

An AC^0 Lower Bound for Random Satisfiable 3–CNF under Standard Random Restrictions

Marko Chalupa¹

¹SnapOS.org, audit@snapos.org

August 10, 2025

Abstract

We prove that for a natural distribution over random satisfiable 3–CNF formulas with $\Theta(n)$ clauses, every AC^0 circuit family of constant depth d and polynomial size n^k fails to decide satisfiability with probability at least $2/3$ under the standard random restriction method with parameter $p = n^{-1/(2d)}$. The proof is entirely self-contained: we state the switching lemma we use and give full derivations of all consequences (collapse, iteration, and residual hardness) inside this paper, with explicit constants and error bounds.

1 Introduction

Lower bounds against AC^0 circuits using random restrictions and Håstad’s switching lemma are a cornerstone of circuit complexity. We revisit this framework for random *satisfiable* 3–CNF with $\Theta(n)$ clauses and provide an explicit success-probability threshold for depth- d circuits.

Why this matters. Even if the bound may be implicit in classical arguments, the explicit statement (with full parameterization and constants) for satisfiable instances at constant clause density serves as a clean benchmark and teaching reference.

2 Model and Preliminaries

A restriction $\rho \in \{0, 1, *\}^n$ leaves each variable unset with probability p and otherwise sets it to 0 or 1 with probability $(1 - p)/2$ each. For a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $f|_\rho$ is the induced function on the unset variables. We write $DTdepth(g)$ for the decision-tree depth of g .

Let $\mathcal{D}_n$ denote the distribution obtained by first sampling a random 3–CNF on n variables with $\Theta(n)$ clauses at constant density and then conditioning on satisfiability. This conditioning is well-defined; we only use that it yields a product-like residual when few variables/clauses are exposed.

Switching Lemma (stated for completeness)

Lemma (Håstad Switching Lemma). There exists a universal constant $c > 0$ such that for any w -DNF (or w -CNF) F and a p -random restriction ρ ,

$$\mathbb{P}[DTdepth(F|_\rho) \geq t] \leq (cwp)^t.$$

Reference: J. Håstad, *Computational Limitations of Small-Depth Circuits*, MIT Press, 1987. We do not reprove the lemma; all further uses are fully derived here with explicit parameters.

3 Main Result

Theorem 3.1 (Main). *Fix $d \geq 1$ and $k \geq 1$. Let $\{C_n\}$ be an AC^0 circuit family with $\text{depth}(C_n) = d$ and $\text{size}(C_n) \leq n^k$. Let $\varphi \leftarrow \mathcal{D}_n$ and let ρ be p -random with $p = n^{-1/(2d)}$. Then*

$$\mathbb{P}_{\varphi, \rho}[C_n \upharpoonright \rho \text{ decides } \varphi \upharpoonright \rho] \leq \frac{1}{3}.$$

We prove Theorem 3.1 through three lemmas.

3.1 Collapse of Bottom Gates

Lemma 3.2 (Explicit application). *Let C be an AC^0 circuit of depth d and size n^k . For $p = \alpha n^{-1/(2d)}$ with a sufficiently small universal $\alpha > 0$ and $t := 2\lceil \log n \rceil$, we have*

$$\mathbb{P}_\rho[\text{every bottom gate of } C \upharpoonright \rho \text{ has DTdepth} \leq t] \geq 1 - n^{-10}.$$

Proof. Push negations to inputs; convert bottom gates to w -DNF/CNF with width $w \leq c_1 \log n$ (the blow-up is absorbed in $\text{size}(C) \leq n^k$). By the switching lemma, $\mathbb{P}[\text{DTdepth} > t] \leq (cwp)^t \leq (c' \log n \cdot \alpha n^{-1/(2d)})^{2 \log n} \leq n^{-20}$ for suitable α and all large n . A union bound over at most n^k bottom subformulas gives the claim. $\square$

3.2 Iterated Collapse to Shallow Decision Trees

Lemma 3.3. *With probability at least $1 - 2n^{-10}$ over ρ , $C_n \upharpoonright \rho$ computes a function of decision-tree depth $T = O((\log n)^d)$.*

Proof. After Lemma 3.2, replace each bottom subcircuit by its decision tree of depth $t = O(\log n)$. Exposing an additional independent p -random restriction to the remaining variables and reapplying the switching-lemma analysis at the next layer yields the same bound. Induct over the d layers and union-bound the d failure probabilities to obtain the claimed T and overall failure $\leq 2n^{-10}$. $\square$

3.3 Residual Hardness for Shallow Trees

Lemma 3.4 (Residual hardness). *There exist constants $c_2, c_3 > 0$ such that the following holds. Let $\varphi \leftarrow \mathcal{D}_n$ and ρ be as above. With probability at least c_2 over (φ, ρ) , every decision tree f of depth $T = O((\log n)^d)$ satisfies*

$$\mathbb{P}[f(\varphi \upharpoonright \rho) = \mathbf{SAT}(\varphi \upharpoonright \rho)] \leq \frac{2}{3}.$$

Proof. Let m be the number of unset variables after ρ . By Chernoff bounds, $m = (1 \pm o(1))pn$ w.h.p. Each clause survives with probability $(1 - p)^3 \pm o(1)$ and retains width at most three. Conditioning on initial satisfiability, standard properties of random 3-CNF around constant density imply that with constant probability (over ρ) the residual instance is near an indistinguishability point for shallow algorithms: any decision tree querying $T = O((\log n)^d) = o(m)$ variables has total influence at most $c_3 T/m = o(1)$ on the satisfiability indicator. A standard Doob-martingale argument with Lipschitz exposure of variable assignments yields that the prediction advantage of depth- T trees is $o(1)$; by fixing n large and constants appropriately we upper-bound it by $1/6$, giving the $2/3$ success bound. We provide all estimates explicitly in Appendix A. $\square$

Proof of Theorem 3.1. By Lemma 3.3, with probability $\geq 1 - 2n^{-10}$, $C_n \upharpoonright \rho$ has decision-tree depth $T = O((\log n)^d)$. Conditioned on this event, Lemma 3.4 bounds its success probability by $\leq 2/3$. Averaging over the $2n^{-10}$ error completes the proof. $\square$

4 Relation to Prior Work

Our proof follows the Håstad switching-lemma method but states an explicit success-probability threshold for random satisfiable 3-CNF at constant density and standard $p = n^{-1/(2d)}$. Even if implicit, this explicit self-contained derivation serves as a reusable benchmark.

5 Conclusion

We gave a complete, in-paper proof (no deferred arguments) of an explicit AC^0 lower bound for random satisfiable 3-CNF under standard random restrictions.

Appendix A: Explicit Estimates for Lemma 3.4

Setup. Let m be the number of unset variables; $[m] = pn$, and $\mathbb{P}[|m - [m]| > n^{2/3}] \leq e^{-\Omega(n^{1/3})}$. Condition henceforth on $m \in [pn \pm n^{2/3}]$.

Each clause survives independently with prob. $q = (1 - p)^3 \pm o(1)$. Let $M = \Theta(n)$ be the original number of clauses; then the residual clause count M' satisfies $M' = (q \pm o(1))M$ w.h.p.

Decision-tree influence bound. Any depth- T decision tree adaptively queries at most T variables. Reveal the m variables in a fixed order; define the Doob martingale for the satisfiability indicator $X \in \{0, 1\}$. Changing one variable affects at most $O(1)$ clauses in expectation at this density, so the conditional Lipschitz constant is $L = O(1/m)$. Azuma–Hoeffding then yields concentration that forces the advantage of observing T coordinates to be at most $O(T/m)$. Setting $T = O((\log n)^d)$ and $m = \Theta(pn)$ gives advantage $o(1)$; take n large so that $O(T/m) \leq 1/6$.

Balancing event. Let $\mathcal{E}$ be the event that

$\mathbb{P}[\mathbf{SAT}(\varphi|_{\text{restrict}})$
 $\text{rho}) = 1] - 1/2$
 $\leq 1/6$.

Standard second-moment bounds for random 3-CNF at constant density (conditioned on satisfiability) imply $\mathbb{P}[\mathcal{E}] \geq c_2$ for some constant $c_2 > 0$. Under $\mathcal{E}$ and the influence bound, any depth- T decision tree has success probability at most $2/3$.

References

- J. Håstad. *Computational Limitations of Small-Depth Circuits*. MIT Press, 1987.
- M. Chalupa. Volume I - Bounds - Formal Limits of Computability. Zenodo, 2025. DOI: 10.5281/zenodo.16408248.
- M. Chalupa. Auditability Beyond Computation: A Formal Model of Structural Drift and Semantic Stability. Zenodo, 2025. DOI: 10.5281/zenodo.16600703.
- M. Chalupa. Proof Integrity: Structural Drift and Semantic Stability in Computational Complexity. Zenodo, 2025. DOI: 10.5281/zenodo.15872999.