (H_{j-1})_\rho = (H_{j-1})_\rho - v_C \cdot (H_{j-1})_{\rho^C}.$$

Since $v_C \wedge J$ is a b -CNF for every b -CNF J , multiplying every summand of an expansion of $(H_{j-1})_{\rho^C}$ by v_C gives an expansion of $v_C \cdot (H_{j-1})_{\rho^C}$ with the same coefficients, so

$$\text{size}_b((H_j)_\rho) \leq \text{size}_b((H_{j-1})_\rho) + \text{size}_b((H_{j-1})_{\rho^C}).$$

Every ρ under which C is wide arises from a restriction ρ^C that falsifies C by making a set of $\ell > b$ variables of C live, which multiplies its probability by $(2p/(1-p))^\ell$, since each of these variables is live with probability p instead of being fixed to its value in ρ^C with probability $(1-p)/2$, and there are at most $\binom{k}{\ell}$ such sets, so, by the definition of θ ,

$$\mathbb{E} \left[\text{size}_b((H_{j-1})_{\rho^C}) \mathbf{1}_{C \text{ is wide under } \rho} \right] \leq \theta \mathbb{E} \left[\text{size}_b((H_{j-1})_\rho) \mathbf{1}_{\rho \text{ falsifies } C} \right].$$

Taking the expectation of the three cases, we get

$$\begin{aligned} \mathbb{E} \text{size}_b((H_j)_\rho) &\leq \mathbb{E} [\text{size}_b((H_{j-1})_\rho) \mathbf{1}_{\rho \text{ does not falsify } C}] + \mathbb{E} [\text{size}_b((H_{j-1})_{\rho^C}) \mathbf{1}_{C \text{ is wide under } \rho}] \\ &\leq \mathbb{E} [\text{size}_b((H_{j-1})_\rho) \mathbf{1}_{\rho \text{ does not falsify } C}] + \theta \mathbb{E} [\text{size}_b((H_{j-1})_\rho) \mathbf{1}_{\rho \text{ falsifies } C}] \\ &\leq \mathbb{E} \text{size}_b((H_{j-1})_\rho), \end{aligned}$$

and by induction on j , $\mathbb{E} \text{size}_b(H_\rho) \leq \mathbb{E} \text{size}_b((H_0)_\rho) \leq 1$. □

4 Lower Bound

We now prove [Theorem 1.1](#). We first find a slice f_n^a whose restrictions have small correlation with all k -CNFs. Then we reduce the depth to three by random restrictions and the switching lemma, which turns the restricted circuit into an OR of few k -CNFs.

Our hard function is the following trilinear function, studied by Goldreich and Tal [\[GT18\]](#).

Definition 4.1. For $x, y \in \{0, 1\}^n$ and $a \in \{0, 1\}^{2n-1}$, with coordinates numbered from zero, let

$$f_n(x, y, a) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{i+j} x_i y_j \bmod 2.$$

The function f_n has $4n - 1$ input bits and can be computed by a circuit with one parity gate on top of n^2 AND gates of fan-in three.

It is convenient to view x and y as the polynomials $x(Z) = \sum_i x_i Z^i$ and $y(Z) = \sum_j y_j Z^j$ over $\mathbb{F}_2$. The coefficient of Z^ℓ in their product is $\sum_{i+j=\ell} x_i y_j \bmod 2$, so f_n is the inner product of a with the coefficient vector of the product:

$$f_n(x, y, a) = \sum_{\ell=0}^{2n-2} a_\ell \cdot [Z^\ell] (x(Z)y(Z)) \bmod 2,$$

where $[Z^\ell]x(Z)y(Z)$ is the coefficient of Z^ℓ in the polynomial $x(Z)y(Z)$.

Fixing a gives the function $f_n^a: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ defined by $f_n^a(x, y) = f_n(x, y, a)$, which we call a *slice*. It is the bilinear form $x^\top R y$ over $\mathbb{F}_2$ given by the Hankel matrix $R = (a_{i+j})_{i,j}$, which is constant along every antidiagonal. Reversing the order of $y_0, \dots, y_{n-1}$ turns R into a Toeplitz matrix, which is constant along every diagonal.

For a restriction ρ of the $2n$ variables $x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1}$, let $T_x, T_y \subseteq \{0, \dots, n-1\}$ be the sets of indices i such that x_i is live and j such that y_j is live, so that $|\text{live}(\rho)| = |T_x| + |T_y|$. For sets $A, B \subseteq \mathbb{Z}$ and an integer j , we write $A + B = \{\alpha + \beta : \alpha \in A, \beta \in B\}$ and $A + j = A + \{j\}$.

We start with a lower bound on the sumset of a small set and a random set.

Lemma 4.2. Let $T \subseteq \{0, \dots, n-1\}$ be a random set that contains every element independently with probability p , where $pn \leq n^{3/5}$ is sufficiently large, and let $u \leq (pn)^{1/4}$ be a positive integer. Then, except with probability $n^{-\Omega(pn)}$, every set $A \subseteq \{0, \dots, n-1\}$ of at most u elements satisfies

$$|A + T| \geq |A| (|T| - pn/4).$$

Proof. Fix a set $A \subseteq \{0, \dots, n-1\}$ such that $|A| \leq u$, and call two distinct integers j and j' *intersecting* if $(A + j) \cap (A + j') \neq \emptyset$, that is, if $j - j'$ is a difference of two elements of A . So, fewer than $nu^2/2$ pairs of elements of $\{0, \dots, n-1\}$ are intersecting. Choose intersecting pairs of elements of T one by one, each disjoint from the pairs chosen before, until no such pair is left. Then no two of the remaining elements j of T are intersecting, so their sets $A + j$ are pairwise disjoint. Hence, if fewer than $pn/8$ pairs are chosen, then $|A + T| \geq |A| (|T| - pn/4)$. Otherwise, T contains h pairwise disjoint intersecting pairs for some $h = \lceil pn/8 \rceil$. There are at most $\binom{\lfloor nu^2/2 \rfloor}{h} \leq (enu^2/(2h))^h$ choices of such pairs, and their $2h$ elements all lie in T with probability p^{2h} . Since $4eu^2p \leq 4e(pn)^{3/2}/n \leq 4en^{-1/10} \leq n^{-1/20}$ for large n , this happens with probability at most

$$\left(\frac{enu^2p^2}{2h} \right)^h \leq (4eu^2p)^h \leq n^{-pn/160}.$$

A union bound over the at most $(n+1)^u \leq n^{2(pn)^{1/4}}$ sets A completes the proof. $\square$

Next, we bound the u -th moment of the correlation.

Lemma 4.3. *Let $u \geq 2$ be even, and let ρ be a restriction of x and y such that $|T_x| \geq 2u$ and every set $A \subseteq \{0, \dots, n-1\}$ of at most u elements satisfies $|A + T_y| \geq |A| |T_y|/2$. Let $J: \{0, 1\}^{\text{live}(\rho)} \rightarrow [-1, 1]$. If a is uniform in $\{0, 1\}^{2n-1}$ and g^a is the sign of f_n^a , then*

$$\mathbb{E}_a \left[\left(\mathbb{E}_z [g_\rho^a(z) J(z)] \right)^u \right] \leq 2^{-u|T_x|/4} + 2^{-u|T_y|/4}.$$

The worst case is when $J \equiv 1$, so it is convenient to keep in mind while reading the proof.

Proof. We first reduce the moment to the probability of an equation. Let $z^{(1)}, \dots, z^{(u)}$ be independent uniform points of $\{0, 1\}^{\text{live}(\rho)}$, and let $x^{(\ell)}$ and $y^{(\ell)}$ be the values of x and y given by ρ and $z^{(\ell)}$. Since u is even, the product $g_\rho^a(z^{(1)}) \cdots g_\rho^a(z^{(u)})$ is 1 if the inner product of a with the coefficient vector of the polynomial $\sum_\ell x^{(\ell)}(Z) y^{(\ell)}(Z)$ is zero, and -1 otherwise. Hence, expanding the u -th power and using $|J| \leq 1$, we get

$$\begin{aligned} \mathbb{E}_a \left[\left(\mathbb{E}_z [g_\rho^a(z) J(z)] \right)^u \right] &= \mathbb{E} \left[J(z^{(1)}) \cdots J(z^{(u)}) \mathbb{E}_a \left[g_\rho^a(z^{(1)}) \cdots g_\rho^a(z^{(u)}) \right] \right] \\ &\leq \Pr \left[\sum_{\ell=1}^u x^{(\ell)}(Z) y^{(\ell)}(Z) = 0 \right]. \end{aligned}$$

Now fix $x^{(1)}, \dots, x^{(u)}$. For every $\ell \in [u]$, split

$$y^{(\ell)}(Z) = c(Z) + \sum_{j \in T_y} y_j^{(\ell)} Z^j, \quad \text{where } c(Z) = \sum_{j \notin T_y} y_j^{(\ell)} Z^j$$

is the same for all ℓ , since ρ fixes the variables y_j with $j \notin T_y$. Hence

$$\sum_{\ell=1}^u x^{(\ell)}(Z) y^{(\ell)}(Z) = c(Z) \sum_{\ell=1}^u x^{(\ell)}(Z) + \sum_{\ell=1}^u \sum_{j \in T_y} y_j^{(\ell)} Z^j x^{(\ell)}(Z),$$

where the first summand is a fixed polynomial, and the second summand is a uniform polynomial on the space S spanned by the polynomials $Z^j x^{(\ell)}(Z)$ with $j \in T_y$ and $\ell \in [u]$. So the second summand equals the first one with probability at most $2^{-\dim S}$, and this bounds the probability that the sum is zero.

For fixed $x^{(1)}, \dots, x^{(u)}$, the span of $x^{(1)}(Z), \dots, x^{(u)}(Z)$ has a basis of polynomials with distinct degrees; let A be the set of these degrees, so that $|A|$ is the dimension of the span. The product of Z^j and the basis polynomial of degree α lies in S and has degree $\alpha + j$. Polynomials with distinct degrees are linearly independent, so $\dim S \geq |A + T_y| \geq |A| |T_y|/2$, where the last inequality follows from the statement.

It remains to show that $|A|$ is likely to be large. The coefficients of the polynomials $x^{(\ell)}(Z)$ at the positions in T_x are independent uniform bits, so $|A|$ is at least the rank of a uniform random $|T_x| \times u$ matrix over $\mathbb{F}_2$. If this rank is less than $u/2$, then the u columns of the matrix lie in a subspace of $\mathbb{F}_2^{T_x}$ of dimension $u/2$. There are at most $2^{|T_x|u/2}$ such subspaces, and all u columns lie in a fixed one with probability $2^{-(|T_x|-u/2)u}$. Hence $|A| < u/2$ with probability at most $2^{-u(|T_x|-u/2)/2} \leq 2^{-u|T_x|/4}$, since $|T_x| \geq 2u$ from the statement.

If $|A| \geq u/2$, then $\dim S \geq |A| |T_y|/2 \geq u|T_y|/4$ by the previous paragraph, so for these $x^{(1)}, \dots, x^{(u)}$, the sum is zero with probability at most $2^{-u|T_y|/4}$ over the $y^{(\ell)}$. Adding the two cases, the sum is zero with probability at most $2^{-u|T_x|/4} + 2^{-u|T_y|/4}$, as claimed. $\square$

In our proof we use two random restrictions. The first one, φ , of density q , comes from the depth reduction (Lemma 2.3), which uses the switching Lemma 2.2 to turn a depth- d circuit into an OR of k -CNFs, and the next lemma shows that the slice function f_n^a stays hard after this restriction. The second restriction, ρ , of density p , appears only in the proof of Lemma 4.4 and turns k -CNFs into b -CNFs as in the overview, so $m = qpn$ in Lemma 4.4 is the expected number of live variables of x after *both* restrictions.

Lemma 4.4. *For an integer $b \geq 2$, let M be such that every b -CNF on t variables is a sum of at most $2^{t/128}$ b -CNFs with at most Mt clauses each and with pairwise disjoint sets of satisfying assignments. Let $k \geq b$ be an integer and $0 < q \leq 1$, let $p = b/(64k)$, and suppose that $m = qpn$ is sufficiently large and satisfies $m \leq n^{3/5}$ and $bM \leq m^{1/8}$.*

Then there is $a \in \{0, 1\}^{2n-1}$ such that the sign g^a of f_n^a satisfies $\mathbb{E}_\varphi \text{corr}_k(g_\varphi^a) \leq 2^{-\Omega(m)}$, where φ is a q -random restriction of x and y .

Proof. Let $\varepsilon = 2^{-m/32}$, and given φ , let ρ be a p -random restriction of its live variables. Then the composition $\varphi\rho$, which fixes the coordinates fixed by φ or by ρ , is a qp -random restriction of x and y , so on average it leaves m variables of x and m variables of y alive. Let u be the largest even integer with $u \leq m^{1/4}$, and let $T_x = \{i : x_i \in \text{live}(\varphi\rho)\}$ and $T_y = \{j : y_j \in \text{live}(\varphi\rho)\}$ be the sets of indices of the live variables of x and of y . We call $\varphi\rho$ *good* for a if $|T_x|, |T_y| \in [m/2, 2m]$, every set $A \subseteq \{0, \dots, n-1\}$ of at most u elements satisfies $|A + T_y| \geq |A| |T_y|/2$, and $\text{corr}_b(g_{\varphi\rho}^a) \leq \varepsilon$. We first find a for which $\varphi\rho$ is not good with probability at most 4ε .

Choose $a \in \{0, 1\}^{2n-1}$ uniformly at random. A binomial random variable with mean μ is less than $\mu/2$ with probability at most $e^{-\mu/8}$ and more than 2μ with probability at most $e^{-\mu/3}$, so $|T_x|$ or $|T_y|$ lies outside $[m/2, 2m]$ with probability at most $4 \cdot 2^{-m/8} \leq 2\varepsilon$. Hence, by Lemma 4.2 for the set T_y of $\varphi\rho$, which contains every index independently with probability qp , where $qpn = m \leq n^{3/5}$ and $u \leq m^{1/4}$, except with probability $n^{-\Omega(m)} \leq \varepsilon$, every set A , such that $|A| \leq u$ satisfies $|A + T_y| \geq |A| (|T_y| - m/4) \geq |A| |T_y|/2$ if $|T_y| \geq m/2$.

Now fix φ and ρ that satisfy these two conditions, and let $t = |\text{live}(\varphi\rho)|$, so that $t \leq 4m$. Since $|T_x| \geq m/2 \geq 2u$, Lemma 4.3 and Markov's inequality show that, for every $J: \{0, 1\}^{\text{live}(\varphi\rho)} \rightarrow \{0, 1\}$,

$$\Pr_a \left[\left| \mathbb{E}[g_{\varphi\rho}^a J] \right| > 2^{-m/16} \right] \leq 2^{um/16} \left(2^{-u|T_x|/4} + 2^{-u|T_y|/4} \right) \leq 2^{1-um/16}.$$

A clause of width at most b is given by b slots, each holding one of the $2t$ literals or nothing, so there are at most $(2t+1)^b$ such clauses. Hence the number of b -CNFs with at most Mt clauses is bounded by

$$\left((2t+1)^b + 1 \right)^{Mt} \leq 2^{O(bMt \log t)} \leq 2^{O(m^{9/8} \log m)},$$

since $t \leq 4m$ and $bM \leq m^{1/8}$. By the union bound, the probability that some of them, say J , has $|\mathbb{E}[g_{\varphi\rho}^a J]| > 2^{-m/16}$ is at most

$$2^{O(m^{9/8} \log m)} \cdot 2^{1-um/16} \leq 2^{-um/32} \leq \varepsilon,$$

where the first inequality holds because $u \geq m^{1/4}/2$ and m is large. If none of them fails, then every b -CNF J on $\{0, 1\}^{\text{live}(\varphi\rho)}$ is a sum of at most $2^{t/128} \leq 2^{m/32}$ such CNFs J_i by Lemma 2.1, so

$$\left| \mathbb{E}[g_{\varphi\rho}^a J] \right| \leq \sum_i \left| \mathbb{E}[g_{\varphi\rho}^a J_i] \right| \leq 2^{m/32} \cdot 2^{-m/16} = \varepsilon.$$

Thus $\varphi\rho$ is not good with probability at most $2\varepsilon + \varepsilon + \varepsilon = 4\varepsilon$.

Since $k \geq b$, we have $p \leq 1/64$, so every summand of θ in Lemma 3.1 is at most $(4pk)^\ell/\ell! \leq (b/16)^\ell/\ell! \leq (eb/(16\ell))^\ell \leq 4^{-\ell}$, and $\theta < 1$. Now fix φ , and let H be a k -CNF on its live coordinates. By Lemma 3.1, applied to H and ρ with the live coordinates of φ in place of V , we have $\mathbb{E}_\rho \text{size}_b(H_\rho) \leq 1$. By (2) for ρ , the correlation $|\mathbb{E}[g_\varphi^a H]|$ is at most the average over ρ of $|\mathbb{E}[g_{\varphi\rho}^a H_\rho]|$, which is at most $\text{size}_b(H_\rho)\varepsilon$ by (1) if $\varphi\rho$ is good, and at most one otherwise. Hence

$$|\mathbb{E}[g_\varphi^a H]| \leq \mathbb{E}_\rho [\text{size}_b(H_\rho)] \cdot \varepsilon + \Pr_\rho[\varphi\rho \text{ is not good}] \leq \varepsilon + \Pr_\rho[\varphi\rho \text{ is not good}].$$

Note that the right side does not depend on H , so it bounds $\text{corr}_k(g_\varphi^a)$, and averaging over φ gives $\mathbb{E}_\varphi \text{corr}_k(g_\varphi^a) \leq \varepsilon + 4\varepsilon = 5\varepsilon$, which is $2^{-\Omega(m)}$. $\square$

Now we are ready to prove the main theorem.

Proof of Theorem 1.1. Fix $d \geq 3$. By Lemma 2.1 with $\kappa = 1/128$, the number of clauses per variable is $M = b^{O(b)}$, so $\log(bM) = O(b \log b)$. Hence we can choose $b = \Theta(\log n / \log \log n)$ such that $bM \leq n^{1/(8d)}$. We will show that, for all sufficiently large n , every depth- d circuit for f_n has more than s gates, where $\log s = c(n \log n / \log \log n)^{1/(d-1)}$ for a small constant $c = c(d) > 0$. Also, all the constants in the O - and Θ -notation below depend only on d .

Applying Lemma 2.3 for functions of the $2n$ variables x and y gives $k = \Theta(\log s)$ and q with $1/q = \Theta(\log^{d-3} s)$. Let $p = b/(64k)$, as in Lemma 4.4, and let

$$m = qpn = \frac{qbn}{64k} = \Theta\left(\frac{bn}{\log^{d-2} s}\right) = \Theta\left(\frac{(bn)^{1/(d-1)}}{c^{d-2}}\right).$$

For large n , we have $n^{1/(d-1)} \leq m \leq n^{3/5}$, and $bM \leq n^{1/(8d)} \leq m^{1/8}$. Hence Lemma 4.4 gives $a \in \{0, 1\}^{2n-1}$ such that the sign g^a of f_n^a satisfies $\mathbb{E}_\varphi \text{corr}_k(g_\varphi^a) \leq 2^{-\Omega(m)}$, where φ is a q -random restriction of x and y . The constant 1 is a k -CNF, so $|\mathbb{E}[g_\varphi^a]| \leq \text{corr}_k(g_\varphi^a)$, and by (2), $|\mathbb{E}g^a| \leq 2^{-\Omega(m)} \leq 1/3$ for large n , so both f_n^a and $1 - f_n^a$ have expectation at least $1/3$.

Suppose that a depth- d circuit with at most s gates computes f_n . We fix its inputs a as above and get a depth- d circuit on the $2n$ variables x and y with at most s gates that computes f_n^a . If its output gate is an AND gate, we exchange AND and OR gates and negate all literals and constants; by De Morgan's laws, this gives a circuit of the same size and depth with an OR output gate that computes $1 - f_n^a$. As shown above, both f_n^a and $1 - f_n^a$ have expectation at least $1/3$, and their signs g^a and $-g^a$ have the same correlations with k -CNFs, so the two cases are symmetric, and we assume that the circuit has an OR output gate and computes f_n^a . By Lemma 2.3, with probability at least $3/4$ over φ , the function $(f_n^a)_\varphi$ is the OR of at most $s^{O(1)}$ k -CNFs. Each of them, say H , accepts only inputs accepted by $(f_n^a)_\varphi$, so $g_\varphi^a H = H$ and $\mathbb{E}H = \mathbb{E}[g_\varphi^a H] \leq \text{corr}_k(g_\varphi^a)$; hence $\mathbb{E}(f_n^a)_\varphi \leq s^{O(1)} \text{corr}_k(g_\varphi^a)$. For the other restrictions, we use $\mathbb{E}(f_n^a)_\varphi \leq 1$. Averaging over φ by (2), we get

$$\frac{1}{3} \leq \mathbb{E}f_n^a \leq \frac{1}{4} + s^{O(1)} \mathbb{E}_\varphi \text{corr}_k(g_\varphi^a) \leq \frac{1}{4} + s^{O(1)} 2^{-\Omega(m)},$$

so $1/12 \leq s^{O(1)} 2^{-\Omega(m)}$. However, by the bounds on $\log s$ and m above, $m/\log s = \Theta(c^{-(d-1)})$. Hence, if c is small enough, then $s^{O(1)} 2^{-\Omega(m)}$ tends to zero as n grows, contradiction. Thus every depth- d circuit for f_n has more than s gates. $\square$

One can observe that proof above shows that for every fixed $d \geq 3$, the slice f_n^a of a uniformly random a requires depth- d circuits of size $2^{\Omega((n \log n / \log \log n)^{1/(d-1)})}$, except with probability $2^{-\Omega((n \log n / \log \log n)^{1/(d-1)})}$. Since the slices are the bilinear forms $x^\top R y$ given by Hankel matrices R , or equivalently by Toeplitz matrices, this shows that for almost every $n \times n$ Toeplitz matrix R over $\mathbb{F}_2$, the bilinear form $x^\top R y$ requires depth- d circuits of this size.

Also, the proof uses f_n only in [Lemma 4.4](#), so it gives the same bound for every function with a linear number of input bits that has a slice for which [Lemma 4.4](#) holds and the function of [\[Ope26\]](#) also has this property. Hence [Theorem 1.1](#) also holds for their function; for depth three, this improves the exponent $\sqrt{n \log \log n / \log \log \log n}$ given by their argument to $\sqrt{n \log n / \log \log n}$.

5 Upper Bound

Recall that

$$f_n(x, y, a) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{i+j} x_i y_j \bmod 2.$$

Theorem 5.1. *For every fixed $d \geq 3$, the function f_n is computed by a depth- d circuit with $2^{O(n^{2/d})}$ gates.*

Together with [Theorem 1.1](#), this shows that for every fixed $d \geq 3$, the depth- d complexity of f_n is $2^{n^{\Theta(1/d)}}$.

Proof. Let $r = \lceil n^{2/d} \rceil$, and split $\{0, \dots, n-1\}$ into $\ell = \lceil n/r \rceil$ intervals $I_1, \dots, I_\ell$ of at most r consecutive integers. For $\beta, \gamma \in [\ell]$, let $f_{\beta, \gamma}$ be the sum modulo 2 of the summands $a_{i+j} x_i y_j$ of f_n with $i \in I_\beta$ and $j \in I_\gamma$, so that f_n is the parity of the ℓ^2 functions $f_{\beta, \gamma}$. The function $f_{\beta, \gamma}$ depends on fewer than $4r$ input bits, and both $f_{\beta, \gamma}$ and its negation are computed by CNFs with at most 2^{4r} clauses and by DNFs with at most 2^{4r} terms.

Now take a depth- $(d-1)$ circuit with $2^{O(\ell^{2/(d-2)})}$ gates that computes the parity of ℓ^2 bits, one for each pair (β, γ) [\[Hås89\]](#). We replace each of its input literals by the corresponding function $f_{\beta, \gamma}$ or its negation: an AND gate that reads this literal reads the clauses of a CNF for this function instead, and an OR gate reads the terms of a DNF. Then every gate computes the same function of the values of the $f_{\beta, \gamma}$ as before, so the output gate computes f_n and add at most $4\ell^2 \cdot 2^{4r}$ gates. Since $\ell \leq 2n/r \leq 2n^{1-2/d}$, we have $\ell^{2/(d-2)} \leq 4n^{2/d}$, and since $r = O(n^{2/d})$, the circuit has $2^{O(n^{2/d})}$ gates. $\square$

References

- [Ajt83] Miklós Ajtai. Σ_1^1 -formulae on finite structures. *Ann. Pure Appl. Log.*, 24(1):1–48, 1983.
- [Ama23] Kazuyuki Amano. Depth-three circuits for inner product and majority functions. In Satoru Iwata and Naonori Kakimura, editors, *34th International Symposium on Algorithms and Computation, ISAAC 2023, Kyoto, Japan, December 3-6, 2023*, volume 283 of *LIPICs*, pages 7:1–7:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.
- [Baz09] Louay M. J. Bazzi. Polylogarithmic independence can fool DNF formulas. *SIAM J. Comput.*, 38(6):2220–2272, 2009.

- [Bon70] Aline Bonami. Étude des coefficients de Fourier des fonctions de $L^p(G)$. *Annales de l'Institut Fourier*, 20(2):335–402, 1970.
- [Bop86] Ravi B. Boppana. Threshold functions and bounded depth monotone circuits. *J. Comput. Syst. Sci.*, 32(2):222–229, 1986.
- [Cal09] Chris Calabro. *The exponential complexity of satisfiability problems*. PhD thesis, University of California, San Diego, USA, 2009.
- [CIP06] Chris Calabro, Russell Impagliazzo, and Ramamohan Paturi. A duality between clause width and clause density for SAT. In *21st Annual IEEE Conference on Computational Complexity (CCC 2006), 16-20 July 2006, Prague, Czech Republic*, pages 252–260. IEEE Computer Society, 2006.
- [DHM⁺14] Holger Dell, Thore Husfeldt, Dániel Marx, Nina Taslaman, and Martin Wahlén. Exponential time complexity of the permanent and the Tutte polynomial. *ACM Trans. Algorithms*, 10(4):21:1–21:32, 2014. Full version: arXiv:1206.1775.
- [ER60] Paul Erdős and Richard Rado. Intersection theorems for systems of sets. *Journal of the London Mathematical Society*, s1-35(1):85–90, 1960.
- [FSS84] Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Math. Syst. Theory*, 17(1):13–27, 1984.
- [GKW21] Alexander Golovnev, Alexander S. Kulikov, and R. Ryan Williams. Circuit depth reductions. In James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference, ITCs 2021, Virtual Conference, January 6-8, 2021*, volume 185 of *LIPIcs*, pages 24:1–24:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
- [Gol22] Oded Goldreich. Improved bounds on the AN-complexity of $O(1)$ -linear functions. *Comput. Complex.*, 31(2):7, 2022.
- [GPP⁺24] Mohit Gurumukhani, Ramamohan Paturi, Pavel Pudlák, Michael E. Saks, and Navid Talebanfard. Local enumeration and majority lower bounds. In Rahul Santhanam, editor, *39th Computational Complexity Conference, CCC 2024, Ann Arbor, MI, USA, July 22-25, 2024*, volume 300 of *LIPIcs*, pages 17:1–17:25. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.
- [GRSS23] Mika Göös, Artur Riazanov, Anastasia Sofronova, and Dmitry Sokolov. Top-down lower bounds for depth-four circuits. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 1048–1055. IEEE, 2023.
- [GT18] Oded Goldreich and Avishay Tal. Matrix rigidity of random Toeplitz matrices. *Comput. Complex.*, 27(2):305–350, 2018.
- [GT20] Oded Goldreich and Avishay Tal. On constant-depth canonical Boolean circuits for computing multilinear functions. In *Computational Complexity and Property Testing*, volume 12050 of *Lecture Notes in Computer Science*, pages 306–325. Springer, 2020.

- [GW20] Oded Goldreich and Avi Wigderson. On the size of depth-three Boolean circuits for computing multilinear functions. In *Computational Complexity and Property Testing*, volume 12050 of *Lecture Notes in Computer Science*, pages 41–86. Springer, 2020.
- [Hås89] Johan Håstad. Almost optimal lower bounds for small depth circuits. *Adv. Comput. Res.*, 5:143–170, 1989.
- [Hås14] Johan Håstad. On the correlation of parity and small-depth circuits. *SIAM J. Comput.*, 43(5):1699–1708, 2014.
- [HJP95] Johan Håstad, Stasys Jukna, and Pavel Pudlák. Top-down lower bounds for depth-three circuits. *Comput. Complex.*, 5(2):99–112, 1995.
- [IMP12] Russell Impagliazzo, William Matthews, and Ramamohan Paturi. A satisfiability algorithm for AC^0 . In Yuval Rabani, editor, *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2012, Kyoto, Japan, January 17-19, 2012*, pages 961–972. SIAM, 2012.
- [IPZ01] Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *J. Comput. Syst. Sci.*, 63(4):512–530, 2001.
- [Kor26] Oliver Korten. Top-down lower bounds for all depths. *CoRR*, abs/2609.38677, 2026.
- [KPPY84] Maria M. Klawe, Wolfgang J. Paul, Nicholas Pippenger, and Mihalis Yannakakis. On monotone formulae with restricted depth (preliminary version). In *Proceedings of the 16th Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1984, Washington, DC, USA*, pages 480–487. ACM, 1984.
- [KR26] Gülce Kardeş and Benjamin Rossman. On top-down and local lower bounds for AC^0 circuits. *CoRR*, abs/2609.01759, 2026.
- [LR26] Victor Lecomte and Prasanna Ramakrishnan. Optimal shallow circuits for majority. *CoRR*, abs/2609.34029, 2026.
- [LRT22] Victor Lecomte, Prasanna Ramakrishnan, and Li-Yang Tan. The composition complexity of majority. In Shachar Lovett, editor, *37th Computational Complexity Conference, CCC 2022, Philadelphia, PA, USA, July 20-23, 2022*, volume 234 of *LIPIcs*, pages 19:1–19:26. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.
- [LSX26] Daniel Lokshtanov, Saket Saurabh, and Jie Xue. The sparsification lemma via measure and conquer. In *2026 Symposium on Simplicity in Algorithms, SOSA 2026*, pages 291–297. SIAM, 2026.
- [MRW05] Peter Bro Miltersen, Jaikumar Radhakrishnan, and Ingo Wegener. On converting CNF to DNF. *Theor. Comput. Sci.*, 347(1-2):325–335, 2005.
- [O’D14] Ryan O’Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.
- [Ope26] OpenAI. Beyond the Square-Root Exponent for Depth-Three Boolean Circuits. OpenAI Math Release preprint [OAI:Beyond-the-Square-Root-Exponent-for-Depth-Three-Boolean-Circuits-September-23-2026](#), 2026.

- [PPSZ05] Ramamohan Paturi, Pavel Pudlák, Michael E. Saks, and Francis Zane. An improved exponential-time algorithm for k -SAT. *J. ACM*, 52(3):337–364, 2005.
- [PPZ99] Ramamohan Paturi, Pavel Pudlák, and Francis Zane. Satisfiability coding lemma. *Chic. J. Theor. Comput. Sci.*, 1999(11), 1999.
- [Raz09] Alexander A. Razborov. A simple proof of Bazzi’s theorem. *ACM Trans. Comput. Theory*, 1(1):3:1–3:5, 2009.
- [SS12] Rahul Santhanam and Srikanth Srinivasan. On the limits of sparsification. In Artur Czumaj, Kurt Mehlhorn, Andrew M. Pitts, and Roger Wattenhofer, editors, *Automata, Languages, and Programming - 39th International Colloquium, ICALP 2012, Warwick, UK, July 9-13, 2012, Proceedings, Part I*, volume 7391 of *Lecture Notes in Computer Science*, pages 774–785. Springer, 2012.
- [Sub61] B. A. Subbotovskaya. Realizations of linear functions by formulas using $+$, $\cdot$, $-$. *Soviet Math. Dokl.*, 2:110–112, 1961.
- [Val77] Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In Jozef Gruska, editor, *Mathematical Foundations of Computer Science 1977, 6th Symposium, Tatranska Lomnica, Czechoslovakia, September 5-9, 1977, Proceedings*, volume 53 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 1977.
- [Val83] Leslie G. Valiant. Exponential lower bounds for restricted monotone circuits. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA*, pages 110–117. ACM, 1983.
- [Vio09] Emanuele Viola. On the power of small-depth computation. *Found. Trends Theor. Comput. Sci.*, 5(1):1–72, 2009.
- [Yao85] Andrew Chi-Chih Yao. Separating the polynomial-time hierarchy by oracles (preliminary version). In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*, pages 1–10. IEEE Computer Society, 1985.